

POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

ISSN: 1302-0900 (PRINT), ISSN: 2147-9429 (ONLINE)

URL: http://dergipark.org.tr/politeknik

CLARIVATE ANALYTICS EMERGING SOURCES CITATION INDEX INDEXED

Ağ adli bilişimi süreç gereksinimlerinin belirlenmesi ve yazılım tanımlı ağlarda incelenmesi

Determination of network forensics process requirements and analysis in software-defined networks

***Yazar(lar) (Author(s))**: Altuğ ÇİL[1], Mehmet DEMİRCİ[2]*

ORCID[1]: 0000-0002-3714-0432

ORCID[2]: 0000-0002-1088-5215

ERKEN GÖRÜNÜM

Bu makaleye şu şekilde atıfta bulunabilirsiniz(To cite to this article): Çil A. ve Demirci M., "Ağ adli bilişimi süreç gereksinimlerinin belirlenmesi ve yazılım tanımlı ağlarda incelenmesi", ***Politeknik Dergisi***, *(*): *, (*).

Erişim linki (To link to this article): http://dergipark.org.tr/politeknik/archive

DOI: 10.2339/politeknik.1141107

Ağ Adli Bilişimi Süreç Gereksinimlerinin Belirlenmesi ve Yazılım Tanımlı Ağlarda İncelenmesi

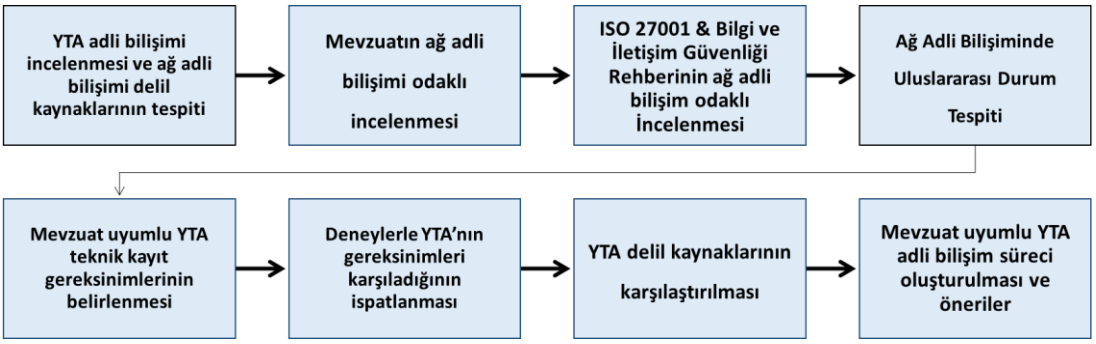
Determination of Network Forensics Process Requirements and Analysis in Software-Defined Networks

Önemli noktalar (Highlights)

- *Ağ adli bilişimi gereksinimlerinin belirlenmesi. / Identification of network forensics requirements.*
- *Gereksinimlerin yazılım tanımlı ağlardaki (YTA) durum tespiti. / Due diligence of requirements in software-defined networks (SDN).*
- *Mevzuat uyumlu YTA adli bilişim yönetim sürecinin oluşturulması. / Establishment of legislation compliant SDN forensic management process.*

Grafik Özet (Graphical Abstract)

Mevzuatın ve uluslararası düzeyde idari ve teknik YTA adli bilişim tespitinin yapılmasının ardından gerçekleşen deneylerle YTA'nın mevzuat gereksinimlerini karşıladığı ispatlanmış, YTA delil kaynakları karşılaştırılması gerçekleştirilmiş ve mevzuat uyumlu bir YTA adli bilişim süreci önerilmiştir. / After the legislative and international level administrative and technical SDN forensics detection, it has been proven that SDN meets the requirements of the legislation, SDN evidence sources are compared and a legislation-compliant SDN forensics process is proposed.



Şekil. Süreç ve incelemeler diyagramı / **Figure.** Process and reviews diagram

Amaç (Aim)

Ağ adli bilişim gereksinimlerinin tek bir kaynakta belirlenerek YTA'da incelenmesi./ Determining network forensic requirements in a single source and examining them in SDN.

Tasarım ve Yöntem (Design & Methodology)

YTA adli bilişim süreçleri mininet ortamı ile test edilmiştir. / SDN forensics processes have been tested with the mininet environment.

Özgünlük (Originality)

İlk defa mevzuat ve uygulamalarla uyumlu bir YTA adli bilişim yönetim süreci önerilmiştir./ For the first time, an SDN forensic management process compatible with legislation and practices has been proposed.

Bulgular (Findings)

Teknik kayıt gereksinimlerindeki kayıtlar en az eforla elde edilebilen en önemli delil kaynaklarıdır./ Records in technical record requirements are the most important sources of evidence that can be obtained with the least effort.

Sonuç (Conclusion)

YTA geleneksel ağ adli bilişim süreçlerinin asgari kriterlerini sağlamaktadır./ SDN meets the minimum criteria of traditional network forensics processes.

Etik Standartların Beyanı (*Declaration of Ethical Standards*)

Bu makalenin yazar(lar)ı çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler. / The author(s) of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

Ağ Adli Bilişimi Süreç Gereksinimlerinin Belirlenmesi ve Yazılım Tanımlı Ağlarda İncelenmesi

Araştırma Makalesi / Research Article

Altuğ ÇİL[1,2*], Mehmet DEMİRCİ[3,1]

[1]Bilişim Enstitüsü, Gazi Üniversitesi, Ankara, Türkiye
[2]Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK), Ankara, Türkiye
[3]Bilgisayar Mühendisliği Bölümü, Mühendislik Fakültesi, Gazi Üniversitesi, Ankara, Türkiye

(Geliş/Received : 06.07.2022 ; Kabul/Accepted : 28.11.2022 ; Erken Görünüm/Early View : 16.12.2022)

ÖZ

Türkiye'de internet üzerinden işlenen suçların aydınlatılması amacıyla adli, idari ve teknik süreçleri tanımlayan mevzuat ve uygulamalar mevcuttur. Ancak bunların ağ adli bilişimi odağında incelenmediği, sağlıklı ve mevzuata uygun ağ adli bilişimi süreçleri için gereksinimlerin belirlenmediği ve yazılım tanımlı ağlar (YTA) üzerinde incelenmediği görülmüştür. Bu çalışmada YTA adli bilişimi ve bilirkişiliği için gerekli delil kaynaklarının tespiti, Türkiye'de kullanılan mevzuat ve uygulamaların ağ adli bilişimi odağında temel gereksinimlerinin belirlenmesi, gereksinimlerin YTA ortamına uygulanabilirliğinin gösterilmesi ve bir YTA adli bilişim süreci oluşturulması amaçlanmıştır. Uluslararası çapta yapılan diğer teknik ve idari ağ adli bilişim çalışmalarının da incelenmesinin ardından YTA deneyleri adli bilişim süreçleri gözetilerek gerçekleştirilmiştir. Deney sonuçları YTA'nın belirlenen gereksinimleri sağladığını göstermiştir. Geliştirilebilir alanlar, uluslararası çapta yapılan diğer çalışmalar da ele alınarak tartışılmış olup, mevzuat ve uygulamaların YTA'ya tam uyum sağlaması için önerilerde bulunulmuştur. Türkiye'de adli bilişim alanında alınabilecek önlemlerin de değerlendirilmesinin ardından YTA adli bilişim yönetimi niteliğinde olan bir süreç önerisinde bulunulmuştur. YTA adli bilişiminin sadece güney arayüzü verileriyle yapılabilmesinin mümkün olduğu ancak bu konuda idari düzenlemelerin gerektiği, mevzuat kapsamında belirlenen verilerin en önemli veriler olmasına rağmen en az eforla elde edilebileceği ve sınır ötesi adli bilişim çalışmalarının gerekli olduğu sonuçları elde edilmiştir.

Anahtar Kelimeler: Adli bilişim, yazılım tanımlı ağ, bilgisayar ağları, siber güvenlik, bilişim suçları.

Determination of Network Forensics Process Requirements and Analysis in Software-Defined Networks

ABSTRACT

In Türkiye, there are legislation and practices that define the judicial, administrative and technical processes for the purpose of illuminating the cybercrimes. However studies in the perspective of network forensics are scarce thus the requirements for healthy and regulatory network forensics processes are not determined, and have not been examined on software-defined networks (SDN). This study aimed to determine the necessary evidence sources for SDN forensics, the basic requirements of the legislation and applications used in Türkiye in the focus of network forensics, and to show the applicability of the requirements to the SDN environment and to create an SDN forensic process. SDN experiments were carried out in light of forensic processes and previous international studies. The results showed that SDN met the specified requirements. Suggestions were made to ensure full compliance of legislation and practices with SDN. After the evaluation of measures that can be taken in the field of forensic informatics, a framework for SDN forensic management has been proposed. Conclusively, SDN forensics can only be performed with the southern interface data and a legislative regulation is necessary. The significant data required by the legislation can be obtained with the least effort via SDN forensics.

Keywords: Forensics, software-defined networks, computer networks, cyber security, cyber crimes.

1. GİRİŞ (INTRODUCTION)

Bilgisayar, tablet, cep telefonları vb. cihazların kullanımının artmasıyla bireysel internet kullanımında artış yaşanmıştır. 2011 yılında %45 olan bireylerde internet kullanım oranı 2021 yılında %82,6'ya artarken, internet erişimi imkânı olan haneler ise 2011 yılında %42,9 iken 2021 yılında %92 seviyesine ulaşmıştır. En az haftada bir defa internet kullanan kesimin oranı ise %80,5'tir [1]. 2021 yılında şirketlerin %86'sı son 1 yılda en az bir siber saldırıya uğramıştır [2]. İnternet kullanımın ve siber suçların bu derece yüksek bir hızla artması ağ ortamında gerçekleştirilen adli bilişim çalışmalarının önemini de artırmaktadır.

Geleneksel ağların yerine yenilikçi bir ağ modeli sunan yazılım tanımlı ağların (YTA) kullanım oranı günden güne artmaktadır. 2020 yılında 13,7 Milyar ABD Doları olan YTA küresel pazar büyüklüğünün 2025 yılına kadar 32,7 Milyar ABD Dolarına çıkması beklenmektedir [3]. Bu sebepten YTA'da adli bilişime odaklanmak kritik

*Sorumlu Yazar (Corresponding Author)
e-posta : altug.cil@tubitak.gov.tr

ERKEN GÖRÜNÜM

öneme sahiptir. Adli bilişim konusunda Türkiye'de üniversiteler, kamu kurumları ve özel sektör tarafından gerçekleştirilen çalışmalar genellikle siber suçları aydınlatmak ve delil elde etmek amaçlı eğitim ve araştırmalar şeklindedir [4-6]. Adli bilişim çalışmalarının ana ekseninde yer alan delil elde etme süreçleri başta olmak üzere, inceleme ve diğer aşamaların [7-12] mevzuatlara uygun olması gerekmektedir. Türkiye'de bilişim suçlarının adli ve idari kapsamını belirleyen çeşitli Kanun ve Yönetmelikler bulunmaktadır [13-20]. Mevzuatın yanı sıra bilgi güvenliği kapsamında dünya çapında kabul görmüş standartlar ve kamu kurumlarımızın hazırlamış olduğu rehberler de bulunmaktadır [21-25].

Ağ adli bilişim çalışmalarının tüm adli bilişim çalışmaları gibi mevzuat ve uygulamalara uygun olması gerekmektedir. Ayrıca ağ adli bilişim çalışmaları teknik olarak ileri seviye bilgi gerektiren süreçlerdir ve bir süreç kapsamında yönetilmelidir. Ülkeler ve kuruluşlar özelinde adli bilişim süreçlerinin incelendiği ve çözüm önerilerinin geleneksel ağ bakış açılarıyla tartışıldığı çalışmalar ve rehberler mevcuttur [26-48]. Geleneksel ağlarda veri elde etme yöntemlerinin belirlenmesi, bilişim suçlarının araştırılması, adli bilişimde kullanılan programların analiz edilmesi, siber güvenlik seviyelerinin araştırılması ve çözüm yollarının önerilmesi üzerine çalışmalar mevcuttur [7-12, 49,50].

Adli bilişim çalışmalarının amacı genellikle geçmişe yönelik gerçekleşen olayları aydınlatmaktır. Adli bilişim analizi yapılması için bir siber güvenlik açığının olması şart değildir. Rutin bir erişimin aydınlatılabilmesi de adli bilişimin kapsamı dâhilindedir. Adli bilişimde en önemli husus kayıt tutmak ve bu kayıtları usulüne uygun şekilde değerlendirebilmektir. Bu kayıtların tutulması, erişilmesi ve değerlendirilmesi süreçlerinde mevzuata uyum sağlanmadığı durumda, gerçekleştirilen ağ adli bilişim süreçleri de geçerliliğini ve güvenilirliğini yitirecektir.

Türkiye'de geçerli olan mevzuatın ağ adli bilişimi açısından incelenmesi üzerine bir çalışma yapılmamıştır. Mevzuat ve uygulamalar geleneksel ağlarda adli bilişim üzerine hususları içermekte olup, zaten geleneksel ağ süreçlerine uygun olarak tasarlanmış olduklarından gereksinimlerin geleneksel ağlarda uygulanabilirliğinin teknik olarak mümkün olacağı kabul edilebilir. Ancak adli bilişim gereksinimlerine YTA adli bilişimi kapsamında erişilip erişilemeyeceği hususunda da bir araştırma yoktur.

Tüm değerlendirmeler göz önüne alındığında bu çalışma aşağıda sıralanan amaçları içermektedir;

- Mevzuat ve uygulamalardaki ağ adli bilişim gereksinimlerinin belirlenmesi,
- Gereksinimlerin YTA ortamındaki durumunun deneylerle tespit edilmesi,
- YTA adli bilişiminde delil kaynaklarının tespit edilmesi ve kıyaslanması,
- Mevzuat uyumlu YTA adli bilişim süreci oluşturulması.

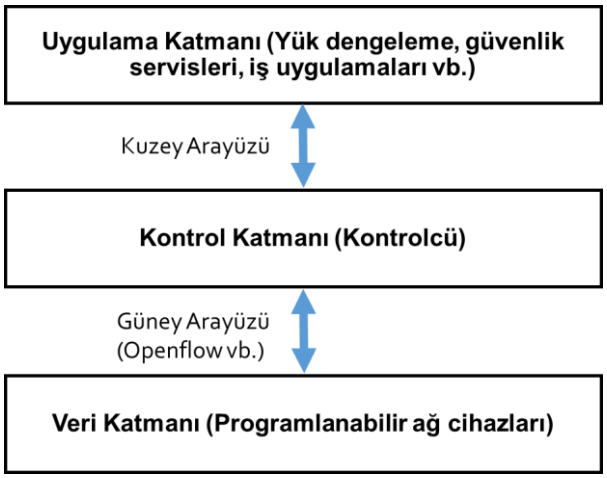
YTA adli bilişiminde bilirkişilik ve uluslararası düzeyde teknik ve idari ağ adli bilişim çalışmalarına dair bilgilerin ilk defa sunulduğu ve tespit edilen güzel uygulama örneklerinin tüm süreç gözetilerek ilk defa tartışıldığı bu makalenin mevzuat uyumlu YTA adli bilişimi süreçleri açısından öncü bir çalışma olacağı düşünülmektedir.

2. YAZILIM TANIMLI AĞLAR VE AĞ ADLİ BİLİŞİMİ (SOFTWARE-DEFINED NETWORKS AND NETWORK FORENSICS)

2.1. Yazılım Tanımlı Ağlarda Güvenlik ve Adli Bilişim (Security and Forensics in Software-Defined Networks)

YTA tüm ağın etkin bir şekilde yönetilebilmesi için artan talepleri karşılayamayan geleneksel ağ mimarisini basit ve yönetilebilir bir ağa dönüştürülebilen bir teknolojidir [51] ve dinamik akış kontrolü, merkezi ağ kontrolü, ağ programlanabilirliği ve daha basit veri düzlemi hususlarında avantaj sağlamaktadır [52]. Farklı üreticilerin ağ cihazları YTA ile yönetilebilir olup YTA kontrolcüsü tüm ağın yönetiminden sorumludur.

Şekil 1'de gösterildiği üzere YTA; uygulama, kontrol ve veri katmanı olmak üzere üç farklı katmandan oluşur. Altyapı katmanında OpenvSwitch gibi sanal anahtarlar ve fiziksel anahtarlar bir arada bulunurken, kontrol katmanında yer alan kontrolcü yönlendirme ve paket bırakma gibi hususlarda karar alıcı yapıdır. Kontrol katmanı ve veri katmanı güney arayüzü aracılığıyla iletişim sağlamakta olup, bu otomasyon süreci için en yaygın kullanılan protokol OpenFlow'dur. Uygulama katmanı ise saldırı tespit ve önleme sistemleri, güvenlik duvarı gibi sistemlerin yönetiminden sorumluyken, kontrol katmanı arasındaki iletişim kuzey arayüzü aracılığıyla sağlanmaktadır [53].



Şekil 1. Yazılım tanımlı ağ mimarisi (Software-defined network architecture)

YTA'da güvenlik, YTA'nın kendi çerçevesinden güvenlik için faydalanmak ve YTA'nın kendi güvenliğini sağlamak olarak iki ana başlıkta incelenebilir. YTA'da güvenlik üzerine odaklanma gerçekleşmeden tüm

ERKEN GÖRÜNÜM

özelliklerin sağlıklı gelişerek desteklenmesi mümkün değildir [53]. Diğer güvenlik araştırmalarına kıyasla, YTA güvenliği odaklı çalışmaların nispeten yavaş ilerlediği değerlendirilmekle birlikte YTA'nın yeni özellikleri ve kolay yönetimi dikkate alındığında, yeni ve gelişmiş ağ güvenliği sistemlerinin gelişiminde fayda sağlayabileceği değerlendirilmektedir [52]. Ancak tersine bir yorum olarak bizzat YTA'nın kendi süreçlerinin yeniliğinden dolayı doğrudan YTA kaynaklı güvenlik açıkları da oluşabilir.

YTA alanında bazı güvenlik çalışmaları yapılmış olsa da YTA'da adli bilişim çalışmaları yeterli değildir [54]. Geleneksel ağlar için yapılan adli bilişim çalışmaları da farklı katmanlar ve yeni teknolojiler içeren YTA açısından yeni yaklaşımlar gerektirmektedir [55]. YTA ağlarında web istatistiklerini toplayan [56], makine öğrenmesi yöntemleriyle ping seli ataklarını kontrolcü tabanlı engelleyen [57] sistemler geliştirilmiştir. Çalışmalar güney arayüzünün veri toplamak için en iyi yerlerden biri olduğunu göstermiş olsa da [54] güney arayüzü tarafından işletilen süreçler saldırganların ana hedefidir [55]. YTA adli bilişimi için günlükler ve bellek bilgilerinin de dikkate alınması önerilmektedir [58].

2.2. Yazılım Tanımlı Ağ Adli Bilişiminde Delil Kaynakları ve Bilirkişilik (Evidence Sources and Expertise in Software-Defined Network Forensics)

Adli bilişim genel hatlarıyla; Bilgisayar, Ağ ve Gömülü Cihaz Adli Bilişimi olarak üç alt alana ayrılabilir. Bilgisayar adli bilişimi genellikle depolama ürünleri üzerinde veri kurtarma çalışmalarına dayanan yapıya sahipken, ağ adli bilişimi ise anlık olarak veya depolandıktan sonra incelenen yerel veya geniş alan ağı odaklı verilerin elde edilmesine yönelik çalışmaları içermektedir. Gömülü cihazların en başında ise akıllı telefonlar gelmektedir [5]. Adli bilişim çalışmaları, bilgi edinme, strateji oluşturma, delil toplama, analiz ve raporlama olarak beş aşamadan oluşmaktadır [59].

Adli bilişimde ağ analizi yapmak için ağ üzerinde akan verileri, canlı olarak veya paket halinde depolanmış şekilde, analiz edebilmek amacıyla bazı programlar kullanılmaktadır. Bu programlar yardımıyla port bilgisi, paket yakalama ve veri elde etme işlemleri gerçekleştirilebilmektedir. Ağ üzerinde gerçekleşebilecek adli bilişim süreçleri, verilerin yakalanması, kaydedilmesi ve analizi olarak tanımlanabilmektedir. Bu doğrultuda adli bir vakada çeşitli yardımcı programlar vasıtasıyla süreçler tamamlanabilmektedir [49].

Ağ analizleri canlı bir şekilde yapılabildiği gibi, kayıt altına alınan veriler üzerinden geçmişe yönelik analizler yapılması da mümkündür. Bu analizler sırasında "kim, ne, neden, nasıl, nerede ve ne zaman" sorularına cevaplar aranmalı ve hukuki zemine uyum göz ardı edilmemelidir [50,60]. İncelemelerde elde edilen veri setlerinde, "bulunabilirlik, erişilebilirlik, birlikte çalışabilirlik ve yeniden kullanılabilirlik" gereksinimleri aranmaktadır [61].

Ağ üzerinden işlenmiş olup olmadığına bakılmaksızın bazı durumlarda delil elde etmek amacıyla kişilerin bilgisayarlarından, sabit disklerinden elde edilen verilerin dijital delil olarak kullanılabilmesi durumu Ceza Muhakemeleri Kanunu'nun (CMK) 134. maddesinde yer almaktadır. Bu sistemlere el konulabileceği, el konulan bütün verilerin yedeklemesinin yapılması, kopya çıkarılarak şüpheli ve vekiline verilmesi ve bu durumların tutanak altına alınması gerektiği Kanunda belirtilmiştir [20]. Bahsi geçen mevzuatın uygulayıcılarının başında kolluk birimlerinin bilişim suçlarıyla mücadele birimleri yer almakta olup, ana başlık olarak siber suç soruşturma, önleme ve adli bilişim alanlarında görevler yürütülmektedir [6]. Deliller; gerçekçi, geçmişteki somut olayı temsil edici, akılcı, kanuna uygun yollarla elde edilmiş ve muhakemenin taraflarının da bilmesini sağlayacak bir şekilde müşterek olmalıdır [5].

CMK 63-1'e göre çözümü uzmanlık gerektiren hallerde bilirkişi ataması yapılabilir. Adli bilişim alanındaki bilirkişilikler teknik bilgi gerektiren ve sayısal delillerden faydalanılan bir uzmanlık alanıdır. Sayısal deliller; programlar, sabit diskler, işletim sistemleri ve bilgisayar ağları gibi ortamlardan elde edilebilir. Son yıllarda vaka başına düşen on katlık artış göz önüne alındığında sayısal delile en hızlı şekilde ulaşabilmek adına veriler arasında bir önceliklendirme yapılması gerekebilir. Olay yerinde önceliklendirme ve laboratuvar ortamında önceliklendirme olarak ele alınacak süreçte Cumhuriyet savcılığı bilişim sistemlerinde bir arama kararı verdiğinde, arama kararı verilen veriler bir öncelik temsil etmekle birlikte sürecin detayında adli bilişim uzmanı teknik açından ikinci bir önceliklendirme yapmalıdır. Arama kararı kolluk kuvvetlerinin gerçekleştirdiği bir bilirkişilik işlevi olarak düşünülebilir. Ancak arama kararında da sayısal delile ulaşma amacıyla ayrıca bilirkişi görevlendirilebilir. Laboratuvar ortamında ise bilirkişiye tahsis edilen süre içerisinde sürecin sonlanması açısından önceliklendirme önemlidir. Yakın zamanda kaybolma ihtimali olan bilgiler ile delil içermesi muhtemel ve yakın zamanda kaybolmayacak olan bilgilere öncelik tanınması gerekmektedir [7].

Windows işletim sistemlerinden; dosya işlemleri, internet geçmişi, kayıt defterleri, RAM bilgileri gibi sistemlere erişim sağlanabilmektedir ve bu sayede açılan dokümanlar, e-posta adres bilgileri, oturum açma bilgisi, parola değiştirme zamanı gibi çok sayıda bilgiye de erişim sağlanabilir. Bunların yanı sıra canlı olarak ağ bağlantı bilgileri, son açılıştan sonra geçen süre, sanallaştırma sistemi varsa bu sisteme ait olan MAC adresleri ve ağ bağdaştırıcı bilgilerine de erişim mümkündür [8]. Linux işletim sistemlerinden de kullanıcı bilgisi, ağ durumu, dosya değişiklik kodu, yüklenen modüller gibi bilgilerin elde edilmesi mümkündür [9]. Silinmiş verilerin çeşitli yazılımlar yardımıyla kurtarılması mümkün olup bu süreç delil elde etme aşamasında efor seviyesi yüksek olan aşamalardandır. Disk üzerinden veya silinen dosyaların arasından anahtar kelimelerle aramalar yaparak aranılan

ERKEN GÖRÜNÜM

odak bilgiye erişim mümkündür [11]. Mobil cihazların adli bilişimine dair piyasada kullanılan yazılımlar yardımıyla ilk müdahale aşamasından, imaj alma ve veri elde aşamasına kadar geniş bir süreç önerisi gerçekleştirilmiş olup, mobil cihazların da internet ortamında gerçekleştirilen suçlarda ve suçların aydınlatılmasında önemli rol oynayabileceği gösterilmiştir [10]. Bulut bilişimde adli bilişim süreçleriyse diğer adli bilişim süreçlerine göre yasal, organizasyonel ve teknik açıdan daha geniş kapsamlıdır. Dinamik veri, verilerin yerinin tespiti, zaman farklılıkları, delillerin elde edilmesi gibi süreçlerde zorluklar içeren bulut bilişimde adli bilişim süreçleri için henüz bir yasal zemin standardı mevcut değildir ve yeni yöntemler gerekmektedir [12].

RAM üzerindeki uçucu bilgilerden zararlı yazılımların tespiti de mümkündür. Uçucu verilerin işletim sisteminden kaybolmaması adına cihazlar, doğrudan güç kaynağı çekilerek kapatılmalıdır. Aksi durumda internet ön bellek dosyaları, swap dosyaları, hazırda beklet dosyaları gibi geçici süreyle tutulan tüm dosyalar kaybedilme riski taşıyacaktır [11]. RAM bilgisinin sağlıklı şekilde alınabilmesi için sistemin imajının çalışır durumdayken alınması önemlidir ancak sistem kapansa dahi işletim sistemi RAM bilgisine dair önemli bilgiler sağlayabilir [9].

Ağ bağlantıları akıp giden bir formattadır ve geçmiş bağlantı bilgileri tutulmamaktadır. Aktif bağlantılara dair bilgiler Windows kayıt defteri, DHCP sunucusu, etki alanı gibi ortamlarda ve kablosuz ağ bağlantı kimliklerinde bulunmaktadır. Bu bilgiler de diğer uçucu bilgiler gibi geçici süre ile depolanmaktadır [11].

Ağ bağlantısı içeren bir ortamda çevre birimler de dikkate alınarak açıklanan bu delil kaynaklarının, bilirkişiler tarafından önem, efor, uçuculuk ve öncelik açısından da ele alınarak işletilmesi gerekmektedir. Bu süreç esnasında kurumlar tarafından zaten kayıt altına alınması gereken teknik kayıt gereksinimleri olduğu bilinmektedir. Bu çalışma kapsamında belirlenecek teknik kayıt gereksinimlerinin YTA ortamında elde edilmesi de bu çalışma içerisinde tartışıldıktan sonra YTA delil kaynaklarına dair bir karşılaştırmalı analiz sunulacaktır.

3. MEVZUAT VE UYGULAMALARIN AĞ ADLİ BİLİŞİM ÇALIŞMALARI KAPSAMINDA DEĞERLENDİRİLMESİ (EVALUATION OF LEGISLATION AND PRACTICES WITHIN THE SCOPE OF NETWORK FORENSIC STUDIES)

3.1. Mevzuatın Ağ Adli Bilişimi Gereksinimleri Açısından İncelenmesi (Examining the Legislation in Terms of Network Forensics Requirements)

Tam bir denetim ve engellemenin oto-kontrol mekanizmasına sahip olan internet ortamında uygulanmasının mümkün olmadığı söylenemez [6]. Ancak denetim seviyesinin en üst seviyelere ulaşması adına mevzuatta paydaşların sorumlulukları ve çeşitli yükümlülükler belirtilmiş olup, süreçlerin sağlıklı uygulanması için de standart ve rehberler yayımlanmıştır.

Bilişim suçlarıyla mücadele kapsamında yer alan mevzuatın başında 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" [13] yer almaktadır. Bahsi geçen kanun çeşitli yönetmeliklerle de detaylandırılmıştır [14-16]. Kanunda internet ortamındaki yayınlara belirsiz sayıda kişilerin ulaşması hususuna değinilmiş olup bu yayınların paydaşları da aşağıda belirtilmiştir;

- İçerik sağlayıcı, bir web sayfası veya bir platform aracılığıyla bilgi paylaşan kişilerdir. Yer sağlayıcılar, hizmet veya içerikleri barındıran sistemleri sağlayan gerçek/tüzel kişilerdir.
- Erişim sağlayıcılar ise genel tabirle internet servis sağlayıcılarıdır.
- Toplu kullanım sağlayıcılar, çalışanlarına, ziyaretçilerine vb. internet kullanımı sağlayan işyerlerini, Kamu kurumlarını vb. (ticari ve ticari olmayan) ifade etmektedir.
- Sosyal ağların dünya genelindeki artan kullanımı göz önünde bulundurulmuş ve 2020 yılında yapılan güncellemeyle Kanuna Sosyal Ağ Sağlayıcıların yükümlülükleri de eklenmiştir [17].

Kanunda gerekli verilerin tespit edilmesi amacıyla yapılacak izleme ve elde etme çalışmaları "trafik bilgisi" olarak tanımlanmıştır ve Kanun ile yönetmeliklerde yer alan yukarıdaki paydaşlar için benzer bilgilerin kayıt altına alınması gerektiği belirtilmiştir. Erişim yasağı getirilen hedefler için alan adı veya IP adresi bazlı, öncelikli olarak kısmi veya mümkün değilse tamamen engelleme yapılabilmesi durumları da belirtilmiştir. Ayrıca kayıt altına alınan trafik bilgilerinin saklanma süreleri de belirtilmiştir [13].

Toplu kullanım sağlayıcılarından özellikle otomatik IP adresi dağıtımlarına dair detay bilgilerin kayıt altına alınması beklenmektedir. Otomatik IP adresleri DHCP (Dynamic Host Configuration Protocol) sunucuları tarafından, belirlenen kurallar dâhilinde dağıtılmaktadır. Bu yapılarda kullanıcılar sıklıkla değiştiğinden sabit IP adresi kullanımının mümkün olmadığı değerlendirilmiştir. Bu sebepten dağıtımı yapılan IP adreslerine dair bilgilerin, kullanıcı bilgileriyle eşleştirilerek kayıt altına alınması gerekmektedir. Toplu kullanım sağlayıcılar filtreleme sistemi kullanmalı ve ayrıca doğruluk, bütünlük ve gizlilik kriterlerini sağlayarak erişim kayıtlarını iki yıllık süre kapsamında saklamalıdır [14].

Erişim sağlayıcıları içeriğin hukuki kapsamını kontrol etmekle yükümlü olmasa da yasaklanan hedefleri teknik olarak engelleme imkânı bulunduğu ölçüde engelleyebilmelidir. Trafik bilgileri, abone bilgileriyle birlikte dosya bütünlüğü de korunarak saklanmalıdır. Trafik bilgilerinde belirtilen IP adresi OSI katmanı

ERKEN GÖRÜNÜM

üçüncü seviyede yer alan, yönlendirilebilir IP adresleri olduğundan bu açıdan toplu kullanım sağlayıcılardan farklılık göstermektedir. Erişim sağlayıcılar trafik bilgilerini bir yıl saklamakla mükellefken yer sağlayıcılarda bu süre altı ay olarak belirlenmiştir. Yer sağlayıcıların tutması gereken trafik bilgisine dair yönetmelikte verilen bilgilerde dikkat çeken bir detay GET, POST komut detayları ve sonuç bilgisi gibi bilgilerin de kayıt altına alınması gerekliliğidir [15]. Bu bilgilerin yanı sıra erişim sağlayıcılar vekil sunucu trafik bilgisini de kayıt altına almalı ve bir yıl süreyle saklamalıdır. İnternete bağlı bir bilgisayarla diğer bilgisayarlar arasındaki iletişimi bir geçiş yolu şeklinde sağlayan [62] vekil sunucu trafik bilgisine dair tanımlamaların yapıldığı yönetmelikte, tanımlardaki bilgilere benzeyen bilgilerin de tutulması gerektiğini belirten "gibi bilgiler" ifadesi mevcuttur [16].

Verilerin zaman damgasının "Elektronik İmza Kanunu"nda yer alan tanımında imzanın niteliğinden bahsedilmediğinden, kayıtların saklanması aşamasında gerekli olan zaman damgasının nitelikli veya nitelikli olmayan elektronik imza ile imzalanabileceği değerlendirilmiştir [63]. "Elektronik Haberleşme Kanunu"nda ise ağ adli analizi hususunda değerlendirilebilecek bir çerçeve çizilmediği görülmüştür [18].

Bilişim suçlarına dair verilecek cezalara dair hükümler Türk Ceza Kanunu'nun (TCK) 10. Bölümünde ele alınmıştır. Bir sisteme izinsiz girme, içerik değiştirme, virüs benzeri programlar yükleme, çalışmaz hale getirmeye çalışma, başkasının kredi kartını kullanma gibi suçlar Kanunda genel ifadelerle tarif edilmiştir. Dikkat çeken başka bir husus da TCK 138-1'de kanuni süresi geçen verilerin yok edilmemesi durumunda, sorumlulara bir ile iki yıl arasında hapis cezası verilmesidir [19].

3.2. ISO 27001 Standardı (ISO 27001 Standard)

Yürürlükte olan mevzuatın yanı sıra dikkate alınarak süreçlerde uygulanabilecek bir başka husus olarak da standartlar ele alınabilir. ISO (International Organization for Standardization) standartlarının geliştirilmesi genellikle yaklaşık 3 yıl sürmektedir ve ISO'nun Türkiye temsilcisi Türk Standartları Enstitüsü'dür [21, 64]. Bu süre zarfında yapılan iş süreçlerinin aynı standartta olması amacıyla üye ülkelerdeki uzmanlar bir araya gelmekte ve tüm paydaşların ihtiyaçları doğrultusunda çalışmalar yapılmaktadır. Birçok uzman görüşüyle oluşan bu standartlar, standartlara uyum sağlamış olan kurumların çok daha verimli çalışmasını ve tercih edilir olmasını sağlar. Geliştirilen standartlar çalışan sayısı fark etmeksizin uygulanabilir olmaktadır ve bir işin nasıl yapılacağından çok ne yapılacağını tarif etmektedir. ISO 27001 standardı da insan kaynakları, fiziksel güvenlik, bilişim sistemleri güvenliği vb. konuları, yön verici doğrultuda kapsamakta ve Siber Güvenlik uygulama çerçevesinin temelini oluşturmaktadır [65]. ISO 27701 (Kişisel Veri Yönetim Sistemi Standardı), ISO 27002 (Bilgi Teknolojisi Güvenlik Teknikleri Standardı) gibi standartların da bilgi güvenliği düzeyini artırma hedefi bulunmakla birlikte ana çerçeve ISO 27001 üzerinden işletilmektedir.

Kamu kurumlarının gerçekleştirdiği ihalelerde ve bazı yönetmeliklerde ön şart olarak beklenen [65] ISO 27001 standardının ek maddelerinde 114 adet kontrol yer almakta olup, A.12 maddesi işletim güvenliğini ele almaktadır. Veri kaybına karşı koruma usulleri bu madde içerisinde tarif edilmiş olup kullanıcı işlemleri, kural dışılıklar, hatalar gibi olay kayıtlarının üretilmesini, saklanmasını ve düzenli olarak gözden geçirilmesinin gerekli olduğu belirtilmiştir. Bu bilgi işlem sistemlerinin saatlerinin tek bir referans zaman kaynağına göre senkronize edilmesi gerektiği de belirtilmiştir. Ayrıca sistem yedeklemelerinin sistematik bir şekilde yapılması gerektiği de belirtilen başka bir husustur. A.16 maddesi Bilgi güvenliği ihlallerini ve iyileştirmeleri ele almaktadır ve kanıt olarak kullanılabilecek bilginin teşhisi, toplanması, edinimi ve korunması için prosedürler tanımlaması ve uygulamasının gerektiği belirtilmiştir. A.18 maddesinde ilgili tüm yasal mevzuat, düzenleyici, sözleşmeden doğan şartlarıyla, kurumun bu şartlarla ilgili süreçleri yazılı bir şekilde açıkça tanımlanması ve güncel tutması gerektiği belirtilmektedir. Ayrıca kriptografik kontrollerin de bu şekilde uygulanması ve kayıtların sahtecilik, yok etme ve yetkisiz erişim gibi durumlara karşı korunması gerektiği belirtilmiştir [22]. Bu madde kapsamında mevcut ülkedeki tüm ilgili mevzuata uyum da ISO 27001'in ayrılmaz bir parçası olup, standardın ötesinde de sorumluluklar getirebilmektedir.

3.3. Bilgi ve İletişim Güvenliği Rehberi (Information and Communication Security Guide)

Kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerce bilgi ve iletişim güvenliği tedbirlerine ilişkin olarak 06.07.2019 tarihinde "Bilgi ve İletişim Güvenliği Tedbirleri" konulu Cumhurbaşkanlığı genelgesi yayımlanmıştır [23]. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) tarafından, Türkiye'de ilk defa referans doküman olma özelliği taşıyan ve güvenlik tedbirlerinin belirlenmesiyle, belirlenen tedbirlerin uygulanması için yürütülecek faaliyetlerin tanımlanması amacını taşıyan "Bilgi ve İletişim Güvenliği Rehberi" başlıklı kılavuz Temmuz 2020'de yayımlanmıştır [24].

Rehberde yer alan Ağ ve Sistem Güvenliği tedbirlerinde kayıt tutma odağında "İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi", "Siber Güvenlik Olay Yönetimi" ve "Kimlik Doğrulama ve Erişim Yönetimi" tedbirleri mevcuttur. Rehberde ağ adli bilişimi üzerine tutulacak kayıtlar ve tedbirler aşağıdaki şekilde belirtilmiştir [24]:

- DHCP sunucularında ve varsa IP adres yönetimi aracında kayıt mekanizmasının kullanılması gerekmekte olup bu durum yönetmelikle de uyum göstermektedir [14,24].
- Tüm isteklere ait URL bilgileri kaydedilmelidir.

ÖRNEK ÇALIŞMA

- Gerekli görülen durumlarda kaynak ve hedef arasındaki tüm trafik izlenebilmelidir.
- Kurum tarafından onaylanmayan veya mevzuat gereği erişimi yasak olan sitelere bağlantıyı engellemek amaçlı ağ tabanlı URL filtreleri uygulanmalıdır [14,24].
- Kayıtlar mevzuatta belirtilen süreler kadar tutulmalı ve muhafazaları için tanımlanan süre sona erince güvenli bir şekilde yok edilmelidir.
- Ağa bağlı tüm sistemlerin düzenli olarak zaman bilgisi alınmalı ve yedekli yapıda bir zaman sunucusu kullanılmalıdır.
- Yedekleme planı oluşturulmalı, plan periyodik olarak gözden geçirilmeli, yedekleme işlemleri için iz kayıtları oluşturulmalı, yedekten geri dönüş testleri yapılmalı ve yedekleme medyaları saklanmalıdır.
- Bulut hizmeti kullanımında kritik veriler yurt içinde depolanmalı, yönetimsel işlemler kayıt altına alınmalı, bulut bilişim sunucularında bulunan bellek ve disk bölgeleri otomatik olarak geri döndürülemez şekilde silinmeli ve güvenlik göstergeleri denetlenmelidir.

CBDDO tarafından hazırlanan başka bir rehber olan Bilgi ve İletişim Güvenliği Denetim Rehberinde denetim çalışmalarının belirli bir yöntemle gerçekleştirilmesi, denetimin bağımsız bir şekilde planlanması ve yürütülmesi gerektiği belirtilmiştir. Ayrıca denetim sonuçlarının CBDDO'ya gönderilmesi gerektiği belirtilen rehberde ağ üzerinden elde edilebilecek kayıtlara dair ek bir yönerge bulunmamaktadır [25].

3.4. Ağ Adli Bilişiminde Uluslararası Durum Tespiti (International Due Diligence in Network Forensics)

ENISA (The European Union Agency for Cybersecurity) Avrupa Birliği (AB) üyesi ülkelerin siber güvenlik seviyelerinin artırılması için rehberlik eden bir çatı kurumdur [31]. 2017 yılından itibaren tüm AB üye ülkeleri ulusal siber güvenlik stratejilerini açıklamaktadır. Bu stratejiler adli bilişim odaklı bilgilerden ziyade siber suçların önlenmesi amacıyla üye ülkelerle olan işbirliklerine odaklanmaktadır [32]. ENISA ayrıca yayınladığı teknik dokümanlar aracılığıyla üye ülkelerin siber güvenlik ve adli bilişim hazırlıklarını desteklemektedir. Disk, hafıza, web sunucu ve diğer dijital çevre bileşenlerinin adli bilişim süreçlerinde nasıl konumlandırılacağı bilgilerinin yer aldığı rehberlerin [26, 27, 30] yanı sıra, ağ adli bilişim süreç rehberlerinde [28, 29] verilerin nasıl toplanması gerektiğine dair bilgiler, kullanıcı ve ağ üzerinden elde edilebilecek veriler, Windows ve Linux işletim sistemlerindeki teknik öneriler ve kayıt formatlarına dair teknik öneriler bulunurken üye ülkelerin veya AB normlarının adli bilişim üzerindeki uygulanmasına dair bilgi ve tartışmalar dokümanlarda yer almamaktadır. ENFSI (The European Network of Forensic Science Institutes) ise adli araştırmalar alanında bilgi iletişim teknolojileri, ilaç ve patlayıcı gibi adli 17 teknik alt alanda [34] Avrupa'da adli araştırma konularının kalitesini artırmayı hedeflemektedir. Türkiye'de aralarında Emniyet Genel Müdürlüğü (EGM) ve Jandarma Genel Komutanlığı (JGK) Kriminal Daire Başkanlıklarının da bulunduğu dört farklı kuruluş ENFSI üyesidir [33]. Kurumun web sayfasında yer alan bilgilerde ağ adli bilişim adına bir yönlendirme veya detaylı bilgilendirme içeren rehber bulunmamaktadır.

Geleneksel ağ ve YTA adli bilişimini idari gereksinimler ışığında teknik boyutlarıyla ele alan bir çalışma literatürde olmasa da çeşitli ülkeler için adli bilişimin hukuki statüsünün incelendiği çalışmalar yapılmıştır. İtalya'daki dijital delillerin nasıl ele alınacağını belirten çalışma kişisel haklar ve kolluk kuvvetleri süreçlerini aktarmaktadır [36]. Ayrıca İtalya'da elde edilen delillerin kopyalama, yeniden üretme, bütünlük içermesi gibi konularda hukuka uygunluğunu sağlamak için yürürlükte olan yasalara değinilmiş olup adli bilişim süreçlerinin aşamalarına dair önerilerde bulunulmuştur. Çalışma ağ adli bilişiminin gelecek çalışmalar için olan önemi vurgulamaktadır ancak ağ adli bilişimi özelinde bilgi içermemektedir [43].

Latin Amerika odaklı bir çalışmada siber suçların ülkelerin kendi coğrafyalarıyla sınırlı olmadığı vurgulanmış ve sınır ötesi adli bilişim önerilerinde bulunulmuştur [37]. Ayrıca şirketlerin kendine özel şifreleme sistemlerinin ve anti-adli bilişim uygulamalarının adli bilişim süreçlerini zorladığına dikkat çekilmiştir. Adli bilişimin küresel çapta sağlıklı yapılabilmesi için süreçlerde devletler ve şirketlerin ortak paydada yer alması gerekmektedir [42].

Ülkelerin adli bilişim hazırlık seviyelerinin hazır olmasını tavsiye eden bir diğer çalışmada kanun ve standartlar özelinde ülkeler incelenmiştir. Karşılaştırmalı olarak ABD, Almanya, Birleşik Krallık ve Güney Kore gibi ülkelerin durumlarının da verildiği çalışmada uluslararası farklılıklar gözler önüne serilirken çeşitli strateji ve planlamalarla birlikte Asya ülkelerinin de siber suçlarla olan cezalara dair adımlar attığı belirtilmiştir [44]. Adli bilişimin ele alınmasında ABD'de hangi hukuk normlarının incelenmesi gerektiğine dair yapılan çalışmada ise adli bilişim süreçlerinin anayasa hukuku, ceza muhakemesi, delil hukuku, sözleşme hukuku ve mülkiyet hukuku gibi normları ele alınması gerektiği belirtilmiştir [41]. ABD'de dijital ortamlarda yapılacak incelemelerde kolluk kuvvetlerine destek olması amacıyla yasalara uyumlu bir adli bilişim sürecine ait belge ve rapor örneklerini içeren bir rehber NIJ (National Institute of Justice) tarafından yayımlanmıştır [35].

Endonezya'da siber suçlarla mücadele kapsamında adli bilişim süreci ve dijital delillerin nasıl bir süreçle ele alınacağı üzerinde durulmuş ve bir idari süreç önerilmiştir [38]. Avusturalya'da ise adli bilişim çalışmalarının devlet, kültür ve teknik gibi farklı açıları incelenmiştir. [39]. Çin'e özgü adli bilişim süreçlerini ele alan bir çalışmada delil toplama süreçlerinin doğruluk ve güvenirliğinin artırılmasına yönelik akredite edilmiş bir kurum eksikliğine dikkat çekilmiştir [40]. Suudi Arabistan'da siber suçlar kapsamında verilen para veya

ERKEN GÖRÜNÜM

hapis cezaları bilgilerinin yer aldığı çalışmada da adli bilişim süreçlerinin delilin elde edilmesi, korunması gibi kanuni yönlerden eksiklikleri olduğu belirtilmiştir. Ayrıca elde edilebilecek delillerin nerelerden, hangi yöntemlerle elde edilebileceği konusunda genel bilgiler aktarılmıştır [45]. Gana için yapılan çalışmada da benzer şekilde kanun ve kurumların adli bilişim süreçleri için yetersizliği vurgulanmış olup Birleşik Krallık ve ABD gibi gelişmiş ülkelerle işbirliğinin kapasite artırımı açısından gerekli olduğu belirtilmiştir [46].

Adli bilişim süreçlerinde Birleşmiş Milletler Genel Kurulu kişisel özgürlük ve gizliliğin korunması gerektiğini vurgularken Avrupa Komisyonu ise adli bilişimin insan hakları yönergeleriyle tam uyumlu olarak çalışması gerektiğinin altını çizmektedir [47]. Adli bilişim süreçlerinin gerçekleştirilmesi için kullanılan araçların gelişim sürecinden uygulama aşamasına kadar hukuki zemine uyması gerekmektedir [48].

AB, kişisel verilerin gizliliğini sağlamak amacıyla GDPR (General Data Protection Regulation) tüzüğünü kullanmaktadır. Uygulama katmanında hukuki temelleri ele alarak kişisel verilerin işlenmesiyle, veri katmanıyla olan haberleşmede ortaya çıkmamasını hedefleyen bir YTA tasarımı gerçekleştirilmiş olup, kontrolcünün gerçek zamanlı olarak kişisel veri erişim kontrolü yapmasına olanak sağlanmıştır. [66]. Türkiye'de bu kapsamda "Kişisel Verilerin Korunması Kanunu" (KVKK) yürürlükte olup, kişisel verilerin işlenmesinde yeni teknolojilerin yeni süreçleri ortaya çıkarması gerektiği vurgulanmış ve mevzuatta her yeni sistem için müstakil düzenlemelerin yapılması gerektiği değerlendirilmiştir [67].

Bir AB yönergesi olan EECC (European Electronic Communications Code) elektronik iletişim ağlarını düzenlemektedir. Bu yönergenin geleneksel ağlarla ilgili hususlarının YTA açısından uyarlanmasıyla elde edilecek kazanımları vardır ancak YTA özelinde fırsat değerlendirmeleri ve politikalar henüz mevcut değildir [68].

3.5. Mevzuat ve Uygulamalar Çerçevesinde Ağ Adli Bilişimi İçin Gerekli Olan İdari ve Teknik Gereksinimler (Administrative and Technical Requirements for Network Forensics in the Framework of Legislation and Practice)

Güncel mevzuat ve uygulamaların ağ adli bilişim süreçleriyle olan ilişkisi incelendiğinde mevzuattaki bilgilerin, bazı hususlar dışında, genel çerçevede ve çok fazla detay verilmeksizin tarif edildiği görülmektedir. ISO 27001 standardıyla Bilgi ve İletişim Güvenliği Rehberi ışığında yapılan değerlendirmede, süreçlerin aşağıdaki temel şartları sağlaması gerektiği sonucuna varılmıştır:

- Bilişim suçlarına karşı etkin kayıt mekanizmasının kullanılması,
- Tutulan kayıtların mevzuatta belirtilen suçları aydınlatıcı şekilde bir elektronik delil sağlanması amacıyla uyumlu olacak şekilde elde edilmesi,
- Tutulan kayıtların yedekli ve güvenli bir şekilde saklanması ve kayıtların mevzuatta belirtilen sürelerin sonunda güvenli bir şekilde imha edilmesi,
- Saklanan kayıtlarının doğruluğunu, bütünlüğünü ve gizliliğini sağlamak amacıyla güvenlik sistemlerinin, özetleme algoritmalarının, zaman damgası mekanizmalarının ve yedekli yapıların kullanılması,
- Zaman damgasının tek bir referans kaynağına göre ve elektronik imza onaylı olarak kullanılması,
- Kullanıcı işlemleri, kural dışılıklar, hatalar gibi olay kayıtlarının üretilmesi, saklanması ve düzenli olarak gözden geçirilmesi,
- Bilgi güvenliği ihlalleri ve rutin toplanan kayıtlar için hukuki normlara ve sözleşmelere uygun güncel bir süreç çerçevesinde hareket ederek bu sürecin bir denetim mekanizmasına ve gerekli görülen önlemlere tabi olması,
- Verilerin yurt içinde depolanması,
- Gizlilik içeren verilerin internet ortamına kapalı, fiziksel güvenlikli ve kayıt tutularak saklanması,
- Ağ adli bilişimi ile doğrudan ilgili olmasa da ağ verilerinin tutulduğu disklerin güvenlik ve erişim kriterlerinin belirlenmesi,
- URL bilgilerine kullanıcı oturum bilgilerinin gömülmesi,
- URL, IP adresi vb. bazlı filtreleme sistemleri kullanımı ile erişimi engellenebilmesi,
- İnternet ortamına erişimde sabit IP adresi kullanımı ve internet erişimdeki IP adresi bilgilerinin kayıt altına alınması,
- Gerekli görülen durumlarda kaynak ve hedef arasındaki tüm trafiğin izlenebilmesi için kayıt mekanizmaları (pcap vb. formatta) kurulması,
- İnternet ortamına sadece gerekli olan hizmetlerin/kullanıcıların yetkilendirilmesi,
- Abone/kullanıcı bilgilerinin (ad, soyadı, adres, telefon vb.) teknik bilgilerle eşleştirilebilir olması.

Yukarıda sıralanan genel çerçeve hususlar, odaklı olarak hangi verinin kayıt altına alınmasını belirtmemekte olup daha çok teknik süreçleri oluşturmaktadır. Mevzuata uygun trafik bilgisi kayıt sürecinin gerçekleştirilebilmesi amacıyla her türlü erişimde tüm paydaşların aşağıdaki bilgileri kayıt altına alması gerektiği değerlendirilmiştir:

- Kaynak-hedef IP adresi bilgisi,
- Port numarası ve protokol tipi bilgisi,
- Hizmetin başlama-bitiş zamanı ve türü,
- Aktarılan veri miktarı,
- Dağıtımı yapılan IP adresi bilgileri ve bu adreslerin başlama-bitiş zamanlarıyla MAC adresleri,
- Tüm URL istekleri,

ERKEN GÖRÜNÜM

- Web erişimlerinde istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgisi.

Yukarıda sıralanan idari süreçlerin ve teknik kayıt gereksinimlerinin tüm kurumlar tarafından uygulanarak, sürecin eksiksiz şekilde takip edilmesi bir zorunluluktur ve adli vakaların aydınlatılması açısından son derece önem arz etmektedir.

4. AĞ ADLİ BİLİŞİM GEREKSİNİMLERİNİN YAZILIM TANIMLI AĞ ORTAMINDA TEST EDİLMESİ VE YORUMLANMASI (TESTING AND INTERPRETATION OF NETWORK FORENSIC REQUIREMENTS IN A SOFTWARE-DEFINED NETWORK ENVIRONMENT)

4.1. Deney Ortamı ve Kapsamı (Experiment Environment and Scope)

YTA oluşturmayı ve test etmeyi amaçlayan simülatörlerin başında Mininet gelmektedir [69]. Deney ortamında sanallaştırma sistemi olarak VirtualBox [70], işletim sistemi olarak Ubuntu [71], kontrolcü olarak Ryu [72], sanal anahtar olarak OpenvSwitch [73], paket yakalama/filtreleme amaçlı program olarak Wireshark [74] kullanılmıştır. Mininet ortamında oluşturulan ağlar yerel ağları test etmek amaçlı kullanılmaktadır. Bu çalışmanın kapsamı yerel ağdaki adli bilişim kayıtlarından ziyade internet ortamını ilgilendirdiğinden dolayı Mininet ortamındaki sanal kullanıcıların da internete erişmesi gerekmekte olduğundan sanal kullanıcıların internet erişimi alması amacıyla sanallaştırma sistemindeki bağdaştırıcı ayarları güncellenmiş ve DNS ayarları sistemsel olarak değiştirilmiştir. OpenFlow 1.3. sürümü kullanan Ryu kontrolcünün kullanıldığı test ortamında deneyler tek bir kullanıcının internet erişimine odaklanacağından yüksek sayıda kullanıcılı bir topolojiye ihtiyaç duyulmamış, internet ortamına erişim kayıtlarının yanı sıra yerel ağdaki karakteristik uygulamaların da etki edip etmediğinin gözlemlenebilmesi amacıyla iki sanal kullanıcılı bir topoloji kurulmuştur. Bu çalışmadaki deneyler belirlenen yedi teknik kayıt gereksiniminin YTA ortamından elde edilebilmesi durumunu araştırmak amacıyla gerçekleştirilmiştir.

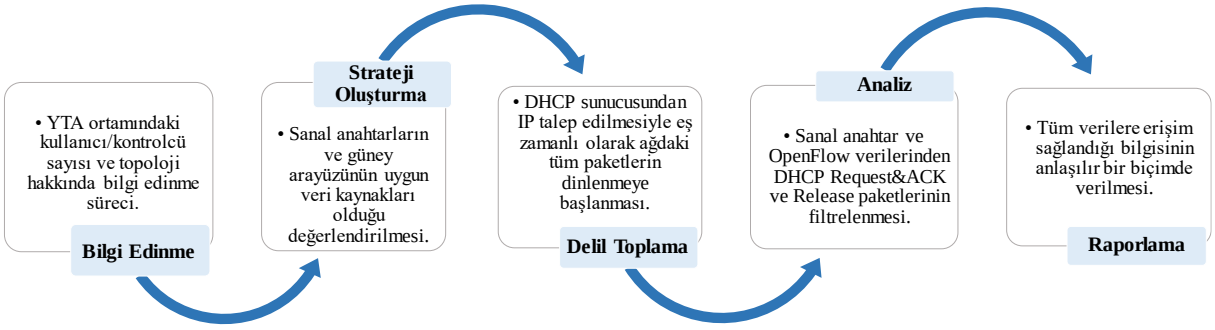
Deneyler kapsamında gerçekleştirilen süreçler OSCAR adli bilişim yöntemiyle gerçekleştirilmiştir. Bu yöntem özetle bir adli bilişim sürecinin bilgi edinme, strateji oluşturma, delil toplama, analiz ve raporlama olarak beş aşamadan oluşmasıdır. Olayın ne zaman/nasıl olduğu ve nasıl keşfedildiğine dair bilgi edinilen ilk aşamanın hukuki altyapıları da gözeterek işletilmesi gerekir. Strateji aşamasında delillerin elde edilme maliyeti ve değeri tartışıldıktan sonra, delil toplama aşamasında delillerin kendisinin elde edilerek kayıt altına alınması ve güvenli bir ortamda tutulması önemlidir. Analiz aşamasında farklı kaynaklardan gelmiş olan bilgiler, sürecin gidişatı göz önünde bulundurularak doğru şekilde ilişkilendirilmelidir. Raporlama aşamasında ise teknik bilgisi olmayan kişilerce de anlaşılabilecek şekilde bir rapor hazırlanmalıdır [59].

4.2. Otomatik IP Adresi Dağıtım Kayıtları Deneyi (Automatic IP Address Distribution Records Experiment)

Şekil 2'de gösterilen deney sürecinde, bilgi edinme aşamasında ortamın YTA olduğu, kaç kullanıcıya sahip olduğu, bu ağ ortamından bilgi elde etmek için hangi mevzuatın gerekli olduğu ele alınmalıdır. İki kullanıcı ve bir YTA kontrolcüsüne sahip olan bu ağ ortamında, kapsamı bu çalışmada belirlenen mevzuat hükümleri kapsamında araştırma yapılması kararlaştırılmıştır. Strateji oluşturma aşamasında gerekli bilgilerin elde edilmesi için sanal anahtarların ve güney arayüzünün uygun veri kaynakları olduğu değerlendirilmiştir. Delil toplama aşamasında Mininet sanal kullanıcılarından birisinin otomatik IP adresi alma talebinde bulunmasıyla birlikte sanal anahtar ve güney arayüzünde tüm paketler için dinleme başlatılmıştır. Analiz aşamasında elde edilen paketlerdeki bilgiler Wireshark yardımıyla incelenmiş ve sanal anahtarlar üzerinde "DHCP REQUEST" ve "DHCP ACK" paketlerine erişim sağlanmıştır. İlgili paketlerde IP talep eden cihazın MAC adresi bilgisi, aldığı IP adresi bilgisi ve IP adresi alma zamanına erişilmiştir. Ayrıca OpenFlow paketleri de incelenmiş olup bu paketlerde de giriş ve çıkış yapan paket detaylarında otomatik IP adresi alma süreciyle ilgili sıralanan detaylara erişilmiştir.

Mevzuat ve uygulamalarda IP adresinin başlangıç zamanının yanı sıra bitiş zamanına dair de bilgi

ERKEN GÖRÜNÜM



Şekil 2. Otomatik IP adresi deney süreci (Automatic IP address testing process)

gerekmekte olduğu değerlendirildiğinden ayrıca Mininet sanal kullanıcısı üzerinde DHCP adresinden vazgeçme süreci de test edilmiş olup bu durumun da kayıtlara yansıyıp yansımadığı paket dinlemeleri ile incelenmiştir. Bu kapsamda ağ üzerinden elde edilen paketler incelendiğinde ise "DHCP RELEASE" paketlerinin de gerekli tüm detaylarıyla hem sanal anahtarlar hem de OpenFlow paketleri içerisinde yer aldığı ve tespit edilebildiği görülmüştür. Bu doğrultuda aynı IP adresini başka bir MAC adresine sahip kullanıcı almadığı sürece bu IP adresini aynı kişi kullanmış olarak kabul edilebilir. Yapılan IP adresi dağıtımı testlerinde dağıtılan IP adreslerine YTA sistemleri üzerinden erişim hususunda bir eksiklik bulunmamakla birlikte, bu durumun bir süreç haline getirilerek bu bilgilerin uzak bir sunucuya iletilmesi veya merkezi bir DHCP sunucusu kullanılarak kayıtların bu sunucuda tutulmasının gerekli ve faydalı olacağı değerlendirilmiştir.

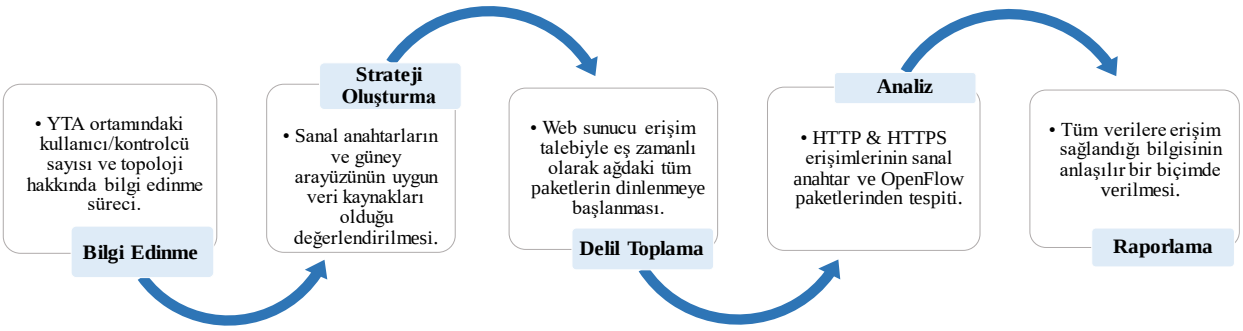
4.3. HTTP/HTTPS Erişim Deneyleri (HTTP/HTTPS Access Experiments)

Şekil 3'te gösterilen HTTP/HTTPS deneyleri kapsamında bilgi edinme ve strateji oluşturma aşamaları bir önceki deneyle aynı olup deney kapsamında delil toplama aşamasında incelenecek trafik için URL istekleriyle GET-POST ve sonuç bilgilerine erişim denemeleri gerçekleştirilmiştir. Bu aşamada tüm paketler kayıt altına alınmıştır. GET işlemleri için "wget" modülü kullanılmıştır. Analiz aşamasında sorgu yapılan bir web sayfasında ön tanımlı olarak HTTPS iletişimi gerçekleştiği tespit edilmiş olup, paket incelemeleri sonucunda, bu bağlantıyı güvenli hale taşıyacak olan el sıkışma ve şifreleme süreçlerinin (The Transport Layer Security (TLS) Protocol Version 1.3) gerçekleştiği tespit edilmiştir. HTTPS bağlantısı kurulmadan önce gerçekleşen ve güvenli bağlantı olarak talep edilmeyen DNS sorgusundan hangi web sayfasının talep edildiği, hangi IP adresine ve MAC adresine sahip olan kullanıcının bu bilgileri talep ettiği bilgisi görülmüştür. Ancak şifreli gerçekleşen diğer süreçlerde, gerekli kriptografik anahtar bilgilerine sahip olunmadan tüm bağlantı bilgilerine erişmek mümkün görünmemektedir.

Mevzuatta belirtilen kapsamın HTTP erişimleri olduğu değerlendirilmiş olup süreçlere bu kapsamda devam edilmiştir. GET paketleri denemesi için "wget", POST bilgisi elde edilmesi içinse "curl" kullanılan deney ortamında, POST paketlerinde doğası gereği bir veri (anlamlı bir kelime) iletimi de sağlanmış olup paketler içerisinde ilgili kelime bilgisinin bulunup bulunmadığı da test edilmiştir. Her iki denemede de GET ve POST taleplerine ve taleplerin başarı ile sonuçlandığına dair bilgilere, kaynak-hedef bilgilerine, IP adresi, MAC adresi bilgilerine, URL bilgilerine, zaman bilgilerine erişimin sanal anahtar üzerinden sağlandığı raporlanmıştır. Ayrıca POST paketi içerisinde iletilen anlamlı kelime paketlerde yapılan inceleme sonucu erişilmiş olup etkin bir dinleme ile iletilen bilgilerin de sanal anahtarlar üzerinden erişilebilir olduğunu kanıtlamaktadır. OpenFlow paketlerinde zaman bilgisinin yanı sıra kaynak ve hedef bilgisi de yer almaktadır. OpenFlow paketlerinde erişime ait GET-POST işlemlerine dair detay bilgiler, GET-POST komutları HTTP talep türü olduklarından dolayı doğası gereği elde edilememiş olsa da paketlerin yorumlanmasıyla bu sürecin bir HTTP talebi olduğu bilgisi elde edilmiştir.

4.4. Yazılım Tanımlı Ağlarda URL Filtreleme (URL Filtering on Software-Defined Networks)

Bir diğer gereksinim olarak tespit edilen URL filtreleme hususunda ise kontrolcüde erişim listesi benzeri bir yapılandırma ile IP adresi ve protokol bazlı bir filtrelemenin kontrolcü tabanlı bir modülle yapılabildiği görülmüştür [75]. Bu doğrultuda ek bir filtreleme sistemine ihtiyaç duyulmadan bir web sayfasına erişimin engellenebileceği görülmektedir. Ancak URL filtreleme yapılabilmesi için engellenmesi talep edilen hedeflerin URL bilgilerinin isim sorguları yapılarak güncel şekilde kontrolcüye iletilmesi ve otomatik şekilde IP adreslerinin engel listesine eklenmesi gerekmektedir. Pratikte bir web sayfası genellikle alt alan adlarıyla birlikte aynı IP adresini kullanmaktadır. Mevzuatta içerik filtrelemenin, öncelikli olarak bir web sayfasının erişim engeli alınan bölümü için yapılması, eğer bu durum teknik olarak mümkün değilse tüm web sayfasına erişimin engellenmesi beklenmektedir. Bu kapsamda değerlendirildiğinde, erişimin tamamen engellenmesi durumunun mevzuatta beklenen ilk şartı sağlamadığı ve kontrolcü tabanlı olup doğrudan URL tabanlı filtreleme yapabilen bir modül geliştirilmesinin ve işletilmesinin



Şekil 3. HTTP/HTTPS erişimi deney süreci (HTTP/HTTPS access test process)

ERKEN GÖRÜNÜM

fayda sağlayacağı değerlendirilmiştir. Kontrolcü tabanlı olarak URL filtreleme işleminin gerçekleştirilememesi durumundaysa merkezi bir URL filtreleme sisteminin kurulması zaruridir.

4.5. Yazılım Tanımlı Ağ Deneylerinin Raporlanması ve Delil Kaynaklarının Değerlendirmesi (Reporting of Software Defined-Network Experiments and Evaluation of Evidence Sources)

Ağ adli bilişim gereksinimlerinin YTA ortamında test edilmesi ve yorumlanması kapsamında gerçekleşen deneyler ve yapılan araştırmalar sonucunda, teknik kayıt gereksinimlerinin sanal anahtarlar ve OpenFlow paketlerinden elde edilebildiği görülmüştür. İlgili kayıtlara dair bilgiler sanal anahtar paketlerinde doğrudan görünür durumdayken doğası gereği OpenFlow paketlerinden GET-POST komut detayları ve aktarılan veri miktarı detaylı paket incelemeleri ve yorumlarla elde edilmiştir.

YTA'yı geleneksel ağlardan ayıran temel unsurlar kontrolcü ve sanal anahtarlardır. Sanal anahtarlar kontrolcü tarafından belirlenen kuralları işletmekle yükümlüdür [76]. Sanal anahtarlar da geleneksel anahtarlarla aynı kapsamda sadece geçici olarak komşuluk tabloları gibi bilgileri içermektedir. Bu veriler ağ cihazları üzerinde geçici süre yer almaktadır. İlgili veriler NetFlow ve Sflow gibi akış tabanlı sistemlerle de elde edilebilir. Bu sistemler kullanım amacına bağlı olarak örnekleme yapma yeteneğine sahip olsalar da [77] mevzuattaki teknik kayıt gereksinimlerini yerine getirmek için her paketin kayıt altına alınması gerekir. Geleneksel ağlarda olduğu gibi YTA kullanılan ağlarda da güvenlik duvarı, saldırı tespit sistemi gibi çevre birimlerinin yardımıyla delil elde etmek mümkündür.

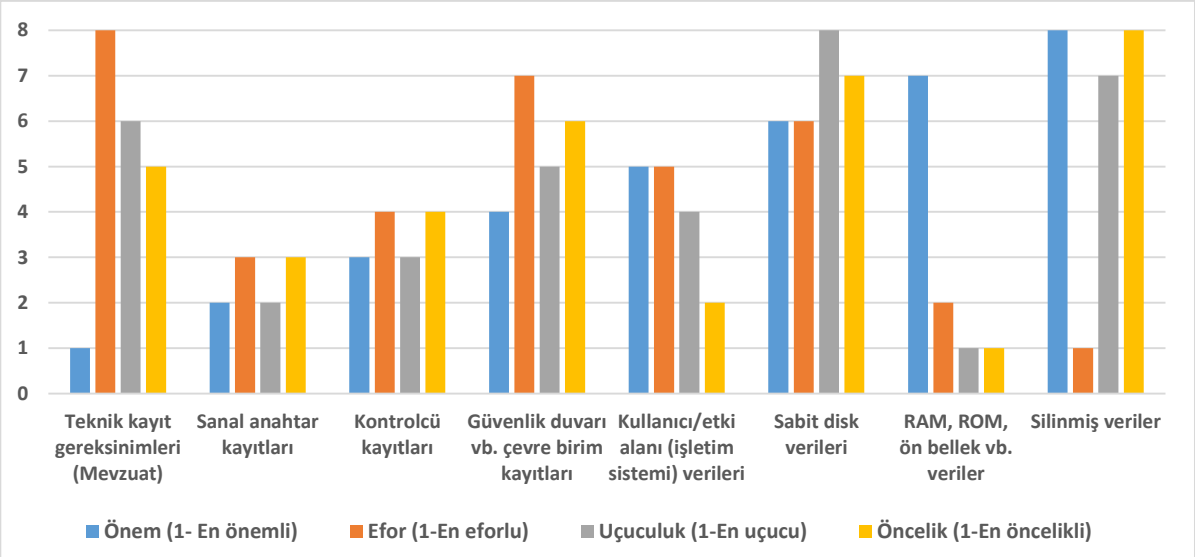
Bölüm 2.2'de incelenen ağ adli bilişiminde delil kaynakları YTA ortamında çevre birimler de göz önünde bulundurularak önem, efor, uçuculuk ve öncelik açısından Şekil 4'te yer alan sekiz başlık altında toplanmış ve birbirleriyle kıyaslanmıştır. YTA ağlarından elde edilmesi belirlen yedi teknik kayıt gereksinimi mevzuat kapsamında toplanması zorunlu veriler olduğundan, benzer paket inceleme süreçleriyle elde edildiğinden ve güvenli bir şekilde muhafaza edilme zorunluluğu olduğundan teknik kayıt gereksinimlerinin kendi arasında denk önem, efor, uçuculuk ve önceliğe sahip olduğu değerlendirilmiştir.

YTA ortamında ve çevre birimlerde arama süreçlerinin gerçekleştirileceği durumda teknik kayıt gereksinimlerinin adli ve idari sorumlulukları yerine getirmek açısından, yasal dayanak ve zorunluluk da ele alındığında en fazla öneme sahip olduğu sonucuna varılmıştır. Ayrıca geçmişe yönelik bir incelemede teknik kayıt gereksinimleri zaten elde edilmiş olacağından dolayı en az eforla elde edilebilecektir. En yüksek efor gerektiren sürecin ise silinmiş verilerin kurtarılarak incelenmesi olduğu değerlendirilmiştir.

En uçucu bilgileri içerdiği bilinen RAM bölgesinden erişilebilecek bilgiler arasında arama tanımlaması içerisinde yer alan bilgiler bulunduğu düşünülüyorsa bunlara öncelik tanınması gerekmektedir. Sanal anahtar, kontrolcü, kullanıcı ve güvenlik duvarı kayıtlarından elde edilecek delillerin de, zaten elde edilmiş ve saklanması zorunlu olan teknik kayıt gereksinimleri delillerinden daha uçucu oldukları değerlendirilmiştir.

Uçuculuk ve öncelik arasında yakın bir ilişki olduğu değerlendirilse de her durumda daha uçucu olan delil kaynağına öncelik verilmesi doğru değildir. Bu sebepten Şekil 4'te gösterildiği gibi, faydalı delil içerebilme durumları da göz önüne alınarak öncelik sıralaması yapılmıştır. Örneğin silinmiş verilerin üzerine yeni veri yazılması durumunda tekrar elde edilmesi daha da zorlaşabilir veya imkânsız olabilir. Bu sebepten silinmiş

İNCELEME



Şekil 4. Yazılım tanımlı ağlarda delil kaynaklarının önem, efor, uçuculuk ve öncelik açısından karşılaştırmalı grafiği (Comparative graph of software-defined network evidence sources in terms of importance, effort, volatility, and priority)

veriler, sabit diskte yer alan silinmemiş diğer bilgilere göre daha uçucu olarak değerlendirilebilirken daha az önceliklidir. Güvenlik duvarından elde edilebilecek detay bilgilerin tamamı mevzuat kapsamında belirlenen süre kadar saklanmak zorunda olmadığından teknik kayıt gereksinimlerine göre daha uçucu olabileceği halde, elde edilebilecek bilgiler göz önüne alındığında daha az öncelikli olduğu değerlendirilmiştir. Belirlenen sekiz başlığa dair önem, efor, uçuculuk ve öncelik karşılaştırılması Şekil 4'te sunulmuştur.

5. TARTIŞMA VE ÖNERİLER (DISCUSSION AND RECOMMENDATIONS)

Mevzuat ve uygulamaların detaylıca incelendiği bu çalışma kapsamında bu süreçlerin, ortaya çıkan gereksinimlerin ardından oluşturulduğu değerlendirilmiştir. Mevzuat hazırlama zaman alabilecek süreçler içerdiğinden dolayı genel çerçevelerle hazırlanan üst normların gereksinim duyulduğu anda alt basamak normlarla hızlıca şekillendirilmesi, teknolojinin hızlı gelişimine paralel olması açısından önemlidir. Mevzuat ve uygulamalar birbirini doğrular (Ör: otomatik IP dağıtım bilgilerinin tutulması ve URL filtreleme [14,24]) ve sıralı bir şekilde oluşturulmuştur. ISO 27001 standardı da ilgili ülke yasa ve kriterlerine uyum sağlanması gerektiğini belirtmektedir.

Mevzuatta bazı hususlar net bir şekilde ele alınmışken hiçbirinde [13-19,23,25] kayıt formatı belirlenmemiştir. Bu durum farklı üreticilerin cihazlarını kullanan yapılar açısından fayda sağlayacak olup, tek bir markanın ürününe duyulabilecek ihtiyacı bertaraf etmiştir. CMK'da yer alan delil elde etme, özet alma teknikleri, veri kurtarma teknikleri gibi hususların detaylandırılmamış olması da genel çerçeveden bir yapı oluşturduğunda faydalı olarak değerlendirilebilir. Ancak bilimselliği ispatlanmış yöntemlerin sabit bir politika olarak uygulanması, standardı sağlama açısından faydalı olacaktır. Öte yandan vekil sunucu trafik bilgisi beklentisinde [16] olduğu gibi, spesifik beklentilerin ardından benzeri bilgilerin de kayıt altına alınması gerektiğini belirten hükümler ise belirsizliklere yol açabilecektir. Mevzuatta belirtilen GET, POST bilgilerinin kayıt altına alınması [15] yapısı gereği sadece HTTP bağlantılarında gerçekleştirilebilir. HTTPS yayınlarını kullanıcı cihazlarına sertifika yükleyip araya girerek dinlemek mümkün olsa da bu sürece dair mevzuat hükmü bulunmamaktadır. Bu durumun hukuki altyapısı da ayrıca gözden geçirilmelidir.

Tutulan kayıtların mevzuatta belirlenen sürelerden sonra yok edilmesi gerekmektedir [19,24]. Bu kapsamdaki işlemin fiziksel yok edilme olmadığı, kayıtların geri döndürülemez şekilde silinmesi olduğu yönünde yorumlama yapılmıştır. Bu silme yöntemine dair bir standardın (diske kaç defa üzerine yazma işlemi yapılacağı ve hangi yöntemle uygulanacağı vb.) belirlenerek politika olarak uygulanmasının sağlıklı olacağı değerlendirilmiştir.

Ağ adli bilişim gereksinimlerini tespit için çok sayıda kaynak [13-25] yerine tek bir referans adli bilişim rehberi olmasının süreç sağlığı açısından faydalı olacağı değerlendirilmiştir. Bu rehberin bağlayıcı bir doküman olması kurumların hukuki olarak yerine getirmeyi atlayabilecekleri hususları hatırlatıcı bir doküman olacağından, meydana gelebilecek adli ve idari yaptırımların önüne geçilecektir. Kapsamı bu makalede önerilen ağ adli bilişim süreci mevzuat hükümlerince zaten toplanması zorunlu olan veriler üzerine inşa edilmiş olduğundan, bu tarz bir rehbere öncülük edebileceği ve adli bilişim uzmanlarına yol gösterebileceği düşünülmektedir.

Türkiye'de lisans ve lisansüstü düzeyde adli bilişim programları mevcut olup, kamu kurumları da araştırmalar yürütmektedir. EGM, JGK, Adalet Bakanlığı ve TÜBİTAK bu kurumlar arasında yer almakta olup kamu kurumlarıyla birlikte özel sektöre ait kaynaklar ve insan gücünün de kullanımıyla birlikte süreçlerin daha sağlıklı ilerleyebileceği değerlendirilmiştir [4]. Artan siber suçlar ve adli bilişimin çok yönlü süreçleri göz önüne alındığında adli bilişim süreçlerinden sorumlu bir kurum belirlenmesi veya yeni bir kurum oluşturulması da planlanabilir. Bu kurumun mevzuat geliştirilmesinde ve adli bilişim süreçlerinin oluşturulmasında/takibinde ana misyonu yüklenmesi, süreçlerin tek elden ve standart şekilde gerçekleştirilmesine olanak sağlayabilecektir.

Uluslararası çapta diğer ülkeler için gerçekleştirilen araştırmalarda ağ adli bilişiminin bu çalışmada yapıldığı gibi ulusal mevzuata uyumunun teknik açıdan değerlendirildiği bir çalışma mevcut değildir. YTA açısından mevzuatın durumunu sorgulayan bir çalışma da bulunmamaktadır. YTA politikaları henüz AB'de de mevcut değildir [68]. Diğer ülkelerde de çeşitli eksiklikler vurgulanmış olup [42,45,46] adli bilişimin çözümünün tek bir ülkeden geçmediği, doğası gereği sınır ötesi bir sürecin gerekli olduğu sonucuna varılmıştır [37,42]. Türkiye'de incelenen mevzuatlarda verilerin yurt içinde saklanması gerektiğine dair bilgiler mevcut olup [24] ülkeler arası adli bilişim süreçlerine uyum için çalışmaların yapılması önem arz etmektedir. Bu çalışmalarda, yazılım geliştiren şirketlerle işbirliği yapılabilmesi durumunun da göz önünde bulundurulması süreç açısından sağlıklı olacaktır [42]. Ayrıca yurt dışı örneklerde olduğu gibi adli bilişim rehberlerinin [28,29,35] yayınlaması ve kişisel verilerin korunması süreçlerinin her aşamada göz önünde bulundurulması da faydalı olacaktır.

Tespiti yapılan gereksinimlerin tamamının YTA ortamında yapılabildiği, deney sonuçlarıyla görülmüştür. Deneyler kapsamında elde edilen paketlerin incelenmesi sonucunda, mevzuatta beklenen erişimlerin OpenvSwitch sanal anahtarlar ile elde edilebildiği net olarak ortaya konulmuştur. Bu durum farklı sanal anahtarlar kullanıldığında farklılık gösterebilir. Ancak çalışma prensipleri göz önüne alındığında diğer standartlaşmış sanal anahtarların da geleneksel ağ yapısındaki standartlaşmış protokolleri kullanması

İADE-İ GÖRÜNÜM

sebebiyle sonucun farklı olmayacağı değerlendirilmiştir. Sadece OpenFlow paketlerine odaklanıldığında ise mevzuatta özellikle belirtilmiş olan bazı bilgilere erişim, GET-POST paketlerinin yapısı gereği gerçekleştirilememiş olsa da teknik yorumlarla birlikte sonuca erişilebildiği görülmüştür. Adli bilişim süreçlerinin sadece OpenFlow paketleri vasıtasıyla yapılıp yapılmayacağının tek başına bir başka araştırma konusu olabileceği değerlendirilmektedir. Gerçekleştirilen tüm deneylerdeki paket dinlemelerinde yakalanan tüm paketlerin %29'unun OpenFlow paketleri olduğu ve ayrıca yakalanan tüm paketlerin toplam boyutunun da %14'ünün OpenFlow paketlerine ait olduğu gerçekleştirilen deneylerde görülmüştür. Yapılan deneylerin kapsamına (OpenFlow sürümü, topoloji, kontrolcü vb.) göre bu oranların değişebileceği bir gerçek olmakla birlikte, sadece OpenFlow paketleri üzerine kurulacak bir adli bilişim sürecinin incelenecek paket sayısı ve boyutu anlamında büyük avantaj sağlayacağı değerlendirilmiştir. Bu şekilde daha merkeziyetçi ve üreticiden bağımsız bir yapı elde edilebilir. Şu an yürürlükte olan mevzuatta ağın bu bölgesinden elde edilen verilere dair bir bilgi bulunmadığından hayata geçirilecek mevzuat ve süreçlerde OpenFlow vb. güney arayüzü verilerinden de faydalanabileceğinin vurgulanmasının hukuki anlamda da destekleyici olacağı değerlendirilmiştir.

YTA'nın, ağ yönetimini kolaylaştırmanın [78] yanı sıra, adli bilişim süreçlerinde gerekli olan delillerin elde edilmesine de imkân verdiği bu çalışmada gösterilmiştir. Veri trafiğine ilişkin kayıtların ağdan eksiksiz bir şekilde alınması ve saklanması, makine öğrenmesi veya derin öğrenme tabanlı saldırı tespit yöntemlerinin performansı [79] ve bir sonraki saldırının gerçekleşme zamanının tahmini [80] için büyük önem teşkil etmektedir. YTA'nın doğru kullanımıyla birlikte adli bilişim süreçlerinde daha etkili analiz kabiliyetine ulaşılabileceği değerlendirilmektedir. Bununla birlikte, YTA'da adli bilişim uygulamalarını Türkiye'deki mevzuat ve uygulamalara uygun şekilde gerçekleştirmek için belirlenen süreçlerin karmaşık ve takip edilmesi zor bir durum oluşturma riski bulunmaktadır. Bu nedenle, süreçlerin teknik takibinin otomatik şekilde yapılmasını sağlayacak modüllerden oluşan merkezi YTA yönetim sisteminin geliştirilmesinin faydalı olacağı ve oluşacak sistemin aşağıdaki asgari şartlara uyum göstermesi gerektiği değerlendirilmiştir:

- Gerekli olan verilerin kurum/kuruluşun niteliği kapsamında belirlenmesi,
- Uygulayıcı ve denetleyici birimlerin sorumluluklarının yazılı olarak belirlenmesi ve yetkili personele tebliğ edilmesi,
- YTA üzerinden geçen paketlerin (sanal anahtarlar ve OpenFlow paketleri) canlı olarak kayıt altına alınması,
- Aktarılan veri miktarının kayıt altına alınması,
- Teknik kayıt gereksinimlerinin otomatik bir şekilde filtrelenerek (veri boyutunun büyümemesi açısından) merkezi bir sunucuya iletilmesi,
- Merkezi sunucuda teknik bilgilerle abone/kullanıcı bilgilerinin eşleşmesinin güvenli bir şekilde gerçekleştirilmesi,
- Kayıt altına alınan tüm verilerin elektronik imzalı şekilde özetlenmesi ve zaman damgalı şekilde saklanması,
- Erişim engellenmesi ve içerik filtreleme amaçlı, URL bazlı da çalışabilecek ve kısmi engelleme yapabilecek, donanım ve yazılımların çalıştırılması,
- Yurt içinde tutulan merkezi sunucunun ve veritabanlarının yedekli ve güvenli bir ortamda yedekli şekilde muhafaza edilmesi,
- Saklanan verilerin mevzuatta belirtilen sürelerin sonunda güvenli bir şekilde imha edilmesi.

6. SONUÇ (CONCLUSION)

Ağ adli bilişim süreçlerinin mevzuat ve uygulamalar kapsamında, bilirkişilik süreçleri ve uluslararası durumlar da ele alınarak ilk defa incelendiği bu makalede ağ adli bilişim gereksinimlerinin YTA'daki durum tespiti ilk defa gerçekleştirilmiştir. Deney sonuçları, geleneksel ağlar için belirlenmiş olan ağ adli bilişim süreçlerinin YTA'da da uygulanabilir olduğunu göstermiştir. Ayrıca güney arayüzü verileriyle, toplam trafiğin sadece %14'ü ile gerekli bilgilere erişimin mümkün olduğu gözlemlenmiş olup YTA adli bilişiminde güney ara yüzü verilerinin hukuksal olarak tam geçerli olması için çalışmalar yapılması gereklidir.

Ağ adli bilişim çalışmalarının bilgi edinme, strateji oluşturma, delil toplama, analiz ve raporlama olarak beş aşamadan oluşması gereklidir ve mevzuat kapsamında toplanması gereken YTA delillerinin en az eforla elde edilebilen ve en önemli veriler olduğu gösterilmiştir. Tüm çevre sistemler ele alındığında, bir YTA ortamında en uçucu bilgilerin RAM bölgesinden erişilebilecek bilgiler olduğu, en çok eforla elde edilebilecek bilgilerinse silinmiş veriler olduğu görülmüştür. Bu sonuçlarla ağ adli bilişim bilirkişilik süreçlerine de katkılar sunulmuş olup, süreçlerin zaten kaydı mevzuat kapsamında tutulması zorunlu olan bilgiler üzerinden ilerletilmesinin sağlıklı olacağı değerlendirilmiştir.

Mevzuatın birbiriyle uyumlu olduğu ve teknik açıdan yeterli olduğu görülmüştür. Uluslararası standartlarla diğer ülke mevzuatlarına dair çalışmalar incelendiğinde, sınır ötesi adli bilişim süreçlerinin ve yazılım geliştiren şirketlerin bilgi paylaşım sorumluluklarının hukuki ve teknik açıdan oluşturularak, adli bilişim hazırlık seviyesinin artırılması gerektiği sonucuna varılmıştır.

YTA adli bilişim gereksinimlerinin Türkiye'de otomatik olarak işletileceği, milli bir YTA modülünü oluşturmak gelecek çalışma hedeflerimiz arasındadır. Uluslararası düzeyde teknik ve idari ağ adli bilişim çalışmalarının YTA odağında ilk defa incelendiği bu çalışmada, kişisel verilerin korunduğu kabul edilmiştir. Bu çalışmadaki öneri ve sonuçlardan faydalanarak KVKK ile tam uyumlu, kişisel verilerin korunmasını sağlayacak YTA

EKLENİ GÖRÜNÜM

modülü geliştirme çalışmaları gerçekleştirilebilir. Ayrıca bu çalışmanın kurumsal düzeyde hazırlanacak YTA adli bilişimi rehberlerine ve kurumların YTA adli bilişimi odağında rol ve sorumluluklarının belirlenmesinde yol gösterici nitelikte olacağı değerlendirilmektedir.

ETİK STANDARTLARIN BEYANI
(DECLARATION OF ETHICAL STANDARDS)

Bu makalenin yazar(lar)ı çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler.

YAZARLARIN KATKILARI (AUTHORS' CONTRIBUTIONS)

Altuğ ÇİL: Amaç ve hedeflerin belirlenmesi, araştırmanın ve deneylerin yapılması, görselleştirme, analiz, sonuçların elde edilmesi ve makale yazımı. / Setting goals and objectives, conducting research and experiments, visualizing, analyzing, obtaining results and writing article.

Mehmet DEMİRCİ: Doğrulama, denetim, süreç yönetimi, inceleme ve makale yazım düzenlemesi. / Validation, audit, process management, review and article editing.

ÇIKAR ÇATIŞMASI (CONFLICT OF INTEREST)

Bu çalışmada herhangi bir çıkar çatışması yoktur. / There is no conflict of interest in this study.

KAYNAKLAR (REFERENCES)

[1] Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, ***Türkiye İstatistik Kurumu (TÜİK)***, (2021).

[2] Dijitalleşen Dünyada Bilişim suçları ve Mücadele Yöntemleri, ***Bilgi Teknolojileri ve İletişim Kurumu (BTK)***, (2022) .

[3] Yazılım Tanımlı Ağlar Küresel Pazar araştırması, ***Markets and Markets***, İnternet: https://www.marketsandmarkets.com/Market-Reports/software-defined-networking-sdn-market-655.html#:~:text=%5B465%20Pages%20Report%5D%20The%20global,productivity%20for%20field%2Dbased%20services , (Erişim Tarihi: 03.07.2022)

[4] Akbal E. and Güneş F., "Adli Bilişim Mühendisliği Eğitiminin Kurumlar Açısında Önemi", ***Düzce Üniversitesi Bilim ve Teknoloji Dergisi***, 4: 395-402, (2016).

[5] Özen M. and Özocak, G. "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)", ***Ankara Barosu Dergisi***, 1: 43-77, (2015).

[6] Yılmaz F. and Güllüpınar F., "Türkiye'de Bilişim Suçlarının Kriminolojik Açıdan Değerlendirilmesi: Bilişim Suçlarının Hukuksal ve Sosyolojik Boyutlarının Analizi", ***Uluslararası Toplum Araştırmaları Dergisi (OPUS),*** 15-1: 5371-5409, (2020).

[7] Değirmenci O., "Adli Bilişimde Önceliklendirme (Triyaj)Yönteminin Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi", ***Bilişim Hukuku Dergisi***, 2:47-49, (2020).

[8] Önel B. ve Irmak E., "Adli bilişim ve dijital delillerin windows işletim sistemi üzerinde incelenmesi", ***Politeknik Dergisi***, 24(3): 1187-1196, (2021).

[9] Gençoğlu M.T. ve Sert Ç., "Siber Olaylara Müdahale ve Analiz Süreci", ***Fırat Üniversitesi Müh. Bil. Dergisi,*** 33(2):471-479, (2021).

[10] Yılmaz F. ve Çakır H., "Karar Destek Sistemlerinin Mobil Cihaz Adli Bilişimi Süreçlerine Uygulanmasına Yönelik Bır Öneri Çalışması", ***Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,*** 7(1):24-45, (2021).

[11] Çakır H. ve Kılıç M.S., "Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış", ***Polis Bilimleri Dergisi***, 15(3):23-44, (2013).

[12] Emekci A., Kuğu E. Ve Temiztürk M., "Adli Bilişim Ezberlerini Bozan Bir Düzlem: Bulut Bilişim", ***Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,*** 2(1):8-14, (2016).

[13] 5651 sayılı kanun, "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", (2007).

[14] "İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik", (2007).

[15] "Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik", (2007).

[16] "İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik", (2007).

[17] 7253 sayılı kanun, "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun", (2020).

[18] 5809 sayılı kanun, "Elektronik Haberleşme Kanunu", (2008).

[19] 5237 sayılı kanun, "Türk Ceza Kanunu", (2004).

[20] 5271 sayılı kanun, "Ceza Muhakemesi Kanunu", (2004).

[21] ISO Members, ***International Organization for Standardization (ISO)***, https://www.iso.org/members.html .

[22] ISO 27001 EK-A Maddeleri, ***İnternet***:https://www.baib.gov.tr/files/downloads/PageFiles/9d398db4-4a83-41f5-9dc7-002fa6c5248f/Files/27001%20ek-a%20maddeleri.pdf , (Erişim Tarihi: 03.07.2022).

[23] Bilgi ve İletişim Güvenliği Tedbirleri, ***30823 sayılı Cumhurbaşkanlığı Genelgesi***, (2019).

[24] Bilgi ve İletişim Güvenliği Rehberi, ***CBDDO***, (2020).

[25] Bilgi ve İletişim Güvenliği Denetim Rehberi, ***CBDDO***, (2021).

[26] Forensic analysis Local Incident Response Handbook, Document for teachers, ***ENISA***, (2016).

[27] Forensic Analysis Webserver analysis Handbook, Document for teachers, ***ENISA***, (2016).

[28] Forensic analysis Network Incident Response Handbook,Document for teachers,***ENISA***,(2016).

[29] Introduction to Network Forensics Final v1.1, ***ENISA***, (2019)

ERKEN GÖRÜNÜM

[30] Digital forensics Handbook, Document for teachers, ***ENISA***, (2013).

[31] National Cybersecurity Strategies, ***ENISA***, https://www.enisa.europa.eu/topics/national-cyber-security-strategies .

[32] National Cyber Security Strategies - Interactive Map, ***ENISA***, İnternet: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map .

[33] The European Network of Forensic Science Institutes, ***ENFSI***, https://enfsi.eu/.

[34] Expert Working Groups, ***ENFSI***, https://enfsi.eu/about-enfsi/structure/working-groups/.

[35] Forensic Examination of Digital Evidence: A Guide for Law Enforcement, ***NIJ***, (2004).

[36] Bartoli L. And Lasagni G., "The Handling Of Digital Evidence In Italy", Digital Forensic Evidence: Towards Common European Standards in Antifraud Administrative and Criminal Investigations, ***Wolters Kluwer/CEDAM,*** 87-121, (2021).

[37] Perez L.C.D., Resendiz A.L.Q.,Alvarez G.V. and Medina R.V., "A review of cross-border cooperation regulation for digital forensics in LATAM from the soft systems methodology", ***Applied Computing and Informatics***, Vol. ahead-of-print No. ahead-of-print, (2022).

[38] Prayudi Y., Ashari A. and Priyambodo T.K., "A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia", ***I. J. Computer Network and Information Security,*** 11:1-8, (2015).

[39] Elyas M., Maynard S.B.,Ahmad A. and Lonie A., "Towards A Systemic Framework for Digital Forensic Readiness", ***Journal of Computer Information Systems***, 54(3):97-105, (2014).

[40] Guo H. and Hou J., "Review of the accreditation of digital forensics in China", ***Forensic Sciences Research***, 3(3):194-201, (2018).

[41] Nance K. and Ryan D.J., "Legal Aspects of Digital Forensics: A Research Agenda", ***44th Hawaii International Conference on System Sciences***, Hawaii, 1-6, (2011).

[42] Losavio M.M.,Pastukov P., Polyakova S., Zhang X., Chow K.P., Koltay A., James J. And Ortiz M.E., "The juridical spheres for digital forensics and electronic evidence in the insecure electronic world", ***WIREs Forensic Science,*** 1(5):1-13, (2019).

[43] Fenu G. and Solinas F., "Computer Forensics Between The Italian Legislation and Pragmatic Questions", ***International Journal of Cyber-Security and Digital Forensics,*** 2:9-24, (2013).

[44] Park S., Akatyev N., Jang Y., Hwang J., Kim D., Yu W., Shin H., Han C. and Kim J., "A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement", ***Digital Investigation***, 24:93-100, (2018).

[45] Al-Murjan A. and Xynos K., "Network Forensic Investigation of Internal Misuse/Crime in Saudi Arabia: A Hacking Case", ***Annual ADFSL Conference on Digital Forensics, Security and Law,*** 1:15-32, (2016).

[46] Apau R. and Koranteng F.N., "An overview of the digital forensic investigation infrastructure of Ghana", ***Forensic Science International:Synergy***, 2:299-309, (2020).

[47] Karyda M. and Mitrou L., "Internet Forensics: Legal and Technical Issues", ***Second International Workshop on Digital Forensics and Incident Analysis,*** Greece**,** 3-12, (2007).

[48] Adams C.W., "Legal Issues Pertaining to the Development of Digital Forensic Tools", ***Third International Workshop on Systematic Approaches to Digital Forensic Engineering***, Oakland, 123-132, (2008).

[49] Atalay N. S., Doğan Ş., Akbal E. and Tüncer T., "Adli Bilişim Alanında Ağ Analizi", ***BEÜ Fen Bilimleri Dergisi***, 8 (2): 582-594, (2019).

[50] Shrivastava G., Sharma K. and Kumari R., "Network Forensics: Today and Tomorrow", ***IEEE International Conference on Computing for Sustainable Global Development (INDIACom)***, New Delhi-India, 2234-2238, (2016).

[51] Rawat D. B. and Reddy S. R., "Software Defined Networking Architecture, Security and Energy Efficiency: A Survey", ***IEEE Communications Surveys & Tutorials***, 19 (1): 1-7, (2017).

[52] Shin S., Xu L., Hong S. and Gu G., "Enhancing Network Security through Software Defined Networking (SDN)", ***25th International Conference on Computer Communication and Networks (ICCCN),*** Hawaii-USA, 1-9, (2016).

[53] Yan Z., Zhang P. and Vasilakos V., "A security and trust framework for virtualized networks and software-defined networking", ***Security and Communication Networks***, 9: 3059-3069, (2016).

[54] Pandya M.K., Homayoun S. and Dehghantanha A., "Forensics Investigation of OpenFlow-Based SDN Platforms", ***Cyber Threat Intelligence, Springer***, Advances in Information Security vol 70, (2018).

[55] Akbari I., Tahoun E., Salahuddin M.A., Limam N. and Boutaba R., "ATMoS: Autonomous Threat Mitigation in SDN using Reinforcement Learning", ***IEEE/IFIP Network Operations and Management Symposium,*** Hungary, 1-9, (2020).

[56] Muragaa W.H., Seman K. and Marhusin M.F., "A POX Controller Module to Collect Web Traffic Statistics in SDN Environment", ***World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering,*** 10:2105-2110, (2017).

[57] Mahamat S.B. and Çeken C., "Anomaly Detection in Software-Defined Networking Using Machine Learning", ***Düzce University Journal of Science & Technology,*** 7:748-756, (2019).

[58] Zhang S., Meng X. and Wang L., "SDNForensics: A Comprehensive Forensics Framework for Software Defined Network", ***Proceedings of the International Conference on Computer Networks and Communication Technology (CNCT 2016),*** Atlantis Press, 92-99, (2016).

[59] Volarevic I., Tomic M. and Milohanic L., "Network Forensics", ***45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO),*** Croatia, 1025-1030, (2022).

ERKEN GÖRÜNÜM

[60] Ieong R.S.C., "FORZA – Digital forensics investigation framework that incorporate legal issues", ***Digital Investigation***, 3S: 29-36, (2006).

[61] Ring M., Wunderlich S., Scheuring D., Landes D. and Hotho A., "A survey of network-based intrusion detection data sets", ***C o m p u t e r s & Se c u r i t y***, 8 6: 1 4 7 – 1 6 7, (2019).

[62] Vekil sunucu nedir?, ***Eskişehir Osmangazi Üniversitesi***, İnternet: https://bidb.ogu.edu.tr/hizmetler/Sayfa/Index/38/vekil-sunucu-nedir , (Erişim Tarihi: 03.07.2022)

[63] Durnagöl Y., "5651 Sayılı Kanun Kapsamında İnternet Aktörlerine Getirilen Yükümlülükler İle İdari Ve Cezai Yaptırımlar", ***Türkiye Adalet Akademisi Dergisi (TAAD),*** 2: 375-416, (2011).

[64] Developing Standarts, ***International Organization for Standardization (ISO)***, https://www.iso.org/developing-standards.html .

[65] Tatlıgil İ. S., "ISO/IEC JTC 1/SC 27 "BT Güvenlik Teknikleri" Standardlarının Siber Güvenliğe Katkısı", ***Yüksek Lisans Tezi,*** T.C. İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, (2020).

[66] Ujcich B.E. and Sanders W.H., "Data Protection Intents for Software-Defined Networking", ***2019 IEEE Conference on Network Softwarization (NetSoft)***, France, 271-275, (2019).

[67] Özkaya Ö. ve Toprak İ., "Türkiye'de Güvenlik Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi", ***MANAS Sosyal Araştırmalar Dergisi,*** 11(3): 1291-1305, (2022).

[68] Gijrath S.J.H., "(Re-)defining software defined networks under the European electronic communications code", ***Computer Law & Security Review***, 40, 105492, (2021).

[69] Program: ***Mininet version 2.3.0***, (2021).

[70] Program: ***Oracle VirtualBox version 6.1,*** (2021).

[71] Program: ***Ubuntu, Desktop version 20.04***, (2021).

[72] Program: ***Ryu Controller version 4.34***, (2017).

[73] Program: Linux Foundation Collaborative Project, ***Openvswitch version 2.13.1***, (2016).

[74] Program: ***Wireshark version 3.2.3***, (2021).

[75] Ryu Firewall, ***İnternet***: https://github.com/gwacter-zz/sdn-workshop/blob/master/exercises/06-ryu-firewall.md , (Erişim Tarihi: 03.07.2022).

[76] van Adrichem N.L.M., Doerr C. and Kuipers F.A., "OpenNetMon: Network monitoring in OpenFlow Software-Defined Networks", ***2014 IEEE Network Operations and Management Symposium (NOMS)***, Poland, 1-8, (2014).

[77] Nougnanke K.B., Bruyere M. and Labit Y., "Low-Overhead Near-Real-Time Flow Statistics Collection in SDN," ***2020 6th IEEE Conference on Network Softwarization (NetSoft)***, Belgium, 155-159, (2020).

[78] Özdem M. and Alkan M., "SDN based management platform for intranet services", ***Journal of Polytechnic***, 24(3): 989-995, (2021).

[79] Awadh K. and Akbas A., "Intrusion detection model based on TF.IDF and C4.5 algorithms", ***Journal of Polytechnic***, 24(4): 1691-1698, (2021).

[80] Utku A. ve Akcayol M. A., "Derin öğrenme tabanlı model ile bir olayın sonraki olma zamanının tahmini", ***Politeknik Dergisi***, 24(1):1-15, (2021).

İNCELEN GÖRÜNÜM