
GAZİ ÜNİVERSİTESİ
Gazi
1926

ADLİ BİLİŞİM LABORATUVAR KURULUMUNDA STANDARTLAŞMA

HALİL İBRAHİM ARICAN

YÜKSEK LİSANS TEZİ
ADLİ BİLİŞİM ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

HAZİRAN 2024

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Halil İbrahim ARICAN

25/06/2024

ADLİ BİLİŞİM LABORATUVAR KURULUMUNDA STANDARTLAŞMA

(Yüksek Lisans Tezi)

Halil İbrahim ARICAN

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Haziran 2024

ÖZET

Son yıllarda teknolojideki büyüme insan yaşamının da dönüştürülmesinde önemli rol oynamıştır. Bireylerin iletişim şekilleri ve yaşam kaliteleri de bu büyümeye paralel olarak artmıştır. Teknolojik imkânların artması suçlular açısından da kendisini göstermiş ve olay yerinden elde edilen dijital delillerin sayısı artmıştır. Her ne kadar elde edilen dijital delillerin olay yerinde incelenmesi esas olsa da delillerin çok büyük veriler ihtiva etmesi ve incelemenin uzun zaman alması nedeniyle elde edilen deliller adli bilişim laboratuvarlarına gönderilmektedir. Bu noktada elde edilen verilerin güvenilirliği ve yapılan işlemlerin belirli standartlar ve prosedürler çerçevesinde yapılıp yapılmadığı soruları karşımıza çıkmaktadır.

Şu anda adli bilişim laboratuvarları özelinde kabul edilen uluslararası bir standart mevcut değildir. ISO/IEC 17025, laboratuvarlarda test ve kalibrasyon yeterliliği için genel bir standarttır ve adli bilişim laboratuvarlarını akredite etmek için uyarlanmıştır. Bununla birlikte, ISO/IEC 17025, dijital delillerle ilgili pek çok konuyu ele almadan bırakırken, yalnızca sınırlı bir dizi riske değinmiştir. Adli bilişim laboratuvarı gereksinimlerini inceleyen çok az çalışma olmasına rağmen, yeni bir adli bilişim laboratuvarı için güvenli uygulamaların oluşturulması yoğun bir çaba gerektirmektedir. Bu bağlamda çalışmanın amacı, dünya genelinde adli bilişim laboratuvarı standartlarında iyi uygulamalar geliştiren örnekleri inceleyerek ülkemize uygulanabilirliğini değerlendirmek, aynı zamanda bu çalışma kapsamında geliştirilen örnek model dâhil olmak üzere bu standartları yerine getirebilecek bir kılavuz niteliğindeki kriterleri ve yol haritasını belirlemek ve adli bilişim laboratuvarı kuracak olan kurum ve kuruluşlara rehberlik etmek üzere zorluklara yönelik çözüm önerileri sunmaktır.

Bilim Kodu : 92401
Anahtar Kelimeler : Adli bilişim, Adli Bilişim Laboratuvarları, Standardizasyon
Sayfa Adedi : 179
Danışman : Doç. Dr. Nursel YALÇIN

STANDARDIZATION IN ESTABLISHMENT OF DIGITAL FORENSICS LABORATORY (M. Sc. Thesis)

Halil İbrahim ARICAN

GAZİ UNIVERSITY

INSTITUTE OF INFORMATICS

June 2024

ABSTRACT

In recent years, the growth in technology has played an important role in transforming human life. Communication styles and quality of life of individuals have also increased in parallel with this growth. The increase in technological possibilities has also shown itself in terms of criminals and the number of digital evidence obtained from the crime scene has increased. Although it is essential to examine the digital evidence obtained at the crime scene, the evidences obtained are sent to digital forensic laboratories because the evidence contains very large data and the examination takes a long time. At this point, questions arise about the reliability of the data obtained and whether the transactions are carried out within the framework of certain standards and procedures.

Currently, there is no international standard accepted specifically for digital forensic laboratories. ISO/IEC 17025 is a general standard for testing and calibration competence in laboratories and has been adapted to accredit digital forensic laboratories. However, ISO/IEC 17025 has only addressed a limited set of risks, while leaving many issues related to digital evidence unaddressed. Although there are few studies examining digital forensic laboratory requirements, establishing secure applications for a new digital forensic laboratory requires a lot of effort. In this context, the aim of this study is to evaluate the applicability of good practices developed in digital forensics laboratory standards worldwide by examining exemplary cases, including the example model developed within this study, determine a guide of criteria and roadmap that can meet these standards, and provide solutions to challenges in order to guide institutions and organizations intending to establish a digital forensics laboratory.

Bilim Kodu : 92401
Anahtar Kelimeler : Digital forensics, Digital Forensic Laboratories, Standardization
Sayfa Adedi : 179
Danışman : Assoc.Prof. Nursel YALÇIN

TEŞEKKÜR

Yüksek lisans tez çalışmamın yürütülmesi ve sonuçlanmasındaki destek ve katkılarından dolayı danışman hocam, Sayın Doç. Dr. Nursel YALÇIN'a;

Model örnekleri bölümüne katkılarından dolayı değerli arkadaşım Sayın Mustafa GÜNGÖR'e;

Çalışma süresince bana büyük bir sabır gösteren değerli eşim Derya ARICAN ve kızım Duru ARICAN'a en içten en içten sevgi, saygı ve şükranlarımı sunarım.

Halil İbrahim ARICAN

İÇİNDEKİLER

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AFNOR	Association Française de Normalisation (Fransız Standardizasyon Kuruluşu)
AK	Avrupa Konseyi
ANAB	American National Accredition Board (Amerika Ulusal Akreditasyon Kurulu)
ASTM	American Society for Testing and Materials (Amerikan Test ve Malzeme Kurumu)
ATK	Adli Tıp Kurumu
BM	Birleşmiş Milletler
BSI	British Standards Institution (İngiliz Standart Enstitüsü)
CASCO	ISO committee for conformity assessment (ISO Uygunluk Değerlendirme Komitesi)
C-PROC	Europen Council Cybercrime Program Office (Avrupa Konseyi Siber Suç Program Ofisi)
DIN	Deutsches Institut für Normung e.V. (Alman Standardizasyon Enstitüsü)
FBI	Federal Bureau of Investigation (Federal Soruşturma Bürosu)
FSD	File System Dump (Dosya Sistemi Dökümü)
GLACY	Global Action on Cybercrime(Siber Suçlara Karşı Küresel Eylem)
IACIS	The International Association Of Computer İnvestigative Specialists (Uluslararası Bilgisayar Araştırma Uzmanları Birliği)
ICAC	Internet crimes aganist children (Çocuklara karşı işlenen internet suçları)
IEC	International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonu)
IEEE	Institute of Electrical and Electronics Engineer (Elektrik ve Elektronik Mühendisleri Enstitüsü)
ILAC	International Laboratory Accreditation Cooperation (Uluslararası Laboratuvar Akreditasyon İşbirliği)

INTERPOL	The International Criminal Police Organization (Uluslararası Kriminal Polis Teşkilatı)
IOT	Internet of things (Nesnelerin interneti)
ISO	International Organization for Standardization (Uluslararası Standardizasyon Kuruluşu)
ITU	International Telecommunication Union (Uluslararası Telekomünikasyon Birliği)
JISC	Japanese Industrial Standards Committee (Japon Endüstriyel Standartlar Komitesi)
JKDB	Jandarma Kriminal Daire Başkanlığı (Yeni adı Jandarma Kriminal Başkanlığı)
NCB	National Central Bureau (Ulusal Merkez Bürosu)
NIST	The National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)
NSB	National Standart Body (Ulusal Standardizasyon Kuruluşu)
NW3C	The National White Collar Crime Center (Ulusal Beyaz Yaka Suç Merkezi)
QMS	Quality Management Systems (Kalite Yönetim Sistemleri)
SA	Standards Australia (Avusturalya Standartları)
SAE	Society of Automobile Engineers(Otomotiv Mühendisleri Topluluğu)
SDO	Standart Development Organization (Standart Geliştirme Kuruluşu)
SIS	Swedish Standards Institute (İsveç Standartları Enstitüsü)
STK	Sivil Toplum Kuruluşu
SWGDE	Scientific Working Group on Digital Evidence (Dijital Kanıt Üzerine Bilimsel Çalışma Grubu)
TAPPI	The Technical Association of the Pulp and Paper Industry (Amerikan Kâğıt ve Selüloz Derneği)
TC	Technical Committee (Teknik Komite)
TDK	Türk Dil Kurumu
TSE	Türk Standartları Enstitüsü
UNE	Asociación Española de Normalización (İspanya Standardizasyon Kuruluşu)

1. GİRİŞ

Teknolojinin gelişmesiyle veri kaydetme alışkanlıkları, verinin kaydedildiği mecralar ve bu mecralara erişme teknikleri de esaslı ölçüde değişmiştir. Dijital ortamlar asıl, kâğıt ve benzeri ortamlar ise istisna halini almıştır. Teknolojinin sunduğu hizmetler insanların davranışlarını ve dolayısıyla gündelik yaşam pratiklerini de değiştirmelerine neden olmaktadır. Sadece haberleşmenin yanı sıra "anlık mesajlaşma" uygulamalarının insanlara görüntülü konuşma, resim, video, ses kaydı gönderebilme, konum paylaşma vb. gibi kolaylıklar sağlaması da bu uygulamaları çok hızlı bir şekilde popüler hale getirmiştir. Bu cihazlar sürekli olarak daha karmaşık hale gelmekte ve kullanıcılara çok çeşitli hizmetler sunmaktadırlar.

Teknoloji suçlulara yeni suç işleme alanları oluştururken suçla mücadele yöntemlerini de geliştirmiştir. Dijital cihazlardan elde edilen verilerin delil olarak kullanılabilmesi için meydana gelen maddi olayla bağlantısının kurulması gerekmektedir. Klasik delillerin özelliklerini de taşıyan dijital delillerin klasik delillerden toplama, inceleme gibi birçok yönden farkı bulunmaktadır.

Dijital delillerin başka bir özelliği de bilimsel bir şekilde elde edilmiş olmalarıdır. Mahkeme önünde delillerin geçerliliği ancak bilimsel yollarla elde edildiği takdirde değer kazanacaktır. Bahse konu bilimsel yolların yazılı olduğu bir mevzuat yoktur. Fakat yapılan sempozyum, konferans, çalıştay gibi etkinlikler ve bazı kurumların bir araya gelerek yayınladıkları ilke ve standartlar ile kılavuz oluşturulmaya çalışılmaktadır. Dijital delillerden veri elde etme süreci adli bilişim olarak tanımlanmaktadır. Adli bilişim sürecinin ceza muhakemesi çerçevesinde bir bütün olarak incelenmesi gerekmektedir. Bu süreç dinamik bir süreç olup sadece kurallarının ortaya konmasıyla son bulacak bir kavram değildir. Teknolojinin ilerlemesinin kaçınılmaz olduğu günümüzde bilişim kavramının da günden güne değişmesi beklenen bir sonuçtur. Geliştirilen farklı cihazlar, suçların işlenme şekillerinin değişmesi gibi etmenler adli bilişim uzmanlarının da kendini geliştirmesini ve değişikliklere hızlı adapte olmasını sağlamıştır.

Her ne kadar elde edilen dijital delillerin olay yerinde incelenmesi esas olsa da delillerin çok büyük veriler ihtiva etmesi ve incelemenin uzun zaman alması nedeniyle elde edilen deliller adli bilişim laboratuvarlarına gönderilmektedir. Bu noktada elde edilen verilerin güvenilirliği ve yapılan işlemlerin belirli standartlar ve prosedürler çerçevesinde yapılıp yapılmadığı soruları karşımıza çıkmaktadır.

Literatür araştırması yapıldığında adli bilişim aşamalarına yönelik çalışmaların olduğu fakat analizlerin yapıldığı adli bilişim laboratuvarlarının kurulumuna dair çok fazla çalışma olmadığı

görülmüştür. Standartlar, ürün yapımından, organizasyonlar ve ihtiyaçları için bir çerçeve oluşturan malzemelerin tedarikine yönelik hizmetlerin sunulmasına kadar geniş bir faaliyet yelpazesini kapsar. Örneğin, kalite yönetim standartları, kaliteli iş üretmek ve potansiyel başarısızlıkları en aza indirmek için tasarlanmıştır. Ayrıca çalışanların laboratuvar sonuçlarına koyabileceği güveni etkileyen, işlenmemiş riskleri açık bırakan uluslararası belirli bir adli bilişim laboratuvar standardı yoktur.

Bununla birlikte, genel bir standart olan ISO/IEC 17025, test ve kalibrasyon laboratuvarlarının yetkinliği, bir adli bilişim laboratuvarını akredite edecek şekilde uyarlanmaktadır. Bu standardı dijital delilleri işlemeye yönelik özel gerekliliklere uyacak şekilde ayarlamak, alanda uzmanlık gerektirir. Ayrıca, laboratuvarlar için en iyi uygulamalara yönelik başka kılavuzlar da mevcuttur, ancak bu yönergeler laboratuvarlar arasında tutarlılığı garanti etmeyebilir. Her laboratuvar kendi en iyi uygulamalarını ve yönergelerini seçerken, müşterilerine sonuç tutarlılığının genel olarak aktarılacağından emin olamaz. En kötü senaryoda, iki bilirkişi aynı delile dayanarak farklı görüş verebilir.

Ayrıca uygulamada adli bilişim alanında bilirkişilik yapan bazı kişiler laboratuvar ortamında bile çalışmamakta, elinde olan bazı ücretli/ücretsiz yazılımlarla ofis ortamında inceleme yapmaktadır. Elde edilen sonuçların doğru ya da yanlış olmasından bağımsız olarak böyle bir durumda yargı makamlarının nezdinde delilin güvenilirliği kaybolmakta ve hüküm sürecinde delil hiç yokmuş gibi davranılmaktadır.

Günümüzde işlenen suçların büyük bir kısmı dijital bir delil içermektedir. Adli bilişime duyulan ihtiyacın her geçen gün artacağı öngörülmektedir. Bu nedenle hem özel sektördeki firmaların hem de kamu kuruluşlarının bu alanda yapacağı çalışmaların da artması beklenmektedir. Adli bilişim laboratuvarlarının nasıl kurulması gerektiği ve hangi kriterlerin esas alınması gerektiği konularında yapılacak yeni çalışmalara ihtiyaç bulunmaktadır.

Problem durumu / Konunun tanımı

Ulusal ve uluslararası alanda adli bilişim laboratuvarlarının kurulumuna dair herhangi bir standart bulunmamaktadır. Adli bilişim aşamalarının uluslararası birçok standardı mevcuttur. Fakat buna rağmen adli bilişim laboratuvarlarının kurulum esaslarına dair kabul görmüş bir standart bulunmamaktadır.

Araştırmanın Amacı

Çalışma kapsamında, standardizasyon kavramının önemi ve standartlara yönelik ulusal ve uluslararası kapsamda çalışma yapan kurum ve kuruluşların incelenmesi; adli bilişim laboratuvarlarının kurulması konusunda en iyi uygulamalar rehberi hazırlayan kurumların modellerinin gözden geçirilmesi; bu modellerin karşılaştırılarak ülkemizde nasıl bir yol izlenebileceğinin değerlendirilmesi ve adli bilişim laboratuvarı kuracak olan kurum ve kuruluşlara bir rehber olması amacıyla model önerisi sunulması amaçlanmaktadır. Araştırma sırasında aşağıdaki sorulara cevap aranması hedeflenmektedir:

1. Adli bilişim laboratuvarı kurmak isteyen bir kurum/kişi hangi etkenleri düşünerek işe başlamalıdır?
2. Adli bilişim laboratuvarı kurulum esasları hakkında uluslararası alanda kabul görmüş bir dizi standart mevcut mudur?

Araştırmanın önemi

Adli bilişim laboratuvarlarının kurulumu konusunda yapılan literatür araştırmalarında çok az sayıda çalışmaya rastlanmıştır. ISO/IEC 17025, test ve kalibrasyon laboratuvarlarının yetkinliği standartları genel olarak bir standart olup adli bilişim laboratuvarları kurulumu için tam olarak gereken kriterleri sağlamamaktadır. Bu nedenle adli bilişim laboratuvarları özelinde farklı ve yeni bir dizi standart gerekmektedir.

Uluslararası alanda adli bilişim laboratuvarlarının kurulması konusunda kamu kurumu ve özel kuruluşların yaptığı birtakım rehberler mevcuttur. Ayrıca bazı üniversitelerin adli bilişim laboratuvarı kurma çalışmaları akademik makalelere dönüştürülmüştür. Ülkemizde adli bilişim laboratuvarı kurmak isteyen herhangi bir kurum ya da kuruluşun yararlanabileceği bir çalışma bulunmaması nedeniyle yapılacak olan bu çalışma bu alanda yapılmış ilk çalışma olacaktır.

Sınırlılıklar

Çalışmanın, adli bilişim laboratuvarları kurulumunda esas olan laboratuvar yönetimi, iş akış süreçleri ve kalite gereklilikleri konularını içermesi çalışmanın sınırlılıklarındandır. Yazılım ve donanım konusunda belirli marka ve firma isimleri kullanılmayacaktır.

Yapılacak olan çalışmadan laboratuvar yönetimi kapsamında laboratuvarın fiziki yapısı, tesisleri, personel görev tanımları, çeşitli bölümlere giriş yetkileri, iş güvenliği, laboratuvarda bulunması gereken yazılım ve donanımlar ile kullanılan ekipman incelenecektir.

Gelen vakanın incelenmesi kapsamında ise talep makamlarından gelen inceleme istekleri, bulgunun laboratuvara girdiği andan itibaren takip edilen süreçler (kayıt altına alınması, fotoğraflanması vb.), son olarak ise laboratuvardan çıkış işlemleri incelenerek dikkat edilecek hususlar ortaya konacaktır.

Kalite gereklilikleri kapsamında uygulanan metotların kalite standartları ve akreditasyon sistemi incelenecektir.

Araştırmanın Kapsamı

Adli bilişim laboratuvarlarının kurulumunda standartlaşma hakkında yapılan bu çalışmada öncelikle adli bilişim kavramı, aşamaları ve laboratuvar kavramları açıklanacaktır. Standardizasyonun ne olduğu dünya genelinde hangi tür standardizasyon kuruluşlarının bulunduğu ve adli bilişime dair literatürde yer alan standartlar incelenecektir. Konunun esas objesi adli bilişim laboratuvarı olduğundan dolayı bu konuda belirli bir standardın olup olmadığı incelenecektir. Direk laboratuvar kurulumu hakkında olmasa da adli bilişime dair var olan standartların hangi konuları kapsadığı ve sınırları incelenecektir. Literatür araştırmasının sonunda ise adli bilişim laboratuvarının kurulumuna dair bugüne kadar çalışılmayan konular var ise onların tespiti yapılacaktır. Herkes tarafından kabul görmüş bir standardın tespit edilememesi halinde ise adli bilişim laboratuvarını kuran ve büyük çapta incelemeler yapan ülkelerin/kurumların bu kurulumu hangi esaslar dâhilinde yaptığı incelenecektir.

Yapılan bu çalışma ile Çalışmanın *"Adli Bilişim ve Adli Bilişim Laboratuvarı Kavramı"* başlıklı ikinci bölümünde; adli bilişim kavramı ve aşamaları, adli bilişim laboratuvarı kavramı, genel özellikleri incelenmektedir.

Çalışmanın *"Standardizasyon"* başlıklı üçüncü bölümünde; standart kavramı, adli bilişim alanında kullanılan standartlar, ISO/IEC 17000 ailesi ve adli bilişim alanında konulan standartların adli bilişim incelemelerini ne kadar karşıladığı konusunda yapılan çalışmalar incelenmekte ve adli bilişim laboratuvarlarının kurulumu konusunda belirli standartların olmadığı olguları ortaya konulmaktadır.

Çalışmanın *"Adli bilişim Laboratuvarı Kurulumu İçin Örnek Modeller"* başlıklı dördüncü bölümünde; çeşitli kurum ve kuruluşların adli bilişim laboratuvarı kurulum esaslarını düzenleyen örnek modelleri incelenmektedir.

Çalışmanın *"Adli bilişim Laboratuvarı Kurulumu İçin Model Önerisi "* başlıklı beşinci bölümünde; incelenen modellerin birbirleri ile karşılaştırılması ve Türkiye için uygun olan modelin ya da

karşılaştırma sonucunda ortaya çıkacak yeni bir modelin (hibrit) tasarlanması, hangi kurumlar (özel,kamu) için uygun olabileceği konuları incelenmektedir.

Çalışmanın *"Sonuç ve Öneriler"* başlıklı altıncı bölümünde; adli bilişim laboratuvarlarının kurulumunda standartlaşmanın önemine ilişkin sonraki çalışmaların ne olabileceği hakkında öneriler sunulmakta, genel değerlendirmelerde bulunulmaktadır.

Tanımlar

Bulut Tabanlı Adli Bilişim İncelemeleri: Adli bilişim incelemelerinin bulut ortamında icra edilmesidir.

Chip-off: .Elektronik cihazın bellek yongasının çıkarılarak verilerin yongadan alınması işlemidir. Hassas ve ince işçilik gerektiren bir yöntemdir.

Dosya Sistemi ve Mantıksal Kopya Alma Yöntemi: Cep telefonunun içeriğindeki mevcut veriler ile silinmiş verilerin bir kısmının tespit edilebildiği kopya alma yöntemidir.

Fiziksel Kopya Alma Yöntemi: Cihaz içerisindeki mevcut ve silinmiş verilerin tespit edilebildiği kopya alma yöntemidir.

Jail Breaking: IOS işletim sistemine sahip cihazlarda, verilerin kurtarılması üreticinin cihaz için tasarladığı standart uygulamaların dışında bir uygulamanın cihaza yüklenerek cihazın tam kontrolünün ele alınmasıdır.

JTAG: Elektronik cihazın hiç sökülmeden ana kart üzerindeki belirli noktalara temas sağlanarak yapılabilen bir veri çıkarma yöntemidir.

Triyaj: Çok büyük kapasiteli elektronik delillerin incelemesinde yapılan önceliklendirme yöntemidir. Zamanın kısıtlı olduğu ya da durumun kritik olduğu olaylarda sadece istenen verinin çıkarılması için diğer inceleme yöntemlerinin atlanarak daha pratik bir incelemenin yapılmasıdır.

Uygulama (Application): Belirli özellikleri bir kullanıcının erişebileceği bir şekilde bir araya getiren yazılımdır.

Wear-levelling (Aşınma Dengeleme): Aşınma dengeleme, hiçbir hücrenin diğerinden daha hızlı yıpranmaması için SSD'deki (Katı Hal Sürücüsü) tüm hücrelerin eşit şekilde kullanılmasını sağlayan bir işlemdir. Aşınma dengeleme, her hücrenin kaç kez yazıldığını veya silindiğini takip ederek ve hücrelerin kullanımını dengelemek için verileri hareket ettirerek çalışır.

Write-amplification: Bir SSD'nin (Katı Hal Sürücüsü) üzerine veri yazma işlemi sırasında meydana gelen ve yazılan veri miktarının işletim sistemi tarafından istenenden fazla olmasını ifade eder. Bu durum, veri silme ve yeniden yazma işlemlerinden kaynaklanır.

2. ADLİ BİLİŞİM VE ADLİ BİLİŞİM LABORATUVARI KAVRAMI

Çalışmanın bu bölümünde adli bilişim kavramı, aşamaları; adli bilişim laboratuvarı kavramı, Türkiye'deki adli bilişim laboratuvarları ve dünya genelindeki laboratuvarlar incelenmektedir.

2.1. Adli Bilişim Kavramı

Bilişim sistemlerinin insan hayatına girdikten sonra işlenen suçlarda sıkça kullanılması ve suçun aydınlatılması için suçta kullanılan cihazların içindeki verilerin zarar görmeden analiz edilmesi işlemi "adli bilişim" olarak tanımlanmaktadır. Adli bilişim kavramının doktrinde birçok tanımı mevcuttur.

Yargı makamında delil olarak kullanılmak üzere sayısal cihazların ve bilişim sistemlerinin içindeki verilerin bilimsel olarak analiz edilmesidir (Busing ve diğerleri, 2005). Adli bilişim davada tarafların iddialarını doğrulayan ya da çürüten elektronik cihazlarda bulunan bilgileri yargı makamının önüne getirmeye yarayan bir analiz faaliyetidir (Keser Berber, 2004).

Adli bilişim kavramı ilk zamanlarda bilgisayar adli bilişimi (computer forensics) olarak doktrinde yer almasına rağmen teknolojinin gelişmesi ve veri barındıran türlü cihazların çıkmasıyla genel anlamda adli bilişim (digital forensics) olarak adlandırılmaya başlanmıştır.

Diğer bir tanıma göre adli bilişim tek bir disiplinden ibaret değildir. Bilgisayar alanında uzman kişiler, kolluk kuvvetleri, yargı makamları, hukukçular, kalite standartları konusunda çalışan firmalar ve kurumların bir araya gelerek oluşturdukları disiplinler arası bir alandır (Buchholz ve Spafford, 2004).

Adli bilişim adli bilimlerin alt branşını oluşturan bir disiplin olup yıllardır var olan adli kimya, adli biyoloji, adli tıp gibi bilimlere kıyasla yeni bir alandır. Adli bilişim delil ile ilk temas anından itibaren yargı makamlarının huzuruna çıkana kadar olan süreci kapsamaktadır. Adli bilişim disiplininin gelişimini tamamladığını söylemek zordur. Çünkü teknoloji sürekli gelişmekte ve üretilen cihazlar içlerinde yeni kabiliyetler barındırmaktadır. Örneğin on beş yıl öncesine kadar bulut teknolojisi diye bir kavram insan hayatında yokken şimdi işlenen suçlarda şüphelinin bulut hesaplarına girilebilmekte ve delil elde edilmektedir.

Adli bilişim süreci sadece veri barındıran cihazın içindeki verilerin çıkartılması işlemi değildir. Aynı zamanda bilişim sistemlerine yöneltilen tehditlerin tespit edilmesi ve önlenmesine ilişkin faaliyetleri de kapsamaktadır.

Sayısal delillerin takdiri ve değerlendirilmesi yargı makamlarının konusu iken toplanması, zarar görmelerinin önlenmesi ve sistematik bir şekilde sunumu adli bilişimin alanına girmektedir (Orta, 2015). Adli bilişimin çalışma alanları gün geçtikçe artmaktadır. Yukarıda da belirtildiği üzere önceden sadece bilgisayar ve içinden çıkan sabit diskler adli bilişim açısından incelenmekteyken günümüzde akıllı bir buzdolabının bile veri depolaması ve adli bir olayı aydınlatmak için incelenebilmesi mümkün hale gelmiştir.

Adli bilişimin çalışma alanları aslında sayısal veri elde edilebilecek bütün ortamlar olabilir. Bu alanların her biri ayrı bir uzmanlık bilgisi gerektirmektedir. Kısaca adli bilişimin çalışma alanlarını şu şekilde sıralayabiliriz;

- ✓ Bilgisayar Analizi
- ✓ Mobil Cihaz Analizi
- ✓ Ağ Analizi
- ✓ Web Analizi
- ✓ Bulut Tabanlı Alan Analizi
- ✓ Iot Cihaz Analizi (Nesnelerin İnterneti)
- ✓ Veritabanı Analizi

Bu çalışma alanlarında yapılan işlemleri şu şekilde özetlemek mümkündür;

- ✓ Sistem (işletim sistemi veya uygulama) kayıtlarının incelenmesi
- ✓ Farklı sistemler arasında kayıt ilişkilendirilmesi ve olay/işlem takibi
- ✓ Veri saklama
- ✓ Veri kurtarma
- ✓ Veri dönüştürme
- ✓ Veri imha etme
- ✓ Şifreleme, şifre çözme
- ✓ Gizlenmiş dosya bulma

Ayrıca adli kelimesi ile birlikte kullanılması adli bilişimin sadece adli olaylarda kullanıldığı anlamına gelmemektedir. Kamu ve özel sektörde de birçok firma ve kurum çok büyük hacimdeki bilgilerini saklamak, güvenli bir dijital yapı oluşturmak, olası bir veri kaybı durumunda silinen verileri kurtarmak gibi işlemler için adli bilişim yöntemlerini kullanmaktadır (Şengül ve diğerleri, 2014).

2.2. Adli Bilişim Aşamaları

Adli bilişim süreci delillerin toplanmasından mahkeme önüne getirilmesine kadar olan süreci kapsamaktadır. Adli bilişim incelemesi, her safhasında belirli, bilimsel olarak doğrulanmış tekniklerin kullanıldığı bütünsel bir kavramdır.

Sayısal delillerin yargılama makamının önüne gelene kadar korunması fiziksel ve elektronik koruma olarak ikiye ayrılmaktadır. Elektronik koruma, delillerin bütünlüğünün bozulmaması, herhangi bir silinme, bozulma, yer değiştirme olmamasını ifade eder. Sayısal delillerin en büyük dezavantajı çok hassas olmaları ve küçük bir hata sonucunda bile geri döndürülemez şekilde tahrip veya tahrif edilmeleridir. İncelemelerin kopyalar üzerinde yapılması ve yazma korumalı cihazlar kullanılması elektronik koruma kapsamında yapılacak işlemlerden birkaçıdır. Fiziksel koruma ise bahse konu veri barındıran cihazın fiziksel olarak korunmasıdır. Herhangi bir şekilde düşürülmemesi, darbe almaması vb. önlemler fiziksel korumaya yönelik önlemlerdir (Gözüşirin, 2011).

Adli bilişim faaliyeti sadece cihazın kopyası (imaj) alınarak içindekileri ortaya çıkarmak değildir. Şüphesiz imaj alma bu sürecin en önemli faaliyetlerinden biridir. Fakat delillere ulaşma aşamasında adli bilişim uzmanının ve olay yerindeki kolluğun rolü çok büyüktür. Sayısal deliller gözle görülemeyen delillerdir. Delilleri görülebilir hale getirilebilmek için çeşitli donanım ve yazılımlar kullanılmaktadır. Sayısal delillere uygulanan işlemlerin kaydedilmesi ve işlem geçmiş raporunun oluşturulması çok önemli bir faaliyettir. Adli bilişim yazılımlarının sürümlerine göre değişik sonuçlar verdiği göz önünde bulundurulmalı ve kullanılan yazılımların sürümleri belirtilmelidir. Sonradan inceleme yapacak başka bir uzmanın da bu süreci test etmesi ve aynı sonuçlara ulaşması gerekmektedir. Aksi halde yanlış bir müdahale sonucunda sehven ya da kasten delillerin yok edilmesi ya da tahrif edilmesi bilirkişinin duruma göre hukuki, idari ya da cezai sorumluluğunu doğuracaktır.

Adli bilişim sürecinin temelde olay yeri ve laboratuvar olmak üzere iki ayağı mevcuttur. Ülkemizde uygulamada olay yerinde adli bilişim uzmanı, personel yetersizliğinden dolayı olmamaktadır. Olay yeri safhasını temel adli bilişim eğitimi almış olay yeri inceleme uzmanları yürütmektedir. Laboratuvar safhasını ise alanında yetkin adli bilişim uzmanları yürütmekte olup iki safhanın da birbirinden önemli olduğu söylenebilir. Adli bilişim aşamalarını temel olarak dört safhada ele almak mümkündür. Bunlar sayısal delillerin toplanması, incelenmesi, analizi ve raporlanması aşamalarıdır. Literatürde bu aşamalar değişik isimlerle adlandırılmıştır. Bu aşamaları 3 başlık altında inceleyen yazarlar da vardır (Henkoğlu, 2020). Keser bu safhalara belge hazırlama safhasını ekleyerek beş aşamada incelemiştir (Keser Berber, 2004). Ayrıca bazı yazarlar muhafaza, kurtarma aşamalarını ekleyerek 6 aşamada

incelemişlerdir (Kleiman, 2011) . Bu çalışmada adli bilişim aşamaları temel olarak toplama, inceleme, analiz ve raporlama başlıkları altında incelenecektir.

2.2.1. Toplama

Toplama safhasında verilerin tanımlanması, elde edilmesi alt safhaları mevcuttur. Bu safha genel olarak toplanacak verinin niteliği, bulunduğu yer, verinin toplanma metoduna ilişkin planlama safhasıdır. Ayrıca cihazların kopyalarının alınması, kopyası alınamayan ya da laboratuvar incelemesi gerektiren cihazların paketlenmesi ve nakli de bu aşamada gerçekleşmektedir. Çoğu yazar bu aşamanın en önemli aşama olduğunu, bu aşamada yapılacak bir hatanın geri dönüşü olmayacağını belirtmektedir. Sürecin gerektirdiği hukuki izinleri almak, olay yeri muhafazası ve kolluğun faaliyetleri bu aşamanın içindedir (Sansurooah., 2006).

Bilişim sistemleri işlenen bir suçta bir amaç ya da suçun işlenmesi için bir araç olabilmektedir. Suç yolu olarak bilinen kavramda bir suçun icra edildiği bir kaynak noktası gerçekleştirildiği bir hedef noktası ve bu ikisi arasında bir yol olduğu düşünüldüğünde sayısal delillerin toplanması, bu yol üzerinde bırakılmış birtakım elektronik iz, emare ve kalıntıları tespit etmekle başlamaktadır (Stephenson., 2002).

Ülkemizde sayısal delillerin nasıl toplanacağına ilişkin yasal bir düzenleme bulunmamaktadır. Ülke genelinde yapılan çalıştay, konferans, panel gibi etkinliklerle yol haritası çizilmeye çalışılmış ayrıca yabancı devletlerin mevzuatlarından kıyas yoluyla uygulamalar geliştirilmiştir. Bunun nedeni adli bilişim incelemelerinin diğer bilimlere kıyasla yeni olması ve ülkemizdeki bilişim sistemlerin altyapısının zayıf olmasıdır. Sayısal delillerin toplanmasında tavsiye edilen, delillerin adli bilişim uzmanlarınca toplanmasıdır. Fakat uygulamada adli bilişim uzmanı sayısı yetersiz olduğundan dolayı olay yeri inceleme ekipleri tarafından deliller toplanmaktadır. Müdahale mümkün olan en az sayıda kişiyle yapılmalı ve yetkisiz kişilerin sayısal delille teması önlenmelidir. Öncelikle bilişim sisteminin bulunduğu yerin kablo bağlantılarının ve bilgisayar tertibatının fotoğrafları çekilmelidir. Ayrıca hangi cihazların nerelere bağlı olduklarının bir tutanakla kayıt altına alınması gerekir. Bahse konu sayısal delile uzaktan erişim yoluyla ulaşılabileceği göz önüne alınarak internet bağlantısı ya da kurum içi ağ (intranet) bağlantısı kesilmelidir. İncelenecek elektronik cihazın yanında şifre vb. olabilecek notlara dikkat edilmeli ve kayıt altına alınmalıdır. Olay yerindeki açık bilgisayar üzerindeki RAM bellekte ve ağ üzerinde bulunan uçucu veriler toplanmadan bilgisayarlar kapatılmamalıdır. Bilgisayarların kapatılma şekli de önem arz etmektedir. Bazı işletim sistemleri (Örn. Linux) son komutları belleğinde tutmaktadır. Bilgisayar fişinin direk çekilmesi bu son komutlara ulaşılmasını imkânsız hale getirebilir.

Bilgisayara yüklenmiş bazı uygulamalar bilgisayar doğru kapatılmadığında hafızasındaki verileri otomatik olarak silmektedir. İşletim sistemi ve yüklü uygulamalar değerlendirilerek bilgisayar kapatılmalıdır. Aynı şekilde kapalı cihazlara rastlanıldığında bilgisayar açılmamalıdır (Moore, 2013).

Olay yerinde sadece bilişim cihazları değil bu cihazlardan alınan çıktıların da bir sayısal delil olduğu göz önünde bulundurulmalıdır. Bu deliller de usulüne uygun şekilde toplanmalı ve paketlenmelidir. Ayrıca toplama aşamasına kadar hiçbir delile dokunulmamalı, bilgisayar faresinin (mouse) oynatılması gibi en küçük bir müdahalenin bile bilgisayarlarda değişiklik yarattığı göz önünde bulundurulmalıdır. Sayısal delillerin hassas olmasından dolayı delilin güvenilirliğine şüphe düşürecek davranışlardan kaçınılmalıdır (Başlar, 2015).

Olay yerinden toplanan sayısal deliller usulüne uygun bir şekilde etiketlenmeli ve kayıt altına alınmalıdır. İlk durumda olay yerinde çekilen video kayıtları ve fotoğrafların daha sonra sistemi tekrar birleştirme ihtiyacı duyulduğunda yardımcı olacağı unutulmamalıdır.

Sayısal delillerin üzerlerinde başka kriminalistik incelemeler (parmak izi, biyoloji) yapılabileceği göz önünde bulundurulmalı ve ona göre önlemler alınmalıdır. İmkân olduğu sürece sayısal deliller anti-statik paketlere konulmalıdır. Bu mümkün değilse plastik kutular yerine karton kutu ve zarflar tercih edilmeli herhangi bir çarpma ve düşme durumuna karşı sağlam bir şekilde paketlenmelidir. Sabit disk, CD, DVD gibi sayısal deliller katlanmamalı ve bükülmemelidir. Üzerine yapıştırılacak etiketlerin özelliklerini bozabileceği düşünülerek etiketleme işlemi yapılmalıdır (Mukasey ve diğerleri, 2009).

2.2.2. İnceleme

İnceleme aşaması eğer olay yerinde kopyalama işlemi yapılmadıysa (uygulamada çoğunlukla olay yerinde kopya alma işlemi yapılmamaktadır) delillerin birebir kopyalarının alınacağı aşamadır. Alınacak kopya fiziksel ya da mantıksal kopya olabilir. Fiziksel kopya dosyaların derinliğine incelenmesi, tüm kullanılmamış alanların incelenmesi ve silinmiş verilerin geri getirilmesi süreçlerini kapsar. Mantıksal kopya ise cihazın özelliğine göre içindeki mevcut dosyaların çıkartılması ve bazı silinmiş dosyaların geri getirilmesini işlemlerini kapsar (Sansurooah., 2006).

Sayısal delillerin toplanma aşamasından sonra delillerin incelenmesi aşamasına geçilmektedir. Sayısal delillerin çözümlenmesi kopyanın alınmasından hemen sonra yapılmamaktadır. Alınan kopyanın üzerinde birtakım inceleme faaliyetleri yapılarak suça konu olayla ilgili olabileceği değerlendirilen veriler ayrı bir bölüme alınmaktadır. Bu aşama olay yeri inceleme ekiplerinde yeterli teçhizat ve

donanım olmaması ve inceleme faaliyetinin adli bilişim alanında yüksek bir tecrübe gerektirmesinden dolayı genellikle laboratuvar ortamında yapılmaktadır.

Bu aşamada yapılacak işlemler genel olarak silinmiş verilerin kurtarılması, verilerin tanımlanması ve verilerin içeriklerinin araştırılmasıdır. Suça konu dosyalar belirlenerek farklı bir bilgisayar ortamına alınmakta diğer olayla ilgisi olmayan verilerden arındırılmaktadır.

Sayısal delillerin incelenmesi adli bilişim uzmanının kendisini yaptığı manuel arama ve adli bilişim yazılımlarının yaptığı otomatik aramadan oluşmaktadır. Veri depolayan cihazların kapasitelerinin gün geçtikte arttığı düşünüldüğünde otomatik arama uygulamada sıklıkla tercih edilmektedir. Manuel arama adli bilişim uzmanının belirli kıstaslar çerçevesinde kopya içindeki bütün dosyaları gözden geçirmesi demektir. Bu işlem çok uzun sürmekte ve bütün verilerin kontrol edilmesi şüphelinin suçla alakası olmayan kişisel verilerini de kapsadığı için özel hayatın gizliliğine orantısız müdahaleyi oluşturmaktadır. Otomatik arama ise yazılımlara girilen birtakım parametreler doğrultusunda yazılımın kopya içinden eşleştirdiği verileri çıkararak kullanıcıya sunmasıdır. En yaygın kullanılan otomatik arama uygulaması "anahtar kelime arama metodu" olarak karşımıza çıkmaktadır. Tek bir kelime ya da birden çok kelime içeren bir liste kopya üzerinde yazılım vasıtası ile aranmaktadır. Çıkan sonuçlar üzerinden inceleme yapan uzman yine bir ayıklama işlemini manuel olarak kendisi yapmaktadır (Değirmenci, 2014).

Yapılan aramaların sonucunda birtakım şifreli dosyaların ya da silinmiş verilerin gözden kaçabileceği unutulmamalıdır. Bu nedenle arama yapılmadan önce alınan kopyaya birtakım işlemler uygulanarak tüm dosyalar üzerinde arama yapılması sağlanmaktadır. Bunlar silinmiş verilerin kurtarılması, şifreli verilerin şifrelerinin kırılması ve gizlenmiş verilerin açığa çıkarılması işlemleridir.

2.2.3. Analiz

Analiz aşaması kopya üzerinden çıkan verilerin bahse konu suç oluşturan olay ile alakasının incelendiği ve bağlantı kurulduğu aşamadır. Bu aşamada uygulama günlükleri, dosya üst bilgisi ve zaman mühürleri doğrulukları test edilirken adli bilişim yazılımları ile dosyalar analiz edilir (Sansurooah., 2006).

Bu aşamada cihazlardan elde edilen tüm verilerin (silinmiş, gizlenmiş dahil) inceleme konusu suç ile irtibatları ortaya çıkartılmaya çalışılmaktadır. Maddi olayın oluş şekli, zamanı, kimler tarafından gerçekleştiği konularının elde edilen veriler ile ispat edilmesi ya da desteklenmesi analiz aşamasının amacıdır. Aynı şekilde elde edilen veriler kişilerin masumiyetini de kanıtlayabilmektedir. Örneğin

şüphelinin işlenen suç zamanı olay yerinde olmadığının ispatlanması için cihazdaki konum bilgileri kullanılabilir. Cihazdan elde edilen sayısal verilerin maddi olay ile bağlantısı kurulduğu anda delil niteliği kazanmakta ve yargılama safhasına kadar muhafaza edilmektedir. Analiz işlemi genellikle laboratuvar ortamında yapılan bir işlemdir.

İncelemeyi yapan adli bilişim uzmanlarının analiz işlemine geçmeden önce suç konusu olayla ilgili hangi verileri toplayacağını, hangi bölümlerde ne çeşit verilerin saklandığını bilmesi gerekmektedir (Duman, 2012).

Verilerin zaman unsuru değerlendirilerek bir sıraya konulması, olayın tekrar yapılandırılması için esastır. Örneğin elde edilen sosyal medya konuşmalarının zaman damgalarına bakılarak bir sıraya konmasının olayla ilgili anlamlı sonuçlar çıkarması mümkündür (Olsson ve Boldt, 2009).

Son olarak analiz aşamasında yapılacak her işlemin de belgelenmesi gerekmektedir. Yazılımların sonucunu gösteren cihaz çıktıları yazılımın sürümünü, analizin zamanı gibi birçok bilgiyi de içinde barındırmaktadır. Bu kayıtların, yapılan işin güvenilirliğini ve bilimselliğini sağlayacağından dolayı mahkeme safhasında önemi çok büyüktür (Orta, 2015).

2.2.4. Raporlama

Son aşama olan raporlama aşaması adli bilişim uzmanının ulaştığı sonuçları belirli sorulara cevap verecek şekilde mahkemeye sunmak üzere rapora dökmesidir. Burada yapılan işlemler ve kullanılan metotlar detaylıca açıklanır (Kaya, 2019). Kullanılan dil bilişim uzmanı olmayan herkesin anlayabileceği teknik terimlerden olabildiğince arınmış ve akıcı bir dil olmalıdır (Sansurooah., 2006).

Analizi yapılan sayısal delillerin yargılama makamlarına gönderilmesi için yapılan işlerin ve varılan sonuçların bir rapor haline getirilmesi gerekmektedir. Savcı ya da hâkim rapora bakarak hukuki bir değerlendirme yapacağı için kişinin mahkûmiyetinin ya da masumiyetinin ispatlanmasında raporlama aşaması çok önemli bir yer tutmaktadır (Çakır ve Kılıç, 2013).

Elde edilen veriler ile maddi olay arasındaki irtibatı sağlamak kadar bunu adli bilişim alanında bilgisi olmayan diğer kişilere aktarmak çok önemlidir. Çünkü yapılan analiz sonuçlarının hukuki anlamda bir değer taşıması için yargılama makamlarının bu analizleri anlaması ve hukuki değerlendirmeleri kendilerinin yapması gerekmektedir (Kutcha, 2002).

Adli bilişim uzmanları incelemelerini nasıl yaptıklarını, vardıkları sonuca nasıl ulaştıklarını, verilerin nerelerden elde edildiğini, hangi donanım ve yazılımları kullandıklarını (sürümleri dâhil), raporlarında ayrıntılı bir şekilde belirtmelidir (Değirmenci, 2014).

Analizlerin rapora yansıtılması belli bir mantık silsilesinde olmalıdır. Adli bilişimin amacı geçmişteki maddi olayı yeniden yapılandırarak muhakeme makamlarına yardımcı olmaktır. Bu nedenle raporda belirtilen sonuçların olay akışına göre belirli bir mantık sırasını takip etmesi gerekmektedir. Adli bilişim uzmanının alanında çok iyi bir incelemeci olmasından öte vardığı sonuçları muhakeme süjelerine tutarlı bir akış içerisinde aktarması gerekmektedir (Yetim, 2008).

2.3. Adli Bilişim Laboratuvarı

Günümüzde işlenen bilişim suçlarının içeriklerine bakıldığında gelişen teknoloji ile beraber çok büyük kapasiteli veri taşıma cihazlarının bulunduğu gözlemlenmektedir. Her ne kadar tavsiye edilen yapılacak analizin olay yerinde yapılması olsa da cihazların yüksek miktarda veri taşıma kapasiteleri yüzünden bu işlemler çok uzun saatler gerektirmektedir. Yapılan analizlerin büyük bir çoğunluğu bu nedenle laboratuvarlarda yapılmaktadır. Adli bilişim laboratuvarlarına duyulan ihtiyaç gün geçtikçe artmaktadır.

Adli bilişim laboratuvarlarının kurulması için teknik bilginin yanı sıra eğitim, planlama yönetim maliyet gibi hususların değerlendirilmesi gerekmektedir. Örneğin belirli suç tiplerinin işlendiği bölgeler tespit edilmeli ve o bölgelere gerekli olan incelemeleri (görüntü, ses) yapacak laboratuvarlar kurulmalıdır. Böylelikle maliyet ve etkinlik bakımında kaynakların da doğru kullanılması sağlanmalıdır.

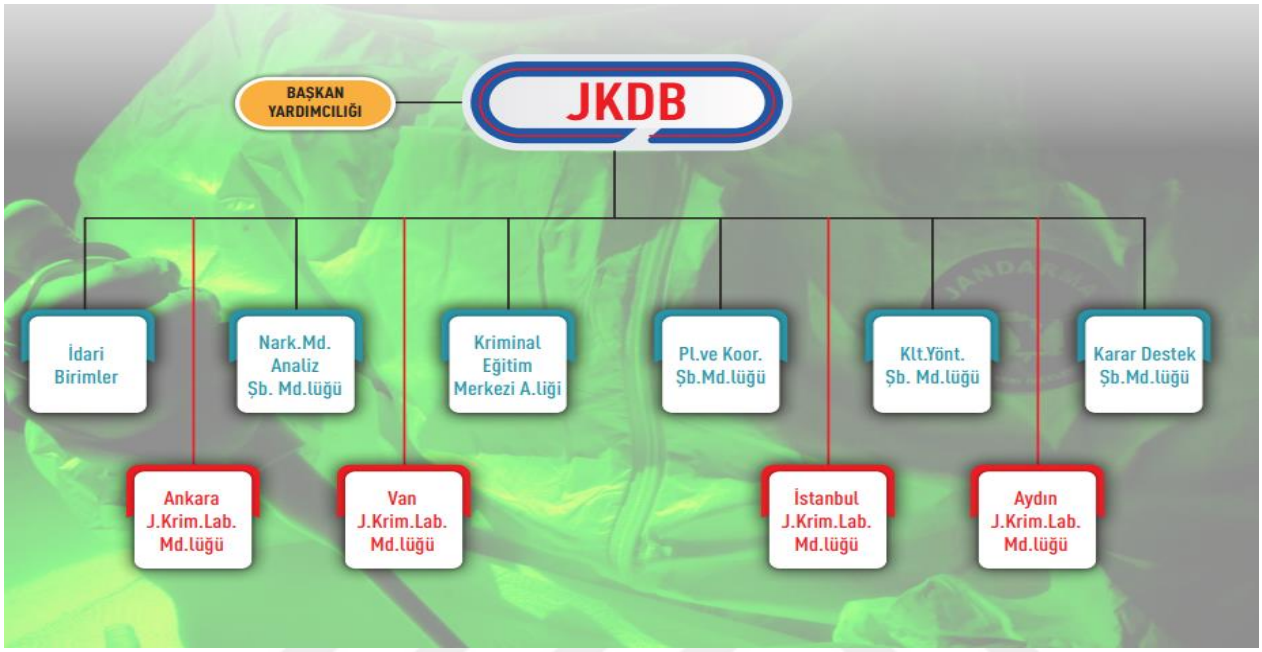
2.3.1. Ülkemizdeki adli bilişim laboratuvarları

Diğer adli bilimlere nispeten yeni sayılan adli bilişim ülkemizde de hızlıca gelişmeye ve konunun önemi gün geçtikçe artmaya devam etmektedir. Adli bilişim incelemesi yapan büyük ve küçük çapta birçok kişi/kurum bulunmaktadır. Bu başlık altında kamu kurumlarının adli bilişim laboratuvarları incelenecektir.

2.3.1.1. Jandarma Kriminal Başkanlığı

Olay yerlerinden elde edilen bulguları incelemek ve bilirkişi raporu yazmakla görevli Jandarma Kriminal Başkanlığı, Jandarma Genel Komutanlığı bünyesinde bulunmaktadır. Kriminal Başkanlığı; Kriminal Eğitim Merkezi, Bilimsel Araştırma ve Destek Birimleri, İdari Birimler, Narkotik Madde

Analiz Şube Müdürlüğü ile İnceleme ve Analiz Faaliyetlerinin Yürütüldüğü Ankara, Aydın, İstanbul ve Van Jandarma Kriminal Laboratuvarlarından oluşmaktadır. Başkanlığın kuruluş şeması Şekil 2.1'de gösterilmiştir.



Şekil 2.1. Jandarma Kriminal Başkanlığı kuruluş şeması

Kaynak: Jandarma Kriminal Başkanlığı (https://www.jandarma.gov.tr/kurumlar/jandarma.gov.tr/Jandarma/Kriminal-Tanitim-KATALOG-020623.pdf)

Jandarma Kriminal Başkanlığı bünyesinde adli bilişim laboratuvarları tek başına bir laboratuvar olarak değil, adli bilimler laboratuvarının bir parçası olarak kurulmuştur. Ankara, İstanbul ve Van laboratuvarlarında adli bilişim laboratuvarı mevcut olup Aydın laboratuvarında ise sadece görüntü incelemeleri yapan bir birim bulunmaktadır.

Laboratuvarların dışında ülke genelinde birçok il jandarma komutanlığı bünyesinde kriminal adli bilişim timleri yer almaktadır. Bu timler kapsamlı inceleme gerektirmeyen vakalarda veri ve görüntü incelemeleri yapmaktadır (Jandarma Kriminal Başkanlığı, 2024).

2.3.1.2. Emniyet Genel Müdürlüğü Kriminal Daire Başkanlığı

Emniyet Genel Müdürlüğü bünyesinde görev yapan Kriminal Daire Başkanlığı ilk kuruluşta küçük bir laboratuvar olarak teşkil edilmiş sonrasında 1998 yılında bağlıları olan kriminal laboratuvar müdürlüklüleriyle beraber kurulmuştur.

Kriminal Polis Laboratuvarı Müdürlükleri sırasıyla; 1962 yılında İstanbul (ilk kuruluş) 1972 yılında İzmir, 1979 yılında Adana, 1981 yılında Samsun, 1983 yılında Diyarbakır, 1985 yılında Erzurum, 1997 yılında Bursa, 2001 yılında Antalya, 2003 yılında Kayseri ve 2004 yılında Ankara olmak üzere toplam 10 ilde bağlı bölgelerine hizmet vermektedirler.

Yine jandarmada olduğu gibi Emniyet Kriminal Daire başkanlığı bünyesinde bulunan adli bilişim laboratuvarları tek başına değil Bölge Kriminal Polis Laboratuvarlarının bir parçası olarak görev yapmaktadır.

Ses-Görüntü-Data İnceleme Şube olarak görev yapan birimler Ankara ve Diyarbakır illerinde bulunmaktadır (Kriminal Daire Başkanlığı, 2024).

2.3.1.3. Adli Tıp Kurumu

1917 yılında Adalet Bakanlığı bünyesinde kurulan Adli Tıp Kurumu ülke geneline yayılmış ihtisas daireleri, il ve ilçe şube müdürlükleri ile adli bilirkişilik hizmeti vermektedir. Bu kurumda adli bilişim laboratuvarı sadece İstanbul'da bulunan merkez teşkilatı altında Adli Bilişim İhtisas Dairesi olarak görev yapmaktadır. Adli Bilişim İhtisas Dairesi altında aşağıdaki birimler yer almaktadır (Adli Tıp, 2024);

- Veri inceleme şubesi
- Mobil cihazlar inceleme şubesi
- Kriptoloji ve elektronik cihazlar inceleme şubesi
- Ses ve görüntü inceleme şubesi
- ARGE şubesi

2.3.2. Dünya genelinde adli bilişim laboratuvarları

Dünya genelinde adli bilişim laboratuvarları çok çeşitli olmakla beraber bunların tam bir sayısını vermek mümkün değildir. Diğer disiplinlere yönelik adli bilimler laboratuvarlarının çoğu, daha büyük bir adli inceleme laboratuvarının parçasıdır ve muhtemelen bir adli bilişim bölümüne sahiptir. Ayrıca,

adli bilişim laboratuvarları, Çocuklara Karşı İnternet Suçları (Internet Crimes Aganist Children-ICAC) laboratuvarları veya Federal, eyalet merkezli emniyet teşkilatlarındaki Bölgesel Adli Bilişim Laboratuvarları ve yerel düzeylerde, genel müfettişliklerde ve savcılıklarda yalnızca dijital delilleri işleyen uzmanlaşmış laboratuvarlarda da bulunmaktadır. Adli bilişim aynı zamanda istihbarat alanında da önemli bir varlığa sahiptir ve genellikle e-Keşif olarak anılan, hukuk davalarında yaygın olarak kullanılmaktadır. Bu genişlik nedeniyle adli bilişim topluluğunun büyüklüğünü tahmin etmek zordur (Lyle ve diğerleri, 2022).

Örneğin Uluslararası Bilgisayar Araştırma Uzmanları Birliği'nin (The International Association Of Computer İnvestigative Specialists-IACIS) eğitim listesinde 2.214 grup yer almaktadır. IACIS, dünya çapındaki adli bilişim ve siber güvenlik topluluğuna eğitim ve sertifikasyon sağlamaktadır ve üyeleri arasında federal, eyalet ve kolluk kuvvetlerinin yanı sıra diğer profesyonel adli bilişim uygulayıcıları da bulunmaktadır (IACIS, 2024).

ANSI Ulusal Akreditasyon Kurulu (American National Accredition Board-ANAB), Kuzey Amerika'daki en büyük akreditasyon organıdır ve adli bilişim laboratuvarları da dahil olmak üzere hem kamu hem de özel kuruluşlara eğitim ve akreditasyon sağlar. Amerika Birleşik Devletleri'ndeki aktif ANAB onaylı kuruluşların 91'i dijital kanıtları incelemektedir (Lyle ve diğerleri, 2022).

Dijital Kanıt Üzerine Bilimsel Çalışma Grubu (Scientific Working Group on Digital Evidence-SWGDE), kılavuz belgelerin geliştirilmesi yoluyla dijital ve multimedya adli toplulukları içinde iletişimi, işbirliğini teşvik etmeyi ve kalite ve tutarlılığı sağlamayı amaçlamaktadır. SWGDE'nin 70 üyesi öncelikle federal, eyalet ve yerel kolluk kuvvetlerinin yanı sıra akademik, kurumsal ve sivil adli bilişim gruplarından gelmektedir (SWGDE, 2024).

Ulusal Beyaz Yaka Suç Merkezi (The National White Collar Crime Center-NW3C), federal, eyalet, yerel kolluk kuvvetleri, savcılık ve düzenleyici kurumlar için yüksek teknoloji suçlarının önlenmesi ve soruşturulmasına yönelik eğitim ve mesleki gelişim kursları sunmaktadır. Bilgisayar adli bilişim, mali ve siber suçlar ve istihbarat analizi konularında eğitim ve analitik teknik destek sağlamaktadır. 2022'deki eğitim katılımcıları listesinde 9700 benzersiz grup listelenmektedir (NW3C, 2024).

Verilen örneklere bakıldığında dünya genelinde adli bilişim topluluklarının çok fazla olduğu açıkça görülmektedir; sadece federal, eyalet ve yerel suç laboratuvarlarında değil aynı zamanda savcılıklarda, özel danışmanlık firmalarında ve kurumsal siber güvenlik operasyonlarında da ufak birimler şeklinde bulunmaktadırlar.

3. STANDARDİZASYON

Çalışmanın bu bölümünde Standardizasyon kavramı açıklanarak standart belirleyen kuruluşlar (ISO,BSI gibi) açıklanacaktır. ISO/IEC 17000 ailesi açıklanacak ve bu standartların adli bilişim incelemelerini ne kadar kapsadığı incelenecektir.

3.1. Kavram

Standartlar modern toplumların vazgeçilmez bir unsuru haline gelmiştir. Ürün ve hizmetlerin belli bir kalitede sunulmasıyla kullanıcılarına güven sağlamayı amaçlamaktadır. Kullanıcılar belirli bir standarda sahip ürün ve hizmetleri kullanırken bu ürün ve hizmetlerin güvenilir olduğuna, beklenen düzeyde çalıştığına ve beklenen sonucu sağlayacağına güvenebilir.

Standart kelimesinin kelime anlamı TDK (Türk Dil Kurumu) sözlüğünde "Bir işletmede, bir ürünü, bir çalışma yöntemini, üretilecek miktarı, bütçenin para miktarını belirlemek için konulmuş kural." olarak tanımlanmıştır (TDK, 2024). Ayrıca TS EN 45020'de standartlar; üzerinde uzlaşı ile oluşturulmuş, yetkilendirilmiş bir kuruluş tarafından onaylanan sürekli tekrar eden faaliyetlerin süreçlerine ilişkin kuralların ve prensiplerin belirlendiği dokümanlar olarak tanımlanmıştır. Yine aynı dokümanda standardizasyon ise belirlenmiş konularda uygulanacak olan standartların oluşturulması, yayınlanması ve uygulanması şeklinde tanımlanmıştır. (TSE EN 45020).

Gönüllü, alanında uzman kişiler ve topluluklar tarafından hazırlanan, üzerinde uzlaşı sağlanmış standartlar, ulusal ve uluslararası altyapılarda, ekonomilerde ve ticarette çok fark edilmese de hayati bir rol oynamaktadır. Adlandırma, tanımlama ve belirleme, ölçme ve test etme, yönetme ve raporlama için üzerinde anlaşmaya varılmış yollar sağlanarak oluşturulan standartlar şunları sağlar:

- ✓ Pazarlar ve pazar geliştirme için temel destek;
- ✓ Ürünlerin, süreçlerin ve hizmetlerin kalitesini, güvenliğini, birlikte çalışabilirliğini ve güvenilirliğini sağlamak için kabul görmüş bir araç;
- ✓ Tedarik için teknik bir temel;
- ✓ Uygun düzenleme için teknik destek
- ✓ Optimizasyon ve en iyi uygulama yoluyla çeşitliliğe ve maliyetin azalması.

Standartların çoğu, teknik konuları (çeliğin işlenmesi, bilgisayar ağları arasında bağlantı, yağların viskozite tayini vb.) ele alırken son otuz yılda birçok kuruluş tarafından artan bir kabul görmüştür.

Gönüllü, mutabakata dayalı standartlar, işletmeye ve genel olarak topluma teknik özellikler, test yöntemleri ve ölçüm protokollerinden çok daha fazla katkıda bulunabilir (Hatto, 2013).

Standartlar ve hukuki düzenlemeler arasındaki en önemli fark hukuki düzenlemelere uymanın zorunlu olmasıdır. Standartlar temel olarak uyulması zorunlu düzenlemeler değildir. Hukuki düzenlemeler, uyulmaması halinde yaptırımlara tabi olabilecek yasal olarak uygulanabilir gereklilikleri belirtirken, standartlar, uyulması gereken herhangi bir yasal yükümlülüğün bulunmadığı ihtiyari kurallardır. Ek olarak, standartlara uyum kavramsal olarak gönüllü olmakla birlikte, dava durumunda, kovuşturmaya yol açan olayın etkisini azaltabilecek veya ortadan kaldırabilecek mevcut bir standarda uyulmaması, davanın reddini gerektiren ya da bulgunun yargı makamları önünde değerlendirilmesini engelleyen ispat vasıtası olarak kabul edilebilir.

Hukuki düzenlemelerin içeriği ve yapısı, en azından demokratik toplumlarda, sıklıkla halkın istişaresine tabi olsa da, bunlar zorunlu olarak demokratik ve uzlaşmaya dayalı bir sürecin sonucu değildir aynı fikirde olmayan kişiler için bile bağlayıcıdırlar. Bununla birlikte, bir kuruluş gönüllü olarak bir standarda uymayı kabul ettiğinde, bunu muhtemelen standardın meşru olduğunu düşündüğü için yapar. Bu meşruiyet, standart geliştirme ve onay süreçlerinde kullanılan prosedürlerden, standardın yayınlanmasından etkilenmesi muhtemel olan paydaşların aktif katılımından, özellikle de yükümlülüğü kabul etmek ve onaylamak için fikir birliğinin kullanılmasından kaynaklanmaktadır. Buna ek olarak, standartların oluşturulmasına katılımın neredeyse her zaman gönüllü olması ve bu nedenle kendi kendine hizmet etmek olarak görülmesi de meşruiyet kavramını desteklemeye yardımcı olur (Hatto, 2013).

Standartlar genel çerçevede resmi ve gayri resmî standartlar olarak ikiye ayrılmaktadır. Resmi olanlar ulusal standardizasyon kuruluşları (National Standart Body, NSB) tarafından yayınlanan standartlardır. Ulusal Standardizasyon Kuruluşları genelde her ülkede bir tane bulunmakta olup bu kuruluşlar bulunduğu ülkede standardizasyon ile ilgili üst kuruluş görevini icra ederler (Tantra, 2016).

Ulusal Standardizasyon kuruluşları herhangi bir konu hakkında standart belirlememektedir. Bu kuruluşlar ihtiyaç halinde teknik komiteler, çalışma grupları ve alt gruplar ile birlikte toplantılar düzenleyerek ilgili konu hakkında toplu bir uzlaşı yaratmaya çalışırlar. Bu süreçlerin hepsi şeffaflıkla yürütülür ve konu hakkında teknik bilgiye sahip kişi ve kurumların görüşleri alınır. Uzlaşı sağlandıktan sonra belirlenen standartlara son hali verilerek yayınlanır. Yayınlanan standartlara bir numara verilerek yürüklükteki standartlarda yerini alır. Çizelge 3.1'de bazı ülkelerin resmi standart kuruluşları ve kurulma yılları gösterilmiştir.

Çizelge 3.1. Çeşitli ülkelere ait standardizasyon kuruluşları

Organizasyon	**Kuruluş Yılı**
TSE (Türk Standartları Enstitüsü)-Türkiye	1960
BSI(British Standards Institution)-İngiltere	1901
DIN (Deutsches Institut für Normung e.V.) - Almanya	1917
ANSI (American National Standards Institute) - ABD	1918
JISC (Japanese Industrial Standards Committee) – Japonya	1949
SA (Standards Australia) – Avustralya	1922
AFNOR (Association française de normalisation) - Fransa	1926
UNE (Asociación Española de Normalización) - İspanya	1986
Swedish Standards Institute (SIS)-İsveç	1922

Gayri resmî standartlar bazı sektörlerin önde gelen kuruluşları tarafından oluşturulan standartlardır. Bu standart geliştirme kuruluşları (Standart Development Organization, SDO) da ülkeler tarafından bilinmekte ve son derece saygı görmektedirler. Gayri resmî standart geliştirme kuruluşlarına örnek olarak ASTM International (önceki adıyla American Society for Testing and Materials), IEEE (Elektrik ve Elektronik Mühendisleri Enstitüsü), SAE (Otomotiv Mühendisleri Topluluğu), TAPPI (Amerikan Kâğıt ve Selüloz Derneği) verilebilir. Resmi ve gayri resmi Standartları geliştirme süreci aynıdır, ancak standartların onayı, resmi standartlar söz konusu olduğunda NSB'ler ve gayri resmi Standartlar için SDO'lar gibi farklı kuruluşlar tarafından üstlenilir. Resmi standartlar için (en azından resmi onay süreçleri açısından) süreçler, gayri resmi standartlarda olduğu gibi organizasyon veya bireysel temsil yerine ulusal temsil yoluyla işler. Bu nedenle, bazen materyali hazırlayan uzmanlar kendi başlarına katılsalar bile, sonuçta ortaya çıkan belgeleri onaylayan veya reddeden ulusal kuruluş üyeliğidir, hâlbuki gayrı resmi standartlara katılım ve onay bir organizasyon ve/veya bireysel üyelik temelindedir (Hatto, 2013).

Uluslararası alanda standardizasyon ile ilgili faaliyet gösteren ve hiçbir devlet ile bağı olmayan ISO (International Organization for Standardization), IEC (International Electrotechnical Commission), ve ITU (International Telecommunication Union) gibi bağımsız kuruluşlar da mevcuttur.

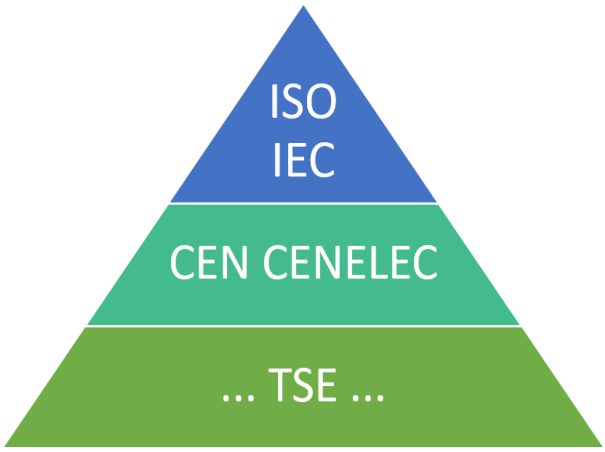
1906 yılında kurulan IEC (Uluslararası Elektroteknik Komisyonu), tüm elektrik, elektronik ve ilgili teknolojiler için kısaca "elektroteknoloji" olarak da tanımlanan, uluslararası standartların hazırlanması ve yayınlanması konusunda kurulmuş bir sivil toplum kuruluşudur. IEC, 170'den fazla üye ülkesi bulunan ve dünya genelinde 20.000 uzmanın çalışmalarını koordine eden, kar amacı gütmeyen, küresel bir üyelik organizasyonudur (IEC, 2023).

ITU (Uluslararası Telekomünikasyon Birliği), bilgi ve iletişim teknolojileri odaklı, uluslararası standardizasyonda faaliyet gösteren bir kuruluştur. Ülkelerin üyeliklerinin yanında sektörden de katılıma açık bir ortam sunmaktadır. Güncel durumda 191 üye ülke ve 700 sektör üyesi ile bulunmakta ve merkezi Cenevre'de yer almaktadır (TSE, 2023).

Uluslararası Standardizasyon kuruluşlarının başında gelen Uluslararası Standardizasyon Örgütü (ISO), bir Sivil Toplum Kuruluşudur (STK). Birleşmiş Milletler (BM) ile ilişkisini sürdürür. 167 ulusal standardizasyon kuruluşu üyesi bulunmaktadır. Üyeleri aracılığıyla, bilgi paylaşmak ve yeni uygulamaları desteklemek için gönüllü, fikir birliğine dayalı, çeşitli sektörlerle ilgili Uluslararası Standartlar geliştirmek için uzmanları bir araya getirmektedir (Seo, 2013).

ISO, Standartlarını TC (Teknik komite) ve alt toplulukları aracılığıyla geliştirir. Şu anda 813 komitesi bulunmaktadır. Bunlar, standart üretim ve gözden geçirme sürecinde işbirliği yapmak amacıyla tartışmalar için bir bilgi yönetim sistemi aracılığıyla elektronik ortamda toplanırlar (Riillo,2013).

Standardizasyon kuruluşları arasında yazılı anlaşmalar gereği hiyerarşik bir sistem oluşturulmuştur. Bu sistemde eğer bir konu ile ilgili bir standart varsa diğer kuruluşlar ve üyeler başka bir standart yayınlamazlar. Bu uygulama zaten içeriği çok zengin ve karmaşık olan standardizasyonu daha anlaşılır ve basit hale getirmek için yapılmaktadır. Buna göre yayında olan bir uluslararası standart var ise Avrupa standardizasyon kuruluşları bu standardın başına kendi kısaltmalarını ekleyerek adapte ederler. Aynı şekilde ulusal standardizasyon kuruluşları da üyelik koşullarına göre ya Avrupa Standardizasyon kuruluşunun ya da uluslararası standardizasyon kuruluşunun orijinal metnini alarak kendi sistemlerine adapte ederler. Şekil 3.1'de bu hiyerarşiyi açıklayan örnek bir görsel bulunmaktadır.



Şekil 3.1. Standardizasyon kuruluşları hiyerarşik yapısı örneği

Kaynak: TSE (https://www.tse.org.tr/IcerikDetay?ID=2900&ParentID=9189)

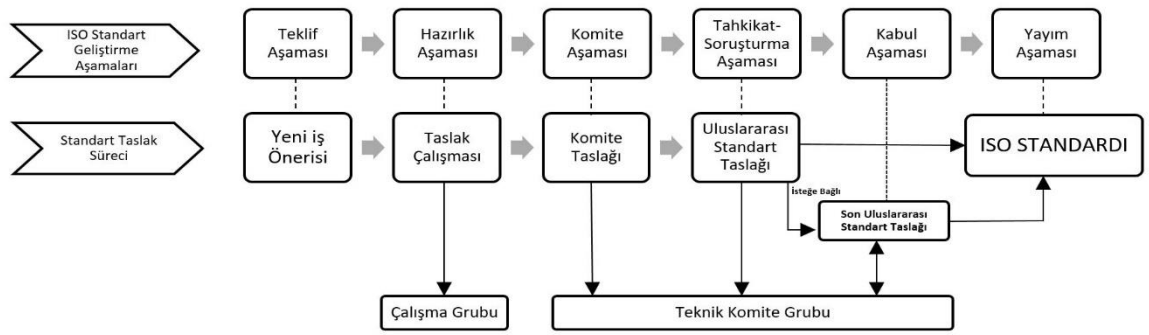
ISO, IEC ile ortak standartlar geliştirir. ISO, standartların geliştirilmesinde Teknik ve Proje Komitelerini kullanır. Teknik Komite (TC), bir standardın geliştirilmesi ile görevlendirilebilecek kalıcı bir komitedir. Belirli bir standardın geliştirilmesi için bir Proje Komitesi (PC) oluşturulur ve ardından dağıtılır (International Organisaton for Standardization [ISO] Directives Part 1,2023).

ISO üyesi ülkeler, Standartlar geliştiren bir PC veya TC Komitesinin "P" veya "O" üyesi olmak için kaydolabilirler. Katılımcı (P) üyeler, kendi ülkelerindeki SDO içinde bir ayna komitesi oluşturan oy kullanan üyelerdir. Gözlemci (O) üyeler toplantılara katılıp görüş bildirebilir ancak oy kullanamazlar (ISO/IES Directives Part 1,2023).

ISO standart geliştirme sürecinin temel ilkeleri, standartların pazardaki bir ihtiyaca cevap vermesi, küresel uzman görüşüne dayalı olması, çok paydaşlı bir süreçle geliştirilmesi ve fikir birliğine dayalı olmasıdır. Kararlar bir formüle göre fikir birliği ile alınır. ISO içinde, oy veren katılımcı üye ülkelerin üçte ikisi olumlu olduğunda ve toplam olası oyların dörtte birinden fazlası olumsuz olduğunda karar verilir (ISO/IES Directives Part 1,2023).

Standartların geliştirilmesi için tüm üye ülkelerin uyması gereken ve ISO Direktifleri Bölüm 1 ve 2'de ayrıntılı olarak açıklanan katı ISO kuralları vardır. Adli bir bakış açısıyla, zorluk, metodoloji açısından çok kuralcı standartlar geliştirmek, mevcut kabul görmüş uygulamayı tanımak değil, ancak yine de sonuçların güvenilirliği ve tutarlılığına ilişkin beklentileri tanımlamaktır. Yayınlanan standartların uygulanabilirliğini ve geniş topluluk kabulünü sağlamak için geniş paydaş katılımına sahip olmak da önemlidir(ISO/IES Directives Part 1-2,2023).

ISO süreci, şu altı aşamayı takip eder: teklif, hazırlık, komite, soruşturma, onay ve yayın aşamaları. Bunlar, Şekil 3.2'de gösterildiği gibi Çalışma Grupları, Teknik/Proje Komitesi ve ISO üyesi ülkeler tarafından değerlendirilen standart taslak geliştirme aşamalarıyla bağlantılıdır (Wilson ve Wilde, 2018).



Şekil 3.2. ISO standartları geliştirme sürecinin gösterimi

Kaynak: (Wilson ve Wilde, 2018)

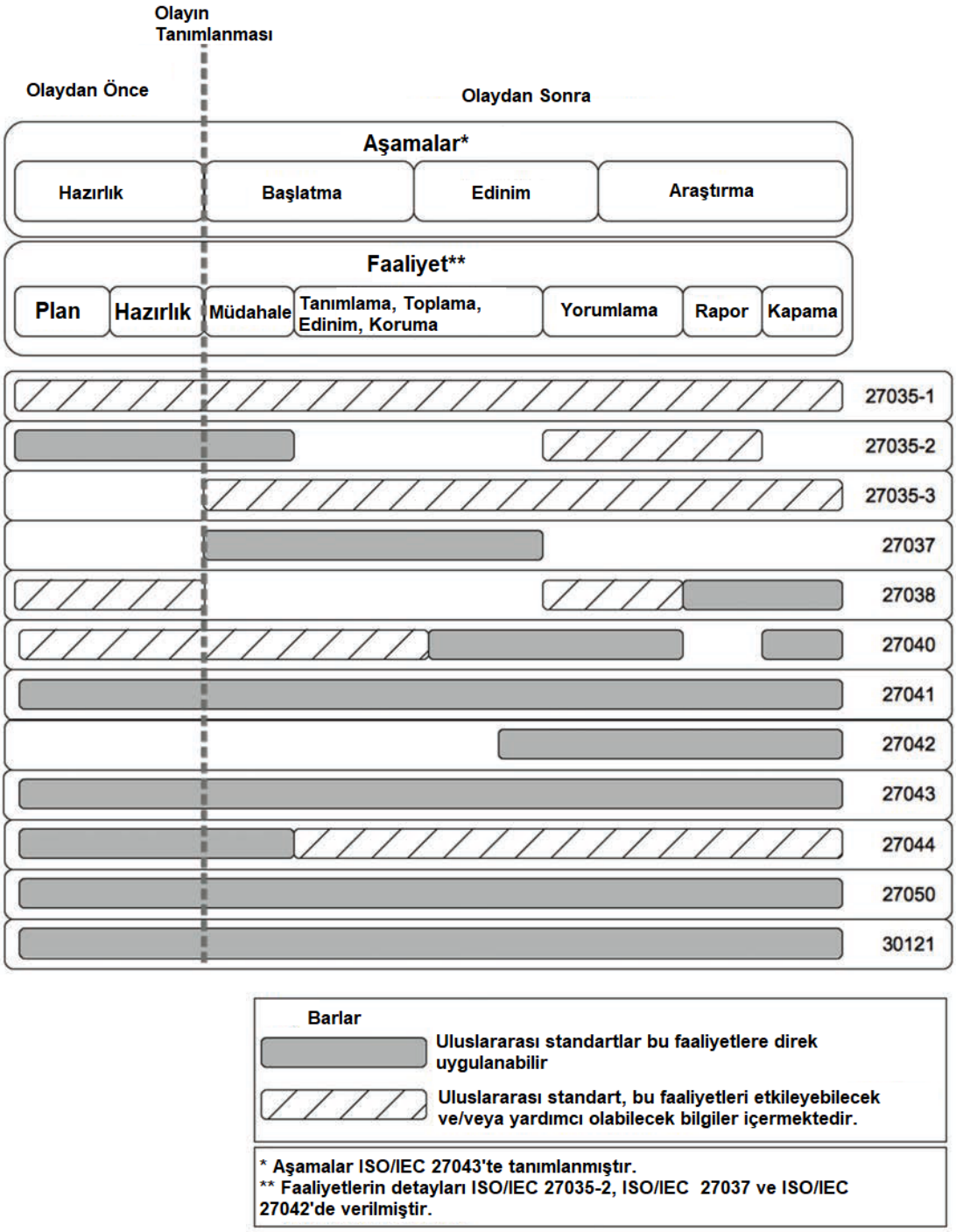
ISO uluslararası standardizasyon kuruluşları arasında adli bilişime yönelik standartlar yayımlayan en büyük kuruluştur. Bu nedenle çalışmanın bundan sonraki kısımlarında uluslararası bir standardizasyon kuruluşu olan ISO ve yayımladığı standartlar temel alınacaktır. Ayrıca adli bilişim ile ilgili standartlar yayımlayan diğer SDO'lara değinilecektir.

3.2. Adli Bilişim Standartları

Adli bilişim laboratuvarı standardının bulunmayışı şu anda oluşturulan bir dizi adli bilişim standardı tarafından karşılanmaktadır. Aşağıda belirtilen her bir standart bir ya da daha fazla adli bilişim sürecine yönelik prosedürleri kapsamakla beraber adli bilişim laboratuvarı konusundaki boşlukları kapatmayı amaçlamaktadır.

ISO tarafından adli bilişim konusunda oluşturulan ve 27000 ailesi olarak da bilinen standartlar bilgi güvenliği olay yönetimi, dijital delil yönetiminde güvenlik teknikleri, dijital redaksiyon, depolama güvenliği, olay soruşturma yöntemi, dijital delil yorumlama ve analizi, güvenlik bilgisi ve olay yönetimi, soruşturma modelleri ve elektronik keşif konularını kapsamaktadır (Klipper, 2011).

Dijital delil soruşturması, keşif sürecinden kaynaklanan maksimum yararlı etkiyi sağlamak için laboratuvarın ya da bilirkişinin yetki alanı dâhilinde dijital delil elde etmeye ve analiz etmeye odaklanır. ISO Standartlarından olan 27000 ailesi standartları adli bilişim deliller için birincil katmanlardan biri olan dijital delil analizi prosedürlerinde önemli bir rol oynamaktadır (Veber ve Klima, 2014). Şekil 3.3'te mevcut adli bilişim standartları ve süreçlere uygulanma şekilleri gösterilmiştir.



Şekil 3.3. Adli bilişim standartları ve süreçlere uygulanma şekilleri

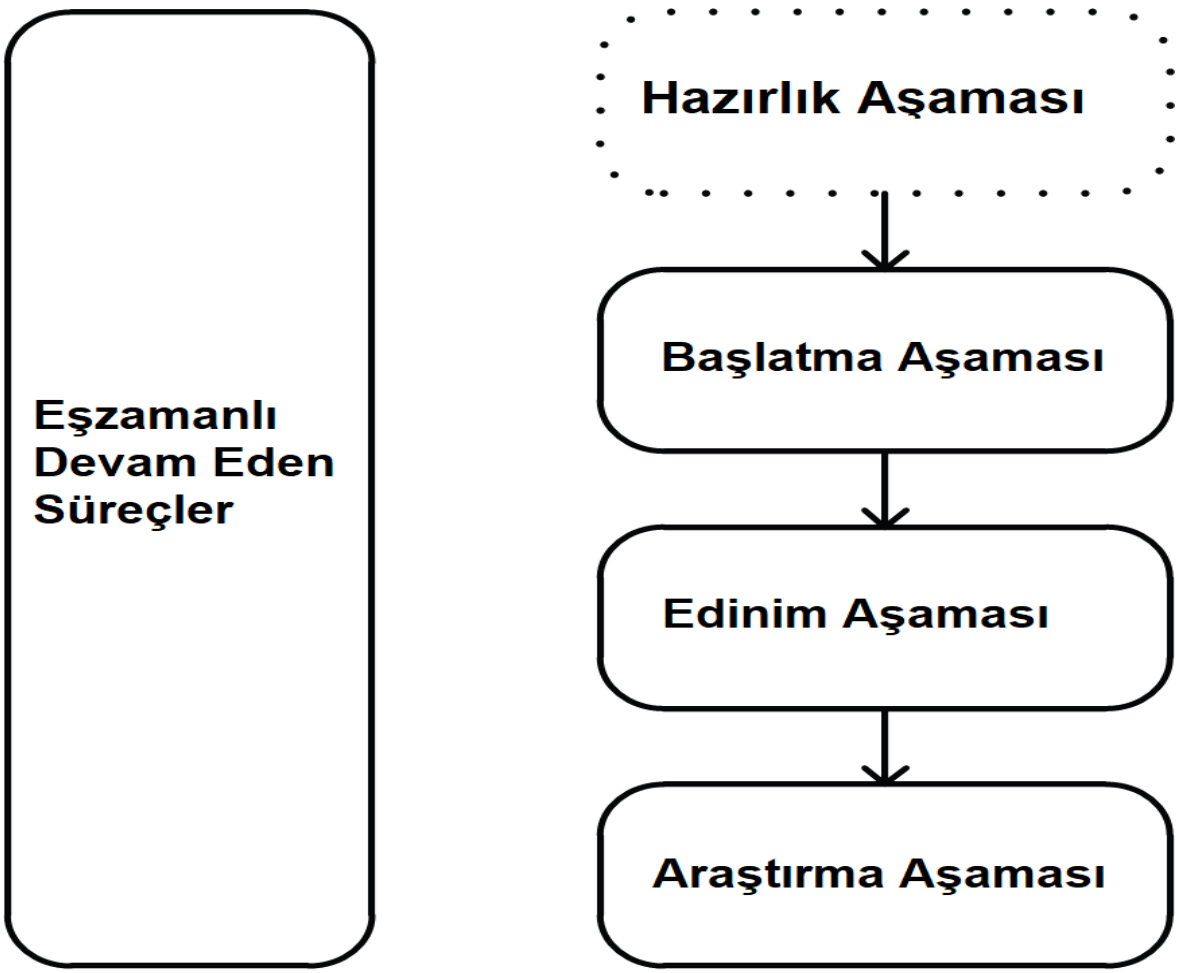
Kaynak: TS EN ISO/IEC 27043, 2021

Şekil 3.3'te görülen dijital delillerin incelenmelerine ilişkin ISO/IEC standartlarının tam isimleri şu şekildedir:

- 27035: Bilgi Teknolojisi-Bilgi Güvenliği Olay Yönetimi. Bu Standart kendi içinde üç bölüme ayrılmıştır. 27035-1(Prensipler ve süreç), 27035-2(Olaya müdahale için planlama ve hazırlık kılavuzu), 27035-3(Bilgi Teknolojileri olayına müdahale için kılavuz).
- 27037: Dijital delillerin tanımlanması, toplanması, elde edilmesi ve korunmasına ilişkin kılavuz
- 27038: Dijital redaksiyon için şartname
- 27040: Depolama güvenliği
- 27041: Olay inceleme yönteminin uygunluğunun ve yeterliliğinin sağlanmasına ilişkin kılavuz
- 27042: Dijital delillerin analizi ve yorumlanması için kılavuzlar
- 27043: Olay soruşturma ilke ve süreçleri
- 27044: Güvenlik bilgileri ve olay yönetimi için kılavuzlar
- 27050: Bilgi Teknolojisi-Elektronik Keşif. Bu standart kendi içinde dört bölüme ayrılmıştır. 27050-1(Genel bakış ve kavramlar), 27050-2 (Elektronik keşfin yönetişimi ve yönetimi için kılavuz), 27050-3 (Elektronik keşif için uygulama kodu), 27050-4 (Teknik hazırlık)
- 30121: Dijital adli risk çerçevesinin yönetimi

Resim 3.3'te ISO standartlarının adli bilişim incelemelerini bir dizi süreç olarak tanımladığını görmekteyiz. Süreçleri genel olarak kapsayan 27041 ve 27043 standartları olayın hazırlık aşamasından delillerin kabulü, incelenmesi, raporlanması ve dosyanın kapatılmasına kadar olan süreç için tavsiyeler sunmaktadır. 27043 standardı 27041'e göre daha geniş bir süreci ele almaktadır. 27043 standardı olayın soruşturulmasında ilke ve süreçleri ortaya koyarken 27041 standardı ise bu süreçte kullanılan yöntemlerin uygunluğu ve yeterliliği hakkında tavsiyeler vermektedir (Yalçın ve Kılıç, 2019).

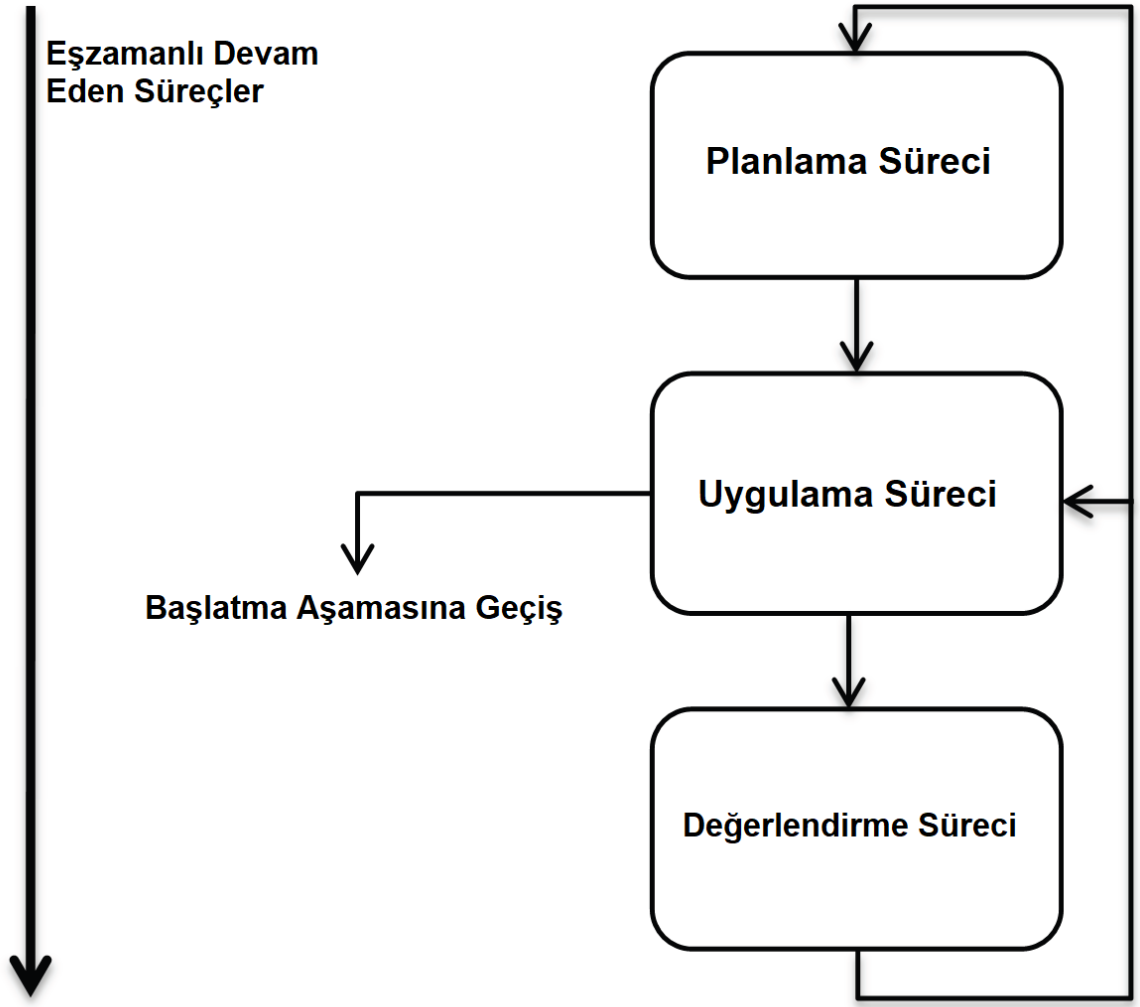
27043 standardı olay soruşturma süreçlerini hazırlık, başlatma, edinim ve araştırma süreçleri olacak şekilde dört aşamaya ayırmıştır. Şekil 3.4'te dijital araştırma süreçlerinin bu aşamaları gösterilmiştir.



Şekil 3.4. Dijital araştırma süreçlerinin aşamaları

Kaynak: TS EN ISO/IEC 27043, 2021

ISO 27043 standardında hazırlık aşamasını planlama, uygulama ve değerlendirme olarak üçe ayırmıştır. Şekil 3.5'te bu süreçler gösterilmektedir.



Şekil 3.5. Hazırlık aşaması

Kaynak: TS EN ISO/IEC 27043, 2021

Planlama süreci; senaryo tanımlama süreci, potansiyel dijital delil kaynaklarının tanımlanması süreçleri, olay öncesi toplamanın planlaması süreci, verilerin saklanması ve işlenmesi süreçleri, potansiyel dijital delilin temsili, olay tespit süreci ve organizasyon sistem mimarisi sürecini tanımlama alt süreçlerinden oluşur.

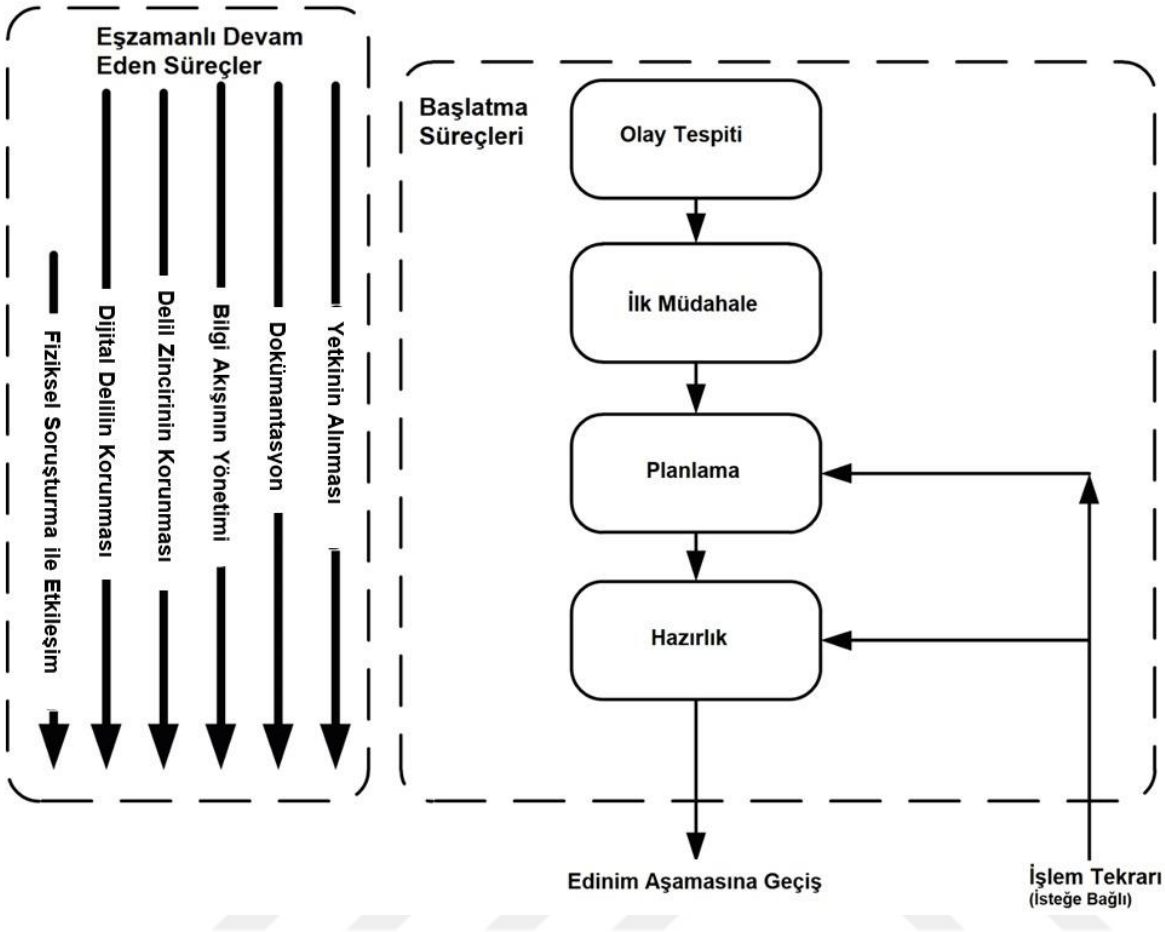
Uygulama süreci, planlama süreçleri grubunda planlanan faaliyetlerin uygulanması içindir. Sonuç olarak, bu grup, sistem mimarisi sürecinin uygulanmasını, olay tespit sürecini ve potansiyel dijital

delili temsil eden olay öncesi verilerin analizini içerir. Ek olarak, potansiyel dijital delilleri temsil eden verilerin toplanması, saklanması ve yönetimini de ele alır.

Son olarak, değerlendirme sürecidir. Bu grup, önceki süreçlerdeki uygulama başarısının değerlendirilmesine odaklanır. Bu grup, uygulama süreci ve uygulama sonuçlarının değerlendirilmesini içerir (TS ISO/IEC 27043:2021).

Ayrıca genel ilkeleri belirleyen 27043 standardının hazırlık aşaması 27035-2 (Olaya müdahale için planlama ve hazırlık kılavuzu) ile doğrudan ilişkilidir. 27035-2 standardı, olayları zamanında tespit etmek ve olayla ilgili tüm olası delilleri toplamak amacıyla kuruluş içindeki güvenlik olaylarının tespitine yönelik hazırlıklara odaklanır (Sonntag, 2013). ISO 27035-2 "Planlama ve Hazırlanma" işlemlerinden oluşur. Planlama ve hazırlanma kısımlarının ana noktaları; risk yönetimi ile ilgili olanlar da dâhil olmak üzere, hem kurumsal düzeyde hem de sistem, hizmet ve ağ düzeylerinde güncellenen bilgi güvenliği politikaları, olay yönetim ekibinin kurulması, teknik ve diğer destek konularından oluşmaktadır (ISO, 2023).

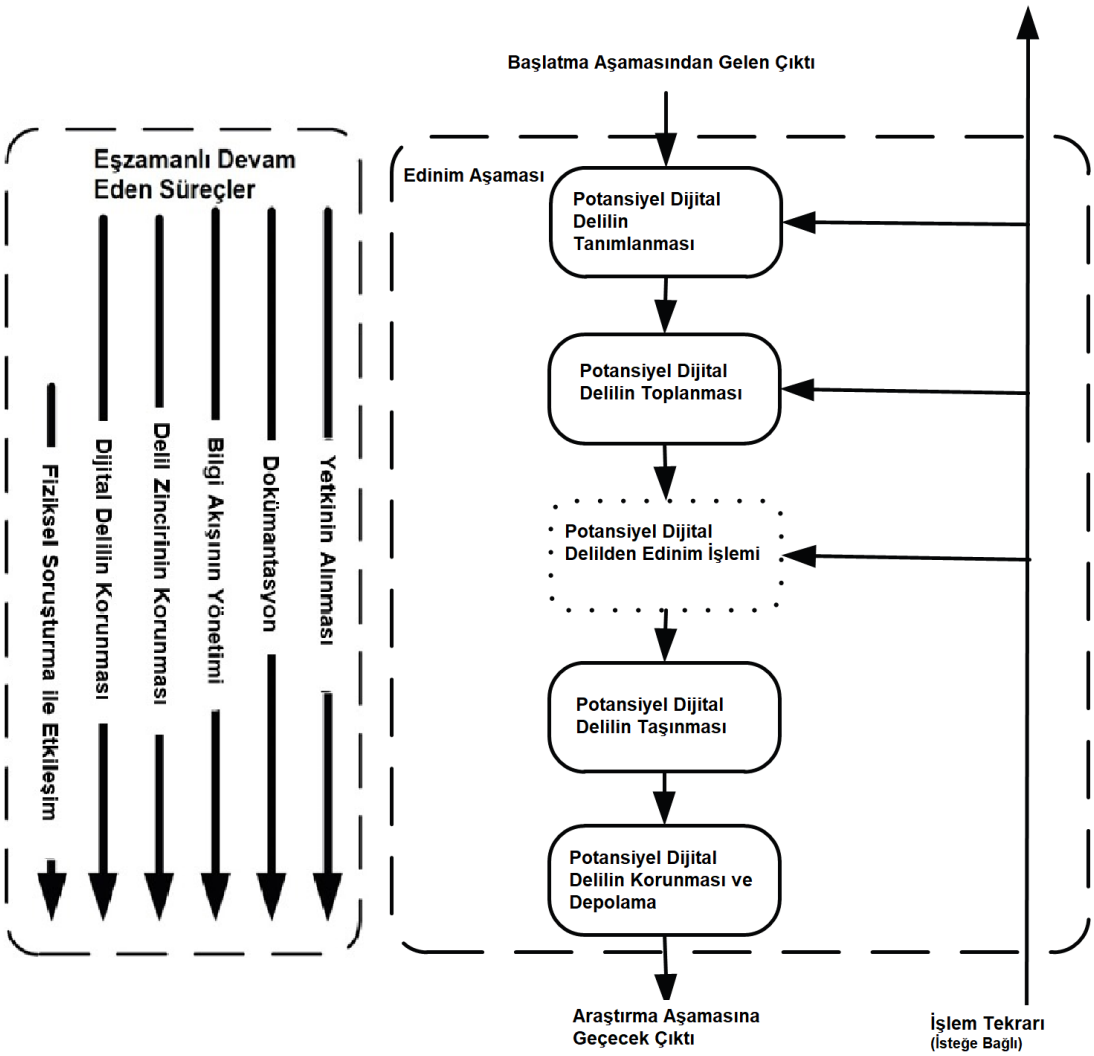
Başlatma aşaması, olayla bağlantılı bir dizi faaliyettir ve bir soruşturma başlatır. Bu aşama, olayı tespit ederek dijital soruşturmayı başlatır ve olay inceleme süreçlerinin geri kalanı için hazırlık ile birlikte bu olaya ilk müdahaleyi başlatır. Bu aşama; olay tespiti, ilk müdahale, gerekli bilgilerin neyin ve nasıl elde edileceğini planlama ve tasarlama ve bir duruma hangi araç(lar)ın ve tekniklerin uygun olduğuna karar verme süreçlerinden oluşmaktadır. Soruşturma için planlama ve hazırlık, kolluğun olay yeri ile ilk temasını ve bu soruşturmayı yürütmek için stratejik bir plan oluşturulmasını içerir. Bu nedenle, soruşturmanın başarısını etkileyecek tüm soruların (ne, neden, kim, nasıl ve ne zaman) bu aşamada açıklığa kavuşturulması gerekir. Başlatma aşamasının özetlenmiş hali Şekil 3.6'da mevcuttur.



Şekil 3.6. Başlatma aşaması

Kaynak: TS EN ISO/IEC 27043, 2021

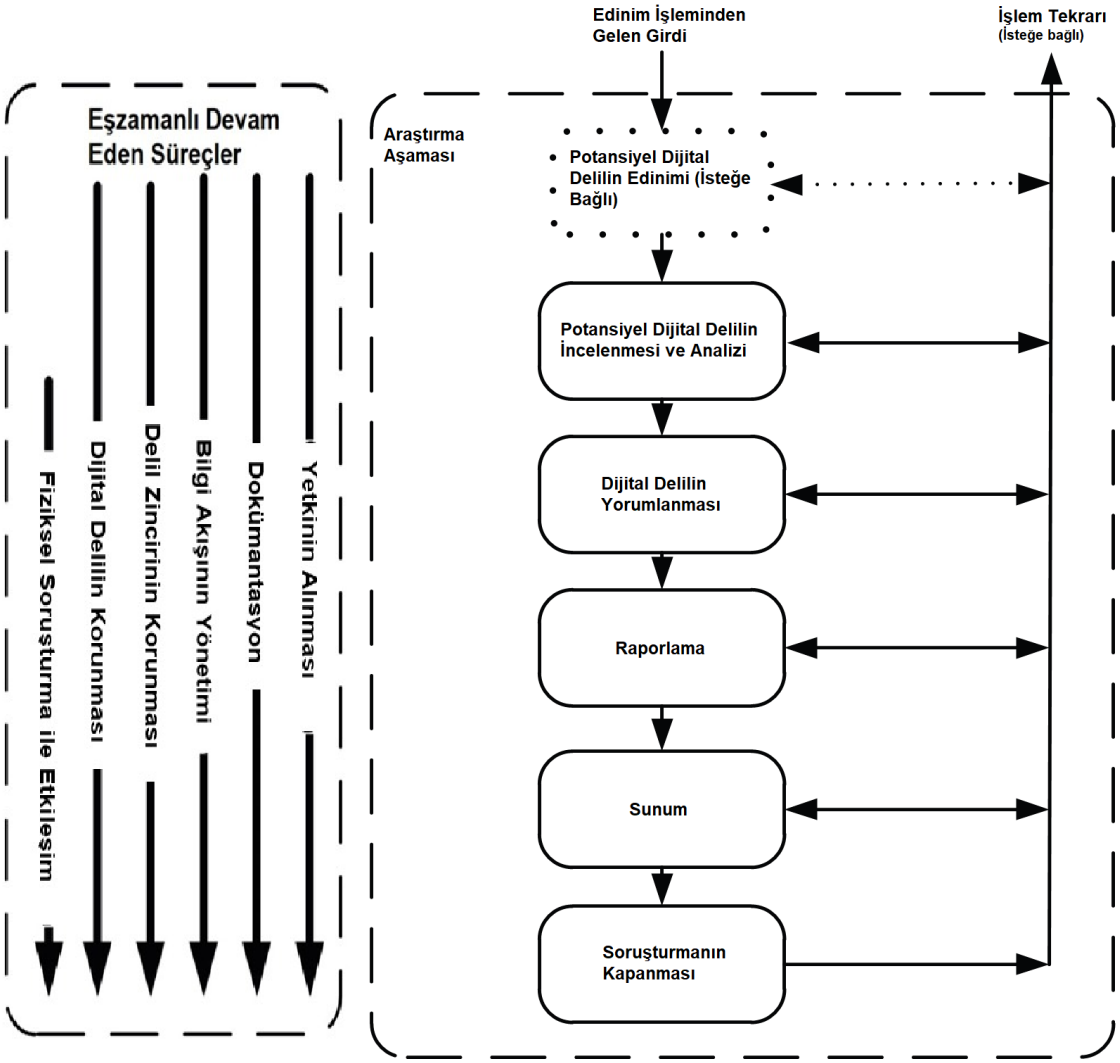
Edinim aşaması, potansiyel dijital delillerin elde edilmesiyle ilgilenen bir dizi faaliyettir. Potansiyel dijital delilin tanımlanması, toplaması, taşınması ve depolamadan oluşur. Edinim işlemleri ayrıca 27037'deki tanımlama, edinim, toplama ve koruma işlemleri ile 27042'deki değerlendirme ve analiz faaliyetleri ile doğrudan ilişkilidir. Bu üç standart eşzamanlı bir şekilde yürütülmekte olup 27037'ye göre yürütülen farklı cihazlardan yapılacak olacak olan edinim işlemi 27042'e göre birlikte ve olayın niteliğine göre yorumlanabilmektedir. Edinim aşamasının özetlenmiş hali Şekil 3.7'da mevcuttur.



Şekil 3.7. Edinim aşaması

Kaynak: TS EN ISO/IEC 27043, 2021

Son olarak araştırma aşaması vardır. Bu aşama, dijital delillerin incelenmesini gerektirecek adli vakanın araştırılmasına odaklanır. Bu aşamadaki faaliyetler temel olarak dijital delillerin analizine ve vaka ile olan bağlantısına odaklanmaktadır. Delillerin yorumlanması ve uzmanlık raporunun yazılması ve sunulmasını içerir. Ayrıca, bu aşama, soruşturma hipotez(ler)inin kabul veya reddinin kaydedilmesi ve çıkarılan derslerin kaydedilmesinin ardından (gerekirse) delilin iade edildiği soruşturmanın kapatılma sürecini de içerir. Bu aşama tamamıyla ISO/IEC 27042 "Dijital kanıtların analizi ve yorumlanması için kılavuzlar" kapsamındadır. Bu faaliyetler Şekil 3.8'de görülmektedir.



Şekil 3.8. Araştırma aşaması

Kaynak: TS EN ISO/IEC 27043, 2021

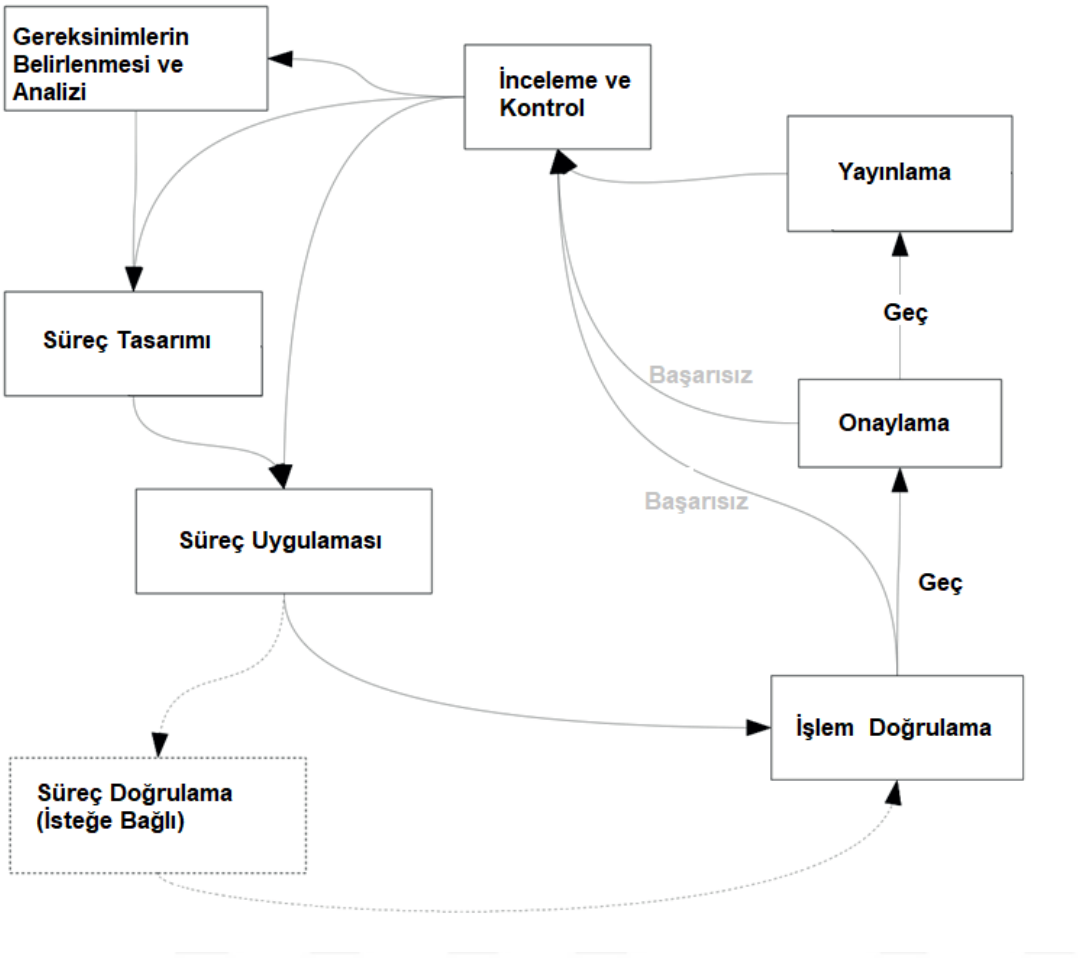
Şekil 3.6, 3.7, 3.8'de toplanan bulguları tanımlamak, analiz etmek ve bulguların adli vaka ile ilgisini ortaya koymak için işleyen dijital soruşturma süreçleri sınıflarının yanında çalışan eşzamanlı süreçler vardır. Şekil 3.3'deki süreç sınıflarını yürüten birincil standartlara ek olarak, adli bilişim incelemelerine dâhil olan iki başka standart türü daha vardır. Bunlar, tüm adli bilişim süreçleri arasında çalışan standartlar (ISO/IEC 27041, ISO/IEC 27050 ve ISO/IEC 30121) ve her sürece sınıfı içinde küçük bir katkı sağlayan standartlardır (ISO/IEC 27038 ve ISO/IEC 27040).

ISO/IEC 27041 standardı, kullanılan soruşturma sürecinin soruşturma altındaki olay ve gereken sonuçlara uygun olduğuna dair güvence sağlamakla ilgilidir. Aynı zamanda, soyut bir düzeyde, basit ama sağlam araştırma yöntemlerinin geliştirilmesine yardımcı olması gereken, görünüşte karmaşık süreçleri bir dizi daha küçük parçalara ayırma kavramını da açıklar. Her ne kadar parça parça etkili olan diğer standartlar kendi içinde tutarlı ve sağlam olsa da uygulanan yöntemlerin bütünsel olarak birliğini sağlamaya yönelik bir standarttır. Adli vakalarda elde edilen dijital delillerin hepsi aynı laboratuvarda incelenemeyeceği ya da vakanın aynı mahkeme önünde görülemeyeceği düşünüldüğünde elde edilen sonuçların güvenilir olması gerekmektedir. Standardın amacı yayınlanan kalite dokümanında, bilgi güvenliği olaylarının soruşturulması ve soruşturmaya hazırlık konusunda rehberlik sağlayan diğer standartları ve belgeleri tamamlamak olarak tanımlanmıştır. Kapsamlı bir kılavuz olmamasına rağmen ihtiyaç duyulduğunda araç, teknik ve yöntemlerin uygun şekilde seçilmesini ve amaca uygun olduğunun gösterilmesini sağlamayı amaçlayan bazı temel ilkeleri ortaya koyar (TS ISO, 2016).

Soruşturmalarda kullanılmak üzere bir model devreye alınmadan önce, amaca uygun olduğundan emin olmak için uygun bir geliştirme sürecinden geçmelidir. Bu geliştirme sürecinin aşamaları şu şekilde tanımlanabilir;

- Gereksinimlerin belirlenmesi ve analizi
- Süreç tasarımı
- Süreç uygulaması
- Süreç doğrulaması (isteğe bağlı ve zorunlu olmayan)
- İşlem doğrulama
- Onaylama
- Yayımlama
- İnceleme ve Kontrol

Şekil 3.9’da geliştirme sürecinin aşamaları ve döngüsü gösterilmiştir.



Şekil 3.9. Geliştirme sürecinin aşamaları ve döngüsü

Kaynak: TS EN ISO/IEC 27041, 2016ISO/IEC 27050

"Elektronik keşif" standardı adli bilişim yaşam döngüsüne dört bölümlü bir standart olarak katkıda bulunur: ISO/IEC 27050-1:2019 "Genel bakış ve kavramlar", ISO/IEC 27050-2:2018 " Elektronik keşfin yönetişimi ve yönetimi için kılavuz" ve ISO/IEC 27050-3:2020 "Elektronik keşif için uygulama kuralları" ve ISO/IEC 27050-4:2021 “Teknik hazırlık”. Elektronik keşif sisteminin yönetimine, süreçlerine ve hazır olmasına ek olarak yasal bir bakış açısı sağlar. Herhangi bir yerel yargı sistemi gerekliliğiyle çelişmek ve/veya bunların yerine geçmek için tasarlanmamış olup, eylem için bir çerçeve ve kontrol tablosu sağlamak üzere tasarlanmıştır (Hibbard, 2014).

ISO/IEC 30121:2015 “Dijital adli risk çerçevesinin yönetimi”, bir kurumun bilgi Teknolojisine yönelik güvenlik çözümlerinin ve teknolojilerinin verilerini tek başına koruyamadığı durumlarda, işletmeler için bir adli bilişim standardı işlevi görür (DATE, 2013). Bu Standart, öncelikle, bir olayın meydana gelmesinden önce, oluş sırasında ve sonrasında, olay yönetimi süreçleri ve dijital adli risk

gerekliliği ilişkisinin ele alındığı yerlerde işlev görür. Kurumlar içinde dijital ortamlarda gerçekleşen işlemler bazen kasıtlı bir şekilde bazen de kasıt olmadan yasaya aykırı olabilir. Yürütülecek bu işlemlerin meydana getirdiği riskler belirlenmeli ve kurumlar bu çerçevede önlem almalıdır (Grobler, 2012).

3.3. Genel Laboratuvar Standartları

ISO/IEC 17025 hükümlerinin uygulanabilirliği de dâhil olmak üzere, Uluslararası Standartların, adli bilişim laboratuvarlarının gereksinimlerini karşılayacak şekilde uyarlanmasının zorluklarını görebilmek için bu standartların biraz daha detaylandırılması gerekmektedir. Ayrıca, bazı Uluslararası Standartlarında yer alan Kalite Yönetim Sistemleri (Quality Management Systems-QMS) alanındaki adli bilişim laboratuvarlarının gerekliliklerinin kapsamının da açıklığa kavuşturulması gerekmektedir. Standartlar arasındaki kapsam ve içerik karşılaştırması, boşlukları ortaya çıkaracak ve adli bilişim laboratuvarları hakkında oluşturulabilecek bir standardizasyonun doldurması gereken alanları gösterecektir.

Yukarıda atıfta bulunulan ISO/IEC 27000 ailesi içindeki on bir adli bilişim standardına ek olarak, başka bir ISO grubundan adli bilimler laboratuvarı gerekliliklerine katkıda bulunan çeşitli standartlar bulunmaktadır. Genel olarak Standartlar, kendini tanıma, akreditasyon veya sertifikasyon yoluyla uygulanabilir; burada kendini tanıma, kuruluşun kendi kendini değerlendirmesine bağlıdır.

Akreditasyon ve sertifikasyon genellikle birbirleri ile karıştırılmaktadır. Sertifikasyon, söz konusu ürün, hizmet veya sistemin belirli gereksinimleri karşıladığına dair bağımsız bir kuruluş tarafından yazılı bir güvencenin (sertifika) sağlanması anlamına gelir. Bu, yönetime dayalı standartlarda ayrıntılı olarak açıklanan gereklilikler kullanılarak gerçekleştirilir. Akreditasyon, bir tesisin uluslararası standartlara göre faaliyet gösterdiğinin teknik uzmanlar kullanan bağımsız bir kuruluş (genellikle akreditasyon kuruluşu olarak bilinir) tarafından resmi olarak tanınması anlamına gelir. Buna uygunluk değerlendirmesi de denir ve yeterliliğe dayalı standartlar kullanılarak gerçekleştirilir. Bu nedenle, sertifikasyon bir ürünün, hizmetin veya sistemin belirlenmiş gerekliliklere göre değerlendirilmesi anlamına gelirken, akreditasyon bir kurum veya kuruluşun, belirlenmiş gereksinimlere göre teknik bilgiye dayalı olarak yeterliliğinin değerlendirilmesi anlamına gelir. Akreditasyon kurumlar için geçerli iken sertifika aynı zamanda bir kişi için de geçerli olabilir (ISO, 2023).

Akreditasyon ve sertifikasyon, bu hizmeti gerçekleştirmek üzere akredite olan üçüncü taraf kuruluşlar tarafından gerçekleştirilir. Birçok akreditasyon kuruluşu Uluslararası Laboratuvar Akreditasyon İşbirliği'nin (ILAC) imzacısıdır. ILAC, "ISO/IEC 17011:2017 Uygunluk değerlendirmesi-Uygunluk

değerlendirme kuruluşlarının değerlendirmesini ve akreditasyonunu sağlayan kuruluşlar için genel şartlar ve ek gereklilikler dokümanları" uyarınca faaliyet gösteren akreditasyon birimlerinin uluslararası kuruluşudur. ILAC, ILAC Düzenlemesi olarak da adlandırılan uluslararası, çok taraflı Karşılıklı Tanıma Düzenlemesi (MRA) kapsamında uygunluk değerlendirme kuruluşlarının akreditasyonunda yer almaktadır (Uluslararası Laboratuvar Akreditasyon İşbirliği, [ILAC], 2023).

Laboratuvar yeterliliğine dayalı Standartlar, ISO Uygunluk Değerlendirme Komitesi (CASCO) adı verilen bir ISO komitesi tarafından yönetilir ve geliştirilir (ISO, 2023). CASCO, bir kuruluşun güvenilir bir hizmet sunma konusunda yetkin olduğunu akredite etmek ve onaylamak için kullanılan üç farklı türde laboratuvar standardı geliştirmiştir;

- ✓ **Test laboratuvarları:** ISO/IEC 17025:2017 "Test ve kalibrasyon laboratuvarlarının yeterliliği için genel gereklilikler" standardı. Bu Standart, genel gerekliliklerin yerine getirilmesi nedeniyle herhangi bir test laboratuvarı için (adli bilişim laboratuvarları dâhil) geçerli bir standarttır (ISO, 2017).

- ✓ **Tıbbi test laboratuvarları:** ISO 15189:2022 "Tıbbi laboratuvarlar, Kalite ve yeterlilik gereksinimleri" standardı. Bu Standart, ISO/IEC 17025'in bir alt kümesidir ancak tıbbi laboratuvarların kalite yönetim sistemlerine odaklanır (ISO, 2022).

- ✓ **Denetleme kuruluşları:** ISO/IEC 17020:2012 "Uygunluk değerlendirmesi, Denetleme gerçekleştiren çeşitli türdeki kuruluşların işleyişine yönelik gereklilikler" standardı. Bu Standart, kuruluşlara belge vermeyi sağlamak amacıyla başlangıç kuruluşları için sınav kriterlerini içerir (ISO, 2017).

Yukarıdaki yeterliliğe dayalı standartlara ek olarak, laboratuvar denetiminin kullanımında adli bilişim laboratuvarlarına uygulanabilecek, yönetime dayalı başka standartlar da bulunmaktadır;

- ✓ **Kalite Yönetim Sistemleri için ISO 9000 serisi:** ISO 9001:2015 "Kalite yönetim sistemleri. Gereksinimler", ISO/TS 9002:2016 “Kalite yönetim sistemleri. ISO 9001:2015’in Uygulama Rehberi (ISO,2021).

- ✓ **Çevre yönetimi:** ISO 14001:2015 "Çevre yönetim sistemleri. Kullanım kılavuzuyla birlikte gereksinimler" (ISO, 2015).

Olay öncesi aşamadan vaka kapanışına kadar adli bilişim süreçlerin tutarlılığını artırmak için teknik, yönetim ve denetim de dâhil olmak üzere süreçlerin tüm seviyelerinin standartlaştırılması

gerekmektedir. Delil araştırmasının temel aşamalarından biri, delillerin adli bilişim laboratuvarında incelenmesidir ve akredite bir adli bilişim laboratuvarı güvenilir bir sonuç üretilebilmesini sağlayabilir. Adli bilişim alanında genel laboratuvar akreditasyonu için ISO/IEC 17025 kullanılabilir. ISO/IEC 17025, laboratuvarı işlemlerinin yeterliliği için genel gereklilikleri belirten normatif bir referanstır. Bu standart laboratuvarlar ve laboratuvar faaliyetleri için geçerlidir. ISO/IEC 17025, standart, standart dışı ve laboratuvar tarafından geliştirilen çeşitli test yöntemlerini kullanarak adli analiz ve inceleme yapan laboratuvarlara rehberlik eder (Sommer, 2018).

Uluslararası Standardizasyon Örgütü'ne göre ISO/IEC 17025:2017 aşağıdaki maddelerden oluşmaktadır (ISO, 2023);

- ✓ **Genel gereklilikler:** Laboratuvarın tarafsızlığını ve gizliliğini belitirten bölüm,
- ✓ **Yapısal gereklilikler:** Bu madde, laboratuvarın yasal kimliğinin yanı sıra laboratuvar faaliyetlerinin ve sorumluluğunun açık bir şekilde tanımlanmasını kapsar. Laboratuvar hiyerarşisini ve çalışanların (teknik ve servis desteği) ve yönetimin sorumluluklarını ve yetkilerini açıklığa kavuşturmalıdır. Ayrıca laboratuvar faaliyetlerinin etkinliğini sağlamak için kuruluşun iç birimleri arasındaki ilişkileri ve müşteriler ile olan iletişimi de burada yer alır.
- ✓ **Kaynak gereksinimleri:** Bu bölüm, tanımlanan laboratuvar faaliyet kapsamını gerçekleştirmek için gerekli olan tesisler, personel, laboratuvar ekipmanı, sistem ve tanımlanmış destek hizmetleri gibi iç ve dış kaynakların derinlemesine kullanılabilirliğini kapsar.
- ✓ **Süreç gereklilikleri:** Bu bölüm, sözleşmelerin, ihalelerin ve taleplerin incelenmesi de dahil olmak üzere laboratuvar yaşam döngüsü süreçlerinin tamamını kapsar. Ayrıca test yöntemlerinin seçilmesi, doğrulanması ve onaylanmasının yanı sıra testlerin örneklenmesi ve işlenmesini de kapsar. Ayrıca laboratuvar kayıtlarının önemine ve belirsizlik değerlendirmesinin ölçümüne değinmektedir. Bu bölüm aynı zamanda sonuçların geçerliliği, sonucun raporlanması ve müşteri şikâyetlerinin ele alınması süreçlerine de odaklanmaktadır. Ayrıca laboratuvarın veri ve bilgi yönetimini kontrol etme gerekliliğini belirtir.
- ✓ **Yönetim sistemi gereklilikleri:** Bu madde, laboratuvar sonuçlarının kalitesini güvence altına alan laboratuvar yönetim sisteminin kurulması, belgelenmesi, uygulanması ve sürdürülmesine ilişkin gereklilikleri kapsar. Yukarıdaki maddelerin bu sistemde uygulanması zorunlu olduğundan, bu yönetim sistemi yukarıdaki maddelerin gerekliliklerini destekleyebilmelidir.

3.4. Mevcut Standartlara Dair Bazı Problemler

Önceki bölümlerde standartlarla ilgili ilgili literatür ve özellikle adli bilişim laboratuvarlarıyla ilgili seçilen literatür gözden geçirilmiştir. Bu bölümde öne çıkan sorunlar ve mevcut standartların neden adli bilişim laboratuvarlarını tam olarak kapsamadığı konuları incelenecektir.

Hong Guoa ve Junlei Houb, akreditasyon için ISO/IEC 17025 kullanımının, test yeterliliğinin uluslararası tanınırlığı, performans kıyaslaması ve pazarlama avantajı gibi çeşitli nedenleri olduğunu belirtmektedir. Ancak aynı yazarlar, bu standardın adli bilişim laboratuvarı için en uygun olup olmadığına dair tartışmaların olduğunu, özellikle de bu standardın Birleşik Krallık'ta adli bilişim laboratuvarı akreditasyonu için zorunlu bir gereklilik haline geldiğini belirtmişlerdir. Ayrıca birçok adli bilişim uzmanının, maliyetler, talimatların anlaşılamaması, kötü uygulama ve tutarsızlık gibi birçok nedenden dolayı ISO/IEC 17025'e karşı çıktığını da belirtmiştir. Ayrıca standardın uygulanması uzmanlık becerisi gerektirmektedir. ISO/IEC 17025, özellikle adli bilişim laboratuvarları için tasarlanmamasına rağmen, adli bilişim laboratuvarında kontrollerin uygulanması için bir başlangıç noktası olarak yararlı olabileceğini belirtmektedir (Guo ve Hou, 2018).

ISO/IEC 17025'in 1999, 2005 ve 2017 olmak üç versiyonu bulunmaktadır.1999 versiyonu ile 2005 arasındaki önemli gelişme, üst yönetimin yönetim sisteminin sürekli iyileştirilmesine yönelik taahhüt ve sorumluluk gereksiniminin yanı sıra, iletişim mekanizması da dâhil olmak üzere müşteriyle olan ilişkiye odaklanmasıdır. Bu, ISO 9001:2015 "Kalite yönetim sistemleri, Gereksinimler" standardı ile uyumludur.

Hykš ve Koliš tarafından yayınlanan önceki bir çalışmada, ISO/IEC 17025'in (2005 versiyonu) doğrudan adli bilişim laboratuvarına uyarlanabilirliği analiz edilmiş ve sonuç Çizelge 3.2'de sunulmuştur.

Çizelge 3.2. ISO/IEC 17025 gerekliliklerinin (2005 versiyonu) adli bilişim laboratuvarında uygulanması

Madde Numarası	**Madde Başlığı**	**Uygulanabilirlik**
4	Yönetim gereklilikleri	Tamamen uygulanabilir
4.1	Organizasyon(Kısmen)	Kısmen uygulanabilir
4.2	Yönetim sistemi	Tamamen uygulanabilir
4.3	Doküman kontrolü	Tamamen uygulanabilir
4.4	Taleplerin ve ihalelerin incelenmesi, sözleşmeler	Tamamen uygulanabilir
4.5	Test ve kalibrasyonların bir alt firmaya Verilmesi	Tamamen uygulanabilir
4.6	Hizmet ve malzeme satın alma	Tamamen uygulanabilir
4.7	Müşteriye hizmet	Tamamen uygulanabilir
4.8	Şikayetler ve/veya kalibrasyon çalışmaları	Tamamen uygulanabilir
4.9	Uygun olmayan testlerin kontrolü ve/veya kalibrasyon çalışması	Tamamen uygulanabilir
4.10	Gelişim	Tamamen uygulanabilir
4.11	Düzeltici faaliyet	Tamamen uygulanabilir
4.12	Önleyici faaliyet	Tamamen uygulanabilir
4.13	Kayıtların kontrolü	Tamamen uygulanabilir
4.14	İç denetimler	Tamamen uygulanabilir
4.15	Yönetim incelemeleri	Tamamen uygulanabilir
5	Teknik gereklilikler	
5.1	Genel	Tamamen uygulanabilir

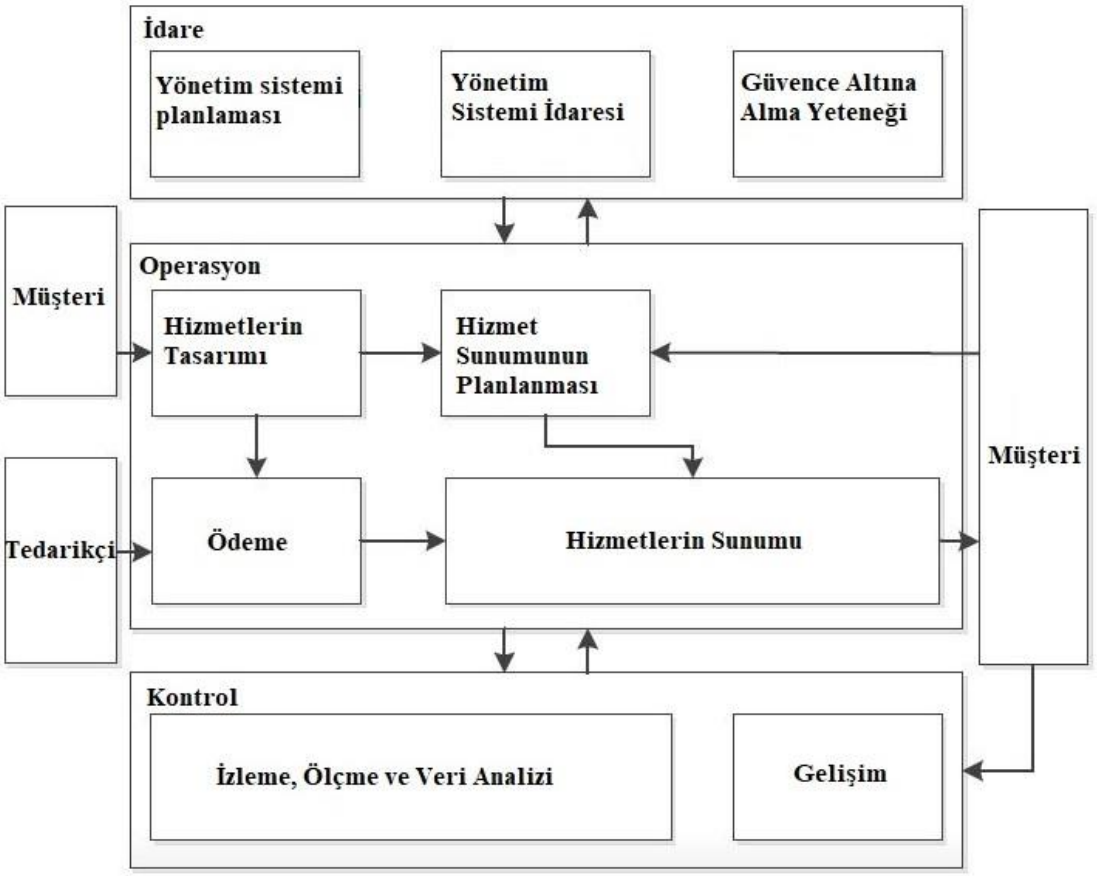
5.2	Personel	Tamamen uygulanabilir
5.3	Konaklama ve çevre koşulları	Uygulanamaz
5.4	Test ve kalibrasyon metotları ve metotların doğrulanması	Kısmen uygulanabilir
5.5	Ekipman	Uygulanamaz
5.6	Ölçüm izlenebilirliği	Kısmen uygulanabilir
5.7	Örnekleme	Uygulanamaz
5.8	Testlerin ve kalibrasyon öğelerinin muhafazası	Tamamen uygulanabilir
5.9	Test ve kalibrasyon sonuçlarının kalitesinin güvence altına alınması	Tamamen uygulanabilir
5.10	Sonuçların raporlanması	Tamamen uygulanabilir

Kaynak: Hykš ve Koliš, 2014

ISO/IEC 17025'in adli bilişim laboratuvarına uygunluğunun analizinin sonucu üç nitelikli durumla sonuçlanmaktadır. Tamamen uygulanabilir maddeler, hariç tutulması gereken maddeler ve kısmen uygulanabilir maddeler. Ayrıca, adli bilişim laboratuvarı için geçerli olmayan ancak uygulamadaki bir boşluğu doldurmak için değiştirilebilecek maddeler de bulunmaktadır. Örneğin madde 4.8'de şikayetlerden ve/veya kalibrasyon çalışmaları, dönüştürülerek adli bilişim laboratuvarının şikayet süreçlerini devralabilir. Yukarıda belirtildiği gibi yönetim sistemi maddesi, laboratuvar sonuçlarının kalitesini güvence altına alan laboratuvar yönetim sisteminin kurulması, belgelenmesi, uygulanması ve sürdürülmesi gerekliliğini kapsamaktadır. Maddelerin sistem içerisinde uygulanması zorunlu olduğundan, sistem diğer tüm maddeleri de destekleyebilecek kapasitede olmalıdır. Unutulmamalıdır ki, uluslararası standartların gerekliliklerine dayalı bir yönetim sistemi tasarlamanın, organizasyonun performansını yakalama ve geliştirme konusunda bazı sınırlamaları vardır (Hykš ve Koliš, 2014).

ISO/IEC 17025, özellikle adli bilişim laboratuvarları için tasarlanmasa da, bir yönetim sisteminin tasarlanması durumunda başlangıç olarak faydalı olabilir. Ayrıca, yaygın olarak kullanılan bir Kalite Yönetim Sistemi Standardı olan ISO 9001 bulunmaktadır. Bu Standart, doğası gereği herhangi bir kuruluş tarafından benimsenebilecek bir yönetim sisteminin temel gereksinimlerini sağlar (ISO, 2021).

ISO 9001, bir milyondan fazla sertifikasıyla dünyada en yaygın kullanılan uluslararası standartlardan biridir. Bu uluslararası standardın basitleştirilmiş yapısı Şekil 3.10'da gösterilmektedir (Hykš ve Koliš, 2014).



Şekil 3.10. Süreç açısından ISO 9001'in gereklilikleri

Kaynak: Hykš ve Koliš, 2014

Adli bilişim laboratuvarı yönetim sisteminin tasarlanması durumunda tüm ISO 9001 süreçleri tam olarak uygulanabilir. ISO/IEC 17025 ve ISO 9001'in, adli bilişim laboratuvarı yönetim sisteminin gerekliliklerini yerine getirmek için eşleştirilmesi gerekir çünkü ikisi de sistemin tüm yönlerini kapsamaz. Hykš ve Koliš (2014), Çizelge 3.3'te, ISO/IEC 17025 ve ISO 9001 arasında adli bilişim laboratuvar yönetim sistemi gerekliliklerinin kapsamının karşılaştırmasını özetlemektedir.

Çizelge 3.3. ISO 9001 ve ISO/IEC 17025 gereksinimlerinin kapsamının karşılaştırılması

ISO 9001		**ISO/IEC 17025**	
Madde	**Gereksinim**	**Madde**	**Gereksinimin kapsamı**
4.1	Yönetim sisteminin yapısı ve kapsamı	4.1, 4.2	Kısmen kapsıyor
4.2	Kalite rehberi, dokümanların kontrolü	4.2, 4.3, 4.12	Tamamen kapsıyor
5.1	Üst yönetimin bağlılığının sağlanması	4.1, 4.2, 4.15	Tamamen kapsıyor
5.2	Müşteri gereksinimlerinin belirlenmesi ve yerine getirilmesi	4.4	Tamamen kapsıyor
5.3	Kalite politikası	4.2	Tamamen kapsıyor
5.4	Hedeflerin belirlenmesi ve yönetim sistemi planlaması	4.2	Tamamen kapsıyor
5.5	Sorumluluk ve yetki, kalite yöneticisi ve iç iletişim	4.1, 4.2, 4.11	Kısmen kapsıyor
5.6	Yönetim incelemesi	4.15	Tamamen kapsıyor
6.1	Kaynak sağlanması	4.4, 4.7, 4.10, 5.4, 5.10	Tamamen kapsıyor
6.2	Personel kapasitesi	4.1, 5.2, 5.5	Tamamen kapsıyor
6.3	Altyapı kapasitesi	4.1, 4.6, 4.12, 5.3, 5.4, 5.5, 5.6, 5.8, 5.10	Tamamen kapsıyor
6.4	Çalışma ortamı kapasitesi	5.3	Tamamen kapsıyor
7.1	Hizmet sunumunun planlanması	4.1, 4.2, 5.1, 5.4, 5.9	Tamamen kapsıyor

7.2	Müşteri gereksinimlerinin yerine getirilmesinin sağlanması, müşteri ile iletişimin sağlanması	4.4, 4.5, 4.7, 4.8, 5.4, 5.9, 5.10	Tamamen kapsıyor
7.3	Hizmetlerin tasarımı	5.4, 5.9	Kısmen kapsıyor
7.4	Tedarikçilerin seçimi ve değerlendirilmesi	4.6	Tamamen kapsıyor
7.5	Hizmetlerin sağlanmasının kontrolü, süreçlerin doğrulanması, ürünün tanımlanması ve korunması	4.1, 4.6, 4.12, 5.1, 5.2, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10	Kısmen kapsıyor
7.6	Ölçüm ekipmanlarının kalibrasyonu ve doğrulanması	5.4, 5.5	Tamamen kapsıyor
8.1	Devamlı gelişim	4.10, 5.4, 5.9	Tamamen kapsıyor
8.2	İzleme ve ölçme, iç denetim	4.5, 4.6, 4.9, 4.10, 4.11, 4.14, 5.5, 5.8, 5.9	Kısmen kapsıyor
8.3	Uygun olmayan hizmetlerin kontrolü	4.9	Tamamen kapsıyor
8.4	Veri analizi	4.10, 5.9	Tamamen kapsıyor
8.5	Önleyici ve düzeltici faaliyetler	4.9,4.10, 4.11, 4.12	Tamamen kapsıyor

Kaynak: Hykš ve Koliš, 2014

Kısmi kapsam durumunda, ISO/IEC 17025, ISO 9001 gereksinimlerinin tüm kapsamını kapsamadığından, bunun yerine ISO 9001'deki koşulların kullanılması tavsiye edilmektedir. Öte yandan gerekliliklerin tam olarak karşılanması durumunda bu gereklilikleri yerine getirmek için ISO/IEC 17025 kullanılabilir. Bu Standartlar kapsamındaki yönetim sistemi gereklilikleri arasındaki en büyük boşluk, ISO/IEC 17025, ISO 9001 ile karşılaştırıldığında süreç bazlı bir yapıya ihtiyaç duymaz. Adli bilişim laboratuvarının spesifik faaliyetleri göz önüne alındığında, süreç ve proje yaklaşımını birleştiren model, ISO 9001 gerekliliklerini yerine getirecek şekilde geliştirilmesi gerekmektedir. Bu iki uluslararası standart arasındaki diğer farklar önemsizdir. ISO 9001 ve ISO/IEC

17025 gerekliliklerinin birleşiminin kullanılması, adli bilişim laboratuvarının özelliklerine saygılı, etkili ve verimli bir yönetim sisteminin uygulanmasına yol açacaktır (Hykš ve Koliš, 2014).

Adli bilişim laboratuvarı akreditasyonu tartışmalarından bir tanesi de kullanılan adli bilişim araçlarının doğrulanması veya araçların akreditasyonu konularıdır. Validasyon ve doğrulama arasındaki ayrım, ISO/IEC 17025:2017'de şu şekilde açıklamaktadır;

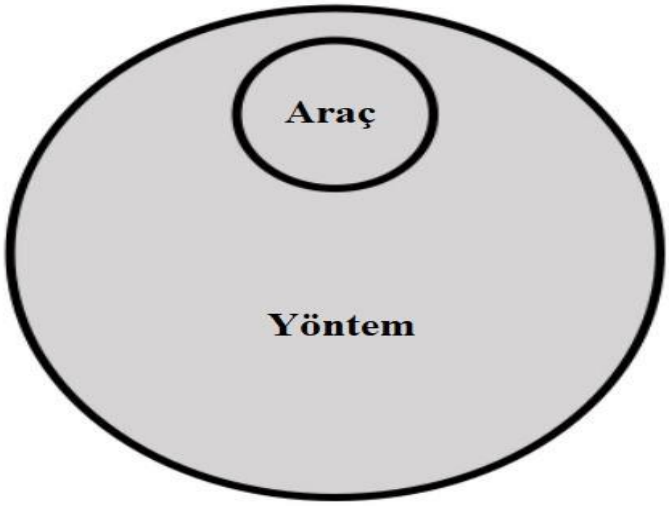
Doğrulama: Belirli bir öğenin belirli gereksinimleri karşıladığına dair nesnel kanıtların sağlanması.

Validasyon: Belirtilen gerekliliklerin amaçlanan kullanıma uygun olduğunun doğrulanması.

Bir başka tanımda ise doğrulama ve validasyon kavramlarının ayrımı için şu sorular konuyu kavramak adına yardımcı olacaktır; Doğrulama için "Ürünü doğru mu üretiyoruz?" validasyon için ise "Doğru ürünü mü üretiyoruz?" (Boehm, 1984).

Araç ve yöntem gereklilikleri ile ilgili olarak Marshall ve Paige (2018) çalışmalarında adli bilişim yöntem tanımları ile gereksinimler arasında bir dereceye kadar örtüşme olduğunu ifade etmektedir. Bu çalışmada örtüşme için üç potansiyel durum gösterilmiştir;

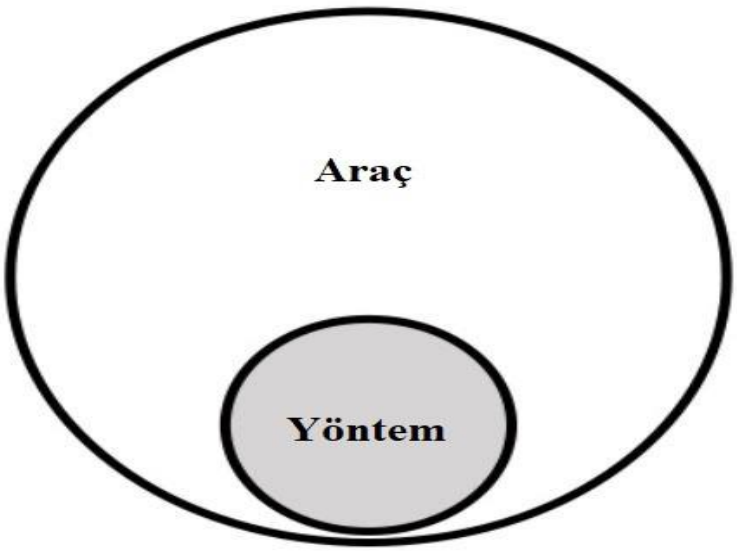
> **Durum 1:** Araç gereksinimlerinin yöntemin bir alt kümesi olduğu yer. Bu durum genellikle spesifik araçlar kullanıldığında veya tanımlanan yöntemin bir parçası olarak küçük bir araç kullanıldığında ortaya çıkar. Bu durumda validasyon gri alanın tümüne uygulanmalıdır. Şekil 3.11'de durum görsel hale getirilmiştir.



Şekil 3.11.Adli bilişim aracının, yöntemin tamamen içinde olduğu durum

Kaynak: Marshall ve Paige, 2018

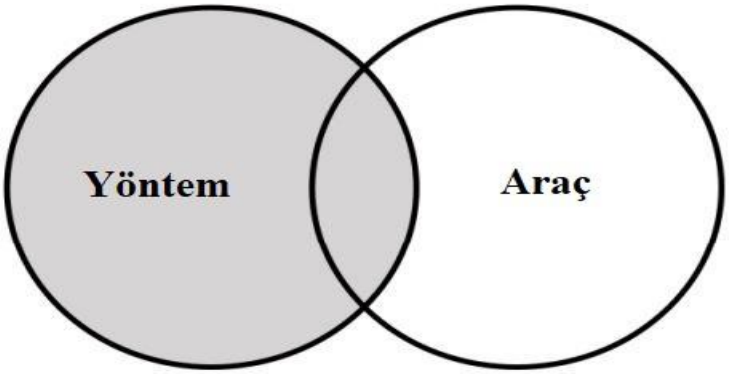
Durum 2: Yöntemin kullanılan adli bilişim aracının bir alt kümesi olduğu durum. Bu senaryo nadirdir ancak yöntemin, aracın üreticisi tarafından tanımlanan süreci tam olarak takip etmesi ve bu kullanımın, aracın işlevselliğinin yalnızca bir alt kümesi olması durumunda mümkündür. Burada yine yöntemin validasyonu önem arz etmektedir. Şekil 3.12'de durum görsel hale getirilmiştir.



Şekil 3.12. Adli bilişim yönteminin, aracın tamamen içinde olduğu durum

Kaynak: Marshall ve Paige, 2018

Durum 3: Araç ile yöntem arasında etkileşimin olduğu ve en yaygın olan durumdur. Bu durumda araç, tüm teknik gereksinimler konusunda yöntemle etkileşime girecek, ancak teknik olmayan ve karşılanmayan başka gereksinimler de olacaktır. Gri alan yine validasyonun kapsadığı yeri göstermektedir. Şekil 3.13'de durum görsel hale getirilmiştir.



Şekil 3.13. Adli bilişim yönteminin ve aracın etkileşimde olduğu durum

Kaynak: Marshall ve Paige, 2018

Marshall ve Paige (2018), söz konusu mekanizmanın pratikte uygulanmasına yönelik araştırmaları sırasında, adli bilişim araç üreticilerinin (yazılım ve donanım), laboratuvarlarının ISO 17025 doğrulama gerekliliklerine uyumu konusunda müşterilerine destek olmalarına izin verilmesinin tavsiye edildiğini belirtmektedir. Öte yandan bu desteğin, ticari açıdan sır olarak tanımlanan bilgilerden taviz verilmeden, test edilen kanıtların açıklanması yoluyla gerçekleştirilmesi gerekmektedir. Ne yazık ki, adli bilişim araçları üreticilerinin çalışmada işbirliği yapamaması veya müşteri gereksinimlerini (Laboratuvar ihtiyaçlarını) nasıl tespit ettiklerine ilişkin ayrıntıları açıklama konusunda isteksiz olmaları nedeniyle bu çalışma, adli bilişim araçları hakkında gerekli bilgiler için herhangi bir değerli sonuca ulaşamamıştır.

ISO 17025 standartlarının tam olarak adli bilişim incelemelerine uymaması konusunda bir diğer noktada adli bilişim incelemelerinde geliştirilen metotların ve kullanılan araçların diğer adli bilimlere kıyasla her zaman aynı ve tutarlı sonucu vermemeleridir. Örneğin, Amerika Birleşik Devletleri kanunlarında dijital deliller için Daubert Standardı uygulanmaktadır. Bu standartta adli bilişim aracından elde edilen çıktıları da içeren bilimsel kanıtların güvenilirliği, Yargıç tarafından (jüri yerine)

ön duruşma "Daubert duruşmasında" belirlenir. Daubert duruşmasında hakimin sorumluluğu, delilleri izole etmek için kullanılan temel metodoloji ve tekniklerin sağlam olup olmadığına ve sonuç olarak delilin güvenilir olup olmadığına karar vermektir. Daubert standardı, bir prosedür değerlendirilirken kılavuz olarak kullanılan dört genel kategoriyi tanımlar:

Test etme: Prosedür test edilebilir mi ve test edildi mi?

Hata oranı: Bu prosedür için bilinen bir hata oranı var mı?

Yayın: Prosedür yayınlandı mı ve hakem değerlendirmesine tabi mi?

Kabul: Prosedür ilgili bilim camiasında genel olarak kabul ediliyor mu?

Bu yaklaşımın eksikliği, bilimin her alanının, özellikle de "daha yeni" alanların hakemli dergilere sahip olmaması, adli bilişimin (veya bilgisayar) kısa geçmişi ve hızla değişen ortamıyla açıkça bu kategoriye girmemesiydi (Watson ve Jones, 2019).

Ayrıca Daubert standardının ve aslında ISO 17025'in bir başka sorunu da belirli bir araç veya yöntemle ilişkili "hata oranlarına" yapılan vurgudur. Çoğu geleneksel adli prosedür bağlamında hata oranları önemlidir. Ancak burada da adli bilişim ile zayıf bir uyum mevcuttur. Bu konu, Dijital Kanıt Üzerine Bilimsel Çalışma Grubu (SWGDE) tarafından, yazarların bu tür hataların türlerini listelediği "Hata Azaltma Analizi ile Adli Bilişim Sonuçlarına Güven Oluşturmak" adlı yayınında tartışılmıştır (Dijital Kanıt Üzerine Bilimsel Çalışma Grubu [SWGDE], 2018). Yazarlar oluşabilecek hata türlerini listelemiş ve bunlardan ne kadar azının hata oranları tahminlerine uygun olduğunu göstermiştir. Çıkan sonuç hiçbir testin, adli bilişim aracının tüm kullanım örneklerinde doğru şekilde çalıştığını kanıtlayamamasıdır. Tüm testler beklenen sonuçları üretse bile yeni bir test senaryosu beklenmedik sonuçları ortaya çıkarmaktadır (Sommer, 2018).

Adli bilişim laboratuvarlarının standardizasyon gerekliliklerine ilişkin yukarıdaki belirtilen konular ve sorunlar, adli bilişim laboratuvarları için tasarlanmamış genel standartların kullanımıyla ilgilidir. Bu standartların adli bilişim kapsamında uygulanması bazı tavizler gerektirir ve genellikle dijital delillerde risk kapsamını azaltamayan kuruluşlara aşırı yük oluşturma eğilimindedir. Ayrıca, genel doğası ve gerekli beceri düzeyleri göz önüne alındığında tutarlılık eksikliğinden kaynaklanan yüksek maliyetler, yapılan testlerin ve doğrulamaların birden fazla yinelenmesine neden olur. Yukarıdaki analiz, yönetim sisteminin tasarlanması konusunda ISO/IEC 17025'in ISO 9001 ile örtüştüğünü vurgulamaktadır; dolayısıyla her ikisi de birlikte ve koordineli uygulandığında adli bilişime dair kalite yönetim

sisteminin tüm yönlerini kapsamak için yeterlidir. Tüm faaliyetlerde tutarlılığı sağlamak için ISO/IEC 17025'in olay öncesinden olay sonrası aşamadaki dosyanın kapatma faaliyetine kadar diğer on adli bilişim standardı ile eşleştirilmesi gerekmektedir. Ayrıca, ISO/IEC 17025'teki gerekliliklerin düzeltilmesi, adli bilişim laboratuvarı durumu için geçerli olmayan öğeler içermesi nedeniyle zorunludur.

3.5. Çalışmaya Dair Seçilen Problem

Adalet sistemi suçluları kovuşturur ve delillere dayalı davaları inceler. Dijital deliller değişkendir ve yargı makamına sunmak için uzman yardımı gerektirmektedir. Dijital delillerin toplanmasından bilirkişi raporunun sunumuna kadar işlenmesi, saklama zincirinin her adımında gerçeğe uygun şekilde korunduğuna dair güvence gerektirmektedir. Uluslararası Standartlar ile bağlantılı bir standardizasyonun ortaya konması, dijital delil süreçlerinin kalitesini ve herkesin delillere duyabileceği güveni sağlayabilir. Bu aşamalar içerisindeki kritik alanlardan biri laboratuvardaki delillerin incelenmesidir. Araştırmacılar, belirli bir adli bilişim laboratuvarı standardının bulunmadığını dile getirmişlerdir. Araştırmacılar, 2000 yılının sonlarında yeni bir standart oluşturmak için bir taslak oluşturmanın gerekliliğini dile getirmişler fakat oluşturulmaya çalışılan bu taslak henüz tamamlanmamıştır. Bu çalışmada adli bilişim standartlarının uygulamaları geliştirmek açısından ne kadar faydalı olduğunu ve oluşturulan dokümanlardaki eksik olan unsurların neler olduğunu göstermek için literatür analiz edilmiştir. Ayrıca çalışmada, laboratuvarlar için en iyi uygulamalar ile uluslararası standartlar arasındaki örtüşmenin analizi ve uygulamaya yönelik mevcut kılavuzun yeterliliği ifade edilmektedir.

Birleşik bir adli bilişim standardının bulunmaması, her bir standardın bir veya daha fazla adli bilişim süreci ve faaliyetini kapsamada rol oynadığı ya da standartlardan birindeki boşluğu tamamladığı, bir dizi birlikte çalışabilen standardın kullanımına yol açmaktadır. ISO/IEC 27000 ailesi dokümanları, adli bilişim soruşturmalarında önemli bir rol oynamaktadır. Yukarıdaki bölümde belirtilen on standart, toplama, inceleme, analiz ve raporlama aşamalarında adli bilişim döngüsüyle etkileşime girer. Buna ek olarak, diğer ISO gruplarından adli laboratuvar gereksinimlerine katkıda bulunan çeşitli ilgili standartlar da bulunmaktadır. ISO/IEC 17025, bir adli bilişim laboratuvarını akredite etmek için kullanılabilecek, laboratuvar operasyonunun yeterliliğine ilişkin genel gereklilikleri belirleyen uygulanabilir bir normatif standarttır. ISO/IEC ayrıca kalite yönetim sistemini oluşturmak için yönetim standardı olarak yeterliliğe dayalı bir ISO 9001'e sahiptir. Aynı zamanda ISO/IEC 17025'in yönetim sistemi bölümündeki boşluğu da doldurmaktadır. Bölüm 4'te, mevcut literatürde bulunan ve adli bilişim laboratuvarlarının kurulumuna ilişkin oluşturulan çeşitli taslak standartlar incelenecektir.

Dünya genelindeki çeşitli kurumların adli bilişim laboratuvarlarına yönelik geliştirdiği taslaklar incelenerek Türkiye'deki duruma yönelik bir analiz yapılacak ve çözüme yönelik önerilerde bulunulacaktır.

4. ADLİ BİLİŞİM LABORATUVARI KURULUMU İÇİN ÖRNEK MODELLER

Çalışmanın bu bölümünde adli bilişim laboratuvarları ile ilgili yapılan bazı standardizasyon çalışmaları ve ortaya çıkan örnek modeller incelenecektir. Modeller uluslararası çapta bazı topluluklar tarafından oluşturulmuş fakat henüz uluslararası bir standarda kavuşmamıştır. Bu nedenle bir rehber niteliğindedir. Fakat yeni kurulacak laboratuvarlara fikir vermesi açısından yararlı olacaktır.

4.1. Avrupa Birliği/Avrupa Konseyi Modeli

Avrupa Konseyi merkezi Strazburg'da bulunan, 1949'da kurulan ve şu anda 46 Avrupa ülkesini kapsayan uluslararası bir organizasyondur. Türkiye'nin de üyesi olduğu organizasyon demokrasiyi, insan haklarını ve hukukun üstünlüğünü teşvik etmek için kurulmuştur. Tüm Avrupa Konseyi üye devletleri insan haklarını, demokratik değerleri ve hukukun üstünlüğünü korumaya dair hazırlanmış Avrupa İnsan Hakları Sözleşmesinin tarafıdır. Avrupa Konseyi, Kadınlara Karşı Şiddeti ve Aile içi Şiddeti Önleme ve bu tür şiddetle Mücadele Sözleşmesi ve Siber Suçlarla Mücadele Sözleşmesi gibi uluslararası sözleşmelerle insan haklarını yaygınlaştırmaya çalışmaktadır. Bu alanda üye ülkelerin kaydettiği ilerlemeyi izler ve bağımsız uzman izleme kurumlarıyla önerilerde bulunur. (COE, 2024).

Budapeşte Sözleşmesi olarak da bilinen Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi 1 Temmuz 2004te yürürlüğe girmiş olup 4 ana bölümden oluşmuş ve sonradan kabul edilen ek protokol ile birlikte 48 maddeyi ihtiva etmektedir. Sözleşmenin amacı internet ortamında işlenen suçlar ve bilgisayar sistemleri ve verileriyle alakalı suçların daha etkin soruşturulması, elektronik delillerin güvenli bir şekilde toplanması ve incelenmesi konularında taraf ülkelerin uyguladığı prosedürlerde bir standart sağlamaktır. Taraf olmayan ülkelere ise bir rehber niteliğinde tavsiyeler vermektedir. Sözleşme taraf ülkelere birtakım yükümlülükler getirmektedir. Adli bilişim ile alakalı gerek teknik konularda gerekse hukuki konularda asgari standartları belirleyip üye ülkelerin bu standartlara uymasını sağlamak sözleşmenin ana hedeflerindendir (Karadeniz, 2022).

Bu amaçla Romanya'nın Bükreş kentindeki Avrupa Konseyi Siber Suç Program Ofisi (C-PROC), Budapeşte standartları temelinde siber suçların ve elektronik kanıtların yarattığı zorluklara yanıt vermek için dünya çapındaki ülkelere yasal sistem kapasitelerini güçlendirme konusunda yardımcı olmaktan sorumlu birim olarak kurulmuştur. Ofis aşağıda belirtilen konularda üye ülkelere destek sağlamaktadır;

- Hukukun üstünlüğü ve insan hakları (veri koruma dahil) standartlarına uygun olarak siber suçlara ve elektronik delillere ilişkin mevzuatın güçlendirilmesi,
- Hakim, savcı ve kolluk kuvvetlerine eğitim,
- Uzman siber suç ve adli bilişim birimlerinin kurulması ve kurumlar arası işbirliğinin geliştirilmesi,
- Kamu/özel sektör işbirliğinin teşvik edilmesi,
- Çocukları çevrimiçi cinsel şiddete karşı koruma,
- Uluslararası işbirliğinin etkinliğinin arttırılması.

C-PROC, kapasite geliştirme işleviyle, Taraf Devletlerin Budapeşte Sözleşmesinin uygulanmasını takip ettiği Siber Suçlar Sözleşmesi Komitesi'nin (The Cybercrime Convention Committee ,T-CY) çalışmalarını tamamlamaktadır (COE, 2024).

Avrupa Konseyi Siber Suç Program Ofisi bu kapsamda ilki 2013-2016 tarihleri arasında gerçekleşen sonrasında 2016-2024 tarihleri arasında daha fazla ülkenin katılımıyla birlikte program genişleterek devam edilen "Siber Suçlara Karşı Küresel Eylem" projesini (Global Action on Cybercrime (GLACY) yapmaktadır. GLACY, Avrupa Birliği ve Avrupa Konseyi'nin Budapeşte Sözleşmesi'nin uygulanmasında dünya çapındaki ülkeleri desteklemeyi amaçlayan ortak bir projesidir. GLACY'nin özel hedefi, Ceza hukuku yetkililerinin, siber suçlara ilişkin Budapeşte Sözleşmesi temelinde siber suçlar ve elektronik deliller konusunda uluslararası işbirliği yapmalarını sağlamaktır. Projenin konuları arasında mevzuatın uyumlaştırılması, adli eğitimler, ülkelerin kanun uygulama kapasiteleri, uluslararası işbirliği, bilgi paylaşımı gibi birçok husus bulunmaktadır (COE,2024).

Üye ülkelerin adli bilişim alanında uzmanları, hukuk alanında hakim ve savcıları, ve akedemik alanda üniversitelerden gelen öğretim üyeleri belirli zamanlarda toplantılar düzenleyerek raporlar ve tavsiye niteliğinde rehberler yayınlamaktadır. Bu çalışma kapsamında inceleyeceğimiz rehber Haziran 2017 yılında yayınlanan "Adli Bilişim-Adli Bilişim Laboratuvarın Yönetimi ve Prosedürleri İçin Temel Kılavuz" belgesidir (COE,2017). Rehber bütünüyle bu çalışmaya konmayacak olup sadece rehberi oluştururken dikkat edilen noktalar ve sistematik incelenecektir. Bazı anahtar noktalara vurgu yapılarak adli bilişim laboratuvarı kurulumunda dikkat edilmesi gereken önemli noktalar öne çıkartılacaktır. Rehber aşağıda belirtilen dört bölümden oluşturulmuştur;

- Giriş
- Adli Bilişim Laboratuvarının Yönetimi
- Adli Bilişim Laboratuvar Süreçleri ve Prosedürleri

- Ekler (Laboratuvarın işletilmesinde kullanılan bazı matbu formlar)

4.1.1. Giriş

Giriş bölümünde rehberin amacı, kimler tarafından kullanılacağı, semboller ve açıklamaları ve adli bilişimin tanımı ve prosedürleri yer almaktadır.

Laboratuvar ortamında izlenecek pratik süreç ve prosedürlerin yanı sıra, laboratuvarın işletilmesiyle ilgili yönetim konularını ve böyle bir laboratuvarın kurulmasındaki stratejik hususları da ele almaktadır. Rehberin aynı zamanda savcıların ve hakimlerin de kullanımına sunulmasına vurgu yapılmaktadır. Her ne kadar yargı mensuplarının hukuk dışındaki beceriler konusunda bilgi sahibi olmaları veya uzmanlaşmaları zorunlu olmasa da, çağdaş suç eylemleri ve bunların failleri, hem savcılık hizmetlerinde hem de mahkemelerde çalışan profesyonellerin siber suçlara ilişkin bilgilerini daha iyi anlamaları ve geliştirmeleri ve bilgi düzeylerini yükseltmeleri için ek baskı oluşturmaktadır. Rehberin onlar tarafından da incelenmesi siber suçlara veya elektronik delillere ilişkin ceza davalarında karar verme yeteneklerini arttıracaktır.

Rehberin amacı, adli bilişim laboratuvarlarının yöneticilerine ve uygulayıcılarına, ürettikleri her türlü delilin gerçekliğinin ve sonradan mahkeme huzurunda kabul edilebilirliğinin teminin sağlayacak şekilde kurulması ve işletilmesi konusunda destek sağlamaktır. Rehberin, adım adım talimatlar içeren bir kullanım kılavuzu olması amaçlanmasa da, bir adli bilişim laboratuvarının geliştirilmesinde ve işletilmesinde sıklıkla ortaya çıkan türdeki sorunlara genel bir bakış sağlanmakta ve bunlarla nasıl başa çıkılacağı konusunda tavsiyeler sunmaktadır. Ayrıca rehber, okuyanların bu tür talimatların ulusal düzeyde olup olmadığını kontrol etmesi için okuyucuya tavsiye vermektedir.

Rehber, mevcut olabilecek donanım ve yazılım seçeneklerine ilişkin herhangi bir öneride bulunmamaktadır. Her ülke ve kuruluş, ihtiyaçları ve mevcut fonları dikkate alınarak neyin uygun olduğuna karar verecektir. Adli bilişim ekipmanlarının ve ticari yazılımların uzun vadeli çok pahalı bir taahhüt olabileceği ve ilk karar verildikten sonra değiştirilmesinin kolay olmadığı unutulmamalıdır.

Bu rehber iki spesifik okuyucu kategorisi için tasarlanmıştır:

1. Genel bir adli bilişim stratejisinin bir parçasını oluşturacak olan adli bilişim laboratuvarının geliştirilmesinden ve yönetiminden sorumlu olanlar,

2. Adli bilişim laboratuvarında adli bilişim süreçleri ve prosedürleriyle ilgili teknik rollerde istihdam edilen personel.

İlk gruba yönelik rehber, adli bilişim stratejileri geliştirmekten sorumlu olanlara, adli bilişimle başa çıkma kapasitesinin oluşturulması konusunda kararlar verenlere ve laboratuvarların yönetiminden sorumlu olanlara yardımcı olmak üzere tasarlanmıştır. Tüm ülkelere, hatta ülkeler içindeki farklı kuruluşlara uygulanabilecek tek bir çözümün olmadığı kabul edilmektedir. Rehber, yöneticilerin pek çoğunun aşina olmadığı bir konu hakkında karar vermelerine yardımcı olmak için tasarlanmıştır.

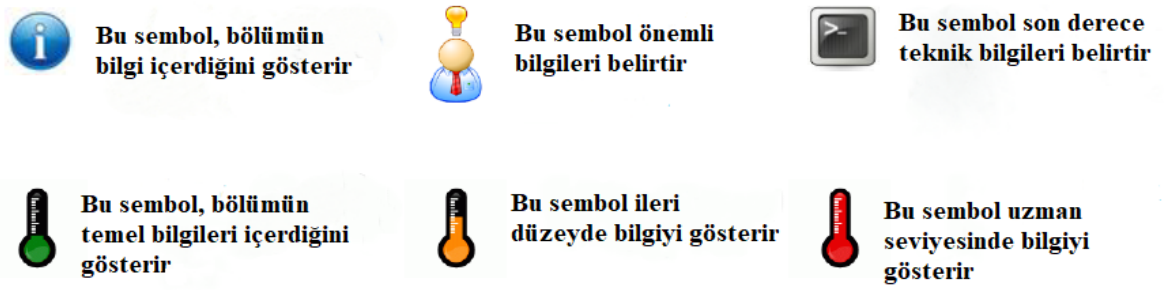
İkinci grup ise laboratuvar faaliyetlerinden doğrudan sorumlu olanlar ile elektronik delillerin elde edilmesi, işlenmesi, analiz edilmesi ve sunulması işlevini yerine getirecek personelden oluşmaktadır. Bu gruba yönelik rehberlik, elektronik delil süreciyle ilgili işlevlere daha spesifik olacak ve ulusal ve uluslararası ceza hukuku sistemlerinin gerekliliklerini karşılayacak prosedürlerin benimsenmesine olanak tanıyacaktır.

Bu rehber, ülkelerin adli bilişim yeteneklerini geliştirirken dikkate alabilecekleri bir şablon belge olarak görülmelidir. Verilen tavsiyelerin, ulusal mevzuat, uygulama ve prosedürlere göre hem stratejik hem de taktik düzeylerde kullanılması amaçlanmaktadır. Elektronik Delil ile ilgili uluslararası düzeyde kabul görmüş genel ilkeler, laboratuvar ortamında yürütülen prosedürlerle aynı derecede ilgilidir ve uyumludur. Rehber hazırlanırken yararlanılan elektronik delillerin incelenmesindeki prensipler aşağıda belirtilmiştir;

1. **Veri bütünlüğü:** Yapılan hiçbir işlem, daha sonra mahkemede delil olarak kullanılabilecek herhangi bir veriyi, elektronik cihazı veya ortamı önemli ölçüde değiştirmemelidir.
2. **Denetim izi:** Elektronik kanıtların işlenmesi sırasında gerçekleştirilen tüm eylemlerin kaydı oluşturulmalı ve daha sonra denetlenebilmeleri için saklanmalıdır. Bağımsız bir üçüncü tarafın yalnızca bu eylemleri tekrarlayabilmesi değil aynı zamanda aynı sonuca ulaşabilmesi de gerekir.
3. **Uzman desteği:** Planlanan bir operasyon sırasında elektronik delil bulunması bekleniyorsa, operasyondan sorumlu kişi bunu uzmanlara/dış danışmanlara zamanında bildirmeli ve mümkünse hazır bulunmalarını sağlamalıdır.
4. **Uygun eğitim:** İlk müdahale ekipleri, olay yerinde uzman bulunmadığı takdirde elektronik kanıtları aramak ve ele geçirmek için gerekli ve uygun eğitime sahip olmalıdır.
5. **Yasallık:** Davadan sorumlu kişi ve kurum, yasalara, delillere ilişkin güvencelere ve genel adli tıp ve usul ilkelerine harfiyen uyulmasını sağlamaktan sorumludur. Okuyucular, adli bilişim süreciyle ilgili kendi ülkelerindeki yasalara ve buradan elde edilen delillerin kabul edilebilirliğine tam olarak hakim olduklarından emin olmalıdırlar. Ulusal hukuk her zaman birincil referans noktası olmalıdır. Rehberde verilen tavsiyelerin herhangi bir ulusal mevzuata

aykırı olması beklenmez veya bu yönde bir niyet yoktur ve her zaman ulusal kanunlara, kurallara ve prosedürlere tabidir.

Ayrıca giriş bölümünde rehber boyunca eşlik ettikleri bölümün içeriğinin önemini veya zorluğunu belirtmek için çeşitli semboller kullanılmıştır. Semboller örnek olarak Şekil 4.1'de gösterilmiştir.



Şekil 4.1. Semboller ve açıklamaları

Giriş bölümü devamında adli bilişimin tanımı ve izlenecek prosedürler için kullanılacak matbu formlar(ekler) tanıtılmıştır. Ekler kısmında bu formlar ayrıca incelenecektir. Son olarak Budapeşte Sözleşmesine atıfta bulunulmuş ve rehberi hazırlarken yararlanılan kaynaklar sayılmıştır.

4.1.2. Adli bilişim laboratuvarının yönetimi

Adli bilişim laboratuvarları dünya çapında özel kurumlar ve kolluk kuvvetleri tarafından düzenli olarak kurulmaktadır. Bazıları profesyonel olarak kurulur ve yoğun yatırım yapılır, diğerleri ise bilgisayarı ve ücretsiz olarak temin edilebilen adli bilişim araçlarına sahip tek bir kişi olabilir. Adli bilişim laboratuvarı kurmayı ve bu laboratuvara güvenmeyi düşünen herkes, kendi yetki alanlarının gereksinimlerini dikkatli bir şekilde araştırmalı ve ülkenin ceza hukuku sistemindeki diğer aktörlerine danışmalıdır. Bu bölüm araştırma, bütçe (kapasite), bina (laboratuvar konumu, güvenliği), görevli personel ve laboratuvarın fiziksel gereklilikleri gibi alt başlıklar altında incelenmiştir. Sistematiği anlamak açısından çalışmamızda aynı sıra takip edilecektir.

4.1.2.1. Araştırma

Dijital cihazlara el konulması, suç türleri, yeri, el koyan görevlilerin uzmanlığı ve varsa adli bilişim analizin yapılıp yapılmadığı hakkında güncel istatistikler oluşturmak için ilk araştırmalar yapılmalıdır. Bu bilgi, bu tür araştırmaların ne kadar hızlı büyüdüğü ve adli bilişim laboratuvarının başlangıç büyüklüğü göz önünde bulundurulduğunda ve yatırım ihtiyacını belirlerken nereden başlanacağı

konusunda uygun bir referans vermelidir. Araştırma, ceza hukuku sistemi içerisinde adli bilişim hizmetlerinin oluşturulmasını ve yönetimini kapsayan herhangi bir yasal veya usule ilişkin gerekliliğin olup olmadığını ortaya koymalıdır. Benzer coğrafya ve demografik yapıya sahip, hâlihazırda adli bilişim yeteneği oluşturmuş olan ülkelerle karşılaştırma yapmak yararlı bir çalışma olacaktır.

Aşağıdaki soruların cevabını bulmak, karar vericilerin oluşturulacak adli bilişim laboratuvarının gereksinimlerinin kapsamını anlamalarına ve tanımalarına yardımcı olacaktır:

- Son 3 yıl, 2 yıl ve 1 yılda dijital verilerin kullanımıyla rapor edilen kaç suç kolaylaştırılmıştır?
- Bu tür soruşturmalarda bariz ve belgelenmiş bir artış var mı?
- Dijital adli soruşturma gerekliyse,

  - Analizi kim yaptı?
  - Prosedürler nerede takip edildi?
  - Sonuç ne oldu?
  - Bazı işlevler mevcut kaynaklarla yürütülemedi mi?

- Benzer gereksinimlere sahip olan ve işbirliği sunulan herhangi bir vakanın kabulünü hızlandırabilecek başka teşkilatlar var mı?

Bu ilk araştırma yapıldıktan sonra karar vericiler, adli bilişim laboratuvarının rolü ve büyüklüğü ile tüm paydaşlara etkili bir kaynak sağlamak için gereken personel sayısı hakkında daha iyi bir fikre sahip olacaktır.

4.1.2.2. Bütçeleme/Kapasite

Bir iş senaryosunu tamamlarken göz önünde bulundurulması gereken birçok faktör vardır. Bunların en önemlisi genel maliyettir. Bu iki ana alana ayrılabilir:

- İlk 'tek seferlik' harcama (sermaye maliyetleri) – Tesis, yenileme, güvenlik, ofis/laboratuvar ekipmanı, donanım ve yazılım.
- Devam eden maliyetler – personel, eğitim, yazılım lisansları, danışmanlık vb.

Aşağıdaki bölümler, bu alanların her biri için özel hususlara yardımcı olacak ve amaca uygun, ölçeklenebilir ve dayanıklı bir adli bilişim laboratuvarının kurulmasına yardımcı olacak daha ayrıntılı bilgiler sağlayacaktır. Bütçenin tam olarak oluşturulması tek seferde yapılacak bir faaliyet olmayıp sürekli güncelleme gerektiren bir husustur.

4.1.2.3. Bina

Talep ve bütçe, uygun tesislerin mevcudiyeti, büyüklüğü ve konumunda önemli bir rol oynayacaktır. Uygun tesisleri belirlerken aşağıdaki faktörler dikkate alınmalıdır;

- **Güvenlik:** Tesisin, hassas kanıt niteliğindeki verileri depolamak ve araştırmak için yeterli güvenliği sağlaması gerekecektir. Güvence altına alınması gereken yalnızca kanıt niteliğindeki veriler değildir, aynı zamanda yöneticilerin kişisel bilgilerin, değerli yazılım ve donanımın ve çalışan personele ait kişisel bilgilerin güvenliğini de dikkate alması gerekir.

  İzinsiz girişin önlenmesi ve tesise gelen ziyaretçilerin izlenmesi, laboratuvara erişimi sınırlanmalıdır. Adli bilişim laboratuvarında tutulan hassas veriler nedeniyle, içerideki delillerin sürekliliğini korumaya yardımcı olmak için bir tür giriş ve çıkış kaydının bulundurulması tavsiye edilir. Bunu yapmanın en basit yolu, giriş/çıkış defterine sahip olmaktır ancak bu, ikinci bir kişinin her zaman hazır bulunmasını gerektirir. Diğer erişim kontrolü türleri arasında fiziksel kilitler ve anahtarlar, elektronik tuş takımları, kaydırmalı kartlar, CCTV ve biyometrik kayıtla ile giriş çıkış bulunur.

  Tesis ideal olarak her odada ve her giriş noktasında (dış kapılar ve pencereler) hareket sensörleri yardımıyla kullanılmalıdır. İzinsiz girişi ve hırsızlığı önlemek için pencereler ve kapılar yeniden güçlendirilmeli ve dış kaynaklardan gözlemlenmeyi önleyecek şekilde kapatılmalıdır.Yangın algılama ve 'kuru' yangın söndürme de önemlidir ve insanları, malzemeleri ve delilleri korumak için uygulanmalıdır.
- **Konum:** Herhangi bir adli bilişim laboratuvarının yerini değerlendirirken çeşitli faktörler devreye girecektir. Uygun tesislerin mevcudiyeti, uygun konumun belirlenmesinde önemli bir faktör olacaktır. İdeal olarak merkezi bir konumda bulunan bir bina tercih edilen bir seçim olacaktır. Laboratuvarın hizmet vereceği iş alanı belirlendikten sonra, iş senaryosunda daha bilinçli bir yer seçimi belirlenecektir.

  Mümkün ise adli bilişim laboratuvarı diğer adli bilimler inceleme alanlarından başka bir binada olmalıdır. Pencerelerin olmaması veya mümkün olduğunca az olması daha iyidir çünkü bunlar ofisin güvenliği açısından bir zafiyettir ve hassas verilerin dışarıdan gözlemlenme olasılığını artırır. Belirlenen yerde pencere varsa, bunlar parmaklık veya panjurla sabitlenmeli ve tüm camlar buzlu veya opak olmalıdır.

  Adli bilişim laboratuvarına delillerin ulaştırılması ve burada incelenmesi, laboratuvarın fiziksel konumu nedeniyle engellenmemelidir. Fiziksel konumla ilgili hususlar şunları içermelidir;

- Zemin katın üzerindeyse, büyük miktarda bilgisayar kanıtını taşımak için bir asansör mevcut mu?
- Otopark laboratuvara ne kadar uzaklıkta?
- Bina veya ofis, verilerin güvenliğini sağlayacak ve içindeki kişileri koruyacak kadar sağlam mı?
- Duvarlar, zemin ve tavan fiziksel veya çevresel hasara dayanabilecek kadar güçlü mü?
- Sel, yangın, doğal afetler ve toplumsal karışıklıklardan kaynaklanan risk nedir?
- Soruşturmalara zarar vermek isteyen terör veya suç örgütlerinin saldırısı engellenebilir mi?

- **Büyüklük:** Herhangi bir laboratuvarın büyüklüğünü değerlendirirken, içinde gerçekleştirilecek çeşitli görevleri hesaba katan değerlendirmeler yapılmalıdır. Kontaminasyon (kirlenme) ve delillerin kaybını önlemek için belirli faaliyet türlerini denemek ve ayırmak en iyi uygulamadır.

  Kanıtların gerçek laboratuvara erişime izin verilmeden teslim edilebileceği veya toplanabileceği resepsiyon tipi bir alan, adli bilişim laboratuvarının planlamasına dahil edilmelidir. Delillerin ve hassas verilerin saklanacağı güvenli bir alana duyulan ihtiyaç yüksek bir önceliktir. Bu, adli bilişim laboratuvarının içinde bulunan bir oda olmalıdır. Alternatif olarak, saklanması muhtemel delil miktarına bağlı olarak sabit bir metal kafes ya da çelik dolaplar kullanılabilir. Depolama odasına her türlü erişim ve delillerin kaldırılması ya da iade edilmesi kayıt altına alınmalıdır. Laboratuvara erişimde olduğu gibi, bunu başarmanın da birçok farklı fiziksel ve sanal yöntemi vardır.

  Her adli bilişim uzmanının ekipmanı için büyük bir masaya, vaka dosyalarını saklayacak dosya dolaplarına ve rahat sandalyelere ihtiyacı olacaktır. Adli bilişim laboratuvarının bir sunucuya ihtiyacı olacaktır; Sunucu, laboratuvar içinde ve varsa ayrı bir odada güvenli bir şekilde saklanabilir.

  Uzmanlara araştırmalarından uzakta olacak şekilde bir dinlenme alanı sağlamak önem arz etmektedir. Brifingler veya toplantılar için ek bir odanın yanı sıra laboratuvar yöneticisinin kullanabileceği ek bir ofisin dikkate alınması tavsiye edilir.

  Yukarıdakilere ek olarak adli bilişim laboratuvarının yerleştirilmesi için en uygun yerin seçilmesinde, fotokopi makineleri, yazıcılar, tarayıcılar, dosyalar, eşya çantaları, etiketler, kanıt etiketleri, ofis ekipmanı ve personelin kişisel eşyaları gibi delil niteliğinde olmayan ekipmanların depolanmasına ayrılmış alanlar da dikkate alınmalıdır.

  Seçilen bina veya ofis, dijital adli soruşturma talebinde beklenen bir artış olması durumunda genişleyecek kadar büyük olmalıdır. Gerekli laboratuvar boyutunu belirledikten sonra böyle

bir tesisin ömrü düşünülmeli mevcut birçok adli bilişim tesisinin, iş yükündeki katlanarak artan artışlar nedeniyle kısa sürede yer değiştirmeyi veya genişlemeyi gerekli bulduğu akıldan çıkarılmamalıdır. Araştırma aşamasında toplanan bilgiler gelecekteki genişleme ihtiyacına ilişkin iyi bir fikir verecektir. Yer değiştirmek veya genişletmek son derece pahalıdır, bu nedenle ilk iş planında genişlemeye yer açmak faydalı olabilir.

- **Havalandırma:** Çalışan birçok bilgisayarın bulunduğu bir oda çok fazla ısı üreteceğinden, klima hayati önem taşımaktadır. Bir sunucu kendi alanına konumlandırılmışsa bu alanın soğutulması gerekir. Aşırı ısınma veri kaybına ve donanımın zarar görmesine neden olabilir. İdeal olarak bir ekstraksiyon ünitesi satın alınmalı ve personele en yüksek konforu sağlayacak ve laboratuvarın sıcaklık ve nemini kontrol edecek bir alana kurulmalıdır. Saklanan kanıtların bozulmasını önlemek için delil depolama birimlerinin kendi kliması veya iklim kontrol sistemi olmalıdır.

4.1.2.4. Görevli personel

İş gerekçesini belirleyen ve hazırlayan kişinin laboratuvar yöneticisi olması veya böyle bir yöneticinin işe alımlarda yer alması muhtemeldir. En iyi uygulama, laboratuvar yöneticisinin, laboratuvar içindeki farklı rolleri yerine getirecek personelin işe alınması sürecine dâhil edilmesi gerektiğini göstermektedir.

Laboratuvarın büyüklüğüne ve personel sayısına bağlı olarak, gerekli olan farklı fonksiyonları dikkate almaları gerekir. Ekibin her üyesinin kendi iş tanımını net bir şekilde anlayabilmesi için personelin rolleri ve sorumluluklarının belgelenmesi ve ayrıntılı iş tanımlarının hazırlanması gerekecektir. Pek çok adli bilişim laboratuvarında yüksek vasıflı personelin, zamanlarının çoğunu kendi kapasite seviyelerinin altındaki sıradan görevleri üstlenerek harcadığını gösteren güçlü kanıtlar vardır. Bunu önlemek için üstlenilecek faaliyetlerin iş profillerinde açıkça tanımlanması gerektiğini bilmek önemlidir. Dikkate alınması gereken rol ve sorumluluklar aşağıdakileri içerir;

- **Laboratuvar Yöneticisi:** Yöneticinin ileri düzeyde teknik bilgiye sahip olması ve elektronik delillere ilişkin yasal gerekliliklerin yanı sıra izlenecek prosedür ve süreçlere ilişkin güçlü bir anlayışa sahip olması gerekir. Laboratuvar yöneticisi, laboratuvarın orijinal kurulumu, binanın tanımlanması, ekipman ve yazılımın satın alınması ve laboratuvarın prosedür ve işlevlerinin belirlenmesi üzerinde kontrole sahip olmalıdır. Birim içinde çalışan herkesin işe alınmasından, eğitilmesinden, danışmanlığından ve yönlendirilmesinden sorumlu olmalıdırlar.

- **Adli Bilişim Uzmanı:** Uzmanlar teknik bilgiye ve mümkün olduğu yerde uygun niteliklere ihtiyaç duyacaktır. İdeal olarak adli bilişim yazılımı kullanımı konusunda eğitim almış olmaları gerekir. Alternatif olarak bu personelin kendilerini uygun bir beceri düzeyine ulaştırmak için özel adli bilişim eğitimi alması gerekecektir. Adli bilişim uzmanlarının mevzuat bilgisine sahip olması ve farklı suç türlerini araştırırken kanıtlanması gereken noktaların farkında olması gerekir. Bu roller analitik ve araştırmacı bir zihniyet gerektirir; adli bilişim uzmanı bulgularını açık ve anlaşılır bir formatta sunabilmelidir. Adli bilişim uzmanlarının iyi sözlü ve yazılı iletişim becerilerine sahip olması önemlidir.
- **Adli Bilişim Teknikeri:** Adli bilişim teknikerinin rolü, bilgisayar sabit disklerinin ve diğer depolama ortamlarının adli açıdan sağlam kopyalarını (imajlarını) almaktır. Laboratuvarın büyüklüğüne bağlı olarak birden fazla teknisyene ihtiyaç duyulabilir. Adli bilişim teknikerinin iyi bir teknik bilgiye sahip olması ve dijital verileri adli olarak elde etmenin çeşitli yöntemleri hakkında bilgi sahibi olması gerekecektir. Temel beceri gereksinimlerinden biri, ayrıntılara dikkat etmek ve tüm eylemleri açıkça belgeleyebilmek, imajı alınan verilerin doğrulanması ve kanıtların sürekliliğidir.
- **Yönetim:** Kanıtların devamlılığı ve gözetim zincirinin gerekli şekilde kaydedilmesi her laboratuvarın önemli rollerinden biridir. Laboratuvarın büyüklüğüne ve incelenecek elektronik kanıt miktarına bağlı olarak yönetici rolünün doldurulması gerekebilir. İşin büyüklüğüne göre yönetim kısmı birden fazla kişiden oluşabilir. Yönetim her yeni vakayı belgeleme, delil numaralarını/seri numaralarını kontrol etme ve vaka dosyalarının muhasebeleştirilmesi sorumluluğunu üstlenecektir. Diğer hususlar şunları içerir:
    - Soruşturmanın ciddiyeti hakkında karar vermek,
    - Vakaların önceliklendirilmesi.
    - Bilgilerin vaka yönetimi sistemine girilmesi.
    - Dış kurumlarla, kolluk kuvvetleri ile ve laboratuvar ekibinin geri kalanıyla irtibat.
    - Güçlü sözlü ve yazılı iletişim ve detaylara dikkat.

İşe alım, iş gerekçesi kabul edildikten ve tesisler belirlendikten hemen sonra başlamalıdır. Donanım ve yazılımın tanımlanması ve seçimine yardımcı olacak kilit personelin hazır bulunması faydalı olacaktır. Bu kilit personel hâlihazırda eğitim almış veya belirli bir adli yazılım türüne aşina olabilir ve bununla çalışmayı tercih edebilir.

Bazı adli bilişim laboratuvarlarında tamamen kolluk kuvvetleri bazılarında yalnızca destek personeli, bazılarında ise her ikisinin birleşimi bulunabilmektedir. Her seçeneğin artıları ve eksileri vardır.

Kolluk kuvvetleri daha iyi soruşturma bilgisine sahip olma eğilimindedir ve mevzuata ve cezai eylemi kanıtlayacak noktalara daha aşinadır. Diğer iş fırsatlarına geçme olasılıkları daha düşüktür ve mesai saatleri dışında da çalışmaya daha fazla alışkındırlar.

Destek personeli (kolluk kuvveti olmayan) daha üstün teknik niteliklere sahip olabilir ve daha fazla eğitim almış olabilir. Dijital verilerin araştırılmasında pratik deneyime sahip olabilirler ancak kariyerlerinde ilerleme ve özel sektöre geçme konusunda daha istekli olabilirler. Her ikisinin karışımı genel teknik yeteneğinizi geliştirebilir ve daha çeşitli bir ekip oluşturabilir.

Adli bilişim laboratuvarında çalışmak üzere işe alınan kişinin bir tür özgeçmiş kontrolü veya hakkında güvenlik incelemesi yapılması gerekecektir. Laboratuvardaki tüm personel, hassas verilere ve ciddi suç faaliyetlerine ilişkin kanıtlara erişebilecektir. Kendisinin veya yakınlarının daha önce herhangi bir suç faaliyetine, özellikle de sahtekârlık ve terör suçlarına karışmadığının tespit edilmesi önemlidir. Ayrıca kendilerini rüşvete veya yolsuzluğa açık hale getirebilecek mali zorlukların olup olmadığının belirlenmesi de ihtiyatlı bir davranış olacaktır.

Personel işe alındıktan sonra yeteneklerini sürekli olarak geliştirmek, personeli motive etmek ve elde tutmak önemlidir. Ulaşılabilir bir personel geliştirme programının oluşturulması bunu destekleyebilir. İlk belgeler, rollerini ve sorumluluklarını, üstlerini ve amirlerini açıkça göstermelidir. Bu ilk belgeler, acil eğitim ihtiyaçlarını veya isteklerini tanımlamalı ve bu planı ele almak üzere kabul edilen düzenlemeleri kaydetmelidir. Bu tür düzenlemeler, personeli eğitim kurslarına gönderebilir veya planlanan bir zaman dilimi içerisinde onların meslektaşlarını takip etmeleri ve onlardan öğrenmeleri için düzenleme yapabilir. Örneğin, tüm adli bilişim uzmanlarının, adli bilişim araçlarını kullanma güvenini ve mahkemede güvenilir delil sunma hususunu sağlamak için harici sertifikalı eğitime ihtiyacı olacaktır.

Teknolojideki gelişmeler çok hızlı ilerlemektedir ve adli bilişim uzmanlarının, adli bilişim bilimindeki gelişmelere ayak uydurabilmeleri için düzenli olarak eğitilmeleri gerekmektedir. Yönetimin ayrıca bu uzmanların araştırma ve geliştirme yapması için vaka incelemesi dışında biraz zaman ayırması gerekecektir. Yeni araçlar ve uygulamalar piyasaya çıktıkça, uzmanlar adli bilişim laboratuvarı için değerli araçları belirlemek amacıyla bunları değerlendirmelidir.

Personelin devamlılığı, başarılı bir adli bilişim laboratuvarını yönetmenin anahtarı olacaktır. Personelin eğitimi için çok fazla zaman ve para harcanacaktır ve özellikle eğitilip daha deneyimli olmaya başladıktan sonra personelin elde tutulması hayati önem taşımaktadır. Her bir personel için sağlam kişisel gelişim planlarına sahip olmak, onlara hedefler sunacak ve kariyer yolları ile gelecekteki

fırsatları daha iyi anlamalarını sağlayacaktır. Personeli elde tutmanın sadece maaş meselesi olmadığı her zaman unutulmamalıdır. Personelin gelişebileceği bir çalışma ortamının geliştirilmesi aynı derecede önemlidir.

Personel mentorluğu, gelişim ve eğitim açısından eşit öneme sahiptir. Mentorluk, deneyimli bir personelin yeni bir personele deneme süresi boyunca destek sunması sürecidir. Uygun olması halinde deneme süresi, bireyin eğitim ve gelişim düzeyi belirlendikten sonra belirlenmelidir. Mentorun rolü rehberlik ve destek, muhtemelen bir arkadaş ve sırdaş olmanın yanı sıra bilgi kaynağıdır. Mentor ihtiyacının zaman geçtikçe azalacağı, yeni personelin yeni görevine alışmasıyla ise tamamen ortadan kalkacağı öngörülmektedir.

Tüm personelin, ilerlemelerini tartışmak için bölüm yöneticileriyle düzenli değerlendirmelere ihtiyacı olacaktır. Bunların 6 aylık aralıklarla yapılması ve son 6 aydaki performanslarının ve gelecek 6 ay için ihtiyaç/gereksinim ve isteklerinin gözden geçirilmesi önerilmektedir.

Adli bilişim laboratuvarları genellikle hızlı tempolu ve streslidir. Ciddi cezai soruşturmalarla uğraşırken, soruşturmacılar şüpheliyi daha fazla gözaltına almak, suçlamak veya serbest bırakmak ya da mağdurların daha fazla acı çekmesini önlemek için delil niteliğinde sonuçlar elde etmek için baskı yaparken, zaman baskısıyla karşılaşılması yaygındır. Baskı altında hatalar yapılabileceğinden uzmanların çalışmalarının izlenmesi gerekir. Yöneticilerin, bireylerin iş yükünü değerlendirmek için uzmanlarını gözlemlemesi ve vaka çalışması stresli hale gelirse destek ve müdahale sunması gerekir.

Uzmanlar için tek sorun zaman baskısı değildir. Birçok vakada çocuk istismarı, cinsel istismar veya terörizm konularını tasvir eden üzücü resimler, videolar ve metinler yer almaktadır. Bazı durumlarda bu tür delillerin miktarı strese neden olabilir; Bazen dijital görüntülerde tasvir edilen ahlaksızlık uzmanı daha fazla etkileyecektir. Yöneticinin, laboratuvara gelen vakaları uzmanlara dağıtımı sırasında dikkat etmesi gereken bir nokta da aynı uzmana sürekli aynı çeşit vakaların verilmemesidir. Laboratuvar personelinin tavır ve davranışları izlenmelidir; böylece herhangi bir sorun, daha da büyüyüp personelin sağlığını olumsuz yönde etkileme fırsatına sahip olmadan önce tanımlanıp ele alınabilir.

Tüm laboratuvar personeline düzenli danışmanlık sunulması gerektiği önemli noktalardan birisidir. Bu danışmanlık 3 ila 6 aylık düzenli aralıklarla sağlanmalıdır ve personel, meslektaşları arasında olumsuz bir algı yaratılacağı korkusuyla danışmanlık hizmeti almak konusunda isteksiz olabileceğinden, zorunlu olması halinde daha etkili olabilir.

Teknolojinin büyümeye devam edeceği ve suçluların dijital cihazların kullanımıyla daha fazla suç işleyeceği yaygın olarak kabul edilmektedir. Bu nedenle, ekibin her bir üyesini, ihtiyaç duyulduğunda daha üst düzey bir rol üstlenmeye istekli ve yetenekli olmaları konusunda eğiten, destekleyen ve yetiştiren bir program sunarak laboratuvarın büyümesine hazırlanmak mantıklı olacaktır. Yedekleme planlaması, eğitimli personeli yetiştirmenin ve elde tutmanın etkili bir yöntemidir. Yaşanan olaylar, yetenekli, deneyimli ve nitelikli adli bilişim uzmanlarının elde tutulmasının zor olduğunu göstermektedir. Bir yedekleme planının oluşturulması, birçok adli bilişim laboratuvarında uzun ömürlülüğü ve başarıyı desteklemektedir.

Laboratuvar yöneticisi, tüm personelin ve laboratuvara gelen ziyaretçilerin sağlık ve güvenliğinin sağlanması sorumluluğunu üstlenmelidir. Mevcut koşulları ve durumları inceleyerek ve tehlikeli olduğu, sağlık veya güvenliğe zarar verme potansiyeli olduğu düşünülen her şeyi ele alarak risk değerlendirmeleri yapmalıdır. Yönetici aynı zamanda yasal sağlık ve güvenlik gereksinimlerinin de farkında olmalıdır. Sağlık ve güvenlik önlemleri laboratuvarı ziyaret edebilecek kişiler için de eşit şekilde uygulanmalı ve bu kişilerin yasa dışı veya rahatsız edici materyalleri görmemelerini veya bunlara maruz kalmamalarını sağlayacak önlemler alınmalıdır. Adli bilişim laboratuvarlarında karşılaşılan standart sağlık ve güvenlik özelliklerinden bazıları şunlardır:

- Anti-statik paspaslar ve bilek kayışları – ekipman ve delillerin statik hasar görmesi riskini azaltır,
- Kirlenmiş Maddeler – cerrahi eldiven veya diğer koruyucu giysilerin kullanımıyla temasın önlenmesi,
- Taşıma/kaldırma - yaralanmaları önlemek için personelin ağır eşyaları kaldırmanın doğru yolunu bilmesini sağlamak,
- Kauçuk paspas – elektrik çarpması riskini azaltmak için,
- Devre kesiciler - elektrik çarpması veya verilerin zarar görmesi riskini azaltmak için.

4.1.2.5. Fiziksel laboratuvar gereksinimleri

Uygun tesislerin konumu belirlendikten ve adli bilişim ekibi için ilk işe alım süreçleri başladıktan sonra, fiziksel laboratuvarın kurulmasının değerlendirilmesi önemlidir.

- **Ofis Ekipmanı:** Herhangi bir laboratuvarın büyüklüğü, gerekli ofis ekipmanının miktarını belirleyecektir.

Yönetim masası - İdeal olarak, iki monitörü ve iki bilgisayarı, bir telefonu ve önemli miktarda evrakı alabilecek kadar büyük bir resepsiyon masası gerektiren bir alan olması gerekmektedir. Ayrıca, bu delillerin yönetim tarafından kontrol edilmesine, belgelenmesine ve kaydedilmesine olanak sağlamak amacıyla, gelen ve giden delillerin ve vaka kâğıtlarının saklanacağı bitişikte geniş alanlı bir masaya sahip olunması yararlı olacaktır. Yönetici için bir sandalye ve ziyaretçiler için bir sandalye düşünülebilir. Bu alanın laboratuvarın geri kalanından daha az güvenli olacağı ve dolayısıyla bu alanda hiçbir vaka kağıdının veya hassas evrakın saklanmaması öngörülmektedir.

Delil deposu – Bu tesis, çeşitli bilgisayar ve cep telefonu kanıtlarını önemli bir süre boyunca saklayacak kadar büyük olmalıdır. Bilgisayarlar her şekil ve boyutta olabilir ve bazı sunucular çok büyük ve ağırdır. Bunun tersine, cep telefonları ve harici depolama aygıtları, güvenli bir şekilde saklanmadıkları takdirde kolaylıkla zarar görebilir veya kaybolabilir. Delil deposu erişim kontrolü olan güvenli bir oda olmalıdır. Ağır eşyaların çok uzaklara taşınması ihtiyacını ortadan kaldırmak için yönetime ve kopya alma alanına yakın yerleştirilmelidir. İdeal olarak, her durumda delillerin kolayca tanımlanmasını sağlamak amacıyla delilleri ayırmak için güçlü raflar ve bir numaralandırma sistemi kurulmalıdır. Her bir vaka için delillerin kesin konumu vaka yönetimi sistemine not edilmeli ve kopya alma tamamlandıktan sonra deliller aynı konuma geri gönderilmelidir. Faraday korumasını uygulayarak güvenli depoyu radyo dalgalarından yalıtmayı da düşünmek faydalı olabilir. Bu, kablosuz iletişim özelliğine sahip cihazların izolasyonunu sağlayacaktır. Polis nezaretindeyken mobil cihazların içeriklerinin uzaktan silindiği vakalar rapor edilmiştir. Faraday kafesi çok pahalıdır ve Faraday torbalarının kullanılması bir alternatif olabilir. Son çare olarak geçici önlem olarak cihazların tamamen güçlü gümüş folyo ile kapatılması cihazlarla iletişimi engelleyecektir.

Adli kopya alma departmanı – Bilgisayarlar kopyası alınmak üzere sökülürken, kopya alma departmanı, vidaların ve küçük bileşenlerin kaybını önlemek için tercihen yükseltilmiş kenarlara sahip geniş, temiz bir yüzey alanına ihtiyaç duyacaktır. Tüm çalışma yüzeylerinde antistatik matlar bulunmalıdır. Kopya alma öncesinde tüm kanıtların fotoğraflanması gerektiğinden, dijital kamera ve pil şarj cihazları için bir alan düzenlenmelidir. Her kopya alan personel, iki monitörü ve iki bilgisayarı, kopya alma donanımını, telefonu ve evrakları alabilecek kadar geniş bir masa alanına ihtiyaç duyacaktır. Her kopya alan personel için bir sandalye, tercihen konforlu bir operatör koltuğu, bel desteği ve yükseklik ayarı da sağlanmalıdır.

Uzmanın İş İstasyonu- Adli bilişim uzmanı, birkaç monitörü, iki bilgisayarı, çeşitli evrakları, mobil cihazları ve mobil cihaz çıkarma donanımlarını ve araçlarını tutacak kadar büyük bir

masa alanına ihtiyaç duyacaktır. Monitör başında geçirilen zamanın miktarı nedeniyle yine rahat bir sandalye faydalı olacaktır. Ayrıca masaların, başkalarının yanlışlıkla ekranlardaki hassas verileri görüntülemesini önleyecek şekilde konumlandırılması veya bölme tipi bir ortam sağlamak için iş istasyonlarının arasına gizlilik ekranları yerleştirilmesi de tavsiye edilebilir.

Sunucu odası – Merkezi sunucuya ayrılan alanın, içinde saklanabilecek hassas veri miktarı nedeniyle güvenli olması gerekecektir. Aşırı ısınmayı önlemek için yeterli klimaya ve UPS(güç kaynağı) için alana ihtiyaç duyulmaktadır.

- **Yazılım ve Donanım: Donanım** – Adli bilişim laboratuvarı, birçok hassas verinin analiz edildiği ve depolandığı yüksek teknolojiye sahip bir ortam olmalıdır. Bu nedenle her türlü dış bağlantıdan izole edilmiş bir inceleme ağına ihtiyaç duyulacaktır. Tüm laboratuvar personeli bu ağı kullanacağından, bu ağın dayanıklı, güvenli ve hızlı olması gerekecektir. Herhangi bir sunucu veya sistemi kurarken en iyi uygulama, mevcut en yüksek işlem gücünü ve uygun bir veri depolama dizisini tercih etmek olacaktır. Bu sistem, ya tüm sunuculara ayrı ayrı sağlanacak şekilde ya da laboratuvar içindeki yalnızca özel bir bilgisayara sağlanacak şekilde ekibe İnternet erişimi sağlamalıdır. Bu, uzmanlara ve personele e-postaları kontrol etmek, araştırma yapmak, yamaları, güncellemeleri ve araçları indirmek için kolay kullanım olanağı sağlamalıdır.

  Her uzman, iki monitörün işlerini kolaylaştırmasını tercih eder. Nihai raporlarını oluşturmaya gelince, raporun bir ekranda açık olması ve soruşturmanın diğer ekranda olması çok daha kolaydır. Ayrıca çok sayıda küçük resmi görüntülerken de yardımcı olabilir. Bu ekstra bir masraf olsa da, bu görüntüleme yeteneğine sahip olmanın faydaları, uzmanların kanıt için daha doğru raporlar sunmasını destekleyebilecek sağlam bir sistemin yanı sıra zaman tasarrufu da sağlayacaktır.

  Kopya alma bilgisayarlarından sorumlu olanlar, verilerde ve orijinal kanıtların bütünlüğünde herhangi bir değişikliği önlemek için sterilize edilmiş depolama disklerine ve yazma engelleyicilere ihtiyaç duyacaktır. Piyasada çok sayıda yazma engelleyici türü ve ayrıca kullanılabilecek çeşitli yazılım araçları bulunmaktadır.

  Laboratuvar, işletim verilerinin yedeklenmesine ek olarak üç ek depolama sorunu türüyle de ilgilenecektir; orijinal kanıtlar, adli olarak oluşturulan kopyalar ve soruşturma sonrasında oluşturulan veriler. Tüm bunların nasıl saklanacağı, arşivleneceği ve yedekleneceği konusuna dikkat edilmelidir. Dayanıklılık sağlamak için sıkı bir yedekleme ve arşiv rejimi uygulanmalıdır.

  Adli bilişim ekibinden herhangi birinin arama emirlerinin uygulanmasına yardımcı olması ve 'sahada' veri toplama ve analiz yapması muhtemelse, 'sahada' bir kite ihtiyaç duyacaklardır (Ek-

2’ de örnek bir taşınabilir iş istasyonu konfigürasyonu mevcuttur). Taşınabilir bir iş istasyonu veya dizüstü bilgisayar ve kopya alma araçlarına ek olarak, aşağıdaki ekipmanların satın alınmasına da dikkat edilmelidir;

- Eşya çantaları, güvenlik etiketleri ve delil etiketleri
- El feneri
- Tornavidalar
- Steril eldiven ve giysiler
- Bant
- İletişim cihazları
- Güç uzatmaları, kablo uçları ve adaptörler
- Kamera, video kaydedici
- Ekipmanın taşınması için saklama kutuları veya uygun çanta.

Yazılım – Çoğu adli bilişim yazılım türüyle ilişkili olarak yalnızca ilk satın almanın değil aynı zamanda devam eden lisanslama, destek ve eğitim maliyetlerinin de bulunduğunu dikkate almak önemlidir. Lisansların başlangıç ve devam eden maliyetleri önemli olabilir ve edinilen donanım ve yazılımın laboratuvar gereksinimlerine ve personelin tercihine doğru şekilde uyduğundan emin olmak için satın almadan önce araştırma yapılmalıdır. Ek-1, bir laboratuvar yöneticisinin, işlevselliğin yanı sıra satın alma, lisans yenileme ve eğitim maliyetlerini de dikkate alarak farklı adli yazılım ürünleri arasında nasıl bir karşılaştırma oluşturabileceğini gösteren örnek bir matris göstermektedir.

Bazı adli bilişim uzmanlarının tüm araştırmaları açık kaynak veya ücretsiz yazılım kullanarak yürütebildiğini belirtmekte fayda var; ancak bu tür ürünlerle ilgili destek ve eğitim fırsatlarının eksikliği söz konusudur. Çoğu standart 'ikili araç doğrulaması' gerektirecektir ve uzmanların bulgularını karşılaştırıp doğrulaması için ek yazılım satın alınması gerekebilir.

Herhangi bir laboratuvarın düzgün çalışması için temel gereksinim, bir tür vaka yönetimi sistemidir. Bu, laboratuvarda tutulan deliller ve vakalarla ilgili tüm idari bilgileri içeren bir veri tabanıdır ve uzmanların süreçlerinin bütünlüğü açısından temel olacaktır. Bir vaka yönetimi sistemi minimum aşağıdaki bilgileri içermelidir:

- Delili laboratuvara teslim eden ve teslim alan tarih, saat ve kişi,
- Yazılım tarafından oluşturulan benzersiz referans numarası,
- Vaka numarası veya suç numarası,

- Talep makamı/soruşturma görevlisi/savcının adı ve iletişim bilgileri,
- Suçun türü,
- Delillerle temas kuran tüm laboratuvar personeli,
- Kanıtlanması gereken noktalar veya soruşturmadan beklenenler,
- Zaman Faktörleri (Teslimat tarihleri ve beklenen mahkeme tarihleri vb.),
- Kopya alınma tarihi (Kim tarafından ve kopyası alınan öğelerin ayrıntıları),
- Alınan kopyanın hash sonuçları,
- Soruşturmanın başlatıldığı tarih,
- Soruşturmaya katılan adli bilişim görevlileri ve personeli,
- Meslektaşlar ve yöneticiler tarafından yapılan kalite güvencesinin ayrıntıları,
- Soruşturmanın tamamlandığı tarih,
- Soruşturmanın sonucu,
- Delillerin toplandığı tarih ve saat bilgileri.

Tüm bu bilgiler, eylemlerin ve kanıtların sürekliliğini, güvenilirliğini ve doğrulanmasını göstermek açısından hayati öneme sahiptir. Adli laboratuvar mevcut ticari yazılım paketlerinden birini kullanmadığı sürece, bir yazılım veri tabanı teknik açıdan yetkin bir kişi tarafından oluşturulmalıdır.

- **Kalite güvencesi/inceleme prosedürü:** Her türlü delilde olduğu gibi, dijital bulguların da mahkemeye sunulduktan sonra sorgulanması mümkündür. Elektronik delillerin değişken doğası nedeniyle, delillerin bütünlüğünü ve bulguların geçerliliğini sağlayacak adımların atılması zorunludur. Laboratuvar tarafından üstlenilen işin kalitesini izlemeye yönelik prosedürlerin en baştan oluşturulması ve uygulanması çok önemlidir. Tüm personel ve yöneticiler, kalite yönetim sistemindeki rolleri konusunda tam bilgi sahibi olmalı ve tüm durumlarda prosedürlere uymalıdır. Rastgele kalite yönetim kontrolleri, laboratuvarlar arası karşılaştırmalar ve idari incelemeler, bir vakanın tamamlanmış olarak etiketlenmesinden önce gerçekleştirilmelidir.

  Yöneticiler, kaliteyi, bilgi güvenliğini ve adli bilişim tekniklerinin doğrulanmasını sürdürmek için tanınmış, dışarıdan denetlenen standartların getirilmesini dikkate almalıdır (ISO 9001, ISO 27001, ISO 17025 gibi).
- **Triyaj İncelemesi ve Raporlama:** Başlangıçtan itibaren iş yükünün önceliklendirilmesine yönelik yöntemlerin uygulamaya konulması mantıklı olacaktır. Daha ciddi veya zaman açısından kritik vakaları tespit eden ve bunları öncelik listesine yerleştiren bir sürece sahip

olunarak, acil ve acil olmayan vakalarda verimli personel akışını destekleyecek etkili bir sistem oluşturulur. Triyaj için düşünülen tüm durumlarda risk değerlendirmesi yapılmalı ve kararlar kaydedilmelidir. Bir mahkeme gelecekte bu tür kararların ardındaki gerekçeleri inceleyebilmeli ve değerlendirebilmelidir.

- **Verilerin saklanması:** Yoğun bir adli bilişim laboratuvarında bir veri saklama politikasının yürürlükte olması önemlidir. Eğer bu uygulanmazsa ve baştan takip edilmezse, laboratuvarda verileri tutmak için yeterli depolama alanının bulunmadığı bir durum hızla ortaya çıkabilir. Uygulandıktan sonra laboratuvarın hâlâ uyumlu olduğundan emin olmak için düzenli kontroller yapılmalıdır. Bazı yargı bölgelerinde, özellikle ciddi durumlarda, verilerin saklanmasına ilişkin yasal gereklilikler vardır. Bu tür gereklilikler herhangi bir politikanın ön saflarında yer almalıdır.
- **Tüm paydaşların eğitimi ve öğretimi:** Laboratuvarın göreve başlamasından önce talep makamlarına bir bilgisayar, tablet, telefon veya herhangi bir dijital cihazın incelenmesinden makul olarak ne beklenebileceği konusunda bilgi verilmelidir.

  Elektronik delillere el konulması sırasında hataları önlemek için, kolluk kuvvetlerine, dijital cihazlara el konulduğu sırada eylemlerinin sonuçlarını tam olarak değerlendirmeleri için talimatlar içeren kılavuz ve rehberlerin dağıtılması gerekli olacaktır. Savcılar ve hâkimler ayrıca, soruşturma veya hüküm vermekte oldukları münferit davalarda doğru prosedürlerin benimsendiğinden emin olmak için kolluğun izlediği prosedürler hakkında da bilgi sahibi olmalıdır.

4.1.3. Adli bilişim laboratuvar süreçleri ve prosedürleri

Bu bölüm, genellikle adli bilişim incelemesinde yer alan süreç ve prosedürleri kapsar. Ana süreçlere daha iyi bir genel bakış sağlamak amacıyla genel, kronolojik bir süreç modeli kullanılır. Adli bilişim incelemesinin tüm aşamalarında, elektronik delillerin özelliklerinin hatırlanması hayati önem taşımaktadır.

Açıklayıcı metne ek olarak, süreç ve prosedürlerin daha hızlı anlaşılmasına ve hatırlanmasına görsel olarak yardımcı olmak amacıyla bir dizi faydalı kaynak oluşturulmuştur. Bu kaynaklar ekler bölümünde yer almakta olup ileriki bölümde gösterilecektir.

Rehberin bu bölümünde adli bilişim aşamalarından bahsedilmektedir. Aşamalarda kullanılan teknikler ve metotlar kapsamlı ve karmaşık olmalarından dolayı sadece tanımları ve yapılacak işin niteliği özet olarak anlatılacaktır.

4.1.3.1. Genel süreç modeli

Adli bilişim incelemesi içeren bir vakada standart prosedür genellikle dört aşamadan oluşur:

- ✓ Toplama(Edinim)
- ✓ İnceleme (İşleme)
- ✓ Analiz
- ✓ Raporlama(Sunum)

Aşağıdaki alt bölümlerde bu aşamalar daha ayrıntılı olarak açıklanacaktır. Her aşama ayrıntılı olarak açıklanan çeşitli prosedürlerden oluşur.

Her durum farklı olduğundan yukarıdaki aşamaların tümü her zaman gerekli değildir. Laboratuvar yöneticileri, örneğin son derece acil durumlarda veya alışılmadık derecede yüksek miktarda veri içeren durumlarda, toplama adımının atlanabileceğine ve işleme aşamasında triyaj yaklaşımının takip edilebileceğine, analiz aşamasının ise aşırı derecede kısaltılabileceğine karar verebilir. Bu tür kararlar soruşturmanın amacına ve davanın özelliklerine bağlı olmalıdır.

4.1.3.2 Toplama (Edinim) aşaması

Elektronik delillerin adli açıdan sağlam bir şekilde elde edilmesi gerekmektedir. Verilerin elde edilmesi, genellikle, bir arama sırasında çalışan bir bilgisayar sisteminden uçucu verilerin toplanmasıyla veya ele geçirilen bir bilgisayardan bir depolama ortamının elde edilmesiyle veya bir soruşturma sırasında herhangi bir başka aşamada gerçekleştirilir. Toplama adımında özel olarak tanımlanmış ve test edilmiş prosedürlerin uygulanması, geri dönüşü olmayan hataların yapılmaması için çok önemlidir. Toplama sürecinin akış şeması Ek-3'te gösterilmiştir. Gözetim zincirinin her aşamada sağlam tutulması, tüm adımların dikkatlice belgelenmesi ve elde edilen tüm görsellerin ve kopyaların doğrulanması önemlidir. Genel yönergelere her zaman uyulmasını sağlamak için çok dikkatli olunmalıdır. Edinme sürecini başlatmayı düşünmeden önce, laboratuvar yöneticisi ya da delil işlem görevlisi, veri edinimi için uygun iznin mevcut olup olmadığını kontrol etmelidir (mahkeme kararı, savcı kararı vb.). Uygun izin mevcutsa delillerin doğru teslimine özel dikkat gösterilmelidir. Aşağıdaki hususlara özellikle dikkat edilmelidir:

- ✓ Tüm deliller etiketlendi mi?
- ✓ Tüm delil etiketleri eksiksiz ve doğru şekilde doldurulmuş mu?
- ✓ Delil kaydı tam ve doğru mu?

- ✓ Gözetim zinciri tam olarak belgelenmiş mi?
- ✓ Delillerde herhangi bir hasar var mı? Eğer öyleyse, bunlar belgelendi mi?
- ✓ Tüm güvenlik mühürleri sağlam mı?
- ✓ Dahili depolama ortamı da dahil olmak üzere tüm delillerin fotoğrafı çekilmelidir.

Örnek bir gözetim zinciri kaydı Ek 7'de yer almaktadır.

- **Bilgisayarların Toplanması (Edinimi) :** Orijinal kanıtların bütünlüğünü korumak için, kopya alma teknisyenleri ve adli bilişim uzmanları, bu bölümde açıklandığı gibi bir bilgisayar sisteminin depolama ortamının adli açıdan sağlam bir şekilde kopyasını almalıdır. Bu adli kopya daha sonra adli bilişim incelemesindeki tüm sonraki adımların temeli olacaktır.

  Edinme sürecinin amacı, bilgisayarın depolama ortamının adli açıdan sağlam bir kopyasını/imajını üretmek olduğundan, adli bilişim uzmanının bu kopyanın, kendisine ait olmayan başka herhangi bir veri içermeyen bir hedef ortamda saklanmasını sağlaması gerekir. Hedef kopyanın/imajın diğer verilerle (örneğin incelemeyi yapan kişinin dosyalarından veya geçmiş vakalardan) çapraz kontaminasyonunu önlemek için, yeni kopyayı tutması gereken ortamın sterilize edilmesi gerekir.

  Bir bilgisayarı analiz etmek, bir araştırmacının fiziksel bir suç mahallini incelemesine benzer; çünkü delillerin bozulmadan, mümkün olduğunca orijinal durumuna yakın ve kirlenmemiş olarak korunması gerekir. Geleneksel suç mahalli araştırmacıları, parmak izi ve DNA kanıtlarıyla oynanmasını önlemek için eldiven ve tulum kullanırken, adli bilişim incelemecileri, yazma engelleme mekanizmalarını kullanarak orijinal depolama ortamının veri bütünlüğünü korumalıdır. Tipik olarak iki tür yazma engelleme yöntemi vardır; bir yanda donanım yazma engelleyicileri, diğer yanda yazılım yazma engelleyicileri. Donanım yazma engelleyicileri genellikle iki farklı çeşitte mevcuttur; Bir adli iş istasyonuna veya kopya alma sunucusuna bağlı olan yazmayı engelleyen cihazlar veya bir bilgisayar sistemine bağlı değilken bağlı bir depolama ortamına yazma-engelleyen disk çoğaltıcılar. Mümkün olan her yerde donanım tabanlı yazma engelleyiciler veya disk çoğaltıcılar kullanılmalıdır çünkü bunlar delil üzerine yazma işlemlerini fiziksel olarak engeller ve bunu yaparken çok güvenilir çalışırlar.

  Bir depolama ortamının kopyasının alınması, özel kopya alma yazılımı kullanılarak yapılabilir. Bu sürece yardımcı olabilecek ücretsiz ve ticari ürünler mevcuttur. Parça parça kopya veya adli kopya formatlarından birinde kopya alabilen ve kopyayı doğrulayabilen güvenilir ve hızlı yazılım seçilmelidir.

Fiziksel ve mantıksal olacak şekilde iki tür kopya vardır. Fiziksel bir kopya tüm ham verileri içerirken, mantıksal bir kopya genellikle tüm bu verilerin yalnızca tahsis edilmiş bir alt kümesini içerir. Örneğin disk düzeyinde fiziksel bir kopya, bölümleme şeması, tüm bölümler ve hatta bölümlenmemiş alanlar da dâhil olmak üzere tüm diski içerirken, disk düzeyindeki mantıksal bir kopya yalnızca bir mantıksal bölümün kopyasıdır.

Bir adli bilişim uzmanının genellikle tüm diskin tam fiziksel kopyasını hedeflemesi gerekir çünkü bu, silinmiş ve önceden tahsis edilmiş alanları içermektedir. Bununla birlikte, şifrelemeyle uğraşırken, şifrelenmiş verilerin fiziksel bir kopyası yerine kilidi açılmış verilerin mantıksal bir kopyası tercih edilir. Kopya alma işlemine dair örnek bir form Ek-8'de gösterilmiştir.

Adli bilişim sürecinin sonraki aşamalarında, tüm ileri işlemler ve analizler genellikle verilerin adli kopyası üzerinde gerçekleştirilir. Bu nedenle orijinal depolama ortamının ve kopyanın tamamen aynı verileri içerdiğini doğrulamak çok önemlidir. Bunu kanıtlamak için her iki veri setine de matematiksel bir algoritma uygulanmalıdır. Bu algoritma hash değeri adı verilen çok karmaşık bir sayı üretir. Her iki dosyanın/cihazın hash değeri aynıysa, dosyalar/cihazların aynı olduğu kabul edilir. En ufak bir değişiklik hash değerinde büyük bir farka neden olacaktır. En yaygın kullanılan hash algoritmaları MD5, SHA-1 ve SHA-256'dır. Tek hash algoritmaları karma çarpışmalara maruz kalabileceğinden, kopyayı/görüntüyü doğrulamak için en az iki hash algoritmasının kullanılması tavsiye edilir.

Hash doğrulamalarının kopya alma sürecinde iki noktada yapılması iyi bir uygulamadır. Orijinal ortamın hash değerinin üretilebilmesi için ilk hash hesaplamasının kopya alma işleminin başında yapılması gerekir. İkinci hash hesaplaması kopya alma işleminin sonunda yapılmalıdır. Bu ikinci hesaplamanın, orijinal ortamdaki verilerin görüntüleme işlemi sırasında değişmediğini ve kopya/görüntü üzerindeki verilerin tam olarak aynı olduğunu kanıtlamak için hem orijinal ortam hem de kopya/görüntü üzerinde yapılması gerekir. Hash tabanlı doğrulama olumlu bir sonuç getirse bile, adli bilişim uzmanı, verilerin orijinal göründüğünden ve verilerin görüntüleme süreci öncesinde veya sırasında değiştirilmiş veya tahrif edilmiş olabileceğini düşündüren herhangi bir özellik sergilemediğinden emin olmak için verileri önceden incelemelidir.

Bir adli bilişim laboratuvarının, adli kopyaların yedeklerini saklayacak bir depolama tesisine sahip olması gerekir. Yalnızca bir yedeğe değil, aynı zamanda başka bir yedeğe de sahip olmak iyi bir uygulamadır. Adli bilişim uzmanı, kendi çalışma kopyasıyla analizi yürütürken, başka bir sistemde (örn. kopya alma sunucusu) saklanan bir yedek bulunmalıdır.

- **Mobil Cihazların Toplanması (Edinimi):** Bilgisayar tabanlı incelemelerde olduğu gibi, mobil cihazların edinimi sırasında amaç, mobil cihazda depolanan verilerin mümkün olan en iyi kopyasını üretmektir. Ancak mobil cihazlarda, cihazın kendi sınırlamaları ve mevcut adli bilişim çözümlerinin sınırlamaları nedeniyle orijinal verilerin tam ve sağlam bir kopyasını oluşturmak mümkün olmayabilir. Bir mobil cihazın mümkün olan en iyi kopyasını elde etmek için, kopya alma işlemine izin verecek şekilde cihazda değişiklikler yapılması gerekebilir.

  Adli bilişim görevlileri, mobil cihazları kullanırken, pil içerdiklerinden ve kaza ile kolayca açılabildiklerinden ekstra dikkatli olmalıdır. Bunun, son kullanım için saat ve tarih bilgileri gibi süreçteki kanıt niteliğindeki verileri değiştirmesi muhtemeldir. Uzmanlar, ilk kullanım sırasında güç düğmelerini tanımlamaya ve ağ izolasyonunu her zaman sağlamaya özel dikkat göstermelidir.

  Birçok cihaz, kopya işlemlerinin 'Canlı' durumdayken yapılmasını gerektirdiğinden, 'İzolasyon' aşaması önemlidir. Bu, incelemeyi yapan kişinin, kopya alma boyunca cihazın işleyişini kullanabilmesi için cihazı açması gerekeceği anlamına gelir. Mobil cihazın izole edilmemesi ve ilgili mobil ağ veya kablosuz internet bağlantısı gibi harici ağlara bağlanmasına izin verilmemesi durumunda cihazdaki veriler değişebilir. Bunun bir örneği, bazı mobil cihazları uzaktan silmenin mümkün olmasıdır.

  Mobil cihaz delilinin kopya alma işlemine geçmeden önce tanımlanması gerekir. Cihazda, eğer cep telefonu ise, genellikle ahizenin iç kısmına yapıştırılmış veya cihazın arkasında basılı bir ekipman etiketi bulunur. Etiket, Uluslararası Mobil Ekipman Kimlik Numarasını (IMEI), Mobil Ekipman Kimlik Numarasını (MEID) veya Seri Numarasını içerecektir. Bu veriler, cihazları benzersiz şekilde tanımlamak için kullanılabilir. Daha sonra marka, model ve IMEI/MEID bilgileri, hangi düzeyde desteğin mevcut olduğunu belirlemek amacıyla adli bilişim paketlerini kullanarak cihazı aramak için kullanılabilir.

  Ayrıca bu aşamada, cihazdan hangi kanıtların istendiğini belirlemek için, sorumlu memur tarafından delille birlikte verilen vaka evrakları incelenmelidir. Bu, incelemeyi yapan kişinin incelemenin hangi düzeyde yapılması gerektiği konusunda karar vermesine yardımcı olabilir. Tam incelemeden önce cihazın sahibinden bilinen tüm şifreler, alınmaya çalışılmalıdır. Bu, cihaz için hangi seviyede destek mevcut olursa olsun, en azından canlı ve kullanıcının erişebildiği verilere erişim verilebilmesini sağlayacaktır.

Bu bilgi toplandıktan sonra adli bilişim uzmanı, cihazı ve SIM/IDEN kartları veya hafıza kartları gibi ilgili ek medya kartlarını nasıl inceleyeceklerine ilişkin bir eylem planı hazırlamalıdır. Bu plan, SIM / IDEN kart(lar)ından ve hafıza kart(lar)ından (varsa) veri edinilmesini ve incelemenin hangi düzeyde ve neden gerçekleştirileceğini içermelidir.

Mobil cihazların kopyaları alınırken, daha önce incelenen delillerle ilgili herhangi bir veri içermeyen temiz bir hedef ortamın kullanılması en iyi uygulama olarak kabul edilir. Laboratuvar veya klonlanmış SIM kartları kullanılıyorsa, inceleme görevlileri laboratuvar SIM kartının son takılan SIM kartındaki verileri içerdiğinden emin olmalıdır.

Cep telefonlarına kopya alınırken uygulanan bazı özel teknikler nedeniyle (IOS için bootloader, Android için rooting vb.) yazma engelleme yazılım ve donanımları kullanmak oldukça zordur. Bu nedenle, incelemecinin mobil cihazları kullanırken yaptıkları eylemlerin sonuçlarının tam olarak farkında olması ve bu eylemleri tutarlı bir şekilde açıklayabilmesi zorunludur.

İncelemenin tüm aşamalarında, incelenen mobil cihazın tüm dış bağlantılardan izole edilmesi önemlidir. Bu, cihazın depolanan verileri değiştirmesini önler. Bir dizi modern cihaz, uzaktan (ve güvenli bir şekilde) silinme kapasitesine sahiptir. Cihazların izole edilmesi bu durumun önlenmesine yardımcı olacaktır.

Mobil cihazlar, ayrı işleme ve araştırma teknikleri gerektiren üç farklı ortamla sunulur:

- SIM / IDEN Kartları – Uzman cep telefonu adli bilişim araçları ve ekipmanı gerektirir.
- Hafıza Kartları – Bilgisayarın sabit diski veya flash sürücüsü olarak incelenebilir.
- Cihazın Dahili Belleği – Uzman adli bilişim araçları ve yazılımı gerektirir.

Bu cihazların kopyalarının alınmasını ve verilerin incelenmesini destekleyecek yeterli donanımın yanı sıra gerekli adli bilişim araçları da laboratuvara sağlanmalıdır.

Bu aşamada SIM/IDEN kartının mantıksal edinimi ve hafıza kartının fiziksel edinimi gerçekleştirilmelidir. Hafıza kartı ancak incelendikten sonra cihaza geri takılmalıdır. Bunun nedeni, bazı telefonların hafıza kartında veri saklamasıdır ve eğer hafıza kartı mevcut değilse, bu durum telefonda veri kaybına neden olabilir. Zaman ve kaynaklar izin veriyorsa, hafıza kartının bire bir kopyası oluşturulmalı ve bu klon telefona yerleştirilmelidir. Cihazı mobil ağdan izole etmek için, cihazda bulunan SIM/IDEN kartının inceleme süresince cihazın dışında kalması iyi bir uygulamadır. Bununla birlikte, SIM/IDEN kart içeren cihazların çoğunluğu,

açıldığında bu kartın içinde bulunmasını gerektirir veya veri kaybına karşı hassastır. Bununla mücadele etmek için, cihaz içinde bir laboratuvar veya klonlanmış SIM/IDEN oluşturulur ve kullanılır, böylece cihaz bir SIM/IDEN kartının varlığını fark eder, ancak yine de herhangi bir mobil ağ ile iletişim. Bu aşamada eğer cihaz bootloader fiziki incelemesi için adli çözümlerle destekleniyorsa bunun yapılması gerekmektedir. Çoğu zaman bu, SIM/IDEN kartına gerek kalmadan gerçekleştirilebilir. Bu, adli çözümün cihaza bir önyükleyici yüklemesine ve cihazı belirli bir şekilde başlatmasına olanak tanır; bu, cihazdaki kullanıcı verilerinde herhangi bir değişiklik yapmadan cihazın dahili belleğinin tamamının kopyalanmasına olanak tanır. Bu nitelikteki bir fiziksel inceleme aynı zamanda, PIN'ler veya modeller gibi herhangi bir cihaz kilit kodunu potansiyel olarak kurtarabilir ve bu, adli bilişim uzmanının, cihaz açıldıktan sonra cihaza tam erişim elde etmesine olanak tanır.

İncelenen cihaz bu tür bir inceleme için desteklenmiyorsa, cihaz herhangi bir ağdan izole edilmiş haldeyken açılmalıdır. Kullanıcı korumasıyla karşılaşılırsa ve cihazın yanında PIN, şifre veya desen sağlanmadıysa, adli bilişim uzmanı korumayı atlayarak mümkün olan en iyi düzeyde incelemeyi denemelidir. Bunun mümkün olmaması durumunda incelemeden önce kullanıcının PIN kodu, şifresi veya deseni istenecektir. PIN, şifre veya desen incelemeden önce zaten biliniyorsa, cihaza tam erişim sağlanabilmesi için bu girilmelidir. Koruma için doğru çözümün elde edilmesi mümkün değilse, verilere erişmek için tipik PIN'leri veya kalıpları denemek gerekli olabilir. Yanlış kodun çok fazla denenmesi durumunda birçok cihaz güvenli veri imhası uygulayacağından, bu risksiz değildir. Doğru olan bulununcaya kadar tüm olası kombinasyonları tahmin ederek şifrelere "Brute-Force" tekniği uygulayabilen ticari adli bilişim araçları mevcuttur. Parolaları tahmin ederken, bilinen gerçeklerden (doğum tarihleri veya diğer parolalar gibi) veya bilinen yaygın parolalardan (1234, 1379, 0000 vb. gibi) oluşan bir sözlük oluşturmak en iyisidir.

Mevcut ve seçilen ekstraksiyon aracına bağlı olarak kopya alma süreci değişecektir. Çoğu adli bilişim aracında, başarılı bir çıkarma işlemi oluşturmak için izlenmesi gereken prosedürü açıklayan bir kılavuz bulunur. Elektronik deliller üzerindeki etkiyi en aza indirmek ve verilerin bütünlüğünü mümkün olan en yüksek standartta korumaya çalışmak her aşamada önemlidir. Bazı mobil cihazlarda, cihazlardan başarıyla veri çıkarmak için sistem dosyalarını veya işletim sistemini değiştirmenin veya bazı durumlarda özel bir uygulamayı yükleyip kurmanın gerekli olabileceğini dikkate almak önemlidir.

Mobil cihazların analizi genellikle özel bir yazılımın ve doğru kablonun kullanılmasını gerektirir. JTAG veya Chip-Off gibi daha gelişmiş inceleme teknikleri, lehimleme ekipmanı ve cihazın bellek yongalarından ham verileri okumak için özel aparatlar dahil olmak üzere daha fazla araç gerektirecektir.

Mobil cihazlar için beş farklı inceleme düzeyi vardır ve mümkün olan en iyi çıkarım ilk sırada listelenir:

- Fiziksel
- Dosya Sistemi Dökümü (File System Dump-FSD)
- Mantıksal
- Manuel
- JTAG / Chip-Off / Rooting / Jail Breaking

Cihazın fiziksel bir kopyası, tüm ham ikili verilerin cihazın deposundan alınması işlemidir. Bu ham verilerin daha sonraki bir aşamada yazılım tarafından analiz edilmesi ve işlenmesi gerekir. Bu yöntem tipik olarak, incelemecinin canlı ve silinmiş verilere, işletim sistemi dosyalarına ve normalde kullanıcının erişemediği cihaz alanlarına erişmesine olanak sağlar.

Mobil cihazlar için bilgisayar cihazlarından farklı olarak daha fazla kopya alma stratejisi mevcuttur. Diğer ana strateji ise Dosya Sistemi Dökümüdür (File System Dump-FSD). Bir FSD, Fiziksel ve Mantıksal edinimin bir melezi gibidir. FSD'ler, cihazın dosya sistemini alır ve işleme aşamasında verileri yorumlar. Bu, incelemecilerin, örneğin mantıksal bir alımda mevcut olmayabilecek ve fiziksel bir alım sırasında erişilemeyebilecek silinmiş mesajları tutan veritabanlarını almasına olanak tanır. Ancak, fiziksel bir alımla geri getirilmesi mümkün olan silinmiş verilerin tümü bir FSD sırasında edinilmeyecektir.

Mobil cihazın mantıksal olarak edinilmesi, cihazdan bilgilerin alınmasını ve cihazın verileri analiz için sunmasına izin verilmesini içerecektir. Bu genellikle cihazın kendisindeki verilere erişmeye eşdeğerdir. Bu yöntem genellikle yalnızca canlı verileri incelemecinin kullanımına sunacaktır. Başka bir yöntem bulunmuyorsa “manuel inceleme” adı verilen yönteme başvurulabilir. Bu yöntem, cihaza ulaşarak ekranda görüntülenen verilerin fotoğraflarla kaydedilmesini, videoya kaydedilmesini veya verilerin yazıya geçirilmesini içerir. Verilerin gereksiz yere değiştirilmemesine ve bilgilerin doğru kaydedilmesine dikkat edilmelidir. Bu yöntemle yalnızca mobil cihazın gösterdiği veriler kurtarılabilir. Örneğin bazı mobil cihazlar tam saat ve tarih bilgilerini göstermeyebilir.

Hasar görmüş veya kilitlenmiş mobil cihazlar için iki yöntem daha kullanılabilir. Bunlar JTAG ve Chip-Off incelemeleridir. JTAG incelemesi, cihazın ana kartına kadar cihazın sökülmesini ve karttaki bağlantılara bazı bağlantıların lehimlenmesini gerektirir. Bu, incelemecinin cihazda depolanan verilerin tam fiziksel kopyasını almasını sağlar. Chip-Off aynı zamanda aygıtın tam fiziksel kopyasının çıkarılmasına da olanak tanır, ancak aygıtın bellek yongasının bellek kartından kalıcı olarak çıkarılmasını gerektirir.

Bazı mobil cihazlara yapılabilecek daha az yıkıcı bir diğer değişiklik, cihazı "Rootlama" veya "Jail Breaking" olarak bilinen işlemdir. Bu süreç, çalışan kullanıcının izinlerini yükseltmek için işletim sisteminin özelliklerinden yararlanmayı içerir. Bu süreç, sistem dosyalarının değiştirilmesini içerir ve potansiyel olarak cihaza zarar verebilir ve bu nedenle, kullanılan teknikler listesinin alt sıralarında yer almalıdır.

Çıkarma girişimlerinin sırası önemlidir. İncelemeciler, en az tahribatlı ve en fazla verimi sağlayacak inceleme yöntemini ilk önce uygulamaya çalışmalıdır. Bu, incelemecilerin daha sonraki aşamalarda hasar görebilecek veya üzerine yazılabilecek alanları yakalamasına olanak tanır. JTAG ve Chip-Off gibi çıkarma yöntemleri yalnızca son çare olarak düşünülmelidir, çünkü özellikle Chip-Off'ta süreç yıkıcı ve kurtarılamaz olabilir.

Veriler çıkarıldıktan sonra, çıkarılan bu veriler cihazda manuel olarak doğrulanmalıdır. Bu, adli bilişim uzmanının, adli çözüm tarafından elde edilen verilerin, doğru saat/tarih bilgileri gibi, cihazda görüntülenen verilerle eşleşip eşleşmediğini kontrol etmesini gerektirecektir. Bu, çıkarılan verilerdeki hataları veya verilerin eksik olup olmadığını belirler (Çoğu zaman Facebook Messenger sohbet dizileri gibi tüm sohbet mesajları cihazdan çıkarılmaz). Herhangi bir tutarsızlık varsa, eksik veya yanlış verileri denemek ve elde etmek için daha fazla çıkarma yapılabilir veya verileri manuel olarak kaydetmek için manuel bir inceleme yapılabilir.

4.1.3.3. İnceleme (İşleme) aşaması

İşleme sırasında adli bilişim uzmanları belirli cihazlara veya verilere öncelik verebilir ve ele geçirilen herhangi bir dijital depolama içeriğinin tam bir kopyasını üretebilir. Kopya üzerinde çalışarak (asla orijinal değil) akıllı, duruma özel filtreler (veri madenciliği) uygulayabilirler veya sadece kopyayı işleyebilirler (örn. silinen dosyaları kurtararak, kapsayıcıları monte ederek, şifrelemeyi kırarak, internet geçmişi, sohbet gibi uygulama verilerini ayrıştırarak vb.). Bu işleme adımları, belirli vaka kategorileri için sıklıkla tekrarlanabilir. Kaynak açısından yoğun olmalarına ve çok fazla bilgi işlem gücüne ve zamana ihtiyaç duymalarına rağmen, genellikle gece boyunca, hafta sonu boyunca veya

kullanılmayan ikinci bir adli iş istasyonunda çalıştırılabilirler. İnceleme sürecinin akış şeması Ek-4'te gösterilmiştir.

- **Bilgisayarların İncelenmesi (İşlenmesi):** Bilgisayarların tuttukları verile gün geçtikçe artmaktadır. Yapılacak işleri hızlı bir şekilde halledip aynı zamanda çok yüksek miktarda veriyi depolamak uzmanlar için kolay olmayabilir. Bu nedenle farklı işleme yaklaşımları dikkate alınmalıdır. Bunlardan ilki vakaya özel hususları incelemektir. Bir vakayı incelemeden önce vaka memuruna bu vaka için ne tür verilere ihtiyaç duyulduğunu sormak önemlidir. Sağlanan bilgiler, hangi verilerin ilgili olduğu ve hangi verilerin filtrelenebileceği kapsamını içermelidir. Bu bilgiye dayanarak uzman hangi işleme seçeneklerinin uygulanabileceğini değerlendirebilir. Diğer bir yöntem Triyaj yöntemidir. Çok sayıda bilgisayar sistemi ve depolama ortamının kullanıldığı durumlarda, adli bilişim laboratuvarının her delili makul bir süre içinde analiz etmesi mümkün olmayabilir. İşte o zaman bir triyaj tekniği yardımcı olabilir. Adli bilişim bağlamında önceliklendirme, hangi vakanın, hangi delilin ve hangi tür verinin ilk olarak, ikinci olarak vb. inceleneceğini belirlemek için vakalara veya faaliyetlere öncelik verilen süreçtir. Bu süreç, bazı delillerin veya verilerin hiç incelenmemesi (özel triyaj) veya bazı verilerin daha sonraki bir aşamada analiz edilmesi (öncelik triyaj) olarak ayrılabilir. Triyaj, araştırmanın değerini, karmaşıklığını, maliyetini ve araştırmanın gerçekleştirilmesi gereken sırayı dikkate alır. Triyaj bazı avantajlar sunarken, ele alınması gereken dezavantajlar da vardır. Triyaj tam bir incelemenin yerini alamaz. Bu nedenle triyaj günlük olarak kullanılmamalıdır. Kanıt elde etmek için yalnızca otomatik tekniklerin kullanılması ve/veya tüm verilerin yalnızca küçük bir alt kümesinin incelenmesi, kanıtların gözden kaçması riskini beraberinde getirir. Çok kısa bir zaman diliminde analiz edilecek çok sayıda delilin bulunması, yasal sorunlar nedeniyle delillerin muhafaza edilemiyor olması, mümkün olduğu kadar çabuk bilgi almanın önemli olduğu durumlarda (örneğin terör vakalarında) triyaj işlemi kullanılabilir.

  Diskin ayrılan alanlarında hiçbir kanıt dosyası bulunamazsa, silinen verilerin kurtarılması önemli olabilir. Veri kurtarma farklı düzeylerde mümkündür. Her şeyden önce adli bilişim uzmanı, adli yazılımda bir diskin tüm bölümlerinin gösterilip gösterilmediğini veya kayda değer bölüm boşlukları olup olmadığını kontrol etmelidir. Bir kopyaya analiz edilmeden önce filtrelerin uygulanması, adli bilişim uzmanının görüntülemesi ve analiz etmesi gereken veri miktarının azaltılmasına yardımcı olabilir. Popüler filtreleme teknikleri, bilinen işletim sistemi veya program dosyalarını filtrelemek (beyaz listeye alma) veya bilinen yasa dışı materyallerin

veri tabanlarıyla hash eşleşmelerini özel olarak aramak (kara listeye alma) için hash setleri kullanmaktır.

- **Mobil Cihazların İncelenmesi (İşlenmesi):** Bilgisayar delillerinin işlenmesinde olduğu gibi, cep telefonlarının sayısı ve depolama kapasitesi de artmaktadır. Bu artışın yanı sıra, eklenen işlevsellik ve mobil cihazlara olan bağımlılık, adli analiz için zengin miktarda verinin kullanılmasına yol açmaktadır. Mobil cihazların işlenmesi, cihazlar arasında kullanılan donanım ve yazılımların çok değişken olması nedeniyle genellikle bilgisayarlara göre farklı bir yaklaşım gerektirir. Uygulamalar çok daha sık güncellenir ve değişiklikler genellikle büyük olabilir. Bu nedenle, özel adli bilişim araçları verilerin çoğunu otomatik olarak işleyecektir, ancak bu işlemenin manuel olarak doğrulanması genellikle gereklidir. Mobil verilerin filtrelenmesi genellikle veri türü düzeyinde gerçekleştirilir. Veriler, iletişim verileri ve medya dosyaları gibi gruplar halinde işlenirken araçlar tarafından filtrelenir. Bu gruplar daha sonra daha da bölünür; örneğin iletişim verileri çağrı kayıtlarına ve mesajlara bölünebilir. Uzmana sunulan filtreleme düzeyi, kullanılan araca bağlıdır; ancak bu filtreleme, uzmanların şüpheliler arasında iletişim kurmak için gönderilen ve alınan SMS mesajları ve çağrı kayıtları gibi önemli veri türlerini hızlı bir şekilde incelemesine olanak tanır.

4.1.3.4. Analiz aşaması

Analiz aşamasında incelemeyi yapan kişi aslında kopyalar üzerinde elektronik kanıt arar. Bu adım çok zaman alıcı olabilir ve çeşitli dosya sistemlerinden, işletim sistemlerinden ve uygulamalardan gelen izleri yorumlamak için çok fazla uzman bilgisi gerektirebilir. Analiz aşaması için gereken süre ve iş yükü üzerinde birçok farklı faktörün etkisi vardır. Bu faktörler şunları içerir; analiz edilecek depolama ortamının miktarı, depolama ortamının boyutu, kullanılan dosya sistemlerinin karmaşıklığı, işletim sisteminin kullanım düzeyi, kullanıcının karmaşıklığı. Analiz aşamasının akış şeması Ek-5'te gösterilmiştir. Örnek bir analiz kontrol formu Ek-9'da gösterilmiştir.

- **Bilgisayarların Analizi:** Bir bilgisayar sistemini analiz eden uzman, tipik olarak yalnızca vakayla ilgili izleri bulmakla kalmaz, aynı zamanda potansiyel olarak bir failin niyetine ilişkin kanıtlar da bulabilir (örneğin, suçun nasıl işleneceğine ilişkin internet aramaları). Bir incelemecinin adli analiz sırasında keşfedebileceği dijital iz türleri hakkında daha iyi bir fikir edinmek için iki tür dijital iz arasında ayrım yapmak mantıklıdır. Bunlardan ilki kaçınılabilir izlerdir. Bunlar, işletim sistemi ve uygulamalar tarafından varsayılan olarak depolanan ancak sistemin depolamayacak şekilde yapılandırılabileceği izlerdir. Örnek olarak bir web

tarayıcısını ele alalım. Bu yazılım, şüphelinin göz atma geçmişinin yanı sıra indirme işlemlerinin, form girişlerinin, çerezlerin vb. ayrıntılarını saklar, ancak şüpheli tarafından devre dışı bırakılabilir veya silinebilir. İkinci dijital iz türü ise kaçınılmaz izlerdir. Kaçınılmaz izler devre dışı bırakılamayan veya geçici olarak durdurulması büyük çaba gerektiren izlerdir. Şüpheli kendi izlerini gizlemeye çalışsa bile bu tür izleri bulma olasılığı da aynı oranda yüksektir (Ayrılmamış alanlar, RAM, bazı uygulama izleri vb.). Her vaka tipik olarak özellikle ilgili bazı izleri içerir. Örneğin bir dolandırıcılık vakasında belgeler, elektronik tablolar ve e-postalar genellikle daha alakalıyken, çocuk istismarı vakalarında resimler, videolar ve iletişim izleri daha alakalıdır. Ancak bu vaka kategorileri içinde bile her vaka aynı değildir. Bazı vakalarda çok sayıda bilgisayar sistemi ve depolama ortamı yer alırken, adli bilişim laboratuvarlarının iş yükü zaten çok yüksektir. Adli analiz ile içerik analizi arasındaki ayrım, işi adli bilişim uzmanları ve vaka araştırmacıları arasında daha eşit bir şekilde dağıtabilir. İçerik analizi vaka bilgisine sahip araştırmacılar tarafından yapılırken, Adli bilişim uzmanı delillerin kurtarılmasına, ayrıştırılmasına, birleştirilmesine ve işlenmesine odaklanabilir. Karmaşık veri yapılarının görselleştirilmesine yardımcı olmak için görselleştirme yardımcıları faydalı olabilir. Bu yardımlara zaman çizelgeleri (şüphelinin giriş çıkış yaptığı saatler, ağa bağlanma zaman vb.), ilişki diyagramları (kim kiminle ne zaman nerede tanıştı, görüştü vb.), para akışı diyagramları örnek gösterilebilir. Grafiksel gösterimler veriler arasındaki korelasyonun anlaşılmasını kolaylaştırır. Ayrıca araştırmacının yeni bağlantılar bulmasını da sağlayabilirler.

- **Mobil Cihazların Analizi:** Mobil cihazlar, söz konusu iletişimlerin saatleri ve tarihlerinin yanı sıra iletişim kayıtlarını ve günlüklerini içerir. Buna ek olarak mobil cihazlarda bir soruşturmada kullanılabilecek medya dosyaları ve konum verileri de bulunacaktır. Mobil cihazlarda bulunan dijital izler üç ayrı gruba ayrılabilir: iletişim verileri, medya dosyaları ve diğer veriler. İletişim verileri, arama kayıtlarını, SMS mesajlarını ve diğer mesajlaşma hizmeti mesajlarını içerebilir. Medya dosyaları, bilgisayarlarda olduğu gibi, dosya tarafından gösterilenin ötesinde bilgiler içerebilir. Örneğin bir cep telefonuyla yakalanan medya dosyalarındaki meta veriler büyük olasılıkla dosyanın içine gömülü coğrafi etiketler veya diğer yararlı konum verilerini içerecektir.

4.1.3.5. Sunum (Raporlama) aşaması

Analiz aşamasında deliller bulunduktan sonra incelemeyi yapan kişinin yargılama için bir rapor hazırlaması gerekir. Uzmanın görevi karmaşık teknik bağlamları göstermek ve hakimlerin, savcıların

ve ilgili diğer tarafların kolayca anlayabileceği gerçeklere dönüştürmektir. Ayrıca bu gerçekleri yorumlamaları ve bunların anlamları hakkında görüş bildirmeleri de beklenebilir.

Adli bilişim raporu, daha önce gerçekleştirilen adımların tüm prosedürlerini ve sonuçlarını yansıtır. Bu, önceki tüm çalışmaların tek sonucudur ve bu nedenle ceza hukuku sistemindeki diğer tüm kişiler için temel unsurdur. Raporlama aşamasının akış şeması Ek-6'da gösterilmiştir.

Raporun mahkemelerde bir kişinin suçluluğunu veya masumiyetini kanıtlamaya yardımcı olmak için kullanılması, onu son derece önemli bir belge haline getirmekle kalmıyor, aynı zamanda adli bilişim uzmanı için bazı zorluklara da neden olmaktadır. En büyük zorluklardan biri raporu teknik bilgisi olmayan kişiler için anlaşılır kılmaktır. Bu nedenle adli bilişim raporunun açık, anlaşılır bir dille yazılması ve inceleme sırasında bulunanların özetini kısa bir formatta içermesi gerekir. Bir adli bilişim raporu aşağıdaki ana bölümlerden oluşmalıdır:

1. Talep ve yetkiye ilişkin bilgiler
2. Delillere ilişkin bilgiler
3. İnceleme yöntemlerine ilişkin bilgiler (kişi/yazılım/donanım)
4. Edinme süreci
5. Analiz süreci
6. Sonuç

Bir raporun örnek düzeni Ek 10'da gösterilmiştir.

Adli bilişim laboratuvarında rapordan kimin sorumlu olduğu ve delilleri mahkemede kimin sunacağı açıkça tanımlanmalıdır. Tipik olarak bu kişi, raporda adı geçen ve raporu imzalayan kişiyle aynıdır.

Bilim ve teknolojinin karmaşık konularını içeren deliller davalarda giderek artan bir rol oynamaktadır. Bu nedenle bazı ülkeler ve mahkemeler atanmış bilirkişilerin listelerini tutmaktadır. Bir bilirkişinin atanması genellikle mahkemenin bu tür konularla ilgilenme yeteneğini geliştirmesinin bir yolu olarak önerilmektedir. Bir bilirkişinin hakları ve görevleri genellikle ülkeden ülkeye farklılık gösterir. Adli bilişim uzmanlarının kendi mevzuatlarını, mahkeme prosedürlerini, rollerini ve bu roldeki hak ve görevlerini öğrenmeleri önemlidir.

Bazı mahkemeler alternatif sunum yöntemlerinin kullanılmasına izin vermektedir. Bunlar, projektörlü bilgisayarlarda, sanal makinelerde vb. canlı gösteriler gibi açıklayıcı medyayı içerebilir. İsteniyorsa,

kabul ediliyorsa ve gerekliyse, bu olasılıkların duruşma öncesinde hâkimle tartışılması hayati önem taşımaktadır.

4.1.4. Ekler

Rehber içinde atıfta bulunulan ekler aşağıdaki gibidir;

- Ek 1 - Adli yazılım karşılaştırma matrisi
- Ek 2 - Örnek cihaz taşıma çantası içeriği
- Ek 3 – Toplama (Edinim) Süreci Akış Şeması
- Ek 4 – İnceleme (İşleme) Akış Şeması
- Ek 5 – Analiz Akış Şeması
- Ek 6 – Sunum(Raporlama) Akış Şeması
- Ek 7 – Gözetim zinciri kaydı
- Ek 8 – Adli Kopya Alma Çalışma Sayfası
- Ek 9 – Adli Bilişim Analiz Formu /Tablosu
- Ek 10 – Adli Bilişim Rapor Şablonu

4.2. Interpol Modeli

Tam adı Uluslararası Kriminal Polis Teşkilatı olan ve hâlihazırda 196 üye ülkesi bulunan Interpol, 1923 yılında kurulmuş olan hükümetler arası bir kuruluştur.

Üye ülkeler için suç ve suçlulara ilişkin verileri paylaşmalarına ve verilere erişmelerine olanak tanımakta, bir dizi teknik ve operasyonel destek sunmaktadır. Tüm ülkeleri I-24/7 adı verilen iletişim sistemiyle birbirine bağlamaktadır. Ülkeler bu güvenli ağı birbirleriyle ve Genel Sekreterlik ile iletişim kurmak için kullanırlar. Ayrıca veri tabanları ve hizmetlere hem merkezi hem de uzak konumlardan gerçek zamanlı olarak erişim sağlamaktadırlar. Interpol Genel Sekreterliği, çeşitli suçlarla mücadele etmek için günlük faaliyetleri koordine eder. Genel Sekreter tarafından yönetilen birimin personeli hem polis hem de sivillerden teşkil edilmiş olup ve Lyon'da bir genel merkez, Singapur'da küresel bir inovasyon kompleksi ve farklı bölgelerde çok sayıda uydu ofisten oluşmaktadır. Her ülkede bir INTERPOL Ulusal Merkez Bürosu (National Central Bureau-NCB), Genel Sekreterlik ve diğer NCB'ler için merkezi iletişim noktası sağlar. Bir NCB, ulusal polis yetkilileri tarafından yönetilir ve genellikle polisin bağlı olduğu bakanlıkta yer alır. Şu anda dünya üzerinde en acil olduğu düşünülen terörizm, siber suçlar, organize suçlar, mali suçlar ve yolsuzlukla mücadele konularında çalışmalarını yoğunlaştırmaktadırlar (Interpol, 2024).

Merkezi Singapurda bulunan Interpol Inovasyon Merkezi bilgi alışverişinde bulunmak ve yeni teknolojileri ve ortaya çıkan siber tehditleri keşfetmek için kolluk kuvvetleri, akademik personel ve özel sektör ortaklarını bir araya getirerek çeşitli çalışmalar yapmaktadır.

İnovasyon Merkezinin çalışmaları dört tematik laboratuvara ayrılmıştır (Interpol, 2024):

1. **INTERPOL Sorumlu Yapay Zeka Laboratuvarı** - Yapay zeka kullanımına odaklanarak yapay zeka (AI) farkındalığını, bilgisini ve uzman alışverişini kolaylaştırır;
2. **Siber Uzay ve Yeni Teknolojiler Laboratuvarı -** Siber uzayda ortaya çıkan tehditleri engellemenin, tahmin etmenin ve araştırmanın temel yollarını değerlendirir;
3. **Adli Bilişim Laboratuvarı -** Ele geçirilen mobil cihazlar, insansız hava sistemleri ve bilişim ekipmanları dahil olmak üzere adli bilişim araştırmalarında operasyonel yardım sağlar;
4. **Gelecek ve Öngörü Laboratuvarı -** Teknoloji, strateji ve politikadaki küresel gelişmeleri tanımlar ve analiz eder.

Çalışmamızın ikinci modeli olarak Interpol Inovasyon Merkezinin adli bilişim laboratuvarlarında çalışan kolluk personeli ve laboratuvar personeli için Mayıs 2019 yılında yayımladığı "Adli Bilişim Laboratuvarları İçin Küresel Kılavuz" rehberi incelenecektir.

Rehbere bakıldığında Avrupa Konseyinin yayımladığı rehberle benzerlikler gösterdiği görülmektedir. Açıklama ve teşekkür kısmında da Avrupa Konseyinin hazırladığı rehberden ilham alınarak hazırlandığı belirtilmektedir. Bu nedenle çalışmamızda rehberin tümü incelenmeyecek olup fikir vermesi açısından sadece farklılıkları ortaya konacaktır. Rehber aşağıda belirtilen 7 bölümden oluşturulmuştur;

- Giriş
- Adli Bilişime Giriş
- Adli Bilişim Laboratuvarının Yönetimi
- Adli Bilişim Vakasının Yönetimi
- Laboratuvar Analiz Prosedürü
- Kalite Güvencesi
- Özet ve Ekler

4.2.1. Giriş

Bu rehber, bir adli bilişim laboratuvarı kurma ve yönetme prosedürlerini özetlemekte ve elektronik kanıtların yönetimi ve işlenmesi için teknik yönergeler sağlamaktadır. Bu rehber, ülkelerin adli bilişim yeteneklerini geliştirmeyi düşünürken kullanılabilecek bir şablon belge olarak görülmelidir. Verilen tavsiyelerin ulusal mevzuat, uygulama ve prosedürlere uygun olarak hem stratejik hem de taktik düzeylerde kullanılması amaçlanmaktadır. Belgenin INTERPOL üyesi ülkeler tarafından kullanılması amaçlanmıştır. Bu rehberin amacı, adli bilişim laboratuvarları tarafından üretilen elektronik delillerin, üye ülkelerin mahkemelerinde ve uluslararası ceza hukuku sistemlerinde kabul edilebilir olmasını sağlamaktır.

Rehber temel olarak iki farklı gruba odaklanmaktadır: Birincisi, laboratuvar adına karar veren adli bilişim stratejistleri ve yöneticileridir; ikinci grup ise günlük olarak elektronik delillerle ilgilenen teknik personeli içermektedir. Ayrıca savcılar, hakimler ve avukatlar da davaları açısından hayati önem taşıyabilecek adli bilişim sürecini anlama konusunda bu belgeden yararlanacaktır.

Rehberin amacı, kendi ulusal yasal çerçevelerinin gerekliliklerini takip etmek zorunda olan adli bilişim laboratuvarlarına sınırlamalar getirmek değildir. Bu rehberde verilen tavsiyelerin herhangi bir üye ülkedeki herhangi bir ulusal mevzuatla çelişmesi amaçlanmamaktadır.

4.2.2. Adli bilişime giriş

Rehberin bu bölümünde Avrupa Konseyi modelindeki gibi adli bilişimin tanımı yapılmakta ve dijital delillerin özelliklerinden bahsedilmektedir. Dijital delillerin incelenmesindeki prensipler yer almakta ve dikkat edilecek hususlar vurgulanmaktadır.

4.2.3. Adli bilişim laboratuvarının yönetimi

Rehberin bu bölümünde yine Avrupa Konseyi bölümünde olduğu gibi laboratuvar planı yaparken dikkat edilecek hususlar (son yıllardaki suç istatistikleri, büyüklük vb.), bina, fiziksel güvenlik, tesisler ve ziyaretçiler için alınacak tedbirlere yer verilmiştir. Görevli personel, laboratuvarın fiziki gereksinimleri konuları da bu başlık altında incelenmiştir.

Avrupa Konseyi modelinden farklı olarak fiziksel güvenlik başlığı altında laboratuvarda olması gereken fiziksel güvenlik tedbirleri için bir kontrol listesi (checklist) hazırlanmıştır. Hazırlanan "Fiziksel Güvenlik İçin Kontrol Listesi" Çizelge 4.1'de sunulmuştur.

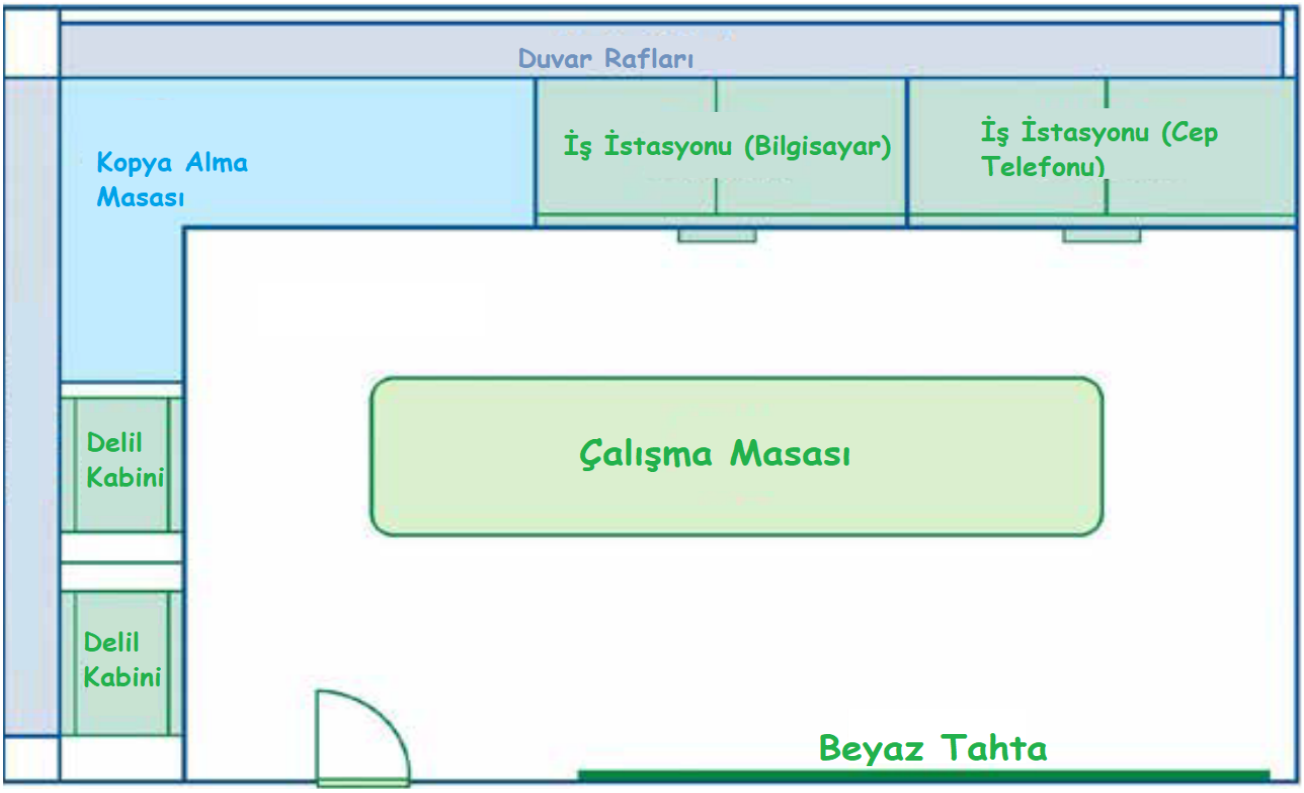
Çizelge 4.1. Fiziki güvenlik için kontrol listesi

Fiziksel Güvenlik İçin Kontrol Listesi		
1	**Kamera sistemi** Gözetim sistemi, izinsiz erişim ve izinsiz girişlere karşı tesisleri izlemek için kullanılır. Kurulumu yapan kişiler, maksimum güvenliği sağlamak için en iyi stratejik yerin yanı sıra en iyi çözünürlüğü de dikkate almalıdır.	Evet/Hayır
2	**Erişim kontrolü** Erişim kontrolü, bütçeye bağlı olarak fiziksel kilitler ve anahtarlar, elektronik tuş takımları, kaydırmalı kartlar ve/veya biyometrik veri şeklinde olabilir.	Evet/Hayır
3	**Yangın kontrol sistemi** Bir laboratuvarın binada kurulu bir yangın algılama sistemi ve yangın söndürme sistemi bulunmalıdır. Yangın söndürme sistemi için kullanılan malzeme delillere, ekipmanlara veya personele zarar vermemelidir.	Evet/Hayır
4	**Pencere, kapı ve duvar koruması** Gerektiğinde, hırsızlıkları önlemek için pencereler parmaklık ve kilitlerle güçlendirilmelidir. Laboratuvarın cam pencereleri ve duvarları varsa, hassas verilerin görüntülenmemesine dikkat edilmelidir. Binayı yangından korumak için merdiven boşluğu veya koridor gibi yerlerde yanmaz kapı kullanılması düşünülebilir	Evet/Hayır
5	**Yeterli elektrik prizi, sigorta, kesici ve akım yükü** Sorunsuz çalışmayı sağlamak ve yangın tehlikelerine yol açan ve personelin güvenliği açısından risk oluşturan aşırı güç yüklemelerini önlemek için laboratuvara yeterli miktarda elektrik prizi, sigorta ve akım kesici takılmalıdır.	Evet/Hayır
6	**Antistatik döşeme** Antistatik zemin kaplama, çalışanlara, ekipmanlara ve kanıtlara zarar verebilecek olası elektrostatik deşarjın azaltılmasına yardımcı olur.	Evet/Hayır
7	**Radyo frekans karıştırma sistemi** Laboratuvarın, örneğin Faraday kafesi veya sinyal bozucu cihaz kullanarak ağ sinyallerini engelleyecek bir sistem kurması önerilir.	Evet/Hayır

	Radyo karıştırma sistemi tüm ağ sinyallerini engelleyecek ve delillere herhangi bir izinsiz girişi önleyecektir. Mevcut kablosuz teknolojiyle, açık akıllı telefonların veya dizüstü bilgisayarların otomatik olarak mevcut kablosuz ağlara bağlanmayı denemesi ve dolayısıyla verilerini değiştirmesi olasılığı mevcuttur. Bu tür sistemlerin kullanımına izin verildiğini ve diğer sistemlere müdahale etmediğini doğrulamak için ulusal mevzuat kontrol edilmelidir.	
8	**Soğutma sistemi** Bir laboratuvarın işi yürütecek gelişmiş bilgisayarlara sahip olması ve laboratuvarda önemli miktarda ısı üretmesi yaygındır. Aşırı ısınma veri kaybına ve donanımın zarar görmesine neden olabilir. Laboratuvar, kanıt depolama odası ve sunucu odası da dâhil olmak üzere oda sıcaklığını kontrol etmek için bir soğutma sistemi kurmalıdır.	Evet/Hayır
9	**Tesis Dışı Veri Depolama Yedeklemesi** Büyük miktarda veri, tamamen işlevsel hale geldiğinde laboratuvar tarafından depolanır ve doğası gereği hassas olabilir. Veriler genellikle bir sunucuda saklanır. Verilerin laboratuvardan uzakta, tesis dışındaki bir sunucuya yedeklenmesi en iyi uygulamadır. Laboratuvarın etkilendiği bir felaket durumunda, önemli verilere erişim sağlamak için tesis dışı depolama kullanılabilir. Tesis dışında bir veri depolama yedeğine sahip olmak, operasyonların minimum sürede çalışır duruma gelmesini sağlayan olağanüstü durum kurtarma planının bir parçasıdır.	Evet/Hayır
10	**Arşiv-Veri Depolama / Uzun Süreli Veri Depolama** Veriler, analizden sonra daha sonraki bir tarihte, daha sonraki adli işlemlerde veya davaya ilişkin yeni delil veya bulguların ışığında alınabilecek şekilde saklanmalıdır. Depolama süresi ulusal yasa gerekliliklere uyarlanmalıdır.	Evet/Hayır

Kaynak:Interpol(https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics)

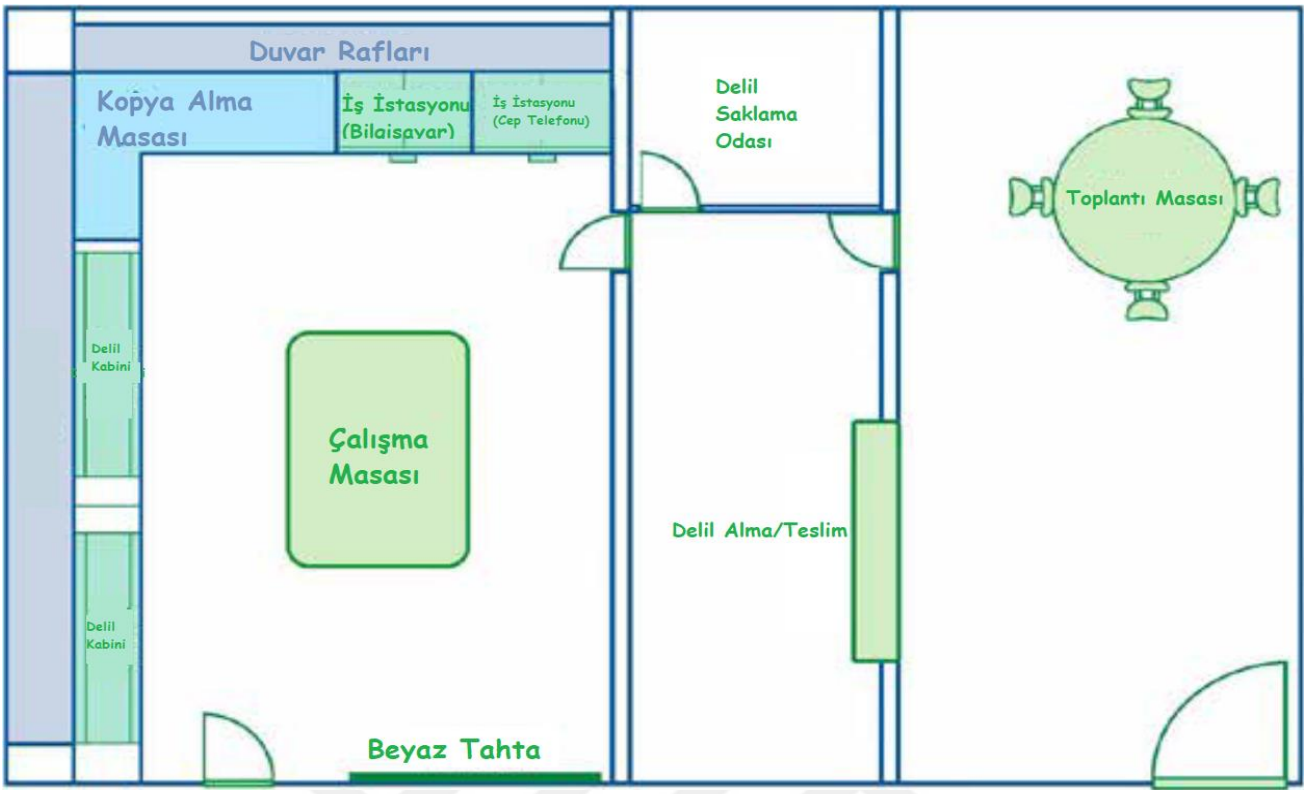
Ayrıca rehberde tesisler başlığı altında örnek bir laboratuvar yerleşim planı taslağı verilmiştir. Temel yerleşim planı ve gelişmiş yerleşim planı olarak iki çeşit yerleşim planı oluşturulmuş olup Şekil 4.2'de temel yerleşim planı gösterilmiştir.



Şekil 4.2. Adli bilişim laboratuvarı temel yerleşim planı

Kaynak:Interpol(https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics)

Eğer laboratuvar kuracak kurum orta büyüklükte bir laboratuvar geliştirmeye karar verirse kat planı için Şekil 4.3'de plan uygulanabilir.



Şekil 4.3. Adli bilişim laboratuvarı gelişmiş yerleşim planı

Kaynak:Interpol(https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics)

Interpol'ün hazırladığı rehberde bina başlığı altında laboratuvara gelen ziyaretçiler içinde ayrıca bir kontrol listesi hazırlanmış olup Çizelge 4.2 de sunulmuştur.

Çizelge 4.2. Ziyaretçi kontrol listesi

Ziyaretçi Kontrol Listesi		
1	**Kayıt** Ziyaretçilerin laboratuvara girmeden önce bir form kullanarak veya çevrimiçi bir sistem aracılığıyla kayıt yaptırmaları gerekmektedir. Büyük bir ziyaretçi grubu için, eşlik eden laboratuvar personeli, grubun büyüklüğünü ve ziyaretin amacını dikkate alarak uygun kayıt süreçlerini düzenlemelidir.	Evet/Hayır
2	**Kimlik Kartı** Özellikle uzun süreli ziyaretlerde ziyaretçiye geçici kimlik kartı verilebilir. Kimlik kartı, ziyaretçiyi laboratuvar personelinden açıkça ayırt etmelidir.	Evet/Hayır
3	**Mihmandar** Laboratuvarda iken ziyaretçilere her zaman laboratuvar personeli eşlik etmelidir.	Evet/Hayır
4	**Ziyaretçi Politikası** Ziyaretçilerin okuyabilmesi için laboratuvar ortak alanında ziyaretçi politikasına ilişkin açık işaretler veya bir poster sergilenmelidir. Fotoğraf çekme, yeme-içme, laboratuvar ekipmanlarına ve elektronik delillere dokunma vb. kurallar ziyaretçilere açıkça belirtilmelidir.	Evet/Hayır
5	**Yasadışı Malzemelerin Görüntülenmesi** Açık işaretler, potansiyel olarak yasa dışı ve uygunsuz görsellerin laboratuvar içerisinde analiz edildiğini ve görüntülendiğini belirtmelidir.	Evet/Hayır

Kaynak:Interpol (https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics)

Interpol'ün rehberinde görevli personel, eğitim, danışmanlık gibi personel konuları Avrupa Konseyinin rehberinden farklılık göstermemektedir. Bu nedenle bu bölümde incelenmemiştir.

Ekipman başlığı altında ise standart bir adli bilişim laboratuvarında bulunması gereken yazılım ve donanımlara dair bir kontrol listesi yayımlanmış olup Çizelge 4.3'te gösterilmiştir. Okuyucuya,

listenin kapsamlı olmadığını ve alınan vakaların niteliğine bağlı olarak daha fazla ekipmanın gerekli olabileceğini dikkate alması tavsiyesi verilmiştir.

Çizelge 4.3. Standart adli bilişim laboratuvarı ekipman kontrol listesi

No	Ekipman	Durum
1	Dizüstü Bilgisayar	Var/Yok
2	Bilgisayar İnceleme Yazılımı	Var/Yok
3	Veri Kurtarma Yazılımı	Var/Yok
4	Mobil Cihaz İnceleme Yazılımı	Var/Yok
5	İnternet İnceleme Yazılımı	Var/Yok
6	Sanal Makine Yazılımı	Var/Yok
7	Bağlantı (Docking) Sistemi	Var/Yok
8	Yazma Engelleme Sistemi	Var/Yok
9	Kopya Alma Donanımı	Var/Yok
10	Boş depolama ortamı – kısa ve uzun vadede elektronik kanıtlardan elde edilen verileri depolamak için: USB bellek, harici sabit disk, sabit disk, sunucu	Var/Yok
11	Bilgisayar araç seti (Toolkit)	Var/Yok
12	Güç Kabloları, uzantılar	Var/Yok
13	Yazıcı	Var/Yok
14	Evrak İmha Cihazı	Var/Yok

Kaynak:Interpol (https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics)

4.2.4. Adli bilişim vakasının yönetimi

Avrupa Konseyi rehberinde adli bilişim laboratuvar süreçleri ve prosedürleri başlığı altında incelenen konular Interpol rehberinde de incelenmiştir. Fakat Interpol rehberinde Avrupa Konseyinin rehberinden farklı olarak laboratuvara ilk gelen delile adım adım hangi prosedürlerin uygulanacağı da ayrıntılı bir şekilde açıklanmıştır.

Avrupa Konseyi rehberinde esas olarak adli bilişim aşamaları alınırken (Toplama, inceleme, analiz, raporlama) alınırken Interpol'ün hazırladığı rehberde delilin laboratuvara ilk girişi esas alınmış ve

talimatlar ona göre hazırlanmıştır. Bu bölümde Avrupa Konseyi rehberinden farklı olarak hazırlanan delilin laboratuvara giriş anından dosyanın kapanmasına kadar yapılan işlemler incelenecektir.

Adli bilişim laboratuvarı, vakaları almaya başlamadan önce bir vaka yönetimi prosedürü oluşturmalıdır. Aşağıdaki şekilde gösterildiği ve sonraki bölümlerde ayrıntılı olarak açıklandığı gibi, genellikle bir vakayı yönetmede yedi adım vardır. Bir davayı yürütmeden önce laboratuvar, ilgili mevzuata uyduğundan ve takip ettiğinden emin olmalıdır. Yönetici veya inceleme uzmanı, delillerin işlenmesine yönelik yasal iznin, izinler veya resmi belgeler yoluyla mevcut olduğundan emin olmalıdır. Delilin kabulünden dosyanın kapanmasına kadar olan 7 aşama Şekil 4.4'te gösterilmiştir.

Şekil 4.4. Vaka yönetim prosedürü

Kaynak:Interpol(https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics)

4.2.4.1. Talebin alınması

Adli bilişim laboratuvar çalışması, talep sahibinden resmi bir talep alınmasıyla başlar. Bu resmi talep mektup, e-posta veya faks şeklinde olabilir. Resmi talepte sunulan bilgiler, söz konusu suçun tanımını, ilgili eylemi, elektronik delil ayrıntılarını, davanın amacını ve muhtemelen tutuklama emrini (mahkeme kararı) içermelidir.

Laboratuvar yöneticisi veya atanmış personel daha sonra talebi inceleyecek ve aşağıdaki kriterlere göre vakanın uygun olup olmadığına karar verecektir:

- Dosya adli bilişim kapsamındadır, yani deliller elektroniktir ve DNA veya parmak izleri gibi başka türlü değildir,
- Mevcut yöntemler ve araçlar,
- Dosyayı yürütecek personel mevcut,
- Yasal zorunluluk yerine getirildi (mahkeme, savcılık kararı vb.)

Laboratuvar daha sonra davayı kabul edip edemeyeceğine ilişkin talebe resmi olarak yanıt verecektir. Kararın kabul edilmesi halinde laboratuvar, elektronik delillerin talep sahibinden teslimi için bir tarih sağlayacaktır.

4.2.4.2. Dosya kaydı

Laboratuvar davanın mümkün olduğuna karar verdiğinde, talep sahibi elektronik delillerle birlikte laboratuvara gelecektir (ya da posta veya kurye vasıtasıyla gönderecektir). Laboratuvar, bu vaka için benzersiz bir devam eden vaka numarası oluşturur ve bir vaka kayıt formunu doldurur.

Elektronik kanıtların etkili bir şekilde incelenebilmesi için, incelemeyi yapan kişilere, talepte bulunan tarafından açık ve spesifik bir vaka talebinin sağlanması gerekmektedir. Bir cihazda bulunan belgeler, videolar, konumlar vb. gibi büyük miktarda ve çeşitli türde veriler nedeniyle, bir incelemecini açık ve spesifik bir talep olmadan verileri incelemesi mümkün değildir.

Bu bilgiye dayanarak, incelemeyi yapan kişi delilleri işlemek için kullanılacak yöntem ve araçları planlayabilir. Her iki taraf da, yani talep sahibi ve laboratuvar personeli, formu imzalamalıdır. Artık çalışmalar resmi olarak başlamıştır. Laboratuvar daha sonra vakayla ilgili tüm verileri depolamak için depolama ortamında bir klasör oluşturacaktır.

4.2.4.3. Delilin kaydı

Elektronik deliller alındığında, muhafazanın laboratuvara devredilmesinden önce delilin mühürlenmesi önemlidir. Delilin bütünlüğüne ilişkin her türlü makul şüpheyi ortadan kaldırmak için, hem talepte bulunan hem de incelemeyi yapan kişi, bir taraftan diğerine aktarım süreci sırasında delillere başka hiç kimsenin erişim sağlamadığını gösterebilmelidir.

Sunulan her elektronik kanıt parçası kaydedilmeli ve kayıt formunda delil ayrıntılarıyla birlikte belgelenen benzersiz bir delil etiketi atanmalıdır. Delil kayıt formunun bir örneği Ek 11'de Delil Kayıt Formu Örneği'nde gösterilmiştir.

Bu kayıt, her delilin sim kartları ve hafıza kartları gibi alt öğelerini de içerir. Etiketlerin alt öğeleri ana öğeye kadar izleyebilmesi gerekir. Örneğin, bir cep telefonu 20190105(2)-MP01 olarak etiketlenmişse sim kart 20190105(2)-MP01-SIM01 olarak etiketlenebilir.

Delildeki herhangi bir kusurun, delil kayıt formunda belgelenmesi gerektiğine dikkat etmek önemlidir. Bunun amacı laboratuvarı gelecekte olumsuz iddialardan korumaktır. Delille ilgili her türlü elektronik kopya belge vaka klasörüne yüklenmelidir.

Artık delillerin saklama zinciri başlamış olup, formun delili alan personel tarafından doldurulması gerekmektedir. Delil kullanımda değilken bir delil depolama odasında saklanmalıdır.

4.2.4.4. Delilin fotoğraflanması

Delilin fotoğrafı delilin durumunu kaydetmek ve delili gelecekte etkili bir şekilde tanımlamak için çekilmektedir. Delilin genel görünümünün yanı sıra yakın plan görünümünü de fotoğraflamak yararlı bir uygulamadır. Ekran aktifse ekran görüntüsünün de fotoğrafı çekilmelidir. Daha sonra resimler vaka klasörüne yüklenmelidir. Gelecekteki durumuna ilişkin referans olması amacıyla talep sahibine iade etmeden önce delilin fotoğrafının çekilmesi tavsiye edilir.

4.2.4.5. Analizin yapılması

Analizin laboratuvar analiz modeline uygun olarak yapılması gerekmektedir. Süreç boyunca, adli bilişim uzmanları, talep sahibi ile iletişimi sürdürmeli ve inceleme sırasında ortaya çıkabilecek her türlü sapma veya sınırlamayı bildirmelidir. Bazı uzmanların adli bilişim alanında uzun yıllara dayanan bilgi birikimi vardır ve bu nedenle uzman ile talep sahibi arasında etkili bir iletişim olduğunda doğru verileri tahsis edebilirler.

4.2.4.6. Delilin iadesi

Analiz tamamlandıktan sonra laboratuvar, kanıtları almak için talep sahibi ile iletişime geçer. Laboratuvardaki yaygın uygulama, seyahat süresinden tasarruf etmek için delilin adli bilişim raporuyla birlikte talep sahibine iade edilmesidir. Delili iade etmeden önce laboratuvarın delili mühürlemesi gerekmektedir. Mühürde laboratuvarın logosu, ismi, delilin etiketi ve mühürlendiği tarih ve saat bulunması tavsiye edilir. Örnek bir Delil Mühürleme şekli ve formu Ek 12'de gösterilmiştir.

4.2.4.7. Dosyanın kapanması

İşlem daha sonra tamamlanır ve laboratuvar dosyayı kapatabilir. Dosyayı kapatmak için her iki tarafın da işin tamamlandığı ve raporun talep sahibine teslim edildiği konusunda mutabakata varması gerekir. Bu bir form imzalanarak yapılabilir.

Dosyanın tamamlanmasının ardından ileriye giden yol, gerekirse davanın adli sonuçları hakkında bilirkişi ifadesi vermek üzere inceleme uzmanının mahkemeye çıkmasını içerir. Talep sahibi, mahkemede kendisine ihtiyaç duyulduğunda inceleme uzmanını bilgilendirir.

4.2.5. Laboratuvar analiz prosedürü

Interpol'ün yayımladığı rehber laboratuvar analiz prosedürü başlığı altında tıpkı Avrupa konseyinin rehberinde olduğu gibi adli bilişimin aşamaları ve hangi aşamada hangi delile ne tür inceleme

prosedürleri uygulanacağı yer almaktadır. Bu bölüm Avrupa Konseyinin hazırladığı rehberden bir farklılık göstermemektedir. Bu nedenle burada tekrar incelenmeyecektir. Rehberde bu başlık altında raporlama(sunum) konusu da işlenmiş olup bu konuda da Avrupa Konseyinin rehberinden farklı bir uygulama gözükmemektedir.

4.2.6. Kalite güvencesi

Avrupa Konseyi yayımladığı rehberde kalite güvencesi ve gereksinimlerine "Fiziksel Laboratuvar Gereksinimleri" başlığı altında yer verirken Interpol bu konuya daha ayrıntılı bir şekilde yaklaşarak ana bir başlık haline getirmiştir. Bu nedenle bu bölümde Interpol'ün rehberi incelenecektir.

Adli bilişim raporu mahkemede sunarken, inceleme yapanların yalnızca analiz sürecini açıklaması gerekmeyebilir. Ayrıca yeterliliklerini, kullandıkları ekipmanı, seçtikleri yöntemi, delil işleme yöntemini ve çok daha fazlasını açıklamaları istenebilmektedir. Bahsedilen konuları ele alacak prosedürlerin adli bilişim laboratuvarında oluşturulması ve uygulanması önemlidir. Rehberde bu konu kalite güvence bileşenleri ve adli bilişim laboratuvarı akreditasyonu olacak şekilde iki başlık altında yer almaktadır.

4.2.6.1. Kalite güvence bileşenleri

Interpol rehberinde çok detaylı bir kalite güvence kontrol listesi yayımlamıştır. Temel seviyede yayınlanan fakat sadece içindekilerle sınırlı olmayan kalite güvence kontrol listesi Çizelge 4.4'te sunulmuştur.

Çizelge 4.4. Kalite güvence bileşenleri kontrol listesi

Kalite Güvence Bileşenleri Kontrol Listesi	
Laboratuvar	A. Laboratuvar düzeyinde bir Organizasyon Şeması oluşturun. B. Her yıl iç denetim yapın. C. İç ve dış şikayetleri ele almak için bir prosedür oluşturun. D. Belgeleri kontrol etmek için bir prosedür oluşturun.
Tesis ve Çevre Durumu	A. Laboratuvar binalarını oluşturun – erişim ve çıkışlar. B. Bir erişim listesi oluşturun ve anahtarları, ayrı ayrı atanmış kimlik kartlarını veya biyometrik cihazları kullanarak erişimi sınırlayın. C. Laboratuvar ortamını düzenli olarak izleyin (sıcaklık, nem, temizlik). D. Bir Sağlık ve Güvenlik programı oluşturun.

	e. Ziyaretçi politikasını oluşturun. F. Düzenli temizlik yapın.
Ekipman	A. Ekipmanın taşınması, transferi, depolanması, kullanımı, onarımı, imhası ve planlı bakımı için bir prosedür oluşturun. B. Kullanıma almadan önce ekipmanın özelliklerine uygun çalıştığından emin olun. C. Bakım programını uygulayın. D. Donanım yazılımlarını gereksinimlere göre güncelleyin. e. Ekipman belgelerini, kılavuzlarını ve garantilerini koruyun.
Personel	A. İstihdam Nitelikleri: • İşe almadan önce özgeçmiş taraması yapın. • İşe alındıktan sonra personel için iş tanımlarını hazırlayın B. Mesleki Gelişim ve Eğitim: • Personel için bir eğitim programı oluşturun • Personeli eğitime gönderin. • Yeni işe alınan personel için danışmanlar atayın. • Yeni işe alınan personel için yetkinlik testleri yapılarak personelin yetkinliğini değerlendirin. • Yıllık yeterlilik testleri yaparak mevcut personelin yeterliliğini değerlendirin. • Harici veya laboratuvarlar arası yeterlilik testlerine katılın. • Teknik sertifikalar alın. Mevcut personelin becerilerini sürdürmesi için sürekli eğitim programı oluşturun.
Deney Metodu	A. Laboratuvar incelemelerini yürütmek için Standart Operasyon Prosedürleri oluşturun. B. Adli bilişim yöntemlerine ilişkin bir belgeyi güncellenmiş ve uzmanların kullanımına açık tutun. C. Laboratuvarın bunları doğru şekilde kullanabilmesini sağlamak için tanıtılan yöntemler üzerinde doğrulama yapın. D. Herhangi bir yöntemi kullanırken doğrulama gerçekleştirin: standart dışı yöntem, laboratuvarda geliştirilen yöntem veya kapsamı dışında kullanılan standart yöntem.

	e. Kullanım kolaylığı için laboratuvarda SWGDE gibi uluslararası kabul görmüş bir yöntem kullanın.
İnceleme Talebi	Hizmet talebine ilişkin bir politika ve prosedür oluşturun ve uygulayın. Bu şunları içermelidir: A. İsteği kabul etme veya reddetme süreci. B. Talebin yeniden gönderilmesi süreci. C. Kısa bir talep veya vaka amacına sahip olma gerekliliği. D. Bir formu imzalayarak, bir e-postayı yanıtlayarak veya bir mektuba yanıt vererek, her iki tarafın da inceleme işi başlamadan önce ve teslim edildikten sonra iş üzerinde anlaştığını belirten, talep sahibi ve İncelemeyi Yapan tarafından verilen resmi onay. e. Talebi belgelemek için kullanılacak formlar veya diğer yöntemler.
Delil Saklama	Delillerin ele alınmasına ilişkin bir politika ve prosedürler oluşturun ve uygulayın. Bu şunları içermelidir: A. Delillerin korunması B. Delil etiketleme C. Delil mühürleme D. Belgelenecek öğeler - gözetim zinciri dahil E. Gözetimsiz bırakılan deliller F. Delillerin güvenliği ve işlenmesi için önlemler G. Depolama ve saklama *Delillerin saklanmasıyla ilgili ayrıntılar için oluşturulmuş örnek form Ek 13'te gösterilmiştir.
Adli İnceleme Sonucu	A. Adli sonuçları desteklemek için teknik kayıtları tutun. Kayıtlar, süreci yürüten uzmanları ve tarihi belirtmelidir. Önceki kayıtlarda yapılan değişiklikler takip edilmelidir. B. Adli sonuçların teknik ve idari incelemesini yapın. C. Adli tıp sonucunu talep sahibine vermeden önce yetkilendirin. D. Adli rapor için ortak bir format oluşturun. Adli Raporun oluşturulması için gereken örnek kriterler formu Ek 14'te gösterilmiştir. E. Görüş verirken bunun adli raporda açıkça belirtilmesi gerekir. F. Adli raporun değiştirilmesine yönelik bir süreç oluşturun.

Kaynak:Interpol(https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics)

4.2.6.2. Laboratuvar akreditasyonu

Adli sonuçlar yargı sistemini etkiler, dolayısıyla doğru ve güvenilir olmaları gerekir. Laboratuvar, akreditasyon programına katılarak çıkardığı rapor sonuçlarına olan güveni garanti edebilir ve gösterebilir. Akreditasyon kurumu, küresel standardı karşıladığından emin olmak için laboratuvar sürecini yıllık olarak değerlendirecektir.

Akreditasyon programına katılım tavsiye edilse de genel olarak gönüllülük esasına dayalıdır ve çoğu ülkede zorunlu değildir. Akreditasyon programıyla ilgilenen bir laboratuvar, sürecin ayrıntıları için kendi ülkesinin akreditasyon kurumuna başvurabilir.

Akredite olmanın bazı önemli faydaları şunlardır:

1. **Adli sonuçlara güvenin sağlanması**
   Bir laboratuvara yılda çok sayıda vaka geldiğinde, laboratuvarın inceleme çalışmalarının ve inceleme uzmanlarının performansını izlemesi genellikle zordur. ISO 17025 standardı, adli sonucun kalite yönünün izlenmesi sürecini tanımlar. Akreditasyonla birlikte bu süreç, laboratuvarın performansını sürdürmeye devam etmesini sağlamak için yıllık olarak değerlendirilecektir. Buna ek olarak, kanıtların yönetilmesi ve incelenmesi süreci uluslararası standartlara uygun olmalı ve paydaşlara laboratuvar tarafından üretilen adli sonuçlar konusunda güven sağlamalıdır.
2. **Standartlaştırılmış süreçlerle daha sistematik bir sistem**
   Birkaç inceleme uzmanının bulunduğu bir laboratuvar, her bir inceleme uzmanının aynı süreç dizisini takip etmesini sağlamalıdır. Bunun amacı, mahkemedeki ifadelerin aynı laboratuvardan gelen her bir inceleme uzmanı arasında tutarlı olmasını sağlamaktır. Böylece savcılar, hakimler ve diğer mahkeme personeli tarafından anında anlaşılmasını kolaylaştırmaktır. Bu akreditasyonun mevcut olması, laboratuvarın gerekli standart süreçleri oluşturmasını ve aynı zamanda uzmanların bunları uygulamasını sağlar.
3. **Kaliteli sonuçlar üretilmesi**
   ISO 17025'in gerekliliklerinden biri de laboratuvar süreçlerinde sürekli iyileştirmeler yapılmasıdır. Laboratuvar, sürekli iyileştirmeler uygulayarak ve daha kaliteli sonuçlar üretmesini sağlayarak akreditasyondan yararlanabilir.

4.2.7. Özet ve Ekler

Elektronik deliller, benzersiz ve geleneksel delil türlerinden farklı olan doğası gereği incelenmesi zor ve hassas ve delillerdir. Bu nedenle gerekli şekilde ve dikkatle incelenmedirler. Bu belgenin amacı, bir adli bilişim laboratuvarının yönetimi ve elektronik kanıtların incelenmesi için standart yönergeleri sağlamaktır. Bunun amacı, INTERPOL üyesi ülkeler tarafından üretilen elektronik delillerin ve sonuçların diğer yargı mercilerinde de kabul edilmesini sağlamaktır.

İnceleme uzmanları ve laboratuvar yönetimi her zaman metodolojileri, kılavuzları ve prosedürleri teknolojideki güncel gelişmelere göre güncellemeye çalışmalıdır. Ancak o zaman suçluları hep birlikte ortadan kaldırabilir ve adaleti olması gerektiği gibi sağlayabiliriz.

Bu rehber Avrupa Konseyi modelinin eklerine benzer ekleri içermektedir. Rehber içinde farklı olan eklere atıf yapılarak ekler bölümünde gösterilmiştir. Bu nedenle Interpol modelinin ekleri dahil edilmemiş olup aşağıda isimleri verilmiştir:

- Laboratuvar yetenek kontrol listesi
- Temel laboratuvar ekipmanı kontrol listesi
- Vaka kayıt formu örneği
- Delil kayıt formu örneği
- Delil etiketleme ve mühürleme örneği
- Veri kopyalama kontrol listesi
- Toplama (Edinim) akış şeması
- Bilgisayar inceleme akış şeması
- Delil verilerini inceleme süreci
- Adli Raporun oluşturulması için gereken örnek kriterler
- Elektronik delil saklama kontrol formu
- Laboratuvara gönderilen talep formu

4.3. Diğer Modellerden Örnekler

Yukarıda verilen örnek modeller tamamen adli bilişim laboratuvarı kurulumu için tasarlanmış ve saygın kurumların hazırladığı rehberlerden alınmıştır. Bunların dışında çeşitli adli bilimler laboratuvarı kurulum rehberleri içinde adli bilişim laboratuvarı için ayrılan bölümlerde de tavsiyeler bulunmaktadır. Bu başlık altında bu örneklere yer verilecektir. Ayrıca adli bilişim incelemeleri içinde

bulunan ses ve görüntü incelemeleri konularında da bazı farklı uygulamalar mevcuttur. Bu başlık altında ses ve görüntü inceleme laboratuvarları konusunda tavsiyeler bulunmaktadır.

4.3.1. NIST modeli

1901'de kurulan Ulusal Standartlar ve Teknoloji Enstitüsü (The National Institute of Standards and Technology-NIST) şu anda ABD Ticaret Bakanlığı'nın bir parçası olarak faaliyetlerine devam etmektedir. NIST, ABD'nin en eski fizik bilimi laboratuvarlarından biridir. NIST kurulduğu yıllarda, o zamanlar Birleşik Krallık, Almanya ve diğer ekonomik rakiplerin yeteneklerinin gerisinde kalan ikinci sınıf bir ölçüm altyapısıyla ABD'nin endüstriyel rekabet gücüne yönelik büyük bir zorluğu ortadan kaldırmak için kurulmuştur (Ulusal Standartlar ve Teknoloji Enstitüsü [NIST], 2024).

Akıllı elektrik şebekesi ve elektronik sağlık kayıtlarından atom saatlerine, gelişmiş nanomateryallere ve bilgisayar çiplerine kadar birçok ürün ve hizmet, bir şekilde Ulusal Standartlar ve Teknoloji Enstitüsü tarafından sağlanan teknolojiye, ölçüme ve standartlara dayanmaktadır. Temelde NIST ölçüm bilimi vasıtalarını kullanarak çeşitli sektörlerdeki aktörlere standartlar sağlamaktadır. Standartların geliştirilmesi ve kullanılması için de bünyesinde birçok sektörden çalışanla birlikte çeşitli bilim laboratuvarlarına sahiptir (NIST, 2024).

Ulusal Standartlar ve Teknoloji Enstitüsü'nün ana araştırma bileşenlerinden biri olan Bilgi Teknolojisi Laboratuvarı (Informatıon Technology Laboratory-ITL), bilgi teknolojisinde araştırma ve geliştirme yoluyla ölçüm bilimini, standartları ve teknolojiyi geliştirerek ABD'nin endüstriyel rekabet gücünü teşvik etme yönünde geniş bir misyona sahiptir (NIST, 2024).

ITL, Ulusal ölçüm ve standartlar altyapısı için teknik liderlik sağlayarak ABD ekonomisini desteklemektedir. ITL, bilgi teknolojisinin geliştirilmesini ve verimli kullanımını ilerletmek için testler, test yöntemleri, referans verileri, kavram kanıt uygulamaları ve teknik analizler geliştirmektedir. ITL'nin sorumlulukları arasında federal bilgisayar sistemlerindeki hassas sınıflandırılmamış bilgilerin uygun maliyetli güvenliği ve gizliliği için teknik, fiziksel, idari ve yönetim standartlarının ve yönergelerinin geliştirilmesi yer almaktadır (Lyle ve diğerleri, 2008).

NIST bünyesinde bulunan Adli Bilim Laboratuvarları Tesisleri Teknik Çalışma Grubu (The Forensic Science Laboratories Facilities Technical Working Group-TWG) 2013 yılında adli bilimler laboratuvarının kurulumu hakkında bir rehber yayınlamıştır. Rehberin adli bilişim laboratuvarı bölümünde verdiği tavsiyeler Çizelge 4.5'te gösterilmiştir (Aguilar ve diğerleri, 2013).

Çizelge 4.5. Adli bilişim bölümü

Alan Tipi	Tasarım Hususları
Ana Laboratuvar	• Analist başına 15 metrekarelik U şeklinde iş istasyonu • Süreç içi kanıtlar için güvenli kanıt saklama kabinine sahip bireysel analist iş istasyonları • Gerektiğinde ekipman ve prosedürler için laboratuvar lavabolu çeşitli tezgah • Tüm iş istasyonlarında birden fazla elektrik ve veri çıkışı • Hassas malzemelerin araştırılması nedeniyle tüm pencerelerde (iç ve dış) karartma panjurları
Delil Saklama Odası	• Gerektiğinde iş istasyonunda süreç içi depolama için ilave alan • Ağır/hacimli bilgisayar bileşenleri için ağır hizmet tipi raflar
Video (Görüntü) Analiz Odası	• Işık seviyesi kontrolü • Personel ve vaka yüküne bağlı olarak oda sayısı • Önerilen minimum boyut: 100 metrekare
Ses Analiz Odası	• Akustik olarak izole edilmiş oda • Personel ve vaka yoğunluğuna bağlı olarak yeterli miktarda oda
Radyo Frekansı Korumalı Oda	• Analist başına 8 ayaklı inceleme tezgahı • Girişte korumalı, kilitli ön oda • Önerilen minimum boyut: 100 metrekare

Kaynak: (Aguilar ve diğerleri, 2013)

4.3.2. ASTM standardı

Gayri resmî standart geliştirme kuruluşlarından biri olan ve 1902 yılında kurulan ASTM International (önceki adıyla American Society for Testing and Materials) metaller, inşaat, petrol, tüketici ürünleri, bilişim konularında geliştirilmiş teknik standartları bünyesinde bulundurmaktadır. Bugün ürün kalitesini iyileştirmek, sağlık ve güvenliği geliştirmek, pazar erişimini ve ticareti güçlendirmek ve

tüketici güvenini oluşturmak için dünya çapında 12.000'den fazla ASTM standardı kullanılmaktadır. Bünyesinde 140 ülkeden sayısı 30000 civarında teknik personel bulundurmaktadır. Standartları teknik komiteleri aracılığla oluşturan kurumda 140'tan fazla standart teknik komitesi bulunmaktadır. ASTM, standart geliştirmenin ötesinde, yan kuruluşu olan Güvenlik Ekipmanları Enstitüsü aracılığıyla sertifikasyon ve beyanın yanı sıra teknik eğitim programları ve yeterlilik testleri de sunmaktadır. ASTM'nin genel merkezi West Conshohocken, Pensilvanya'da bulunmaktadır ve ofisleri Belçika, Kanada, Çin, Peru ve Washington, D.C.'de bulunmaktadır (ASTM, 2024).

ASTM 2023 yılında "Adli Ses Laboratuvarı Kurulumu ve Bakımı için Standart Kılavuz (E3150)" standardını yeniden güncelleyerek yayınlamıştır. Bu kılavuz, adli ses laboratuvarı alanının oluşturulmasının yanı sıra laboratuvarda bulunan ekipmanın yapılandırılması, doğrulanması ve bakımına ilişkin tavsiyeleri ortaya koymaktadır. Aşağıda adli ses incelemeleri için kurulacak laboratuvara ilişkin ASTM (E3150) standardının önemli noktaları yer almaktadır;

- **Genel-** Bir ses laboratuvarının tasarlanması ve yapılandırılmasında, laboratuvarın akustik ortamının/odasının yanı sıra iklim kontrolünün de dikkate alınması önemlidir.
- **Çevre—**Adli ses laboratuvarının içindeki ve çevresindeki ekipmandan bağımsız fiziksel ortam, üretilen işin kalitesi üzerinde büyük bir etkiye sahip olabilir.
- **Akustik—**Adli ses laboratuvarının akustik ortamı, adli ses analizinin kalitesini etkileyebilecek ortam sesleri ve etkilerinin (örneğin, malzemeler, rezonanslar, yankı) toplamıdır. Bir kayıtta hangi seslerin mevcut olduğu konusunda kafa karışıklığını önlemek için ses laboratuvarındaki dikkat dağıtıcı ses unsurlarını ortadan kaldırmak veya en aza indirmek gereklidir.
- **Akustik engeller:**
    - Arka planda sohbet, TV, radyo ve müzik;
    - Bilgisayar ve ekipman soğutma fanları;
    - Klima üniteleri ve hava akışı;
    - Titreşim.
- Laboratuvardaki dış gürültüyü azaltmak için aşağıdaki gibi adımlar atılabilir:
    - Yankılanma ve yankıyı absorbe etmek için akustik köpük veya başka malzemelerin kullanılması,
    - Laboratuvarın akustik tuzaklarla tasarlanması,
    - Gereksiz hava kanallarının yeniden yönlendirilmesi,
    - Mevcut hava kanalları içerisinde akustik perdeleme kullanılması,
    - Kapatıldığında her tarafı sıkıca kapanan ağır ahşap kapıların kullanılması,

  - Yabancı sesleri azaltmak ve incelenen sinyalin duyulabilirliğini en üst düzeye çıkarmak için incelemeler sırasında yüksek kaliteli kulaklıkların kullanılması.
- **Sıcaklık ve Nem—**Laboratuvarın sıcaklığının ve neminin ekipman üreticisinin standartları dahilinde olduğundan emin olun. Ekipmanın kendisi ısı üretir ve sinyali etkileyebilecek ısı oluşumunu önlemek için yeterli havalandırma gerektirir.
- **Elektromanyetik Parazit—**Çeşitli elektromanyetik kaynaklardan kaynaklanan parazit, sinyal kalitesini etkileyebilir. Aşağıdaki önlemler alınabilir;
  - Güç hatları, motorlar, lamba karartıcıları, floresan ışıklar ve kesintisiz güç kaynakları gibi alternatif akım (AC) kaynakları, yanlış yönlendirilmiş sinyal kablolarında gürültüye neden olabilecek manyetik pikap döngüleri oluşturabilir. Transformatörleri ve güç hatlarını sinyal hatlarından ayırın. Güç ve sinyal hatlarının kesişmesi gerekiyorsa, bunların birbirine 90° açıyla geçmesini sağlayın.
  - Yanlış topraklama, topraklama döngüleri oluşturabilir. Bu olguya birçok faktör katkıda bulunmaktadır. Topraklama döngülerini en aza indirmek için ekipmanı ve rafları uygun şekilde topraklayın.
  - Hoparlörler gibi yakındaki herhangi bir manyetik ortamın bütünlüğünü etkileyecek kadar güçlü manyetik alanlar üreten öğeler, kanıt niteliğindeki kayıtlardan mümkün olduğunca uzak tutulmalı veya laboratuvardan uzaklaştırılmalıdır.
  - Cep telefonları, çağrı cihazları, radyolar ve diğer radyo frekansı (RF) ileten cihazlar, kablolara veya ekipmanlara müdahale edebilir ve kapatılmalı veya laboratuvardan çıkarılmalıdır.
  - Katot ışın tüpü (CRT) video monitörleri yakındaki veya bağlı ses ekipmanlarında duyulabilir gürültüye neden olabilir. Oynatma/kaydetme cihazlarını CRT monitörlerin yanına yerleştirmeyin.
- **Sistem Yapılandırması—**Ekipmanın, kabloların, konektörlerin, arayüzlerin ve yazılımın kalitesi ve düzeni, ses sinyalini doğrudan etkiler.
  - Bilgisayar ve Ağ Sistemleri—Kanıtlara erişme yetkisi olmayan kişilerden izole edilmiş bir sistem üzerinde kanıtları işleyin. Bilgisayarların ve ağ sistemlerinin güvenliğinin sağlanması da önemlidir. İnternette benzersiz codec bileşenleri, özel oynatıcılar vb. aramak için ayrı bir bilgisayarın olması önerilir.
  - Ses Ekipmanı—Mümkün olan yerlerde profesyonel ve yayın sınıfı ekipman kullanarak, eldeki göreve uygun oynatma, işleme ve kayıt ekipmanını seçin.

- Sinyal Yolu—Sinyal yolu, ses verilerinin kaynaktan tüm konektörler, arayüzler, kablolar ve yazılımlar aracılığıyla hedefe kadar olan tam yoludur. En az miktarda bozulmaya sahip sinyal yollarını tasarlayın. Sinyal kaybını en aza indirmek ve parazit olasılığını azaltmak için yeterli kalitede ve minimum uzunlukta kablolar ve konektörler kullanın. Analog ses çalışmaları için, dengeli hatların kullanımını dengesiz hatlar üzerinden en üst düzeye çıkarın. Adaptörleri ekipmanı birbirine bağlamak için istiflemekten kaçının. İlgili özel ara yüzler için tasarlanmış bir kablonun kullanılması tercih edilir. Analog ara yüzlerin empedansının ve seviyesinin farkında olun. Adli ses analizlerinin gerçekleştirilmesi için hoparlörler önerilmez; ancak inceleme sırasında başka şekilde kullanılırsa, hoparlörlerin ses sinyalinin tam frekans spektrumunu yeniden üretebilecek kapasitede olduğundan emin olun.
- İletim Formatı—Ses verilerini en az miktarda bozulma, kayıp veya zayıflamayla ileten sinyal formatını seçin. Bu karar, kullanılan ekipmanda hangi formatların mevcut olduğuna bağlıdır. Dijitalden analoğa ve analogdan dijitale dönüşümlerin sayısını en aza indirin.

- **Sistem Doğrulaması—**Ekipman ve ara bağlantılar yapılandırıldıktan, güncellendikten veya değiştirildikten sonra, her şeyin beklendiği gibi çalıştığını doğrulamak için çeşitli bileşenler aracılığıyla test sinyalleri çalıştırın.
  - Kalibrasyon—Kalibrasyon, ölçümler ile bilinen standart değerler arasındaki ilişkiyi kurma işlemidir. Eğer bir ekipman parçası, sayısal sonuçların incelemelerle belirleyici bir öneme sahip olduğu ölçümlerin temelini oluşturuyorsa, o zaman bunun kalibre edilmesi kritik önem taşır. Sinyal oluşturucular ve spektrum analizörleri gibi bu ölçümleri üreten ekipmanlar izlenebilir bir standarda göre kalibre edilmelidir. Kalibrasyon, herhangi bir önemli bakım veya onarımdan sonra veya kontrol testinde başarısız olunması durumunda üreticinin spesifikasyonlarına göre gerçekleştirilmelidir.
  - Yeni veya Geçici Ekipman—Belirli ses delilleri, laboratuvarın normal bir parçası olmayan ekipmanlar gerektirecektir. Bu yeni veya geçici ekipman şunları içerebilir:
    - Gönderilen cihazlar,
    - Sunulan medyanın formatını desteklemek için edinilen ekipman veya codec'ler,
    - Daha eski veya arşivlenmiş ekipman ve
    - Yeni alınan ekipman.
  - Sesli gösterimlerin oynatılmasının optimize edilmesi, bu ekipmanın sisteme ara yüzlenmesini gerektirebilir. Alışılmadık ekipmanların doğru şekilde kullanıldığından emin olmak için mevcut kullanım kılavuzlarına bakın. Bilinmeyen veya test edilmemiş

yazılımları sisteme yüklerken yedekleme ve virüs taraması gibi makul önlemleri alın. Üçüncü taraf codec'ler veya yardımcı programlar arasındaki olası dengesizlik veya uyumsuzluk nedeniyle, bu programların kullanımının bağımsız bir bilgisayar veya sanal makineyle sınırlandırılması önerilir. Yeni veya tanıdık olmayan herhangi bir yazılım veya ekipmanı, inceleme materyallerinde kullanmadan önce bilinen veriler üzerinde test edin.

- **Bakım—**Hareketli parçalara veya aşınmaya maruz kalan parçalara sahip ekipmanlar, rutin muayene ve bakıma tabi tutulmalıdır. Bu görevin düzenli olarak ve üreticinin spesifikasyonlarına göre yapılmasını sağlamak için kayıtlar tutulmalıdır. Bakım aşağıdakileri içerebilir ancak bunlarla sınırlı değildir:
    - Bant destelerindeki elektromanyetik kafaların temizlenmesi ve mıknatıslığının giderilmesi,
    - Bant destelerindeki ırgatların ve makaraların temizlenmesi ve kontrol edilmesi ve
    - Azimut hizalaması.
    - Dijital ekipman ve bilgisayarların bakımı şunları içerebilir:
        - Sabit sürücülerin birleştirilmesi;
        - Antivirüs yazılımlarının güncellenmesi ve bilgisayarlarda virüs kontrolü yapılması;
        - Gerektiğinde bilgisayar işletim sistemlerinin güncellenmesi;
        - Yazılımın, ürün yazılımının, sürücülerin ve kodeklerin güncellenmesi.
- İnceleme sırasında ekipmanın birbirine nasıl bağlandığını, kullanılan sinyal formatlarını, yeni veya geçici ekipmanı ve yeni ekipman üzerinde yapılan doğrulama testlerini belgeleyin.

4.3.3. FBI örneği

Federal araştırma bürosunun (Federal Bureau of Iinvestigation-FBI) 2003 yılında yayımladığı "Modern Adli Ses-Görüntü Laboratuvarının Donatılması" makalesi de ses ve görüntü incelemeleri laboratuvarları için etkili bir kılavuzdur. Bugün ASTM dâhil bir çok standart kuruluşu bu konuda rehberlerini hazırlarken hala bu kaynaktan faydalanmaktadır. (Koenig ve diğerleri, 2003).

Yayımlanan rehber giriş, adli ses ve görüntü incelemeleri, ekipman ve maliyetler ve laboratuvar alanıyla ilgili hususlar olmak üzere 4 bölümden oluşmaktadır. Adli ses ve görüntü incelemeleri laboratuvarı hakkında yayımlanan rehber ve verilen tavsiyeler aşağıda sıralanmıştır.

4.3.3.1. Giriş

Modern bir adli ses-video laboratuvarının kurulması veya kapasitesinin arttırılması, fizik, elektrik ve elektronik mühendisliği, bilgisayar bilimi, analog ve dijital teori, akustik, dijital sinyal analizi, dijital görüntüleme ve diğer ilgili alanlar dâhil olmak üzere çeşitli disiplinlerden yararlanır. Bu disiplinler, adli bilişim uzmanının güvenilir incelemeler yapabilmesini sağlamak için çok çeşitli elektronik ekipmanlara ihtiyaç duyar. Modern bir ses/görüntü adli bilişim laboratuvarının kurulması veya kapasitesinin arttırılması sırasında aşağıdaki faktörler dikkate alınmalıdır:

- Potansiyel çalışanların belirlenmesi
- Belirli ses ve video analiz alanlarında uzun bir çıraklık veya eşdeğer personel deneyimi
- Dijital sinyal analizi, kayıt teorisi, ses ölçümü ve video görüntüleme gibi alanlarda uzmanlık eğitimi almak
- Diğer yerleşik laboratuvarlardan destek ve rehberlik istemek
- Laboratuvarı çok sayıda analog ve dijital ses ve video formatını oynatacak ve kaydedecek şekilde donatmak ve ardından ses anlaşılırlığını iyileştirme, sesleri karşılaştırma, ses dışı sinyalleri tanımlama, kayıtları doğrulama, video görüntülerini iyileştirme ve diğer ilgili analizleri yürütme yeteneğinin sağlanması
- Profesyonel ses, video, geliştirme, sinyal analizi, görüntüleme ve diğer ilgili ekipmanların tedarik edilmesi
- Laboratuvar için fiziksel alanın belirlenmesi

4.3.3.2. Adli ses ve görüntü incelemeleri

Modern ses-görüntü adli bilişim laboratuvarları, cezai soruşturmaları, hükümet istihbaratını, hukuk davalarını, personel ve idari konuları ve diğer ilgili konuları desteklemek için analog veya dijital ses-görüntü kayıtlarını analiz etme kapasitesine sahiptir. Bazı laboratuvarlar ses ve görüntü kayıtları üzerinde geniş bir yelpazede incelemeler yaparken, diğerleri yalnızca çoğaltma ve sıklıkla talep edilen birkaç analiz sağlar.

En sık gerçekleştirilen sekiz ses ve görüntü incelemesi, karmaşıklık düzeyi en düşükten en yükseğe doğru olacak şekilde aşağıda listelenmiştir:

Oynatma ve çoğaltma: Kayıtları oynatma ve standart formatlarda yüksek kaliteli, kolayca kullanılabilir kopyalar sağlama yeteneği. Tam donanımlı bir laboratuvar, çoğu ses-video formatının

yanı sıra özel kayıtlarla da çalışabilir (örneğin, kolluk kuvvetleri formatları, 911 kayıt kayıtları, hızlandırılmış video).

Onarım: Standart ses-video analog ve dijital formatlarındaki yırtılmış veya gerilmiş bantları onarma yeteneği

Ses geliştirme: Kayıtların ses anlaşılırlığını iyileştirme ve ses kayıtlarının ve video formatlarındaki ses bilgilerinin geliştirilmiş kopyalarını hazırlama yeteneği

Ses tanımlama: Benzer ve farklı özellikleri tanımlayarak bilinmeyen kayıtlı sesleri bilinen ses örnekleriyle karşılaştırma yeteneği

Video görüntüsü çoğaltma ve geliştirme: Video kayıtlarını çoğaltma veya iyileştirme yeteneği

Sinyal analizi: Kaynağını ve özelliklerini (örn. telefon sinyalleri, silah sesleri) belirlemek için ses dışı sinyalleri ölçme, tanımlama ve karşılaştırma yeteneği.

Orijinallik: Orijinalliği, sürekliliği ve bütünlüğü belirleyerek ses-video kayıtlarının orijinalliğini çözümleme yeteneği

Dijital veri analizi ve alımı: Ticari ve tescilli kayıt cihazlarındaki dijital ses-video kayıtlarını çıkarma ve analiz etme yeteneği

4.3.3.3. Ekipman ve maliyetler

Sıklıkla yapılan sekiz adet adli ses ve görüntü incelemesi için gerekli ekipman gereksinimleri aşağıda listelenmiştir. Faz numaraları, en temel ve daha karmaşık ekipman gerekliliklerini temsil eder. Bu bölümde verilen maliyetler günün şartlarına değiştiği için maliyet konusu incelenmeyecektir. Ayrıca rehberde personel ve eğitim konularına değinilmemiştir.

- **Faz 1: Playback, Çoğaltma ve Onarım:** Ses ve video kayıtlarının yüksek kalitede oynatılmasına ve standart formatta çoğaltılmasına olanak sağlamak için bir laboratuvarın aşağıdaki ekipmanlara sahip olması gerekir:
    - Ağır hizmet tipi taşımalara sahip standart profesyonel ses kasetçalarları, her standart hızda + yüzde 10 veya daha fazla hız ayarı, üç kafalı tasarım, Dolby gürültü azaltma sistemleri (B, C ve S) ve gerçek zamanlı sayaçlar. Yararlı eklemeler arasında saniyede 15/16, 17/8 ve 3¾ inç (ips) olarak ayarlanmış hızlar, en az 15/32 ila 3¾ ips arasında

sürekli oynatma hızı ayarı ve kendi ses düzeyi kontrolüne sahip bir kulaklık girişi yer alır.

- Saniyede 0,7 ila 2,4 santimetre sürekli oynatma hızları, doğru ölçüm, kulaklık ses seviyesi kontrolleri ve profesyonel kalitede taşıma ve elektronik sistemler dahil olmak üzere, adli uygulamalar için optimize edilmiş profesyonel ses mikro kaset oynatma birimleri.
- Açık makara, mini kaset, gövde üzerinde minyatür, NT dijital ve oynatma hızı, parça konfigürasyonu ve laboratuvarda alınması beklenen kayıt türleriyle eşleşen diğer özelliklere sahip diğer analog ve dijital cihazları içeren özel ses oynatma sistemleri. Seçilen kayıtların oynatılması, yalnızca emniyet teşkilatlarının kullanabileceği özel cihazlar ve/veya yazılım gerektirebilir.
- Analog U-Matic'ten VHS, VHS-C, SVHS, 8mm, Hi8, hızlandırılmış, 6mm dijital ve 8mm dijital dahil olmak üzere en yeni dijital konfigürasyonlara kadar değişen formatlara sahip video kaydediciler/oynatma üniteleri. Yüksek kaliteli veya profesyonel disk kaydediciler mümkün olan en iyi oynatma ve/veya kaydı sağlar. Video oynatımında, her bir kafanın (alan) ilgili parçayı tam olarak takip etmesi ihtiyacına vurgu yapılmalıdır. Bu, çıktı sonuçlarını optimize etmek amacıyla benzer türde bir dizi video oynatma biriminin tedarik edilmesini gerektirebilir. Video çoğaltmada doğal kayıpları en aza indirmek için ara kopyalara ihtiyaç duyulduğunda, profesyonel bir analog veya dijital format ya da yarı profesyonel format (yani SVHS) birimi mevcut olmalıdır.
- Laboratuvarda beklenen çeşitli video formatları için zamanlama hatalarını düzeltmek ve ayrı alanları ve kareleri yakalayıp hafızasında tutmak için profesyonel bir dijital zaman tabanlı düzeltici.
- Laboratuvarda oynatılacak en yüksek kalite formatının tam bant genişliğini ve çözünürlüğünü doğru bir şekilde görüntüleyen bir video monitörü. Uzun vadeli renk saflığını sağlamak için elde taşınabilen bir ekran manyetiklik gidericisinin de mevcut olması gerekir.
- Ekipman için doğru genişliğe sahip ekipman rafları, genellikle 19 inçtir. Bağlantı bölmeleri, aralayıcı paneller ve kablo hatları dahil olmak üzere profesyonel kalitede aksesuarlar içermelidirler.
- Geniş çalışma ve ekipman alanı sağlamak için sağlam ve en az 30 x 60 inç boyutunda çalışma alanı ve ekipman masaları. Geçici kullanım dışında katlanır masalardan kaçının.

- Gerekli tüm ekipman bağlantılarını yönetmek için yüksek kaliteli kablolama, konektörler ve adaptörler
- Uygun birleştirme blokları, düzenleme tırnakları, tıraş bıçakları, muhafazaları açmak için küçük bıçaklar, manyetik olmayan lider bant, bant temizleme solventi ve minyatür, mıknatıslanmayan alet kitlerini içeren bant onarım malzemeleri
- Parçacık boyutları 0,2 ila 1,5 mikron aralığında olan ferro-sıvı çözeltisi. Daha küçük parçacık boyutları analog bantlardan tutarlı bir şekilde çıkarılamaz.
- Ferrofluid solüsyonunun uygulanmasından sonra bandın iz konfigürasyonunu ve azimut hizalamasını kontrol etmek için on çarpanlı bir büyüteç
- Kulak çevresini tamamen kapatan, iyi yastıklı, ağır hizmet tipi, profesyonel kalitede kulaklıklar. Daha ucuz tüketici kulaklıkları ses açısından profesyonel modellere eşit olabilir, ancak genellikle laboratuvardaki ağır hizmet kullanımına dayanamazlar.
- Kopya hazırlamak için boş, yüksek kaliteli ses ve video kaydedilebilir ortam
- Oynatma ve kayıt ekipmanının kalibrasyonu için doğru test kayıtları

- **Faz 2: Ses Geliştirme:** Kaydedilen ses bilgilerinin ses anlaşılırlığında anlamlı iyileştirmelere olanak sağlamak için bir ses-video laboratuvarının aşağıdaki donanıma sahip olması gerekir:
  - İncelemecinin bir ve iki kanallı uyarlanabilir, bant geçiren, tarak, çentik, spektral ters, parametrik ve grafik ekolayzır dahil olmak üzere bir dizi farklı filtre algoritmasına erişmesine ve uygulamasına olanak tanıyan dijital uyarlanabilir bir geliştirme işlemcisi. Dijital uyarlamalı geliştirme işlemcisi aynı zamanda sıkıştırma ve sınırlama işlevlerinin kullanımına da izin vermelidir. En iyi konfigürasyonlar, yazılım kontrollü donanım uygulamalarıdır çünkü tamamen yazılım programları gerçek zamanlı olarak karmaşık filtreler uygulamayabilir ve bilgisayar aynı anda başka işlemler yaparken ses sinyalleri bozulmaya karşı hassastır. Bu filtreleme sistemlerinin tümü, yüksek kaliteli 16 bit veya daha yüksek, analogdan dijitale ve dijitalden analoğa dönüştürücüler, en az iki giriş kanalı ve en az 32 kHz'e kadar bir örnekleme hızı aralığı içermelidir.
  - En az iki kanallı, ayarlanabilir ve otomatik sıkıştırma oranlarına, tutma- serbest bırakma sürelerine ve en az 40 dB kazanç azaltımına sahip ayrı bir kompresör/sınırlayıcı
  - Ses sinyalinin ayrıntılı görsel sunumunu sağlayan bir spektrum analizörü. Ünite, tek kanal özelliğine sahip, hızlı Fourier dönüşümü tasarımına (gerçek zamanlı analizör değil) sahip olmalıdır. Laboratuvarın aynı zamanda sinyal analizi ve/veya orijinallik incelemeleri de yapması halinde, çift kanallı veya daha büyük bir üniteye ihtiyaç duyulacaktır. Hızlı Fourier dönüşüm cihazı, 16 bit veya daha yüksek çözünürlüğe, en az 0-100 Hz'den 0-20 kHz'e kadar ayarlanabilen frekans görüntüleme aralıklarına,

değişken sayıda ortalamaya ve herhangi bir frekans aralığında en az 800 satır çözünürlüğe sahip olmalıdır. . Yakınlaştırma özelliği bazı uygulamalar için de yararlı bir özellik olabilir.

- Dijital geliştirme cihazlarının kontrol edilmesi ve diğer uygun yazılımların çalıştırılması da dahil olmak üzere bir dizi uygulama için kullanılabilen gelişmiş bir bilgisayar sistemi.
- Hızlı Fourier dönüşüm grafiklerinin basılı kopyalarını, dijital geliştirme cihazlarının filtre ayarlarını ve diğer uygulanabilir bilgileri sağlayan bir bilgisayar yazıcısı.
- Ses kayıtlarının hassas, doğrusal olmayan zaman ve genlik işlemleri için gerçek zamanlı olmayan yazılım programları. Adli alana uygulanabilir işlevlerden bazıları, oynatma hızının genel veya yerel olarak düzeltilmesi, genlik ayarlamaları ve normalleştirme için perde değiştirmeyi içerir. Bu yazılım programları ayrıca bir kaydın belirli bölümlerinin redaksiyonlarının daha kolay ve doğru bir şekilde gerçekleştirilmesine de olanak tanır.

- **Faz 3: Ses Tanımlama:** Mevcut laboratuvar spektrografik ve/veya bilgisayar ses karşılaştırma sistemleri kesin sonuçlar vermemektedir, ancak adli koşullar altında toplanan konuşma örneklerinin dikkatli bir şekilde analiz edilmesiyle anlamlı bulgular mümkündür. Minimum gereksinimler aşağıdaki ekipmanı içerir :
  - Özellikle gürültülü kayıt koşullarında mükemmel ses spektrogramları üreten bir analog ses spektrografı.
  - Konuşma ve adli topluluklar için optimize edilmiş, dijital olarak hesaplanmış spektrogramlar üreten özel spektrogram yazılımı. Bu yazılım kullanıcı dostu olmalı ve operatörün grafik sunumun tüm önemli zaman ve frekans özelliklerini kontrol etmesine olanak sağlamalıdır.
  - İki veya daha fazla kayıtlı ses örneğinin seçici olarak izole edilmesini ve yeni bir kayıtta birleştirilmesini sağlayan düzenleme yazılımı.
  - İşitsel karşılaştırma için ayrı ses örnekleri içeren iki giriş sinyali arasında hızlı geçiş yapılmasını sağlayan bir kulaklık değiştirme kutusu.
- **Faz 4: Video Çoğaltma ve Geliştirme:** Video kayıtlarının en doğru şekilde çoğaltılmasına ve geliştirilmesine olanak sağlamak için, bir ses-görüntü inceleme laboratuvarının aşağıdaki ekipmanlara sahip olması gerekir:

- Laboratuvarda beklenen herhangi bir analog format için tek bir alanın/karenin tüm çözünürlüğünü ve sürekli videoyu doğru bir şekilde yakalayan bir video yakalama cihazı. Girişler en azından kompozit ve S-Video içermelidir.
- Hızlı bir işlemciye, büyük bir monitöre, yeterli rasgele erişim belleğine, dijital video girişi (ör. FireWire) ve laboratuvarın video uygulamalarını yönetmek için kapsamlı sabit disk depolama alanına sahip yüksek hızlı bir bilgisayar sistemi.
- Video kanıtlarından basılı kopya görüntüler sağlayan renkli ve siyah beyaz bilgisayar ve video yazıcıları. Sistemdeki diğer bileşenler gibi, yazıcılar da yakalanan ve/veya geliştirilmiş alanların/karelerin tamamını yeniden üretmek için yeterli çözünürlüğe sahip olmalıdır.
- Görsel ayrıntıları keskinleştirmek, büyütmek, geliştirmek, düzenlemek ve düzeltmek için uygun algoritmalara sahip, sürekli video ve sabit video iyileştirmeye yönelik yazılım programları

- **Faz 5: Sinyal Analizi ve Orijinallik:** Bu aşama, ses sinyallerinin sinyal analizini ve ses ve video formatlarının özgünlük analizlerini içerir. Asgari gereksinimler aşağıdaki ekipmanı içerir:
  - Faz 4 bilgisayar sistemi
  - Darbeli çapraz ve tarama altı modları, bileşen ve bileşik girişler ve en az 600 satır yatay çözünürlük içeren profesyonel video monitörleri. Beklenen tüm dijital formatları en yüksek düzeyde çözünürlüğe kadar tam olarak yeniden üretebilmelidirler. Tüm analog ve dijital kayıtları yönetmek için birden fazla monitöre ihtiyaç duyulabilir.
  - Gerçek zamanlı bir analizör değil, hızlı Fourier dönüşümü tasarımına sahip çift kanallı bir spektrum analizörü. Gerekli özellikler yakınlaştırma, iki kanallı karşılaştırma algoritmaları ve uzun vadeli ortalamayı içerir.
  - Genişliği 0,0125 ila 2 inç arasında değişen bant yüzeyinin doğru resimlerinin üretilmesine olanak tanıyan makrofotografik veya dijital kamera sistemi. Dijital kamera kullanılıyorsa çözünürlüğü en az 2000 x 2000 piksel olmalıdır.
  - 16 bit veya daha yüksek çözünürlüğe, en az 44,1 kHz örnekleme hızlarına, iki veya daha fazla giriş ve çıkış kanalına ve düşük gürültü ve bozulma özelliklerine sahip, yüksek kaliteli bir laboratuvar bilgisayarı ses kartı.
  - .wav üzerinde ve bilgisayar formatlı diğer ses dosyalarında dalga biçimi, dar bant spektrumu, spektrografik ve diğer analizleri gerçekleştirme yeteneğine sahip sinyal analiz yazılımı. Görüntülenen verilerin seçilen bölümlerinin işitsel olarak incelenmesine olanak sağlamalı, çeşitli analizlerin yüksek kaliteli çıktılarına olanak

sağlamalı ve çeşitli ekranlar arasındaki zaman korelasyonu ile ekranda birden fazla pencere görüntüleme kapasitesine sahip olmalıdır.

- Orijinal kanıtların herhangi bir görsel veya işitsel bilgi kaybı olmaksızın çoğaltılmasına olanak tanıyan profesyonel ses ve video dijital kayıt cihazları.

- **Faz 6: Dijital Veri Analizi ve Erişimi:** Bu aşama, araştırma alanında kullanılan çeşitli ses ve video kayıt cihazlarında bulunan dijital verilerin aktarılmasını, analizini ve (gerektiğinde) alınmasını içerir. Dijital adli kayıtlar, bant (DAT, NT-2, DDS), optik (CD-R/RW, DVD-R/+R/-RW/+RW/RAM), manyeto-optik dahil olmak üzere çeşitli ortam türlerinde mevcut olabilir. (MiniDisc) ve rastgele erişim (FLASH bellek yongaları, sabit sürücüler). Bu kayıtlar standart bir formatta veya kayıtlı verileri oynatmak ve analiz etmek için özel donanım ve/veya yazılım gerektiren özel kayıt cihazlarına kaydedilmiş olabilir. Bu aşama için ihtiyaç duyulan ekipmanın çoğu faz 1'den 5'e kadar tartışılmıştır; ancak aşağıdaki öğeleri içeren birkaç ek gereksinim vardır:
  - Kullanıcının dijital verileri bit seviyesine kadar görüntülemesine olanak tanıyan yazılım. Tescilli kayıt cihazları, genellikle yalnızca kolluk teşkilatlarının kullanabileceği ek donanım ve/veya gelişmiş yazılım gerektirebilir.
  - Daha yüksek kapasiteli formatlarda bulunan büyük veri dosyalarını arşivlemek için yeterli depolama kapasitesine sahip, çıkarılabilir, yazılabilir bir dijital ortam

4.3.3.4. Laboratuvar alanı ile ilgili hususlar

Laboratuvar, dışarıdaki gürültüyü ve titreşimi azaltacak, laboratuvar ekipmanının seslerini azaltacak ve radyo frekansı girişimini ve manyetik alanları en aza indirecek şekilde yapılandırılmalı veya inşa edilmelidir. Ekipman, ayrı elektrik devreleri, uygun aydınlatma ve güvenli ve yeterli depolama dahil olmak üzere yeterli uygun çalışma alanı için en uygun şekilde düzenlenmelidir. Dış gürültü ve titreşimi azaltmak için aşağıdaki stratejiler uygulanmalıdır:

- Laboratuvarı tren rayları, havaalanları, oyun alanları ve kalabalık caddeler gibi gürültülü dış ortamlardan uzağa yerleştirerek dış gürültüyü mümkün olduğu kadar ortadan kaldırın.
- Nakliye iskelelerinden, kafeteryalardan veya makine atölyelerinden kaçınarak bina gürültüsü ile laboratuvar arasındaki mesafeyi artırın. Laboratuvarı uzaklaştırmak, laboratuvar alanının aynı binada daha sessiz bir yere veya farklı bir binaya taşınması anlamına gelebilir. Laboratuvarın taşınması mümkün değilse gürültünün taşınması bir seçenek olabilir. Örneğin, dinlenme alanlarında bulunan yemek masalarının ve en gürültülü ekipmanların laboratuvarla en uzakta olmasını sağlayacak şekilde dizayn edin.

- Laboratuvar duvarları izole edilebilir ve ses geçirmez hale getirilebilir. Ancak mevcut laboratuvarın içine yeni duvarlar inşa etmek, yeni duvarları eski dış duvarlardan izole etmek ve iki duvar arasındaki boşluğu işlemek laboratuvar alanını azaltır, inşaat maliyetlerini artırır ve geçici gürültü ve toz yaratır.
- Düşük gürültülü fanlara sahip ekipman ve bilgisayarlar satın alarak laboratuvarda oluşan gürültüyü azaltın. Gürültülü ekipmanları ses geçirmez izolasyon bölmelerine yerleştirin. Aydınlatmanın ürettiği işitilebilir vızıltıyı ve belirli elektronik ekipmanlarda neden olabileceği düşük seviyeli gürültüyü önlemek için mümkün olduğunca floresan aydınlatmadan kaçının. Isıtma ve klima fanlarının hızını sınırlayın.
- Laboratuvarları ticari radyo ve TV verici istasyonlarından veya polis ve diğer radyo verici kulelerinden uzağa yerleştirerek radyo frekansı girişimini en aza indirin. Bazı ekipmanlar dış alanlara diğerlerine göre daha duyarlı olduğundan, bu ekipmanları laboratuvarda farklı yerlere veya raflarda farklı yüksekliklere yerleştirin. Laboratuvar alanının yer altına yerleştirilmesi genellikle radyo frekansı sorunlarını en aza indirir. Binanın elektrik kablolarından kaynaklanan parazitler genellikle özel AC güç filtreleriyle giderilebilir. Büyük transformatörler veya büyük mıknatıslı hoparlörler herhangi bir ses veya video kanıtının yakınına yerleştirilmemelidir. Taşınabilir bir Gauss ölçer, bölgede sorunlu manyetik alanların olup olmadığını belirleyebilir. Elektriksel ani yükselmeleri ve diğer düzensizlikleri önlemek için laboratuvarın özel elektrik devreleri olmalıdır.
- Ekipmanlar masaların üzerine yerleştirilebilir ancak sağlam ekipman rafları tercih edilir. Raflar daha iyi soğutmayla daha yüksek yoğunluğa izin verir, daha iyi koruma sağlar, kablolamayı ve bağlantılarda hızlı değişiklikleri kolaylaştırır, hareketlidir ve profesyonel görünür.
- Çalışma alanı yeniden düzenlemeyi gerçekleştirebilecek kadar esnek olmalıdır. Zemin alanı mevcut ve gelecekteki ekipmanları barındıracak şekilde planlanmalıdır. Koridorlar, büyük deliller, büyük ekipmanlar ve ekipman onarımı için kolay erişime izin vermelidir. Kanıtları görsel olarak incelemek, işaretlemek ve düzenlemek için yeterli masa alanı bulunmalıdır. Çalışma alanı yeterli aydınlatmaya, tercihen akkor raylı aydınlatmaya sahip olmalıdır.
- Kanıtların saklanması için güvenli bir alan, kontrollü giriş ve alarm mevcut olmalıdır. Depolama alanı manyetik alanlardan arındırılmış olmalı ve sıcaklık ve nem kontrollü olmalıdır.

5. ADLİ BİLİŞİM LABORATUVARI KURULUMU İÇİN MODEL ÖNERİSİ

Adli bilişim laboratuvarının kurulumu için önerilen modele geçmeden önce uygulayıcıların cevaplaması gereken bir dizi soru bulunmakta olup, cevaplara göre modelin şekillenmesi esas alınmalıdır. Verilen modellere bakıldığında öncelikle kurulmak istenen laboratuvarın büyüklüğüne karar verilmesi gerekmektedir. Laboratuvar kurmak isteyen her organizasyon sorulara kendi hedeflerine uyacak şekilde cevap vererek önerilen modeli kendi oluşturacağı laboratuvar planına entegre edebilir. Temel anlamda yol gösterici olacak soruları şu şekilde sıralayabiliriz;

- Kurulacak olan adli bilişim laboratuvarında kaç personel istihdam edilmesi planlanmaktadır? Laboratuvar kurulumunu etkileyen en önemli faktörlerin başında yine insan faktörü yer almaktadır.
- Laboratuvar kurulduğunda çeşitli adli makamlardan (müşterilerden) yeterli sayıda adli bilişim dosyası gelmesi bekleniyor mu? Aslında bu soru kamu yararı gözeten ve bütçesi devlet tarafından karşılanan kurumlar için değil özel bir şekilde kurulacak olan laboratuvarlar için geçerlidir. Görüldüğü üzere adli bilişim laboratuvarı kurmak çok maliyetli bir iştir. Bütçesi devlet tarafından karşılanan kurumlar kurulacak laboratuvarın yerini bu soruya göre şekillendirmelidir. Fakat işletme, bakım, personel gibi bir takım giderleri müşterilerden alacağı ücretler ile sağlayan özel laboratuvarlar bu sorunun cevabını çok objektif bir şekilde verebilmelidir.
- Kurulacak olan laboratuvar tek başına bir adli bilişim laboratuvarı mı olacak yoksa kendisinden daha geniş çapta kurulacak olan bir adli bilimler laboratuvarının parçası mı olacaktır? Bu sorunun cevabı özellikle laboratuvar yönetimini etkileyecektir. Gelen delillerin ilk olarak teslim alınması aşamasından ilgili uzmana atanmasına kadar uygulanan prosedürlerin bu sorunun cevabına göre değişiklik göstereceği açıktır.

5.1. Önerilen Model

Örnek modeller incelendiğinde önerilecek olan model yönetim bölümü ve teknik gereklilikler bölümü olacak şekilde temelde iki bölümden oluşmaktadır. Yönetim bölümü araştırma, bina, fiziki koşullar, görevli personel, eğitimi, işe alımı ve kalite yönetim sistemleri gibi alt bölümlerden oluşmaktadır. Teknik gereklilikler bölümünde ise adli bilişim aşamalarına paralel olacak şekilde her aşamada kullanılan metotlar doğrultusunda raporun son olarak sunumu ve delillerin iadesine kadar olan süreç incelenecektir.

5.1.1. Yönetim

Aşağıdaki alt bölümlerde organizasyonel gereklilikler ve dikkate alınması gereken laboratuvar yönetiminin sorumlulukları sunulmaktadır.

5.1.1.1. Amaç

Kurulması planlanan adli bilişim laboratuvarının amacı belirlenmelidir. Örnek vermek gerekirse üniversite bünyesinde kurulacak olan bir laboratuvarın eğitim hedefi daha ağır basarken bir kolluk kuvveti bünyesinde kurulacak olan bir laboratuvarın daha etkin ve hızlı şekilde dosya inceleyerek soruşturmacı birimlerin işini kolaylaştırması gibi bir hedefi öne alması gerekmektedir. Aynı şekilde kar amacı güden bir özel laboratuvarın amacı daha fazla müşteri kazanmak (fazla sayıda dosya incelemesi) olabilir. Kurulacak olan laboratuvarın amacı belirlendikten sonra personel sayısı, niteliği bina büyüklüğü, konumu gibi etmenler değerlendirilecektir.

5.1.1.2. Bütçe

Kurulacak laboratuvarın büyüklüğünden içine konacak yazılım donanım miktarı ve çalışacak personel sayısına kadar birçok durumu etkileyen bütçe faktörü belirlenecek kalemler arasında en başta yer almaktadır. Adli bilişim laboratuvarı kurmanın maliyeti göz önüne alındığında özel ya da kamu kurumu olması fark etmeksizin bütçenin belirlenmesi gerekmektedir. Ayrıca sarf edilecek masraflar devamlı bir faaliyet olduğundan dolayı bütçenin sürekli güncelleme ihtiyacı bulunmaktadır. Örnek modellerde belirtildiği üzere bütçe tek seferlik harcamalar (bina, kurulum, güvenlik vb.) ve devam eden maliyetler (personel giderleri, eğitim, yazılım lisansları vb.) olarak iki kategoride belirlenebilir.

5.1.1.3. Fiziki koşullar

Fiziki koşulların belirlenmesinde amaç ve bütçe çok önemli bir etkiye sahiptir. Özellikle kurulması planlanan laboratuvar sıfırdan bir inşaat yapılarak kurulacaksa maliyetlerin artacağı göz önünde bulundurulmalıdır.

Burada önemli olan bir diğer husus ise konunun başında belirtilen laboratuvarın tek başına bir adli bilişim laboratuvarı mı yoksa adli bilimler laboratuvarının bir parçası mı olacağı konusudur. Eğer planlanan laboratuvar sadece adli bilişim alanında hizmet veren bir laboratuvar olacaksa laboratuvar girişinden itibaren danışma, delillerin teslim alınma yeri, ilgili bölüme gönderilmesi (veri, görüntü, ses incelemeleri) gibi konularda daha fazla personele ihtiyaç duyulacaktır. Daha büyük bir laboratuvarın

parçası olacaksa delillerin adli bilişim bölümüne kadar olan kayıtları diğer adli bilim branşlarıyla birlikte ortak görevlendirilen personele yaptırılabilir.

Ayrıca güvenlik konusunda da tek laboratuvar kurulma durumunda tüm masraflar adli bilişim yönetimi tarafından karşılanırken ortak laboratuvar kurulması durumunda maliyetler bölünebilir.

Laboratuvara gelen ziyaretçiler sadece belirli bir bölümde karşılanmalı incelemenin yapıldığı alanlara girişleri yasaklanmalıdır. Aynı şekilde laboratuvarda görevli personelin giriş ve çıkışları biyometrik verilerle (göz tarama, parmak izi okuma vb.) ya da kart okuyucu sistemler gibi önlemlerle sağlanmalıdır. Unutulmamalıdır ki incelenen materyallerin delil statüsünde olması hukuki olarak yöneticilere sorumluluk yüklemektedir. Ayrıca elektronik delillerin hassaslığı da göz ardı edilemeyecek faktörlerdendir. İnceleme yapılan yerler hariç ortak alanlara kamera sistemleri kurulması gelen ziyaretçilerin kayıt altına alınması da alınacak güvenlik tedbirleri arasında yer almaktadır.

Laboratuvarın konumu da düşünülmesi gereken bir diğer fiziki koşullardandır. Posta ile gelen deliller açısından laboratuvar kurulması gereken il merkezlerinden çok uzakta olmamalıdır.

Binanın depreme dayanıklı olması, yangın söndürme sisteminin bulunması, özellikle elektrik tesisatının çok iyi durumda olması dikkat edilmesi gereken özellikler arasında yer almaktadır. Bazı özel durumlarda (şifre kırma vb.) bilgisayarların sürekli çalışacak durumda olması göz önüne alındığında jeneratör sistemi ve cihazların ısınmasından dolayı oluşabilecek hasarlar da düşünülerek iyi bir iklimlendirme sistemi de laboratuvarda olmalıdır.

Kurulması planlanan laboratuvarın büyüklüğü bütçe ile doğrudan alakalıdır. Bu kapsamda her kurum kendi bünyesinde büyüklüğe karar verecektir. Fakat eğer olanaklar izin veriyorsa şu hususların laboratuvarda sağlanması gerekmektedir;

- Delillerin özel olarak saklanacağı yangına dayanıklı çelik kasalar ya da özel odalar,
- Delil olmayan malzemelerin (inceleme bilgisayarları, tarayıcılar, fotokopi makinaları, evrak personel dolapları ve çalışma masaları vb.) konulacağı yeterli büyüklükte alan,
- Personelin inceleme alanı dışında toplanmasına olanak sağlayacak bir toplantı odası,
- Personelin inceleme alanı dışında dinleneceği bir alan.
- Doğru bir ışıklandırma sistemi çalışma verimliliğini ve doğruluğunu artırmak için önemli bir unsurdur. Doğru renk sıcaklığı ve renk yayılımı sağlayarak, analiz edilen dijital verilerin doğru bir şekilde değerlendirilmesini kolaylaştırır. Gölgeleri azaltarak, çalışma alanlarını daha net hale getirir ve çalışanların odaklanmasını sağlar. Aynı zamanda, yansımaları minimize ederek görsel

rahatsızlıkları önler ve uzun süreli çalışmalar sırasında konforu artırır. Işıklandırma sisteminin esnek olmasıyla farklı çalışma bölgelerinde farklı ışıklandırma seviyelerine uyum sağlanır, böylece her bir görev için uygun aydınlatma koşulları sağlanmış olur. Floresan ışıklar bazı durumlarda rahatsızlık verebilir ve odaklanmayı zorlaştırabilir.

- Ergonomi, ideal bir adli bilişim laboratuvarının vazgeçilmez bir unsuru olarak, çalışanların sağlığını ve performansını önemli ölçüde etkiler. Ergonomik tasarımlı masalar, sandalyeler ve diğer mobilyalar, çalışanların uzun süreli oturmalarda daha rahat olmalarını sağlar ve belirli pozisyonlarda çalışırken vücutlarını doğru bir şekilde destekler. Bu durum, fiziksel rahatsızlıkları önler ve çalışanların işlerine daha fazla odaklanmalarını sağlar. Ergonomik ayarlamaların yapıldığı bir ortamda çalışanlar, daha az yorgunluk hissederler, iş verimlilikleri artar ve iş kazaları riski azalır. Bu nedenle, ergonomi odaklı bir yaklaşım, hem çalışanların sağlığını korur hem de laboratuvarın genel verimliliğini artırır.
- İdeal bir adli bilişim laboratuvarında sağlam bir ağ yapısı, veri güvenliği, veri erişimi ve iş sürekliliği açısından kritik bir rol oynar. Güçlü bir ağ altyapısı, yüksek hızda veri transferi sağlayarak çalışmaların hızlı ve kesintisiz bir şekilde yapılmasına imkân tanır. Veri güvenliği için gereken önlemleri alarak, yetkisiz erişimlere karşı koruma sağlar ve veri bütünlüğünü korur. Ayrıca, ağ üzerindeki cihazların etkili bir şekilde yönetilmesini sağlayarak iş sürekliliğini artırır. Güvenilir ağ yapıları, veri kaybı veya ağ kesintileri gibi olumsuz durumların önüne geçer ve laboratuvarın genel performansını artırır.

5.1.1.4. Personel

Adli bilişim laboratuvarında görevli her personelin görev tanımı net bir şekilde belli olmalıdır. Personel konusunda laboratuvarın tek bir şekilde ya da daha büyük bir laboratuvarın parçası olacak şekilde konumlanması önem kazanmaktadır. Eğer laboratuvar sadece adli bilişim alanında hizmet veren bir laboratuvar ise adli bilişim prosedürleri, dosya dağıtımı, personel eğitimi gibi konuların yanı sıra binanın tüm idari işlerinden sorumlu olacak kişi laboratuvar yöneticisidir. Büyük bir laboratuvarın parçası olması halinde laboratuvar yönetiminin iş tanımı daralmakta ve daha spesifik hale gelmektedir. Çünkü onun da üstü konumunda bulunan ve tüm adli bilimler laboratuvarından sorumlu bir yönetici daha olması muhtemeldir. Adli bilişim laboratuvarında bulunması önerilen roller şu şekilde olabilir;

- Laboratuvar yöneticisi
- Bünyesinde veri, görüntü ve ses inceleme kısımları ayrı ayrı varsa bunların kısım amirleri
- Personel ve idari işler sorumlusu
- Adli bilişim uzmanı
- Adli bilişim uzman yardımcısı

- Tekniker

Laboratuvar yöneticisi laboratuvardaki en yetkili kişi olmakla beraber sorumluluğu en fazla olan kişidir. Yöneticinin inceleme kısmına yönelik teknik bilgisinin yanı sıra delillerin hukuki boyutlarını, laboratuvar yönetim süreçlerini de çok iyi bir şekilde bilmesi beklenmektedir. Tüm personelin işini düzgün bir şekilde yapmasını ve eğitimlerinin tam olmasını sağlamak yöneticinin görevleri arasında yer alır. Ayrıca personeli motive etmek, çalışma sırasında oluşabilecek kazalara karşı önlemler almak, işe alınacak personel hakkında araştırma yapmak, karar vermek ve personeli gözlemleyerek performans raporları hazırlamak da yöneticinin görevleri arasında yer alır.

Kısım amirleri kendi kısımlarındaki personelden ve yürütülen işlerden sorumlu olup bir nevi yöneticinin yardımcısı konumundadırlar.

Personel ve idari işler sorumlusu personelin özlük haklarını (maaş, izin vb.) takip etmeli ayrıca laboratuvarın idari işlerinin yürütülmesini (evrak, yazışma vb.) sağlamalıdır.

Adli bilişim uzmanı esas incelemeyi yapan kişidir. Teknik anlamda inceleme konusuna hâkim olmalı, alanıyla ilgili güncel gelişmeleri takip etmeli, dilbilgisi ve yazılı ifade yeteneği iyi olmalıdır.

Adli bilişim uzman yardımcısı nispeten tecrübesiz, inceleme işini öğrenme aşamasında olan ve uzmana yardımcı olan kişidir. Uzmanda olması gereken yeteneklerin yardımcıda da olması ve geliştirmesi beklenir.

Tekniker laboratuvar faaliyetlerinden uzmanlık gerektirmeyenleri (delil teslim alma, teslim etme, dosya açma, kapama vb.) yapabilen kişidir. Ara eleman görevinde bulunan teknikerden işlerin akışını hızlandırması ve aksaklıkları gidermesi beklenebilir.

Kullanılan cihazların bakımı ve onarımı için genellikle laboratuvar içinde ikiz görev ile görevlendirilen (uzman, uzman yardımcısı ve teknikerden oluşan) bir teknik destek ekibi bulunması uygundur. Bu ekip, cihazlara hızlı bir şekilde müdahale edilmesini sağlar ve laboratuvar personelinin ana işlerine odaklanmasına imkân tanır. Ancak bazı durumlarda, cihazların alındığı firmadan düzenli bakım ve onarım hizmeti almak da uygun olabilir. Özellikle garanti kapsamında olan cihazların bakımı ve onarımı genellikle bu firmalar tarafından yapılmaktadır.

Laboratuvara seçilecek personel açısından mezuniyeti arzu edilen lisans bölümlerinin belirtilmesi adli bilişim laboratuvarında çalışacak personel seçiminde önemli bir faktördür çünkü bu bölümler genellikle adli bilişim alanında gereken temel bilgi ve becerilerin kazanılmasını sağlar. Ancak, bu

belirtme işlemi sadece belirli bir lisans bölümünden mezun olan kişilerin değerlendirilmesi anlamına gelmemelidir. Adayların sahip oldukları deneyim, sertifikalar, proje çalışmaları ve ilgili alanlardaki çalışmaları da dikkate alınmalıdır. Bu sayede laboratuvarlar, hem lisans bölümlerinden mezun olanları hem de farklı yollarla alanlarında uzmanlaşmış kişileri değerlendirerek en uygun ve yetkin personeli seçebilirler.

Adli bilişim laboratuvarı personelinin etik açıdan, güvenilirlik açısından ve objektiflik açısından bazı prensiplere bağlı olduğu söylenebilir. Ancak, bu prensipler genellikle bir "yemin" şeklinde resmileştirilmemiştir. Bununla birlikte, adli bilişim laboratuvarları ve personeli için geçerli olan temel ilkeler ve prensipler şunlardır:

- **Etik İlkeler:** Adli bilişim laboratuvarı personeli, etik kurallara ve yasal düzenlemelere uygun davranmakla yükümlüdür. Bu, özellikle delillerin korunması, manipülasyonun önlenmesi ve kişisel verilerin gizliliğinin korunması gibi alanlarda önemlidir.

- **Güvenilirlik:** Laboratuvar personeli, adli bilişim işlemlerinde güvenilir ve doğru sonuçlar elde etmek için bilimsel yöntemlere ve standartlara uygun hareket etmelidir. Verilerin doğruluğu ve güvenilirliği, adli bilişim laboratuvarlarının itibarı için kritik öneme sahiptir.

- **Objektiflik:** Adli bilişim laboratuvarı personeli, analiz ve değerlendirmelerinde tarafsızlık ve objektiflik ilkesine uygun davranmalıdır. Kişisel önyargılardan arınarak, delilleri tarafsız bir şekilde değerlendirmek ve sonuçlara ulaşmak önemlidir.

- **Sorumluluk:** Laboratuvar personeli, yaptıkları işlerden ve verdiği kararlardan sorumludur. Bu, doğru ve eksiksiz raporlama yapmak, verileri güvenli bir şekilde saklamak ve gerektiğinde bu verilere erişim sağlamak gibi sorumlulukları içerir.

Bu ilkeler ve prensipler, adli bilişim laboratuvarlarında çalışan personelin güvenilirlik, objektiflik ve etik standartlara uygunluğunu sağlamak amacıyla önemlidir. Bu nedenle, laboratuvarlarda çalışan personelin bu ilkelere uyması ve gerektiğinde eğitim alması önemlidir. Ancak, bu prensiplerin bir yemin şeklinde resmileştirilmesi, genellikle kurumsal politika ve eğitim programları aracılığıyla gerçekleştirilir.

5.1.1.5. Laboratuvar düzeni

Kurulacak olan laboratuvar düzeni laboratuvarın büyüklüğü ile doğru orantılı olacaktır. Eğer imkânlar mevcut ise laboratuvar düzeni kurarken şu hususlara dikkat edilmelidir;

➢ Delillerin teslim alınma yeri inceleme bölümleri arasında mesafe olmalı hatta imkân var ise kat olarak farklı katlarda olmalıdır. Böylelikle ziyaretçiler inceleme alanından tamamıyla izole olacaklardır.

➢ Laboratuvar girişinde ziyaretçileri karşılayan bir resepsiyon (danışma) olmalıdır. Eğer laboratuvar büyük bir adli bilimler laboratuvarının parçası ise danışma personeli ortak olarak kullanılabilir.

➢ Laboratuvarın içinde yöneticinin ve varsa kısım amirlerinin ayrı bir odası bulunmalı, bu odalarda kritik evrak ve deliller saklanmamalıdır.

➢ Yine imkânlar doğrultusunda veri inceleme, görüntü inceleme ve ses inceleme kısımları birbirinden ayrı koridorlarda ya da katlarda bulunmalıdır. Delil teslim alma yerleri ortak olarak kullanılabilir. Delili teslim alan tekniker ilgili kısma yönlendirme yapmalıdır.

➢ Laboratuvar içindeki delillerin hem fiziksel hem de dijital ortamda olabileceği durumu düşünülerek birtakım önlemler almak önemlidir. Alınabilecek önlemlerden bazıları şunlardır;

- Fiziksel Delil Koruması:
    - Fiziksel delillerin saklandığı alanlar güvenlik kameraları ve erişim kontrol sistemleri ile korunmalıdır.
    - Yangın ve su baskını gibi risklere karşı önlemler alınmalıdır, bu nedenle laboratuvarın yangın söndürme sistemleri ve su sızıntı algılama cihazları bulunmalıdır.
    - Fiziksel deliller, sadece yetkili personel tarafından erişilebilecek şekilde kilitli dolaplarda veya güvenli saklama alanlarında tutulmalıdır.
- Dijital Delil Koruması:
    - Dijital deliller güvenlik duvarları, antivirüs yazılımları, güvenlik yamaları ve güvenli ağ yapıları kullanılarak korunmalıdır.
    - Veri yedeklemeleri düzenli olarak yapılmalı ve yedeklenen veriler güvenli bir şekilde saklanmalıdır.
    - Dijital delillerin erişimine sınırlı yetkilere sahip olunmalı ve izleme sistemleri ile bu erişimler takip edilmelidir.
- Yangın, Deprem ve Saldırılar Karşı Önlemler:
    - Laboratuvarın yangın söndürme ekipmanları ve acil durum çıkışları belirgin şekilde yerleştirilmelidir.
    - Deprem gibi doğal afetlere karşı düzenli olarak tatbikatlar yapılmalı ve güvenli tahliye yolları oluşturulmalıdır.

    - Saldırı ve siber güvenlik risklerine karşı güvenlik duvarları, güçlü şifreleme yöntemleri, güvenli ağ yapıları ve güvenlik yazılımları kullanılmalıdır.
    - Siber saldırılara karşı sürekli izleme ve güvenlik açıklarının düzenli olarak tespit edilip kapatılması sağlanmalıdır.
- Bilgi Güvenliği Yönetimi:
    - Laboratuvar, bilgi güvenliği politika ve prosedürlerine sahip olmalı ve personel bu kurallara uyum sağlamalıdır.
    - Hassas bilgilerin paylaşımı ve saklanması için kapsamlı bir bilgi güvenliği yönetim sistemi oluşturulmalıdır.
    - Bilgi güvenliği eğitimleri düzenlenmeli ve personel bilinçlendirilmelidir.

Bu önlemler, adli bilişim laboratuvarlarında hem fiziksel hem de dijital delillerin güvenliğini sağlamak için temel adımları içerir. Ancak her laboratuvarın ihtiyaçları farklı olduğundan, bu önlemler laboratuvarın özelliklerine ve risk analizine göre özelleştirilmelidir.

➢ Laboratuvara her gelen elektronik delil çalışır durumda veya hasarsız gelmeyebilir. Bu durumda inceleme kısmından başka laboratuvar içinde bir de onarım kısmı bulunabilir. Gelen delillerin incelemesine yönelik parça değişimleri, onarma işlemleri yapılarak delillerin incelenmesi sağlanabilir. Elektronik delillerin onarılması farklı bir uzmanlık gerektirdiğinden dolayı eğitim alan sabit personel görevlendirilebilir.

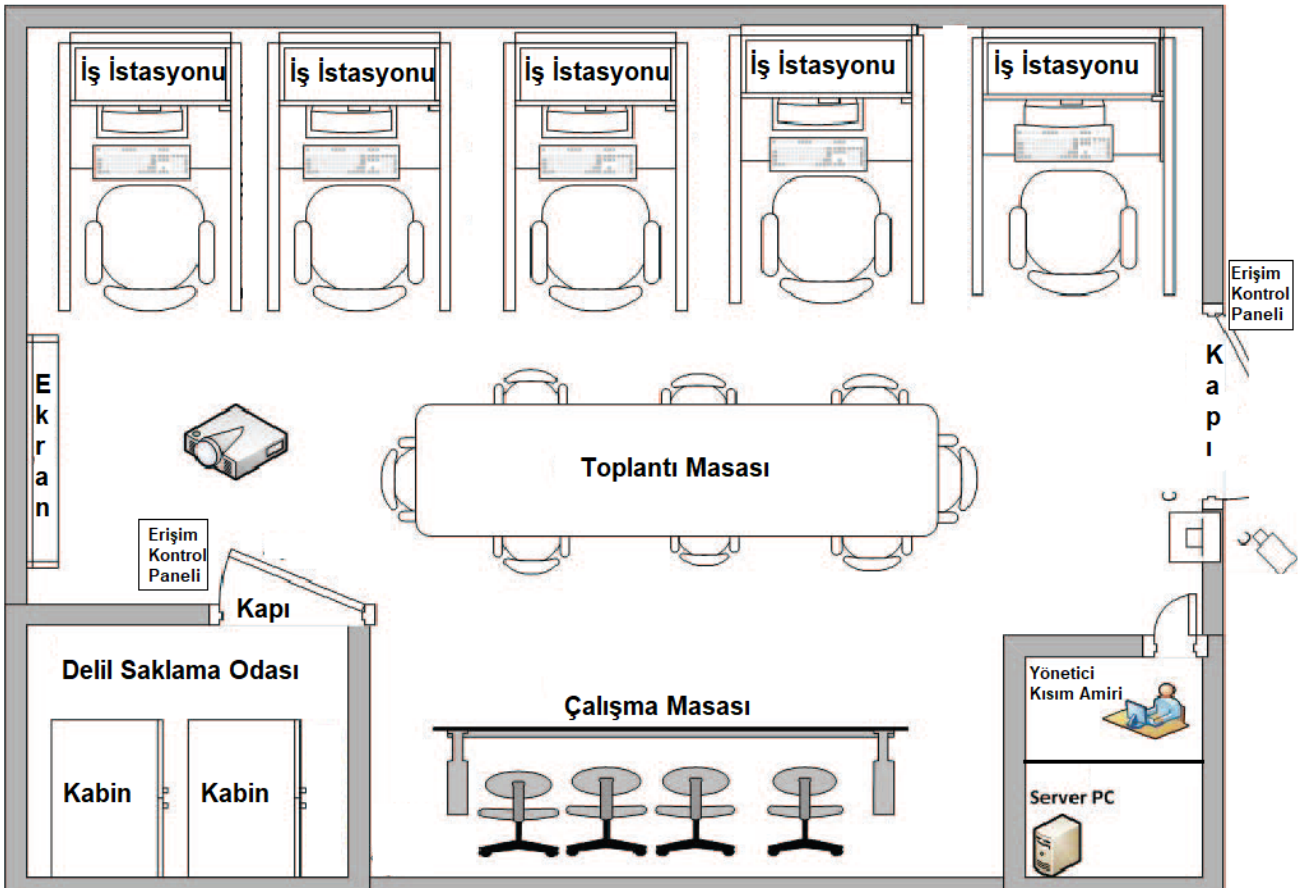
➢ Adli bilişim incelemeleri ilk başlarda bilgisayarlar üzerinden yoğun bir şekilde yapılırken günümüzde akıllı telefonlar daha yoğun bir şekilde suça konu olmaktadır. Bu nedenle bilgisayar ve telefon adli bilişimi yapan birimler iş yoğunluğuna göre ayrılmalı ve personelde bir konuda daha özel uzmanlık sağlanmalıdır.

➢ İnceleme yapılan bilgisayarlar güvenlik nedeniyle internete bağlı olmayacaklardır. Fakat bu bilgisayarlar arasında iletişim sağlanması açısından bir sunucu (server) kurularak sunucunun da ayrı bir odada muhafazası sağlanmalıdır. Ayrıca lisans güncellemeleri ve çeşitli araştırmalar yapmak maksadıyla belirli sayıda internet erişimli bilgisayarlar da laboratuvar da bulunmalıdır. Adli bilişim laboratuvarlarında, inceleme yapılan cihazlar ve internet erişimi olan cihazlar için çeşitli güvenlik önlemleri alınabilir. Bu önlemler arasında, bilgisayarlara girişte kullanıcı adı ve şifre gibi temel kimlik doğrulama yöntemlerinin yanı sıra biyometrik doğrulama yöntemlerinin kullanılması da yer alır. Ayrıca, çoklu doğrulama sistemleri (2FA veya MFA) gibi ek güvenlik katmanları da entegre edilebilir. Laboratuvar içindeki bilgisayarların güvenliği için güvenlik yazılımları, antivirüs programları, güvenlik duvarları ve zararlı yazılım tarama araçları kullanılabilir. Ağ güvenliği önlemleri de büyük

önem taşır; bu nedenle, ağ trafiğinin izlenmesi ve zararlı aktivitelerin tespiti için güvenlik yazılımları ve sanal özel ağlar (VPN) gibi teknolojiler kullanılabilir. Fiziksel güvenlik açısından, bilgisayarların erişim kontrolü ve yetkilendirilmiş personel tarafından kullanılması da sağlanabilir. Son olarak, bilgisayarların işletim sistemleri, uygulamalar ve sürücülerinin düzenli olarak güncellenmesi, güvenlik açıklarının kapatılmasına ve laboratuvarın genel güvenliğinin sağlanmasına yardımcı olur.

➢ Bir uzmana düşen iş istasyonu ve monitör sayısı yine sağlanacak bütçe ile alakalı olmakla beraber mümkünse bir uzman için iki iş istasyonu iki monitör sağlanması uzmanın daha verimli çalışmasını sağlayacaktır.

➢ Uzman personel çalışırken dosyaların gizliliği açısından laboratuvarda bir box (kutu) sistemi kurulması faydalı olacaktır. Bir sorunla karşılaşıldığında ya da ihtilaflı bir konuda tabiki uzmanlar arasında fikir alışverişi olması normaldir fakat her dosyanın kendine özgü gizliliğinden dolayı uzmanların birbirlerinin dosyalarını ve ekranlarını görmemesi dosya gizliliği açısından daha sağlıklı olacaktır. Örnek bir laboratuvar düzeni Şekil 5.1.'de sunulmuştur.



Şekil 5.1. Örnek laboratuvar düzeni

- Kullanılacak yazılım ve donanımın miktarı ve markası konusu yine bütçe ile alakalı bir durum olmakla beraber çift doğrulama yöntemi kullanılması tavsiye edildiğinden dolayı aynı işlevi gören iki yazılımın olması incelemeler açısından daha sağlıklı olacaktır. Yazılımların seçilmesi konusunda Avrupa Birliği modelinde verilen Ek-1 deki kontrol matrisi kullanılabilir.
- Adli bilişim laboratuvarlarında sinyal kesicilerin kullanımı, güvenlik gereksinimlerine ve laboratuvarın fiziksel yapısına bağlı olarak değişebilir. İki ana yaklaşım bulunmaktadır: Birincisi, laboratuvarın tamamında sinyal kesici kullanmak, tüm dış müdahale risklerini minimize eder ve laboratuvar içindeki tüm cihazların korunmasını sağlar. İkinci yaklaşım ise, sinyal kesicileri yalnızca hassas bölgelerde, örneğin mobil cihaz inceleme istasyonlarında kullanmaktır; bu da belirli alanlarda yüksek güvenlik sağlarken diğer kısımlarda normal kablosuz iletişime izin verir. Seçilecek yöntem, laboratuvarın ihtiyaçlarına ve güvenlik politikalarına göre belirlenmelidir, özellikle yüksek risk taşıyan durumlarda tüm laboratuvarın korunması tercih edilebilir.
- Laboratuvarda bir yönetim sistemi yazılımının olması gerekmektedir. Laboratuvar yönetim sistemi sayesinde delilin nereden, ne zaman geldiği, kim tarafından teslim alındığı, delile kimlerin temas ettiği, hangi uzmana atandığı, uzmanın hangi prosedürleri uyguladığı gibi konuların hepsi yetkili yönetici tarafından takip edilebilmelidir. Laboratuvar yönetim sistemi işlerin sağlıklı gittiğini teyit etmek ve kontrol sağlanması için çok önemli bir araçtır. İmkân var ise bu yazılım laboratuvar personeli tarafından da yapılabileceği gibi dışarıdan ticari yazılım paketleri de satın alınabilir. Böyle bir durumda gizlilik sözleşmesi ve kaynak kodların laboratuvar yönetiminde olması dikkat edilmesi gereken konulardandır.
- İnceleme faaliyetleri devam ederken personel eğitimi göz ardı edilmemelidir. Adli bilişimin bitmeyen bir süreç olduğu sürekli akılda tutulmalı ve personel yapılacak eğitimlerle bilgilerini sürekli bir şekilde güncel tutmalıdır.
- Son olarak kalite yönetim sistemi bir adli bilişim laboratuvarının önemli konularından birisidir. Sunulan raporun adli makamlar önünde dikkate alınması, kurumun itibarı ve en önemlisi adaletin sağlanmasına katkı sağlanırken yanlış bir uygulamanın yapılmaması açısından kalite prosedürleri belirlenmeli, görev tanım formları oluşturulmalı, laboratuvar içi ve laboratuvarlar arası doğruluk testleri periyodik olarak yapılmalıdır. Tüm bunların uluslararası kabul görmüş standartlar doğrultusunda yapılması esastır. Akredite olunması müşteriler nezdinde güven sağlamaktadır.

5.1.2. Teknik gereklilikler

Modelin bu bölümünde diğer modellerdeki başlıklar takip edilecektir. Teknik gereklilikler kısmı adli bilişim aşamalarından oluşmaktadır. Bu aşamalar aşağıdaki gibidir;

- Toplama
- İnceleme
- Analiz
- Raporlama

Laboratuvar yöneticisi ya da dosyanın atandığı uzman işin niteliğine göre belirtilen aşamaların hepsini takip etmeden de dosya inceleyebilir. Örneğin Triyaj yöntemini kullanarak zamanın önemli olduğu kritik dosyalarda inceleme süresini kısaltabilir.

5.1.2.1. Toplama

Elektronik biçimde saklanan herhangi bir verinin ve bilginin soyut doğası, geleneksel kanıt biçimlerine kıyasla bunların manipüle edilmesini çok daha kolay hale getirir ve değiştirilmeye daha yatkın hale getirir. Bu durum, delillerin bütünlüğünü sağlamak için bu tür verilerin özel bir şekilde ele alınmasını gerektiren adalet sistemi için özel zorluklar yaratmıştır.

Diğer adli delil türlerine benzer şekilde, elektronik delillerin doğru şekilde elde edilmesi ve işlenmesi davanın sonucu açısından hayati öneme sahiptir. Genel yönergelere her zaman uyulmasını sağlamak için çok dikkatli olunmalıdır. Toplama aşamasında şu genel ilkelere dikkat edilmelidir;

- **Uzmanlar tarafından ele alınması:** Her tür elektronik cihazın, doğru ve uygun prosedürlerin uygulanmasını gerektiren kendine özgü özellikleri vardır. En büyük risklerden biri delillerin kasıtsız olarak değiştirilmesidir. Onaylanmış prosedürlere uyulmaması, mahkemede veri bütünlüğü konusunda delilleri zayıflatabilecek veya geçersiz kılabilecek resmi zorluklara yol açacaktır.
- **Elektronik delil kaynaklarının hızlı gelişimi:** Yeni teknolojiler çok hızlı bir şekilde geliştiği için bunlara uygulanacak prosedür ve tekniklerin de sürekli olarak gözden geçirilmesi ve güncellenmesi gerekmektedir.
- **Uygun prosedürlerin, tekniklerin ve araçların kullanılması:** Daha geleneksel adli bilimler disiplinlerinde olduğu gibi, adli bilişim uzmanları da soruşturmalarını düzgün bir şekilde yürütmek için özel araçlara ve bilgiye ihtiyaç duyarlar. Karşılaşılan durumlar için doğru tekniklerin ve araçların kullanılması zorunludur. Elde edilen bilgilerin delil değeri taşıyabilmesi için prosedürlerin diğer uzmanlar tarafından da denetlenebilir ve tekrarlanabilir olması gerekir.
- **Kabul edilebilirlik:** Nihai amaç, tartışmalı gerçekleri kanıtlamak veya çürütmek için delil kullanmak olduğundan, elektronik delillerin, duruşmada kabul edilebilirliği sağlamak için mevcut mevzuata ve en iyi uygulamalara uygun olarak elde edilmesi gerekir.

Delillerin incelenmeye başlanmasından önce teknikerler tarafından elektronik delilin incelenmesi için gereken hukuki izinler kontrol edilmelidir. Ayrıca delil laboratuvara girdiği andan itibaren kayıt altına alınmalı ve laboratuvar yönetim sistemi vasıtasıyla gözlemlenebilir olması gerekir. Etiketleme işlemi, delilin hasar durumu ve varsa diğer ayırt edici özellikleri belirtilmeli ve kayıt altına alınmalıdır. Bu aşamada bir kontrol listesi için yine Ek-3 teki akış şeması kullanılabilir. Toplama aşaması bilgisayarlar ve mobil cihazlar için farklı prosedürler gerektirdiği için iki alt başlık altında incelenecektir.

5.1.2.1.1. Bilgisayarlar

- **Veri toplama çeşitleri:** Veri toplamanın fiziksel veri toplama ve mantıksal veri toplama olacak şekilde iki düzeyi vardır. Fiziksel veri toplama tüm ham verileri içerirken, mantıksal bir kopya genellikle bu verilerin yalnızca tahsis edilmiş bir alt kümesini içerir. Fiziksel veri edinimi, tam disk düzeyinde, bölümleme şeması, bölümlenmiş alan ve bölümlenmemiş alan dâhil olmak üzere diskte bulunan tüm verileri kopyalar. Disk düzeyinde mantıksal veri toplama yalnızca mantıksal bölümlenmiş bir alanı kopyalar. İncelemeci, silinmiş dosyaları ve ayrılmamış kümeleri içerdiğinden genellikle tüm diskin fiziksel veri toplamasını seçer. Ancak şifrelemeyle uğraşırken, şifrelenmiş verilerin fiziksel olarak edinilmesi yerine kilidi açılmış verilerin mantıksal olarak veri edinilmesi tercih edilir. Bu durumlarda, eğer adli yazılım şifrelenmiş kopyanın montajını destekliyorsa, fiziksel kopya alma yine de tavsiye edilir. Bir kopya oluşturmak için, uzmanın öncelikle delilin durumunu seçmesi gerekir. Sistem çalışır durumdaysa, incelemecinin canlı edinimi seçmesi gerekebilir. Bununla birlikte, eğer sistem kapatılırsa, incelemeyi yapan kişi kapalı edinimi gerçekleştirmeyi seçebilir. Bu toplama yöntemleri arasındaki fark Çizelge 5.1.'de açıklanmaktadır.

Çizelge 5.1. Kapalı ve canlı veri toplama yöntemleri

	Kapalı Veri Toplama	**Canlı Veri Toplama**
Nedir?	Kapalı inceleme çalışmayan bir sistem üzerinde gerçekleştirilir. Sistem kapatıldığında, RAM belleği, çalışan işlemler, önbellek veya bilgisayardaki etkin uygulama işlemleri gibi geçici depolama alanlarındaki geçici veriler artık kullanılamayacaktır.	Canlı edinim, canlı bir sistem üzerinde gerçekleştirilir. Canlı bir sistem, veriler sürekli olarak işlenirken bilgilerin değiştirilebildiği, çalışır durumda olan bir sistemdir. Canlı bir sistemde keşfedilebilecek zengin kanıt değeri nedeniyle sistemin kapatılması, bulutta depolanan veriler, şifrelenmiş veriler, çalışan işlemler, ağa bağlı ve takılı dosya

		sistemi gibi geçici verilerin kaybına neden olabilir.
Nasıl?	Kapalı sistemlerde toplama işleminin gerçekleştirilmesi süreci, normalde adli bilişim ekipmanı kullanılarak otomatik olarak yapıldığından basittir. Mümkünse donanıma bağlamadan önce sabit diskin bilgisayardan çıkarılması gerekir. Bazı durumlarda mini laptoplar ya da SSD depolamalı cihazlar kapalıyken işlem yapılamaz. Bu gibi durumlarda sistemi canlı bir CD/USB ile başlatmak gibi çıkarma işlemini gerçekleştirmek için diğer yöntemler dikkate alınmalıdır.	Bir sistemdeki veriler farklı seviyelerde volatiliteye sahiptir. Sistem kapatıldığında veya yeniden başlatıldığında bu veriler kaybolacaktır. İncelemeci canlı veri elde ettiğinde, en değişken verilerden en az değişken olanlara kadar veri toplamak mantıklı olacaktır. Tipik uçuculuk düzeyi, en çok uçucudan en aza doğru aşağıdaki gibidir: • Bellek • Swap Dosyası • Ağ Süreçleri • Sistem Süreçleri • Dosya Sistemi Bilgileri
Ne zaman?	Kapalı sistem incelemeleri sistem kapalı olduğunda ya da dosyanın kritiklik durumuna göre silinen verilerin canlı verilerden daha önemli olduğu durumlarda yapılabilir.	Canlı sistem incelemeleri sistemin kapatılması durumunda kritik bilgilerin kaybedileceği durumlarda yapılabilir.

Daha sonra uzmanın delili mi klonlayacağı ya da bir kopya dosyası mı (imaj) oluşturacağını seçmesi gerekir. Klon, verileri bir depolama ortamından diğerine parça parça kopyalar. Öte yandan imaj, verileri bir depolama ortamından bir imaj dosyasına parça parça kopyalar. Bu dosya daha sonra başka bir ortamda saklanabilir. İmaj dosyası daha sonra adli analiz için çoğu adli yazılım tarafından okunabildiğinden ikinci teknik daha yaygın olarak kullanılır. Klonlama genellikle simülasyon amacıyla kullanılır. Bunun yapılabilmesinden önce, uzmanın, delilin yalnızca okumaya olanak sağlayan ve delil üzerine herhangi bir yazmayı önleyen bir yöntem olan yazma engelleme sistemi kullandığından emin olması gerekir.

- **Yazma Engelleyici:** Yazma engelleyici, diskin verilerini değiştirmeden verilerin sabit diskten alınmasını sağlayan bir aygıttır. Aygıt okuma komutuna izin verir ancak yazma komutlarının sabit diskte yürütülmesine izin vermez. Çoğu imaj alma aracında, uzmanın bir sabit diski kopyalarken

kullanabileceği yerleşik bir yazma engelleyici bulunur. Yazma engelleme yazılım araçlarıyla ya da Windows kayıt defterindeki değişikliklerle de sağlanabilecekken, adli bilişim laboratuvarlarında donanım çözümlerinin kullanılması tavsiye edilir.

- **Kopyalama Araçları:** Bir depolama ortamının kopyalanması adli yazılım veya donanım kullanılarak gerçekleştirilebilir. Sürece yardımcı olabilecek ücretsiz ve ticari ürünler mevcuttur. Bir araç satın alırken aranacak en önemli kriter kopyayı yürütme hızı ve güvenilirliğidir. Kopyalama yazılımı aşağıdaki gibi özellikleri içerebilir:
  - Gizli alanların tanınması
  - Aynı anda birden fazla cihazın kopyalanması
  - Aynı anda birden fazla hedefe kopyalama
  - Kopyalama sıraları
  - Hash algoritmalarıyla doğrulama
  - Kopyalama sürecinin farklı aşamalarında hash doğrulaması
  - En yaygın adli kopya formatlarını destekleme
  - Şifrelenmiş ve sıkıştırılmış kopyalar üretmek
  - Kesintiye uğramış bir kopyalama sürecini yeniden başlatmak
  - Donanım hatalarına tolerans

İncelemeci her zaman adli bilişim karşıtı tekniklerin olasılığına karşı tetikte olmalıdır. Ana bilgisayar korumalı alanlar (HPA'lar) veya cihaz yapılandırma katmanı (DCO) gibi yalnızca özel ATA komutlarıyla adreslenebilen gizli alanlar, yalnızca mevcut bazı kopyalama yazılımı çözümleri tarafından algılanabilir.

- **Kopya Formatları:** Raw veya dd gibi birkaç yaygın görüntü dosyası formatı vardır. Bu formatlar, orijinal ortamdaki tüm verileri ham bir dosyada saklar. Diğer formatlar arasında EWF ve AFF gibi formatlar mevcuttur. Aşağıdaki gibi özellikler içerirler:
  - Verilerin sıkıştırılması
  - Verilerin şifrelenmesi
  - Hata kontrolleri
  - Hash toplamları
  - Kopyayı parçalara bölme

Ayrıca farklı adli yazılım çözümleri, benzer özelliklere sahip, kendi tescilli kopya formatlarıyla birlikte gelir. Bir kopya formatı seçerken her zaman çoğu adli yazılım çözümü tarafından desteklenen formatı tercih etmek faydalı olacaktır. Bazı laboratuvarlar farklı adli yazılımlar kullanır ve bunun sonucunda,

uzmanın benzersiz bir kopya dosyası formatı seçmesi durumunda kopya dosyasının açılmama ihtimali vardır.

- **İş Akışı:** Bilgisayarlarda yapılacak toplama işlemi öncelikle verinin kopyalanacağı alanın belirlenmesiyle başlar. Yüksek hacimli veriler için kopyalanacak yerin uygun seçilmesi gerekir. Daha sonra yazma engelleyiciye bağlanan delil adli bilişim yazılımıyla kopyalanabilir. Kopyalama işleminin SHA256 algoritmasıyla hash değerinin alınması sonraki işlemler için çok önemlidir. İşlemlerin çoğunu adli bilişim yazılımı otomatik olarak yapsa da wear-levelling, write-amplification gibi işlemleri uzmanın kendisinin yapması gerekebilir. Kopyalama işlemi bittikten sonra doğrulama işleminin de yapılması gerekir. Hem delilin hem de kopyanın hash değerlerinin birbirini tutması gerekmektedir. Toplama aşamasının son adımında yapılan işlemlerin belgelenmesi, uzman tarafından tutulan notlarda kullanılan araç, hash değerleri vb. bilgilerin olması gerekmektedir.

5.1.2.1.2. Mobil cihazlar

- **Veri Toplama Çeşitleri:** İncelemeci çalışmasına başlamadan önce delilden gerekli olan veri türlerini tespit etmek amacıyla talep sahibinden alınan vaka evraklarını incelemesi gerekir. Bu, incelemeyi yapan kişinin vaka için en iyi çıkarma yöntemine karar vermesine yardımcı olabilir. Çalışmayı yürütmeden önce delilin tüm şifrelerini veya modellerini (desen kilitleri vb.) toplamaya çalışılmalıdır. Örneğin manuel yöntemin kullanılması, telefonun kilidinin açılmasını gerektirir. Neredeyse tüm çıkarma yöntemleri, telefonların kilidinin açılmasını gerektirir. Bu nedenle, el koyma anında kilit açma kodunu almaya çalışmak her zaman iyi bir uygulamadır. Mobil cihazlar için, en çok verinin çıkarılabileceği seviyeden en azının çıkarılabileceği seviyeye kadar açıklanan beş farklı veri çıkarma düzeyi vardır. Kullanılan yöntem ne olursa olsun, cihazdan bilgi çıkarıldıktan sonra (SIM ve MicroSD takılıyken), SIM kartın ve Mikro SD'nin ayrı ayrı analiz edilmesi gerekir.
  - Fiziksel Kopya: Fiziksel yöntem, ham ikili verilerin cihazın medya deposundan alınmasıdır. Bu ham verilerin daha sonraki bir aşamada adli yazılım tarafından analiz edilmesi ve işlenmesi gerekir. Bu yöntem genellikle uzmanın canlı ve silinmiş verilere, işletim sistemi dosyalarına ve normalde kullanıcı tarafından erişilemeyen cihaz alanlarına erişmesine olanak tanır.
  - Dosya Sistemi Dökümü (File System Dump -FSD): Dosya Sistemi Dökümü , fiziksel çıkarma ve mantıksal çıkarmanın bir melezidir. Bu yöntemde araç, cihazın dosya sistemini alır ve işleme aşamasında verileri yorumlar. Bu, uzmanın örneğin mantıksal bir çıkarmada mevcut olmayabilen ve fiziksel bir çıkarma sırasında erişilemeyebilen silinmiş mesajları içeren veritabanlarını almasına olanak tanır. Ancak bu yöntemin bir sınırlaması, silinen tüm verileri fiziksel çıkarmanın yapabildiği şekilde geri getirmemesidir.

- Mantıksal Kopya: Mantıksal kopya, mobil cihazdan bilgi almayı ve cihazın verileri analiz için sunmasına izin vermeyi içerir. Bu genellikle cihazın kendisindeki verilere erişmeye eşdeğerdir. Çoğu mobil cihaz adli yazılımı bu tür bir özellik sunar.
- Manuel Kopyalama: Adli yazılımların bir sınırlaması, bazen belirli benzersiz mobil cihazların modellerini veya yakın zamanda piyasaya sürülen modelleri desteklememesidir. Bu durumda, uzmanın manuel yöntemi kullanması genellikle kabul edilebilir. Bu yöntem, ekranda görüntülenen verilere fotoğraf veya video ile veya verilerinin yazıya dönüştürülmesi yoluyla cihaza ve kayıtlara erişir. Android cihazlar için, uzman yazılım araçlarını kullanarak ekran görüntüleri almayı düşünebilir. Bu yöntem, telefonun geliştirici modu etkinken ADB komutu aracılığıyla bağlanmasını gerektirebilir.
- JTAG / Chip-Off / Rooting / Jail Breaking: Hasar görmüş veya şifre ile kilitlenmiş mobil cihazlarda verinin çıkarılması için JTAG ve Chip-Off yöntemleri kullanılabilir. JTAG çıkarma, cihazın mantıksal kartına kadar sökülmesini ve belirli bir kablonun kart üzerindeki belirli bir bağlantıya lehimlenmesini gerektirir. Bu yöntem yüksek teknik beceri gerektirir. Bu yöntemi kullanarak, İncelemecinin ham ikili verileri cihazın medya deposundan alabilmesi gerekir. Chip-Off ayrıca ham ikili verilerin aygıtın deposundan çıkarılmasına da olanak tanır, ancak aygıtın bellek yongasının bellek kartından kalıcı olarak çıkarılmasını gerektirir. İncelemeci Chip-Off işlemini gerçekleştirdiğinde cihaz hasar görecek ve artık kullanılamayacaktır. Yeni cihazlar şifrelenmiş verileri bellek yongalarında saklar. Android 7.0 ve sonraki sürümlerde çalışan cihazlar varsayılan olarak şifrelenir. Bazı mobil cihazlarda kullanılabilecek daha az yıkıcı bir diğer yöntem ise “Rooting” veya “Jail Breaking”dir. Bu süreç, çalışan kullanıcının izinlerini ve ayrıcalıklarını yükseltmek için işletim sisteminin özelliklerinden yararlanmayı içerir (bir Linux bilgisayarında "Kök" erişimi kazanma sürecine benzer). Bu süreç, sistem dosyalarının değiştirilmesini içerdiğinden ve cihaza zarar verme potansiyeli olduğundan, kullanılan teknikler listesinin alt sıralarında yer alır. Ayrıca delilin zarar göreceği bu yöntemleri kullanmadan önce talep makamı ile iletişime geçerek bu yöntemlerin kullanılabileceği ve delilin hasar görebileceği bildirilerek onay alınması gerekir. Alınan onay belgelenerek dosyada saklanmalıdır.

- **Kopyalama araçları ve formatları:** Mobil cihazların analizi genellikle özel bir yazılım, güç kablosu ve veri kablosunun kullanılmasını gerektirir. JTAG veya Chip-Off gibi daha gelişmiş inceleme teknikleri daha fazla araç gerektirir. Bunlar arasında lehimleme ekipmanı ve cihazın bellek yongalarından ham verileri okumaya yönelik özel aparatlar yer almaktadır. Veri çıkarmak için özel araçların kullanılması gerekliliği nedeniyle, cep telefonu verileri genellikle özel bir formatta çıkarılır. Diğer tescilli olmayan formatlar bin dosyalarını ve raw dosyalarını içerir.

- **İş Akışı:** Kopyalama işlemine başlamadan önce cihazın tanımlanması gerekmektedir. Marka, model IMEI numarası gibi özellikler belirlenerek bir etiket yapılması ve cihaza yapıştırılması faydalı olacaktır. Bu işlemin yapılması cihazın desteklendiği adli bilişim yazılımının tespiti için de önemlidir. Sonraki işlem cihazın yalıtımının yapılmasıdır. Faraday çantası ya da jamming sistemleri kullanılabilecek maliyetli yöntemler olup en pratik ve maliyetsiz yol cihazın açılır açılmaz uçak moduna alınmasıdır.

Mobil cihazlara uygulanan kopyalama yöntemlerinin özel yöntemler (Boot loader, rooting vb.) olması nedeniyle mobil cihazın yazma engelleme aracına bağlanmaması tavsiye edilir. Mobil cihazın kendisi, SIM kartı ve varsa hafıza kartı ayrı ayrı kopyalanmalıdır. Mobil cihaz ve SIM kart mobil adli bilişim yazılımları kopyalanabilirken hafıza kartının kopyalanması bilgisayar disklerininki gibi olabilir.

Kopyalama işlemi kullanılan adli bilişim yazılımına göre değişik işlemlerin yapılmasını gerektirebilir. Örneğin bazı telefonlarda telefon önceden açılıp geliştirici modunun açılması, işletim sisteminin değiştirilmesi gibi işlemlerin yapılması gerekebilir. Kullanılan adli bilişim yazılımının yönergeleri takip edilmeli ve hesap verilebilirliğin akılda tutulması gerekir.

Son olarak yedekleme dosyaları veya bulutta tutulan veriler için daha özel kopyalama ve çıkarma yöntemleri kullanılması gerekebilir.

İşlemler yapıldıktan bilgisayar kopyalamasında olduğu gibi burada da doğrulama ve belgeleme işlemleri yapılacaktır. Özellikle kopyalama sırasında cihazın tarih ve saat bilgisi ile yazılımın tarih ve saat bilgisi birbirini tutmaması dikkat edilmesi gereken konular arasındadır.

5.1.2.2. İnceleme

Mümkün olduğunca orijinal kanıtların incelenmesinden kaçınılmalıdır. İncelemeyi yapan kişi her zaman delilin adli kopyası (imaj dosyası) üzerinde çalışmalıdır. Bu kaçınılmazsa, verilere erişim bir yazma engelleyici kullanılarak korunmalıdır. Bazı durumlarda, uzmanların incelemeyi gerçekleştirmek için izole edilmiş dijital bir ortam kullanması gerekir. Bunu başarmak için, inceleme uzmanları sanallaştırma teknolojisini kullanabilir.

5.1.2.2.1.Triyaj

Triyaj, ilgilerine göre analiz süreçleri için vakaların, delillerin veya verilerin önceliklendirilmesi sürecidir. Triyajın sonucuna göre vakalar, bulgular veya veriler, en önemliden en az önemliye doğru

öncelik sırasına göre analiz edilecektir. Bazılarının araştırılan vakayla ilgisizliği nedeniyle hiç analiz edilmemesi mümkündür. Triyaj aşağıdaki gibi durumları ele almak için gerçekleştirilir;

- Çok büyük miktarda delilin veya toplu verinin kısa bir zaman diliminde analiz edilmesi gerekiyorsa,
- Yasal sorunlar nedeniyle deliller laboratuvarda artık saklanamıyorsa,
- Yüksek öncelikli bir durum mevcut ve sonuçların derhal alınması gerekiyorsa; Örnek olarak bir terör saldırısı tehdidi verilebilir.

Triyaj bazı avantajlar sunarken, ele alınması gereken dezavantajlar da vardır. Triyaj tam bir incelemenin yerini alamaz. Triyaj, otomatik işleme kullanılarak gerçekleştirilir; bu, adli bilişim yazılımı tarafından veya delillere veya verilere kişinin kendi yazdığı kodları çalıştırarak sunulur. Bu otomatik işlemenin yalnızca veri alt kümelerini incelemesi ve bazı önemli verilerin dışarıda bırakılması riski vardır. Bu riskin soruşturmacıya, savcıya veya hakime açıklanması gerekir ve bu bilgilere dayanarak söz konusu vaka için önceliklendirme sürecinin lehine veya aleyhine karar vermeleri gerekebilir. Ancak triyaj, başka türlü çözülemeyen bir durumla başa çıkmada geçerli bir yöntem olmayı sürdürmektedir.

5.1.2.2.2. Bilgisayarlar

Bir bilgisayarı incelemek için birçok yöntem ve teknik vardır. Bazıları derinlemesine beceri gerektirirken diğerleri, otomatikleştirilmiş bir süreci yürütmek gibi minimum düzeyde beceri gerektirir. Uzman tarafından çeşitli adli yazılımlar kullanılabilir. Yazılımın kapasitesine bağlı olarak, bazıları şifreleri kurtarabilir, elektronik kanıtlar arasındaki verileri ilişkilendirebilir ve anahtar kelime araması yapabilir.

- **Kapalı ve canlı sistemlerin incelenmesi:** Kapalı sistemler RAM belleğinin, ön belleğin veya çalışan sistemlerin incelenmesine olanak tanımaz. Laboratuvar ortamında en fazla yapılan incelemeler de kapalı sistemler üzerinde yapılanlardır. Bu şekilde mevcut ve silinmiş dosyalar, dosya ve disk boşlukları, işletim sistemi bilgileri, dosya üstverileri, log kayıtları, internet geçmişi, mailler ve sosyal medya kayıtları gibi veriler incelenebilmektedir.

"Canlı sistem", uygulamaların çalışıyor olabileceği ve veriler sürekli olarak işlenirken güncellenebildiği, çalışır durumda olan bir sistemdir. Canlı bir sistemde keşfedilebilecek değerli deliller nedeniyle sistemin kapatılması, bulutta depolanan veriler, şifrelenmiş veriler, çalışan işlemler, ağ bağlantıları ve takılı dosya sistemleri gibi geçici verilerin kaybına neden olabilir. Canlı bir sistem

incelenerek rasgele erişim belleği (RAM), çalışan işlemler, ağ bağlantıları, sistem ayarları, depolama ortamı, bulut hizmetleri gibi veriler elde edilebilmektedir. Durumun niteliği değerlendirilerek sayılan verilerden herhangi biri üzerinden canlı bir sistemin incelemesi yapılabilir.

- **Otomatik İşleme:** Otomatik işleme genellikle adli bilişim yazılımındaki hazır özellikler kullanılarak gerçekleştirilir. Otomatik işlemenin kapsamı genellikle inceleme yapan kişi tarafından incelemenin başlangıcında belirlenir. Bu adım, yüksek bilgi işlem gücü kullanmasına rağmen minimum denetimle gece boyunca veya hafta sonu boyunca çalışabileceğinden zamandan tasarruf sağlar. Bu kapsam, benzer bir soruşturma kapsamındaki diğer davalar için tekrarlanabilir. Otomatik işlemeye yönelik ortak faaliyetler ve sıralar şunlardır:
  - İşletim sistemi ve kullanıcı verilerinin çıkarılması,
  - ZIP, RAR gibi dosyaların ve şifrelenmiş dosyaların eklenmesi,
  - Posta kutuları ve İnternet geçmişi gibi yapay öğelerin ayıklanması ve ayrıştırılması
  - Silinen dosya ve klasörleri kurtarma
  - Silinen bölümleri kurtarma
  - Belirli dosya türlerini kazıma
  - Talebe göre anahtar kelime arama, PDF dosyalarında optik karakter tanıma (OCR), kolay görüntüleme için resimlerin küçük resimlerini oluşturma, videolardan resim çıkarma, videolar için ten rengi algılama, hash karşılaştırma gibi analiz yöntemleri kullanılabilir
  - İşletim sistemi günlüklerinin incelenmesi (Örneğin, Windows olay günlüğü)
- **Veri Kurtarma:** Veri kurtarma, depolama ortamındaki silinmiş, hasar görmüş, gizlenmiş veya kaybolmuş verilerin kurtarılmasını içerir. Bazı durumlarda depolama ortamı hasar görür, bozulur veya biçimlendirilir, bu da verilere erişilememesine neden olur. Bu nedenle veri kurtarma, verilerin ortamdan çıkarılabilmesi için depolama ortamının sabitlenmesi sürecini de içerir. Mantıksal kurtarma ve fiziksel kurtarma olacak şekilde iki tür veri kurtarma vardır. Mantıksal kurtarma, depolama ortamına erişilebildiğinde ancak veriler biçimlendirildiğinde, bozulduğunda, gizlendiğinde veya kaybolduğunda gerçekleştirilir. Kurtarma işlemi genellikle adli yazılım kullanılarak gerçekleştirilir. Fiziksel kurtarma, depolama ortamına mekanik arıza veya elektronik arıza nedeniyle erişilemediğinde gerçekleştirilir. Kurtarma süreci ileri düzeyde beceri gerektirir. Bazı durumlarda, fiziksel kurtarmanın gerçekleştirilmesi için bir onarım işlemine de ihtiyaç duyulur; örneğin, bir sabit diskteki kafanın değiştirilmesi, Diğer durumlarda verileri kurtarmak için özel ekipmanlara ihtiyaç vardır. Örneğin, bir USB flash sürücüdeki kabloyu değiştirirken bir lehimleme makinesi gereklidir. Maliyet yüksek olduğundan ve görevleri gerçekleştirmek için yüksek vasıflı bir uzmana ihtiyaç duyulduğundan, tüm laboratuvarların fiziksel kurtarma kabiliyetine sahip olma lüksü olmayabilir. Çoğu adli analiz yazılımı,

mantıksal bir kurtarma özelliğiyle birlikte gelir; böylece uzman, maliyetlerden tasarruf etmek için sunulan özellikten yararlanabilir veya bu özelliğe yükseltme yapabilir.

- **Filtreleme:** Analiz edilmeden önce bir imaj dosyasına filtrelerin uygulanması, İncelemecinin görüntülemesi ve analiz etmesi gereken veri miktarının azaltılmasına yardımcı olabilir. Popüler filtreleme teknikleri, bilinen işletim sistemlerini veya program dosyalarını filtrelemek (beyaz listeye alma) veya bilinen yasadışı materyallerin veri tabanlarındaki hash eşleşmeleri (kara listeye alma) özel olarak aramak için hash setlerini kullanır. Filtreleme, vakayla yalnızca belirli türdeki bulguların ilgili olduğu durumlarda da uygulanabilir. Dosyalar imza analiziyle (boyut, tarih, sahip ve üst verilerde bulunan daha birçok ayrıntıya göre) filtrelenebilir. Bu filtreleme özelliği çoğu ticari adli yazılımda sunulmaktadır.

5.1.2.2.3. Mobil cihazlar

Mobil cihazlar, işletim sistemlerinin çeşitliliği, sayısız marka ve model, veri bolluğu ve cihazda depolanan veri türlerinin çeşitliliği çok fazla olduğundan, uzman için benzersiz bir zorluk teşkil etmektedir.

- **Otomatik İşleme:** Mobil cihazların işlenmesi, cihazlar arasında kullanılan donanım ve yazılımların büyük ölçüde farklılık göstermesi nedeniyle genellikle bilgisayarlara göre farklı bir yaklaşım gerektirir. Uygulamalar çok daha sık güncellenir ve değişiklikler genellikle büyük olabilir. Bu nedenle, özel adli bilişim araçları verilerin çoğunu otomatik olarak işleyecektir, ancak bu işlemenin manuel olarak doğrulanması genellikle gereklidir.
- **Filtreleme:** Mobil verilerin filtrelenmesi genellikle veri türü düzeyinde gerçekleştirilir. Veriler, iletişim verileri ve medya dosyaları gibi gruplar halinde işlenirken araçlar tarafından filtrelenir. Bu gruplar daha sonra daha da bölünür; örneğin iletişim verileri çağrı kayıtlarına ve mesajlara bölünebilir. Uzmana sunulan filtreleme düzeyi, kullanılan araca bağlıdır; ancak bu filtreleme, uzmanların önemli veri türlerini hızlı bir şekilde incelemesine olanak tanır. Bunlar, şüpheliler arasında iletişim kurmaya yönelik gönderilen ve alınan SMS mesajlarını ve çağrı kayıtlarını içerebilir.

5.1.2.3. Analiz

Analiz aşamasında incelemeyi yapan kişi imajlar üzerinde elektronik kanıtlar arar. Bu çok zaman alıcı olabilir ve çeşitli dosya sistemlerinden, işletim sistemlerinden ve uygulamalardan gelen izleri yorumlamak çok fazla uzman bilgisi gerektirebilir. Analiz aşaması için gereken süre ve iş yükü üzerinde birçok farklı faktörün etkisi vardır. Bu faktörler, analiz edilecek depolama ortamının miktarını, depolama ortamının boyutunu, kullanılan dosya sistemlerinin karmaşıklığını, işletim

sisteminin kullanım düzeyini, kullanıcının karmaşıklığını, kullanılan yazılımın ve tekniklerin karmaşıklığını içerir.

5.1.2.3.1. Bilgisayarlar

- **Dijital İzler:** Bilgisayarlar üzerinde çeşitli işlemler yapılarak değiştirilebilen (tarayıcı geçmişi, günlük dosyalar, log kayıtları, sık kullanılanlar vb.) ve değiştirilmesi zor olan (boş alanlar, tahsis edilmemiş alanlar, RAM vb.) bazı dijital izler mevcuttur.

Bir bilgisayardan çıkarılması gereken veri ve bilgiler vakanın türüne bağlıdır. Örneğin dolandırıcılıkla ilgili bir vakada, bilgisayardan alınan veriler/bilgiler genellikle elektronik tablolar, e-postalar ve ofis belgeleri biçimindedir. Çocuk istismarı durumunda ilgili olası veri/bilgiler resimler, videolar ve iletişim mesajları olabilir. Çeşitli türdeki dijital kalıntıları analiz etme süreci değişik yöntemlerin kullanılmasını gerektirebilir. Analiz edilecek dosya türüne göre yapılacak işlemler EK-5'teki şablondan yararlanılarak gerçekleştirilebilir.

- **E-postalar:** Farklı posta istemcileri farklı türde yapılar üretecektir. Örneğin Outlook, kanıt niteliğindeki verileri PST, OST ve PAB dosyaları gibi kişisel klasör dosyalarında saklar. Thunderbird, mesajları gelen kutusu dosyalarında saklar. Adli yazılımlar genellikle bu dosyaları ayrıştırma yeteneğine sahiptir ancak tüm mesajları çıkarmaları şart değildir. Bazı adli yazılımlar kişisel klasör dosyalarından silinen mesajları geri getiremez, dolayısıyla bu durumda veri kurtarma yöntemine ihtiyaç duyulabilir.
- **Ofis Belgeleri:** Ofis belgelerinin analizi genellikle dosya imza analiziyle başlar ve ardından ilgilenilen dosyaların filtrelenmesi gelir. Dosya imzası analizi, eşleştiğinden emin olmak için dosya başlığını uzantısıyla karşılaştırır. Eşleşmiyorsa, belge başlığının veya uzantısının içeriği gizleyecek şekilde değiştirilme olasılığı olabilir. Dosyaları filtrelemek, anahtar kelime araması kullanmayı içerir. Çoğu adli yazılım her iki görevi de otomatik olarak gerçekleştirebilir.
- **Resimler ve videolar:** Resimler ve videolar üzerinde analiz yapmak için, incelemeyi yapan kişinin öncelikle talep eden taraftan neyi arayacağı konusunda net bir fikir edinmesi gerekir. Aynı fotoğrafların aranmasını içeriyorsa, talep eden kişinin, incelemeyi yapan kişiye gerekli fotoğrafları sağlaması gerekir. Bilinen hash değerlerine sahip dosyalar içeriyorsa, talep eden kişinin, hash değerlerini uzmana sağlaması gerekebilir veya uzman, bilinen veri tabanlarından hashların bir listesini kullanabilir. Bir videonun belirli bir bölümünü içeriyorsa, talepte bulunanın videonun benzersiz özelliklerini belirtmesi gerekir. Resimlerin analizi genellikle imza analiziyle başlar. Daha sonra, uzman küçük resim görünümünü kullanarak galerideki resimleri inceleyebilir. Vaka, bilinen bir dizi

resmin aranmasını gerektiriyorsa (örneğin bir çocuk istismarı vakasında veya çalıntı planlarda), bu görevi gerçekleştirmek için hash karşılaştırma kullanılabilir. Bazı adli yazılımlar benzer resim tespit etme özelliği sunmaktadır, Uzman bu özelliği yazılıma gerekli resmi sağlayarak kullanabilir. Video analizi için bazı yazılımlar videolardan hareketsiz resimler çıkarma özelliğini sunar. Örneğin her X saniyede/dakikada bir Y resim. Çıkarılan bu resimler daha sonra galeri görünümünde de görüntülenebilir. Bu, video dosyalarının çok daha verimli bir şekilde ön izlenmesine olanak tanır. Resimlerin ve video dosyalarının konum veya üretim ayrıntılarının önemli olduğu durumlarda, incelemeyi yapan kişi bu dosyaların üst verilerini çıkarmayı düşünmelidir. Üst veriler, örneğin resmin çekildiği GPS koordinatları, oluşturulma tarihi ve saati ile resmi yakalamak için kullanılan cihaz gibi diğer verileri tanımlayan ve bunlar hakkında bilgi veren veri kümeleridir. Bazı delillerde binlerce fotoğraf ve video bulunabilir ve uzmanın belirli bir video veya resim dosyasını tarayıp bulması imkânsızdır. Bunu yapmanın en iyi yolu tüm resimleri çıkartıp talep sahibine iletmektir. Resimlerin/videoların içeriklerini görüntülemeye yönelik basit görev, herhangi bir adli bilişim uzmanlığı gerektirmez ve bu nedenle talep sahibi tarafından gerçekleştirilebilir.

- **İnternet Tarayıcısı:** İnternet tarayıcıları web sitesi ziyaret geçmişi, yerel önbellek / geçici internet dosyaları, oturum bilgileri, çerezler, kaydedilmiş kullanıcı adları ve şifreler gibi birçok delil taşır. Tarayıcı yapılarını analiz etmek, amaç veya niyet önermek açısından önemli olabilir; Arama motorlarında kullanılan ve amacı kanıtlayabilecek anahtar kelimeler buna bir örnektir. Popüler tarayıcılar arasında Google Chrome, Microsoft Internet Explorer / Edge, Mozilla Firefox ve Apple Safari bulunur. Hepsi verileri kullanıcının ana dizininde saklar. Microsoft tarayıcıları haricinde diğer tüm tarayıcılar, yukarıda bahsedilen yapıları depolamak için SQLite veri tabanlarını kullanır. Çoğu internet analizi adli yazılımı, tarayıcı ayrıştırma olanağı sunar. Ancak gelişen teknoloji nedeniyle bazı tarayıcıların sıklıkla güncellendiği, bazı adli yazılımların veri tabanını güncellemesi biraz zaman aldığı görülmektedir. Bu nedenle, uzmanların internet tarayıcılarının temel yapısını anlaması önemlidir. Günümüzde çoğu tarayıcı SQLite veri tabanları üzerinde çalıştığından, uzmanlar, ücretsiz olarak indirilebilen SQLite veri tabanı tarayıcılarını kullanarak yapıyı manuel olarak ayrıştırmayı düşünebilir. Bu, yalnızca uzmanların belirli bir yazılımdan bağımsız olmalarına olanak sağlamakla kalmaz, aynı zamanda onlara yazılımın sonuçlarını SQLite veri tabanı tarayıcılarına göre çapraz kontrol etme olanağı tanır.
- **Yazılım:** Belirli bir yazılımın analiz edilmesi gerektiğinde, çoğu zaman bu, yazılım izlerinin çıkarılmasını ve anlaşılmasını içermelidir. Bu tür yazılımlara örnek olarak iletişim yazılımları (örn. Whatsapp ve Skype), steganografi yazılımı (örn. OpenStego), şifre kasaları (örn. KeePass), dosya paylaşım yazılımı (örn. uTorrent) ve kripto para birimi yazılımları (örn. Cryptocurrency cüzdanları) dahildir. Çeşitliliklerinden dolayı tüm yazılım izlerinin nasıl analiz edileceğine dair standart

prosedürler bulunmamakla birlikte, genellikle yazılım izleri hakkında güvenilir kaynaklardan bilgi toplanması yoluyla yapılır. Bulgular daha sonra bir simülasyon yapılarak doğrulanabilir.

- **Kullanıcı aktivitesi:** Bilgisayar işletim sistemi açma ve kapatma süreleri, en son kullanılan dosya listeleri, aygıt kullanımı, kullanıcı oturum açma işlemleri, Wi-Fi bağlantıları gibi birçok farklı kullanıcı etkinliğini izler. Bu kullanıcı etkinliğinin analiz edilmesi, kullanıcının davranışının daha iyi anlaşılmasına yardımcı olur ve hatta delil niteliğindeki etkinlikleri kanıtlayabilir. İşletim sistemine bağlı olarak izler çeşitli yerlerde depolanır. Microsoft Windows'ta, izlerin çoğu kayıt defterinde ve olay günlüklerinde depolanır. Linux sistemlerinde verilerin çoğu kullanıcının ana klasöründe veya "/etc" veya "/var" dizinlerinde depolanır.
- **Log Kayıtları:** Log dosyalarının analiz edilmesi, özellikle sistemlere yönelik saldırı durumlarında çok önemlidir. İncelemeyi yapan kişi yalnızca tahsis edilen log dosyalarını değil aynı zamanda silinmiş/ayrılmamış log dosyalarının izlerini de çıkarmalıdır. Log dosyası analizi için özel yazılım mevcuttur. Böyle bir analizin temeli, ya belirli anahtar kelimeleri, anormal kalıpları aramak ya da belirli bir zaman çerçevesine giren logları aramaktır.
- **Şifreleme:** Günümüzde en yaygın işletim sistemleri yerleşik şifreleme olanakları sunmaktadır. Kullanıcının bir sistem sürücüsü için tam disk şifrelemesini etkinleştirmesi kolaydır. Parolaların veya şifreleme anahtarlarının, delilin laboratuvara teslim edilmesinden önce canlı veri adli bilişimi kullanılarak olay yerinde toplanması tavsiye edilir. Mümkün olduğunda diskten diğer şifrelerin (örneğin, tarayıcı şifreleri) çıkarılması da yararlı olabilir. Bu şifreler ve bunların kombinasyonları, özel şifre kırma teknikleri kullanılarak bir saldırı gerçekleştirmek için veya bir sözlük oluşturmak için kullanılabilir. Ek olarak, yazılı parolalar, anahtarlar veya kurtarma dizileri de dahil olmak üzere fiziksel kanıtların toplanması gibi yöntemler kolluk kuvvetleri tarafından yürütülmelidir.
- **Tahsis Edilmemiş Alanlar:** Tahsis edilmemiş alanlar, yukarıda bahsedilen tüm kanıt türlerinden izleri içerebilir. Ayrılmamış alanlardaki belirli dosya türlerinin aranması ve çıkarılması, kazıma yazılımı kullanılarak otomatikleştirilebilir. Veri kazıma çok zaman alıcı bir iş olduğundan, uzmanın ne tür dosyalar aradığını belirtmesi gerekir. Veri kazıma, parçalanmış dosyalarda iyi çalışmaz. Ayrılmamış alanlarda bulunan veriler çoğu zaman belirli bir kullanıcıyla, zaman damgalarıyla ve hatta bir klasör yapısındaki bir konumla ilişkilendirilemez.
- **Bulut ve Uzak Depolama:** Eğer bilgisayarda bulut hizmetleri izleri bulunuyorsa verilerin bilgisayarda değil de bulut sistemlerindeki uzak sunucularda saklanması muhtemeldir. Uzakta depolanan veriler yalnızca tek bir sunucuda saklanmayabilir, buluttaki birden fazla sunucuda da saklanabilir. Çoğu zaman bulut hizmetinin sağlayıcısı bile verinin belirli bölümlerinin hangi sunucuda, veri merkezinde veya hangi ülkede depolandığını söyleyemez. Hatta uzman, bir şirketin bilgisayarlarından tek bir bayt verinin bile alınamadığı durumları bile bulabilir, çünkü bunlar yalnızca

herhangi bir depolama ortamı olmayan istemci bilgisayarlardır ve buluttaki bir sanal makinenin kaynaklarını kullanırlar. Bulutta bulunan sanal makinenin adli kopyasını çıkarmak teknik olarak kolay olsa da dikkat edilmesi gereken bazı hukuki hususlar bulunmaktadır. İlgili mevzuata bağlı olarak, bu tür verilerin ele geçirilmesi için uygun yasal yetkinin belirlenmesi ve alınması sorun teşkil edebilir. Verilerin talep eden ülkedeki yasal prosedürlere uygun olarak elde edildiğinden emin olmak da zor olabilir. Gerçekten de, eğer bir şüpheli, suçunu işlemek için geçici bir sanal makine oluşturup daha sonra bu makineyi silmişse, kurtarılacak hiçbir delil kalmayabilir. Uzaktan depolanan verilerin elde edilmesi ve analiz edilmesi olasılığı mevzuata ve yargı yetkisine bağlıdır. Örneğin bazı yargı bölgelerinde, belirli koşullar altında, incelemecinin verileri elde etmek için şüphelinin bilgisayardaki kimlik bilgilerini kullanarak uzak depolama birimine bağlanmasına izin verilir. Diğer yargı bölgeleri böyle bir erişimi kabul etmeyebilir. Bu durumlarda, sağlayıcıdan verilerin korunmasını ve verilere erişilmesini talep etmek için resmi kanallar kullanılabilir. Ülkemizde şu an için bu duruma uyarlanabilir açık bir mevzuat bulunmamaktadır. Doktrinde CMK 134. maddenin bulut adli bilişim ile bu kayıtlara erişimine izin verdiğini savunan bir takım yazarlar olduğu gibi maddenin bu işleme cevaz vermediğini savunan yazarlar da mevcuttur.

5.1.2.3.2. Mobil cihazlar

Mobil cihazlar, belirli iletişimlerin zamanları ve tarihlerinin yanı sıra iletişim kayıtlarını ve günlüklerini içerir. Buna ek olarak mobil cihazlarda medya dosyaları ve GPS konumları da bulunabilir.

- **Dijital İzler:** Mobil cihazlarda bulunan dijital izler üç farklı gruba ayrılabilir: iletişim verileri, medya dosyaları ve diğer veriler. İletişim verileri, arama kayıtlarını, SMS mesajlarını ve diğer mesajlaşma hizmeti mesajlarını içerebilir. Medya dosyaları, bilgisayarlarda olduğu gibi, dosya tarafından gösterilenin ötesinde bilgiler içerebilir. Örneğin, bir cep telefonunda yakalanan medya dosyalarındaki üst veriler büyük olasılıkla dosyanın içine gömülü coğrafi etiketler veya diğer yararlı konum ve tanımlama verilerini içerecektir.

Mobil cihazlardan arama geçmişi, kişi listesi bilgileri, mesajlar ve e-postalar, medya dosyaları (fotoğraf, video vb.), internet tarayıcı geçmişi bilgileri gibi gelen dosyanın durumuna göre değerlendirilebilecek birçok veri çıkarılabilir. Bu analizler çoğu zaman adli bilişim yazılımı tarafından otomatik olarak yapılabilir ya da uzman tarafından anahtar kelime araması yapılarak elde edilebilir.

Sohbet kayıtları tutulan çeşitli mesajlaşma uygulamalarından (Whatsapp,telegram vb.) veriler elde edilebilir. Instagram, Facebook, Twitter ve Tumblr gibi sosyal ağ hesapları, kullanıcı kimlik bilgilerini cihazın kendisinde saklar. Kimlik bilgilerinin yerel olarak saklanması sayesinde kullanıcıların bu

siteleri her ziyaret etmek istediklerinde oturum açmaları gerekmez. Bu kimlik bilgileri, şüphelinin sosyal medya hesabına erişim sağlamak ve cihazdan veri çıkarılmasını sağlamak için kullanılabildiğinden, incelemeyi yapan kişi için değerlidir. Sosyal medya hesaplarında, kişi listelerinde, kişiler ve gruplar arasındaki mesajlarda, resimlerde, videolarda, kullanıcı aktivitelerinde çok fazla veri depolanmaktadır.

Yine mobil cihazlardan takvim ve notların bilgileri, cihazın hangi ağa bağlandığı hakkındaki bilgiler, haritalar kısmından daha önce gidilen yerler gibi dosya durumuna uygun olacak şekilde veriler elde edilebilir.

5.1.2.4. Raporlama

Bu aşamada o ana kadar yapılan tüm karmaşık işlemler, alınan notlar, kritik noktalar, dosya ile bağlantısı bulunan her ayrıntı, talep makamlarının anlayacağı şekilde sadeleştirilerek ve mümkün olduğunca teknik terimlerden arındırılarak rapora aktarılır.

Vakanın karmaşıklığı nedeniyle bazen incelemeyi yapan kişinin bulguları raporda ifade etmesi zor olabilir. Animasyon, slaytlar, resimler ve canlı gösteriler gibi görsel yardımcıların ve görsel temsillerin kullanılması, anlamayı kolaylaştırmak için iyi yöntemlerdir.

Dosyanın gönderildiği makam, gönderildiği tarih, talep edilen husus, olayın kısa özeti, yapılan incelemeler, kullanılan araçlar (versiyonları dâhil), olayla bağlantısı kurulan deliller ve açıklamalar raporda bulunması gereken unsurlardandır. Örnek bir rapor şablonu için Ek-10'daki şablondan yararlanılabilir.

Mevzuatımızda raporun sadece talep makamına gönderilmesi yeterlidir. Fakat mahkeme tarafından talep edilmesi halinde raporu hazırlayan bilirkişi konumundaki uzman mahkemeye bizzat giderek hazırladığı raporu mahkemeye anlatmak zorundadır.

5.1.3. Görüntü ve ses incelemeleri

Adli bilişim, dünya genelinde genellikle dijital veri incelemeleri ile özdeşleşmiş olsa da, ülkemizde bu alana daha geniş bir perspektiften yaklaşılmaktadır. Ülkemizde adli bilişim kapsamında, dijital verilerin yanı sıra ses ve görüntü incelemeleri de önemli bir yer tutmaktadır. Bu durum, adli bilişim laboratuvarlarının kurulum ve standardizasyon süreçlerinde bu unsurların da dikkate alınmasını gerektirmektedir.

Adli bilişim laboratuvarlarının etkinliği ve güvenilirliği, kullanılan yöntemlerin ve ekipmanların kalitesine, aynı zamanda çalışan personelin uzmanlık seviyesine bağlıdır. Dolayısıyla, laboratuvarların standardizasyonu, hem veri incelemeleri hem de ses ve görüntü incelemeleri için geçerli olacak şekilde planlanmalıdır. Bu bağlamda, adli bilişim laboratuvarlarının kurulumunda sadece dijital veri analizine odaklanmak yetersiz kalacaktır. Görüntü ve ses inceleme laboratuvarlarının da detaylı bir şekilde ele alınması ve bu alanlarda gerekli altyapının oluşturulması, adli süreçlerin bütünlüğü ve doğruluğu açısından büyük önem taşımaktadır.

Görüntü inceleme laboratuvarları, suçların aydınlatılmasında ve delillerin değerlendirilmesinde kritik bir rol oynar. Güvenlik kameraları, mobil cihazlar ve diğer görsel kayıt sistemlerinden elde edilen görüntülerin analiz edilmesi, olayların netleştirilmesi ve suçluların tespit edilmesi açısından hayati önem taşır. Aynı şekilde, ses inceleme laboratuvarları da, telefon kayıtları, gizli dinlemeler ve diğer ses kayıtlarının incelenmesi suretiyle adli olayların çözümüne katkıda bulunur. Ses analizleri, kimlik tespiti, tehdit değerlendirmesi ve suçların aydınlatılması gibi birçok alanda kullanılır.

Bu nedenle, adli bilişim laboratuvarlarının kurulumu ve standardizasyonu sürecinde, görüntü ve ses inceleme laboratuvarlarının da yer alması gerekmektedir. Bu laboratuvarlar için belirli standartların oluşturulması, bu alandaki incelemelerin güvenilirliğini ve doğruluğunu artıracaktır. Bu bölümde sunulan tavsiyeler, adli bilişim laboratuvarlarının kurulumunda dikkate alınması gereken bu önemli unsurları içermektedir.

Adli bilişim kapsamında veri incelemeleri ile ilgili yönetim ve teknik gereklilikler başlıkları altında detaylı incelemeler yapıldıktan sonra, görüntü ve ses inceleme laboratuvarları için de belirli standartlar oluşturulmalıdır. Ancak, dijital delillerin alınması, saklanması ve analizi gibi temel süreçlerin laboratuvar mantığı açısından benzer olduğu göz önünde bulundurularak, bu bölümlerde daha özelleşmiş fiziksel ve teknik gerekliliklere odaklanılacaktır.

5.1.3.1. Görüntü inceleme laboratuvarı

Görüntü inceleme laboratuvarlarının verimli ve doğru bir şekilde çalışabilmesi için bazı özel düzenlemeler yapılmalıdır. Bu düzenlemeler, analizlerin kalitesini artırmak ve uzmanların işlerini daha rahat bir ortamda yapmalarını sağlamak amacıyla önemlidir. Bu laboratuvarlar için özel olarak yapılacak düzenlemeler şu şekilde olabilir;

- **Yüksek Kaliteli Monitörler:** Görüntü analizlerinde kullanılan monitörler, yüksek çözünürlükte olmalı ve renk doğruluğu yüksek olmalıdır. En az 4K (3840 x 2160 piksel) çözünürlük önerilir. 4K çözünürlük, ince detayların net bir şekilde görülmesini sağlar ve görüntü analizlerinin doğruluğunu artırır. En az 27 inç boyutunda monitörler kullanılmalıdır. Bu boyut, geniş bir çalışma alanı sağlayarak görüntülerin detaylı incelenmesini kolaylaştırır. 32 inç veya daha büyük ekranlar da tercih edilebilir. IPS (In-Plane Switching) paneller, renk doğruluğu ve geniş görüş açısı sunar, bu nedenle görüntü analizi için idealdir. VA (Vertical Alignment) paneller de iyi bir kontrast oranı sunar, ancak IPS paneller genellikle tercih edilir. Monitörler, %99 veya daha yüksek sRGB, Adobe RGB ve DCI-P3 renk gamına sahip olmalıdır. Bu, renklerin doğru ve canlı bir şekilde görüntülenmesini sağlar.16-bit renk desteği, daha fazla renk tonlaması ve geçiş sağlar, bu da görüntü analizlerinde avantajlıdır. Monitörler, fabrikadan kalibre edilmiş olarak gelmeli veya düzenli olarak kalibre edilebilmelidir. Renk kalibrasyonu, analizlerin doğruluğunu artırır. En az 300 cd/m² parlaklık ve 1000:1 kontrast oranı önerilmektedir. Yüksek parlaklık ve kontrast oranı, görüntülerin daha net ve ayrıntılı görünmesini sağlar. HDMI, DisplayPort ve USB-C gibi çeşitli bağlantı seçeneklerine sahip olmalıdır. Bu, farklı cihazlarla kolay bağlantı sağlar ve esneklik sunar. Flicker-Free (Titreşimsiz) teknoloji ve mavi ışık filtreleri, uzun süreli kullanımda göz yorgunluğunu azaltır.

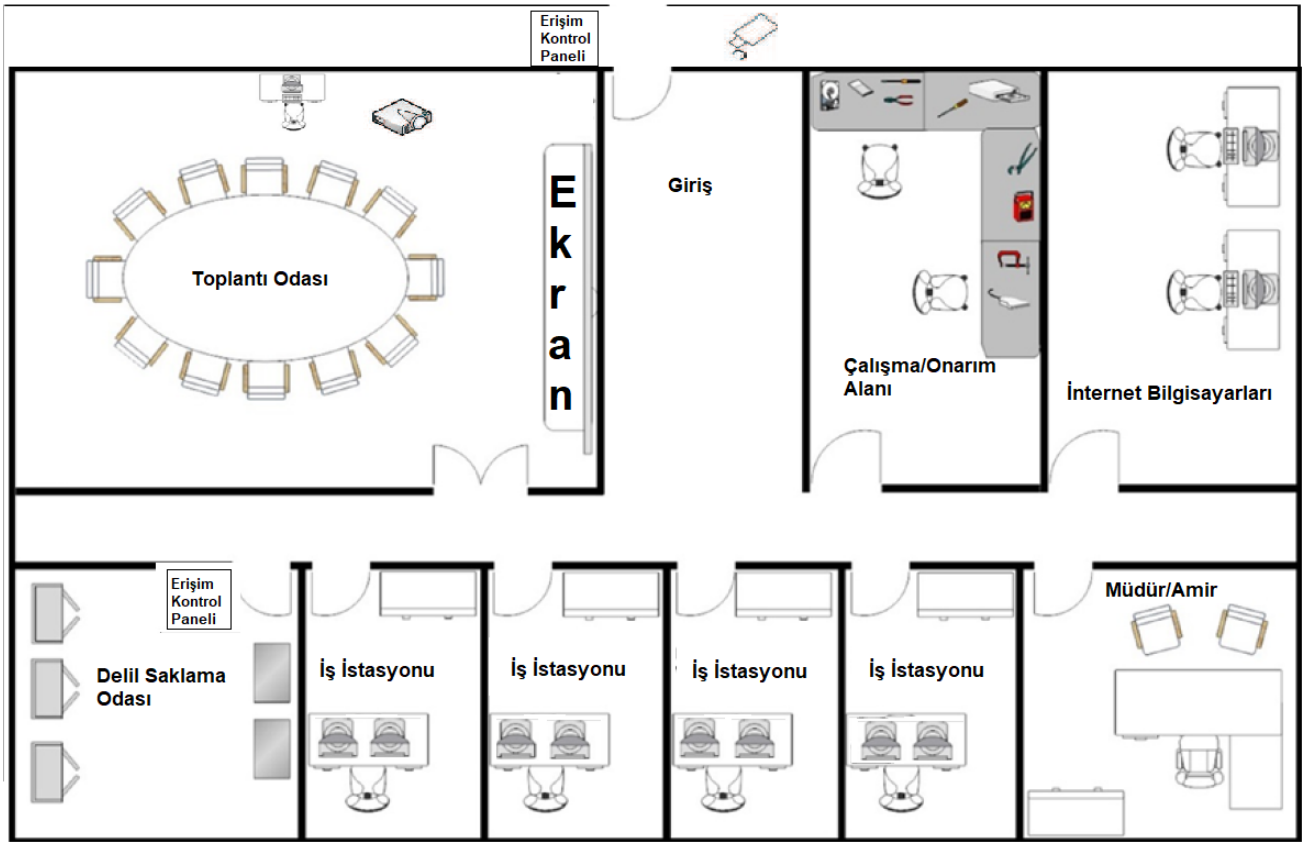
- **Işık Kontrolü:** Laboratuvarın aydınlatması kontrol edilebilir olmalıdır. Parlamaları ve yansımaları önlemek için ortam ışığı gerektiğinde karartılabilir olmalıdır. Bu, analistlerin ekranlarda görüntüleri net bir şekilde görmelerine ve analizlerini doğru yapmalarına yardımcı olur. Aydınlatma seviyesini ayarlamak için dimer anahtarları kullanılmalıdır. Bu anahtarlar, ışığın yoğunluğunu gerektiğinde artırıp azaltarak optimal aydınlatma sağlar. Karartma Perdeleri: Laboratuvar pencerelerinde karartma perdeleri kullanılmalıdır. Bu perdeler, dışarıdan gelen doğal ışığı kontrol ederek iç mekândaki ışık seviyesini ayarlamayı sağlar.Işık geçirmeyen panjurlar, dış ışığı tamamen bloke edebilir ve gerektiğinde tamamen karanlık bir ortam yaratılabilir. Aydınlatma armatürlerinin renk sıcaklığı ayarlanabilir olmalıdır. 5000K-6500K aralığında gün ışığı beyazı, görüntü analizleri için idealdir. Bu renk sıcaklığı, doğal ışığa yakın olup göz yorgunluğunu azaltır ve renklerin doğru algılanmasını sağlar. Işığın homojen dağılımını sağlamak için tavan ve duvarlara dağıtılmış ışık kaynakları kullanılmalıdır. Bu, gölgelerin ve parlak noktaların oluşmasını engeller. LED paneller, geniş alanları homojen şekilde aydınlatır ve enerji verimliliği sağlar. Ayrıca, düşük ısı yayılımı ile uzun süreli kullanımda konfor sunar. Mat yüzeyli ışık armatürleri, parlamaları azaltır ve ekranlarda

yansıma yapmaz. Monitörler için antireflektif ekran filmleri kullanılabilir. Bu filmler, yansıyan ışığı azaltarak ekranların netliğini artırır.

- **Görsel Engelleyiciler:** İş istasyonları arasında görsel engelleyiciler kullanılması, analistlerin dikkatinin dağılmasını önler ve daha odaklanmış bir çalışma ortamı sağlar. Bu engelleyiciler, analistlerin yalnızca kendi ekranlarına odaklanmalarını sağlar ve çevresel dikkat dağıtıcı unsurları en aza indirir. Şeffaf cam paneller, ortamın açık ve ferah görünmesini sağlar. Mat veya buzlu cam seçenekleri ise mahremiyeti artırır ve görsel dikkat dağınıklığını azaltır. Görsel engelleyicilerin yüksekliği, oturan bir çalışanın görüş alanını tamamen kapatacak şekilde olmalıdır. Genellikle 150 cm - 180 cm arası yükseklik ideal kabul edilir.

- **Yazıcılar:** Görüntü inceleme laboratuvarlarında kullanılacak yazıcıların, yüksek kaliteli ve doğru baskılar sağlayabilmesi için belirli özelliklere sahip olması gerekir. Mürekkep püskürtmeli yazıcılar fotoğraf ve yüksek çözünürlüklü görüntülerin baskısı için uygundur. Renk doğruluğu ve detaylar açısından mükemmel sonuçlar verir. En az 1200 dpi (Dots Per Inch) çözünürlük önerilir. Bu, baskıların net ve ayrıntılı olmasını sağlar. Standart CMYK (Cyan, Magenta, Yellow, Black) modunun ötesinde, yüksek kaliteli yazıcılarda ek renk kartuşları kullanılır. Bu kartuşlar, daha geniş bir renk gamı ve daha doğru renk reprodüksiyonu sağlar. Örneğin; CMYK + Light Cyan (LC) ve Light Magenta (LM) daha pürüzsüz ton geçişleri ve daha az grenli baskılar sağlar. CMYK + Light Gray ve Gray siyah beyaz baskılarda daha fazla tonlama ve detay sunar. CMYK + Orange ve Green daha canlı ve doğru renkler için renk gamını genişletir. CMYK + Red, Blue, ve Violet özellikle grafik ve fotoğraf baskılarında renk doğruluğunu artırır. Mat siyah ve fotoğraf siyahında mat kâğıt ve parlak kâğıtlar için ayrı siyah kartuşlar bulunur. Mat Siyah, mat yüzeyli kağıtlarda derin ve zengin siyah tonları sağlar. Fotoğraf Siyahı ise parlak ve yarı parlak kâğıtlarda daha keskin ve parlak siyahlar sunar. Profesyonel fotoğraf yazıcılarında genellikle 8, 10 veya 12 renk kartuşu bulunur. Bu, laboratuvarın yüksek kalite gereksinimlerini karşılamak için önemlidir. Yüksek parlaklık ve canlı renkler için parlak (glossy) fotoğraf kâğıdı, yansıma yapmayan ve dokulu bir yüzeye sahip mat fotoğraf kâğıdı kullanılabilir. Yarı parlak (semi-gloss veya luster) fotoğraf kâğıdı, parlak ve mat arasında bir yüzey sunar. Yüksek kaliteli fotoğraf baskıları için 200-300 GSM(Grams per Square Meter) ağırlığında kâğıtlar tercih edilmelidir. Wi-Fi ve Bluetooth özellikleri, laboratuvarda esneklik ve düzen sağlar. En az 250 sayfalık kâğıt tepsisi kapasiteli yazıcılar tercih edilmelidir. Bu, sık kâğıt değişimini önler ve iş akışını kesintisiz hale getirir. Farklı kâğıt türleri (fotoğraf kâğıdı, karton, etiket) ve boyutları (A4, A3) için çok amaçlı kâğıt

tepsileri bulunmalıdır. Dakikada en az 20-30 sayfa baskı yapabilen yazıcılar tercih edilmelidir. Otomatik duplex (Çift Taraflı) baskı özelliği, kâğıt tüketimini azaltır ve belgelerin daha düzenli olmasını sağlar. Otomatik duplex özelliği, manuel çevirme ihtiyacını ortadan kaldırır. Toner ve mürekkep kartuşlarının maliyeti düşük olmalıdır. Uzun ömürlü tonerler ve büyük kapasiteli mürekkep kartuşları, maliyetleri düşürür ve değiştirme sıklığını azaltır. Yetkisiz erişimi önlemek için güvenlik özellikleri (şifre korumalı baskı, kullanıcı kimlik doğrulaması) bulunmalıdır. Önerilen fiziksel koşulları dikkate alarak, örnek bir görüntü inceleme laboratuvarı düzeni şekil 5.2'de sunulmuştur.



Şekil 5.2. Görüntü inceleme laboratuvarı düzeni

Görüntü inceleme laboratuvarlarında teknik gereklilikler başlığı altında gerçekleştirilen çeşitli analizler ve bu analizler için kullanılan yazılımlara ilişkin hususlar incelenebilir. Görüntü iyileştirme, görüntü ve yüz karşılaştırma, video ve fotoğraf analizi için gerekli olan yazılımlar ve bu faaliyetlere dair yapılan incelemeler laboratuvarın temelini oluşturur.

Görüntü iyileştirme, görüntülerin kalitesini artırmak ve analiz edilebilir hale getirmek için uygulanan işlemleri kapsar. Bu işlemler, parlaklık ve kontrast ayarlamaları, gürültü azaltma, keskinleştirme ve renk düzeltmeleri gibi teknikleri içerir. Kullanılan yazılımlar, yüksek kaliteli algoritmalar ve filtreler

sunarak görüntülerin netliğini ve ayrıntılarını artırır. Görüntülerdeki nesnelerin tanımlanması ve hareketlerin izlenmesi yapılır. Özellikle güvenlik kameraları görüntülerinde araç plakaları, kişilerin hareketleri gibi detaylar incelenir.

Görüntü ve yüz karşılaştırma, iki veya daha fazla görüntünün karşılaştırılarak benzerliklerin ve farklılıkların belirlenmesi sürecidir. Bu işlemler, özellikle kimlik tespiti ve olay yeri incelemelerinde önemlidir. Kullanılan yazılımlar, gelişmiş yüz tanıma algoritmaları ve özellik eşleme teknikleri kullanarak yüksek doğruluk sağlar. Öncelikle görüntünün netliği, çözünürlüğü ve genel kalitesi kontrol edilir. Parlaklık, kontrast ve gürültü azaltma gibi temel iyileştirmeler uygulanır. Gözler, burun, ağız ve yüzün genel yapısı gibi belirleyici noktalar tespit edilir. Yüzün genel geometrisi, oranlar ve açılar belirlenerek yüzdeki doku ve renk özelliklerinin detaylı analizi yapılır.

Tespit edilen yüz özellikleri, eğer varsa veri tabanındaki diğer yüzlerle karşılaştırılır. Bu işlem, özellik vektörlerinin karşılaştırılması yoluyla yapılır. Elde edilen benzerlik skorları kullanılarak karşılaştırma yapılır. Yüksek benzerlik skoru, iki yüzün aynı kişi olma olasılığını artırır. Algoritmaların tespit ettiği eşleşmeler, uzmanlar tarafından manuel olarak incelenir ve doğrulanır.

Görüntü inceleme laboratuvarlarında, delillerin güvenilirliğini sağlamak için kurgu ve manipülasyon tespiti kritik bir rol oynar. İlk adım olarak, görsel inceleme yapılır. Görüntülerin genel yapısı, renk dengesi ve anormallikler gözlemlenir. Bu aşamada, gözle görülebilir değişiklikler ve tutarsızlıklar tespit edilir. Görüntünün orijinaline dair bilgi sağlamak için metadata (EXIF verileri) analiz edilir. Metadata, görüntünün ne zaman, nerede ve hangi cihazla çekildiği gibi bilgileri içerir. Görüntünün değiştirilip değiştirilmediğini doğrulamak için hash değerleri kullanılır. Orijinal hash değeri ile mevcut hash değeri karşılaştırılarak değişiklik olup olmadığı tespit edilir. Görüntülerin orijinalliğini doğrulamak için dijital imzalar kullanılır. Bu, özellikle resmi belgelerde ve sertifikalarda yaygın olarak kullanılır.

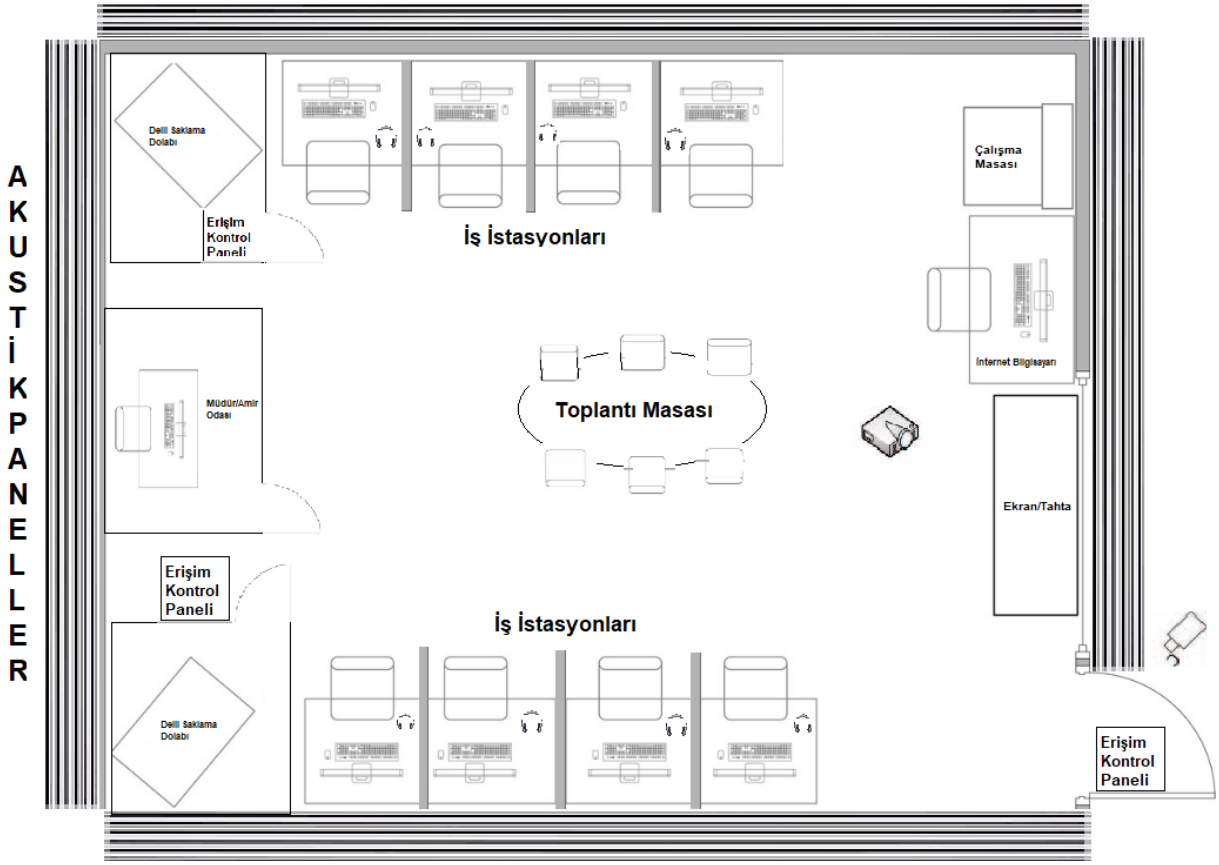
Görüntülerdeki ışık kaynaklarının yönü, gölgelerin uzunluğu ve konumları analiz edilerek tutarsızlıklar tespit edilir. Yanlış gölgeler veya ışık yönleri, manipülasyonun bir göstergesi olabilir. Piksel yapısı ve renk dağılımı incelenir. Renklerdeki ani geçişler, piksellerin uyumsuzluğu ve renk anomalileri manipülasyon belirtileri olabilir. Adli görüntü analiz yazılımları, spesifik manipülasyon tespiti için kullanılabilir. Bu yazılımlar, sahtecilik tespitinde kullanılan özel algoritmalar ve filtreler sunar. Görüntülerin geometri ve perspektif analizi yapılarak, manipülasyon belirtileri aranır. Farklı açılardan çekilen görüntüler karşılaştırılarak tutarsızlıklar tespit edilir.

5.1.3.2. Ses inceleme laboratuvarları

Ses inceleme laboratuvarlarının yüksek hassasiyet ve doğruluk gerektiren analizleri gerçekleştirebilmesi için yine görüntü incelemeleri gibi bazı özel düzenlemeler yapılmalıdır. Ses inceleme laboratuvarları için uygulanacak bu düzenlemeler, dış gürültülerin engellenmesi, ergonomik çalışma alanlarının sağlanması ve yüksek kaliteli ekipmanların kullanılmasını kapsar. Bu laboratuvarlar için özel olarak yapılacak düzenlemeler şunlar olabilir;

- **Akustik Oda:** Akustik odalar, dış seslerden tamamen izole edilmelidir. Bu izolasyon, çevresel gürültülerin analiz sürecini etkilememesi için son derece önemlidir. Oda içinde yankıyı ve eko gibi istenmeyen sesleri azaltmak için akustik paneller kullanılmalıdır. Bu paneller, sesin düzgün bir şekilde yayılmasını sağlar ve analizlerin doğruluğunu artırır. Ayrıca, laboratuvarın kapı ve pencereleri ses geçirmez olmalıdır. Bu, dışarıdan gelen seslerin oda içine sızmasını önler ve ses kayıtlarının netliğini korur. Akustik odaların duvarları ve tavanları, yüksek yoğunluklu malzemelerden yapılmalıdır. Bu malzemeler, sesin geçişini engeller ve dış gürültülerin oda içine sızmasını önler. Ses yalıtımını artırmak için duvarlar çift katmanlı yapılabilir. İki duvar katmanı arasında boşluk bırakılarak sesin yayılması engellenir. Akustik panellerin yüzeyi, ses dalgalarını emerek yankıyı minimize eden özel kaplamalarla kaplanmalıdır. Eğer pencere kullanılıyorsa, çift veya üç katmanlı ses yalıtımlı camlar tercih edilmelidir. Bu camlar, dış seslerin oda içine sızmasını önler. Zeminde kullanılan malzemeler, titreşimi önleyici özellikte olmalıdır. Halı veya özel akustik zemin kaplamaları bu amaçla kullanılabilir. Akustik odanın havalandırma ve klima sistemleri sessiz çalışmalıdır. Bu sistemler, ses yalıtımını bozmayacak şekilde tasarlanmalıdır. Odanın köşelerine yerleştirilen basstrap'ler (düşük frekans emiciler), düşük frekanslı ses dalgalarını emer ve oda akustiğini iyileştirir. Bu, daha dengeli bir ses ortamı sağlar.
- **Yüksek Kaliteli Donanım:** Yapılan incelemelerde yüksek kaliteli kulaklıklar, mikrofonlar ve ses kartları kullanılmalıdır. Kulaklıklar geniş bir frekans yanıtına sahip olmalıdır (örneğin, 20 Hz - 20 kHz). Bu, tüm ses frekanslarının doğru ve net bir şekilde duyulmasını sağlar. Kulaklıkların ses bozulması (THD-Total Harmonic Distortion) düşük olmalıdır. Bu, temiz ve doğru bir ses reprodüksiyonu sağlar. Dış gürültülerin minimuma indirilmesi için kapalı arka tasarıma sahip kulaklıklar tercih edilmelidir. Bu, analistlerin dış etkenlerden etkilenmeden odaklanmasını sağlar. Mikrofonların hassasiyeti yüksek olmalıdır. Bu, düşük ses seviyelerinin bile net bir şekilde kaydedilmesini sağlar. Mikrofonların kendi gürültü seviyeleri düşük olmalıdır. Bu, kayıt sırasında oluşabilecek istenmeyen parazitlerin önlenmesine yardımcı olur. Ses kartları, düşük gecikme süresine sahip olmalıdır. Bu, gerçek zamanlı ses işleme ve

analizlerde kritik öneme sahiptir. Yüksek çözünürlüklü ses kartları, en az 24-bit/96 kHz örnekleme hızına sahip olmalıdır. Bu, ses kayıtlarının ve analizlerinin yüksek doğrulukla yapılmasını sağlar. Ses kartlarının geniş bir dinamik aralığı olmalıdır. Bu, yüksek ve düşük ses seviyelerinin doğru bir şekilde kaydedilmesini sağlar. Önerilen fiziksel koşulları dikkate alarak, örnek bir ses inceleme laboratuvarı düzeni Şekil 5.3'te sunulmuştur.



Şekil 5.3. Ses inceleme laboratuvarı düzeni

Ses inceleme laboratuvarlarında teknik gereklilikler başlığı altında gerçekleştirilen çeşitli analizler ve bu analizler için kullanılan yazılımlara ilişkin hususlar incelenebilir. Gürültü azaltma, ses ve konuşmacı tanıma, ses karşılaştırma, kurgu ve manipülasyon incelemeleri laboratuvarda yapılan temel incelemelerdir.

Gürültü Azaltma ses kaydındaki istenmeyen arka plan gürültülerin özel yazılımlar kullanılarak temizlenmesidir. Gürültü azaltma algoritmaları ve filtreleri kullanan ses işleme yazılımları, gürültü profili oluşturur ve bu profile göre gürültüyü azaltır.

Ses ve konuşmacı tanıma incelemesinde konuşmacı tanıma ve ses kimlik doğrulama özelliklerine sahip yazılımlar ile sesin kimliği doğrulanır ve konuşmacının kimliği belirlenir. Sesin belirli özelliklerini

çıkaran algoritmalar kullanılır. Bu özellikler arasında formant frekansları, temel frekans (pitch), harmonik yapı ve spektral özellikler bulunur. Konuşma tanıma algoritmaları, ses örneklerini eğer varsa veri tabanındaki kayıtlarla karşılaştırarak kimlik tespiti yapar.

Ses karşılaştırma incelemesinde iki veya daha fazla ses kaydının karşılaştırılması yapılır. Frekans Analizi ses kaydının frekans bileşenleri analiz edilerek karakteristik özellikler belirlenir. Spektral analiz ve frekans analiz araçları sunan yazılımlar ile ses kaydının frekans bileşenleri detaylı bir şekilde incelenir, böylece sesin karakteristik özellikleri belirlenir ve analiz edilir. Bu yazılımlar, Fourier dönüşümü gibi matematiksel teknikler kullanarak ses sinyalinin frekans bileşenlerini ayrıştırır ve görselleştirir. Böylece, sesin spektrum analizi yapılabilir, harmonik bileşenler ve diğer frekans özellikleri ortaya çıkarılarak detaylı bir inceleme gerçekleştirilir.Bu süreçte, ses özelliklerinin eşleşme derecesi değerlendirilir ve benzerlik skoru hesaplanır. Elde edilen benzerlik skorları, belirli bir eşik değerine göre değerlendirilir. Yüksek skorlar, ses kayıtlarının aynı kişiye ait olma olasılığını artırır.

Benzerlik analizinin doğruluğu ve hassasiyeti, kullanılan algoritmaların performansına bağlıdır. Algoritmaların tespit ettiği eşleşmeler, uzmanlar tarafından manuel olarak incelenir ve doğrulanır. Bu, otomatik sistemlerin doğruluğunu ve güvenilirliğini artırır.

Kurgu ve manipülasyon tespitinde ses kaydının orijinal olup olmadığını ve herhangi bir manipülasyona uğrayıp uğramadığını tespit etmek için analizler yapılır. Bu, sesin doğal olup olmadığı, kesme, ekleme veya diğer manipülasyon teknikleri kullanılarak değiştirilip değiştirilmediğinin kontrol edilmesiyle gerçekleştirilir. İlk adım olarak, ses kaydının dalga formu ve spektral analizi görsel olarak incelenir. Görüntüdeki anormallikler, kesintiler veya ani değişiklikler manipülasyonun göstergesi olabilir. Ses dosyasının metadata bilgileri incelenir. Dosya oluşturma ve değiştirme tarihleri, kullanılan yazılım bilgileri gibi veriler kontrol edilerek dosyanın orijinal olup olmadığı değerlendirilir. Ses dosyasının hash değeri hesaplanır ve bu değer orijinal hash değeri ile karşılaştırılır. Değerlerin uyumsuz olması, dosyada değişiklik yapıldığını gösterir. Ses kayıtlarının dijital imzaları kontrol edilerek, imzanın geçerliliği ve dosyanın bütünlüğü doğrulanır. Ses sinyalinin frekans bileşenleri analiz edilir. Ani frekans değişiklikleri veya olağandışı harmonik bileşenler manipülasyonun belirtileri olabilir. Sesin zaman-frekans yapısı incelenir. Normalde sürekli olan bir spektrogramda ani değişiklikler veya kesintiler manipülasyonun göstergesi olabilir. Ses sinyalinin faz ve amplitüd bileşenleri incelenir. Tutarsız faz kaymaları veya amplitüd değişiklikleri, kesme veya ekleme işlemlerini gösterebilir. Arka plan gürültüsünün analizi, farklı gürültü profillerinin varlığı manipülasyonu gösterebilir. Doğal bir kayıtta gürültü profili genellikle tutarlı olur.

Günümüzde her ne kadar teknoloji ilerlemiş de olsa eski tip deliller de laboratuvara gelebilmektedir. Manuel ses cihazlarından, örneğin teyp kasetlerden elde edilen deliller öncelikle dijital formata dönüştürülür. Bu süreçte, kayıtların kalitesini korumak ve herhangi bir bilgi kaybını önlemek amacıyla en yüksek kalitede dijitalleştirme yapılır. Dijitalleştirilen kayıtlar, ses kalitesi, gürültü seviyesi ve genel durum açısından ön analizden geçirilir ve gerekli temizleme ve filtreleme işlemleri belirlenir. Ardından, gürültü azaltma, frekans analizi ve filtreleme gibi teknikler kullanılarak ses kaydının kalitesi iyileştirilir. Ses kayıtlarında iyileştirme yaparken dikkat edilmesi gereken nokta, delildeki temel karakteristik özelliklerinin bozulmamasıdır. Bu nedenle, iyileştirme işlemleri sırasında orijinal kaydın bütünlüğünü korumak esastır.

6. SONUÇ VE ÖNERİLER

Teknolojinin hızla gelişmesi, teknolojik yöntemler kullanılarak işlenen suçların artmasına ya da bu yöntemlerin suç mahallinde bulunmasına neden olmuştur. Ancak dijital delillerin doğası gereği, dijital delillerin kirlenmesi veya manipülasyona uğrama olasılığı yüksektir. Dijital deliller, adli bilişim laboratuvarında özel ekipman ve yazılım kullanılarak incelenebilir ve analiz edilebilir, ancak delilin değerinin güvence altına alınması için süreçlerin standartlaştırılması gerekir. Adli bilişim laboratuvarları, bir uluslararası standardın benimsenmesi yoluyla laboratuvarın kalitesini ve yeterliliğini kontrol etmeyi amaçlamalıdır. Adli bilişim laboratuvarlarının kurulmasında belirli bir standart bulunmamaktadır. Araştırmacılar literatürde belirli bir adli bilişim laboratuvarı standardının bulunmadığından bahsetmişlerdir, ancak yıllar geçmesine rağmen bu eksiklik aynı şekilde kalmıştır.

ISO/IEC 17025, test ve kalibrasyon laboratuvarlarının yeterliliği için genel bir standart olarak alınmış, ancak dijital delillere ilişkili belirli risk düzeylerine uygunsuz bir şekilde uygulanmıştır. ISO/IEC 17025 standardı gereksinimlere uyacak şekilde ayarlanmadan ve risk unsurlarını (başarısız noktaları) kapsam dışında bırakmadan bir adli bilişim laboratuvarını akredite etmek üzere uyarlanmıştır. Yeni bir adli bilişim laboratuvarı standardının oluşturulması, adli bilişim topluluğunu harekete geçirmek ve motive etmek için yoğun bir çaba gerektirmektedir.

Araştırma sonucunda, adli bilişim laboratuvarları için kullanılabilecek rehber niteliğindeki modeller ortaya konarak modeller içindeki en iyi örnekler alınıp standart olabilecek bir taslak önerisi sunulmuştur.

Adli bilişim laboratuvarlarının taslak standardın gerekliliklerine uyması, organizasyonel değişikliklere ve yönetim maliyetinin değişmesine neden olacaktır. Sonuç olarak, yöneticiler mecbur kalmadıkça bu maliyetlerden kaçınma eğilimindedir. Araştırmacıya göre laboratuvarları böyle bir değişime yatırım yapmaya teşvik edecek iki senaryo vardır. Birincisi, uyumun kanunen zorunlu olması ve incelenen delilin uygun olmayan bir laboratuvarda gerçekleştirilmesi durumunda mahkemede hiçbir delilin kabul edilmemesidir. İkincisi, avukatlar incelenen dijital delillere ve bunların bütünlüğüne itiraz etmeye teşvik edildiğinde, yapılan uygulamaların daha standart bir hale getirilmesine neden olabilirler.

Adli bilişim laboratuvarlarının gereksinimlerinin kapsanma düzeyi çalışma sırasında karşılaşılan zorluklardan bir tanesidir. Tüm adli bilişim alt alanlarının daha fazla ayrıntıya sahip olması ortaya konacak standart açısından maliyet yükseltici bir faktör olarak karşımıza çıkmaktadır. Ayrıca standart

her laboratuvar tarafından uygulanabilir olması açısından da birtakım zorlukları beraberinde getirmektedir.

Adli bilişim laboratuvarlarının karşılaştığı teknolojik zorluklar, teknoloji kapasitesinin hızla büyümesine uyum sağlamayı gerektirmektedir. Bulut çözümlerine her zaman izin verilmemesi ile birlikte laboratuvarlar ekipman, yazılım, donanım, değişim süreçleri ve prosedürlerine yatırım yapmak zorunda kalmaktadır. Bu nedenle sürekli değişiklikler, süreçlerinin bir parçası olarak dinamiklerini iyileştirmek için tasarlanmış bir kalite yönetim sistemi gerektirecektir. Teknolojinin yönetimi dijital delilleri ve tüm laboratuvar operasyonunu etkilemektedir. Örneğin, bugün incelemenin güvenli laboratuvarda yapılması gerekirken, ileride bir gün laboratuvarların bulutta çalışması gerekebilir, bu da kalite ve yeterlilik süreç ve prosedürleri dâhil olmak üzere tüm işleyiş modelini değiştirecektir. Operasyondaki ani değişiklikler dikkate alınmalıdır. Örneğin, 2020 yılı başlarında ortaya çıkan ve COVİD-19 olarak bilinen koronavirüs salgını, herkesin internet üzerinden faaliyet göstermek zorunda olduğu iş modellerinde değişiklikleri zorunlu kıldı. Gelecekte benzer bir olayın daha uzun bir süre boyunca meydana gelmesi durumunda, adli bilişim laboratuvarlarının sanallaştırılmış adli süreçleri değiştirmesi ve kullanması gerekecektir. Bu nedenle, gelecekteki araştırmalarda adli bilişim laboratuvarının işleyişini değiştirmedeki esnekliğin dikkate alınması tavsiye edilmektedir. Bu araştırmada varılan sonuçlardan bir tanesi de operasyonunun teknik boyutunun sürekli olarak iyileştirilmesi temel amacı ile adli bilişim laboratuvarı bünyesinde bir araştırma merkezi kurulması yönündedir. Bu, duyarlı bir sistem tasarlamayı amaçlayan araştırmalarla gelecekteki zorluklara uyum sağlamanın öneminin bir göstergesidir.

Adli bilişim laboratuvarları, bir ülkeden diğerine tutarlı bir çalışma modeline sahiptir. Bu nedenle laboratuvarların yerel yasalara ve kültürel beklentilere göre özelleştirilmesi konusunda daha fazla araştırma yapılması gerekmektedir. Bu, tek bir kuruluştan veya tek bir ülkeden yapılan değerlendirmenin tüm gereklilikleri karşılamaya yetmediği durumlarda birden fazla kapsamı içerecektir. Örneğin, üniversite laboratuvarları, kolluk laboratuvarları ve özel sektöre ait laboratuvarlar gibi birden fazla laboratuvar türü vardır. Bu laboratuvarların her türünün gereksinimleri farklı olacaktır; bu nedenle gelecekteki araştırmalarda gereksinimlerin farklı türdeki laboratuvarlardan daha özellikli bir şekilde belirlenmesi tavsiye edilmektedir.

Ayrıca, sürekli değişen mevzuatın laboratuvarlar üzerindeki olumsuz etkilerini azaltmak, daha fazla araştırma gerektiren önemli bir zorluktur. Dijital dönüşümün olgunluk düzeyine ulaştığı yaygın olarak bilinmektedir ve bilgisayar teknolojisindeki hızlı büyüme, işletmelerin temel yapısını dönüştürmektedir. Bu durum, dünya genelinde siber suçların sayısında bir artışa yol açmakta ve bu

artış, adli bilişim laboratuvarlarının ele alması gereken vaka sayısında da bir artışa neden olmaktadır. Bu problem için araştırmacıların vakaların yaşam döngüsünü hızlandıracak yöntemleri araştırmaları ve sonuçta kalite garantisi ile hedeflenen hıza ulaşmaları teşvik edilmektedir. Bu öneriler, adli bilişim ekosistemin iyileştirilmesi ve adli bilişim laboratuvarları tarafından sunulan delil incelemesinin kalitesini doğrudan ve dolaylı olarak olumlu yönde etkilemek için yapılmıştır.

Kurum veya bireyler tarafından bir adli bilişim laboratuvarı kurulurken dikkate alınması gereken bazı temel faktörler vardır. İlk olarak, laboratuvarın konumlandırılacağı mekan ve altyapı, adli bilişim faaliyetlerini destekleyecek şekilde uygun büyüklükte ve güvenlikte olmalıdır. İklimlendirme, elektrik ve veri altyapısı gibi unsurlar, laboratuvarın temel ihtiyaçları arasındadır. İkinci olarak, çeşitli adli bilişim incelemelerini desteklemek için gerekli olan donanım ve yazılım araçlarına yatırım yapılmalıdır. Bu araçlar, veri kurtarma, ağ analizi ve dijital medya incelemesi için gereklidir. Üçüncü olarak, laboratuvar personelinin sürekli eğitim alması ve uluslararası kabul görmüş sertifikasyon programlarından sertifika sahibi olmaları önemlidir. Dördüncü olarak, laboratuvarın etkin bir şekilde çalışabilmesi için standart işlem prosedürleri (SOP'ler) ve güvenlik politikaları geliştirilmelidir. Bu prosedürler, dijital kanıtların toplanması, saklanması ve analiz edilmesi süreçlerini düzenlemelidir. Son olarak, laboratuvar faaliyetleri, yerel ve uluslararası yasalara uygun olarak şekillendirilmelidir ki bu, elde edilen dijital kanıtların mahkemede kabul edilebilirliğini artırır. Bu faktörlerin hepsi, bir adli bilişim laboratuvarının başarılı bir şekilde kurulması ve işletilmesi için hayati öneme sahiptir.

Literatür taraması sonucunda adli bilişim laboratuvarı kurulumu ile ilgili uluslararası bir standart bulunamamıştır. Bu konuda örnek modellerde de verildiği üzere saygın kurumların yayınladıkları rehberler mevcuttur. Ayrıca adli bilişim standartları olarak delilin toplanmasından mahkemeye gönderilmesine kadar olan süreçleri vurgulayan ve 27000 ailesi olarak adlandırılan bir dizi standart mevcuttur. Kalite yönetimi konusunda da yine uluslararası bir standart olan ISO 9001 standardından faydalanılabilir. Akreditasyon aşamasında zorunlu tutulan standart ise ISO/IEC 17025 standardı olarak karşımıza çıkmaktadır. Standartlaşma çalışmaları adli bilişim noktasında süreç bazlı ilerlemiş olup tek bir standardın bütün bir süreci kapsaması mümkün olmamaktadır; dolayısıyla, çeşitli standartlar farklı aşamalar ve gereksinimler için geliştirilmiştir.

Bu araştırmanın bilime iki önemli katkısı olmuştur. Öncelikle adli bilişim laboratuvarların standardizasyonuna yönelik teorik çerçeve değerlendirilmiş ve kapsam açısından eksik bulunmuştur. İkinci olarak, adli bilişim laboratuvarlarına ilişkin örnek modellerden yararlanılarak uygulamaya yönelik bir taslak model yazılmıştır. Son olarak bu çalışma, tartışmaya yönelik bir girdi ve yeni bir

çalışma öğesinin temeli olarak adli bilişim incelemelerini standartlaştıran ISO çalışma grubuna taşınabilir.

Ayrıca, adli bilişim ekosisteminin iyileştirilmesinin adli bilişim laboratuvarındaki kanıt incelemesinin kalitesini doğrudan ve dolaylı olarak etkileyeceği gelecekteki araştırmalar için çeşitli önerilerde bulunulmuştur.

KAYNAKLAR

Aguilar, J., Barnes, T., Browne, J., Burney, Y., Byrd, J., Carver, B., Williams, S. (2013). *Forensic science laboratories: handbook for facility planning, design, construction, and relocation*, NIST(7941).

Başlar, Y. (2015). *Ceza yargılamasında elektronik delil*. Yayımlanmamış Doktora Tezi, Sakarya Üniversitesi Sosyal Bilimler Ensititüsü, Sakarya.

Boehm, B. W. (1984). Verifying and validating software requirements and design specifications. *IEEE software*, 1(1), 75-88.

Buchholz, F., & Spafford, E. (2004). On the role of file system metadata in digital forensics. *Digital Investigation*, 1(4), 298-309.

Busing, M. E., Null, J. D., & Forcht, K. A. (2005). Computer forensics: The modern crime fighting tool. *Journal of Computer Information Systems*, 46(2), 115-119.

Çakır, H., & Kılıç, M. S. (2013). Bilişim suçlarına ilişkin delil elde etme yöntemlerine genel bir bakış. *Polis Bilimleri Dergisi*, 15(3), 23-44.

DATE, D. (2013). ISO/IEC JTC 1/SC 27 Information technology-Security techniques Secretariat: DIN, Germany.

Değirmenci, O. (2014). *Ceza muhakemesinde sayısal (dijital) delil*. Seçkin Yayıncılık, Ankara.

Duman, E. (2012). *Bilgisayarda ve bilgisayar ağlarında delil toplama ve Türkiye'deki uygulama sorunları*, Proje Ödevi, Hacettepe Üniversitesi, Ankara.

Gözüşirin, M. (2011). *5237 sayılı Türk Ceza Kanununda bilişim suçları ve bilişim suçları ile mücadeleye ilişkin model önerisi*. Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara.

Grobler, M. (2012). The need for digital evidence standardisation. *International Journal of Digital Crime and Forensics (IJDCF)*, 4(2), 1-12.

Guo, H., & Hou, J. (2018). Review of the accreditation of digital forensics in China. *Forensic Sciences Research*, 3(3), 194-201.

Hatto, P. (2013). *Standards and standardisation: A practical guide for researchers*. Luxembourg: European Commission, Publications Office of the European Union.

Henkoğlu, T. (2014). *Adli bilişim-dijital delillerin elde edilmesi ve analizi*, İstanbul, Pusula Yayıncılık.

Hibbard, E. (2014). *Electronic discovery standardization*. Ave Maria L. Rev., 12, 313.

Hykš, O., & Koliš, K. (2014). Development of the Digital Forensic Laboratory Management System Using ISO 9001 and ISO/IEC 17025. *IDIMT–Interdisciplinary Information Management Talks. Linz: Trauner Verlag*, 87-94.

İnternet: Adli Tıp Kurumu (2024). Organizasyon Şeması. URL: https://www.atk.gov.tr/organizasyon-semasi.html, Son Erişim Tarihi: 03.01.2024.

İnternet: ASTM (2024). Detailed Overview. URL: https://www.astm.org/about/overview/detailed-overview.html, Son Erişim tarihi: 04.03.2024.

İnternet: COE (2017). Digital Forensics A Basic Guide For The Management And Procedures Of A Digital Forensics Laboratory. URL: https://rm.coe.int/glacy-dfl-guide-version-aug-2017-v8/16809ebf68, Son Erişim Tarihi: 25.02.2024.

İnternet: COE (2024). Cybercrime Programme Office (C-PROC). URL: https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc- (Erişim Tarihi:25.02.2024)

İnternet: COE (2024). Global Action on Cybercrime (GLACY). URL: https://www.coe.int/en/web/cybercrime/glacy, Son Erişim Tarihi: 25.02.2024.

İnternet: COE (2024). Who we are. URL: https://www.coe.int/en/web/about-us/who-we-are, Son Erişim Tarihi: 25.02.2024.

İnternet: Competency or management systems based standards? Frequently asked questions (2016). URL: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/casco-faq.pdf, Son Erişim Tarihi: 07.11.2023.

İnternet: IACIS (2024). The International Association Of Computer İnvestigative Specialists. URL: https://www.iacis.com/, Son Erişim Tarihi: 03.01.2024.

İnternet: International Laboratory Accreditation Cooperation (ILAC), About ILAC, (2023). URL: https://ilac.org/about-ilac/, Son Erişim Tarihi: 07.11.2023.

İnternet: International Organization for Standardization (ISO), Certification, (2023). URL: https://www.iso.org/certification.html, Son Erişim Tarihi: 07.11.2023.

İnternet: International Organization for Standardization (ISO), What is CASCO? (2023). URL: https://www.iso.org/casco.html, Son Erişim Tarihi: 07.11.2023.

İnternet: Interpol (2019). Global Guidelines For Digital Forensic Laboratories. URL: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics, Son Erişim Tarihi: 27.02.2024.

İnternet: Interpol (2024). INTERPOL Innovation Centre. URL: https://www.interpol.int/How-we-work/Innovation/INTERPOL-Innovation-Centre, Son Erişim Tarihi: 27.02.2024.

İnternet: Interpol (2024). What is INTERPOL? URL: https://www.interpol.int/Who-we-are/What-is-INTERPOL, Son Erişim Tarihi: 27.02.2024.

İnternet: ISO/IEC 14001:2015, Environmental management systems , Requirements with guidance for use (2015). URL: https://www.iso.org/obp/ui/#iso:std:iso:14001:ed-3:v1:en., Son Erişim Tarihi:: 07.11.2023.

İnternet: ISO/IEC 15189:2022 Medical laboratories, Requirements for quality and competence (2022). URL: https://www.iso.org/standard/56115.html, Son Erişim Tarihi: 07.11.2023.

İnternet: ISO/IEC 17011:2017 Conformity assessment — General requirements for bodies providing assessment and accreditation of conformity assessment bodies and supplementary requirements documents (2017). URL: https://www.iso.org/standard/29332.html, Son Erişim Tarihi: 07.11.2023.

İnternet: ISO/IEC 17020:2012 Conformity Assessment, Requirements for the Operation of Various Types of Bodies Performing Inspection (2017). URL: https://www.iso.org/standard/52994.html., Son Erişim Tarihi: 07.11.2023.

İnternet: ISO/IEC 17025:2017 General Requirements for the Competence of Testing and Calibration Laboratories (2017). URL: https://www.iso.org/standard/66912.html, Son Erişim Tarihi: 07.11.2023.

İnternet: ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories (2023). URL: https://www.iso.org/standard/66912.html, Son Erişim Tarihi: 08.11.2023.

İnternet: ISO/IEC 9001:2015 Quality management systems, Requirements (2021). URL: https://www.iso.org/standard/62085.html., Son Erişim Tarihi: 07.11.2023.

İnternet: Jandarma Kriminal Başkanlığı (2024). Başkanlık Tanıtım Kataloğu. URL: https://www.jandarma.gov.tr/kurumlar/jandarma.gov.tr/Jandarma/Kriminal-Tanitim-KATALOG-020623.pdf, Son Erişim Tarihi: 03.01.2024.

İnternet: Kriminal Daire Başkanlığı (2024). Kriminal Polis Müdürlükleri. URL: https://www.egm.gov.tr/kriminal, Son Erişim Tarihi: 03.01.2024.

İnternet: NIST (2024). About NIST. URL: https://www.nist.gov/about-nist, Son Erişim Tarihi: 23.11.2023.

İnternet: NW3C (2024). Live Courses. URL: https://www.nw3c.org/UI/about/maps/live-courses-2022.html, Son Erişim Tarihi: 03.01.2024.

İnternet: SWGDE (2018). Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis Version: 2.0 (November 20, 2018). URL: https://www.swgde.org/documents/published-complete-listing, Son Erişim Tarihi: 16.11.2023.

İnternet: SWGDE (2024). Member Organizations. URL: https://www.swgde.org/who-we-are/member-organizations, Son Erişim Tarihi: 03.01.2024.

İnternet: TDK (2024). Sözlük. URL: https://sozluk.gov.tr/, Son Erişim Tarihi: 03.01.2024.

Karadeniz, Y. (2022). Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi ve Türk Hukuku'nda karşılığı. *Güvenlik Bilimleri Dergisi*, 11(1), 109-134.

Kaya, M.B. (2019). *Hukuki açıdan bilişim suçları, siber güvenlik ve adli bilişim*, Şeref Sağıroğlu/Mustafa Şenol (ed.), Siber güvenlik ve savunma problemler ve çözümler (213-279), BGD Siber Güvenlik ve Savunma Kitap Serisi 2, Grafiker Yayınları, Ankara,

Keser Berber, L. (2004). *Adli bilişim*, Yetkin Yayınları, Ankara.

Kleiman, D. (2011). The official CHFI study guide (exam 312-49): for computer hacking forensic investigator.

Klipper, S. (2011). Information Security Risk Management. ISO/IEC, 27001, 27005. S99-S107

Koenig, B. E., Lacey, D. S., & Herold, N. (2003). Equipping the modern audio-video forensic laboratory. *Forensic Science Communications*, 5(2).

Kuchta, K. J. (2002). Forensic methodologies: A computer forensic professional's compass!. *Inf. Secur. J. A Glob. Perspect.*, 10(6), 42-49.

Lyle, J. R., Ayers, R. P., Lyle, J. R., & White, D. (2008). Digital forensics at the national institute of standards and technology. US Department of Commerce, National Institute of Standards and Technology (NISTIR 7490).

Lyle, J. R., Guttman, B., Butler, J., Sauerwein, K., Reed, C., & Lloyd, C. (2022). Digital investigation techniques: a NIST scientific foundation review (NISTIR 8354).

Marshall, A. M., & Paige, R. (2018). Requirements in digital forensics method definition: Observations from a UK study. *Digital Investigation*, 27, 23-29.

Moore, R. (2013). The role of computer forensics in criminal investigations. *Crime Online*, 91-104.

Mukasey, M. B., Sedgwick, J. L., & Hagy, D. W. (2008). US Department of Justice, Office of Justice Programs, National Institute of Justice. *Electronic Crime Scene Investigation: A Guide for First Responders*, Second edition. Wahington.

Olsson, J., & Boldt, M. (2009). Computer forensic timeline visualization tool. digital investigation, 6, S78-S87.

Orta, M. (2015). *Bilişim suçları ve elektronik delillerin toplanması, muhafazası, değerlendirilmesi, sunulması:(Adli Bilişim).* Yetkin Yayınları, Ankara.

Riillo, C. A. (2013). Profiles and motivations of standardization players. *International Journal of IT Standards and Standardization Research (IJITSR)*, 11(2), 17-33.

Sansurooah, K. (2006). Taxonomy of computer forensics methodologies and procedures for digital evidence seizure. *Australian Digital Forensics Conference*, 32.

Seo, D. (2013). Analysis of various structures of standards setting organizations (SSOs) that impact tension among members. *International Journal of IT Standards and Standardization Research (IJITSR)*, 11(2), 46-60.

Sommer, P. (2018). Accrediting digital forensics: what are the choices?. *Digital Investigation*, 25, 116-120.

Sonntag, M. (2013). Evidence collection for critical infrastructure. *IDIMT-2013: Information Technology Human Values, Innovation and Economy*, 23-30.

Stephenson, P. (2002). End-to-end digital forensics. *Computer Fraud & Security*, 2002(9), 17-19.

Şengül, G., Atsan, F. K., & Bostan, A. (2014). Adli Bilişim Alanındaki Mevcut Problemler, Çözüm Önerileri ve Gelecek Öngörüleri. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*, 17-18.

Tantra, R. (2016). Nanomaterial characterization: An introduction. John Wiley & Sons, 13-17.

TS EN ISO/IEC 27043 (2021). Bilgi teknolojisi - Güvenlik teknikleri - İhlal Olayı inceleme ilkeleri ve süreçleri (ISO/IEC 27043:2015).

Veber, J., & Klíma, T. (2014). Influence of Standards ISO 27000 Family on Digital Evidence Analysis. *Proceedings of the 22nd Interdisciplinary Information Management Talks*, 103-114.

Watson, D., & Jones, A. (2019). Digital forensics processing and procedures: Meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements.

Wilson-Wilde, L. (2018). The international development of forensic science standards—a review. *Forensic Science International*, 288, 1-9.

Yalçın, N., & Kılıç, B. (2019). Digital Evidences According to ISO/IEC 27035-2, ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042 and ISO/IEC 27043 Standarts. *SETSCI-Conference Proceedings* 4, 444-449.

Yetim, S. (2008). Dijital kanıt araştırma yöntemleri. *İstanbul Barosu Dergisi*, 82(3).

EKLER

EK-1. Adli yazılım karşılaştırma matrisi

Bölüm 1'deki tüm ekipler şablonlardır ve laboratuvar yöneticilerinin yazılım, donanım ve eğitim satın alımları konusunda bilinçli bir karar verebilmeleri için kendi karşılaştırma matrislerini geliştirmelerine yardımcı olmaktır. Bazı tablolarda daha iyi anlayışmalı için örnek veriler verilmiştir. Her adli laboratuvarın kendi oksullar, talepleri ve hatta yasal çerçevesi (örneğin, mahkeme tarafından onaylanmış yazılımların zorunlu listesi) olabileceğini anlamak önemlidir. Bir laboratuvarda dosyaların ve dosya sistemlerinin kurtarılmasıyla ilgili vakaların çözülünürken, başka bir laboratuvarda yalnızca büyük miktarlarda belge ve e-postanın analiz edilmesinin gerekebileceği vakalar bulunabilir. İlk laboratuvar kendi gereksinimlerine uygun belirli bir adli bilişim yazılımını (mükemmel veri işleme, dosya sistemi deteği ve kurtarma yetenekleri) seçerken, diğer laboratuvarlar kendi taleplerine daha iyi uyan başka bir çözümü hedefleyebilir. Tüm adli bilişim laboratuvarları için evrensel en iyi çözüm olan belirli bir yazılım için kesin bir öneri olamaz.

Lütfen her bir yazılım sonuçlarının iki kez kontrol edilmesi gerektiğini unutmayın. İdeal durum, hem verilerin manuel olarak analiz edilmesiyle sonuçların iki kez kontrol edilmesidir. Verilere ve incelemeyi yapan kişinin bilgisine bağlı olarak bu her durumda mümkün olmayabilir. Bu durumda, ilk aracın sonuçları ikinci aracın sonuçlarına göre kontrol edilmedir. Hatta bazı mevzuatlar yasal olarak ikili araç doğrulamasını zorunlu kılmaktadır. Bu nedenle, sonuçların çapraz kontrolünü sağlamak amacıyla bir adli bilişim laboratuvarında birden fazla adli bilişim yazılımının bulunması iyi bir uygulamadır.

1) Adli bilişim laboratuvarları için mevcut yazılımlar

Adli Bilişim laboratuvarını çalıştırmak için çeşitli farklı yazılımlara ihtiyaç vardır. Buna vaka yönetimi yazılımlarının yanı sıra bilgisayar ve mobil adli bilişime yönelik özelliklerle dolu paketler de dahildir. Laboratuvarın görevlerine bağlı olarak ek özel yazılımlar gerekebilir. Adli inceleme yazılımlarının sayısı çok büyük ve çok çeşitlidir.. Özellikle akı kaynak topluluğu neredeyse her gün yeni araçlar yayınlamaktadır. Bu kılavuzun amacı mevcut tüm araçların tam listesini sunmak değildir.

Ek-1 Şekil 1.1. Adli yazılım karşılaştırma matrisi açıklamalar

EK-1 (Devam) Adli yazılım karşılaştırma matrisi

2) Adli analiz için standart yazılımın maliyetine genel bakış

Unutmayın: Yazılım, donanım ve eğitime ilişkin tüm maliyetler tekrarlanan harcamalardır. Bir adli yazılımın ilk satın alınması genellikle tek seferlik bir maliyet olsa da, yıllık lisans yenilemelerinin tekrar eden maliyetleri asla unutulmamalıdır. Lisans güncellemeleri ve hizmet aboneliklerinin fiyatları ürüne bağlı olarak önemli ölçüde farklılık gösterebileceğinden, bu maliyetlere dikkat etmek önemlidir. Bunun yanı sıra, delil işleme performansını en üst düzeye çıkarmak ve güncel adli yazılım gereksinimlerini karşılamak için donanımın düzenli olarak yenilenmesi gerekmektedir. Buna ek olarak, adli bilişim uzmanlarının sürekli mesleki eğitime ihtiyaç duyması nedeniyle eğitim maliyetlerinin tekrarlandığı göz önünde bulundurulmalıdır.

Ürün	Firma	Kategori	Yazılım Maliyeti	Donanım Maliyeti	Eğitim Maliyeti
Ürün A		Örnek: Adli Analiz Mobil Adli Bilişim Uzman için İnternet Tarayıcı Vaka Yönetimi	Fiyat: EUR Lisans Güncelleme: EUR/Yıl	Gereksinimler: İşletim Sistemi CPU RAM GPU DİSK Donanım Maliyeti: EUR	Seçilen Eğitim Eğitim EUR/Gün/Kişi Seyahat EUR/Gün/Kişi
Ürün B			Fiyat: EUR Lisans Güncelleme: EUR/Yıl	Gereksinimler: İşletim Sistemi CPU RAM GPU DİSK Donanım Maliyeti: EUR	Seçilen Eğitim Eğitim EUR/Gün/Kişi Seyahat EUR/Gün/Kişi
Ürün C			Fiyat: EUR Lisans Güncelleme: EUR/Yıl	Gereksinimler: İşletim Sistemi CPU RAM GPU DİSK Donanım Maliyeti: EUR	Seçilen Eğitim Eğitim EUR/Gün/Kişi Seyahat EUR/Gün/Kişi
Ürün D			Fiyat: EUR Lisans Güncelleme: EUR/Yıl	Gereksinimler: İşletim Sistemi CPU RAM GPU DİSK Donanım Maliyeti: EUR	Seçilen Eğitim Eğitim EUR/Gün/Kişi Seyahat EUR/Gün/Kişi

Ek-1 Şekil 1.2. Standart adli bilişim yazılımı maliyet formu

EK-1 (Devam) Adli yazılım karşılaştırma matrisi

	Ürün A	Ürün C	Ürün B	Ürün D
İmza Analizi	Örnek +++	+	++	+++
Hash Karşılaştırması				
Kazıma				
Kopyalama				
Dosyaların Yüklenmesi				
Dosya Sistemi Desteği				
Bölüm (Partition) Kurtarma				
RAID Kurtarma				
Şife Kırma				
Kullanışlılık				
İndeksleme				
E-Mail Analizi				
İnternet İzleri (Browser, Messenger)				
Resimlerin Gösterilmesi				
Dosya İçeriklerinin Ham Hali				
İşaretleme/Etiketleme				
Raporlama				
Uzman Analiz Desteği				
Zaman Çizelgesi Oluşturma				
Kategorize Etme				
Filtre				
Görüntülerin Yüklenmesi				
Esneklik				
Kolay Kurulum				
Ten Rengi Tespiti				
Dosya Arşivleme				
Destek/Güncelleme				
Sürdürülebilirlik				

Ek-1 Şekil 1.3. Adli bilişim yazılımı fonksiyon karşılaştırma matrisi

EK-1(Devam) Adli yazılım karşılaştırma matrisi

Ürün	Eğitim Seçeneği	Kişi Başı Maliyet	Artı / Eksileri
Ürün A, B, C, D	Firma eğitimi	Eğitim: Seyahat:	+ Resmi eğitim sertifikası
	Firma eğitimi (laboratuvarda)	Eğitim:	+ Resmi eğitim sertifikası
	Eğitim lisansı	Lisans: Eğitim:	+ Resmi eğitim sertifikası + Belirli sayıda personel için sınırsız eğitim +yoğun kullanımda uygun maliyet
	Kendi personeli tarafından eğitim	Eğitim:	+ En ucuz seçenek + Eğiticinin kendi personelinin ihtiyacını bilmesi +Resmi eğitim sertifikası yok +Eğiticinin ürünü çok iyi bilmesi gerekir

Ek-1 Şekil 1.4. Eğitim maliyetleri içerik örneği

EK-2 Örnek cihaz taşıma çantası içeriği

Örnek Cihaz Taşıma Çantası İçeriği:

1. İki disk çoğaltıcı.
2. Bir disk çoğaltıcı USB protokol modülü
3. Bir IDE – SATA yazmaya karşı koruma köprüsü
4. Bir adet USB Ultra yazmaya karşı koruma köprüsü
5. Bir adet SCSI Ultra yazmaya karşı koruma köprüsü
6. Bir adet SAS Ultra yazmaya karşı koruma köprüsü
7. Dört adet 3,5 inçlik sabit disk
8. Disk çoğaltıcılar için iki güç kaynağı
9. Dört adet yazmaya karşı korumalı köprü güç kaynağı
10. IDE, SATA, SCSI, USB, firewire veri kabloları ve adaptörleri

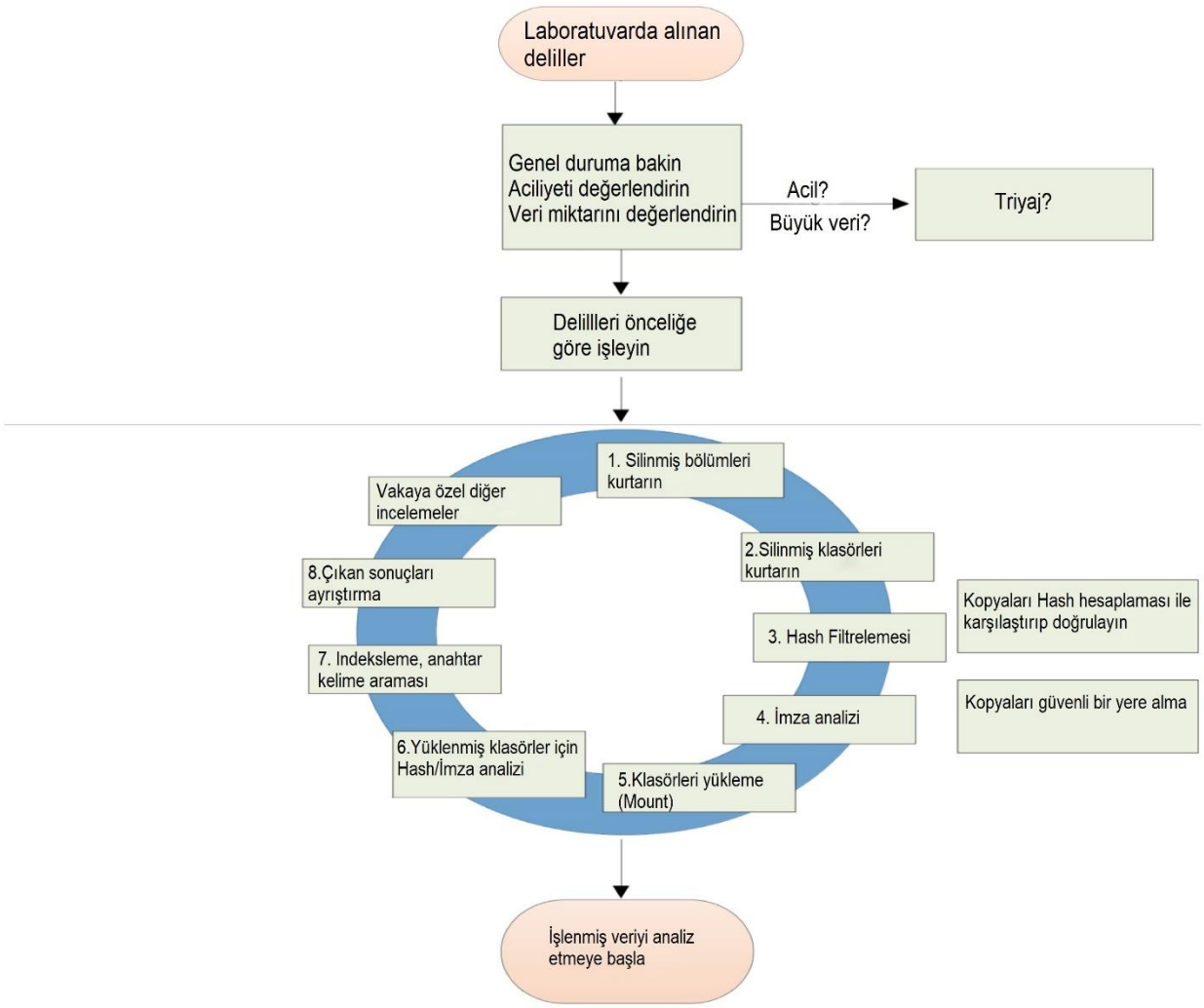
Ek-2 Şekil 2.1. Saha görevi için örnek çanta modeli

EK-3. Toplama (edinim) süreci akış şeması

Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe

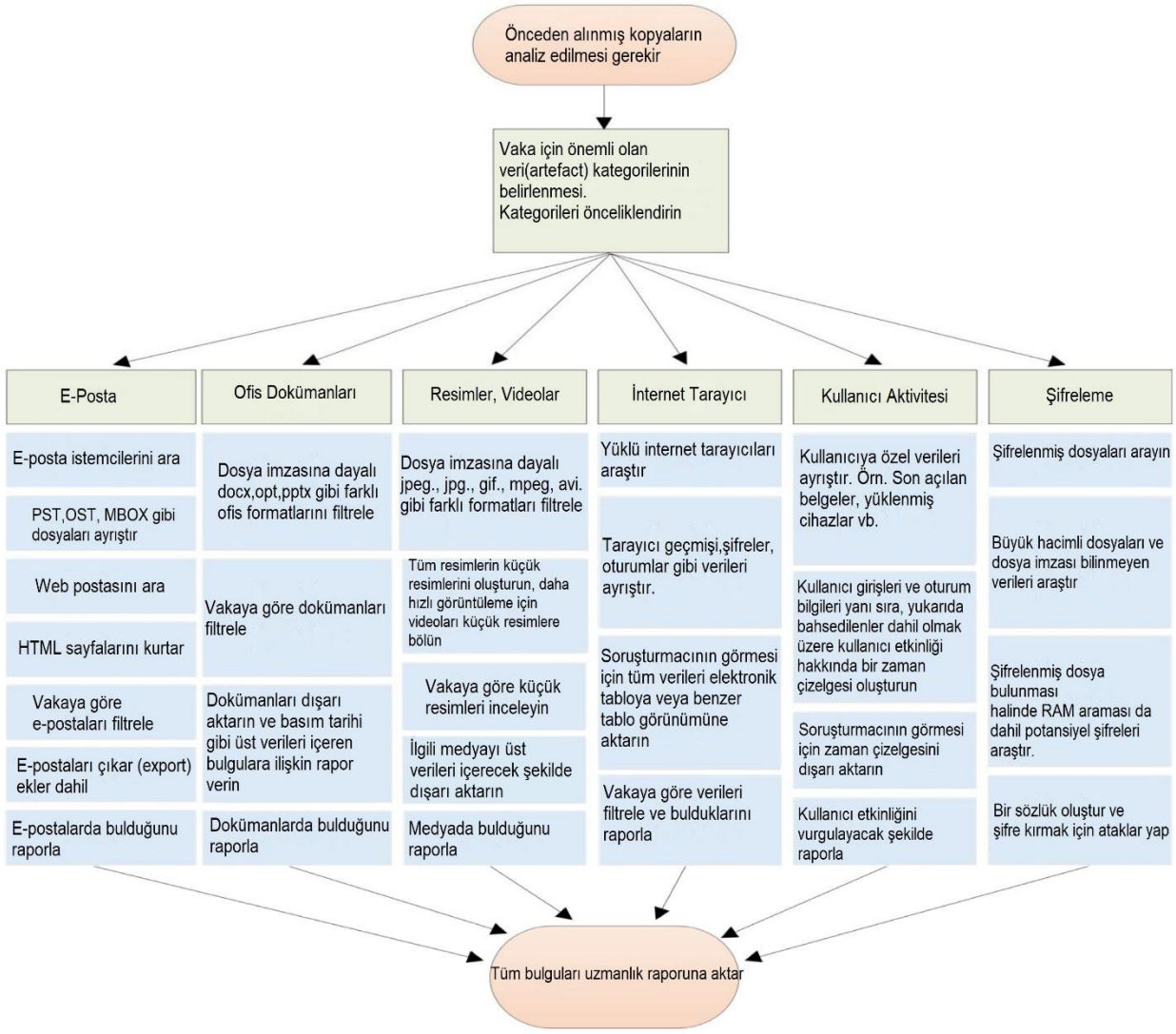
Ek-3 Şekil 3.1. Toplama (edinim) süreci akış şeması

EK-4. İnceleme (işleme) akış şeması



Ek-4 Şekil 4.1. İnceleme (işleme) akış şeması

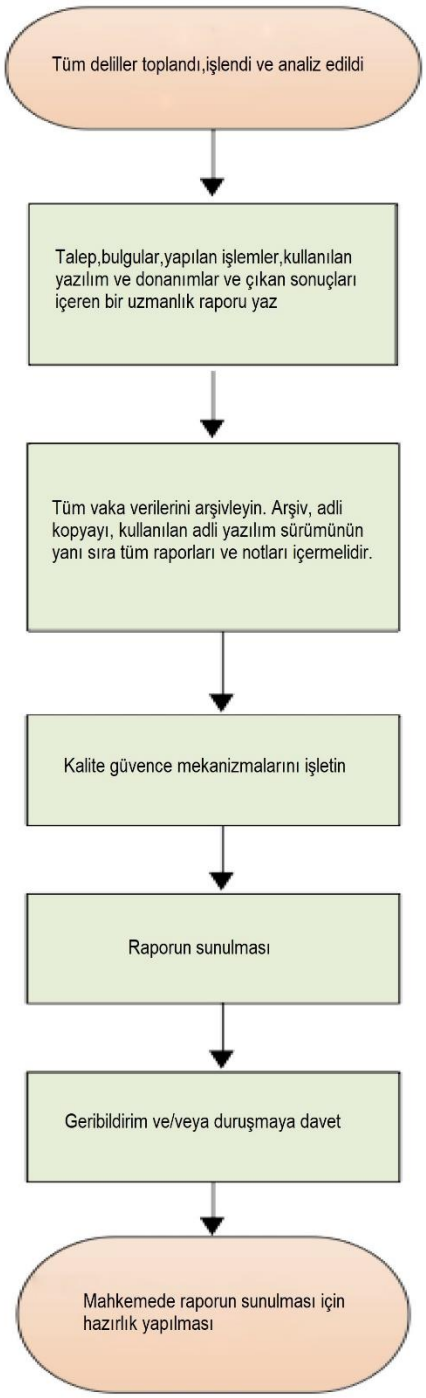
EK-5. Analiz akış şeması



Ek-5 Şekil 5.1. Analiz akış şeması

EK-6. Sunum(raporlama) akış şeması

Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe



Ek-6 Şekil 6.1. Sunum(raporlama) akış şeması

EK-7. Gözetim zinciri kaydı

DELİL İŞLEM TALİMATLARI

Ele geçirilen her eşyaya, olay yerinde doldurulması gereken bir kanıt etiketi yapıştırılır.
Bir eşyayı ilk alan kişi o eşyaya delil referans numarası vererek delil haline getirmelidir.
Bu delil referans numaraları benzersiz olmalı ve kişinin adının ve adının baş harflerinden ve ardından 1'den başlayan bir sıra numarasından oluşmalıdır; örneğin, Ayşe Başar'ın ilk delili AB/1 olacaktır.
Delile müdahalede bulunan veya delili taşıyan her kişi delil etiketini imzalamalıdır.
Her bir delilin, daha sonra o ürüne müdahalede bulunan tüm kişiler tarafından kullanılması gereken benzersiz bir referans numarası olmalıdır.
Bir soruşturmacının, olay yerinde el konulan eşyanın mahkemede gösterilen eşyayla aynı olduğunu göstermesi gerekecektir. Bu nedenle bir eşyanın başka bir kişiye teslim edilmesi veya emanet edilmesi durumunda bu tür işlemlerin tam olarak belgelenmesi çok önemlidir.
Delil haline gelen bir ürünü alan herhangi bir kişi, ilgili delil etiketini imzalamalı, dolayısıyla gözetim zincirini korumalıdır.
Daha sonraki bir raporda veya açıklamada bir delilden söz eden herhangi bir kişi, delilin referans numarasını eklemelidir.
Aynı öğeler aynı zamanda ve yerde bulunursa, bunlar aynı delil referans numarası altında gruplandırılabilir, ancak gruplandırılmış öğelerin (örneğin otuz dört (34) CD) doğru şekilde sayıldığından emin olmak için dikkatli olunmalıdır.

BULGULARA DAİR SORU-CEVAP

Delillerle ilgili tüm soru ve cevaplar eş zamanlı olarak kayıt altına alınmalıdır.
Aramanın sonunda, sorgulanan kişiye her cevabı paraflayıp, eğer doğruysa her sayfanın altını imzalayıp imzalayamayacağı ve son girişten sonra "Bunun söylenenlerin doğru bir kaydı olduğunu kabul ediyorum" gibi kelimeleri yazıp yazmayacağı sorulmalıdır ve imzası alınmalıdır.
Delilllere el koyan herkes ilgili girişleri paraflamalı ve sayfayı imzalamalıdır.
Bir kişinin girişi paraflamayı veya imzalamayı reddettiği durumlarda, hazır bulunan diğer kişi her cevabı paraflamalı ve her sayfayı imzalamalıdır.

Ek-7 Şekil 7.1. Gözetim zinciri talimatları

EK-7 (devam)

Giriş No	Deliller	1. Bulunduğu yer 2. Bulan kişi	3. El konma zamanı 4.Delil referans numarası
		1. 2.	3. 4.
		1. 2.	3. 4.
		1. 2.	3. 4.
		1. 2.	3. 4.
		1. 2.	3. 4.

El Koyan Kişilerin İmzaları .....
.....
.....

Ek-7 Şekil 7.2. Delil kayıt formu

EK-7 (Devam)

Sorular ve Cevaplar	5. Etiketlendiği yer 6. Etiketleyen kişi 7. Etiket numarası	8. Konulduğu yer 9. Koyan kişi 10. Diğer notlar
	5. 6. 7.	8. 9. 10.
	5. 6. 7.	8. 9. 10.
	5. 6. 7.	8. 9. 10.
	5. 6. 7.	8. 9. 10.
	5. 6. 7.	8. 9. 10.

Doğru şekilde kaydedilen her cevabı parafladım.

Sorgulanan kişi/kişilerin imzası/imzaları .....
.....
.....

Ek-7 Şekil 7.3. El koyma tutanağı örneği

EK-8. Adli kopya alma çalışma sayfası

ADLİ KOPYA ALMA ÇALIŞMA SAYFASI

VAKA BİLGİLERİ					
Vaka Numarası:					
Vaka Adı:					
Soruşturmacı:					
Vaka Yöneticisi:					

DELİL BİLGİLERİ					
Sistem Konumu:					
Sistem Tipi:	☐ Masaüstü	☐ Dizüstü	☐ Sunucu	☐ Diğer:	
Delil Tipi:	☐ Sabit Disk	☐ CD/DVD	☐ USB Bellek	☐ RAID	☐ Diğer:
Sistem Durumu:	☐ Açık	☐ Kapalı	☐ Sisteme Bağlı	☐ Diğer	
BIOS Tarih/Zaman					
Güncel Tarih/Zaman					
CPU üzerindeki toplam sabit disk sayısı:					
Sabit diski çıkaran kişi:					
Fotoğraf Çekildi mi?	☐ Evet	☐ Hayır- Nedeni:			

ONAY	
İşbu belgeyle (kurumun adını girin) (ve temsilcilerine) soruşturmaları için gerekli tüm bilgisayar ekipmanının mülkiyetini alma yetkisi veriyorum.	
İmza	Görev
Baskı İsmi	Tarih/Zaman

Ek-8 Şekil 8.1. Adli kopya alma örnek form

EK-8. (devam)

	BİLGİSAYAR	SABİT DİSK/DİĞER
Marka		
Model No:		
Seri No:		

KOPYA ALMA BİLGİLERİ				
Kim tarafından alındığı:				
Kopya alma yeri (Lab,Olay yeri vb.) :				
Kopya Alma Metodu	☐ Encase	☐ FTK	☐ X-ways	
	☐ DD kopya	☐ Mantıksal Kopya	☐ Diğer:	
Kopya Alma Donanımı	☐ Yazma Koruma	☐ Firewire	☐ Bootdisk	☐ Direk Bağlantı
	☐ SCSI-IDE W/B	☐ Xover Kablo	☐ Diğer:	
Kopyanın Yeri	☐ Sabit Disk	☐ Diğer:		
Seri No:				
Disk Sürücüsü No:				
Sabit Disk Büyüklüğü:	GB	MB		
Kopyanın Büyüklüğü:	GB	MB		
Kopya Doğrulandı mı?	Evet	Hayır	Hatalar:	Evet / Hayır
HASH Değeri:				

Ek-8 Şekil 8.2. Adli kopyanın alınacağı delil bilgileri

EK-9. Adli bilişim analiz formu /tablosu

Adli Bilişim Analiz Kontrol Formu

Faaliyet	Başladığı Tarih/Saat	Bittiği Tarih/Saat	İmza	Notlar
Resmi talebin alınması				Kim tarafından :
Uygun kaynakların kontrolü				
Dosyanın atanması				Kime atandı:
Delillerin alınması				Kim teslim aldı:
Delillerin fotoğraflanması				
Delil kaydının güncellenmesi				
Delil formlarının doldurulması (gözetim zinciri vb.)				
Triyaj gerekli mi?				
Önceliklendirme yapılması				Öncelik sıralaması:
Adli kopyanın alınması				Hangi yazılım ile:
Alınan kopyanın doğrulanması				
Kopyanın yedek sunucuya kopyalanması				Klasör ismi:
Vaka özelinde işleme ve araştırma faaliyeti				Vaka parametreleri:
Kopyaların otomatik incelenmesi				
Bölüm (partition) kurtarma				
Dosya kurtarma				
Dosyaların yüklenmesi (Mount)				
İmza analizi				
Hash analizi				Kullanılan Hash seti:
Diğer işleme işlemleri				Diğer işlemler:
Adli analiz				Analiz edilen toplam GB/TB:
E-postaların analizi				

Ek-9 Şekil 9.1. Adli bilişim analizi kontrol formu

EK-9 (devam)

Formun bu bölümündeki analizler gerekli olması halinde yapılacaktır.				
Dokümanların analizi				
Fotoğrafların analizi				
Videoların analizi				
İnternet tarayıcılarının analizi				
Kullanıcı etkinliğinin analizi				
Anahtar kelime araması				**Anahtar kelimeler:**
İndeksleme				
Sohbet uygulamaları analizi				
Veritabanları analizi				
Logların analizi				
Zararlı yazılım kontrolü				
Şifreli dosyaların kontrolü				
Sanal makine kurulumu				
Diğer iletişim verileri analizi				
Adli rapor				
Raporun kalite güvence gereklilikleri kontrolü				
Raporun teslimi				
Dosyanın arşivlenmesi				

Ek-9 Şekil 9.2. Adli bilişim analizi kontrol formu (Devam)

EK-10. Adli bilişim rapor şablonu

ADLİ BİRİMİN BAŞLIĞI (ADI)

Vak Ref. No:

Lab. Ref. No:

Rapor No:

İnceleyen: **Tarih:**

Adli analiz raporu

1. Vaka bilgisi

1.1. Vaka geçmişi
1.2. Rica etmek
1.3. Yetki

2. Deliller

2.1. Delil 1
2.1.1. Fotoğraflar
2.1.2. Tanım
2.2. Delil 2
2.2.1. Fotoğraflar
2.2.2. Tanım

3. İnceleme yöntemleri

3.1. Personel
3.1.1. Nitelikler
3.2. Donanım
3.2.1. Yazma Engelleyici
3.2.2. Adli Bilişim İstasyonu
3.2.3. Kullanılan Diğer Donanım

Vaka No: **İmza:**

Adli Birimin Alt bilgisi (Adres,E-posta vb.)

Ek-10 Şekil 10.1. Örnek rapor şablonu

EK-10 (devam)

3.3. Yazılım
3.3.1. Kopya Alma Yazılımı
3.3.2. İşleme Yazılımı
3.3.3. Analiz Yazılımı
3.3.4. Kullanılan Diğer Yazılımlar

4. İşleme süreci
4.1. Delil 1'in resmi
4.1.1. Alınan aksiyonlar
4.1.2. Hash doğrulamanın sonucu
4.2. Delil 2'nin resmi
4.2.1. Alınan aksiyonlar
4.2.2. Hash doğrulamanın sonucu

5. Analiz süreci
5.1. E-Postaların Analizi (varsa)
5.2. Ofis Dokümanlarının Analizi (varsa)
5.3. Muhasebe verileri (varsa)
5.4. Görüntülerin Analizi (varsa)
5.5. Videoların Analizi (varsa)
5.6. İnternet Tarayıcılarının Analizi (varsa)
5.7. Kullanıcı Etkinliğinin Analizi (varsa)
5.8. Anahtar kelime araması gerçekleştirildi (varsa)
5.9. Sohbet Uygulamaları Analizi (varsa)
5.10. Veritabanlarının analizi (varsa)
5.11. Günlük dosyalarının analizi (varsa)
5.12. Kötü amaçlı yazılım kontrolü? (uygunsa)
5.13. Şifreleme kontrolü? (uygunsa)
5.14. Sanal Makina kurulumu (varsa)
5.15. Diğer iletişim verilerinin analizi (varsa)

6. Sonuçlar

Ekler
a) Bulguların çıktısı
b) Sözlük
c) Teknik detaylara ilişkin rapor

Vaka No: **İmza:**

Adli Birimin Alt Bilgisi (Adres,E-posta vb.)

Ek-10 Şekil 10.2. Örnek rapor şablonu (Devamı)

EK-11 Delil kayıt formu örneği

Bölüm A: Delilin Alınması

No	Lab Delil Etiketi	Marka	Kapasite	Tanımlama (Renk,Çatlak vb.)	Seri No

Talep Eden	Laboratuvar
İmza İsim: Tarih:	İmza İsim: Tarih:

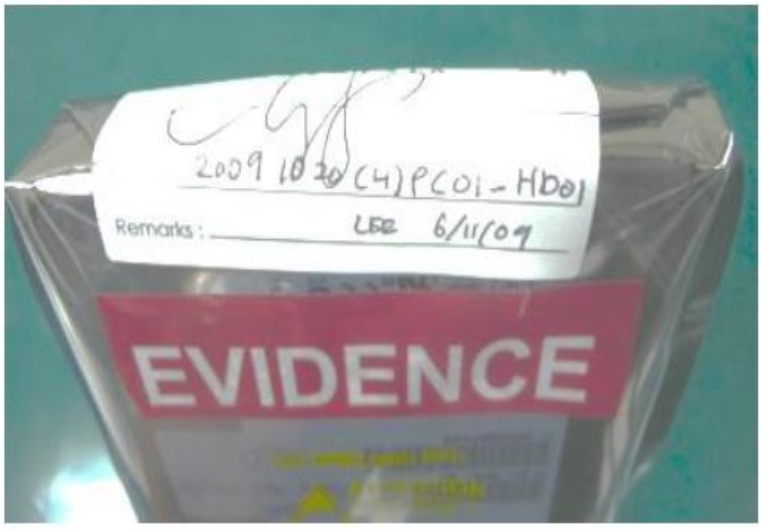
Bölüm B: Delilin İadesi

Laboratuvarın Bölüm A'da listelenen tüm kanıtları bana iade etmesini kabul ettim. Yukarıdaki sütunu imzaladıktan sonra her iki taraf da işin tamamlandığını ve davanın imzalandığını kabul etti.

Talep Eden	Laboratuvar
İmza İsim: Tarih:	İmza İsim: Tarih:

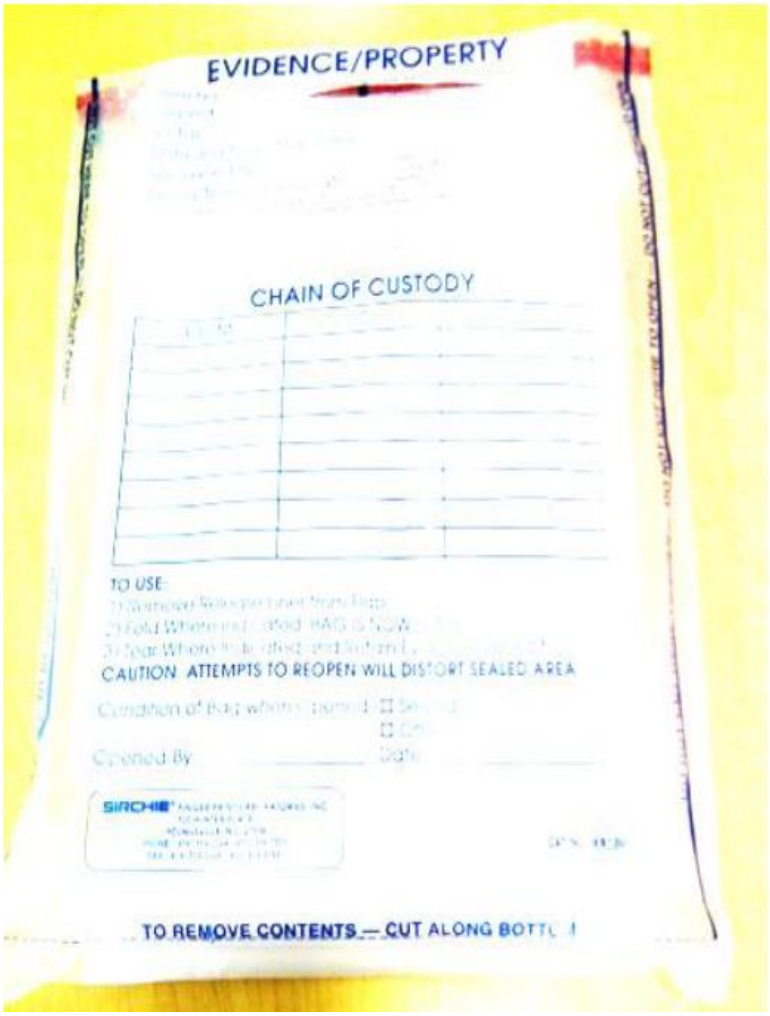
Ek-11 Şekil 11.1. Delil kayıt formu örneği

EK-12 Delil mühürleme örneği



Bir sabit disk olan delil, anti-statik bir plastik torbaya konur ve torbanın ağzına açılmaya dayanıklı bir etiket yapıştırılır. Daha sonra incelemeci, etiketin üzerine delilin etiketi,delilin mühürlendiği tarih ve saat ile birlikte adının baş harflerini koyar.

Bu örnekte delil açılması zor ve dayanıklı bir plastik torbaya konuyor. Delilin ayrıntıları, inceleyen ve gözetim zinciri plastik torbanın üzerinde mevcuttur.



Ek-12 Şekil 12.1. Etiketlenmiş delil ve delil poşeti

EK-13 Elektronik delil saklama kontrol formu

Elektronik Delil Saklama Kontrol Formu	
1	Etiket Deliller laboratuvara teslim edildikten sonra benzersiz bir şekilde etiketlenmelidir. Delil üzerine etiket koymak zorsa, laboratuvar etiketi kanıtın mührüne koyabilir. Etiket, delilin laboratuvarda kaldığı süre boyunca üzerinde kalmalıdır. Etiketler ayrıca alt öğeleri de izleyebilmelidir. Örnek: Bir cep telefonu için LAB-CT01 ve telefonda bulunan Sim kart için LAB-CT01-SIM01.
2	Mühür Deliller uygun bir kap kullanılarak mühürlenmelidir. Kap, delillere yapılan her türlü erişimi tespit edebilmelidir. Delil, Kontrol Uzmanı tarafından imzalanmalı ve tarih atılmalıdır. Delillere her erişildiğinde, bunu yapan kişi, işlem tamamlandıktan sonra, kendi imzasını ve tarihlerini taşıyarak delili yeniden mühürlemelidir.
3	Kayıt Elektronik delillerin tam bir kaydı oluşturulmalıdır. Kaydedilecek öğeler arasında delil türü, seri numarası, üretici, tüm kusurlar ve tüm etiketler yer alır. Laboraturvarda delil envanter listesi de oluşturulmalıdır. Her elektronik delil için bir saklama zinciri kaydı oluşturulmalıdır. En azından benzersiz bir etiket, baş harfler ve tarih içermelidir.
4	Boşta Bırakma İnceleme uzmanının uzun süreli izni ya da yüksek öncelikli vakalara odaklanması nedeniyle inceleme sürecinde olmayan deliller laboratuvarda gözetimsiz bırakılmamalıdır. Kirlenmeyi önlemek için uygun şekilde saklanmalıdır. Deliller taşıma işlemi sırasında da başıboş bırakılmamalıdır.
5	Kirlenmeden uzak tut Elektronik delillere uygun şekilde dikkat edilmeli ve su, ısı, aşırı nem ve elektromanyetik alan gibi kontaminasyon kaynaklarından uzak tutulmalıdır.
6	Depolama Elektronik deliller sınırlı erişime sahip güvenli bir yerde saklanmalıdır. Depo Odasındaki delillerin giriş ve çıkış kaydı güncel tutulmalıdır.
7	Koruma Orijinal delilin bütünlüğünü korumak için orijinal elektronik delilin bir kopyası yapılmalıdır. Orijinal delilin ve kopyasının hash değeri aynı olmalıdır. Elektronik delillerin kopyası üzerinde inceleme ve analiz yapılmalıdır.

Ek-13 Şekil 13.1. Örnek delil saklama kontrol formu

EK-14 Adli Raporun oluşturulması için gereken örnek kriterler

	Adli Raporda Olması Gereken Hususlar
1	Başlık
2	Laboratuvar adı ve adresi
3	Toplama ve incelemenin yapıldığı yer
4	Sayfa numarası ve sayfa sonunun belirtilmesi
5	Talep edenin adı ve irtibat numarası
6	Vakada kullanılan deney metotları
7	Delilin tanımı
8	Delilin laboratuvara geliş tarihi
9	İncelenme tarihi
10	Raporun yazılış tarihi
11	Rapor sonucu
12	Raporu inceleyen kişinin ismi ve ünvanı

Ek-14 Şekil 14.1. Örnek kriterler

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : ARICAN, Halil İbrahim

Uyruğu : T.C.

Doğum tarihi ve yeri

Medeni hali

Telefon

e-mail

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek lisans	Gazi Üniversitesi / Adli Bilişim	Devam ediyor
Lisans	Selçuk Üniversitesi / Hukuk	2019
Lisans	Kara Harp Okulu	2010
Lise	Maltepe Askeri Lisesi	2006

İş Deneyimi

Derece	Eğitim Birimi	Görev
2018-Halen	Jandarma Kriminal Daire Başkanlığı	Şube Müdürü
2017-2018	Somali Türk Görev Gücü Kuvvet Komutanlığı	Takım Komutanı
2016-2017	ANITKABİR Mrs.Bl.K.lığı	Takım Komutanı
2014-2016	Tunceli Pülümür J. Krk.K.lığı	Karakol Komutanı
2012-2014	Hatay J.Komd.Öz.Hrk.Tb.K.lığı	Tim Komutanı

Yabancı Dil

İngilizce

GAZİLİ OLMAK AYRICALIKTIR…