
GAZİ ÜNİVERSİTESİ
Gazi
1926

LİNUX İŞLETİM SİSTEMİNDE LOG DOSYALARININ ADLİ BİLİŞİM AÇISINDAN İNCELENMESİ

Kübra KARADENİZ KELEŞ

YÜKSEK LİSANS TEZİ
ADLİ BİLİŞİM ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

OCAK 2022

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.

Kübra KARADENİZ KELEŞ

05/01/2022

LİNUX İŞLETİM SİSTEMİNDE LOG DOSYALARININ ADLİ BİLİŞİM AÇISINDAN İNCELENMESİ

(Yüksek Lisans Tezi)

Kübra KARADENİZ KELEŞ

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Ocak 2022

ÖZET

İşletim sistemleri teknolojiyle beraber sürekli gelişmektedir. Bu gelişime bağlı olarak adli bilişim yazılımları da kendini güncellemektedir. Bilgisayarlar üzerinde yapılan birçok işlem kayıt altına alınmakta ve bu kayıtlar işletim sistemlerinin yapısına göre değişmektedir. Söz konusu kayıtların önemli bir kısmı ise log dosyalarında tutulmaktadır. Bu sebeple log dosyaları adli bilişim açısından oldukça önemlidir. Ancak adli bilişim yazılımları işletim sistemlerinin gelişmelerini geriden takip etmekte ve genellikle Windows işletim sistemi üzerinde yoğunlaşmaktadır. Birçok adli bilişim yazılımı Linux ve MAC işletim sistemlerini tam olarak desteklememekte bu sebeple incelemeler elle yapılmaktadır. Bu durum adli inceleme sürelerini uzatmaktadır. Bu çalışmada, Linux işletim sistemi incelenerek adli incelemelerde önemli olabilecek log kayıtların analizi yapılmıştır. Yapılan çalışmanın sonucunda suçun aydınlatılmasına fayda sağlayacağı değerlendirilen log kayıtlarının, adli bilişim alanında çalışan bilirkişilere ve adli bilişim dalında eğitim alan öğrencilere yol gösterebilmesi açısından faydalı olacağı değerlendirilmiştir. Çalışmanın ilk aşamasında literatür taraması yapılmıştır. Bir sonraki aşama olarak çalışma kapsamında adli incelemelerde suçun ve suçlunun tespitine yönelik önem arz ettiği değerlendirilen hususlar göz önünde bulundurularak Linux işletim sistemi üzerinde birçok deney yapılmıştır. Gerçekleştirilen bu deneyler sonucunda adli bilişim açısından önemli olabilecek log dosyası kayıtları tespit edilmeye çalışılmıştır. Son aşama olarak yapılan tespitler ile literatür taramasıyla elde edilen bilgilerin karşılaştırılması yapılmış olup log kayıtlarının nerelerde bulunduğunu gösteren bir çizelge oluşturulmuştur.

Bilim Kodu	:	92401
Anahtar Kelimeler	:	Linux işletim sistemi, adli bilişim, işletim sistemi, log dosyaları
Sayfa Adedi	:	69
Danışman	:	Doç. Dr. Çelebi ULUYOL

ANALYSIS OF LOG FILES IN LINUX OPERATING SYSTEM FOR COMPUTER FORENSICS

(M. Sc. Thesis)

Kübra KARADENİZ KELEŞ

GAZİ UNIVERSITY

INFORMATICS INSTITUTE

January 2022

ABSTRACT

Operating systems are constantly evolving with technology. Depending on this development, forensic software is also updated. Many operations on computers are recorded and these records vary according to the structure of the operating systems. An important part of these records are kept in log files. For this reason, log files are very important in terms of forensic computing. However, forensic software follows the development of operating systems and generally concentrates on the Windows operating system. Many forensic software do not fully support Linux and MAC operating systems, so investigations are done manually. In this case, the forensic examinaion period is extended. In this study, the Linux operating system was examined and the log records that could be important in forensic investigations were analyzed. As a result of the study, it has been evaluated that the log records, which are considered to be beneficial for the clarification of the crime, will be useful in terms of guiding the experts working in the field of forensic informatics and the students studying in the field of digital forensics. In the first stage of the study, a literature review was made. As the next step, many experiments were carried out on the Linux operating system, taking into account the issues that are considered to be important for the detection of crime and the in forensic investigations. As a result of these experiments, log file records, which are important in terms of forensic informatics, were tried to be determined. As a final step, the determinations made and the information obtained from the literature review were compared and a table was created showing where the log records are located.

Science Code	:	92401
Key Words	:	Linux operating system, digital forensic, operating system, log files
Page Number	:	69
Supervisor	:	Doç. Dr. Çelebi ULUYOL

TEŞEKKÜR

Adli bilişim yazılımlarının gelişimini daha çok Windows işletim sistemi üzerine yapmaktadır. Bu sebeple yaygın olarak kullanılan adli bilişim yazılımları Linux işletim sistemini ya kısmen desteklemek ya da desteği bulunamamaktadır. Bu çalışma ile adli incelemelerde suçun ve suçlunun tespitine yönelik önem arz ettiği değerlendirilen hususlar göz önünde bulundurarak adli bilişim açısından önemli log dosyalarının incelenmesi konusunda yöntem oluşturması ve inceleme süresinin kısaltılması hedeflenmiştir. Bu çalışmanın şekil bulmasında ve tamamlanmasında her türlü desteği sağlayan proje hocam Doç.Dr.Çelebi ULUYOL'a (Gazi Üniversitesi), tüm hayatım boyunca bana desteğini esirgemeyen aileme, eşime ve çalışmam boyunca bana yardımcı olan tüm arkadaşlarıma ve hocalarıma katkılarından dolayı teşekkür eder, bu alanda çalışmama sebep olan JKDB, Bilişim Teknolojileri İnceleme Şube Müdürlüğüne minnettarlığımı sunarım.

İÇİNDEKİLER

Sayfa

ÖZET iv

ABSTRACT v

TEŞEKKÜR vi

İÇİNDEKİLER vii

ÇİZELGELERİN LİSTESİ ix

RESİMLERİN LİSTESİ x

KISALTMALAR xii

1. GİRİŞ 1

2. TEMEL BİLGİLER 7

2.1. İşletim Sistemi 7

2.2. Dosya Sistemleri 7

2.3. Log Dosyaları 8

2.4. Linux İşletim Sistemi ve Özellikleri 8

3. LİTERATÜR ÖZETİ 13

3.1. Windows İşletim Sisteminin Adli Bilişim Açısından Log Dosyalarının İncelenmesi ile İlgili Araştırmalar 13

3.2. Linux İşletim Sisteminin Adli Bilişim Açısından Log Dosyalarının İncelenmesi ile İlgili Araştırmalar 17

3.3. MacOS İşletim Sisteminin Adli Bilişim Açısından Log Dosyalarının İncelenmesi ile İlgili Araştırmalar 19

4. METODOLOJİ 21

4.1. Kullanılan Yazılımlar ve Donanımlar 21

4.2. Uygulama Adımları 22

4.2.1. Çalışma kapsamındaki verilerin belirlenmesi 22

4.2.2. Çalışma kapsamındaki verilerin oluşturulması 25

4.2.3. Çalışma kapsamındaki verilerin analizi ve incelenmesi 30

Sayfa

5. BULGULAR 33
5.1. Kurulan İşletim Sistemi Bilgisi 33
5.2. Bilgisayar Ad ve ID Bilgisi 33
5.3. Kurulum Zaman Bilgisi 34
5.4. Kullandığı Zaman Diliminin Bilgisi 34
5.5. Ad Bilgisinin Değiştirilme Bilgisi 35
5.6.Oluşturulan ve Silinen Kullanıcı Bilgileri 35
5.7. Kullanıcıların Oturum Açma ve Kapatma Bilgileri 38
5.8. Bilgisayarın Başlatma ve Kapatma Bilgileri 41
5.9. Tarih-Saat ve Saat Dilimi Değişikliği Bilgileri 43
5.10. Bilgisayara Takılan Harici Veri Depolama Cihazların Bilgileri 44
5.11. Bilgisayara Yüklenen Programların Bilgileri 45
5.12. Ağ Yapılandırması, Ağ Üzerinden Erişim, Kablolu Erişim Noktalarına Yapılan Bağlantı İşlemlerinin Bilgileri 47
5.13. Yazıcıdan Çıktı Alınması ile İlgili Bilgiler 49
5.14. Sistem Yedeğinin (Backup) Alınması ile İlgili Bilgiler 51
6. TARTIŞMA 53
7. SONUÇ VE ÖNERİLER 55
KAYNAKLAR 59
EKLER 65
ÖZGEÇMİŞ 69

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 1.1. Adli bilişim yazılımları ve desteklediği işletim sistemleri 3

Çizelge 4.1. Çalışma kapsamında belirtilen problemlerin analizinde kullanılan yazılımlar 30

Çizelge 5.1. wtmp dosyasının çözümlenmesi sonucunda tespit edilen verilerin bilgileri..... 39

RESİMLERİN LİSTESİ

Resim **Sayfa**

Resim 5.1. Bilgisayarda kurulu işletim sistemi ve versiyon bilgisi 33
Resim 5.2. Bilgisayar zaman bilgisi 34
Resim 5.3. Değiştirilen bilgisayar ad bilgisi 35
Resim 5.4. Kullanıcı bilgileri 35
Resim 5.5. Oluşturulan kullanıcı bilgileri(a) 36
Resim 5.6. Oluşturulan kullanıcı bilgileri(b) 37
Resim 5.7. Silinen kullanıcı bilgileri 37
Resim 5.8. wtmp dosya yapısı 38
Resim 5.9. İncelenen örnek olayın yapısı 40
Resim 5.10. Tespit edilen zaman bilgisi 41
Resim 5.11. Başarısız oturum açma bilgisi 41
Resim 5.12. Bilgisayar başlatma bilgisi 41
Resim 5.13. Bilgisayar kapatma zaman bilgisi 42
Resim 5.14. Değiştirilen tarih-zaman bilgisi 43
Resim 5.15. Değiştirilen saat dilimi bilgisi 43
Resim 5.16. Sandisk USB belleğe ait bilgiler 44
Resim 5.17. Oluşan png dosyasının bilgileri 45
Resim 5.18. Oluşan png dosyasının yapısı 45
Resim 5.19. iPhone cep telefonuna ait bilgiler 45
Resim 5.20. Yüklenen programlara ait bilgiler(a) 46
Resim 5.21. Yüklenen programlara ait bilgiler(b) 46
Resim 5.22. Kablolu erişim bağlantı noktaları 47
Resim 5.23. Yerel ağ bağlantısı kurulan IP adres bilgisi 48
Resim 5.24. Ağ Bağlantı Bilgileri 49
Resim 5.25. Bağlantı kurulan yazıcı bilgileri 49

Resim **Sayfa**

Resim 5.26. printers.conf dosya bilgileri 50

Resim 5.27. /var/spool/cups dizini içerisindeki veriler..... 51

Resim 5.28. Free space alanda elde edilen veriler 51

Resim 5.29. Backup dosyaları 52

Resim 5.30. manifest dosya bilgileri..... 52

KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
FSSTND	Dosya sistem hiyerarşisi
GNU	GNU Unix değildir.
lD	Kullanıcı numarası (Identification)
iOS	iPad/iPhone işletim sistemi
MAC	Ortam erişim yönetimi (Media access control)
SSID	Hizmet seti kimliği (Service set identifier)
UUID	Evrensel benzersiz tanımlayıcı **(**Universally unique identifier)

1. GİRİŞ

Teknolojik gelişmelerin, insan hayatına kazandırdığı en büyük buluşlardan biri elektronik cihazlardır. Elektronik cihazlar özellikle bilgisayarlar, doğrudan ya da dolaylı olarak suç işlemede bir araç olarak kullanılabilmektedir. Bilgisayarlar ile kullanıcı arasında iletişimi sağlayan komutlar yani işletim sistemleri ise sürekli güncellenmekte ve gelişmektedir. Bu sebeple kullanıcının gerçekleştirdiği işlemlere ve geride bıraktığı izlere ait kayıtlarda da artış yaşanmaktadır. Bu izlerin tespit edilmesi, işlenen suçun aydınlatılmasında önemli rol oynamaktadır.

Bilgisayarların ilk açılışından kapanışına kadar ki geçen sürede yapılan birçok işlem, işletim sistemleri üzerinde, önemli bir kısmı ise log dosyalarında kayıt altına alınmaktadır. Log dosyaları, yapılan işlemlerin kayıt altına alındığı dosyalardır. Bilişim sistemlerinin hemen hemen her alanında log kayıtları aktif olarak kullanılmaktadır. İşlenen suçların aydınlatılmasında önemli izlerin bulunduğu log kayıtlarının, incelenmesi adli bilişim açısından büyük önem arz etmektedir. Bu kayıtlar sayesinde bilgisayar üzerinde yapılan değişikleri, oturum işlemleri, kullanıcı işlemleri gibi adli bilişim açısından değerli birçok veri hakkında bilgi sahibi olunmaktadır. Ancak her günlük dosyasının kendine özgü bir biçimi vardır. Günlük kayıtları için yaygın olarak benimsenen bir standardın olmamasından dolayı günlük kayıtlarının analiz edilmesi oldukça zordur [1].

Belirli bir yazılım ve işletim sistemi tarafından gerçekleştirilen olayların kayıtlarını içeren ve bu olayları otomatik olarak kaydeden dosyalara log dosyası denilmektedir. Bilişim sistemleri üzerinde log kayıtları sürekli olarak tutulmaktadır.

Log kayıtları genel olarak bilgisayarda kimin oturum açtığı, neler yaptığı, aldığı ve gönderdiği e-postalar gibi kullanıcı etkinliği, disk hataları, kaynak kullanımı ve performans, durum değişikliği, başlatma ve durdurma gibi saldırı girişimleri hakkında bilgiler içerebilmektedir. [2].

Bilişim sistemleri kullanılarak veya bu sistemlere yönelik işlenilen suçların adli olarak incelenmesi esnasında bu dijital hareketliliğin kaydedildiği log dosyalarına ihtiyaç duyulmaktadır. Sistemler üzerinde yapılan değişiklikler bir günlük gibi log dosyalarına kaydedildiğinden bu dosyaların incelenmesi suçun aydınlatılması açısından önem arz etmektedir.

Log dosyalarının içeriği kontrol edildiğinde;

- Olayın kim tarafından gerçekleştirildiği,
- Olayın gerçekleşme zamanı,
- Olayın nasıl gerçekleştiği,
- Kimlerin oturum açmaya çalıştığı,
- Kimlerin sisteme uzaktan bağlandığı,
- Sisteme USB takılıp takılmadığı,
- Wirelles veya kablolu bağlantı kurulup kurulmadığı,
- Erişimlerinin ne yönde olduğuna dair incelemeyi yapan bilirkişiyi sonuca götürecek bilgilere ulaşılabilmektedir.

Linux/Unix sistemlerinde de en önemli dosyalarından biri log dosyalarıdır. Linux ortamında log dosyaları dört farklı kategoriye ayrılabilir. Bunlar; uygulama log dosyaları, etkinlik log dosyaları, servis log dosyaları ve sistem log dosyalarıdır. Linux işletim sistemi diğer işletim sistemleriyle karşılaştırıldığında daha detaylı loglama mekanizmasına sahiptir. Log dosyaları bir ya da birden çok servisin hareketlerini kayıt altına alabilmektedir. Linux işletim sistemleri diğer işletim sistemlerinin aksine, tek satırlık log girdileri tutarak okumayı kolaylaştıran sistem bulundurmaktadır [3].

Linux işletim sistemlerinde bulunan log kayıtları üzerinde bazı deliller elde edilebilir. Bunlara bir kullanıcının veya saldırganın sisteme giriş yapıp yapmadığı, giriş yapması halinde ip adresinin tespiti gibi olaylar örnek verilebilir [4]. Bu sebeple adli olarak incelenmesi istenen Linux işletim sistemine sahip bilgisayarların log dosyaları, işlenen bazı suçların aydınlatılmasında incelemeci açısından önemli kayıtları içermektedir.
Linux işletim sisteminde, adli bilişim incelemeleri açısından önem arz eden log kayıtlarının fazlalığı ve yaygın olarak kullanılan adli bilişim yazılımlarının hali hazırda Linux işletim sistemini tam olarak desteklememesinden dolayı bu çalışmada platform olarak Linux işletim sistemi seçilmiştir.

Çizelge 1.1. Adli bilişim yazılımları ve desteklediği işletim sistemleri

Yazılım Adı ve versiyonu	Windows İşletim Sistemi	Mac OS İşletim Sistemi	Linux İşletim Sistemi
Axiom 4.8.1.22785	Desteği var	Desteği var	Desteği yok
X-Ways 20.0 SR1	Desteği var	Kısmen	Kısmen
Encase 8.11.00.74	Desteği var	Kısmen	Kısmen
IEF v6.8.2.3062	Desteği var	Desteği yok	Desteği yok
Forensic Explorer 5.1.2(9072)	Desteği var	HFS dosya sistemi desteği var	Desteği yok
RecoveryMyFiles v5.1.0	Desteği var	Desteği yok	Desteği yok

Çizelge 1.1' de işletim sistemleri ve bu sistemlerin yazılımlar tarafından desteklenip desteklenmediği gösterilmiştir. Çizelgeye bakıldığında yaygın olarak kullanılan adli bilişim yazılımlarının gelişimlerini Windows işletim sistemleri üzerinde yaptıkları görülmüştür. Söz konusu yazılımların Mac OS ve Linux işletim sistemleri üzerinde gelişimlerini henüz tamamlamadıkları görülmüştür.

Linux işletim sisteminin kurulu olduğu sabit disk imajının Axiom, IEF, Forensic Explorer ve RecoveryMyFiles yazılımları ile yapılan incelemesinde yazılımın dosya sistemini çözümleyemediği görülmüştür. Söz konusu imajın Xways Forensics ve EnCase yazılımlarıyla yapılan incelenmesinde bu yazılımların dosya sistemini çözümleyebildiği görülmüştür. Ancak dosya kurtarma işlemi sonrasında işletim sistemine ait dosyaların eksik kurtarıldığı görülmüştür. Xways yazılımı tarafından mevcut olan log dosyaları isimlerinin kendi isimleri ile kurtarılamadığı görülmüştür.

Ling yaptığı [5] çalışmada sadece messages, lastlog, secure, wtmp, boot.log, xferlog kayıtları hakkında bilgi vermiştir. Zeng ve arkadaşları yaptıkları [6] çalışmada syslog, çekirdek mesajları hakkında genel bilgiler verilmiştir. Bu sebeple log incelemeleri ile ilgili çalışmaların yüzeysel tutulduğu ve adli bilişim açısından önem arz eden log dosyaların farklı farklı çalışmalarda yer aldığı görülmüştür. Yine yapılan incelemelerin canlı sistemler üzerinde olduğu görülmüştür. Örneğin Dos Santos Almeida ve arkadaşları yaptıkları [7] çalışmada, örnek bir deneysel olay oluşturarak incelemeleri canlı sistemler üzerinde

gerçekleştirmişler ve incelemeleri sırasında açık sistemlerde kullanılabilecek WireShark gibi toollar kullanmışlardır. Bu çalışmada ise literatürden farklı olarak kopya üzerinde, kriminal incelemelerde kullanılan adli bilişim yazılımları ile incelemeler gerçekleştirilmiştir.

Kılıç yaptığı [8] çalışmasında, registry ve log kayıtları ile ilgili olarak "Windows işletim sistemi için detaylı olarak incelenen ve dava dosyasına büyük katkılar yapan bu bilgilerin, Linux ve Macintosh işletim sistemleri açısından nasıl elde edileceğinin çok bilinmediği" hususuna değinmiştir. Bu çalışmada, Linux işletim sistemine sahip bilgisayarların adli bilişim açısından incelenmesi neticesinde, söz konusu işletim sistemi ile ilgili elde edilebilecek önemli log kayıtlarının neler olduğu ve bu bulgulara adli bilişim yazılımları kullanarak nasıl ulaşılabileceği hususunda araştırma yapılmıştır.

Çalışmanın ilk aşamasında literatür taraması yapılmıştır. Literatür taramasında, bilişim dünyasında sıkça kullanılan Windows, MAC OS, ve Linux işletim sistemlerinin log dosyalarını adli bilişim açısından inceleyen çalışmalar araştırılmıştır. Literatür taramasından sonra bu çalışmanın amacı, çalışmanın sınırları ve çalışmayı anlamayı kolaylaştırmak için kavram ve tanımlar anlatılmıştır. Çalışmanın ikinci aşamasında, çalışmanın yapılması için gereken araç ve gereçler, çalışmanın yöntemi ve çalışmanın yapılabilmesi için gereken verilerin elde edilmesi, yapılan deneyler anlatılmıştır. Çalışmanın üçüncü aşamasında, deneyler sonucunda elde edilen bulgular anlatılmıştır. Çalışmanın son aşamasında ise tartışma ve sonuçlar anlatılmıştır.

Araştırmanın Sınırları

Linux işletim sistemini oluşturan log kayıtları içerisinde adli bilişim açısından önemli olabileceği değerlendirilen verilerin araştırılması ve bu verilerin analiz edilmesi bu çalışmanın kapsamını oluşturmaktadır.

Linux işletim sistemine ait tüm kayıtların incelenmesi zor olacağı için adli incelemelerde suçun ve suçlunun tespitine yönelik önem arz ettiği değerlendirilen hususlar ile ilgili veriler tespit edilmiş diğer veriler çalışma kapsamı dışında tutulmuştur.

Araştırmanın Amacı

Bu çalışmada literatürden farklı olarak adli kopya üzerinden incelemeler yapılmış ve adli bilişim incelemeleri açısından önem arz eden log dosyaları kriminal incelemelerde kullanılan adli bilişim yazılımları ile desteklenerek adli bilişim uzmanlarının incelemelerine yön verecek tespitler yapılmaya çalışılmıştır. Adli soruşturmalarda görev alan adli bilişim uzmanlarının ihtiyaçları göz önünde bulundurularak bu çalışmada Linux işletim sistemi seçilmiştir. Ek olarak Modig ve Ding [9] çalışmasında, Ubuntu versiyonunun, Nisan 2018 itibarıyla en çok erişilen ilk on web sitesindeki yerini aldığını (DistroWatch tarafından yapılan popülerlik listesine göre) belirtmiştir. Bu sebeple Linux işletim sisteminin Ubuntu versiyonu seçilmiştir.

Bu çalışma kapsamında aşağıda belirtilen problemlere çözüm bulmaya çalışılmıştır.

- İşletim sisteminin kurulma bilgilerine ait log kayıtları nasıl elde edilmektedir?
- Oluşturulan ve silinen kullanıcıların tespitine ait log kayıtları nasıl elde edilmektedir?
- Kullanıcının oturum açma ve kapatma bilgilerine ait log kayıtları nasıl elde edilmektedir?
- Bilgisayarın başlatma ve kapatma tarihine ait log kayıtları nasıl elde edilmektedir?
- Tarih-saat ve saat dilimi değişikliğine ait log kayıtları nasıl elde edilmektedir?
- Bilgisayara takılan harici veri depolama cihazlarına ait log kayıtları nasıl elde edilmektedir?
- Yüklenen programların tespiti amacıyla oluşan log kayıtları nasıl elde edilmektedir?
- Ağ üzerinden erişim ve kablolu erişim noktalarına yapılan bağlantılara ait log kayıtları nasıl elde edilmektedir?
- Yazıcılardan çıktı alındıktan sonra oluşan log kayıtları nasıl elde edilmektedir?
- Backup alınması sonucunda oluşan log kayıtları nasıl elde edilmektedir?

Bulgu olarak incelenmek üzere gönderilen Linux işletim sistemine sahip bilgisayarlar üzerinde; yukarıda belirtilen problemlere çözüm önerisi sunmak, adli bilişim açısından önem arz ettiği değerlendirilen log kayıtlarının nerelerde bulunabileceğinin tespit edilmesi ve analiz edilmesi, ilgili inceleme taleplerine cevap vermek açısından kaynak oluşturması ve inceleme sürecinde zaman tasarrufu sağlanması amaçlanmıştır.

2. TEMEL BİLGİLER

Gerçekleştirilecek uygulama ve analizlerin anlaşılabilirliğini kolaylaştırmak amacıyla işletim sistemi, dosyalama sistemi ve log dosyaların tanımı yapılmış, Linux işletim sistemi ve özelliklerinden kısaca bahsedilmiştir.

2.1. İşletim Sistemi

Kullanıcı ile bilgisayar arasında köprü görevi kurarak iletişimi sağlayan bilgisayar kullanımını kolaylaştıran, çalışan tüm donanımların ve yazılımların yönetimini ve denetimini sağlayan yazılıma işletim sistemi denilmektedir [10].

Günümüzde birçok alanda kullanılan bilgisayarın kullanım yeri ve amaçlarına uygun işletim sistemine sahip olması gerekmektedir. İşletim sistemleri, bilgisayarda bulunan tüm donanımlar ile bilgisayar kullanıcısı arasında ara yüz görevi yaparak iletişim kurmasını sağlayan yazılımdır. İşletim sistemlerinin temel amacı, bilgisayar sistemlerinin verimli ve etkin kullanmasını sağlamaktır.

2.2. Dosya Sistemleri

Verilerin diskler, flash sürücüler gibi fiziksel depolama aygıtlarında depolanmasını ve bunların yönetilmesini sağlar [11]. Depolama aygıtlarına veri yazılırken veriler bir dosya sistemine göre yazılmaktadır. Eğer bir dosya sistemine göre yazılmasaydı hangi verinin nereye yazılacağını ya da yazıldıktan sonra nasıl bulunacağını bilinmeyecektir. Bu nedenle, yeni üretilmiş bir depolama aygıtı ilk olarak biçimlendirilmelidir. Biçimlendirmenin amacı üzerinde hiçbir dosyalama sistemi bulunmayan aygıta hangi dosyalama sisteminin kullanılacağını belirtmektir.

İşletim sistemleri de depolama aygıtındaki bilgilere ulaşmak istediğinde, aygıttaki dosya sistemine bakarak hangi dosyanın nerede olduğunu bulabilecektir. Bir işletim sisteminde, dosya sistemi veri depolama biriminde bulunan veriyi yönetir. Dosya sistemleri verilerin depolandığı dosyalar, dosyaları organize eden, dosyalar hakkında bilgileri saklayan sistem alanından ve kök dizinden oluşan oluşmaktadır.

2.3. Log Dosyaları

İşletim sistemi üzerinde meydana gelen işlemlerin neredeyse tümünün kaydını tutan dosyalardır. Bilgisayar kullanıcısının yazılımlarda hangi işlemin ne zaman, hangi sıra ile yapıldığının geri planda takibini yapan verilerine log dosyası denilmektedir[12].

Günümüzde sunucular, işletim sistemleri, donanımlar, yazılımlar, IOT cihazlar gibi birçok alanda log kayıtları tutulmaktadır. Tutulan log kayıtları incelenererek hata tespiti, güvenliği gibi birçok alanda bilgi sahibi olunmaktadır.

2.4. Linux İşletim Sistemi ve Özellikleri

Linux işletim sistemi 1983 yılında başlatılan GNU Unix Değildir (GNU) Projesine dayanmaktadır. GNU Projesi, kendisini her zaman serbestçe kullanılabilecek kaynak kodu geliştirmeye adayan Richard Stallman tarafından ilan edildi. Tamamen ücretsiz ve açık kaynak kodlu işletim sistemi çekirdeği geliştirmek üzere ortaya çıkmıştır. Projenin temel amacı Unix'e benzer bir işletim sistemi geliştirmek ve bu işletim sisteminin tamamen ücretsiz olmasıdır [13].

Linux işletim sistemi; 1991 yılında Helsinki Üniversitesi öğrencisi Linus Torvalds tarafından Unix işletim sisteminden ilham alınarak geliştirilen açık kaynak kodlu, özgür ve ücretsiz işletim sistemidir. Linux işletim sistemi çok farklı platformlarda çalışabilmektedir [14].

Linux, sistem çekirdeğini oluşturduğundan işletim sisteminin adının belirlenmesini sağlamıştır [15]. Linux aslında GNU/Linux işletim sisteminin sadece çekirdeğine verilen isimdir [16]. Linux işletim sistemi açık kaynak kodlu olması sebebiyle herkes tarafından kodlarının incelenmesi, güncellenmesi, geliştirilmesi ve dağıtılması sağlanmaktadır. Bu sebeple istek ve beklentilere göre şekillendirilebilen bir işletim sistemi olarak tanımlanabilmektedir. Bu yüzden birçok dağıtım ve sürümleri bulunmaktadır.

Linux dağıtımları ve sürümleri arasındaki farklılıkları üç maddede gösterebiliriz:

Amaç; dağıtımlar genellikle farklı amaçlar için tasarlanmıştır. Bazı dağıtımlar sunuculardа, bazıları masaüstü, bazıları ise gömülü sistemlerde kullanmak için tasarlanmıştır. Linux çoğunlukla sunucularda kullanılma eğilimindedir.

- Yapılandırma ve paketleme; bazı dağıtımlar tüm yapılandırma ayarlarını ve dosyalarını aynı konumda tutar, diğerleri bu durumu değiştirir. Uygulama, yükleme ve güncelleme işlemleri dağıtımlar arasında farklılık göstermektedir.
- Destek modeli; bazı dağıtımlar gönüllü topluluk tarafından bazıları ise ticari bir satıcı tarafından desteklenmektedir [16].

Linux işletim sistemlerinin avantajları aşağıda belirtilmiştir.

- Linux işletim sistemi ücretsiz olup Linux işletim sistemine sahip olmak için herhangi ücret ödenmeye gerek yoktur. Ayrıca çalışma performansı için gerekli donanımlarda diğer işletim sistemlerine göre ucuzdur.
- Linux işletim sistemi açık kaynak kodlu olması sebebiyle hızla geliştirilmekte ve güncellenmektedir. Sistemde bir hata veya eksik tespit edilirse, herhangi bir programcı çok kısa sürede bu sorunu gidererek gerekli olan yamayı hizmete sunabilmektedir.
- Linux işletim sistemine sahip sistemler çok daha güvenlidir çünkü bilgisayara hiçbir eklenti otomatik olarak kurulmaz ve tüm güncelleştirmeler kontrol altındadır.

Linux işletim sistemlerinin dezavantajları aşağıda belirtilmiştir.

- Linux işletim sistemi basit bilgisayar kullanıcıların rahatça kullanabileceği düzeyde değildir. Kullanıcıların belirli bir yazılım ve işletim sistemi bilgisine sahip olmalarını gerektirmektedir. Bu sebeple öğrenme süresi diğer işletim sistemlerine göre daha uzundur.
- Linux işletim sisteminin sürekli gelişmesi ve güncellenmesi sebebiyle değişiklerinin takip edilmesinin zor olmakta, tam olarak teknik desteği olmamakta ve doküman eksikliği bulunmaktadır.
- Linux işletim sistemi tüm ihtiyaçlara cevap verememekte geri kalmaktadır.

Linux işletim sisteminin farklı dosya sistemi vardır. Linux işletim sisteminde her şey dosyadır. Unix tabanlı olmasından dolayı “Dosya Sistem Hiyerarşisi (FSSTND)”

benimsenmiştir. Bunun anlamı ise dosya sisteminde oluşan dizinlerin root dizine bağlanmasıdır. Dosya adreslerinde "/" işaretini kullanmaktadır. Küçük-büyük harf duyarlılığına sahiptir.

Linux işletim sisteminde FSSTND'de oluşan bazı temel dizinler ve özellikleri aşağıda belirtilmiştir.

/bin dizini

Sistemin açılışı ve sistem kontrolü için kritik öneme sahip komutların bulunduğu dizindir. Sistem başlatıldığında ilk olarak /bin dizini çalışır hale getirilir.

/boot dizini

Bilgisayarın başlangıç aşamasında gerekli olan tüm dosyaları içerir.

/dev

Device kelimesinin kısaltmasıdır. Sistemde bulunan bütün donanım aygıtların tutulduğu dizindir.

/etc

İşletim sistemine ait bütün ayarları barındıran dizindir. İşletim sisteminin kurulu olduğu bilgisayara özel birçok yapılandırma bilgisini içermektedir.

/home

Kullanıcıların kişisel verileri, kullandığı programlara yaptığı ayarları içeren dizindir. Her kullanıcının kendine ait bir klasörü bulunmaktadır.

/lib

Var olan çekirdek modülleri ve paylaşılan kütüphane dosyaları bu dizinde bulunmaktadır.

/media

Bağlantı kurulan harici depolama birimlerinin bulunduğu dizindir.

/lost+found

Sistemde herhangi bir problem oluştuğunda fsck (File System check) komutu devreye girerek bağlantıları kopmuş kayıp dosyalar bu dizin içerisine atılır. Sistemde bir aksaklık olduğunda, olması gereken bir dosya bulunamadığında bu dizin içerisine bakılmalıdır.

/mnt

Mount kelimesinin kısaltılmış halidir. İşletim sisteminin kurulu olduğu disk bölümü hariç, sistem başlangıcında bağlanan sabit disk bölümleri ve donanım aygıtlarının bağlanma noktasıdır.

/opt

İşletim sistemi için zorunlu olmayan kullanıcı programlarının bulunduğu dizindir.

/proc

Sistemin çalışma süreçlerinin durumu hakkında bilgi içeren sanal dosyaların bulunduğu dizindir.

/root

Linux/Unix sistemlerde, işletim sistemine her türlü müdahalede bulunabilme yetkisine sahip, özel kullanıcı (kök kullanıcı) hesabının ev dizinidir.

/sbin

Linux işletim sisteminde normal kullanıcı ile root kullanıcıların kullanabileceği komutlar birbirinden ayrılmıştır. Root kullanıcı tarafından kullanılabilecek bakım ve yönetim için kullanılan komutlar bu dizin altında tutulmaktadır. Normal kullanıcının komutları ise /usr/sbin altında tutulmaktadır.

/usr

İşletim sistemi aracılığıyla ya da paket yönetim sistemleri kullanılarak yüklenen programlar ve programların çalışması için gerekli kütüphanelerin tutulduğu dizindir.

/temp

Programların geçici depolama alanı olarak kullandığı dizindir.

/var

Log dosyaları ve değişken sistem bilgilerinin bulunduğu dizindir.

Linux işletim sistemi diğer işletim sistemlerine göre daha ayrıntılı log kayıtları tutmaktadır. Genellikle metin tabanlı dosyalardan oluşmaktadır. Ancak bazı log dosyaları ikili tabanda tutulmaktadır. Linux işletim sisteminde log kayıtları, okumayı ve takibi kolaylaştırması amacıyla tek satır halinde tutulmaktadır. Linux işletim sistemlerinde "/var/log" klasörü ile "/etc" klasörü altında sistem kayıt dosyaları tutulmaktadır [8]. Linux işletim sisteminde log kayıtları genellikle "…var\log" dizini altında yer almaktadır. Kurulan bir uygulama farklı yerde log kayıtlarını tutabilir.

3. LİTERATÜR ÖZETİ

Günümüzde kullanılan elektronik cihazların farklı türlerinin bulunması, kullanım amaçlarının farklı olması sebebiyle çok sayıda işletim sistemi türü bulunmaktadır. Bu sebeple çalışmanın bu aşamasında yaygın olarak kullanılan işletim sistemlerinden Windows, MAC OS ve Linux işletim sistemlerine ait log dosyalarını inceleyen literatürdeki çalışmalar ele alınmıştır.

3.1. Windows İşletim Sisteminin Adli Bilişim Açısından Log Dosyalarının İncelenmesi ile İlgili Araştırmalar

Arshad ve arkadaşları [17] yaptıkları çalışmada USB cihazlarının kullanıcılar tarafından kolaylıkla kullanılabilmesi ve geniş depolama kapasitesi sunmasıyla birlikte, veri hırsızlığı açısından önemli tehdit oluşturmasına neden olabileceğini değerlendirerek USB cihazları adli bilişim açısından incelemişlerdir. Tarih-saat bilgileri, cihaz bilgileri ve kurtarılabilen dijital bilgilerin toplanması veri hırsızlığı faaliyetlerine yönelik araştırılması gereken konular olduğundan bu çalışmada üç türden kayıt ve günlük verileri toplanmıştır. Birincisi, cihaz eklenmeden (takılmadan) önce, ikincisi cihazın eklenmesi(takılması) sırasında, üçüncü olarak ise USB cihazın çıkarıldıktan sonra sistemde oluşturduğu kayıtlar toplanmıştır. Bununla birlikte USB cihazın izlenmesine yardımcı olabilecek kayıt defterinden de kanıtlayıcı bilgiler toplanmıştır. Yaptıkları çalışmada Windows 10 kayıtları, Windows 8 ve 10 sürümleri ile karşılaştırılmıştır. Windows 8 ve Windows 10 arasında önemli farklılıkların olmadığı ancak Windows 7'nin son sürümleri ile karşılaşıldığında ise önemli farklılıkların olduğu görülmüştür.

Talebi ve arkadaşları [18] yaptıkları çalışmada, günlük analizinin, adli bilişim sürecinin önemli kısımlarından biri olmasından dolayı Windows 8 platformunda olay günlüğü üzerinde durmuşlar ve olay günlüğünün adli amaçlar için analizini yapmışlardır. Windows NT ile birlikte gelen Windows olay günlüğü sistemi önemli değişiklik ve güncellemelerden sonra Windows 8 de büyük ölçüde değiştiğinden Windows 8 işletim sistemini seçmişlerdir. Çalışmalarında, Windows 8'in olay günlüğü formatını tanıtmışlar sonrasında günlükleri araştırma ve analiz etme yöntemleri açıklamışlardır.

Schuster ve arkadaşları [19] yaptıkları çalışmada, Windows NT adli yazılımları tarafından desteklemekte ve dosya formatı anlaşılabilir durumda olmasından dolayı Windows Vista sürümü üzerinde çalışmışlardır. Vista sürümü ile olay günlüğü hizmeti yeniden tasarlanmıştır. Bu durum adli incelemecileri ve yazılımcıları, alışılmadık yeni sistem davranışları ve geniş ölçüde belgelenmemiş bir dosya biçimiyle karşı karşıya getirmiştir. Bu çalışmada, Windows sistem kaydedicilerinin geçmişi, zaman içinde nelerin, hangi nedenle değiştiği açıklanmaktadır. Sonuçlara dayanarak, bu çalışmada ilk kez yeni günlük dosyası formatının anahtar öğeleri açıklanmaktadır. Günlük çalışma sırasında ortaya çıkabilecek sorunlar üzerinde durulmuştur. Son olarak, günlük parçalarından bilgilerin nasıl kurtarılacağına ilişkin bir yöntem önerilmektedir. Bir soruşturma sırasında bozuk bir olay günlüğünden bilgileri kurtarmak için önerilen bu yöntemi başarıyla uygulamışlardır.

Monteiro ve arkadaşları [20] yaptıkları çalışmada, adli incelemeler için sistem günlüklerinin doğrulanması ve doğrulama mekanizması için bir teknik önermişlerdir. Sistem günlüklerinin güvenliğini sağlamaya yönelik araştırmalar, önleme ve tespit etmeye odaklanan gelişmiş sistem günlüğü protokolleri ortaya çıkarmıştır. Bununla birlikte, bu protokollerin çoğu, güvenlik açısından yeterli olsalar da, adli incelemeler devreye girdiğinde yetersiz olduğundan, hukuki açıdan, olay yerinde bulunan her türlü kanıtın doğrulanması gerektiğinden ve mahkemeye sunulan herhangi bir bulgunun gerçek, inandırıcı ve güvenilir olması gerektiğinden bahsetmişlerdir. Bu çalışma, suç mahallinde yer alan tüm varlıkları, uygulamayı kullanan kullanıcı, kullanılan sistem ve bir kullanıcı tarafından sistemde kullanılan uygulamaları birbirine bağlayan, doğrulayan bir yöntem sunmaktadır.

Ibrahim ve arkadaşları [21] yaptıkları çalışmada, otomatik şifre tahmin saldırısı ve hackleme gibi siber suç faaliyetleri yapmak amacıyla VMware yazılımı kullanarak sanal ortamda Windows işletim sistemi kurmuşlardır. Saldırıdan sonra, mağdur sistemindeki olay kayıtlarının analizini yapmışlardır. Araştırmalarında, Windows işletim sistemindeki kayıt defteri ve Windows olay günlüğü gibi ana kanıt kaynaklarına odaklanmışlardır. Analiz edilen kayıtların kabul edilebilirliğini değerlendirmişlerdir. Ek olarak kanıtlar, suçun işlendiğine dair mahkemeyi ikna edebilirliği açısından değerlendirilmiştir.

Saleh ve arkadaşları [22] yaptıkları çalışmada, log kayıtlarının adli analizinin resmileştirilmesi için bir model önermektedirler. Belirli bir sistemin günlüklerinden çıkarılan olaylar bir ağaç olarak modellenmiştir. Modelin özellikleri dinamik, doğrusal ve

zamansaldır. Model özelliklerine sahip bir mantığın formülleri olarak ifade edilmektedir. Bu mantık için bir model kontrol algoritmasının geliştirilebileceği tablo tabanlı bir kanıtlama sistemi sağlanmaktadır. Önerilen yaklaşımı göstermek için Windows denetim sistemi incelenmiştir. Elde edilen veriler, bir sistemin değişmez özelliklerini, adli hipotezler ile genel veya belirli saldırı imzalarını içermektedir. Ayrıca adli incelemelerde bu sistemin kabul edilebilirliği ve altında yatan doğrulama sorunları tartışılmaktadır.

Murphey [23] yaptığı çalışmada, adli incelemeler için Windows XP ve Windows 2003 işletim sistemlerinde olay günlüklerinin kurtarılmasını ve analizlerini otomatikleştirmek için yöntemler önermektedir. Gerekliliklerin belirlenmesi ve ek olarak uygulanacak yöntemlerin değerlendirilmesini yapmıştır. Gereksinimleri temel alarak, genellikle olay günlüklerinde görülen yaygın bir bozulma türünün onarımını otomatikleştiren yeni, ücretsiz olarak kullanılabilen bir araç sunulmaktadır. Bu araç, birden çok olay günlüğünün onarımını kullanıcı müdahalesi olmadan tek bir adımda otomatikleştirmiştir.

Horsman ve arkadaşları [24] yaptıkları çalışmada, depolanan veri tabanı günlük dosyaları sayesinde Windows 10 Zaman Çizelgesi özelliğinin incelenmesini gerçekleştirmişlerdir. Windows Zaman Çizelgesi ile birlikte etkinlik kutucuğunu kurtarma ve bilgileri işleme becerisini gösteren inceleme sonuçları ve destekleyen deneysel metodolojiler sunulmuştur. Ayrıca, içinde depolanan verilerin yorumlanmasını desteklemek için bir SQL sorgusu yapmışlardır.

Do ve arkadaşları [25] yaptıkları çalışmada, Windows işletim sistemi olay günlüğü dosyalarını analiz etmek için bir Windows olaylarının adli sürecini (WinEFP) sunmuşlardır. WinEFP, Windows adli incelemelerinde karşılaşılan bir dizi ilgili olayı kapsadığından bahsetmişlerdir. Windows olaylarının, incelemecilere adli soruşturmalar için rehberlik sağladığını vurgulamışlardır.

Neyaz ve arkadaşları [26] yaptıkları çalışmada, şüpheli bir sistemde adli inceleme yapabilmek için Windows Olay Görüntüleyicisinin nasıl kullanılabileceğini anlatmaktadırlar. Ayrıca, Windows Olay görüntüleyicisindeki bulguları desteklemek için, Windows kayıt defterinin sisteme bağlı USB cihazlarının bilgilerini tanımlama potansiyelini de tartışmışlardır. Sisteme ilk kez bağlanan bir USB cihazının kurulum bilgilerini içeren

günlük ayrıntılarını çıkarmak ve gerekli tanımlayıcıları ve zaman damgası ayrıntılarını almak için Windows 10 dosya sistemini kullanmışlardır.

Moskvichev ve arkadaşları [27] yaptıkları çalışmada, Windows işletim sistemini kullanan kaynaklardan olay günlüklerini toplamak ve analiz etmek için evrensel bir sistem uygulamışlardır. Günlüklerden veri toplamak için olay yönlendirme teknolojisini kullanmaktadırlar. Windows işletim sistemini çalıştıran kaynaklardan olay günlüğü girdilerini iletmek için mevcut yöntemleri analiz etmişlerdir. Windows işletim sistemi üzerinde çalışan olay kaynaklarının olay toplayıcıya nasıl bağlanacağını ayrıntılı olarak açıklamışlardır. Olay toplayıcısını güvenlik bilgilerine ve olay yönetimine bağlamak için bir şema önermişlerdir.

Al-Saleh ve arkadaşları [28] yaptıkları çalışmada, suç faaliyetlerini gizlemek için bir suçlunun izleyebileceği yollardan biri olan silinmiş kullanıcı hesaplarından kanıtların nasıl toplanacağından, Windows olay günlüklerinde, kayıt defterinde, RAM'de, sayfa dosyasında ve sabit sürücülerde kanıtların aranabileceğinden bahsetmişlerdir.

Shin ve arkadaşları [29] yaptıkları çalışmada, silinen veya hasar gören olay hakkında bazı kurtarma algoritmaları önermişlerdir. Günlük dosyası ve kurtarma algoritmalarının deneyler yoluyla yüksek başarı oranına sahip olduğunu göstermişlerdir.

Shi-bo [30] yaptığı çalışmada, veri kaynağı olarak Windows sistem günlüğünü veri tabanı teknolojisi ile birleştirmiştir. Ayrıca bilgisayar saldırı tespitini günlük temelli olarak gerçekleştirmiştir.

Ning ve arkadaşları [31] yaptıkları çalışmada, Windows günlüğü sistem dosyalarının, Windows sisteminin denetim verilerini elde etmek için API gibi bir mekanizma kullandığından bahsetmişlerdir. Windows günlüğünün analizi ile birlikte bilgisayar günlüğü analizi ve güvenlik denetim tabanlı evrensel model sunmuşlardır.

Söderström ve arkadaşları [32] yaptıkları çalışmada, denetim günlüğünü almak, saklamak ve yönetmek için bir yaklaşım önermişlerdir. Ayrıca, güvenli bir şekilde dağıtılmış ortamlardaki kuruluşların farklı yerel ağlardan tek bir merkezi sunucuya denetim günlüğü işlemleri göndermesinin gerekliliğini belirtmişlerdir.

Polczynski [33] yaptığı çalışmada, günlüklerin gerçekte ne olduğundan, günlük analizinin, güvenlik denetimleri, hata ayıklama, performans denetimleri vb. konular için önemli olduğundan bahsetmiştir. EVTX dosyalarını dönüştürme ve içine ekleme görevi gören özel bir veritabanı ve günlük analizi için LogProcessor programı kullanarak analizler yapmıştır.

Sahoo ve arkadaşları [34] yaptıkları çalışmada, Windows olay günlüğü ortamı ve merkezileştirme gibi günlüğe kaydetme süreçlerine genel bir bakış yapmışlardır. Bu araştırma çalışmasında, depolamayı merkezileştirmek için merkezi sunucu olarak Winsyslog sunucusu kullanılmıştır. Winsyslog sunucusu, Windows olaylarının çevirisi için günlük verilerini ve olay raporlayıcısını ikili formattan syslog formatına dönüştürmüştür. Önerdikleri günlük verilerinin depolanmasını merkezileştiren mimarinin sistem yöneticisini harika bir şekilde basitleştirerek günlüğe kaydetme işlemi yaptığını vurgulamışlardır.

Henkoğlu [35] yaptığı çalışmada, işletim sistemine ait olay günlükleri metin tabanlı olmasına rağmen, kendine has (binary) özelliğinden dolayı, içeriğinin görüntülenebilmesi için yardımcı olay günlüğü izleme programlarının kullanımını gerektiğini belirtmiştir. Uygulama, güvenlik ve sistem olaylarını görüntülemek için, işletim sistemi üzerinde bulunan olay görüntüleyicisi kullanılabileceğinden, Olay Görüntüleyicisini açmak için Windows 7 ve Windows Xp işletim sistemlerinde kullanılabilecek yollardan bahsetmiştir. Olay günlüklerinin uzantısı ya da dosya yapısının değiştirilmiş olması halinde, dosya imzası üzerinden bakılması gerektiğini söylemiştir. Ek olarak Olay günlüklerini görüntülemek için, işletim sistemi olay görüntüleyicisi haricinde, daha kullanışlı ve ücretsiz yazılımların da internet üzerinden temin edilebileceğinden bahsetmiştir.

3.2. Linux İşletim Sisteminin Adli Bilişim Açısından Log Dosyalarının İncelenmesi ile İlgili Araştırmalar

Ling [5] yaptığı çalışmasında, bilgisayar adli biliminin tanımını, bilgisayar adli bilişim ile geleneksel adli bilişim arasındaki farklılıkları dile getirmiştir. Ayrıca bilgisayar adli bilişiminde incelenmesi gereken ek nesneleri açıklamıştır. Ondokuzuncu Bilgisayar Güvenlik Teknolojisi Toplantısında kabul edilen, bilgisayar adli analiz modelinin aşamalarının tanımını yapmıştır. Kayıt sisteminin bağlantı olay günlüğü, denetim günlüğü sistem günlüğü olarak üç bileşenden oluştuğunu belirtmiştir. Linux işletim sisteminde yer

alan bazı logların görevlerini açıklamıştır. Sonuç olarak Linux işletim sistemi adli analizinde esas olarak sistem günlüğüne dayandığını belirtmiştir.

Zeng ve arkadaşları [6] yaptıkları çalışmada, log kayıtlarının ne amaçla kullanıldığını açıklamışlardır. Log kayıtlarının bazı önemli bilgiler tuttuğunu söylemişlerdir. Dijital adli bilişimin log kayıtları analizi ile yapıldığını, kaydedilen log kayıtlarının sanallaştırma yapılarak da analiz edilebileceğini söylemişlerdir. Loglama mekanizmasını açıklamışlardır. Linux loglamada IETF syslog protokolünü, çekirdek mesajlarını, Linux denetim sistemi ile bunlara ait güvenlik sorunlarını açıklamışlardır. Microsoft Windows işletim sistemine ait event logların formatını, yapısını ve güvenlik loglarını açıklamışlardır. Sonuç olarak log dosyalarından veri toplama işleminin sorun olmadığı ancak analiz ve raporlamanın zor olduğunu, Linux/Unix loglama ve Windows loglama gereksinimlerinin, farklı olmadığı, her ikisinin de güvenli kaydetme ve aktarma gerektirdiğini, kendi iç güvenlik açıklarının olduğunu belirtmişleridir.

Chen ve arkadaşları [36] yaptıkları çalışmada, gelişmiş saldırıların yaşam döngüsünü analiz etmek için simüle edilmiş bir ortam oluşturmuşlardır. Ayrıca, Linux günlükleri aracılığıyla gelişmiş saldırıları tanımlayabilen bir saldırı algılama modeli tasarlamışlar ve uygulamışlardır. Normal davranışları kötü niyetli davranışlardan ayırmak için makine öğrenimi modelleri kullanmaktadırlar.

Anuradha ve arkadaşları [37] yaptıkları çalışmada, suça karışan şüpheliler tarafından kullanılan Linux işletim sistemine sahip sabit diskin derinlemesine analizi ile diskte yüklü olan Google Chrome internet tarayıcısının silinmiş tarama verilerinin, günlük dosyaları sayesinde kurtarılmasına odaklanmışlardır.

Dos Santos Almeida ve arkadaşları [7] yaptıkları çalışmada, ilk olarak bilgisayar adli bilişim terimlerini ve adli incelemelerde kullanılan Wireshark, TSK, Stegdetect, Steghide, USBview, NuDetective araçlarını açıklamışlardır. Kavramların uygulanması için pedofili içeriği dosya paylaşımı olan örnek bir deneysel olay oluşturmuşlardır. Çalışma platformu olarak Linux işletim sistemini kullanmaktadırlar. Bilgisayar dinleme, depolama cihazları analizi gibi işlemler yapmaktadırlar. Böylece suçu tam ispatlamayı amaçlamışlardır.

Studiawan ve arkadaşları [38] yaptıkları çalışmada, yaygın olarak kullanılan Linux işletim sistemi, web server sunucuları gibi sistemlerde log dosyalarını otomatik olarak ayrıştıran bir araç sunmaktadırlar. Bu amaca yönelik temel mimari olarak derin makine öğrenimi tekniğini kullanmaktadırlar. Diğer log ayrıştırıcı araçları ile karşılaştırma yaptıklarında önerdikleri aracın performansının daha üstün olduğunu göstermişlerdir.

Urrea ve arkadaşları [39] yaptıkları çalışmada, adli soruşturma sırasında bilgisayar sistemlerinde uçucu bilgilerin kritik öneme sahip olduğunu belirtmiş olup RAM analizi yapmışlardır. Ancak modern işletim sistemleri gereği, programlar ve dosyalar bitişik olarak depolanmamaktadır bu da bir sayfa boyutundan daha büyük dosyaların geri alınması çabalarının çoğunu boşa çıkarmaktadır. Bu sebeple yaptıkları çalışmada RAM'de bulunan bir sayfa boyutundan daha büyük dosyaların alınmasını kolaylaştırmak için SUSE Linux sistem çekirdeği sürüm 2.6.13- 15'teki bellek yönetimi yapılarını araştırmışlardır.

Andrade ve arkadaşları [40] yaptıkları çalışmada, Linux sunucusu incelemişlerdir. Bu araştırmada güvenlik açıklıklarını belirlemede yaygın olarak kullanılan Metasploit, Nessus, Whatweb, Nmap, PHP-Backdoor ve Weevely olmak üzere Linux BackTrack5 araçlarını kullanmışlardır. Pasif saldırılar sonucunda oluşan adli kanıtları analiz ederek bu saldırıların nasıl belirleneceğini tespit etmişlerdir.

3.3. MacOS İşletim Sisteminin Adli Bilişim Açısından Log Dosyalarının İncelenmesi ile İlgili Araştırmalar

Turedi ve arkadaşları [41] yaptıkları çalışmada, MAC OS işletim sisteminin popülerliğinin arttığı ancak adli bilişim araçlarının bu yönde gelişiminin emekleme aşamasında olduğunu belirtmişlerdir. Bu sebeple Mac OS X sistemlerinin inceleme uzmanları tarafından manuel olarak yapılmakta olduğu özellikle günlük dosyaları gibi büyük miktarda verinin incelemesinin maliyetli ve zaman alıcı olduğunu belirtmişlerdir. Bu sorunu çözmek için Mac OS X işletim sisteminin günlük dosyalarının otomatik olarak analizini önermişler ve geliştirmişlerdir. Yaptıkları deney sonucunda günlük dosyalarının etkili bir şekilde analiz edildiğini görmüşlerdir.

Kopytko [42] yaptığı çalışmada, ilk olarak günlük dosyasının içeriği ve günlük dosyalarının kullanım imkanlarını ayrıntılı olarak açıklamıştır. Bu bölümden sonra uygulamanın tasarımı

ve gereksinimlerini açıklamıştır. Uygulamanın amacı, günlükler ve birleşik günlük kayıt sistemi hakkında mevcut bilgileri toplamak ve bunların analizine izin verecek uygulamayı oluşturmaktır. Analiz için Swift ile bir macOS GUI uygulaması olarak Program oluşturmuşlardır.

Nedelkoski ve arkadaşları [43] yaptıkları çalışmada, günlük verilerini ayrıştırmada kullanılan mevcut yaklaşımlar belirli günlük türlerini ayrıştırmasını sağladığı için NuLog adlı yeni bir ayrıştırma tekniği önermektedirler. Günlük ayrıştırma sorununu çözmek için maskelenmiş kelime tahmini öğrenme yöntemi benimsenmiştir. NuLog'un etkinliğini değerlendirmek için deneyler yapılmıştır. Deneylerde Apache, Windows, Mac, Android gibi günlük verilerini kullanmışlardır. Sonuçların, NuLog'un Doğruluk, düzenleme ve sağlamlık açısından mevcut günlük ayrıştırıcılardan daha iyi performans gösterdiğini belirtmişlerdir.

Windows, Linux ve Mac işletim sistemlerine ait log dosyaları inceleyen literatürdeki çalışmalar incelendiğinde çalışmaların çoğunun Windows işletim sistemine ait olduğu görülmektedir. Linux ve Mac işletim sistemlerine ait çok fazla çalışma görülmemektedir.

Popüler olarak kullanılan Xways, Encase, FTK gibi adli bilişim yazılımları Windows işletim sistemini desteklemektedir [44]. Linux ve MAC işletim sistemlerinde adli bilişim uzmanları için veri toplamak zordur[45]. Bu sebeple söz konusu işletim sistemi bulunan bulgularda incelemeler genellikle manuel yapılmaktadır.

Yapılan literatür taraması sonucunda, suçun ve suçlunun tespitine yönelik önem arz ettiği değerlendirilen log kayıtları incelemelerinin, yapılan literatür taraması kapsamında incelenen çalışmalarda kısmen verildiği, yüzeysel tutulduğu ve log kayıtları ile ilgili incelemelerin farklı farklı çalışmalarda yer aldığından dağınık olduğu görülmüştür. Ancak Linux işletim sistemlerinde log kayıtları oldukça fazla ve adli bilişim incelemeleri açısından oldukça önemlidir. Aynı zamanda yapılan incelemelerin canlı sistemler üzerinde yapıldığı görülmüştür. Söz konusu incelemelerde, kriminal incelemelerde kullanılan herhangi bir adli bilişim yazılımı kullanılmadığı ve tespitlerin adli bilişim yazılımı kullanılmaksızın yapıldığı görülmüştür. Ancak adli soruşturmalarda bulgu güvenliğini sağlamak amacıyla genellikle incelemeler bulgunun adli kopyası üzerinde yapılmaktadır.

4. METODOLOJİ

Çalışmanın bu bölümünde kullanılan yazılımlar ve donanımlar ile çalışma kapsamında uygulanan adımlar açıklanmıştır.

4.1. Kullanılan Yazılımlar ve Donanımlar

Linux işletim sistemine sahip bilgisayarlar üzerinde adli bilişim açısından önem arz eden log kayıtlarının incelenmesi aşamasında aşağıda belirtilen donanımlar ve yazılımlar kullanılmıştır.

Veri İnceleme Bilgisayarı

Dijital bulguları incelemek için gerekli olan adli bilişim yazılımlarının yüklü olduğu ve bu adli bilişim yazılımlarının stabil şekilde çalışması için gerekli donanıma sahip yüksek performanslı bilgisayardır. Bu çalışma kapsamında kullanılan yazılımlar veri inceleme bilgisayarına yüklenerek yapılacak olan incelemelere hazır hale getirilmiştir.

AccessData FTK Imager

Harici depolama birimi olarak kullanılan aygıtların (sabit disk, USB bellek, hafıza kartı, CD/DVD vb.) çeşitli formatlarda adli kopyasını almayı, üzerinde ön izleme ve görüntüleme yapmayı sağlayan yazılımdır. Söz konusu yazılım, üzerinde deneyler yapılan sabit diskin adli kopyasını almak için kullanılmıştır.

Encase 6.19.7.2 Yazılımı

Guidance Software şirketi tarafından geliştirilen harici depolama birimi olarak kullanılan aygıtların (sabit disk, USB bellek, hafıza kartı, CD/DVD vb.) adli kopyasını oluşturmayı, analiz ve bu analizleri raporlamayı sağlayan yazılımdır. Söz konusu yazılım adli kopyası alınan sabit diskin incelemesini yapmak için kullanılmıştır.

X-Ways Forensics Yazılımı

Harici depolama birimi olarak kullanılan aygıtların (sabit disk, USB bellek, hafıza kartı, CD/DVD vb.) adli kopyasını oluşturmayı, analiz ve bu analizleri raporlamayı sağlayan, aygıtların içerisinde kaybolan/silinmiş kısımları otomatik olarak tanımlayabilen yazılımdır. Söz konusu yazılım adli kopyası alınan sabit diskin incelemesini yapmak için kullanılmıştır.

Dcode.v4.01

Çeşitli formatlardaki tarih/saat verisini kullanıcı tarafından okunabilen zaman damgalarına dönüştürülmesine yardımcı olan programdır.

Notepad++

Metin, kaynak kodu görüntüleyici ve düzenleyicisidir. Söz konusu yazılım metin tabanlı dosyaların incelemesini yapmak için kullanılmıştır.

plistEditor Pro V 2.5

".plist" uzantılı dosyaları hem ikili formatta hem de XML biçiminde görüntülemeye ve düzenlemeye yardımcı olan araçtır. Söz konusu yazılım ".plist" uzantılı dosyaların incelemesini yapmak için kullanılmıştır.

Bu çalışma kapsamında yapılan deneylerde aşağıda belirtilen araç ve gereçler kullanılmıştır.

- Bilgisayar ve takılı vaziyette bulunan sabit disk
- Format CD'si (Linux İşletim Sistemi (Ubuntu 18.04.4 LTS)
- Farklı marka/model cep telefonları (Android ve İOS işletim sistemine sahip)
- Yazıcılar
- Farklı marka/model USB bellekler ve hafıza kartları

4.2. Uygulama Adımları

Bu çalışmada Linux işletim sistemi üzerinde adli bilişim incelemelerini yürütmek için üç aşamalı bir uygulama gerçekleştirilmiştir.

1. Çalışma kapsamındaki verilerin belirlenmesi
2. Çalışma kapsamındaki verilerin oluşturulması
3. Çalışma kapsamındaki verilerin analizi ve incelenmesi

4.2.1. Çalışma kapsamındaki verilerin belirlenmesi

Bu çalışma kapsamında, adli incelemelerde suçun ve suçlunun tespitine yönelik önem arz ettiği değerlendirilen hususlar doğrultusunda seçilen log kayıtları aşağıda nedenleri ile birlikte belirtilmiştir.

İşletim sisteminin kurulma bilgilerine ait log kayıtları

Bilgisayarda kurulu işletim sistemi ve versiyon bilgisinin tespiti incelemenin önemli aşamalarından bir tanesidir. Uzmanlara, yapılacak işlerin belirlemesinde kolaylık sağlamaktadır. Bir işletim sistemi, yalnızca diğer işletim sistemlerine göre farklılık göstermez, aynı işletim sisteminin farklı sürümleri arasında da farklılıklar bulunmaktadır [46]. İşletim sisteminin sürümleri arasında büyük farklılıklar olabileceğinden sistem dosyalarının belirlenmesi, ağaç yapısının belirlenmesi, kullanılabilecek adli bilişim yazılımlarını belirleyerek inceleme uzmanının inceleme planı hazırlamasını ve zamandan tasarruf etmesini sağlar. Bu da inceleme süresinin kısalmasına etki etmektedir.

Oluşturulan ve silinen kullanıcıların tespitine ait log kayıtları,

Birden fazla kullanıcıya sahip bilgisayarlarda, kullanıcı bilgilerinin tespiti; hangi kullanıcının kaç kez oturum açmış olduğu, hangi işlemleri yapmış olduğu, hangi dosyaya erişim sağlamış olduğu, hangi dosyaları değiştirmiş olduğu vb. bilgilerin tespiti şüphelinin suçluluğunun/suçsuzluğunun tespitine karar verme açısından önem arz etmektedir. Güvenliği ihlal edilmiş bir sistemdeki kullanıcıların incelenmesi mevcut kullanıcılarla sınırlı olmamalı, silinmiş kullanıcılar da incelenmedir [47].

Kullanıcının oturum açma ve kapatma bilgilerine ait log kayıtları,

Kullanıcı hareketlerini izleme, adli sürecin önemli bir parçasıdır. Olağandışı kullanıcı etkinliği, sistem sorunu veya bir güvenlik sorunu olduğunun göstergesidir. Sistem günlükleri sayesinde kullanıcı hareketlerini analiz ederek, kimlik doğrulama sorunları ve bilgisayar korsanlığı etkinliği belirlenebilir [48]. Log bilgilerine bakılarak başarısız oturum açma denemelerinin sayısı ile oturum açma deneme periyotları gerçek suçluya ulaşmada etkin bir tespit yöntemi olarak kullanılabilir. Örneğin; saniyelik zaman dilimi içerisinde yüzlerce başarısız oturum açma denemesi yapılmış olduğu tespit edilmiş ise, bu tespit sonucunda bilgisayarlara, bilgisayar ağlarına veya sunuculara dışarıdan bir saldırı olduğu değerlendirilmesi yapılabilir.

Bilgisayarın başlatma ve kapatma tarihine ait log kayıtları,

Bilgisayarın kapatılma tarihi bilgisi ile bilgisayarda bulunan verilere ait üstveri (dosya konumu, boyutu, en son ne zaman yazıldığı, erişildiği vb.) bilgilerinin tutarlı olması gerekmektedir [5]. Bu sebeple bilgisayarın başlatma ve kapatma tarihlerine bakılarak

araştırılan suçun söz konusu bilgisayarda işlenip işlenmediği hususunda değerlendirme yapılabilir.

Tarih-saat ve saat dilimi değişikliğine ait log kayıtları,
Tarih ve saat bilgileri, birçok adli bilişim incelemesinin temel bir parçasıdır. Çünkü bunlar gerçek dünya ile bilgisayar kanıtları arasında somut bir bağlantı temsil ederler [49]. Bilgisayarda olay günlükleri sistem üzerinde yapılan her işlemin tarih ve saat bilgisi ile beraber kaydedilmesi sonucu oluşmaktadır. Önemli kanıtların değerlendirilmesi ve karşılaştırılması ile doğru bir sonuca varabilmek için sistem saatinin ve kullanılan saat diliminin bilinmesi gerekmektedir. Bu sebeple log kayıtlarında, bilgisayar sistemleri üzerinde yapılan her türlü tarih ve saat değişikliğinin tespit edilmesi araştırılan suçun işlenme zamanı ile birlikte değerlendirilmelidir.

Bilgisayara takılan harici veri depolama cihazlarına ait kayıtlar,
Bilgisayara takılan depolama cihazları ile ilgili izlerin tanımlanması, birçok bilgisayar suçu kategorisinin araştırılmasında paha biçilmez bir parçadır. Örneğin çocuk istismarı soruşturmalarında, ilgili dosyaların herhangi bir bağlı cihaza mı yoksa bu cihazlardan mı aktarıldığını belirlemek zorunludur [50]. Bu sebeple bilgisayara takılan veri depolama cihazlarına ait ayırt edici bilgiler (seri numarası, ürün ID, depolama cihazının ismi, markası vb.) bazı suçların aydınlatılmasında kullanılabilmektedir.

Yüklenen programların tespiti amacıyla oluşan kayıtlar,
Suç işlemek için kullanılmış bilgisayarda yüklü ve daha önce yüklenmiş programları tespit etmek adli bilişim uzmanları için değerli olabilir [51]. Zararlı yazılım veya suça konu programların yüklü olup olmadığı, yüklü ise ne zaman yüklendiği ve kullanıldığı, silindi ise ne zaman silindiği gibi bilgiler toplanmalıdır.

Ağ üzerinden erişim ve kablolu erişim noktalarına yapılan bağlantılara ait log kayıtları,
İncelemesi yapılan bilgisayarda ağ üzerinden ve kablolu erişim noktalarına yapılan bağlantılar incelerek ağda kullanılan IP adres bilgileri elde edilmektedir. Ayrıca cep telefonlarının MAC adreslerinin tespiti ile MAC adresi tespit edilen cep telefonunun o bilgisayarda internet erişimi yapıp yapmadığı hakkında bilgi sahibi olunmaktadır. Bilgisayar, cep telefonu gibi cihazların MAC adreslerinin tespitiyle incelemenin desteklenmesi önemlidir [52].

Yazıcılardan çıktı alındıktan sonra oluşan kayıtlar,

Bir şüpheli şirketten ayrılmadan önce çalmak istediği hedef dosyayı yazdırabilir. Yazdırma programının günlük dosyaları, program aktiviteleri, söz konusu dosyanın basılı görüntülerini içeren dosyalar ve her bastırma işlemi için kullanılan bilgiler(spool dosyaları) registry kayıtları ile ilişkilendirilmesiyle tespit edilebilir [53]. Bu sebeple bu bilgiler incelemeci ve soruşturmacı açısından önem arz etmektedir.

Backup alınması sonucunda oluşan kayıtlar,

Bilgisayarda bir dosyayı silmek tamamen ortadan kalkmayan bir iz oluşturur. Bilgisayar sistemlerinin bilgileri kaydetme biçimi nedeniyle, bir dosya silindiğinde, dosyanın kapladığı alan boşa çıkar, bir başka dosyanın saklanması için kullanılabilir hale getirilir. Adli bilişim uzmanları, üzerine veri yazılana kadar bu dosyayı kurtarabilir. Üzerine veri yazılsa bile bu dosyanın tamamen silindiği anlamına gelmez. Başka bir ortama kopyalanmış, sistem yedeğine kaydedilmiş veya e-posta olarak gönderilmiş olabilir [54]. Bu sebeple yedek dosyalarının incelenmesi sonucunda alınan kopya içerisinde mevcut/silinmiş alanlarda yer almayan verilerin yedek dosyalarının içerisinde yer alabileceği değerlendirilerek incelemelerin alınan yedek dosyaları içerisinde de gerçekleştirilmesi önem arz etmektedir. Log kayıtları incelenerek sistemin yedek dosyasının alınıp alınmadığı hakkında değerlendirme yapılması gerekmektedir.

4.2.2. Çalışma kapsamındaki verilerin oluşturulması

Çalışma kapsamında belirlenen verilerin tespit edilebilmesi için verileri oluşturmak amacıyla çok sayıda deneyler yapılmıştır. Adli bilişim incelemelerinde delil bütünlüğünün önemli olması sebebiyle tüm deneyler aynı sabit disk üzerinde yapılmış, sabit disk üzerinde yapılan her deneyden sonra tek tek adli kopyası alınmamıştır. Bütün deneyler yapıldıktan sonra söz konusu sabit diskin bir adli kopyası alınmıştır. Böylelikle alınan adli kopya üzerinden inceleme yapılarak bulgu bütünlüğünün sağlanması amaçlanmıştır. Bu deneylerin yapılma şekli aşağıda belirtilmiştir.

<u>Linux işletim sistemi kurulumu</u>

Bu çalışma kapsamında belirlenen işletim sitemi Linux işletim sistemi seçildiğinden incelemesi yapılacak olan bilgisayarın BIOS ayarlarında gerekli ayarlar yapılarak Linux

işletim sisteminin Ubuntu 18.04.4 LTS versiyonunun bulunduğu format CD'si ile Linux işletim sistemi 13 Şubat 2020 tarihinde kurulmuştur. Kurulum esnasında kullanıcı adı "kkk", bilgisayar adı "kkk"ve konum "İstanbul" seçilmiştir.

İncelemesi yapılacak bilgisayara Linux işletim sisteminin başarılı bir şekilde kurulumu tamamlandıktan sonra bu çalışmada belirlenen problemlere çözüm bulmak amacıyla standart bilgisayar kullanıcısı tarafından yapılabilecek işlemler gerçekleştirilmiştir. Bilgisayara yeni kullanıcı hesapları açılmış, açılan bazı kullanıcılar tarafından oturum açılmış ve kapanmıştır. Bazı kullanıcılar yanlış şifre girerek oturumlarını açamamıştır. Bazı kullanıcılar işlem yapmadan, bazı kullanıcıları ise bilgisayarı kullandıktan sonra silinmiştir. Bilgisayar farklı tarih ve saatlerde açılmış ve kapanmıştır. Açılan bilgisayarda ad değişikliği, tarih-saat değişikliği ve saat dilimi değişikliği yapılmıştır. Söz konusu bilgisayara çeşitli programlar yüklenmiş ve harici veri depolama cihazları takılmıştır. Bilgisayar üzerinden ağa bağlantı işlemleri gerçekleştirilmiştir. Ağ üzerinde bulunan yazıcılarla çıktı alınmıştır. Bilgisayarın sistem yedeği alınmıştır. Yapılan tüm işlemlerden sonra incelemesi yapılacak bilgisayarın adli kopyası alınmıştır.

Bilgisayarın ad bilgisinin değiştirilmesi

Bilgisayar ad bilgisi değişikliğinin tespit edilmesi amacıyla incelemesi yapılacak bilgisayarda root yetkisiyle açılan terminal ekranına "gedit/etc/hostname" komutu girilmiştir. Açılan dosya içerisinde "kkk" olan kullanıcı adı "kubra" olarak değiştirilmiş ve açılan dosya kaydedilerek kapatılmıştır. İşlem gerçekleştikten sonra "gedit/etc/hosts" komutu girilmiştir. Açılan dosya içerisinde "kkk" olan bilgisayar adı "kubra" olarak değiştirilmiştir ve açılan dosya kaydedilerek kapatılmıştır.

Kullanıcı hesabı oluşturma ve silme

İncelemesi yapılacak bilgisayarda yeni kullanıcı hesabı oluşturma işlemi için birinci yöntem olarak root yetkisiyle açılan terminal ekranına "useradd burak" komutu ile "burak" isimli kullanıcı oluşturulmuştur. Burak isimli kullanıcı için "mkdir/home/burak"komutu kullanılarak ev dizini oluşturulmuştur. Söz konusu kullanıcı için "passwd burak" komutu kullanılarak oturum açma parolası 1 olarak belirlenmiştir. Aynı komutlar kullanılarak

“hikmet” ve “fatma" kullanıcıları da oluşturulmuştur. “hikmet” ve “fatma” isimli kullanıcıların şifreleri “12345” olarak belirlenmiştir.

İncelemesi yapılacak bilgisayarda yeni kullanıcı hesabı oluşturma işlemi için ikinci yöntem olarak arayüz kullanılmıştır. Ayarlar menüsünde bulunan “Users” bölümünden “Kübra” isimli yeni kullanıcı hesabı oluşturulmuştur.

İncelemesi yapılacak bilgisayarda kullanıcı hesabı silme işlemi için birinci yöntem olarak root yetkisiyle açılmış terminal ekranına “sudo userdel hikmet” komutu ile hikmet kullanıcısı silinmiştir. Söz konusu kullanıcıya ait ev dizini ise “sudo rm –r /home/hikmet” komutu kullanılarak silinmiştir. “hikmet” isimli kullanıcı incelenecek bilgisayar üzerinde herhangi bir işlem yapmadan, oturum açma işlemi gerçekleştirmeden silinmiştir. İncelemesi yapılacak bilgisayarda kullanıcı hesabı silme işlemi için ikinci yöntem olarak arayüz kullanılmıştır. Ayarlar menüsünde bulunan “Users” bölümünde silinmek istenen kullanıcı hesabı üzerinden “Remove User” kısmına tıklanarak “Burak” isimli kullanıcı silinmiştir.

Kullanıcıların oturum açma ve kapatma işlemleri

Kullanıcıların oturum açma zaman bilgisinin tespiti edilmesi amacıyla incelemesi yapılacak bilgisayarda kkk kullanıcısının oturumu 13 Şubat 2020 tarihinde saat 16.08’de, burak kullanıcısının oturumu ise 14 Şubat 2020 tarihinde saat 10.35’te açılmıştır. “fatma” isimli kullanıcı ile oturum açma işlemi gerçekleştirilmemiştir.

Kullanıcıların oturum kapatma zaman bilgisinin tespiti edilmesi amacıyla incelemesi yapılacak bilgisayarda kkk kullanıcısının oturumu 13 Şubat 2020 tarihinde saat 16.13’te, burak kullanıcısının oturumu ise 14 Şubat 2020 tarihinde saat 16.23’te kapatılmıştır.

Başarısız oturum açma işlemlerinin tespit edilmesi amacıyla bilgisayarda bulunan “kkk” isimli kullanıcı ile 2 defa, “burak” isimli kullanıcı ile 1 defa ve son olarak da “fatma” isimli kullanıcı ile 1 defa yanlış şifre girilerek oturum açılmaya çalışılmış ancak şifrenin yanlış olması sebebiyle oturumları açılamamıştır.

Bilgisayarın başlatma ve kapatma işlemleri

Bilgisayarın başlatma bilgisinin tespit edilmesi amacıyla incelemesi yapılacak bilgisayar 13 Şubat 2020 tarihinde saat 17.00 ve 17.03 ile 14 Şubat 2020 tarihinde saat 08.20'de açılmıştır. Bilgisayarın kapatma bilgilerinin tespit edilmesi amacıyla incelemesi yapılacak bilgisayar 13 Şubat 2020 tarihinde saat 17.01 ve 17.04 ile 14 Şubat 2020 tarihinde saat 16.23'te kapatılmıştır.

Tarih-saat ve saat dilimi değişikliği

Tarih-saat değişikliğinin tespit edilmesi amacıyla incelemesi yapılacak bilgisayarda root yetkisiyle açılmış terminal ekranına timedatectl set–time '2010-02-03 15:15:15' komutu girilerek tarih "03.02.2010", saat ise "15:15:15" olarak değiştirilmiştir. Terminal ekranına date –s "02/09/2010 18:50:00" komutu girilerek de tarih saat değişikliği yapılmıştır. Saat dilimi değişikliğinin tespit edilmesi amacıyla root yetkisiyle açılmış terminal ekranına timedatectl set–timezone "Australia/Sydney" komutu girilerek saat dilimi "Australia/Sydney" olarak değiştirilmiştir.

Bilgisayara takılan harici veri depolama cihazları

Bilgisayara takılan harici veri depolama cihazlarına ait kayıtların tespiti amacıyla "4C530001050915117191" seri numaralı USB bellek, "000000001532" seri numaralı hafıza kartı, iki adet Android işletim sistemine sahip cep telefonu ve iki adet iOS işletim sistemine sahip cep telefonu bilgisayara takılmıştır.

Bilgisayara programların yüklenmesi

İncelemesi yapılacak bilgisayarda yüklü programların tespit edilmesi amacıyla işletim sistemi ile birlikte kurulan "Ubuntu Software" uygulaması üzerinden "Anlık Mesajlaşma Kişileri" uygulaması yüklenmiştir. Bu uygulama dışında "Teamviewer" ve "Messenger" programlarının internet üzerinden kurulum paketleri indirilerek terminal üzerinden komutlarla işletim sistemi üzerine kurulumu yapılmıştır.

Ağ yapılandırması, ağ üzerinden erişim, kablolu erişim noktalarına yapılan bağlantı işlemleri

Kablolu erişim noktalarına yapılan bağlantı işlemlerini tespit etmek amacıyla Android ve iOS işletim sistemlerine sahip ikişer adet cep telefonları ile incelemesi yapılacak bilgisayar arasında bağlantı kurulmuş olup internet erişimi sağlanmıştır. Ek olarak "192.168.2.141" IP adresine sahip yerel ağ ile bağlantı kurulmuştur.

Yazıcıdan çıktı alınması

Yazıcıdan çıktı alınması ile ilgili tespitlerin yapılması amacıyla incelemesi yapılacak olan bilgisayar ile "192.168.2.141" IP adresine sahip yerel ağda tanımlı farklı yazıcılardan 6 adet yazdırma işlemi gerçekleştirilmiştir. Örneğin; Canon marka LBP251 model "LBP251_e8_4d_d5" isimli yazıcı ile bağlantı kurularak "2018-2019-akademik takvim—1.pdf" isimli dosya yazdırılmıştır ve bu dosya incelenmiştir.

Sistem yedeğinin (backup) alınması

Linux sistemlerde çeşitli yedekleme araçları bulunmaktadır. Amanda(Linux işletim sisteminde backup alma yöntemlerinden biri) ve geleneksel onarma, geri yükleme araçlarının yanı sıra tek tek kopyalar oluşturmak için "rsync" aracı da kullanılabilir. Önerilen varsayılan yedekleme aracı Deja-Dup, rsync aracı kullanılarak yedekleme arşivleri oluşturulmaktadır. [55]. Deja-dup, Duplicity olarak bilinen komut satırı aracı için çoğu Linux işletim sistemlerinde standart yedekleme aracı olarak gelmektedir. Bu çalışmada da standart olarak gelen Deja-dup yöntemiyle yedekleme yapılmıştır.

İncelemesi yapılacak bilgisayarda sistem yedeğinin alınması ile ilgili tespitlerin yapılması için yedekleme menüsünden kaydetme yeri "Belgeler" olarak ayarlanıp 27.02.2020 tarihinde sistem yedeği alınmıştır.

FTK yazılımı ile imaj alma

Yapılan deneylerin sonucunda incelemesi yapılacak bilgisayar üzerinde bulunan disk bilgisayar kasasından çıkarılmıştır. Çıkarılan sabit disk, veri inceleme bilgisayarına yazma korumalı bir şeklide bağlanmıştır. FTK Imager yazılımı kullanılarak söz konusu sabit diskin "E01" uzantılı adli kopyası alınmıştır.

Bu çalışma metodolojisinin ikinci aşaması olan çalışma kapsamındaki verilerin oluşturulması, incelemenin doğruluğunun ispatı için oldukça önemlidir. Burada yapılan tüm deneyler sırasında yapılan tüm işlemler notları alınmalıdır. Alınan imaj adli bilişim prensiplerine göre saklanmalı ve incelenmelidir. Verilerin analizi ve incelenmesi aşamasında alınan kopya ve notların karşılaştırılarak değerlendirilmesi yapılmalıdır.

4.2.3. Çalışma kapsamındaki verilerin analizi ve incelenmesi

Çalışma kapsamında oluşturulan verilerin analizi için alınan kopyanın adli bilişim yazılımlarıyla incelemesi yapılmıştır. Tespiti yapılan kayıtlar, verilerin oluşturulması sırasında alınan notlar ile karşılaştırma yapılarak doğruluğu değerlendirilmiştir. Tespit edilemeyen kayıtlar için anahtar kelimeler oluşturarak anahtar kelime araması yapılmıştır. Anahtar kelime araması sonucunda verilerin tespit edilip edilemediğinin değerlendirmesi yapılmıştır.

Çizelge 4.1. Çalışma kapsamında belirtilen problemlerin analizinde kullanılan yazılımlar

	Xways Forensic	Encase	Notepad++	PlistEditor Pro	Dcode
İşletim sisteminin kurulma bilgilerine ait log kayıtları	Kullanıldı	Kullanılmadı	Kullanılmadı	Kullanılmadı	Kullanılmadı
Oluşturulan ve silinen kullanıcıların tespitine ait log kayıtları	Kullanıldı	Kullanılmadı	Kullanıldı	Kullanılmadı	Kullanılmadı
Kullanıcının oturum açma ve kapatma bilgilerine ait log kayıtları	Kullanılmadı	Kullanıldı	Kullanıldı	Kullanılmadı	Kullanıldı

Çizelge 4.1.(devam) Çalışma kapsamında belirtilen problemlerin analizinde kullanılan yazılımlar

Bilgisayarın başlatma ve kapatma tarihine ait log kayıtları	Kullanıldı	Kullanılmadı	Kullanıldı	Kullanılmadı	Kullanılmadı
Tarih-saat ve saat dilimi değişikliğine ait log kayıtları	Kullanıldı	Kullanılmadı	Kullanıldı	Kullanılmadı	Kullanılmadı
Bilgisayara takılan harici veri depolama cihazlarına ait log kayıtları	Kullanıldı	Kullanılmadı	Kullanıldı	Kullanılmadı	Kullanılmadı
Ağ üzerinden erişim ve kablolu erişim noktalarına yapılan bağlantılara ait log kayıtları	Kullanıldı	Kullanılmadı	Kullanılmadı	Kullanılmadı	Kullanılmadı
Yazıcılardan çıktı alındıktan sonra oluşan log kayıtları	Kullanıldı	Kullanılmadı	Kullanılmadı	Kullanılmadı	Kullanıldı
Backup alınması sonucunda oluşan log kayıtları	Kullanıldı	Kullanılmadı	Kullanılmadı	Kullanılmadı	Kullanılmadı

Çizelge 4.1' de görüldüğü üzere çalışma kapsamında belirtilen problemlerin analizi için kullanılan yazılımlar belirtilmiştir. Çalışma kapsamında "Xways Forensic" yazılımının Linux işletim sistemi dosya sistemlerini kısmen desteklemesinden dolayı alınan adli kopyanın analizinde ve anahtar kelime aramalarında kullanılmıştır. "Notepad" yazılımı disk içerisinde birden fazla sayıda bulunan log dosyalarında anahtar kelime aramalarında kolaylık sağlamasından dolayı söz konusu yazılım kullanılmıştır. Encase adli bilişim yazılımı ise byte byte incelemelerde, byte özelliklerinin daha kolay anlaşılmasını sağladığından söz konusu yazılım kullanılmıştır.

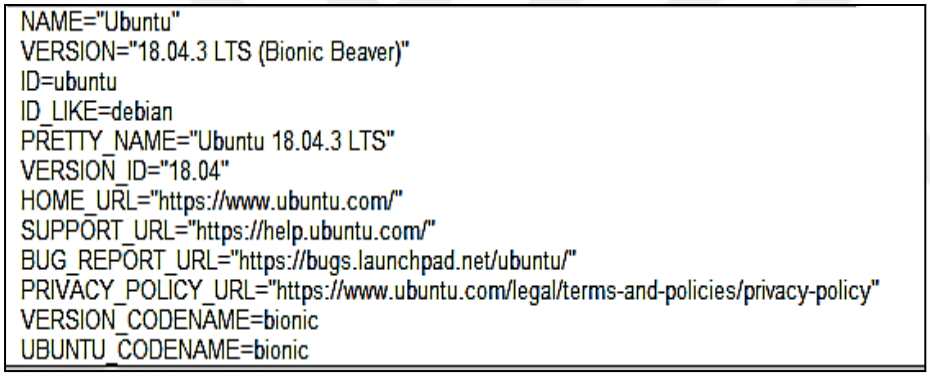
Çalışma sonunda ise yapılan tespitler ile literatür taramasıyla elde edilen bilgiler karşılaştırılarak log kayıtlarının nerelerde bulunduğunu gösteren bir çizelge oluşturulmuştur.

5. BULGULAR

Çalışmanın bu bölümünde, yapılan deneylerin analizi gerçekleştirilerek elde edilen sonuçlar değerlendirilmiştir. Böylelikle önerilen metodolojinin son aşaması olan çalışma kapsamındaki verilerin analizi ve incelenmesi aşaması tamamlanmıştır.

5.1. Kurulan İşletim Sistemi Bilgisi

Alınan adli kopya içerisinde "X-Ways Forensic" yazılımı kullanılarak işletim sistemi ile ilgili kelimelerin anahtar kelime aratılması sonucunda ".../usr/lib/os-release" dosyası (Resim 5.1.). ve ".../etc/release" dosyası içerisinde kurulu işletim sisteminin adı ve versiyon bilgisinin yer aldığı görülmüştür.



Resim 5.1. Bilgisayarda kurulu işletim sistemi ve versiyon bilgisi

Resim 5.1.'de görüldüğü üzere".../usr/lib/os-release" dosyasının "X-Ways Forensic" yazılımı ile analizi sonucunda işletim sisteminin isminin "Ubuntu", versiyonunun "18.04.3 LTS (Bionic Beaver)" ve işletim sisteminin "debian" tabanlı olduğu görülmüştür.

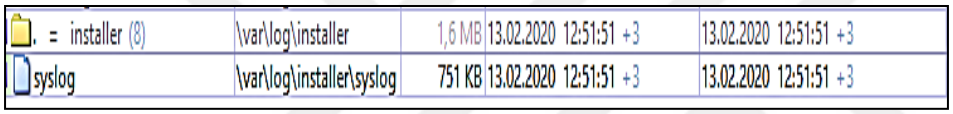
5.2. Bilgisayar Ad ve ID Bilgisi

Alınan adli kopya içerisinde "X-Ways Forensic" yazılımı kullanılarak hostname isminin anahtar kelime olarak aratılması sonucunda "…etc/hostname" dosyası içerisinde bilgisayar ad bilgisi yer aldığı görülmüştür. Dosyanın "X-Ways Forensic" adli bilişim yazılımı ile incelenmesi sonucunda bilgisayar adının "kubra" olduğu tespit edilmiştir. Kurulum esnasında "kkk" olarak tanımlanan bilgisayar adının inceleme aşamasında "kubra" olarak tespit edilmesinin sebebi bilgisayar ad değişikliğinin yapılmasıdır.

Alınan adli kopya içerisinde “X-Ways Forensic” yazılımı kullanılarak incelenmesi sonucunda “…etc/machine-id” dosyası içerisinde makine ID (identifier) numarası yer aldığı görülmüştür.

5.3. Kurulum Zaman Bilgisi

Alınan adli kopyanın “X-Ways Forensic” yazılımı kullanılarak incelemesi sonucunda “…var/log/installer” dizini altında “syslog” dosyasının (Resim 5.2.) bulunduğu görülmüştür. “syslog” dosyasının incelemesi sonucunda kurulum ile ilgili log kayıtlarının tutulduğu görülmüştür. Tutulan log kayıtların 13 Şubat 2020 tarihinde saat 09:19:22’de başladığı saat 09:51:51’de bittiği görülmüştür. Bu bilgilerin sistem kurulma saati hakkında bilgi sağlamak için kullanılabileceği tespit edilmiştir.



Resim 5.2. Bilgisayar zaman bilgisi

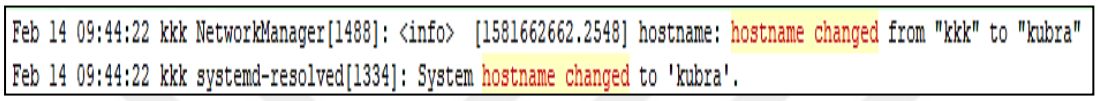
Resim 5.2.’de görüldüğü üzere“…var/log/installer” dosyasının oluşturulma ve değiştirme zaman bilgisinin UTC+3’e göre 13.02.2020 tarihinde saat 12:51 olduğu tespit edilmiştir. “…var/log/installer” klasörü ile syslog dosyalarının oluşturulma ve değiştirme tarihlerinin birbiriyle aynı olduğu, installer klasörünün işletim sistemi kurulumun bittiği anda oluştuğu ve herhangi bir işlemden sonra değişmediği görülmüştür. Bu sebeple söz konusu klasörün işletim sistemi kurulumun tamamlandığı saat hakkında bilgi sahibi olmak için kullanılabileceği tespit edilmiştir.

5.4. Kullandığı Zaman Diliminin Bilgisi

Alınan adli kopya içerisinde “X-Ways Forensic” yazılımı kullanılarak kurulum esnasında seçilen konum olan “İstanbul” kelimesinin anahtar kelime olarak aratılması sonucunda “…etc/localtime” dosyası içerisinde işletim sisteminin kullandığı zaman dilimi bilgisinin yer aldığı görülmüştür. Aynı zamanda “…etc/localtime” dosyasının incelenmesi sonucunda kullanılan zaman diliminin “Europe/İstanbul” olduğu görülmüştür.

5.5. Ad Bilgisinin Değiştirilme Bilgisi

Alınan adli kopya içerisinde "X-Ways Forensic" yazılımı kullanılarak "hostname changed" anahtar kelimesinin aratılması sonucunda "…var/log" dizini altında bulunan syslog dosyası (Resim 5.3.)içerisinde bilgisayar adının değiştirilme bilgisinin bulunduğu görülmüştür. Syslog dosyası, yerel olarak depolanabilen veya uzak bir sisteme gönderilebilen sistem günlüklerini tutan log dosyasıdır [56]. Alınan adli kopya içerisinde syslog, syslog.1, syslog.2, syslog.3, syslog.4, syslog.5, syslog.6 ve syslog.7 olmak üzere sekiz adet syslog dosyası bulunduğu tespit edilmiştir.

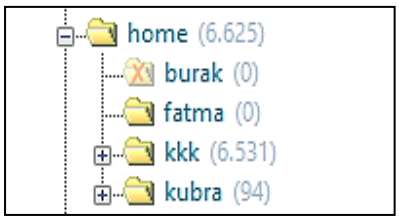


Resim 5.3. Değiştirilen bilgisayar ad bilgisi

Resim 5.3.'te görüldüğü üzere syslog dosyası içerisinde tutulan log kayıdının "14 Şubat 09:44:22'de" "kkk" olan bilgisayar isim bilgisinin "kubra" olarak değiştirildiği görülmüştür.

5.6.Oluşturulan ve Silinen Kullanıcı Bilgileri

Alınan adli kopyanın "X-Ways Forensic" yazılımı kullanılarak incelemesi sonucunda "…/home" dizini altında kullanıcılara ait klasörlerin oluştuğu görülmüştür (Resim 5.4.).



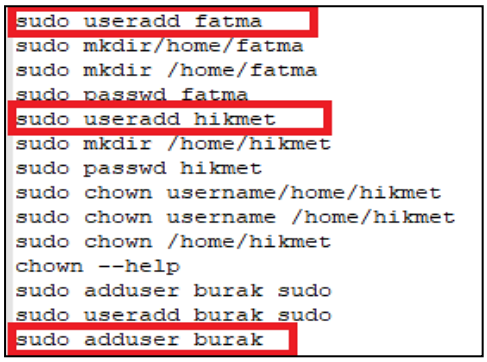
Resim 5.4. Kullanıcı bilgileri

Resim 5.4.'te görüldüğü üzere mevcut kullanıcıların "fatma", "kkk" ve "kubra" isimli kullanıcılar olduğu, silinmiş kullanıcının "burak" isimli kullanıcı olduğu görülmüştür. Herhangi bir işlem yapmadan silinen "hikmet" isimli kullanıcıya ait herhangi bir klasörün bulunmadığı görülmüştür. "fatma" isimli kullanıcının oturum açmaması sebebiyle klasörü altında herhangi bir dosyanın oluşmadığı, "burak" isimli kullanıcının silinmesi sebebiyle klasörünün içerisinde herhangi bir dosyanın bulunmadığı görülmüştür.

Alınan adli kopya içerisinde “X-Ways Forensic” yazılımı kullanılarak kullanıcı isimlerinin anahtar kelime olarak aratılması sonucunda “…etc/passwd” dosyası, “bash_history” dosyaları ve “auth.log” dosyaları içerisinde kullanıcılar hakkında bilgiler tutulduğu görülmüştür.

“…etc/passwd” dosyası incelendiğinde içerisinde mevcut kullanıcılara ait bilgilerin tutulduğu ancak silinen kullanıcılara ait herhangi bir bilgiyi bulundurmadığı görülmüştür.

Alınan adli kopya içerisinde “…/home/kkk” dizini ile “.../root” dizini altında olmak üzere iki adet bash_history dosyalarının bulunduğu görülmüştür. “bash_history” dosyaları incelendiğinde içerisinde terminal ekranı kullanarak eklenen ve silinen kullanıcılar ile ilgili komutların tuttuğu görülmüştür. “bash_history” dosyası, kabuktan çıkıldığı anda konsol üzerinden çalıştırılan her komutu tutan dosyadır. Daha sonra kabuğa girildiğinde bu dosya geçmiş listesini başlatır. HISTSIZE değişkenin değeri dosyaya kaydedilecek geçmiş satırlarının sayısını belirtir [57]. HISTSIZE değeri aşıldığında söz konusu verilere erişim sağlanamayabilir. İncelemesi yapılan adli kopya içerisinde “…/root” dizini ve “…/home/kkk” dizini altında bulunan “bash_history” dosyalarının HISTSIZE boyutunun 1000 komut satırı olduğu görülmüştür.



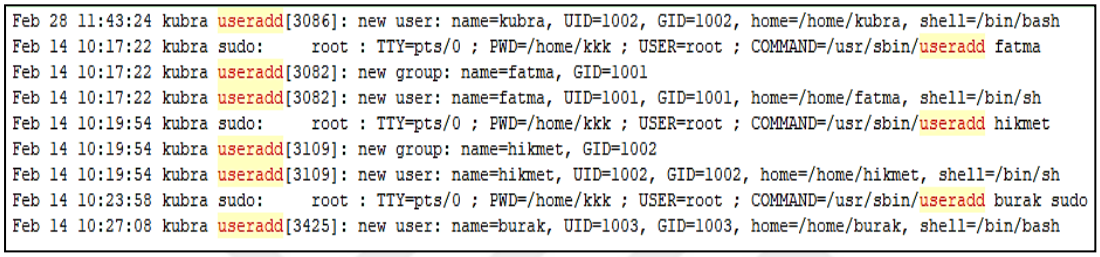
Resim 5.5. Oluşturulan kullanıcı bilgileri(a)

Resim 5.5.’te görüldüğü üzere “fatma”, “hikmet” ve “burak” isimli kullanıcıların oluşturulmasında kullanılan komutların tutulduğu görülmüştür. Ara yüz kullanarak eklenen “kubra” isimli kullanıcı ile ilgili bir bilgi görülmemiştir.

“bash_history” dosyalarının içerisinde komut satırı kullanarak silinen “hikmet” isimli kullanıcıya ait bilgi bulunduğu ancak ara yüz kullanarak silinen “Burak” isimli kullanıcıya ait herhangi bir bilgi bulunmadığı görülmüştür.

Alınan adli kopya içerisinde “auth.log”, “auth.log.1”, “auth.log.2” ve “auth.log.3” olmak üzere dört adet “auth.log” dosyasının bulunduğu görülmüştür. “auth.log” dosyaları, giriş günlükleri de dahil olmak üzere tüm kullanıcı kimlik doğrulama mesajları içeren “…var/log” dizini altında bulunan dosyalardır [58].

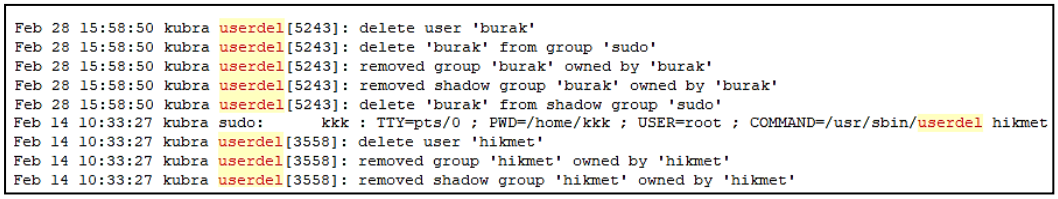
“auth.log” dosyalarının “Notepad++” yazılımı kullanarak “useradd” anahtar kelimesinin aratılması sonucunda eklenen tüm kullanıcılar hakkında bilgilerin tespit edildiği görülmüştür (Resim 5.6.).



Resim 5.6. Oluşturulan kullanıcı bilgileri(b)

Resim 5.6.’da görüldüğü üzere 14 Şubat tarihinde “fatma” isimli kullanıcının saat 10:17:22 de, “hikmet” isimli kullanıcının saat 10:19’da, “burak” isimli kullanıcının saat 10:23’te oluşturulduğu görülmüştür.

“auth.log” dosyalarının “Notepad++” yazılımı kullanarak “userdel” anahtar kelimesinin aratılması sonucunda silinen tüm kullanıcılar hakkında bilgilerin tespit edildiği görülmüştür (Resim 5.7.).



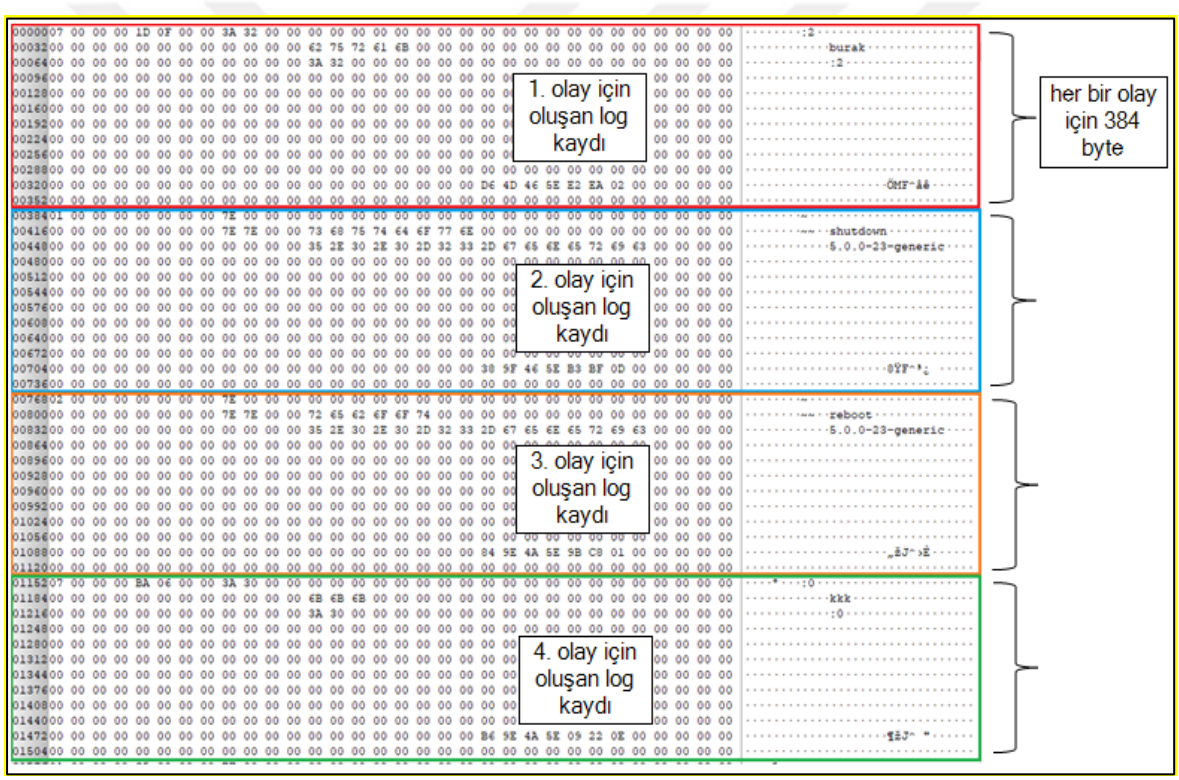
Resim 5.7. Silinen kullanıcı bilgileri

Resim 5.7.’de görüldüğü üzere 14 Şubat tarihinde “hikmet” isimli kullanıcının saat 10:33’te, 28 Şubat tarihinde de “burak” isimli kullanıcının saat 15:58’de silindiği görülmüştür.

5.7. Kullanıcıların Oturum Açma ve Kapatma Bilgileri

Kullanıcıların oturum açma-kapatma, sistem açma-kapatma kayıtlarını “wtmp” isimli dosya tarafından tutulmaktadır. Bu dosyanın boyutu sistem çalışırken büyümektedir. Adli bilişim uzmanları kullanıcı hareketlerini bu dosya sayesinde öğrenir [5]. “Wtmp” dosyaları bilgileri okunmayı zorlaştıran binary formatta tutulmaktadır [59].

Alınan adli kopyanın “X-Ways Forensic” yazılımı kullanılarak incelenmesi sonucunda “…var/log” dizini altında “wtmp” ve “wtmp.1” dosyaları olmak üzere iki adet “wtmp” dosyalarının bulunduğu görülmüştür. “wtmp” dosyasının yapısı Resim 5.8’de sunulmuştur.



Resim 5.8. wtmp dosya yapısı

Resim 5.8.’de görüldüğü üzere wtmp dosyasının ikili formatta olduğu, “X-Ways Forensic” ve “Encase” adli bilişim yazılımlarının söz konusu dosya yapısını çözümlemediği, manuel olarak incelendiğinde ise gerçekleştirilen her bir olayın (kullanıcı oturum açma-kapatma, sistem açma-kapatma) 384 byte olarak little endian biçiminde tutulduğu görülmüştür. Adli bilişim açısından önemli olabileceği değerlendirilen wtmp dosyasının adli bilişim yazılımları tarafından çözümlenmediği görüldüğünden dolayı inceleme süresini kısaltmak amacıyla bu dosyanın byte byte incelemesi yapılmıştır.

Wtmp dosyasının çözümlenmesi sonucunda tespit edilen veriler için Çizelge 5.1 oluşturulmuştur. Çizelge 5.1'i incelediğimiz zaman gerçekleşen her bir olaya ait etkinlik kodu bilgisi, PID id bilgisi, olayı gerçekleştiren kullanıcı bilgisi, host bilgisi ve zaman damgasının olduğu görülmektedir. Wtmp dosyasında her bir olay için ayrılan her bir 384 byte'lık kısımların analizi şu şekilde yapılmıştır: Öncelikle her bir 384 byte'lık bölümlerin ilk byte değeri 0 olarak kabul edildiğinde;

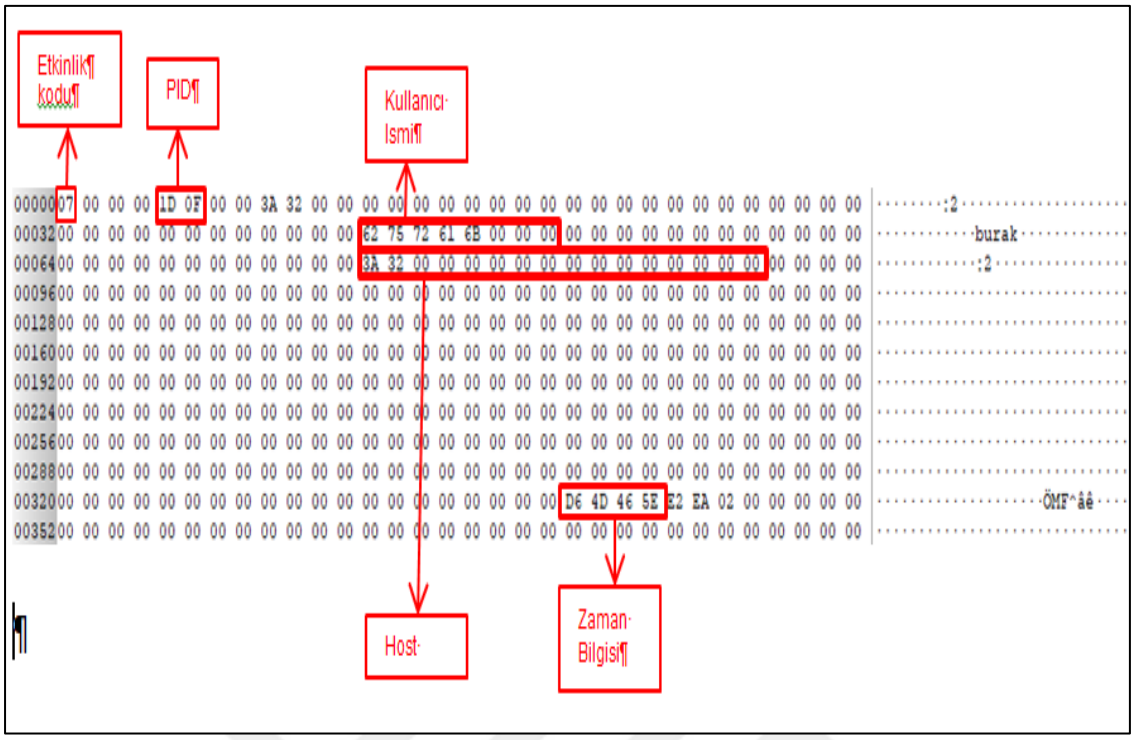
- 0.byte'da başlayan 1byte uzunluğundaki verinin etkinlik kodu bilgisini verdiği,
- 4.byte'da başlayan 2 byte uzunluğundaki verinin uzunluk PID bilgisini verdiği,
- 44.byte'da başlayan8 byte uzunluğundaki verinin kullanıcı bilgisini verdiği,
- 76.byte'da başlayan16 byte uzunluğundaki verinin host bilgisini verdiği,
- 340.byte'da başlayan 4 byte uzunluğundaki verinin zaman damgası bilgisini verdiği tespit edilmiştir.

Çizelge 5.1. Wtmp dosyasının çözümlenmesi sonucunda tespit edilen verilerin bilgileri

	Offset	**Length**
Etkinlik Kodu	0	1h
PID	4h	2h
Kullanıcı	44h	8h
Host	76h	16h
Zaman	340h	4h

Wtmp dosyası ut_type girdi tipindedir. Ut_type alanı log dosyasındaki kayıtların tipini belli eder ve integer değer tutar [60].wtmp dosyasının etkinlik kodu integer değer olarak tutmaktadır. Etkinlik kodunda tutulan 01 değeri RUN_LVL, 02 değeri BOOT_TIME, 07 değeri USER_PROCESS, 08 değeri DEAD_PROCESS olaylarını ifade etmektedir [60].

Yukarıda açıklanan analizler doğrultusunda Resim 5.8'de yer verilen wtmp dosyasındaki ilk384 bytelık olayın incelenmesi Resim 5.9'da gösterilmiştir.

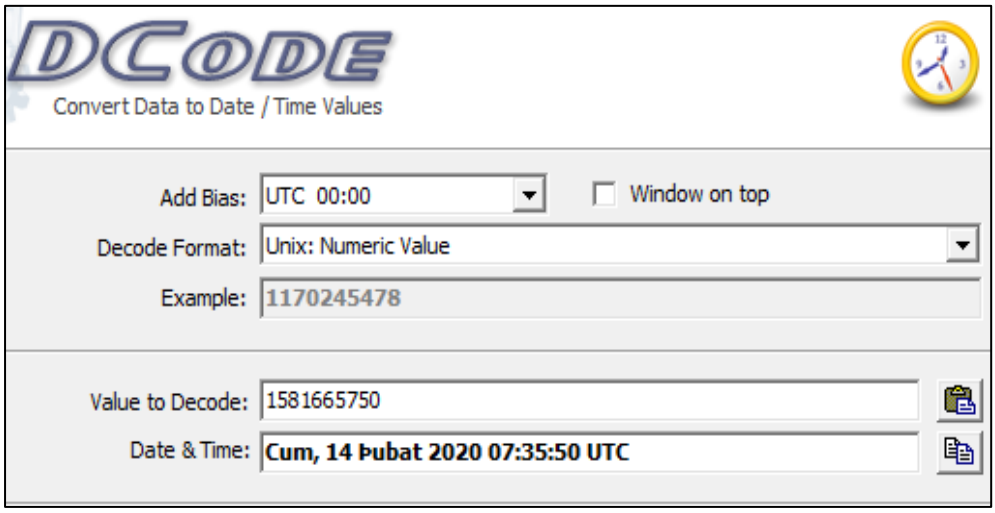


Resim 5.9. İncelenen örnek olayın yapısı

Resim 5.9.'da görüldüğü üzere incelemesi yapılan örnek olayın etkinlik kodunun tutulduğu 0. Byte değerinin "07" olduğu yani bir "USER_PROCESS" olduğu görülmektedir. PID numarasının tutulduğu 4-5.byte arasındaki 2 byte uzunluğunda yer alan hexadecimal değerinin "1D 0F" olduğu görülmektedir. Yukarıda bahsedildiği üzere wtmp dosyasında veriler little endian biçiminde tutulduğu için hexadecimal değerler tersten okunmalıdır. "1D 0F" olarak gözüken hexadecimal değer "0F 1D" olarak okunduğunda decimal değerinin 3869 olduğu yani bu olaya ait PID id değerinin 3869 olduğu anlaşılmaktadır. Olayı gerçekleştiren kullanıcı adının tutulduğu 44-51.bytelar arasındaki 8 byte uzunluğundaki değerin "burak" olduğu görülmektedir. Gerçekleşen olayın zaman bilgisinin tutulduğu 340-343.bytelar arasındaki 4 byte uzunluğundaki verinin "D6 4D 46 5E" olduğu görülmektedir. Aşağıda zaman damgası bilgisinin hesaplanması gösterilmiştir.

İncelenen olayın zaman bilgisinin hesaplanması

İncelemesi yapılan olayın zaman bilgisinin little endian şeklinde tutulmasından dolayı hexadecimal değeri "5E 46 4D D6" olarak yazılmış, decimal değeri hesaplanmıştır. Hesaplanan decimal değerinin "1581665750" olduğu görülmüş, değer "Dcode" yazılımı ile okunabilir tarih- saat formatına dönüştürülmüştür.



Resim 5.10. Tespit edilen zaman bilgisi

Resim 5.10.'da görüldüğü üzere hesaplanan decimal değerin "Cum, 14 Şubat 2020 07:35:50 UTC" olduğu görülmüştür.

"auth.log" dosyalarının "Notepad++" yazılımı kullanarak "authentication failure" anahtar kelimesinin aratılması sonucunda kullanıcıların başarısız oturum açma bilgilerin tespit edildiği görülmüştür (Resim 5.11.).

```
Feb 14 10:16:23 kubra gdm-password]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost=  user=kkk
Feb 14 10:35:42 kubra gdm-password]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty2 ruser= rhost=  user=burak
Feb 14 10:36:34 kubra gdm-password]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty2 ruser= rhost=  user=fatma
Feb 14 13:36:04 kubra gdm-password]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost=  user=kkk
```

Resim 5.11. Başarısız oturum açma bilgisi

Resim 5.11.'de görüldüğü üzere 14 Şubat tarihinde "kkk" isimli kullanıcının saat 10:16:23 ve 13:36:04 olmak üzere iki defa, "burak" isimli kullanıcının saat 10:35:42 olmak üzere bir defa, "fatma" isimli kullanıcının saat 10:36:34 olmak üzere bir defa yanlış şifre girdiği görülmüştür.

5.8. Bilgisayarın Başlatma ve Kapatma Bilgileri

Linux işletim sisteminde sistem açma-kapatma kayıtlarını "wtmp" dosyalarının tutması ve söz konusu dosyaların ikili tabanda tutulduğundan yapısının çözümlenmesinin zor olması sebebiyle bilgisayarın başlatma ve kapatma bilgilerinin tespiti için alternatif yol bulunmaya

çalışılmıştır. Bu sebeple sistem günlüklerini tutan “syslog” dosyaları içerisinde inceleme yapılmıştır. “syslog” dosyalarının incelemesi sonucunda bilgisayarı başlatma ve kapatma sırasında kaydedilen log kayıtlarının farklılık gösterdiği görülmüş ancak “kernel: [0.000000] ibaresi ile başlayan log kayıtları zaman bilgisinin, bilgisayarın başlatılma zaman bilgisi ile uyuştuğu görülmüştür. Söz konusu zaman bilgisinin bilgisayarı başlatma zaman bilgisinin elde edilmesinde kullanılabileceği değerlendirilmiştir.

“syslog” dosyalarının “Notepad++” yazılımı kullanarak “kernel: [0.000000]” anahtar kelimesinin aratılması sonucunda bilgisayarı başlatma zaman bilgilerinin tespit edildiği görülmüştür (Resim 5.12.).

```
Feb 13 17:00:14 kkk kernel: [    0.000000] Linux version 5.0.0-23-generic
Feb 13 17:03:46 kkk kernel: [    0.000000] Linux version 5.0.0-23-generic
Feb 14 08:20:58 kkk kernel: [    0.000000] Linux version 5.0.0-23-generic
```

Resim 5.12. Bilgisayar başlatma bilgisi

Resim 5.12.’de görüldüğü üzere 13 Şubat tarihinde saat 17:00 ve 17:03 ile 14 Şubat saat 08:20’de bilgisayarın “kkk” isimli kullanıcı tarafından başlatıldığı bilgisi görülmüştür.

Alınan adli kopya içerisinde “X-Ways Forensic” yazılımı kullanılarak “kernel: [0.000000]”ibaresinin anahtar kelime olarak aratılması sonucunda syslog dosyaları içerisinde tutulan bilgisayar başlatma zaman bilgilerinin “kern.log” dosyalarının içerisinde de tutulduğu görülmüştür. “Kern.log” dosyaları deamon hizmeti, klogd, çekirdek iletilerini ve olaylarını günlüğe kaydeden dosyalardır [61]. Adli kopya içerisinde “kern.log”, “kern.log.1”, “kern.log.2”, “kern.log.3” , “kern.log.4” olmak üzere beş adet “kern.log” dosyasının bulunduğu görülmüştür.

“syslog” dosyalarının “Notepad++” yazılımı kullanarak “System is powering down” anahtar kelimesinin aratılması sonucunda bilgisayarı kapatma zaman bilgilerinin tespit edildiği görülmüştür (Resim 5.13.).

```
Feb 13 17:01:25 kkk systemd-logind[1440]: System is powering down.
Feb 13 17:04:37 kkk systemd-logind[1437]: System is powering down.
Feb 14 16:23:02 kubra systemd-logind[1486]: System is powering down.
```

Resim 5.13. Bilgisayar kapatma zaman bilgisi

Resim 5.13.'te görüldüğü üzere 13 Şubat tarihinde saat 17:01 ve 17:04'te "kkk" isimli kullanıcı tarafından, 14 Şubat saat 16:23'te "kubra" isimli kullanıcı tarafından bilgisayarın kapatıldığı bilgisi görülmüştür. Bilgisayarın "kkk" isimli olarak açılıp "kubra" isimli olarak kapatılmasının sebebi bilgisayar ad bilgisinin değiştirilmesidir.

5.9. Tarih-Saat ve Saat Dilimi Değişikliği Bilgileri

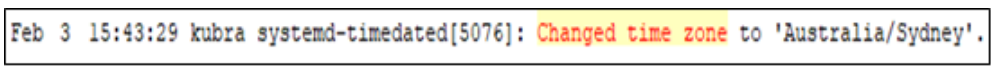
"syslog" dosyalarının "Notepad++" yazılımı kullanarak "Changed local time" anahtar kelimesinin aratılması sonucunda bilgisayar üzerinde yapılan tarih-saat değişikliği bilgisinin tespit edildiği görülmüştür (Resim 5.14.).

Resim 5.14. Değiştirilen tarih-zaman bilgisi

Resim 5.14.'te görüldüğü üzere "kubra" isimli kullanıcı tarafından local zamanın 3 Şubat 2010 saat 15:15 olarak değiştirildiği bilgisi görülmektedir.

Alınan adli kopyanın "X-Ways Forensic" yazılımı kullanılarak incelenmesi sonucunda "date –s" komutu ile yapılan tarih saat değişikliği bilgisinin herhangi bir log dosyasında tutulmadığı sadece "bash_history" dosyası içerisinde değiştirme işlemi için yazılan komut satırının bulunduğu görülmüştür.

"syslog" dosyalarının "Notepad++" yazılımı kullanarak "Changed time zone" anahtar kelimesinin aratılması sonucunda bilgisayar üzerinde yapılan zaman dilimi değişikliği bilgisinin tespit edildiği görülmüştür (Resim 5.15.).

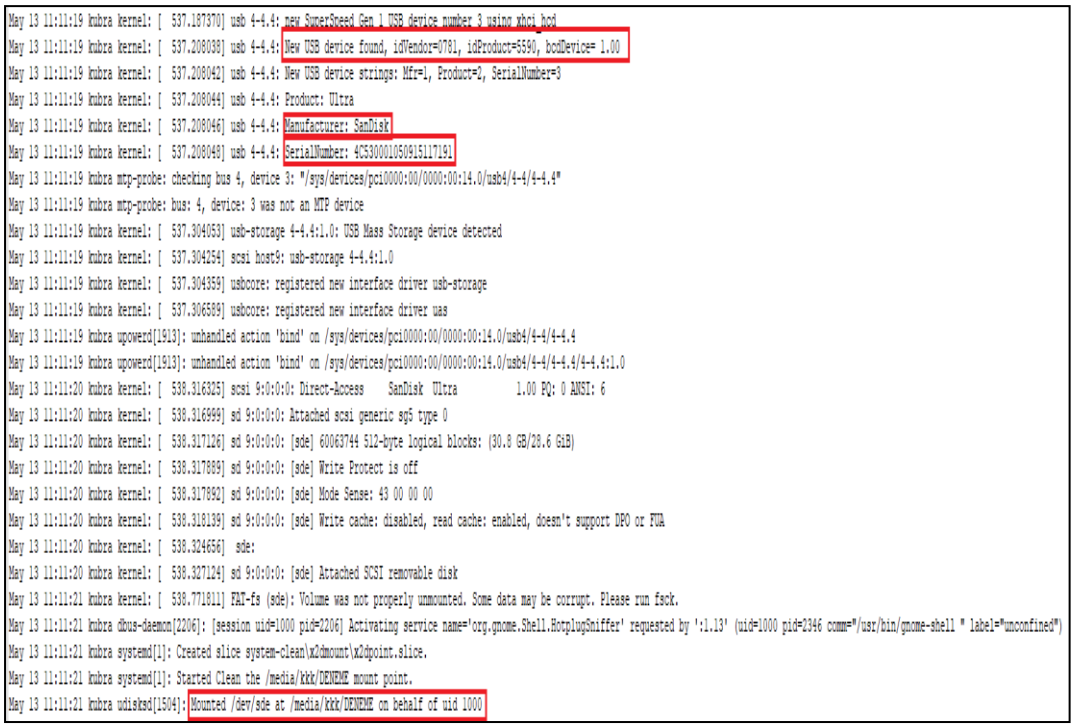


Resim 5.15. Değiştirilen saat dilimi bilgisi

Resim 5.15.'te görüldüğü üzere "kubra" isimli kullanıcı tarafından 3 Şubat saat 15:43'te saat dilimi ayarının "Australia" olarak değiştirildiği bilgisi görülmektedir.

5.10. Bilgisayara Takılan Harici Veri Depolama Cihazların Bilgileri

"syslog" dosyalarının "Notepad++" yazılımı kullanarak "New USB device found" anahtar kelimesinin aratılması sonucunda bilgisayara takılan harici veri depolama cihazları hakkında bilgilerinin tespit edildiği görülmüştür (Resim 5.16.). Söz konusu bilgilerin "kern.log" dosyaları içerisinde de bulunduğu görülmüştür. *(Örnek olarak Sandisk USB bellek verileri gösterilmiştir.)*



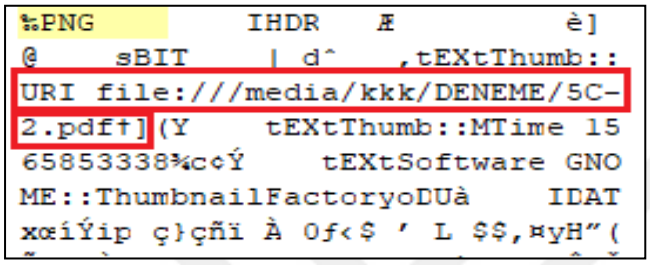
Resim 5.16. Sandisk USB belleğe ait bilgiler

Resim 5.16.'da bilgisayara takılan USB bellek markasının "Sandisk", seri numarasının "4C530001050915117191", takılma zamanının 13 Mayıs saat 11:11'de olduğu, kkk kullanıcısı tarafından takıldığı ve USB bellek isminin "DENEME" olduğu görülmektedir.

Alınan adli kopyanın "X-Ways Forensic" yazılımı kullanılarak incelenmesi sonucunda bilgisayara takılı bulunduğu zamanda USB bellek içerisinden açılan "pdf" dosyalarının ilk sayfaların ve fotoğrafların görüntülerinin "…/home/kkk/.cache/thumbnails/large" dizini içerisinde "png" dosyası olarak kaydedildiği görülmüştür. Örnek olarak "…/home/kkk/.cache/thumbnails/large" dizini altında bulunan bir "png" dosyasının incelemesi yapılmıştır. (Resim 5.17.).

Resim 5.17. Oluşan png dosyasının bilgileri

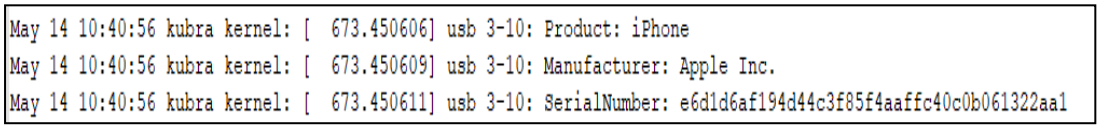
Resim 5.17.'de incelemesi yapılan "…/home/kkk/.cache/thumbnails/large" dizini içerisinde bulunan "png" dosyasının oluşturulma zaman bilgisinin "13.05.2020 14:11(UTC+3)" olduğu görülmektedir.



Resim 5.18. Oluşan png dosyasının yapısı

Resim 5.18.'de incelemesi yapılan "png" dosyasının "X-Ways Forensic" yazılımı ile incelemesi sonucunda dosya isminin "5C-2.pdf" olarak görüldüğü ve bulunduğu USB belleğin adının "DENEME" olduğu görülmüştür.

Alınan adli kopyanın "X-Ways Forensic" yazılımı kullanılarak log dosyalarının incelenmesi sonucunda cep telefonlarına ait universally unique identifier (uuid) numarasının tutulduğu görülmüştür (Resim 5.19.).



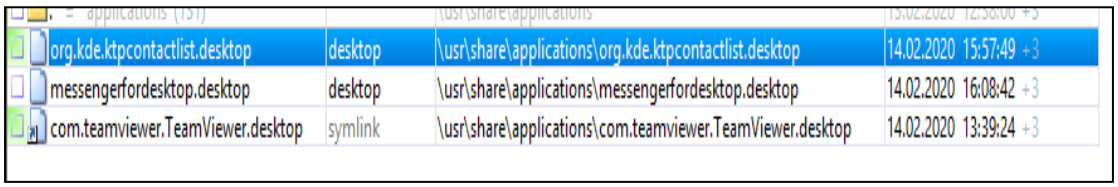
Resim 5.19. iPhone cep telefonuna ait bilgiler

Resim 5.19.'da incelemesi yapılan cep telefonun markasının iPhone, üretici firmanın Apple, seri numarasının "e6d1d6af194d44c3f85f4aaffc40c0b061322aa1" olduğu görülmüştür.

5.11. Bilgisayara Yüklenen Programların Bilgileri

Alınan adli kopyanın "X-Ways Forensic" yazılımı kullanılarak incelenmesi sonucunda yüklü uygulamaların "…/usr/share/applications" dizini altında ".desktop" uzantılı olarak

tutulduğu görülmüştür (Resim 5.20.). ".desktop" dosyası bir uygulamanın nasıl başlatılacağını ve ne tür uygulama olduğuna dair bilgileri içerir [62].



Resim 5.20. Yüklenen programlara ait bilgiler(a)

Resim 5.20.'de "Anlık Mesajlaşma" yazılımının ("org.kde.ktpcontactlist.desktop") yüklenme zaman bilgisinin 14 Şubat 2020 saat 15:57(UTC+3) olduğu, "Messenger" yazılımının ("messengerfordesktop.desktop") yüklenme zaman bilgisinin 14 Şubat 2020 saat 16:08 (UTC+3) olduğu, "Teamviewer" yazılımının ("com.teamviewer.TeamViewer.desktop") yüklenme zaman bilgisinin 14 Şubat 2020 saat 13:39(UTC+3) olduğu görülmüştür.

Alınan adli kopyanın "X-Ways Forensic" yazılımı kullanılarak program isimlerinin anahtar kelime olarak aratılması sonucunda dpkg.log dosyalarında, dosyalarının program yüklemeleri hakkında bilgiler tuttuğu görülmüştür (Resim 5.21.). "dpkg" log dosyaları program yükleme, kaldırma ve güncelleme gibi tüm işlemlerin tutulduğu log kayıtlarıdır [63]. Adli kopya içerisinde "dpkg.log", "dpkg.log.1" olmak üzere iki adet "dpkg.log" dosyasının bulunduğu görülmüştür.

```
2020-02-14 13:39:22 install teamviewer:amd64 <yok> 15.2.2756
2020-02-14 15:57:49 install kde-telepathy-contact-list:amd64 <yok> 4:17.12.3-0ubuntu1
2020-02-14 16:08:40 install messengerfordesktop:amd64 <yok> 2.0.9-171
```

Resim 5.21. Yüklenen programlara ait bilgiler(b)

Resim 5.21.'de "Anlık Mesajlaşma" yazılımının yüklenme zaman bilgisinin 14 Şubat 2020 saat 15:57 olduğu, "Messenger" yazılımının yüklenme zaman bilgisinin 14 Şubat 2020 saat 16:08 olduğu, "Teamviewer" yazılımının yüklenme zaman bilgisinin 14 Şubat 2020 saat 13:39 olduğu görülmüştür.

Alınan adli kopyanın "X-Ways Forensic" yazılımı kullanılarak incelenmesi sonucunda "…/var/lib/dpkg/info" dizini altında bilgisayara yüklenen tüm uygulamalar hakkında bilgiler olduğu görülmüştür. "…/opt" dizini içerisinde ise "Messenger" ve "Teamviewer"

programlarıyla ilgili bilgiler görülmüş, Ubuntu Software üzerinden kurulan "Anlık Mesajlaşma Kişileri" programıyla ilgili herhangi bir bilginin ise bulunmadığı görülmüştür. "…/opt" dizini uygulama yazılım paketlerini eklemek-yüklemek için ayrılmıştır [64].

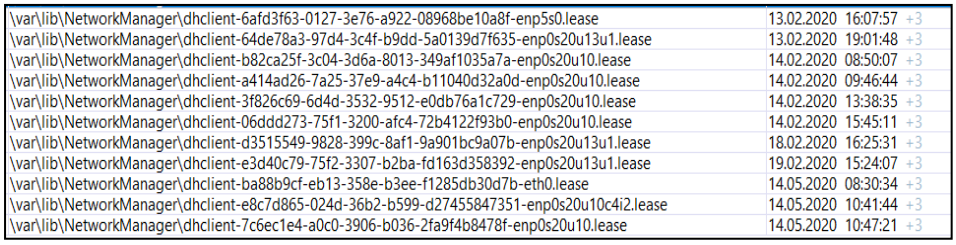
Kurulum paketi internet üzerinden indirip bilgisayara yüklenen Teamviewer uygulamasının kendine özgü log kaydı tuttuğu görülmüştür. Bu sebeple Teamviewer uygulamasının incelenmesi de yapılmıştır.

Teamviewer Uygulamasına Ait Bilgiler

Alınan adli kopyanın "X-Ways Forensic" yazılımı kullanılarak incelenmesi sonucunda "…var/log" dizini altında teamviewer uygulamasına ait "teamviewer15" isimli klasör ve "Connections_incoming.txt" isimli dosyaların oluştuğu görülmüştür. "teamviewer15" isimli klasör içerisinde "install_teamviewerd.log" isimli log dosyasının bulunduğu, log kayıtlarında uygulamanın kurulum saati bilgisinin bulunduğu görülmüştür. Connections_incoming.txt dosyası içerisinde istemci bilgisayardan gelen bağlantıların (ID numarası, Bilgisayar adı vb) bilgilerinin tutulduğu görülmüştür. Teamviewer uygulamasına ait log kayıtlarının "…/home/kkk/.local/share/teamviewer15/logfiles" dizini içerisinde bulunan "TeamViewer15_Logfile.log" dosyasında tutulduğu görülmüştür.

5.12. Ağ Yapılandırması, Ağ Üzerinden Erişim, Kablolu Erişim Noktalarına Yapılan Bağlantı İşlemlerinin Bilgileri

Alınan adli kopyanın "X-Ways Forensic" yazılımı kullanılarak incelenmesi sonucunda"…/var/lib/NetworkManager" dizini içerisinde yapılan her bağlantı için bir dosyanın tutulduğu görülmüştür (Resim 5.22.). dhclient, DHCP sunucusundan istek talebinde bulunur ve istemcinin ağ arabirimini yapılandırır. İstek bilgileri, "…/var/lib/NetworkManager" dizininde dhclient—interface.lease adlı bir dosya içerisinde tutulur [65].

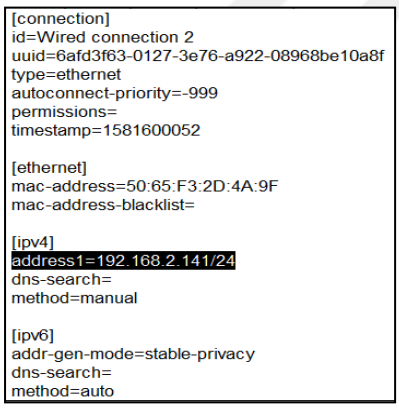


Resim 5.22. Kablolu erişim bağlantı noktaları

Resim 5.22.'de yapılan her bağlantı için dhclient ile başlayıp bağlantının Service Set Identifier (SSID) numarasıyla devam eden ".lease" uzantılı dosya ve bağlantının gerçekleştiği zaman bilgisi görülmektedir.

"…/var/lib/lockdown" dizini altında bilgisayar ile bağlantı kurulan iOS işletim sistemine sahip cep telefonlarının uuid numarası ile başlayan .plist dosyası oluşturduğu görülmüştür. Oluşan .plist dosyaları "plistEditor Pro V 2.5" yazılımıyla incelendiğinde cihazlara ait Wifi Media Access Control (MAC) adreslerinin bulunduğu görülmüştür. Ancak Android cihazlara ait MAC adresleriyle ilgili bir veri tespit edilememiştir. MAC adresi, üretici firma tarafından cihazın ethernet kartına harf ve sayı vererek oluşturulan fiziksel adrestir [66].

"…/etc/NetworkManager/system-connections" dizini altında bulunan "Wired connection 2" dosyası içerisinde, yerel ağ bağlantısı kurulan IP adresine ait bilgiler tespit edilmiştir (Resim 5.23.)."…/etc/NetworkManager/system-connections" dizini altında işletim sistemine bağlanmış ağların listesini tutmaktadır [67].

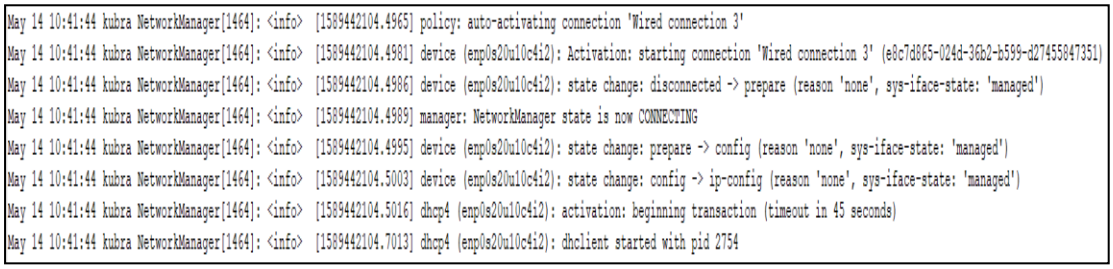


Resim 5.23. Yerel ağ bağlantısı kurulan IP adres bilgisi

Resim 5.23.'te bilgisayar ağ bağlantısının ID bilgisinin Wired connection 2 olduğu, bağlantı adres bilgisinin 192.168.2.141 olduğu, cihazın ethernet MAC adresinin 50.65:F3:2D:4A:9F olduğu, bağlantı zamanının "1581600052" olduğu görülmektedir. "1581600052" değerinin "Dcode" yazılımı ile zaman formatına dönüştürüldüğünde değerin "13 Şubat 2020 13:20:52 UTC" olduğu görülmüştür.

Alınan adli kopyanın "X-Ways Forensic" yazılımı kullanılarak incelenmesi sonucunda yerel ağ bağlantısı ve kablolu ağ bağlantılarına ait log kayıtlarının "syslog" ve "kern.log" dosyalarının içerisinde bulunduğu görülmüştür (Resim 5.24.). (Örnek olarak bağlanılan cep

telefonlarından sadece bir tanesinin “syslog” dosyası içerisinde bulunan bilgilerin görüntüsü alınmıştır.)

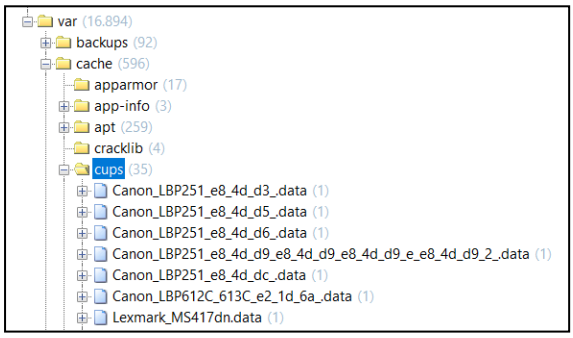


Resim 5.24. Ağ Bağlantı Bilgileri

Resim 5.24.’te “Wired coonection 3” bağlantısının 14 Mayıs tarihinde saat 10:41’de gerçekleştrildiği, SSID numarasının e8c7d865-024d-36b2-b599-d27455847351 olduğu, bağlantının “kubra” isimli kullanıcı tarafından yapıldığı görülmüştür.

5.13. Yazıcıdan Çıktı Alınması ile İlgili Bilgiler

Alınan adli kopyanın “X-Ways Forensic” yazılımı kullanılarak incelenmesi sonucunda“…/var/cache/cups”dizini içerisinde ağ içinde bulunan yazıcıların isimleriyle “.data” uzantılı dosyalar oluştuğu görülmektedir (Resim 5.25.). CUPS yazdırma dizinleri “…/var/cache/cups” adresinde saklanır [68].

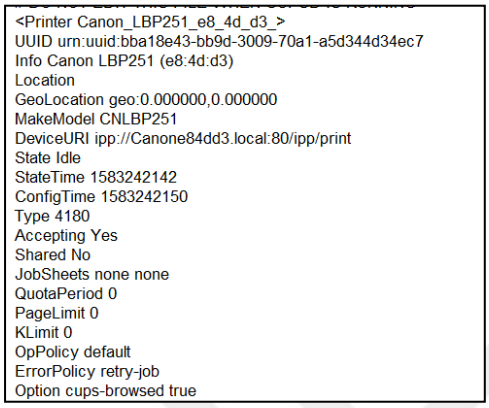


Resim 5.25. Bağlantı kurulan yazıcı bilgileri

Resim 5.25.’te “…/var/cache/cups” dizini içerisinde altı adet Canon marka ve bir adet Lexmark marka yazıcının bulunduğu görülmektedir.

Alınan adli kopyanın “X-Ways Forensic” yazılımı kullanılarak incelenmesi sonucunda “…/etc/cups” dizini, içerisinde bulunan “printers.conf” dosyasının içerisinde ağda bulunan

yazıcıların isimleri, uuid numaraları, yapılandırma zaman bilgileri bulunduğu görülmüştür (Resim 5.26.). *(Örnek olarak Canon marka yazıcılardan birinin verileri gösterilmiştir.)* "…/etc/cups" dizini, Linux sistemlerde yazdırma işlemi ile ilgili bilgilerin bulunduğu dizindir[69].

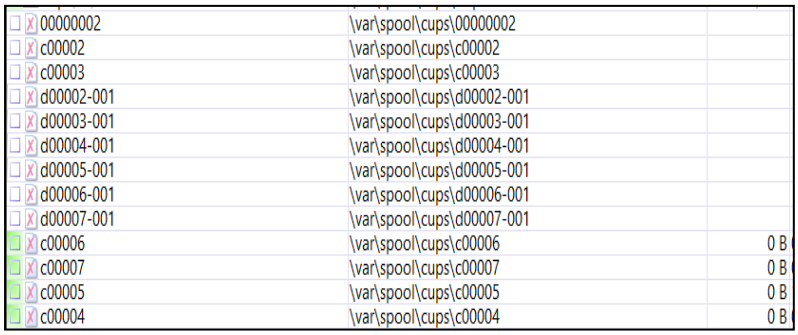


Resim 5.26. printers.conf dosya bilgileri

Resim 5.26.'da yazıcı isminin Canon_LBP251_e8_4d_d3 olduğu uuid numarasının "bba18e43-bb9d-3009-70a1-a5d344d34ec7" olduğu, yapılandırma zamanının "Sal, 03 Mart 2020 13:29:10 UTC" olduğu görülmüştür.

Unix sistemlerde bir dosya yazdırıldığında genel UNIX yazdırma sistemi (CUPS) tarafından iki dosya oluşturulmaktadır. Biri metadata içeren metadata verileri, diğeri ise PostScript formatını içeren veri dosyasıdır. Bu dosyalar "…var/spool/cups" dizini içerisindedir. "c" ile başlayan dosyalar kontrol dosyalarını, "d" ile başlayan dosyalar veri dosyalarını göstermektedir. Kontrol dosyaları periyodik olarak silinmekte ancak veri dosyaları belge yazdırıldıktan sonra hemen silinmektedir [60].

Alınan adli kopyanın "X-Ways Forensic" yazılımı kullanılarak incelenmesi sonucunda "…/var/spool/cups" dizini içerisinde yazdırma ile ilgili dosyaların bulunduğu görülmüştür. (Resim 5.27).



Resim 5.27. /var/spool/cups dizini içerisindeki veriler

Resim 5.27.'de görüldüğü üzere gerçekleştirilen yazma işlemi sonucunda oluşan altı adet kontrol ve altı adet veri dosyalarının bulunduğu görülmektedir. Dosyalar silinmiş olduğundan içerisinde herhangi bir verinin olmadığı görülmüştür.

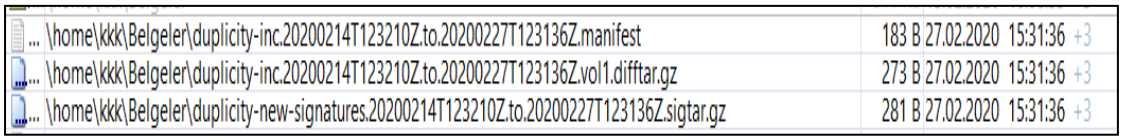
Yapılan incelemeler sonucunda yazdırılan belgelerin ismine ait her hangi bir log kaydı olmadığı ancak free space alanda yer aldığı görülmüştür. Free space alanda bu bilginin bulunmasının zor olacağı düşünüldüğü için incelemeleri kolaylaştırmak amacıyla tespit edilen bilgisayar ile bağlantı kurulan yazıcı bilgilerinden faydalanarak anahtar kelime oluşturulmuştur. Örneğin alınan adli kopya içerisinde "X-Ways Forensic" yazılımı kullanılarak"/printers/" anahtar kelimesi aratıldığında job-name etiketi yanında yazdırılan belge ile bilgiler bulunduğu görülmüştür(Resim 5.28.).

Resim 5.28. Free space alanda elde edilen veriler

Resim 5.28.'de "Free Space" alanda yazıcıya ait isim "Canon_LBP251_e8_4d_d5", yazdıran kullanıcı "kkk" ve yazılan belgenin "2018-2019-akademik takvim—1.pdf" olduğu görülmüştür.

5.14. Sistem Yedeğinin (Backup) Alınması ile İlgili Bilgiler

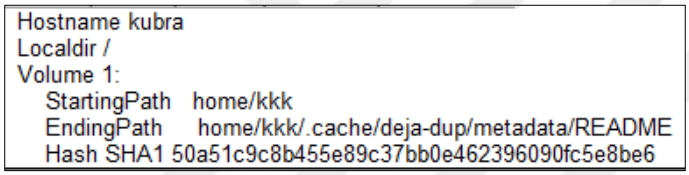
Alınan adli kopya içerisinde "X-Ways Forensic" yazılımı kullanılarak incelenmesi sonucunda "…/home/kkk/Belgeler" dizini ve "…/home/kkk/.cache/deja-dup" dizini içerisinde yedekleme dosyalarına ait ".manifest" ve ".sigtar.gz" uzantılı dosyaların oluştuğu görülmüştür (Resim 5.29.).



Resim 5.29. Backup dosyaları

Resim 5.29.'da "…/home/kkk/Belgeler" dizini içerisinde ".manifest", ".difftar" ve ".sigtar" uzantılı dosyaların 27 Şubat 2020 tarihinde saat 15.31'de oluştuğu görülmüştür.

".difftar" dosyaları içerisinde yedeklemeler bulunmaktadır. ".manifest" dosyası içerisinde yedeklenen dosyaların listelenmektedir. ".sigtar" dosyasında yedeklemeler arasında geçişler olup olmayacağını göstermek için dosyaların imzaları bulunmaktadır. Yedekleme parolalıysa uzantısı ".gpg" olmaktadır [5]. "manifest" uzantılı dosyanın "X-Ways Forensic" yazılımı kullanılarak içeriği görüntülenmiştir. (Resim 5.30.).



Resim 5.30. manifest dosya bilgileri

Resim 5.30.'da başlangıç yolunun home/kkk, bitiş yolunun home/kkk/.cache/deja-dup/metadata/README olduğu, yedekleme dosyasına ait SHA1 değerinin "50a51c9c8b455e89c37bb0e462396090fc5e8be6" olduğu, hostname ismi kubra olan sistemin yedeğinin alındığı görülmektedir.

Alınan adli kopya içerisinde "X-Ways Forensic" yazılımı kullanılarak log dosyalarının incelenmesi sonucunda yedekleme yapıldığına dair bir veri tespit edilememiştir. Deja-dup özelliğiyle yedekleme yapıldığında çok fazla verinin tutulmadığı görülmüştür.

6. TARTIŞMA

Hakim ve savcılar elektronik delillerin değerlendirilmesinde titiz davranarak konuya önem verseler de, delillere ilk müdahaleyi yaparak inceleyen adli bilişim uzmanlarına da bir o kadar zor ve önemli bir görev düşmektedir [70]. Bu çalışmanın, Linux işletim sistemine sahip bir bilgisayarın adli olarak incelemesi konusunda adli bilişim alanında görev yapan veya bu alanda eğitim alan kişilere kaynak olabileceği düşünülmektedir.

"var/log/installer dosyası" işletim sisteminin yüklenme sırasında ne olduğunu görmek için kullanılmaktadır [71]. Yüklenme sırasında oluşan olayların bu dosya içerisinde bulunan "syslog" dosyası içerisinde zaman bilgisiyle tutulduğu görülmüştür. Oluşan olayların zaman bilgisi işletim sisteminin kurulum zamanın bilgisini elde etmede kullanılabileceği görülmüştür. Ayrıca "X-Ways Forensics" yazılımıyla yapılan incelemede "var/log/installer dosyası" oluşturma ve değiştirme zaman bilgisinin bilgisayarda yapılan herhangi bir işlem sonunda değişmediğinden söz konusu dosyanın oluşturulma ve değiştirilme zaman bilgisine bakarak işletim sisteminin kurulma zamanı hakkında bilgi sahibi olunabilmektedir.

Konsol üzerinden çalıştırılan tüm komutları tutan "bash_history" dosyasının "HISTSIZE" değişkeni, komut geçmişi dizisinde kaydedilen maksimum komut sayısını sınırlar. Bu sınır aşıldığında en eski geçmiş komutlarının üzerine yazmaya başlar [72]. Bu çalışmada "X-Ways Forensics" yazılımıyla yapılan anahtar kelime araması sonucunda istenilen verilere ulaşıldığından HISTSIZE değeri aşılmadığı değerlendirilmiştir. Ancak HISTSIZE değeri aşıldığında bazı komutların silinebileceği göz önüne alınmalıdır.

Kullanıcıların oturum açma-kapatma, bilgisayarın başlatma-kapatma bilgilerini tutan "wtmp" dosyası, ikili tabanda tutulur ve metin editörü aracılığıyla içeriğine erişilemez [73]. Bu çalışmada ise "Encase" adli bilişim yazılımı ile "wtmp" dosyasının byte byte incelenmesi sonucunda, tutulan her bir etkinliğin "384 byte" uzunluğunda olduğu görülmüştür.

"Wtmp" dosyası sistem çalışırken büyümesinden dolayı söz konusu dosyasının byte byte çözümlenmesi zor bir hal almaktadır. Bu sebeple bilgisayarın başlatma-kapatma bilgilerinin tespiti için alternatif yol olarak "syslog" ve "kern.log" dosyaları kullanılmıştır. Bu durumun inceleme süresini azaltmakta büyük katkı sağlayacağı göz önünde bulundurulmalıdır.

Linux işletim sisteminin üçüncü parti bir yazılımın veya sistem üzerinde çalışan bir sürecin kendisine özgü log dosyası bulunabilir [74]. Bu çalışmada üçüncü parti uygulaması olarak yüklenen Teamviewer uygulamasının kendine özgü log dosyası tuttuğu görüldüğünden söz konusu uygulamanın tuttuğu log kayıtları incelerek uygulama hakkında bilgiler elde edilmiştir. Bu sebeple suçun üçüncü parti uygulama ile gerçekleştirilmesi durumunda kendine has log kaydetme mekanizmasının bulunabileceği unutulmamalıdır.

Mobil cihazlar ve bilgisayar arasında ağ bağlantısı kurulduğunda işletim sistemi üzerine kaydedilen kayıtlardan biri olan MAC adresi sayesinde, söz konusu mobil cihazın kim tarafından satın alındığı ve nerede satıldığına dair bilgilere ulaşılabilir. MAC adresleri yalnızca o cihaza özgüdür [75]. Bu sebeple bu çalışmada Linux işletim sistemine sahip bilgisayarla iOS ve Android işletim sistemine sahip cep telefonları arasında ağ bağlantısı gerçekleştirilmiştir. Gerçekleştirilen ağ bağlantısı sonrasında "X-Ways Forensics" yazılımıyla cep telefonlara ait MAC adreslerinin anahtar kelime olarak aratılması sonucunda İOS işletim sistemine sahip cep telefonlarının MAC adresleri tespit edilmiş ancak Android işletim sistemlerine sahip cep telefonlarının MAC adreslerinin tespitinin yapılamadığı görülmüştür. İncelemelerde bu durumun göz önünde bulundurulması gerekmektedir.

Linux işletim sisteminde yazdırılan belgelerin veri dosyalarını yazdırma işlemi tamamlandıktan sonra silinse de bu silinen veri dosyalarına ayrılmamış alanda kurtarma işlemi yapılarak erişilebilir. [60]. Bu çalışmada Linux işletim sisteminde yazdırılan belgelere ait "kontrol" ve "veri dosyalarının" yazdırma işlemi bittikten sonra silindiği, ancak "X-Ways Forensics " yazılımıyla yapılan anahtar kelime araması sonucunda bu bilgilerin "Free Space" alanda bulunduğu görülmüştür. Bu sebeple inceleme konusu olan, "yazıcıya gönderilen belge" hakkında toplanabilecek tüm bilgilerin inceleme aşamasında oldukça önemli olduğu unutulmamalıdır.

Linux işletim sistemi yedekleme sırasında yedekleme günlüğü de oluşturabilir [76]. Ancak bu çalışmada "X-Ways Forensics " yazılımıyla yapılan anahtar kelime araması sonucunda log dosyaları içerisinde yedekleme yapıldığına dair bir veri görülememiştir. Deja-dup özelliği kullanarak yedekleme yapıldığında log dosyaları içerisinde yedekleme yapılıp yapılmadığı bilgisine erişilemediğinden bu konu titizlikle araştırılmalıdır.

7. SONUÇ VE ÖNERİLER

Bu çalışma ile Linux işletim sistemine sahip olan bir bilgisayarın analiz edilmesi esnasında karşılaşılan problemler ve çözüm yolları tespit edilmiştir. Adli bilişim incelemeleri açısından önem arz eden log dosyalarının konumları ve içerisinde tuttuğu bilgiler ortaya çıkarılmıştır. Yapılan tespitler ışığında Linux işletim sistemine ait log dosyalarının analizi için kaynak olarak kullanılabilecek bilgiler EK-1'de belirtilmiştir.

Bu çalışmada; Linux işletim sistemi yüklü bilgisayarlar içerisinden adli bilişim açısından önem arz eden kayıtların tespiti amacıyla yöntem kısmında belirtilen deneyler yapılmıştır. Tespit edilen sonuçlar maddeler halinde aşağıda belirtilmektedir.

- ".../usr/lib/os-release" ve …/etc/release dosyaları içerisinde kurulu işletim sistemi adı ve versiyon bilgisi bulunduğu görülmüştür.
- "…etc/hostname dosyasının" içerisinde bilgisayar ad bilgisi yer aldığı görülmüştür.
- "…etc/machine-id" dosyası içerisinde ise makine ID numarasının yer aldığı görülmüştür.
- "installer" dosyasının ise kurulum tamamlandıktan sonra "...var/log" dizinin altında oluştuğu sistem oluşturma tarihi hakkında bilgi verdiği görülmüştür. "…var/log/installer" içerisinde bulunan "syslog" dosyası içerisinde yükleme ile ilgili log kayıtları görülmüştür.
- "syslog" dosyası içerisinde değiştirilen bilgisayar ad bilgisi tespit edilmiştir.
- "…etc/localtime" dosyası içerisinde işletim sisteminin kullandığı zaman dilimi bilgisinin yer aldığı görülmüştür.
- "…etc/passwd" dosyası içerisinde mevcut kullanıcılar hakkında bilgilerin tutulduğu görülmüştür.
- Oluşturulan ve silinen tüm kullanıcılar hakkında bilgilerin auth.log dosyaları içerisinde tutulduğu görülmüştür.
- Kullanıcıların oturum açma ve kapatma, bilgisayarı başlatma ve kapatma bilgilerinin "wtmp" dosyaları içerisinde bulunduğu ancak wtmp dosyasının ikili tabanda olduğu görülmüştür.
- Başarısız oturum açmanın auth.log dosyaları içerisinde tutulduğu görülmüştür.

- Bilgisayarı başlatma ve kapatma zaman bilgisinin syslog ve kern dosyaları içerisinde bulunduğu görülmüştür.
- İşletim sistemi üzerinde yapılan tarih-saat değişikliği, saat dilimi ayar değişikliği bilgisinin syslog dosyaları içerisinde bulunduğu görülmüştür.
- Bilgisayara takılan harici veri depolama cihazları hakkında bilginin syslog ve kern.log dosyaları içerisinde bulunduğu görülmüştür.
- Programların yüklenme zaman bilgilerinin dpkg.log dosyaları içerisinde bulunduğu görülmüştür. Bilgisayara yüklenen Teamviewer uygulamasına ait log kayıtları kendisi tarafından oluşturulan "TeamViewer15_Logfile.log" dosyası içerisinde tutulduğu görülmüştür.
- Yerel ağ bağlantısı ve kablolu ağ bağlantısı log kayıtlarının disk içerisinde bulunan syslog dosyaları ve kern.log dosyaları içerisinde bulunduğu görülmüştür.
- Yazıcı ile ilgili kayıtların "free space" alanda bulunduğu görülmüştür.
- Deja-dup özelliğiyle yedekleme yapıldığında yedekleme yapıldığına dair herhangi bir bilginin log dosyalarında tutulmadığı görülmüştür.

Gelecek Çalışmalara Öneriler

Teknolojinin gelişmesiyle işletim sistemleri sürekli olarak güncellenmekte ve gelişmektedir. İşletim sistemleri üzerinde gerçekleştirilen güncelleme ve gelişme işlemlerini takip etmek adli bilişim açısından oldukça önemlidir. Adli bilişim dalında Türkçe kaynak bulmak oldukça zor olmasından dolayı adli bilişim açısından önemli olabileceği değerlendirilen konular belirtilmiştir.

Bu çalışmada Linux işletim sisteminin Ubuntu sürümü üzerinde çalışılmış olup işletim sistemindeki mevcut log kayıtları üzerinde incelenme yapıldığından Linux işletim sisteminde silinen log kayıtlarının kurtarılması ve kurtarılan log kayıtları ile ilgili çalışmalar yapılabilir. İşletim sistemlerinin versiyonları arasında büyük farklılıklar olabileceğinden Linux işletim sisteminin diğer sürümlerinin incelemesi yapılabilir.

Çalışma kapsamında standart bilgisayar kullanıcısının yapmış olduğu işlemlerle ilgili log kayıtları incelenmiş olduğundan uzaktan yapılacak herhangi bir işlemde veya saldırıda tutulacak log kayıtlarının incelemesi ilgili çalışma yapılabileceği değerlendirilmiştir. Windows, MacOS, Linux işletim sistemlerinde adli bilişim açısından önemli olabileceği

değerlendirilen log kayıtların nerelerde kaydedildiğinin karşılaştırılması da yapılabilir. Ek olarak Linux işletim sisteminin dosya sistemini tam olarak destekleyen adli bilişim yazılımı ile ilgili çalışmalar yapılabileceği değerlendirilmiştir.

KAYNAKLAR

1. Jayathilake, D. (2012,May). *Towards Structured Log Analysis.* Paper presented at the First 9th International Joint Conference on Computer Science and Software Engineering, Thailand.

2. Can, S. (2017). *Bakanlıkta Kullanılan Log Sistemlerinin Merkezileşmesi ve Yönetimi,* Uzmanlık Tezi, Çevre ve Şehircilik Bakanlığı, Ankara, 11.

3. Karaman, C. (2019). *Log Kayıtları ve Analizi.* Türkiye:DRM,148.

4. Aslanbakan, E. (2019). *Bilgi güvenliği ve uygulamalı hacking yöntemleri (Yeni başlayanlar için)*. İstanbul: Pusula, 144.

5. Ling, T. (2013, June). *The Study of Computer Forensics on Linux.* Paper presented at the First International Conference on Computational and Information Sciences, India.

6. Zeng, L., Xiao, Y., Chen, H., Sun, B. and Han, W. (2016). Computer operating system logging and security issues: a survey. *Security and Communication Networks*, *9*(17), 4804-4821.

7. dos Santos Almeida, J., de Santana Nascimento, L. and José, D. A. M. (2019). Computer Forensics: A Linux Case Study Applied to Pedophilia Crime Investigation in Brazil. *International Journal of Cyber-Security and Digital Forensics*,*8*(1), 31-43

8. Kılıç, M. S. (2012). *İşletim Sistemlerinin Adli Bilişim Açısından İncelenmesi,* Yüksek Lisans Tezi, Polis Akademisi Başkanlığı, Ankara, 86.

9. Modig, D. and Ding, J. (2018). Ubuntu, Debian, Fedora, Redhat and OpenSUSE, A comparison in CVE on Linux distributions.

10. Alakoç, Z. (1998). *İşletim Sistemleri, Açık Sistemler(OSI) ve Bir Uygulama(Linux),* Yüksek Lisans Tezi, Cumhuriyet Üniversitesi Sosyal Bilimler Enstitüsü, Sivas, 18.

11. Irum, I., Raza, M. and Sharif, M. (2012). File Systems for Various Operating Systems: A Review. *Research Journal of Applied Sciences, Engineering and Technology*, 2934-2947.

12. Arıcı, N. ve Çiftçi, S. (2007). Bilgisayar Destekli Uzaktan Eğitimde Öğrenci Log Kayıtlarının İncelenerek Analiz Edilmesi. *e-Journal of New World Sciences Academy*, 323.

13. Merlino, J. (2006). *Why Use Linux.* Indiana: Wiley Publising Inc.

14. Güvensan, M. A. (2006). *Linux İşletim Sistemi Çekirdeği ile Bütünleşik Bir Kriptografik Sistemin Tasarımı ve Gerçeklenmesi,* Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, İstanbul, 11.

15. Al-Rayes, H. T. (2019). Studying Main Differences Between Android & Linux Operating System. *International Journal of Electrical & Computer Sciences*, 1.

16. Matotek, D., Turnbull, J. and Lieverdink, P. (2017). *Pro Linux System Administration.* New York: Apress, 664.

17. Arshad, A., Iqbal , W. and Abbas H. (2018). USB Storage Device Forensics for Windows 10. *Journal of Forensic Sciences, 63.*

18. Talebi, J., Dehghantanha, A. and Mahmod, R. (2014). Introducing and Analysis of the Windows 8 Event Log for Forensic Purposes. *In Computational Forensics,* 145-162.

19. Schuster, A. (2007). Introducing the Microsoft Vista event log file format. *Digital Investigation, 4,* 65-72.

20. Monteiro, S.D. and Erbacher, R. (2008). An authentication and validation mechanism for analyzing syslogs forensically. *Operating Systems Review, 42*, 41-50.

21. Ibrahim, N.M., Al-Nemrat, A., Jahankhani, H. and Bashroush, R. (2011). Sufficiency of Windows Event Log as Evidence in Digital Forensics. *ICGS3/e-Democracy.*

22. Saleh, M., Arasteh, A., Sakha, A. and Debbabi, M. (2007). Forensic analysis of logs: Modeling and verification. *Knowl. Based Syst., 20,* 671-682.

23. Murphey, R. (2016). Automated Windows Event Log Forensics By Rich Murphey.

24. Horsman, G., Caithness, A. and Katsavounidis, C. (2019). A Forensic Exploration of the Microsoft Windows 10 Timeline. *Journal of Forensic Sciences, 64.*

25. Do, Q., Martini, B., Looi, J., Wang, Y. and Choo, K.R. (2014, January). *Windows Event Forensic Process.* Paper presented at the First IFIP International Conference on Digital Forensics, Berlin.

26. Neyaz, A. and Shashidhar, N. (2019). USB Artifact Analysis Using Windows Event Viewer, Registry and File System Logs. *Electronics, 8,* 1322.

27. Moskvichev, A.D. and Dolgachev, M.V. (2020, October). *System of Collection and Analysis Event Log from Sources under Control of Windows Operating System.* Paper presented at the First *International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon),* Russia.

28. Al-Saleh, M.I. and Al-Shamaileh, M.J. (2017). Forensic artefacts associated with intentionally deleted user accounts. *International Journal of Electronic Security and Digital Forensics, 9*(2), 167-179.

29. Shin, Y., Cheon, J.and Kim, J. (2016). Study on Recovery Techniques for the Deleted or Damaged Event Log(EVTX) Files. *Journal of the Korea Institute of Information Security and Cryptology, 26*(2), 387-396.

30. Shi-bo, Y. (2013). Host Intrusion Detection Based on Windows Log. *Journal of Jilin Teachers Institute of Engineering and Technology, 29*(1), 71-72.

31. Ning, X. W. and Liu P. Y. (2009). Log system design in support of linkage analysis of security audit and computer forensics. *Computer Engineering and Design, 30*(24), 5580-5583.

32. Söderström, O., and Moradian, E. (2013). Secure audit log management. *Procedia Computer Science*, *22*, 1249-1258.

33. Połczyński, P. A. (2015). *Analysis of event logs in computers (Windows systems)*, Doctoral dissertation, Warsaw University Instytut Informatyki, Poland.

34. Sahoo, P. K., Chottray, R. K. and Pattnaiak, S. (2012). Research issues on windows event log. *International Journal of Computer Applications*, *41*(19).

35. Henkoğlu, T. (2020). *Adli bilişim: Dijital delillerin elde edilmesi ve analizi*. İstanbul: Pusula, 99-100.

36. Chen, L., Xu, A., Kuang, X., Lv, H., Yang, H., Yang, Y., and Li, B. (2020,May). *Detecting Advanced Attacks Based On Linux Logs.* Paper presented at the First *IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), USA.*

37. Anuradha, P., Kumar, T.R., and Sobhana, N. (2016, March). *Recovering deleted browsing artifacts from web browser log files in Linux environment.* Paper presented at the First *Symposium on Colossal Data Analysis and Networking (CDAN),* India.

38. Studiawan, H., Sohel, F. and Payne, C. (2018). *Automatic log parser to support forensic analysis.* Paper presented at the First *16th Australian Digital Forensics Conference,* Australia.

39. Urrea, J. M. (2006). *An analysis of Linux RAM forensics.* NAVAL POSTGRADUATE SCHOOL MONTEREY CA.

40. Andrade, J. J. B. and Gan, D. (2012). *A forensics investigation into attacks on Linux servers*, Master, University of Strathclyde Continuing Centre Computing and Mathematical Sciences, Glasgow.

41. Turedi, Z. and Han, L. (2013). Automatic forensic log file analysis for Mac OS X systems. *International Journal of Electronic Security and Digital Forensics 2*, *5*(2), 124-138.

42. Kopytko, T. K. (2019). *Log analysis in operating system macOS,* Doctoral dissertation, Warsaw University Instytut Informatyki, Poland.

43. Nedelkoski, S., Bogatinovski, J., Acker, A., Cardoso, J. and Kao, O. (2020). Self-Supervised Log Parsing.

44. Martin, D.M. (2016). OS X as a Forensic Platform. 2.

45. Rathod, D. (2017). Mac osx forensics. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 6*(8),1240.

46. Hayes, D. R. (2015). *A Practical Guide to Computer Forensics Investigations.* Indiana:Pearson Education, 53.

47. Malin, C.,H., Casey, E., and Aquilina, J.,M. (2008). Malware Forensics: Investigating and Analyzing Malicious Code. Burlington:Syngress, 224.

48. Wiles, J. and Reyes, A. , (2011). *The Best Damn Cybercrime and Digital Forensics Book Period.* Burlington:Syngress, 541.

49. Boyd, C. and Forster, P. (2004). Time and date issues in forensic computing - a case study. *Digital Investigation,* 1, 18-23.

50. Shaver, J.S. (2015). Exposing Vital Forensic Artifacts of USB Devices in the Windows 10 Registry. Naval Postgraduate School Monterey CA, 1.

51. Hassan, N. A. (2019). *Digital Forensics Basics: A Practical Guide Using Windows OS.* New York: Apress, 201.

52. Gedik, D. (2009). Bilişim Suçlarında IP Tespiti ile Ekran Görüntüleri Çıktılarının İspat Değeri. *Bilişim Hukuku Dergisi*, 1(1),51-84.

53. Goel, S., Gladyshev, P., Johnson, D., Pourzandi, M. and Majumdar S. (2020, October). *Digital Forensics and Cyber Crime.* Paper presented at the First 11th EAI International Conference ICDF2C, Boston.

54. Lange, M.C.S. and Nimsger, K.M. (2004). *Electronic Evidence and Discovery: What Every Lawyer Should Know.* Chicago:American Bar Association, 80.

55. Peterson, R. (2008). *Ubuntu: The Complete Reference.* India:McGraw Hill Professional, 126.

56. Casey, E. (2010). *Digital Forensic and Investigation.* London:Elsevier Akademic Press, 337-338.

57. Sobell, M. G. (2007). *A Practical Guide to Ubuntu Linux.* USA:Prentice Hall PTR, 330-331.

58. Lin, X. (2018). *Introductory Computer Forensics*. Germany: Springer, 308-310.

59. Tomono, A., Uehara, M., Murakam, M. and Yamagiwa, M. (2009, August). *A Log Management System for Internal Control.* Paper presented at the First International Conference on Network-Based Information Systems,USA.

60. Kerrisk, M. (2010). *The Linux Programming Interface: A Linux and Unix System Programming Handbook.* USA:NO Starch Press, 818-827.

61. Jang, M. (2004). *RHCE Red Hat Certified Engineer: Linux Study Guide (exam RH302).* USA:McGraw-Hill Osborne Media, 593.

62. Jasim, M. (2017). *Building Cross-Platform Desktop Applications with Electron.* India:Packt Publishing, 215.

63. Petersen, R. (2018). *Ubuntu 18.04 LTS Desktop: Applications And Administration.* USA:Surfing Turtle Press.

64. Sheer, P. (2002). *Linux: Rute User's Tutorial and Exposition.* (Vol. 31). USA:Prentice Hall,360.

65. Sobell, M. G. (2013). *A Practical Guide to Fedora and Red Hat Enterprise Linux.* UK:Pearson Education, 492.

66. Garg, U., Verma, P., Moudgil, Y. S. and Sharma, S. (2012). MAC and Logical addressing(A Rewiew Study). *International Journal of Engineering Research and Applications*, 474-480.

67. Patil, D.N. and Meshram, B. (2016). Digital Forensic Analysis of Ubuntu File System. *International Journal of Cyber-Security and Digital Forensics*, 4(5), 175-186.

68. Petersen, R. (2020). Linux Mint 20: *Desktops and Administration.* USA:Surfing Turtle Press.

69. Smith, R. W. (2012). *Linux Essentials*. ABD:John Wiley&Sons Inc.

70. Çakır, H. ve Kılıç, M. S. (2013). Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış. *Turkish Journal of Police Studies/Polis Bilimleri Dergisi*, 15(3),23-44.

71. Shackleford, D. (2013). *Virtualization Security: Protecting Virtualized Environments.* USA:John Wiley&Sons Inc., 218.

72. Kruse II, W. G. and Heiser, J. G. (2001). *Computer forensics: Incident response Essentials.* USA:Pearson Education.

73. Cox, K. (2000). *Red Hat Linux administrator's guide*. UK:Premier Press, 320.

74. Parlak, D. ve Çiftçi, Y. (2015). *Centos*. İstanbul:Kodlab, 207.

75. Blackman, D. and Szewczyk, P. (2015, 30 November–2 December). *The Challenges of Seizing and Searching the Contents of Wi-Fi Devices for the Modern Investigator.* Paper presented at the First Australian Digital Forensics Conference, Australia.

76. Parker, T. (1999). *Linux system administrator's survival guide.* USA:Sams Publishing, 359.

EKLER

EK-1. Linux işletim sistemine sahip bir bilgisayarda deneyler neticesinde tespit edilen bulgular

TESPİTLER	BULUNDUĞU DOSYA YOLU	BULUNDUĞU DOSYA ADI	AÇIKLAMA
İşletim Sistemi Versiyon Bilgisinin Tespiti	.../usr/lib ../etc	os-release release	
Bilgisayar Adının Tespiti	…/etc	hostname	
İşletim Sisteminin Kurulma Zamanının Tespiti	…var/log …var/log/installer	İnstaller (Dosyanın oluşma zamanı) syslog	
İşletim Sisteminin Kullandığı Zaman Diliminin Bilgisi	…/etc	localtime	
Mevcut Kullanıcılar	…/etc	passwd	
Mevcut ve Silinen Kullanıcılar	…/var/log	auth.log dosyaları	Anahtar kelime olarak eklenen kullanıcılar için useradd, silinen kullanıcılar için userdel kullanılabilir.
Bilgisayarda Kullanıcıların Giriş-Çıkış İşlem Bilgileri	…/var/log	wtmp dosyaları	

EK-1. (devam) Linux işletim sistemine sahip bir bilgisayarda deneyler neticesinde tespit edilen bulgular

Linux İşletim Sistemine Sahip Bilgisayarın Ad Bilgisinin Değiştirilme Bilgisi	…/var/log	Syslog dosyaları	Anahtar kelime olarak hostname changed kullanılabilir.
Başarısız Oturum Açma Bilgisi	…/var/log	auth.log dosyaları	Anahtar kelime olarak "authentication failure" kullanılabilir.
Sistem Açma-Kapatma Zaman Tespit Bilgisi	…/var/log	syslog ve kern.log dosyaları	Anahtar kelime olarak sistem açma saatini bulmak için "kernel: [0.000000] Linux version", sistem kapatma saatini bulmak için "System is powering down" kullanılabilir.
Kullanıcı Tarafından Yapılan Tarih-Saat ve Saat Dilimi Değişikliği Tespiti	…/var/log	Syslog dosyaları	Anahtar kelime olarak saat-tarih değişikliğini bulmak için "Changed local time", saat dilimi değişikliğini bulmak için "Changed time zone" kullanılabilir.
Bilgisayara Takılan Harici Veri Depolama Cihazları Hakkında Tespit Edilen Bilgiler	…/var/log	syslog ve kern.log dosyaları	Anahtar kelime olarak "New USB device found" kullanılabilir.

EK-1. (devam) Linux işletim sistemine sahip bir bilgisayarda deneyler neticesinde tespit edilen bulgular

USB Bellek içinde erişim sağlanan pdf dosyalarının ve fotoğrafların küçük görüntüleri	home/kkk/.cache/thumbnails	large	
Bilgisayara Yüklenen Programların Bilgileri	…/var/log	dpkg.log dosyaları	
Ağ Yapılandırması, Ağ Üzerinden Erişim, Kablolu Erişim Noktalarına Yapılan Bağlantı İşlemlerinin Bilgileri	…/var/lib/NetworkManager …/var/log	.lease dosyaları syslog dosyaları	
Yazıcı Bilgileri	…/etc/cups	printers.conf	
Alınan Backup Dosyasının Bilgileri	…/home/kkk/.cache/deja-dup	.manifest	

GAZİLİ OLMAK AYRICALIKTIR…