ADLİ BİLİŞİM VE TÜRK CEZA MAHKEMESİ'NDE DİJİTAL DELİLLER

Umut DEMİRCİ

Yüksek Lisans Tezi
Kriminalistik Ana Bilim Dalı
Danışman: Prof. Dr. Rıdvan DURAK
2024

(Her hakkı saklıdır)

T.C.
ATATÜRK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
KRİMİNALİSTİK ANA BİLİM DALI

ADLİ BİLİŞİM VE TÜRK CEZA MAHKEMESİ'NDE DİJİTAL DELİLLER

(Computer Forensics and Digital Evidence in The Turkish Criminal Court)

YÜKSEK LİSANS TEZİ

Umut DEMİRCİ

Danışman: Prof. Dr. Rıdvan DURAK

Erzurum

Temmuz, 2024

FEN BİLİMLERİ ENSTİTÜSÜ
Graduate School of Natural and Applied Sciences

T.C.
ATATÜRK ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü Müdürlüğü
TEZ KABUL VE ONAY TUTANAĞI

ADLİ BİLİŞİM VE TÜRK CEZA MAHKEMESİ'NDE DİJİTAL DELİLLER

Prof. Dr.Rıdvan DURAK danışmanlığında, Umut DEMİRCİ tarafından hazırlanan bu çalışma, 08/07/2024 tarihinde aşağıdaki jüri tarafından Kriminalistik Anabilim Dalı Kriminalistik Bilim Dalı'nda Yüksek Lisans tezi olarak **oybirliği** ile kabul edilmiştir.

Jüri Başkanı:	Prof. Dr. Handan UYSAL *Atatürk Üniversitesi*	Aslı Islak İmzalıdır
Danışman:	Prof. Dr. Rıdvan DURAK *Atatürk Üniversitesi*	Aslı Islak İmzalıdır
Jüri Üyesi:	Doç. Dr. Abdulkerim KARABULUT *Erzurum Teknik Üniversitesi*	Aslı Islak İmzalıdır

Enstitü Yönetim
Kurulunun …./…/…. tarih
ve …… sayılı kararı.

Bu tezin Atatürk Üniversitesi Lisansüstü Eğitim ve Öğretim Yönetmeliği'nin ilgili maddelerinde belirtilen şartları yerine getirdiğini onaylarım.

Prof.Dr. Saltuk Buğrahan CEYHUN
Enstitü Müdürü

Aslı Islak İmzalıdır

Not: Bu tezde kullanılan özgün ve başka kaynaklardan yapılan bildiriş, çizelge, şekil ve fotoğrafların kaynak olarak kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir.

ETİK BİLDİRİM VE İNTİHAL BEYAN FORMU

Yüksek Lisans Tezi olarak Prof. Dr. Rıdvan DURAK danışmanlığında sunulan ''Adli Bilişim ve Türk Ceza Mahkemesi'nde Dijital Deliller'' başlıklı çalışmanın tarafımızdan bilimsel etik ilkelere uyularak yazıldığını, yararlanılan eserlerin kaynakçada gösterildiğini, Fen Bilimleri Enstitüsü tarafından belirlenmiş olan Turnitin Programı benzerlik oranlarının aşılmadığını ve aşağıdaki oranlarda olduğunu beyan ederiz.

Tez Bölümleri	Tezin Benzerlik Oranı (%)	Maksimum Oran (%)
Giriş	0	**30**
Kuramsal Temeller	6	**30**
Materyal ve Metot	21	**35**
Araştırma Bulguları ve Tartışma	18	**20**
Sonuç ve Öneriler	6	**20**
Tezin Geneli	15	**25**

Not: *Yedi kelimeye kadar benzerlikler ile Başlık, Kaynakça, İçindekiler, Teşekkür, Dizin ve Ekler kısımları tarama dışı bırakılabilir. Yukarıdaki azami benzerlik oranları yanında tek bir kaynaktan olan benzerlik oranlarının* ***%5'den*** *büyük olmaması gerekir.*

Beyan edilen bilgilerin doğru olduğunu, aksi halde doğacak hukuki sorumlulukları kabul ve beyan ederiz.

Tez Yazarı (Öğrenci)	Tez Danışmanı
Umut DEMİRCİ	Prof. Dr. Rıdvan DURAK
18.07.2024	18.07.2024
İmza: Aslı Islak İmzalıdır	İmza: Aslı Islak İmzalıdır

Tez ile ilgili YÖKTEZ'de yayınlamasına ilişkin bir engelleme var ise aşağıdaki alanı doldurunuz.

Tezle ilgili patent başvurusu yapılması / patent alma sürecinin devam etmesi sebebiyle Enstitü Yönetim Kurulunun …./…/…. tarih ve …… sayılı kararı ile teze erişim 2 (iki) yıl süreyle engellenmiştir.

Enstitü Yönetim Kurulunun …./…/…. tarih ve …… sayılı kararı ile teze erişim 6 (altı) ay süreyle engellenmiştir.

TEŞEKKÜR

Lisansüstü eğitimim boyunca derin bilgi birikimi, ilham verici rehberliği, verdiği destek, tez sürecinde sergilediği sabır, anlayış ve hoşgörüsüyle her zaman yanımda olan, karşılaştığım her zorlukta bana yol gösteren ve her zaman cesaret verici sözleriyle beni motive eden danışman hocam Prof. Dr. Rıdvan DURAK'a verdiği emek ve katkıları için sonsuz teşekkürlerimi sunuyorum.

Ayrıca ilgisini göstermekten kaçınmayan diğer hocalarıma, hayatım boyunca maddi ve manevi desteğini esirgemeyen aileme ve arkadaşlarıma teşekkürlerimi sunarım.

Umut DEMİRCİ

ÖZET

YÜKSEK LİSANS TEZİ

ADLİ BİLİŞİM VE TÜRK CEZA MAHKEMESİ'NDE DİJİTAL DELİLLER

Umut DEMİRCİ

Danışman: Prof. Dr. Rıdvan DURAK

Amaç: Son yıllarda bilişim teknolojilerinde yaşanan hızlı gelişim; sosyal hayattan iş hayatına kadar hemen her alanda, birçok işlemi bilişim sistemleri üzerinden gerçekleştirmemize olanak sağlamıştır. Günümüz dijital çağında teknoloji; insan hayatını kolaylaştırmasının yanında bir o kadar da suça maruz kalmasına neden olmuştur. Bilişim sistemleri üzerinden işlenen suçların soruşturulmasında adli bilişim yöntemleri uygulanmakta ve bu sayede mahkemelere sunulmak üzere dijital deliller elde edilmektedir. Bu çalışmayla adli bilişim uygulamaları ve dijital delillerin elde edilme sürecinin, temel hak ve hürriyetleri zedelemeden, uluslararası standartlarda ve yasal mevzuata uygun bir şekilde yürütülmesinin sağlanması amaçlanmıştır.

Yöntem: Bu tez çalışmasında, güncel mevzuat hükümleri ve son teknolojik gelişmeler ışığında adli bilişim süreci, dijital delil ve dijital delillerin ceza yargılamalarında ki önemiyle ilgili daha önce yapılmış olan ulusal ve uluslararası birçok farklı çalışma detaylıca incelenerek derlenmiştir. İçerikte yer alan bilgiler nitel bir yaklaşımla ele alınarak sunulmuştur.

Bulgular: Adli bilişim uygulamaları ve dijital delillerin elde edilme sürecinde uluslararası ilke ve standartlara bağlı kalınmaması, dijital delillerin yasal kanıt vasfını yitirmesine ve adil yargısal sonuçların alınamamasına sebep olmaktadır. Gelişen teknolojiye paralel olarak güncellenmeyen mevzuat hükümleri, ilke ve prosedürler ile yetersiz uzman personel ve teknik imkansızlıklar süreci sekteye uğratmaktadır.

Sonuç: Gelişen teknolojiye bağlı olarak bilişim sistemleri üzerinden işlenen suçların türü ve sayısı artmaya devam etmekte buna paralel olarak dijital deliller daha da önemli hale gelmektedir. Adli bilişim uygulamaları ve dijital delillerle alakalı yasa hükümleri ile uluslararası ilke ve prosedürlerin, gelişen teknolojiye cevap verecek şekilde güncellenmesi gerekmektedir. Sürecin uzman personel ve teknolojiye cevap verebilen mevzuat hükümleri eşliğinde yapılması, temel hak ve hürriyetleri zedelemeden adil yargısal sonuçların alınmasını sağlayacaktır. Bu sebeple yasa koyucu ve uygulayıcılarının bu hususlar ışığında gerekli önlemleri alması ve toplumda farkındalık oluşturmaları önem arz etmektedir.

Anahtar Kelimeler: Adli bilişim, dijital delil, suç

Temmuz 2024, Sayfa: 90

ABSTRACT

MASTER'S THESIS

COMPUTER FORENSICS AND DIGITAL EVIDENCE IN THE TURKISH CRIMINAL COURT

Umut DEMİRCİ

Supervisor: Prof. Dr. Rıdvan DURAK

Purpose: The rapid development in information technologies in recent years has enabled us to perform many transactions in almost every field from social life to business life via information systems. In today's digital age, technology has made human life easier as well as causing it to be exposed to crime. In the investigation of crimes committed via information systems, forensic computer methods are applied and thus digital evidence is obtained to be presented to the courts. This study aims to ensure that forensic computer applications and the process of obtaining digital evidence are carried out in accordance with international standards and legal regulations without harming fundamental rights and freedoms.

Method: In this thesis, many different national and international studies on the forensic computer process, digital evidence and the importance of digital evidence in criminal trials have been examined in detail and compiled in the light of current legislative provisions and recent technological developments. The information in the content has been presented with a qualitative approach.

Findings: Failure to adhere to international principles and standards in the process of obtaining digital evidence and digital forensic applications causes digital evidence to lose its legal evidence status and prevents fair judicial results. Legislative provisions, principles and procedures that are not updated in parallel with developing technology, insufficient expert personnel and technical impossibilities disrupt the process.

Results: The type and number of crimes committed through information systems continue to increase due to developing technology, and digital evidence becomes even more important in parallel. Legal provisions and international principles and procedures related to digital forensic applications and digital evidence need to be updated to respond to developing technology. Carrying out the process with expert personnel and legislative provisions that can respond to technology will ensure that fair judicial results are obtained without harming fundamental rights and freedoms. For this reason, it is important for lawmakers and practitioners to take the necessary measures in light of these issues and raise awareness in society.

Keywords: Computer forensics, digital evidence, crime

July 2024, 90 pages

İÇİNDEKİLER

KABUL VE ONAY TUTANAĞI i
ETİK BİLDİRİM VE İNTİHAL BEYAN FORMU ii
TEŞEKKÜR iii
ÖZET iv
ABSTRACT v
ŞEKİLLER DİZİNİ viii
KISALTMALAR ve SİMGELER DİZİNİ ix
GİRİŞ 1
KURAMSAL TEMELLER 3
Adli Bilişim 3
Adli bilişimin tarihi 3
Adli bilişimin önemi 4
Adli bilişimin temel süreçleri 4
Adli bilişim türleri 7
Adli bilişimin zorlukları 10
Delil kavramı 10
Dijital delil kavramı 11
Dijital delillerin niteliği 14
MATERYAL VE METOT 19
Bilgisayar Sistemleri 19
Veri depolama aygıtları 20
Sabit disk 21
Taşınabilir disk 21
USB bellek 22
Hafıza kartı 22
Bilgisayar Ağları 23
Mobil Cihazlar 24
Cep telefonu 24
Tablet 25
Gömülü sistemler 25
Bulut sistemler 26
Dijital Delil İnceleme ve Analiz Yöntemleri 26

Dijital Delil İncelemede Kullanılan Ekipmanlar 27
Yazma koruma ekipmanları 28
Disk imajı alma işlemi 32
Dosya analizi 37
İşletim Sistemi Üzerinde Yapılan Analizler 39
Network analizi 40
Mobil sistemlerin analizi 41
Ceza Muhakemesi Hukukunda Delil Kavramı 42
Akılcılık 44
Temsil edicilik/ gerçekçilik 44
Hukuka uygunluk 45
Önemlilik 45
Müştereklik 45
Güvenilirlik 46
Elde edilebilirlik 47
Ceza Muhakemesi Hukukunda Delil Türleri ve Dijital Delillerin Yeri 47
Doğrudan deliller 47
Beyan 47
Belge 48
Belirtiler 48
Dijital Delillerin Hukuki Geçerliğinin İncelemesi 49
Elektronik imza bilgisi 50
Karma İşlevi (Hash Function) bilgisi 53
Süreç bilgisi 53
Üst veri bilgisi 54
İlişki bilgisi 55
Dijital Delillerin Hukuka Uygunluk Bakımından Değeri 55
Türk Hukukunda Dijital Delillere İlişkin Düzenlemeler 56
CMK kapsamındaki düzenlemeler 57
ARAŞTIRMA BULGULARI ve TARTIŞMA 62
SONUÇ ve ÖNERİLER 70
KAYNAKLAR 76
ÖZGEÇMİŞ 79

ŞEKİLLER DİZİNİ

Şekil 1. Dijital küresel genel bakış 8
Şekil 2. Tipik optik disk 20
Şekil 3. Sabit disk 21
Şekil 4. Taşınabilir disk 21
Şekil 5. USB bellek. 22
Şekil 6. Hafıza kartı 23
Şekil 7. Bilgisayar ağları 23
Şekil 8. Cep telefonu 24
Şekil 9. Tablet 25
Şekil 10. Gömülü sistemler 25
Şekil 11. Bulut sistemler 26
Şekil 12. Adli bilişim süreçleri 28
Şekil 13. Tableau T35u yazma koruma köprü kiti 30
Şekil 14. Tableau T6u yazma koruma köprü kiti SAS disk bağlantısı 30
Şekil 15. Tableau T35689iu Forensic SATA/IDE Bridge modeli 31
Şekil 16. CRU WiebeTech Forensic UltraDock v.5.5 modeli 31
Şekil 17. SAFE Block yazma koruma yazılımı 32
Şekil 18. FTK Imager disk imajı alma aşama 1 33
Şekil 19. FTK Imager disk imajı alma aşama 2 33
Şekil 20. FTK Imager disk imajı alma aşama 3 34
Şekil 21. FTK Imager disk imajı alma aşama 4 34
Şekil 22. FTK Imager disk imajı alma aşama 5 35
Şekil 23. FTK Imager disk imajı alma aşama 6 36
Şekil 24. FTK Imager disk imajı alma aşama 7 36
Şekil 25. FTK Imager disk imajı alma aşama 8. 37
Şekil 26. Encase Forensic v8.07 kullanıcı arayüzü 38
Şekil 27. Accessdata Forensic Toolkit (FTK) v5.2 kullanıcı arayüzü. 39
Şekil 28. Elektronik imza 51
Şekil 29. Hashing algoritması 53
Şekil 30. Bir fotoğrafın gömülü meta verileri 54

KISALTMALAR ve SİMGELER DİZİNİ

BTK : Bilgi Teknolojileri Kurumu

CD : Compact Disc / Yoğun Disk

CMK : Ceza Muhakemesi Kanunu

CRL : Certificate Revocation List İptal Bilgilerini Sertifika İptal Listesi

DVD : Digital Versatile Disc / Çok Amaçlı Sayısal Disk

OCSP : Online Certificate Status Protocol Çevrimiçi Sertifika Durum Protokolü

RAM : Rasgele Erişim Belleği

ROM : Salt Okunur Bellek

TSE : Türkiye Standartları Enstitüsü

USB : Universal Serial Bus Evrensel Seri Veriyolu

GİRİŞ

Suç ve suçluluk kavramları kabaca insan toplumunun ortaya çıkışına paralel olarak ortaya çıkmıştır. Suçun ve zanlıların belirlenmesi için soruşturma başlatılmış, olay yeri ve delillerin incelenmesine ihtiyaç duyulmuştur. Günümüzde suç soruşturmalarında klasik olay yeri ve delil kavramına ek olarak sanal bir olay yeri ve dijital delil kavramı ortaya çıkmıştır. Bilişim teknolojilerinin durdurulamaz gelişimi yeni suçların doğmasına hatta klasik suçların bile bilişim sistemleri üzerinden işlenmesine olanak sağlamıştır. Bu dijital dönüşümün insanlara getirdiği kolaylıkların yanı sıra birçok dezavantajı da beraberinde getirmiştir. Dijital dünyanın her noktasında var olan insan artık bilişim suçlarının hem faili hem de mağduru konumda olmuştur. Bilişim sistemleri olay yerine dönüşmüş, klasik delillerin yerini dijital deliller almıştır. Bu durum bilişim sistemleri üzerinden işlenen suçların soruşturulmasında yeni bir yaklaşımın uygulanmasını zorunlu kılmıştır. Bu yeni yaklaşım adli bilişim olarak literatürde yeri almış, uygulanma süreçleri hukuki ve teknik prosedürlere bağlanmıştır. Bilişim sistemleri üzerinden işlenen suçlarda suçlunun ortaya çıkması ve bir sonuca varmak için dijital delil ve materyalleri toplamak, analiz etmek ve bir sonuca varmak gerekmektedir. Bu bağlamda çalışmamızda adli bilişim kavram ve türleri değerlendirildikten sonra bilişim sistemleri üzerinden elde edilen delillerin teknik yapısı ele alınarak, hukukun üstünlüğü ve evrensel insan hakları ve onurunun zedelenmeden suç soruşturmalarının nasıl yapılması gerektiği açıklanacak ve son olarak Türk hukuk sisteminde bilişim suçlarının yasal dayanağını oluşturan Ceza Muhakemeleri Kanunun ilgili hükümleri incelenerek adli bilişim sürecinin daha sağlıklı ve etkin bir şekilde yürütülmesi adına fikir oluşturulması sağlanacaktır.

Çalışmada, Adli Bilişim ve Türk Ceza Mahkemesi'nde Dijital Deliller başlığı altında, bilişim sistemleri kullanılarak işlenen suçların soruşturmasında kullanılan adli bilişim uygulamaları ve bu uygulamalar neticesinde elde edilen dijital delillerin incelenerek, tüm sürecin yasal prosedüre uygun bir şekilde yürütülmesinde fikir oluşturması amaçlanmıştır.

Dünyanın giderek dijitalleşmesi ve teknolojik gelişmelerin hızlı bir biçimde artış göstermesi sonucunda, adli bilişim ve dijital deliller daha da önem kazanmaktadır. Dijital deliller, ceza davaları, hukuki anlaşmazlıklar, ticari davalar gibi birçok farklı hukuki işlemde önemli bir rol oynamaktadır. Dijital kaynaklardan elde edilen bu deliller adli bilişim teknikleri uygulanarak anlamlı birer metin haline getirilir. Adli bilişim sürecinin sağlıklı ve mevzuata uygun yürütülmesi, dijital delillerin güvenliği ve güvenirliliğinin sağlanması, modern suç

soruşturmalarında hayati öneme sahip olmuştur. Adil yargısal sonuçların alınabilmesi ve suçluların cezalandırılabilmesi için hızla gelişmekte olan teknolojiye uyum sağlayabilecek kapsayıcı düzenlemeler gerçekleştirmenin ve farklı bir metodolojik yaklaşım sergilemenin önemi ortaya çıkmıştır. Bu çalışmayla konuya taraf her kesime farklı bir bakış açısı kazandırmak ve öneriler sunmak hedeflenmiştir.

Araştırma zaman aralığı olarak araştırmanın gerçekleştirildiği 2022- 2024 yılları olması itibariyle kaynakçada sunulan kaynaklardaki bilgiler ile sınırlıdır.

KURAMSAL TEMELLER

Adli Bilişim

Dr. H. B. Wolfe'a göre bir adli bilişim sistemi, mahkeme salonunda tutarlı ve anlamlı bir şekilde sunulabilen yazılım cihazlarından ve çeşitli kayıt cihazlarından ve dijital ortamlardan kanıt toplamak için sistematik bir dizi teknik ve prosedür içermektedir. Daha kesin bir tanımla adli bilişim, dijital delillerin mahkemede toplanması, analiz edilmesi ve sunulması sürecidir. Adli bilişimin kapsamı, suçların soruşturulması ile sınırlı değildir; ayrıca veri kurtarma, günlük izleme, veri toplama (eski veya hasarlı cihazlardan) ve uyumluluk ihtiyaçlarını karşılama ile iç içedir (Shakeel 2003).

Genel olarak adli soruşturma, suç veya yasaklanmış bir faaliyetin olup olmadığının tespitine esas teşkil eden bilgi sistemleri ve depolama birimleri ile ilgili tüm çalışmaları kapsamaktadır (Kılıç 2019).

Adli bilişimin tarihi

Bilgisayarlar ilk defa 1940'ların ortalarında ortaya çıkmış ve bu teknolojinin hızlı gelişimini kısa süre sonra çeşitli bilgisayar suçları izlemiştir. 1960'ların ortalarında, SRI International'dan Donn Parker, siber suçları ve etik olmayan bilgisayar faaliyetlerini araştırmaya başlamış ve "insanların bir bilgisayar merkezine girdiklerinde ahlaklarını kapıda bıraktıklarını" fark etmiştir. Parker'ın çalışmaları sonraki yirmi sene boyunca devam etmiş ve bilgisayar etiği tarihinde bir dönüm noktası olarak kabul edilmiştir. İlk siber suç kovuşturma davası 1966'da ABD'nin Teksas eyaletinde açılmış ve beş sene hapis cezasıyla sonuçlanmıştır. 1970'lerde ve 1980'lerde kişisel bilgisayarlar gerek evde gerekse işyerinde yaygınlaşmış; kolluk kuvvetleri daha sonra yeni bir suç kategorisinin ortaya çıktığını fark etmiştir. Bu suç siber suçtur. Tüm suçlar gibi, bu yeni kategori de başarılı bir şekilde kovuşturma için güvenilir kanıtlar gerekmektedir. Amacı siber suçları araştırmak, belgelemek ve işlemek olan adli bilişim disiplini böyle doğmuştur (Shakeel 2003).

1990'lara gelindiğinde, teknolojik olarak gelişmiş her ülkedeki kolluk kuvvetleri bilişim suçlarının farkındaydı, soruşturma ve kovuşturması için bir sisteme sahipti. Birçok bilimsel araştırma merkezi de kuruldu ve yazılım endüstrisi, bilişim suçlarının araştırılmasına yardımcı olmak için çeşitli özel araçlar sunmaya başladı (Noblett *et al*. 2000) (Bem *et al.* 2008).

Adli bilişimin önemi

Eğitim, yeri ve zamanı ne olursa olsun, tek yönlü ya da karşılıklı iletişimin ön koşulunu varsayar. Dijital araçlar yardımıyla gerçekleştirilen iletişim faaliyetleri sayesinde bilgisayar, tablet ve cep telefonu gibi dijital ortamlarda belge ve veri oluşturmak ve kaydetmek mümkündür. Bazı suçlar artık fiziksel ortamlarda olduğu gibi bu dijital alanlarda da işlenmektedir (Mohammed 2015). Çeşitli dijital ortamlarda suç sonrası delil sayılabilecek veri hazırlama, toplama, analiz ve raporlama gibi süreçler bulunmaktadır (Conlan and Baggili 2016).

Dijital delillere ulaşabilmek için adli bilişim yöntemleri kullanılır (Henkoğlu 2020). Süreçte adli bilişime konu olmuş delillerin kopyalanması önem arz eder. Adli bilişim disiplininin işaret ettiği şekilde usulüne uygun kopyalanmayan dijital materyaller delil niteliği taşımayacaktır. Ayrıca adli bilişimin işaret ettiği yönde dijital materyallerin kopyalanması araştırma sürecinde de kolaylık sağlayacaktır (Akbal ve Doğan 2018).

Adli bilişimin temel süreçleri

Bu başlık altında Adli bilişimin temel süreçlerinde yer alan işlemler açıklanacaktır.

Delil tespiti ve olay yeri incelemesi

Delil, hukuki ispat olarak kullanılmakta olan gözlem ve bilgilerdir. Gerçeğin ortaya çıkması ve hukuki karar verilebilmesi için olay yerinin korunması ve olay yerinden adil bir biçimde delil alınmasının sağlanması gerekmektedir. Olay yeri incelemesi sırasında gerçekleştirilen işlemler kanunla düzenlenmektedir (Düden 2019).

Olay yeri incelemesinin amacı;

1.Bir olayın suç olup olmadığını tespit etmek,
2.Tehlikeli bir durumun koşullarını belirleyebilmek,
3.Olayın geçtiği yerde suça ilişkin delil tespit etmek,
4.İşlenen suçun açıklanması ve yasal makamların doğru karar verebilmesi için olay mahallini belgelemek
5. Soruşturma, olay yeri, şüpheli ve şikâyetçi arasındaki ilişkiyi açıklayabilmek (Düden 2019).

Olay yeri incelemesi bir arama operasyonudur. Suç mahallindeki her nesne delil olarak kullanılmaktadır. Bu nedenle olay mahallinin ilk incelemesi gözlem yoluyla gerçekleştirilmelidir. Olay yeri tespit edildikten sonra kamera ile ayrıntılı olarak kayıt altına alınmalı ve fotoğraflanmalıdır. Gerekirse olay yeri hakkında notlar alınmalıdır. Adli delillerin

toplanması, saklanması ve teslimi yönetmeliğe göre (Resmi Gazete 2019), olay yeri incelemesi sırasında elde edilen bütün deliller bulundukları yerde işaretlenmeli ve numaralandırılmalıdır. Etiket üzerinde; delilin yeri, alındığı belge numarası, polis biriminin adı, tarih, soruşturmacının kimliği ve gerekli diğer bilgiler yazılmalıdır (Düden 2019).

Bilişim sistemi suçları; olay yeri incelemesinin klasik adımlarına ek olarak, özel bilgi ve yetenek gerektiren bazı önlemler vardır. Dijital delillerin değiştirilmesi, yok edilmesi ve manipüle edilmesi kolay olduğundan, olay yeri inceleme esnasında yalnızca uzman personel veri taşıyıcılarını kurcalamalıdır (National Institute of Justice 2004).

Olay yeri incelemesi, bir olaya ilişkin bilimsel gerçeklerin ortaya konulması sürecini ifade etmektedir. Şüphelinin suçuyla ilgili fiziksel delillerin kullanılmasında olay yeri incelemesinin sonuç vereceğini kabul etmemiz gerektiğinden, soruşturma unsuruna ağırlık verilmesi gerekmektedir. Davanın koşullarının bilinmesi ve kontrol edilmesi, gerçekleri keşfedip anlamak, eylem ve olayların gerçekten gerçekleşip gerçekleşmediğini belirlemek için araştırılması gerekmektedir. Olay yeri incelemesinin amacı, suçun bilimsel olarak yeniden yapılandırılmasını sağlamaktır. Sonuçlar araştırma ve hukuki soruları yanıtlamak için kullanılabilmektedir. Her vakanın kendi öngörülemeyen sorunları vardır (Jerry *et al.* 2011).

En başından itibaren mümkün olduğu kadar kanıt sağlamak için derin perde arkası soruşturma yapılması gerekmektedir. Her ne kadar olay yeri incelemesi sıklıkla klasik olay yeri incelemesiyle karıştırılsa da DeForestand (2005)'ın tanımladığı gibi olay yeri incelemesinin aşamaları olay yerinde yapılan çalışmanın ötesine uzanmaktadır. Kanıtlar keşfedildikten sonra laboratuvarda analiz edildiğinde laboratuvar sonuçlarının bilimsel olarak yorumlanması gerekmektedir.

Görünen o ki, olay yeri incelemesi sadece kolluk kuvvetlerinin ve müfettişlerin dikkatli gözetimi altında sarı bant içinde yapılmamakta, aynı şekilde olay esnasında fiziksel delilleri ortaya çıkarmaya çalışan geniş çaplı bir soruşturma veya seriyle ilgili olayları kapsamaktadır. Nihai sonuç, toplu olay yeri incelemesi ve işleminin birleşik sonucudur. Literatürdeki pek çok teknik çalışma, bir kişi için farklı sahne görevlerinin gerekliliğini anlatmaktadır (Jerry *et al.* 2011).

Suç mahalli, suçun işlendiği herhangi bir alan olarak tanımlanmaktadır. Birçok durumda suç olay yeri, tanık olunan veya bazı gerçeklerden veya kanıtlardan anlaşılan şiddet nedeniyle keşfedilmiştir. Açıkçası birçok suç türünün genellikle izlerin bulunduğu alan anlamında bir "sahne"si yoktur. Sahtecilik ve zimmete para geçirme gibi suçlar, işlenmesinde herhangi bir şiddetli veya istisnai fiziksel aktiviteyi gerektirmez. Suçlunun çevresine herhangi

bir etkisi yoktur. Ancak şiddet suçları bir mücadeleyi, bir arbedeyi içermektedir. Suç mahalli, fiziksel çevreyle güçlü bir şekilde temas halindedir. Ancak suç, bu tanımın da ima ettiği gibi her zaman tek bir mekânla sınırlı değildir. Yeniden yapılandırma uzmanı için belirli bir vakayı birden fazla bağlantılı olaydan oluşan bir durum olarak kavramak en iyisidir. Bu zihniyet, olayların zaman çizelgesini oluşturmaya çalışırken, farklı alanların kapsamlı bir şekilde araştırılmasının gerekliliğini kavramak daha kolay hale gelir. Bu amaçla suç mahalli ile ilgili alttakiler söylenebilmektedir (Jerry *et al*. 2011):

- Farklı türde suç mahalleri vardır.
- Olay yeri incelemesi, yeniden inşası ve onarımında en önemli hususlardan biri suç mahallidir.
- Analiz, ne tür bir olay yerinin keşfedildiğinin belirlenmesidir. Bununla kastettiğimiz suç mahallinin suç davranışıyla ilişkisinin suç bağlamında kurulmasıdır. Belirli bir vakada olay yeri tipini belirlerken, yeniden yapılandırma uzmanı uyarılır.
- Hikâyeyi fiziksel kanıtların anlatmasına izin verilmesi gerekmektedir.
- Önyargılı teorileri bir kenara bırakıp, suç mahalli türlerini göz önünde bulundurarak fiziksel kanıtlardan sağlam bir yeniden yapılanmayı sağlamak gerekir.

Toplama

Adli süreçteki ilk adım, olası bilgi kaynaklarının belirlenmesi, bilgilerin tanımlanması, etiketlenmesi, saklanması ve geri alınmasıdır. Bu süreçte, veri bütünlüğü sağlama ve toplama, potansiyel veri kaynaklarını koruyan kılavuzlara ve prosedürlere göre yapılmaktadır. Bu sayede mevcut ağ bağlantıları gibi olası ve geçici dinamik veri kayıplarının önüne geçilmektedir (Kent *et al*. 2006).

Koruma

Ceza Muhakemesi Kanunu'nun "Malların veya Kazançların Tutulması ve Müsadere Edilmesi" başlıklı 123 (1) maddesi, "İspat aracı olarak yararlı görülen ya da eşya veya kazanç müsaderesinin konusunu oluşturan malvarlığı değerleri, muhafaza altına alınır" şeklinde belirtmektedir. Adli tıp uzmanları, olay mahallinde ortaya çıkabilecek her türlü duruma karşı hazırlıklı olmalıdır. Bu süreçte öncelikle olay yeri analizi yapılmalı ve açık dijital cihazlar kontrol edilmelidir. Açığa çıkan cihazlardaki verilerin kaybolmaması ya da yok edilmemesi için bu durum derhal ele alınmalıdır. Mekânda açık cihazlar varsa cihaz açıkken o an canlı görüntü alınabilir. Açık mobil cihazları bloke ederken, bu cihazların uçak modunda

olduğundan veya bağlantısını kesmek için bir taşıma çantasında saklandığından emin olunmalıdır.

Muayene

Adli olaylar sırasında toplanan bilgilerden önemli bilgiler çıkarılır ve bu bilgiler üzerinden bir ön inceleme yapılır. Bu adım aynı zamanda işletim sistemi algılama ve baypas, şifreleme ve veri algılamayı önleyen erişim kontrol mekanizmaları gibi işlemleri de içermektedir (Wiles and Reyes 2007).

Analiz

Muayene aşamasında ilgili bilgiler çıkarıldıktan sonra bu bilgilerin analiz edildiği aşamadır. Adli bilişim, doğru duruma ulaşmak için metodik bir yaklaşım kullanmaya dayanmaktadır. Analiz aşamasında kişiler, yerler, nesneler ve olaylar tanımlanır ve bu nesneler şekillendirilerek bir sonuca varılmaktadır. Dijital veriler, kullanıcı verilerini, kullanıcı verileriyle ilgili meta verileri, etkinlik günlüklerini ve sistem günlüklerini içermektedir. Sistem günlükleri genellikle bu projeyle ilgili bilgileri içerir, fakat adli tıp uzmanları sonuçları belgelendirmeli ve gerçekleştirilen tüm eylemleri anlaşılır ve tartışmasız bir biçimde analiz etmelidir (Dimitriadis *et al*. 2020).

Raporlama

Analiz aşamasında ortaya çıkan bilgiler, kanıtlanmış teknikler kullanılarak açık ve net bir biçimde ifade edilerek yasal mercilere sunulmaktadır. Ayrıca bu aşamada sunulan bilgilerin gerektiğinde nitelikli adli tıp uzmanları tarafından doğrulanabilecek biçimde düzenlenmesi de çok önemlidir (Kent *et al*. 2006).

Adli bilişim türleri

Teknolojinin ve internetin gelişmesiyle birlikte bilişim teknolojileri ve online platformlar günümüzde farklı ve kullanılabilir hale gelmiştir. Günümüz teknolojisinin seyri içerisinde birçok değişikliğe uğramıştır. Bilgi sistemlerini içeren tüm elektronik deliller, adli araştırma alanlarının gelişimini etkilemiştir. Bu tasarıma bağlı olarak teknolojik cihazların güçleri, işlevleri ve görselleri farklı olduğu için bu değişim adli bilişim, ağ adli tıp, mobil suç soruşturma, sosyal medya suç soruşturma gibi farklı uzmanlık türlerinin ortaya çıkmasına neden olmuştur (Barmpatsalou *et al*. 2013).

Bilgisayar adli bilişimi

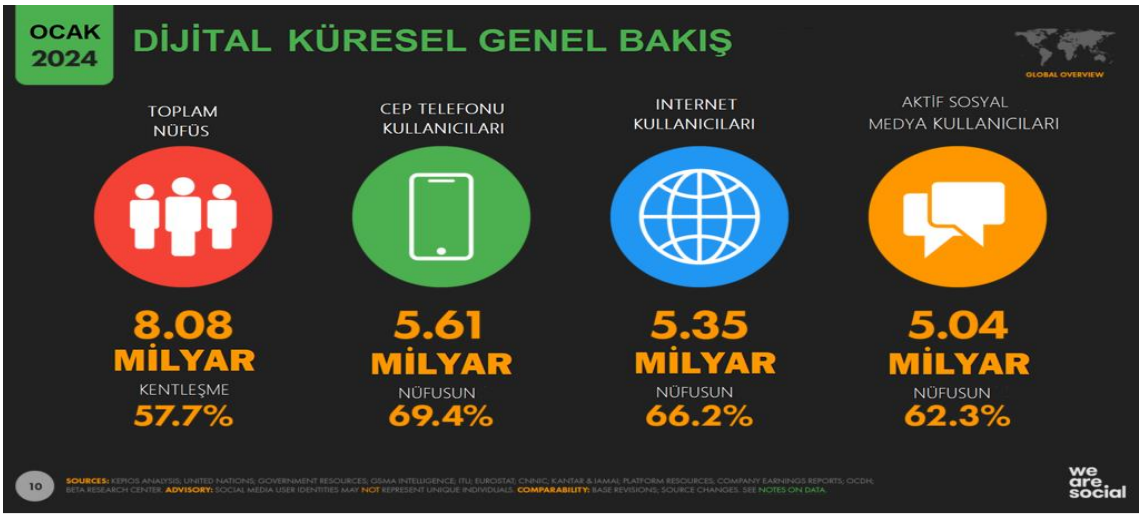
Bu adli soruşturma çeşidi, en eski ve en iyi bilinen adli soruşturma çeşididir. Adli bilişim işlemlerinin büyük çoğunluğu şüpheli veya mağdurun bilgisayarında yapılmaktadır. Adli bilişim, sadece adli soruşturmalarda değil yaşamımızın her alanında, kısaca örneğin elektronik cihazların bulunduğu üniversitelerde, şirketlerde, hastanelerde ve kamu kurumlarında karşımıza çıkan çok geniş bir adli bilim dalıdır (Kent *et al*. 2006).

Ağ adli bilişimi

İnternetin hızlı gelişimi, yeni ve büyük ağların inşası ve telekomünikasyon sistemlerinin devasa boyutları, siber-adli tıp alanının hızla gelişmesine yol açmıştır. Siber adli tıp tarafından kullanılan veriler dinamik ve online olabilmektedir. Siber adli tıp, saldırıları tespit etmek, izlemek, kontrol etmek ve savunmak için aktif ağlardan toplanan verilerin kullanılmasını içermektedir (Barmpatsalou *et al*. 2013).

Mobil cihaz adli bilişimi

Teknik kaynakların mobilizasyonu sayesinde günlük iş ve aktivitelerin büyük bir bölümünü mobil cihazlar ile gerçekleştirmeyi sağlamaktadır. Bu durum cep telefonu kullanımına olan talepte patlamaya sebep olmuştur. GSMA Intelligence yaptığı son araştırma; 2024 yılı başında tekil cep telefonu kullanıcılarının sayısının 5,61 milyar olduğunu, dünya toplam nüfusunun %69,4'ünün artık bir mobil cihaz kullandığını ve küresel toplamın 138 milyon (%2,5) arttığını ortaya koymaktadır (Şekil 1).



Şekil 1. Dijital küresel genel bakış

Mobil cihazlardan veri alma sebepleri, bunları işlemek için kullanılan teknolojiler kadar çeşitli olabilmektedir. Bazen sadece belirli veriler soruşturmayla ilgiliyken, diğer durumlarda tam bir adli soruşturma ve silinen verilerin kurtarılması gerekebilir, bu da

telefonun tüm hafızasının silinmesiyle yapılabilmektedir. Mobil cihazlardaki veri türleri ve bunların nasıl kullanıldığı devamlı olarak gelişmektedir. Bu faktörlerden dolayı, mobil cihazlardan verilerin alınması ve raporlanması için kılavuzlar ve süreçler geliştirmek çok önemlidir. Bu yönergeler ve süreçler, cep telefonu teknolojisi geliştikçe ve değiştikçe düzenli olarak gözden geçirilmeli ve güncellenmelidir (Murphy 2012).

Sosyal ağ adli bilişimi

Sosyal medya, ülkemizde kişilerin birbirleriyle iletişim kurabildikleri, mesaj gönderebildikleri, resim ya da video paylaşabildikleri, beğenip yorum yapabildikleri yaygın bir platformdur. DataReportal'ın Meltwater ve We Are Social ortaklığıyla hazırladığı Digital 2024 isimli son rapora göre, 5,04 milyar aktif sosyal medya kullanıcısı bulunmaktadır. Sirkhet Danışmanlık'ın açıkladığı verilere göre; Türkiye'de 2024 yılı itibariyle 57 milyondan fazla sosyal medya kullanıcısı bulunmaktadır. Bu rakamlarla orantılı olarak günümüzde yaygın olarak kullanılan sosyal ağlar ve bilgi sistemleri aracılığıyla işlenen suçların kapsamı da artmaktadır. Bu sebeple sosyal medya adli bilişimi, adli bilişimin bir alt disiplini olarak gelişmekte ve sosyal medya aracılığıyla işlenen suçların tespitinde çeşitli teknik ve metotlar kullanılmaktadır (Barmpatsalou *et al*. 2013).

Bellek adli bilişimi

Salt okunur bellek (ROM) ve rasgele erişim belleği (RAM), bir mobil cihazdan dijital kanıt toplarken iki önemli etkenlerdir. Kalıcı bellek (RAM), sistem kapatıldığında bütün veriler silinir ve kaybolur. Cihaz aktif olarak çalışırken olay yerinde RAM bellekten veri toplanmalıdır. Çoğu durumda bu, özel bir yazılımın başlatılmasını ve şüpheli sistemin kendisinde çalıştırılmasını, RAM içeriğini bir tür kusurlu harici depolama aygıtına yazmasını gerektirir. Her cihazın belirli bir donanımı vardır. RAM ve ROM her cihazda yer almaktadır. Rastgele Erişim Belleği, belirli bir görevi gerçekleştirirken bilgileri depolayan geçici bir bellektir. Yazılabilir bellek, mobil cihazların dâhili belleğidir. Cihazın pili tamamen boşalırsa ya da cihaz kapanırsa, RAM'de depolanan tüm veriler geri yüklenemez. Bu yüzden bellek adli bilişimi daha çok dikkat ve titizlik gerektirir.

Görüntü ve ses adli bilişimi

Dijital görüntülerin, ses ve video kayıtlarının toplanması, analiz edilmesi ve değerlendirilmesi ile kaydın orijinal olup olmadığına, izin verilip verilmediğine ya da kazara tahrif edilip edilmediğine bağlı olarak gerçekliğinin tespit edilmesi ve doğrulanması süreçlerini içermektedir (Ayers *et al*. 2014).

Diğer adli kanıt türlerinin aksine, ses ve video kayıtları bir suçun gerçek zamanlı, görgü tanığı gibi anlatımını sağlayabilir, soruşturmacılar olup biteni izleyebilir veya duyabilir. Son yıllarda bir soruşturmaya yardımcı olabilecek kayıtlı ses ve video kaynakları katlanarak arttı. Kapalı devre televizyon sistemleri (CCTV) ve benzeri video ve ses kayıt cihazları, işyerlerinde, trafik kavşaklarında, otoparklarda, banka ATM'lerinde, mobil cihazlarda bulunabilmekte, suç soruşturmaları için önemli kaynaklar haline gelmektedir.

Adli bilişimin zorlukları

Bilgisayar ve ağ teknolojisindeki hızlı büyüme ve gelişme, mevcut adli bilişim araçlarını ve tekniklerini etkisiz hale getirmiştir. Adli bilişimin hızlı gelişimi, standardizasyon ve eğitim eksikliğine yol açmıştır. Her soruşturma benzersiz olduğundan, her adli analiz için standart bir prosedür oluşturmak güçtür. Eğitim ihtiyaçlarını karşılamak için bazı şirketler sertifika programları sunmaya başlamıştır. Bu nedenle kolluk kuvvetleri memurları dijital kanıt toplamak ve hızla gelişen teknolojiye ayak uydurmak için eğitmeye çalışılmaktadır. Dijital bir bilgisayarda depolanan kanıtları analiz etmek, adli tıp bilimindeki en büyük zorluklardan birisidir. Ulusal ve uluslararası yasalar bilgi toplanmasını sınırlayabildiğinden, yasalar analistlerin soruşturma yürütme kabiliyetini sınırlayabilmektedir. Dijital adli bilişimdeki bir diğer zorluk da analiz edilecek veri miktarının artmasıdır. Veri miktarı arttıkça, adli bilişimin yürütülme biçimi de artmaktadır. Büyük veri, çok büyük veri olarak kabul edilir ve verinin hacmi, hızı, çeşitliliği ve değişkenliği ile karakterize edilmektedir. Geleceğin en büyük zorlukları bulut bilgi işlem, meta veriler, adli analizden kaçınma, şifreleme, sosyal ağlar, nesnelerin interneti ve kablosuz ağlardır. Adli bilişim teknolojileri, dijital adli tıp toplumunun önünde güçlü bir engel haline gelmektedir. Bu yöntemler, adli analizden kaçınmak için tasarlanmıştır. Ayrıca, adli süreçte kanıtların mevcudiyetini ya da kullanılabilirliğini tehlikeye atmayı amaçlamaktadırlar (Sadıkoğlu *et al*. 2017).

İnternetin sınırları olmadığı için daha geniş bir kitleye hitap eder ve taciz, hakaret, dolandırıcılık ve kötüye kullanım gibi olaylar farklı coğrafi konumlarda yaşayan insanlar tarafından işlenebilmektedir. Ayrıca gelişmiş teknoloji aracılığıyla görüntüleri değiştirme, sesleri manipüle etmek suretiyle, bireylerin mahremiyetine saldırılar yapılmakta, en temel hakları ihlal edilmektedir. Teknolojide ki bu gelişim elektronik medyadaki güvenlik açıklarını arttırmakta, adli bilişim uygulamaları ve soruşturmalarda zorluklara sebep olmaktadır.

Delil kavramı

Delil sözcüğü dilimize Arapçadan geçmiştir. İspat kelimesi, delil sözcüğünün sıfat halidir. Yol gösterme, kılavuzluk ve rehberlik kavramlarına tekabül eden sözcüğü, kendini

bilmeyi, yani başka bir şeyi bilmeyi gerekli kılan, bir şeyin başka bir şeyi bilme durumunda olmak anlamına gelmektedir (Şimşek 2001).

Delil, yargı makamlarının ve özellikle adli makamların görevlerini yerine getirmelerine yarayan bir araçtır (Kunter 1981).

Delil, başta adli makamlar olmak üzere adli makamların gerçeği araştırmak için kullanmış oldukları bir araç olduğu gibi, hâkimin de bir suçun işlenip işlenmediğini araştırmak için kullandığı bir araçtır (Tosun 1984).

Ceza davalarının maddi konusu, geçmiş bir olayın yeniden düzenlenmesidir. Bu yapılanma, yargılama sırasında hâkimin zihninde tarafların yer alması için yapılmaktadır. Delil, bu canlandırmanın ya da başka bir deyişle geçmiş bir olayın parçalarını bugüne taşımanın yoludur. Başka bir deyişle delil, maddi gerçeği keşfetmek için delil olarak kullanılan bir araçtır. Öte yandan, delilin rolü, adli makamın yasal olarak kabul edilen yollarla, fiilin fail tarafından işlenip işlenmediğine dair mutlak kesinliğe ulaşmasını sağlamaktır (Bıçak 2011).

Öte yandan, tanıklığın işlevi, savcının, fiilin fail tarafından işlenip işlenmediğine hukuken kabul edilmiş yollarla tam olarak ikna edilmesini sağlamaktır. Delil özgürlüğü ve vicdani bir delil sistemi kabul edilmektedir çünkü ceza davalarının amacı maddi gerçeğe ulaşmaktır. Buna göre kural olarak bir ceza davasında delil her şey olabilmektedir (Akyürek 2012).

Ceza Kanunu'nun 217. maddesine göre hâkim, önüne sunulan ve tartışılan delilleri özgürce ve vicdani kanaatle değerlendirmektedir. Bilinçli inanç, yetkili bir makamın, aklın rehberliğinde ve kanunun öngördüğü usul ve esaslara göre yaptığı adli işlemler sonucunda önemli bir olayın meydana geldiğine dair makul şüphenin ötesinde bir kanaate varmasıdır (Feyzioğlu 2020).

Bir cismin ya da ifadenin delil olabilmesi, hâkimin belli bir meselenin delili hakkında vicdani kanaatini nasıl oluşturduğuna bağlıdır. Bu nedenle kanun kapsamında elde edilen her türlü nesne delil olarak kullanılabilmektedir.

Dijital delil kavramı

Tarihsel olarak hukuk sistemi, dijital delilleri kulaktan dolma kanıtlar olarak görmüştür çünkü verilerin gerçeklere dayalı olduğunu tespit edecek hiçbir bilimsel teknik yoktu. Bu, mahkemelere sunulan dijital delillerin, gerçekliği ve bütünlüğü makul şüphenin ötesinde belirlenemediği için genellikle reddedileceği anlamına geliyordu. Ancak,

teknolojinin küresel olarak benimsenmesi ve suç faaliyetlerinde kullanılmasıyla birlikte dijital deliller daha yaygın hale geldikçe, kabul edilebilirlik konusunda istisnalar ortaya çıkmaya başladı. Örneğin, Federal Kanıt Kuralları 803(6) uyarınca, dijital delilleri kulaktan dolma delil olarak görme konusunda bir istisna bulunmaktadır; bu durumda dijital delil; bir eylem, olay, durum, görüş veya tanıdır. Ancak dijital delillerin bu istisna kapsamında bir delil olarak nitelendirilebilmesi için dijital delilin orijinal ve güvenilir olduğunun gösterilmesi gerekir. Hangi tür verilerin kabul edilebilir bir delil oluşturduğuna ilişkin kriterler aşağıdaki kategorilere girer:

- Teknoloji tarafından üretilen veriler, algoritmalar (örn. günlük dosyaları) vasıtasıyla oluşturulan ve bakımı yapılan dijital verilerdir. Bu veriler algoritmaların düzgün çalışması şartıyla verilerin doğruluğunun kanıtlanması temelinde dijital delil olarak kabul görebilir.
- Teknoloji tarafından depolanan veriler, kullanıcı girişi ve etkileşimleri vasıtasıyla oluşturulan ve bakımı yapılan herhangi bir dijital veri, veriyi oluşturan kişinin güvenilirliği ve veriyi hiçbir şekilde değiştirmediği kabul edilmesi şartıyla dijital kanıt olarak değerlendirilebilir.

Bu kanıt kategorileri temel alınarak, kanıt türlerine başka bir bakış açısı sağlamak için arka plan verileri, ağ cihazları, yedeklemeler, kimlik doğrulama kayıtları, denetim bilgileri, kullanıcı hareketleri, web tarama geçmişi vb dijital veriler, dijital delil türlerinden bazılarını oluşturacaktır.

Teknoloji tarafından üretilen ve depolanan bütün dijital verileri, tarihsel olarak hukuk sistemleri tarafından kesin kanıt olarak görülmediğini akılda tutmak önemlidir. Ancak teknolojinin bu kadar yaygın hale gelmesi ve gelişmesi göz önüne alındığında mahkemeler, dijital verileri güvenilirliği ve gerçekliği kabul gördükten sonra delil olarak değerlendireceği kaçınılmazdır.

Bu bağlamda, veri ile dijital delil arasındaki ilişkinin bir fonksiyon ilişkisi olduğunu, dijital delilin mutlaka dijital veri niteliğinde bulunması gerektiğini ve buna karşın sadece maddi olayla irtibatlı olan dijital verinin dijital delil olarak nitelendirilebileceğini söyleyebiliriz (Değirmenci 2020).

Veri ile bilgi, bilgi ile de delil arasında fark vardır. İlk olarak karşımıza veriler çıkar. Verilerin anlamlı bir şekilde sıralanması neticesinde ise bilgi elde edilir. Sonrasında soruşturmayı yürüten kişiler veya mahkeme tarafından yapılan inceleme ve değerlendirme ile delil kavramı ortaya çıkar (Zuev 2019).

Bu bağlamda dijital delillerin, soruşturma veya kovuşturma konusu suçla ilgisi olan ve suçun aydınlatılmasında kullanılan bilgiler olduğunu söyleyebiliriz. Dijital deliller çeşitli açılardan ele alınarak tanımlanmaya çalışılmıştır. Bir tanıma göre dijital delil, bir suçun nasıl meydana geldiğine dair bir teoriyi destekleyen veya çürüten veya kast veya mazeret gibi suçun kritik unsurlarını ele alan, bir bilgisayar kullanılarak saklanan veya aktarılan herhangi bir veri olarak tanımlanır. Bir başka tanım, dijital delili, herhangi bir elektronik cihaz aracılığıyla manipüle edilen, üretilen, depolanan veya iletilen potansiyel ispat değeri olarak tanımlamıştır (Jones *et al.* 2018).

Bir diğer tanım uyarınca dijital delil, ikili değer (binary) biçiminde saklanan, iletilen veya elde edilen delil niteliğindeki herhangi bir bilgidir.

Yargıtay'ın yapmış olduğu tanıma göre dijital deliller; "CD, DVD, flash bellek, disket, harici ve dahili harddisk, bilgisayar özelliği içeren noktaları bakımından akıllı telefon ve benzerlerinden elde edilen ve tamamı dijital delil olarak adlandırılan, suiistimale müsait olan veriler..." şeklinde tanımlanmıştır.

Bir başka tanım uyarınca dijital delil;

"iddia edilen bir fiilin ispatında kullanılmak istenen veya kullanılan; elektronik ortamda oluşan/oluşturulan, değiştirilen, iletilen veya saklanan veri, kayıt ve belgeleri" ifade etmektedir (Arslan 2015).

Bir diğer tanımda dijital delil;

"suç konusu fiille ilgili olarak yürütülen bir adli bilişim çalışması esnasında, bilişim sistemleri (bilgisayar, mobil telefon, dijital fotoğraf makineleri, dijital videolar, dijital faks makineleri vb.) ve bu kapsamdaki depolama aygıtları üzerinden elde edilen adli deliller" olarak ifade edilmiştir (Henkoğlu 2014).

Bir başka tanım uyarınca dijital deliller, dijital ortamda tutulan, oluşturulan, depolanan ve iletilen verilerdir. Söz konusu veriye delil değeri kazandıran şey, cezai uyuşmazlığa konu olan suç fiili ile olan ilgisidir (Değirmenci 2020). Elektronik ortamda muhafaza edilen bilgiler muhakeme konusu maddi olayla ilgili ve güvenilir olduğu hallerde delil olarak kabul edilecektir (Sarsıkoğlu 2015).

Bir diğer tanıma göre ise dijital deliller;

"bilişim teknolojisi içeren her türlü donanım, bu donanım üzerinde çalışan her türlü yazılım/yazılımlar tarafından kullanılan/üretilen her türlü veri ile bilişim teknolojisi tarafından kullanılan her türlü elektronik sinyali" ifade etmektedir (Öztürk 2007).

Avrupa Birliğine ait bir proje olan ve 7. Çerçeve Programının bir parçası olarak Avrupa Komisyonu tarafından finanse edilen bir proje olan *"Evidence"* projesinde elektronik delil ve dijital delil tanımına yer verilmiştir. Buna göre;

"elektronik delil herhangi bir elektronik cihaz kullanılarak oluşturulan, işlenen, saklanan veya iletilen, analog bir cihazın ve/veya potansiyel değere sahip dijital bir cihazın çıktısından kaynaklanan herhangi bir veridir. Üretilmiş veya sayısal bir formata dönüştürülmüş elektronik delil ise dijital delildir."

Dijital Delil Hakkında Bilimsel Çalışma Grubu *(The Scientific Working Group on Digital Evidence- SWGDE)*[1] dijital kanıtı, *ikili değer (binary)* biçiminde depolanan veya iletilen, delil değeri olan bilgi olarak tanımlamaktadır. Ancak bu tanım, dijital delillerin ikili değer biçiminde depolandığını yani yalnızca bilgisayarlardan elde edilebildiğini halbuki dijital delillerin diğer başka cihazlardan da elde edilebilmelerinin mümkün oluşu sebebiyle eleştirilmiştir.

Ulusal Polis Şefleri Konseyi *"(National Police Chiefs' Council- NPCC)"*[2] yapılan bir tanıma göre dijital delil, bir bilgisayarda depolanan veya bir bilgisayar tarafından iletilen ve araştırma değeri olan bilgi ve verilerdir.

Ulusal Adalet Enstitüsü ise ''Mahkemede dayanılabilecek ikili biçimde saklanan veya aktarılan bilgiler'' olarak dijital delillerin tanımını yapmaktadır.

Görüldüğü üzere ulusal ve yabancı kaynaklı olmak üzere dijital deliller çeşitli kişiler ve kurumlarca, çeşitli özelliklerine göre ve farklı açılardan birçok şekilde tanımlanmıştır. Tüm bu tanımlamalardan yola çıkarak bir tanım ortaya koyacak olursak dijital deliller; bir suçla bağlantısı olan, bilişim sistemleri bünyesinde ikili değer (binary) biçiminde üretilen, depolanan veya iletilen, uzman kişiler tarafından yürütülen bir adli bilişim faaliyeti neticesinde elde edilebilen, verilerdir.

Dijital delillerin niteliği

Dijital adli bilişimin başlangıcı, teknoloji içeren suçların ilk kez işlendiği 1970'li yıllara dayanmaktadır. Dijital adli tıp tarihi boyunca, önemli kişilerin çabaları ve çalışmalarının dijital adli bilimi bugünkü olgun bilimsel disipline dönüştürdüğü belirli dönemler olmuştur. İnsanlık ve endüstri tarihinin diğer biçimleri gibi, bugün bulunduğumuz

[1] 1992 yılında bir grup devlet temsilcisinin ortak çabası olarak oluşturulan kolluk kuvvetleri üyelerinden oluşan bir ABD örgütüdür ve ABD Gizli Servisi (USSS) ve Federal Soruşturma Bürosu'nun (FBI) ortak çabasıdır. Bkz. https://www.swgde.org/home , 06.04.2023

[2] Ulusal Polis Şefleri Konseyi, 2015 yılında, kendisinden önce var olan Polis Şefleri Birliği *(Association of Chief Police Officers- ACPO),* yerine kurulmuş bir İngiliz kurumudur. Ancak böyle bir değişiklikle birlikte günümüzde de hala ACPO tarafından getirilen kurallar ve tanımlamalar geçerliliğini büyük ölçüde korumaktadır.

noktaya giden yolu hazırlayan, daha önce meydana gelen olayları öğrenmek bu konunun uzmanları için yararlıdır (Sachowski 2018).

Dijital delil, çıplak gözle görülemeyen soyut verilerden oluşmaktadır. Analog ya da fiziksel delillerden farklı olarak bu delilin varlığını anlamak için yardımcı cihazlar ve yazılımlar bulunmaktadır. Örneğin bir metin belgesindeki bilgileri görmek için yazıcıdan yazdırmak ya da ekranda görüntülemek gerekir. Bu tür görüntüleme ile dosyanın meta veri bilgilerini görmek mümkün değildir. Bu bağlamda dijital veriyi anlamlı hale getirmek için kullandığımız araçlar bize verinin sadece bir kısmı hakkında bilgi verebilmektedir. Dolayısıyla bu sonuçlar kendi başlarına delil değildir; delilin kendisi dijital formatın kendisidir. Duyularımızla algılayamadığımız ancak metafizik gibi kanıtlanabilir bir yapıda olmayan dijital kanıtlar, kağıt üzerindeki fiziksel kanıtlardan yapı olarak çok farklıdır. Bu delillere erişim ancak elektronik bazı yardımcılar ile mümkündür. Dijital delillerin özelliklerini listelemeden önce, dijital bilginin yapısal özelliklerini gözden geçirmekte yarar vardır. Bu nitelikler şu şekilde sıralanmaktadır (Değirmenci 2020);

- Dijital veriler kolayca kopyalanabilmekte ve çoğaltılabilmektedir.
- Dijital veriler manyetik alan, sıcaklık ve nem nedeniyle bozulabilmektedir.
- Dijital veriler işlenerek basit şekilde değiştirilebilmektedir.
- Dijital veriler geri alınamayacak biçimde silinebilmektedir.
- Dijital veriler başka gizli ya da şifrelenmiş bilgiler içerebilmektedir. Tüm dijital bilgiler delil olarak kabul edilmemektedir. Daha önce de belirtildiği gibi, bir gerçeği kanıtlamak için bu bilgileri kullanmak onu dijital delil haline getirmektedir. Ama bu tek başına yeterli değildir. Sayısal verilerin yukarıdaki niteliklerinden dolayı, onu manipüle etmek çok basittir. Sayısal verilerin sayısal delil sayılabilmesi için orijinal olduğunun ve üzerinde değişiklik yapılmamış olduğunun da gösterilmesi gerekmektedir. Yine delil olarak sayılan özelliklerin delil olarak kabul edilebilmesi için dijital verilerde de bulunması gerekmektedir (Topaloğlu vd 2014).

En iyi delil kuralı, bir davanın kanıtlanabilmesi için orijinal delilin mahkemede incelenmesi gerektiğini gerektirmektedir. Bu kuralın amacı, yanlış veya tahrif edilmiş belgelerin kararda dikkate alınmasını önlemektir. Doktrin, dijital delillerin parça parça kopyalanabilmesi nedeniyle aslını belirlemenin imkânsız olduğu gerçeğine dayanmaktadır (Değirmenci 2020).

Dijital delillerde bulunması gereken özelliklerden bazılarını şu biçimde sıralamak mümkündür:

i. Makul ve kabul edilebilir olmalıdır.

ii. Orijinal olmalıdır.
iii. Hatasız ve kesin olmalıdır.
iv. Eksiksiz ve kusursuz olmalıdır.
v. İtimat edilebilir ve güvenilir olmalıdır.
vi. Güvenilir (ikna edici) olmalıdır.
vii. Tekrarlanabilir olmalıdır.
viii. Yürürlükteki yasalara uyulmalıdır.

Dijital delil kullanım alanları

Dijital delil, mahkemede delil olarak kabul edilebilecek ikili formatta saklanabilen ya da iletilen bilgidir. Diğer fiziksel olay mahalli ile karşılaştırıldığında bu delil daha çok bilgisayar, tablet ve telefon gibi dijital araçların hafıza cihazlarında bulunmaktadır. Suçların çözümünde ve davaların hazırlanmasında hayati bir rol oynamaktadır. Bununla birlikte, bilgisayarlardan, cep telefonlarından ve diğer cihazlardan elde edilen delillerin karmaşıklığı ve çeşitliliği, kolluk kuvvetleri müfettişlerini genellikle şaşırtabilmektedir (Novak 2021). Dijital görüntüleme yalnız elektronik suçlarda değil, her türlü suçun soruşturulması ve kovuşturulmasında da kullanılabilmektedir. Örneğin, bir şüpheliden alınan e-posta ya da cep telefonu dosyaları, şüphelilerin niyetlerini, suç sırasındaki konumlarını ve başkalarıyla olan fiziksel ilişkilerini ortaya çıkarabilmektedir (Whitcomb 2002).

Dijital delil kaynakları ve veri güvenliği gereksinimleri

Geleneksel olarak dijital kanıtlar öncelikle masaüstü bilgisayarlar, dizüstü bilgisayarlar ve sunucular gibi bilgisayar sistemlerinden toplanmaktadır. Ancak gerçek şu ki, dijital kanıtlar birçok farklı teknolojide yapılandırılmış veya yapılandırılmamış dijital veri biçiminde mevcuttur. Bu ağlar, çıkarılabilir aygıtlar gibi geleneksel bilgisayar sistemleri, mobil cihazlar ve bulut bilişim ortamlarını kapsamaktadır.

Teknolojinin ticari operasyonlarda yaygın olarak kullanılmasıyla birlikte her kuruluş, birçok farklı kaynaktan üretilen potansiyel dijital delil olarak kabul edilen dijital veriye sahip olacaktır. Bu nedenle, potansiyel dijital kanıtların veri kaynaklarını belirlerken dikkatli bir şekilde düşünülmesi gerekmektedir.

Dijital delil elde edilirken delilin nerede bulunma ihtimalinin olduğu, bu bilgiyi işleyen ve saklayan etkenlerin neler olduğu, nasıl işlendiği, saklandığı ve iletildiğinin bilinmesinin önemli olduğu ifade edilebilir. Sayısal gösterim, elektronik ortamın bulunduğu bilişim sisteminde ve bu sistemle beraber kullanılan cihazlarla gerçekleşmektedir. İletim söz

konusu olduğunda, delil bazen iletim cihazlarının kendileri tarafından üretilen veriler, bazen de iletilen veriler olabilmektedir (Orta 2015).

Dijital deliller bilgisayar kütükleri, sabit veya harici diskler, taşınabilir bellekler vb yerlerde olabileceği gibi, Log dosyalarında bulunan Erişim günlükleri, denetim günlükleri, harici günlükler, altyapı günlükleri, kaynak IP adresi, etkinlik zaman damgası, etkinlik türü gibi ilk anda bakılması akla gelmeyen ancak suç konusu olayla ilişkilendirilebilecek ve yeniden yapılandırmak için değerli bir veri kaynağı olması sebebiyle bu veri kaynaklarının da dikkatle incelenmesi önem arz etmektedir.

Dijital delil kaynakları, bir soruşturma veya hukuki süreçte kullanılan elektronik ortamda bulunan kanıtlardır. Bu kaynaklar genellikle dijital cihazlardan elde edilir ve çeşitli formatlarda olabilir. Peki dijital delil kaynakları nelerdir?

Birçok dijital delil kaynağı vardır. Bunlardan bazıları:

- Bilgisayar ve taşınabilir cihazlar
- İnternet ve sosyal medya
- Elektronik iletişim verileri
- Dijital fotoğraflar ve videolar
- GPS ve konum verileri
- Dijital imzalar ve meta veriler
- Bilgisayar ağları ve internet protokol bilgileri
- Bilgisayar programları ve yazılımlar
- Elektronik finansal işlemler

Bu dijital delil kaynakları, adli bilişim uzmanları tarafından toplanmalı, güvenilir bir şekilde saklanmalı ve analiz edilmelidir. Dijital deliller genellikle mahkemelerde hukuki süreçlerde kullanılmaktadır ve bu nedenle toplama ve işleme süreçleri özenle yürütülmelidir.

Dijital verilerin dijital kanıt olarak saklanması ve muhafaza edilmesi, verilerin elde edilmesi kadar önem arz etmektedir. Veri güvenlik kontrolleri uygulanmayan dijital verilerin delil niteliği kazanması mümkün değildir. Dijital verilerin veri güvenlik gereksinimlerinin sağlanması, verilerin korunması, özgünlük ve bütünlük de dahil olmak üzere yasal olarak kabul edilebilirliğini sürdürmesini sağlamaktadır.

Dijital kanıtların kullanımını sağlamanın en iyi yollarından biri, onu kolay erişilebilir bir formata dönüştürmektir. Dijital ses ve video kayıtlarının nispeten büyük dosya boyutları nedeniyle saklanması özellikle zahmetli olabilir. Ayrıca, uzun kayıtlar her zaman en etkili referans araçları anlamına gelmez. Örneğin, 6 saatlik bir video kaydında belirli bir anı

saptamaya çalışmak, hukuk veya soruşturma ekibinin bir üyesi için son derece zaman alıcı olacaktır.

Yapay zeka, kullanıcıların bir zamanlar saatlerce insan emeği gerektiren süreçleri otomatikleştirmesine olanak tanıdığı için birçok farklı sektörde giderek daha değerli bir araç haline geldi. Yapay zekanın hukuk teknolojisindeki rolü de farklı değil. Hukuk uzmanları, veritabanlarını düzenlemek ve dijital kanıtları daha iyi takip etmek için yapay zekâ destekli transkripsiyon hizmetlerini kullanabilir. Ancak profesyonellerin nihai transkriptlerin yeterince doğru ve erişilebilir olmasını sağlamak için gerekli adımları atması gerekir.

Veri güvenliği gereksinimlerinin sağlanması için, yasal mevzuata uygunluk konusunda titizlik ve dikkat, veri güvenliğine karşı tehditlerin farkındalığı, veri güvenliği risklerinin tanımlanması ve dijital delillerin korunmasının değerini göz önünde bulundurmak gerekmektedir. Dijital veriler gizlilik, bütünlük, kullanılabilirlik, süreklilik, kimlik doğrulama, yetkilendirme, inkâr edilemezlik, tanılama gibi ilkeler gibi veri güvenliği gereksinimleri karşıladığı müddetçe hukuk sistemlerinde dijital delil olarak ele alınabilecektir.

MATERYAL VE METOT

Çalışmamızın bu bölümünde, bilişim sistemleri üzerinden işlenen suçların soruşturulmasın da başvurulan adli bilişim uygulamaları ve ortaya çıkarılan dijital delillerle ilgili olarak son güncel veriler ve cihazlar, yasal prosedürler ve adli bilişimin uygulanma sürecinde kullanılan metotlar açıklanmaya çalışılacaktır. Dijital delillerin ele geçirileceği bilişim sistemlerinden kısaca bahsedildikten sonra, adli bilişim uzmanı tarafından delil çıkartma aşamasında kullanılan adli ve soruşturma açısından, delillin kabul edilebilirliği, gerçekliği ve manipülasyona uğramadığının göstergesi olan yazma koruma ekipmanları, hash bilgisinden bahsedilecektir. Adli bilişim uygulamalarının en önemli evresi olan imaj alma işlemi, adli bilişim yazılımı olan FTK uygulaması ile nasıl yapılacağı aşamalarıyla birlikte kısaca gösterilecektir. Bu bölümde deneysel bir uygulama yapılmamış, literatür taraması yapılarak 2024 yılına kadar ki teknolojik veriler ve yasal prosedürlerden faydalanılmıştır.

Bilgisayar Sistemleri

Dijital delillerin var olduğu en eski teknoloji, bilgisayar gibi geleneksel bilgi işlem sistemleridir. Onlarca yıldır süregelen teknolojik gelişmeler çerçevesinde oluşturulan sistemler, dijital delillerin çeşitli varyasyonlar da bulunabildiğini göstermiştir.

Bilgisayar sistemleri günümüzde ticari, kurumsal ve kişisel kullanım gibi birçok alanda önemli bir yer tutmaktadır. Günlük hayatta hemen hemen her türlü iş ve eylemleri bilgisayar sistemleri üzerinden gerçekleştirmekteyiz. Teknolojinin gelişimi göz önünde bulundurulduğunda bilgisayar sistemlerinin kullanım alanları daha da artmakta bu da suça maruz kalma riskini, bilgisayar sistemleri üzerinde suç işlenme olasılığını arttırmaktadır. Bu durum bilgisayar sistemleri üzerinde dijital delil incelemesi yani bilgisayar adli bilişimin önemini göz önüne sermektedir.

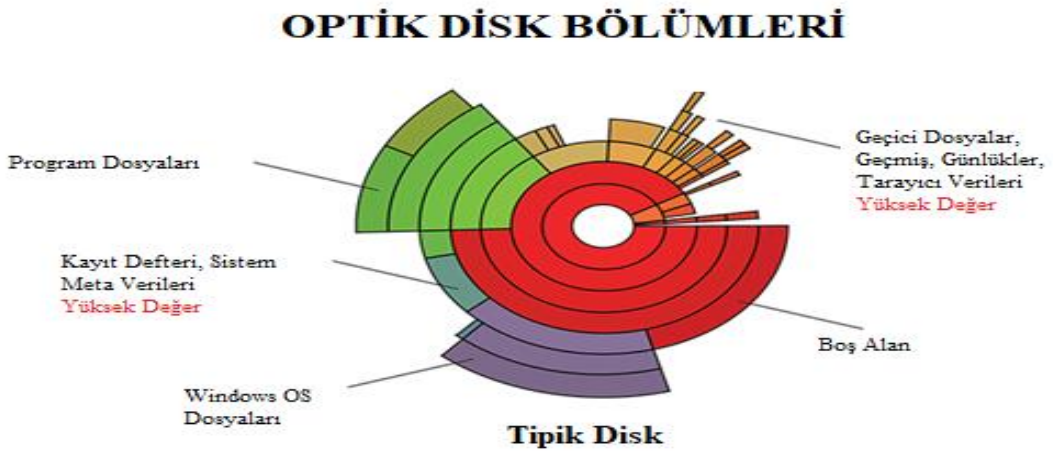
Bilgisayar sistemlerinde yaratılmış birçok farklı dijital veri vardır. Arka plan verileri, RAM bilgileri, parolalar, çalışan işlemler, önbellekler, güvenlik, sistem veya erişim olaylarının kayıtlarını tutan olay günlüğü dosyaları, ana bilgisayar işletim sistemi gibi daha birçok bilgisayar sistemini oluşturan unsurlar dijital delil olarak kullanılmaktadır.

Bilgisayar sistemleri ve bileşenleri sayısal delil elde etmek için kullanılmakta olan en önemli kaynaklardan biridir. Belgeler, fotoğraflar, e-postalar, veri tabanları, finansal bilgiler,

sohbet günlükleri, ağ bağlantı günlükleri ve sistem olay günlükleri, bilgisayar sistemleri aracılığıyla elde edilebilecek olası ipuçlarından bazılarıdır (Henkoğlu 2011).

Veri depolama aygıtları

Veri depolama, devam eden veya gelecekteki işlemler için dijital bilgileri kaydeden ve koruyan manyetik, optik veya mekanik medyayı ifade eder. İki tür dijital bilgi vardır: giriş ve çıkış verileri. Bilgisayar çağının başlarında bu verileri sürekli manuel olarak girmenin dezavantajlarına kısa vadeli çözüm olarak RAM ve ROM bilgisayar bellekleri bulunmuşsa da bu belleklerin hafıza kapasitesi ve teknik özellikleri veri kaybına ve iş yüküne çare olamamıştır. Bu duruma çözüm veri depolama aygıtları olarak bulunmuştur. Veri depolama alanıyla kullanıcılar verileri bir cihaza kaydedebilir. Sayısal bilgilerin kalıcı ya da geçici olarak saklandığı birimlere veri depolama cihazları denmektedir. Kullanım amacına göre değişik biçim ve boyutlarda olabilmektedirler. Bu maddelere örnek olarak; sabit sürücüler, taşınabilir sabit sürücüler, ağ sürücüleri, flash sürücüler, hafıza kartları, optik diskler (CD/DVD), disketler, veri bantları, akıllı kartlar, SIM kart, veri kayıt cihazları gösterilebilir. Bu cihazlar dijital delil toplamanın en önemli kaynakları olup, bulguları soruşturma ve kovuşturma aşamasındaki her adımda (olay yeri inceleme ve raporlama) kullanılmaktadır (Henkoğlu 2011).



Şekil 2. Tipik optik disk

Ayrıca günümüz kuruluşları ve kullanıcıları, büyük veri projeleri, yapay zekâ, makine öğrenimi ve nesnelerin interneti gibi yüksek bilişimsel ihtiyaçlarını karşılamak için veri depolamaya ihtiyaç duymaktadır. Bir diğer veri depolamaya ihtiyaç duyulma nedeni ise; doğal afet, arıza ve siber saldırılar nedeniyle veri kaybına karşı koruma sağlamaktır.

Veri depolama cihazları iki ana kategoriye ayrılır: Doğrudan Alan Depolama ve Ağ Tabanlı Depolama. Doğrudan alan depolama aygıtları disketler, optik diskler, DVD, HDD

gibi doğrudan bilgisayara bağlanan aygıtları, Ağ tabanlı depolama aygıtları ise ağ üzerinden depolama sağlayan bulut depolama aygıtlarıdır.

Sabit disk

Bunlar elektronik bilgileri depolamak için kullanılmakta olan manyetik ortamlardır. Sabit sürücülerdeki veriler; yüzeyi demir oksit veya farklı manyetik özelliklere sahip bir malzeme ile kaplı disklerin üzerine yazılmaktadır. Veriler mıknatıslanma ile saklandığından, örneğin bir elektrik kesintisi sırasında kaybolmaz ve kullanıcı silene kadar kalıcı saklanmaktadır (Şekil 3).



Şekil 3. Sabit disk

Taşınabilir disk

Bilgisayar kasasının içeriğinin dışında bulunur ve bilgisayara USB veya benzeri bir yolla bağlanır yöntemleri sağlayan taşınabilir bir veri depolama aygıtıdır (Şekil 4).



Şekil 4. Taşınabilir disk

USB bellek

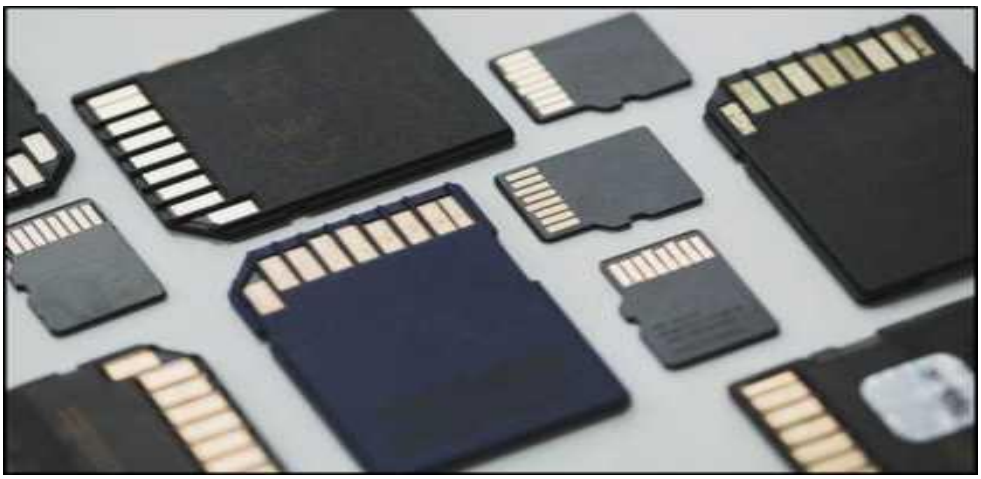
USB bellek, elektriksel olarak silinebilen ve yeniden programlanabilen, elektronik, kalıcı bir bilgisayar belleği depolama ortamıdır. USB bellek bilgisayarlarda, PDA'larda, dijital ses oynatıcılarında, dijital kameralarda, cep telefonlarında, sentezleyicilerde, video oyunlarında, bilimsel cihazlarda, endüstriyel robotiklerde ve tıbbi elektroniklerde kullanılır. USB belleğin okuma erişim süresi hızlıdır ancak statik RAM veya ROM kadar hızlı değildir. Taşınabilir cihazlarda, mekanik sürücülerin mekanik hasara daha yatkın ve darbelere karşı dayanaklılığı nedeniyle USB bellek kullanılması tercih edilir (Şekil 5).



Şekil 5. USB bellek.

Hafıza kartı

"Memory stick" olarak da bilinmekte olan hafıza kartları, elektrik olmadığında bile veri depolayabilen veri depolama cihazlarıdır. Bellek kartı, dijital bilgileri depolamak için kullanılan, genellikle flash bellek kullanan bir elektronik veri depolama aygıtıdır. Bunlar, dijital kameralar gibi dijital taşınabilir elektronik cihazlarda ve ayrıca Nintendo Wii gibi ilk oyun konsollarında yaygın olarak kullanılır. Bu tür cihazlara, çıkıntılı USB flash sürücüler yerine yuvadaki bir kartı kullanarak bellek eklenmesine olanak sağlarlar. Yaygın flash bellek kartı türleri arasında SD kartlar (microSD dahil), Sony'nin Memory Stick'i ve CompactFlash bulunur. SD kartlar günümüzde en yaygın hafıza kartı türüdür (Şekil 6).



Şekil 6. Hafıza kartı

Bilgisayar Ağları

Bir bilgisayar ağı, iki ya da daha fazla bilgisayar sisteminin bilgi paylaşmak için kablolu ya da kablosuz olarak birbirine bağlanmasıyla oluşmaktadır (Şekil 7). Bu ağlardaki veriler bir bilgi akışıdır. Bu nedenle, bu verilerden kanıt elde etmek istiyorsanız, gerçek zamanlı analiz yapmanız gerekmektedir (Değirmenci 2014). Ağ üzerinde çalışan uygulamalara, hizmetlere veya kullanıcılara ek olarak, bilgisayar ağ sistemlerini görüntülemek ayrıca bazı ek kullanıcı bilgilerine (işletim sistemi, tarayıcı programı, bağlı diğer cihazların yazılım ve donanım bilgileri) erişim sağlamaktadır. Çevrimiçi analiz neticesinde elde edilen bilgiler şu şekildedir (Ercan ve Nacak 2009);

- Ağ yapısı ve altyapısı,
- Çeşitli çevrimiçi kaynaklara erişim modu,
- Diğer bağlı ağlara yetkisiz erişim,

Ayrıca bir bilgisayar ile bir ağ aygıtı arasında tanımlayıcı olan IP adresi ve MAC adresi gibi tanımlama bilgileri kullanılarak önemli sayısal deliller elde edilebilmektedir (Henkoğlu 2011).



Şekil 7. Bilgisayar ağları

Mobil Cihazlar

Telefon görüşmesi, anlık ileti, kişisel bilgi asistanı, medya ve oynatma gibi çeşitli fonksiyonları yerine getirebilen cihazlardır. Zaman içinde teknolojinin gelişmesiyle birlikte çok sayıda değişik işlevi bünyesine katmışlar ve insan hayatında vazgeçilmez cihazlar haline gelmişlerdir. Bu sebeple adli tıpta en yaygın sayısal delil kaynağı haline gelmiştir (Çakır ve Kılıç 2013).

Cep telefonu

Telefonlar, başlangıcından bu yana çok hızlı bir teknolojik gelişim geçirmiş ve uzaktaki insanlar arasındaki iletişim için kullanılmıştır. Günümüzde bilgisayarlarla aynı donanım özelliklerine sahip akıllı telefonlar, iletişimin yanı sıra internet erişimi, iş, eğlence, eğitim vb. amaçlar için de kullanılmaktadır (Karaaslan ve Budak 2012).

Akıllı telefon, geleneksel bir cep telefonunun işlevselliğini gelişmiş bilgi işlem yetenekleriyle birleştiren mobil bir cihazdır. Genellikle kullanıcıların web'de gezinme, e-posta ve sosyal medyanın yanı sıra multimedya oynatma ve akış gibi çok çeşitli uygulama ve hizmetlere erişmesine olanak tanıyan bir dokunmatik ekran arayüzüne sahiptir. Akıllı telefonlarda yerleşik kameralar, GPS navigasyonu ve sesli aramalar, kısa mesajlar ve internet tabanlı mesajlaşma uygulamaları dahil olmak üzere çeşitli iletişim yöntemleri desteği bulunur. Akıllı telefonlar, daha gelişmiş donanım yetenekleri ve kapsamlı mobil işletim sistemleri, internete erişim, iş uygulamaları, mobil ödemeler ve müzik, video, oyun, radyo ve televizyon dahil olmak üzere multimedya işlevleriyle eski tasarım özellikli telefonlardan ayrılır (Şekil 8).



Şekil 8. Cep telefonu

Tablet

Kablosuz iletişime sahip, dokunmatik ekranlı ve fiziksel klavyesi olmayan mobil cihazlardır. Akıllı telefonlarla aynı işlevlere sahip olmalarına rağmen ekranları daha büyüktür (Orta 2015) (Şekil 9).



Şekil 9. Tablet

Gömülü sistemler

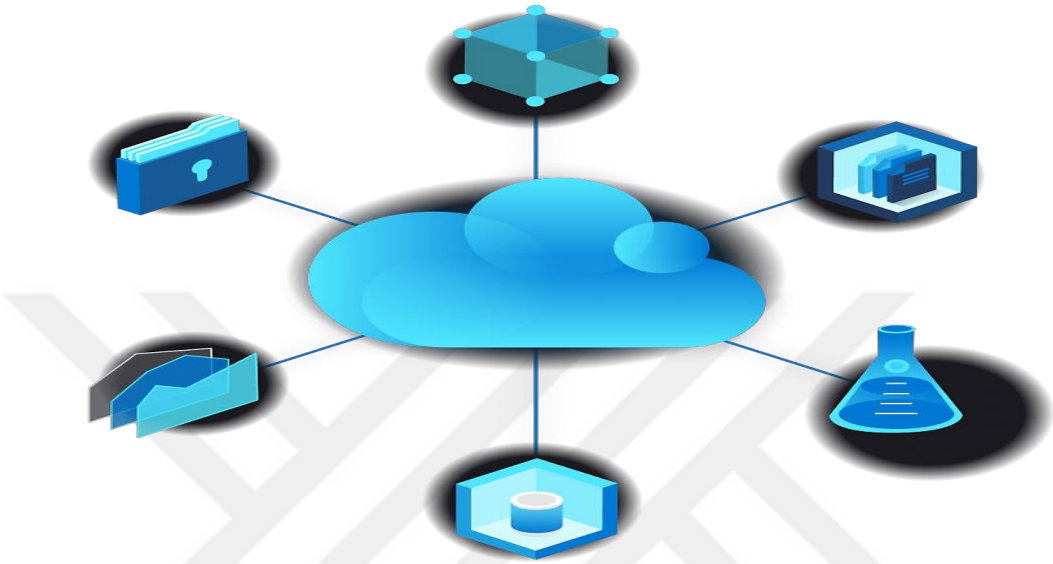
Herhangi bir basit sisteme akıllılık özelliği getiren bir elektronik donanım ve yazılım varlığını tanımlamaktadır. Bilgisayarlar için nispeten sınırlı bir kullanıcı ara yüzü ile bu sistemler tek bir işi yapmak ve tam da onu yapmak için tasarlanmıştır. Gömülü sistemlere örnek olarak oyun konsolları, MP3 oynatıcılar, faks makineleri, yazıcılar, tarayıcılar ve GPS cihazları verilebilir (Şekil 10).



Şekil 10. Gömülü sistemler

Bulut sistemler

Son senelerde popüler duruma gelen bir teknoloji olan bulut teknolojisi, büyük miktarda verinin karmaşık bir sanallaştırılmış platform üstünde depolanmasına olanak sağlayan sistemlerdir (Şekil 11). Burada kullanıcı, veri ağı üzerinden ihtiyaç duyduğu yazılım ve donanım hizmetlerini, hizmet sağlayıcının kiralama yoluyla sağladığı paylaşımlı altyapıyı, altyapı yatırım maliyeti olmadan kullanabilmektedir.



Şekil 11. Bulut sistemler

Bulut teknolojisinin ve uygulama alanlarının hızla büyümesi bu sistemleri suçlular ve suç örgütleri için cazip hale getirmiştir. İnternet kullanımlarının artması ve hızlı erişim seçenekleri, kullanıcının herhangi bir çevrimiçi kaynağa herhangi bir bilgisayardan, tabletten veya akıllı telefondan erişmesine izin vermektedir. Bu durum bulut hizmetlerini özellikle siber suçlar ve klasik suç türleri için sağladığı depolama alanı için uygun yeni bir alan haline getirmiştir (Emekçi vd 2016). Ancak bulut sistemlerinin sanal ortamda dağıtık bilgi işlem modeli, dinamik altyapı topolojisi, veri merkezlerinin farklı ülkelerde yer alması ve içindeki kaynağın çok sayıda kullanıcı tarafından kullanılması gibi niteliklerinden dolayı ülkemizde de araştırmalar yapılmıştır. Ancak bulut sistemler daha karmaşık bir prosedürdür. Geleneksel adli tıp teknikleri, bulut bilişim ortamlarında karşılaşılan sorunları tam olarak çözemediği için; yeni bir bakış açısı getirmek için adli bilişim araştırmaları yapılmalıdır (Kaya 2016).

Dijital Delil İnceleme ve Analiz Yöntemleri

Dijital adli tıp, son 50 yılda önemli ilerlemeler kaydederek bugünkü olgun bilimsel disipline ulaşmıştır. Geleceği tahmin etmek kumarbazın oyunudur; ancak tarihin bize öğrettiği bir şey varsa o da teknoloji ve dijital adli bilimin birbirine paralel olarak gelişmeye devam edeceğidir. Kesin olan bir şey varsa o da dijital adli bilimin gelişmeye ve olgunlaşmaya

devam edeceğidir. Günün sonunda geleceğin uygulayıcıları daha iyi eğitimli olacaklar çünkü kendilerinden önce katkıda bulunan her bireyin onlarca yıllık bilgi birikimine sahiptirler. Öte yandan, gelecekteki teknolojik gelişmeler, dijital adli topluluğun ele alması gereken benzersiz zorlukları da beraberinde getirecektir. Dijital adli bilişimin geleceğinin nerede gelişeceğini gösteren iki örnek bulut ve kuantum bilişimdir (Sachowski 2018).

Adli bilişim uzmanları delil elde edebilmek amacıyla bilgi sistemlerini, medya cihazlarını, ağ cihazlarını, interneti ve kapalı ağ sistemlerini incelemektedir. Süreç boyunca, kullanılmakta olan ekipmanın aktif parçalarında, ayrıca çıkarılan parçalarda, atık alanlarında veya saklanma kısımlarında her zaman kanıt bulunmaktadır (Orta 2015). Bu alanların her birinde adli bilişim, delil bulabilmek ve elde etmek için çeşitli uygun metotlar kullanmaktadır. Bu şekilde elde edilen deliller yardımıyla suçun çözüleceği ve maddi gerçeğe ulaşılacağı varsayılabilmektedir. Dijital delillerin bozulmadan ve zarar görmeden bulunabileceği ortamların toplanması, korunması, soruşturulması ve nihayetinde yasal mercilere teslimi gibi faaliyetler ancak belirli teknik ilkeler dikkate alınarak yapılmalıdır (Ekizer 2014).

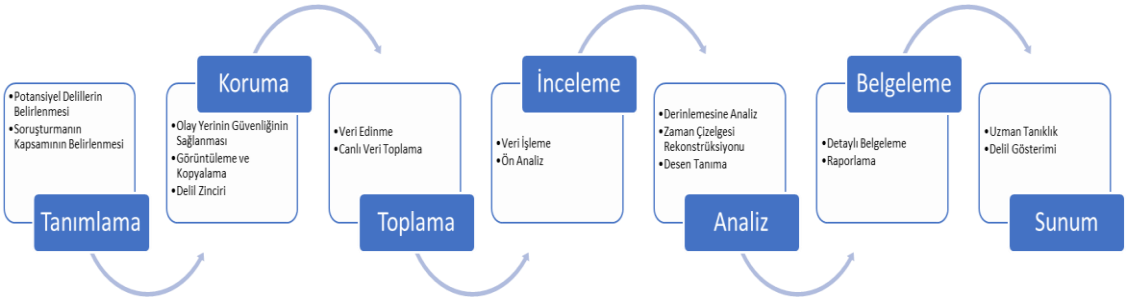
Adli tıp uzmanları, siber suçlara ilişkin kanıt bulmak ve kolluk kuvvetlerine sunmak için verileri toplar, analiz eder ve sunar. Bunların hepsi adli tıp uzmanları tarafından yapılsa da bilimsel gerçekleri göz ardı etmeleri beklenmez ve adli tıp yöntemlerini de izlemeleri gerekir (Orta 2015). Dijital delil inceleme safhasında, veri toplama aşamasında elde edilen bütün bilgilerden soruşturma olayı hakkında bilgi çıkarılmaktadır. Silinen ya da hasar gören verilerin kurtarılması, verilerin sınıflandırılması ve içerik araştırması ayrıntılı bir şekilde yapılmaktadır (Değirmenci 2014).

Elektronik bilginin delile dönüştürülmesi için donanım ve yazılımlara, bu donanım ve yazılımların etkin bir biçimde kullanılması için ise tecrübeli ve eğitimli iş gücüne ihtiyaç duyulmaktadır (Çakır ve Kılıç 2013). Adli bilişim ekipmanı ve yazılımı, teknolojinin ilerlemesiyle günümüzde çok gelişmiştir. Adli tıp uzmanları, silinen dosyaları kurtarmak ve alınan verileri daha doğru bir şekilde analiz etmek için bu donanımı ve yazılımı kullanır. Kullanılan donanım ve yazılımlar doğru, tekrarlanabilir ve tarafsız sonuçlar vermelidir (Orta 2015).

Dijital Delil İncelemede Kullanılan Ekipmanlar

Dijital delillerin araştırılmasında kullanılmakta olan ekipmanlar, adli bilişim sürecinde kullanılmakta olan araç ve gereçlerden meydana gelmektedir. Bu süreç, Şekil 12' de gösterilen aşamalardan oluşmakta ve ilk müdahale ile başlayan adımları içermektedir. Olay mahalline giderek inceleme ve tahliller neticesinde elde edilen sonuçları ilgili adli makama

sunmaktadır. Bu nedenle adli bilgi donanımı, bir tanım yapılacak olursa, "veri taşıyıcılarından delil elde etmek için kullanılan, bilgilerin sayısal bir saklama ortamında saklandığı ve işlendiği, yazılım, donanım veya bunların bir kombinasyonu ile diğer araç ve gereçler" olarak tanımlanabilir (Bakan ve Saluk 2014).



Şekil 12. Adli bilişim süreçleri

Tornavida takımları, bağlantı kabloları gibi aksesuarlardan, bireysel çoğaltma için kullanılmakta olan aparatlara ve araştırma safhasında kullanılmakta olan yazılımlara, hatta özel kutu ya da ambalajlara kadar bu cihazlarda kullanılan bütün araç ve gereçler yer alabilmektedir. Dijital delillerin toplanması, sınıflandırılması, paketlenmesi ve taşınmasında kullanılmakta olan araç ve gereçlerin güncel olması sağlanmalıdır. Teknoloji ilerledikçe kullanılan araç ve gereçler de gözden geçirilmeli ve güncellenmelidir (Berber 2004).

Adli bilişimde kullanılmakta olan cihazların belirli standartlara sahip olması ve test edilmiş olması konunun hassasiyetine göre büyük önem taşımaktadır. Türkiye'de TSE kuruluşu ile ilgili çalışmalar yapılmış olmasına rağmen, test cihazları için hala bir standart bulunmamaktadır. Amerika Birleşik Devletleri ele alındığında, Ulusal Standartlar ve Teknoloji Enstitüsü'nün "Adli Bilişim Aracı Testi" projesi kapsamında adli yazılım ve donanım testleri yapılmakta ve sonuçları web sitesinde yayınlanmaktadır (Bakan ve Saluk 2014).

Yazma koruma ekipmanları

Dijital delillerin adli analizinin başlangıcı, görüntü elde etme sürecidir. Bununla birlikte, ortamın zarar görmesi veya verilerin araştırmacı tarafından kasıtlı veya kasıtsız olarak değiştirilebileceği durumlarda, görüntü elde etme sürecinde yazma koruma cihazları kullanılmaktadır. Verilerin saklandığı ortam birimi bu cihazlar aracılığıyla bilgisayar sistemine bağlandığında bu ortama yazmadan sadece okuma gerçekleşir (Bakan ve Saluk 2014).

Yazmaya karşı koruma, disk veya hafıza kartı gibi bir depolama aygıtına veri yazılmasını veya değiştirilmesini önleyen bir özellik veya mekanizmadır. Saklanan bilgileri

salt okunur hale getirerek bütünlüğünü ve güvenliğini sağlar, kazara veya yetkisiz değişikliklere karşı korur.

Bir depolama aygıtının yazmaya karşı korumalı olması, içindeki verilerin değiştirilemeyeceği veya silinemeyeceği anlamına gelir. Cihaz, yazmaya karşı koruma özelliğini etkinleştirmek veya devre dışı bırakmak için fiziksel bir anahtar, bir yazılım ayarı veya her ikisinin bir kombinasyonunu kullanır. Yazmaya karşı koruma anahtarı etkinleştirildiğinde, yeni veri yazma veya mevcut verileri değiştirme girişimleri engellenerek, kasıtsız veya kötü niyetli değişiklikler önlenir.

Tüm adli bilimlerde olduğu gibi adli incelemelerde de delillerin değiştirilmemesi önemlidir. Bu ilkeye göre adli tıp uzmanları gerekli önlemleri almalı ve yazmaya karşı koruma cihazları kullanmalıdır. Yazmaya karşı koruma cihazları genellikle giriş, çıkış ve güç kaynağından oluşmaktadır. Kayıt veri deposu giriş kısmına bağlanır ve sabit disk veya bilgisayar çıkış kısmına bağlanmaktadır. Bir güç kaynağı ünitesi ise giriş ve çıkış bölümlerine bağlı cihazların kullanımına izin vermektedir. Yazmaya karşı korumalı aygıtlar için giriş modülleri çoğunlukla IDE, SATA veya SCSI tipinde olabilmektedir.

Çıkış aygıtı çoğunlukla USB veya Firewire tipindedir. Adli tıp uzmanı, incelenmekte olan veri depolama cihazının türü ile görüntünün çekildiği depolama cihazının türüne göre uygun bağlantıyı yapmalıdır (Say 2006).

Adli kopyalama sırasında donanımsız, yazılımsal yazma koruma metotları ile verinin hash değerini değiştirmeden kopyalama yapmak mümkündür. Yazılım çözümleri bunu BIOS'ta INT 13h kodunu devre dışı bırakarak yapar. Ancak BIOS sürücüleri devre dışı bırakılabildiği için yazılım yazmaya karşı koruma metotları önerilmemektedir (Bakan ve Saluk 2014).

Aşağıda, genel özellikleriyle birlikte yazma koruması donanım ve yazılım örnekleri verilmiştir. Tablo yazma koruma cihazları; Amerika Birleşik Devletleri'nde kurulmuş bir şirket olan Guidance Software'in ticari markasıdır. 1997 senesinde kurulan Guidance Software, e-keşif, bilgi alma ve adli bilgi işlem alanlarını kullanarak dünya çapında adli tıp hizmetleri sağlayan kolluk kuvvetlerine, özel şirketlere ve çok çeşitli özel kuruluşlara yazılım ve donanım çözümleri sunmaktadır. Birkaç model vardır (EMT Electronics 2018). Tableau T35u, IDE/SATA sabit diskler için, yazmaya karşı korumalı bir USB 3.0 arabirimi kullanarak yüksek hızlı veri aktarımını garanti edebilen, yazmaya karşı korumalı bir kit modelidir. Şekil 13. T35u modeline genel bir bakışı göstermektedir. Model taşınabilir bir modeldir.



Şekil 13. Tableau T35u yazma koruma köprü kiti

Tableau T6u SAS serisi yazmaya karşı korumalı köprüler, SAS depolama aygıtlarından yüksek hızlı veri aktarımı için özel olarak tasarlanmıştır. Tableau T6es modelinin yerini almıştır. Saniyede 200 MB veri aktarabilmektedir (Opentext 2018).



Şekil 14. Tableau T6u yazma koruma köprü kiti SAS disk bağlantısı

Tableau model T356789iu, iş istasyonu tipi bilgisayarlar için OEM tarafından üretilmiş bir yazmaya karşı koruma aygıtıdır. "IDE, SATA, SAS, USB 3.0/2.0/1.1 ve FireWire 800/400" gibi birçok bağlantıya izin vermektedir. T35689iu modelinin yerini almıştır. Bilgisayara USB 3.0 bağlantısı ile bağlanmaktadır (EMT Electronics 2018).



Şekil 15. Tableau T35689iu Forensic SATA/IDE Bridge modeli

WiebeTech yazmaya karşı koruma cihazları; Amerikan CRU firmasının çeşitli modelleri bulunan bir markasıdır. Forensic UltraDock v5.5 modeli, "PATA/IDE ve SATA sürücüleri" destekler ve ayrıca değişik sürücü modelleri için adaptör desteği sağlamaktadır. Ekranı, bağlı disk hakkında bilgi göstermektedir. HPA ve DCO alanları kullanılabilir ve bağlantılı pano üzerinde değişiklik yapılabilmektedir. "USB 3.0/2.0, eSATA, FireWire 400/800 bağlantıları" ile bir bilgisayara bağlanabilmektedir.



Şekil 16. CRU WiebeTech Forensic UltraDock v.5.5 modeli

SAFE Blok Yazma Koruması yazılımı; Amerika Birleşik Devletleri'ndeki ForensicSoft şirketi tarafından geliştirilmiştir. Windows tabanlı yazma koruması yazılımı, "IDE (PATA ve SATA), SCSI, FC, SAS, USB ve IEEE1394 aracılığıyla" bilgisayara bağlı herhangi bir ortama yazmaya karşı koruma sağlayabilmektedir. Tüm Windows tabanlı görüntü alma programları ile uyumludur. Yazma koruması aynı anda istenildiği kadar depolama biriminde gerçekleştirilebilmektedir (ForensicSoft 2016).



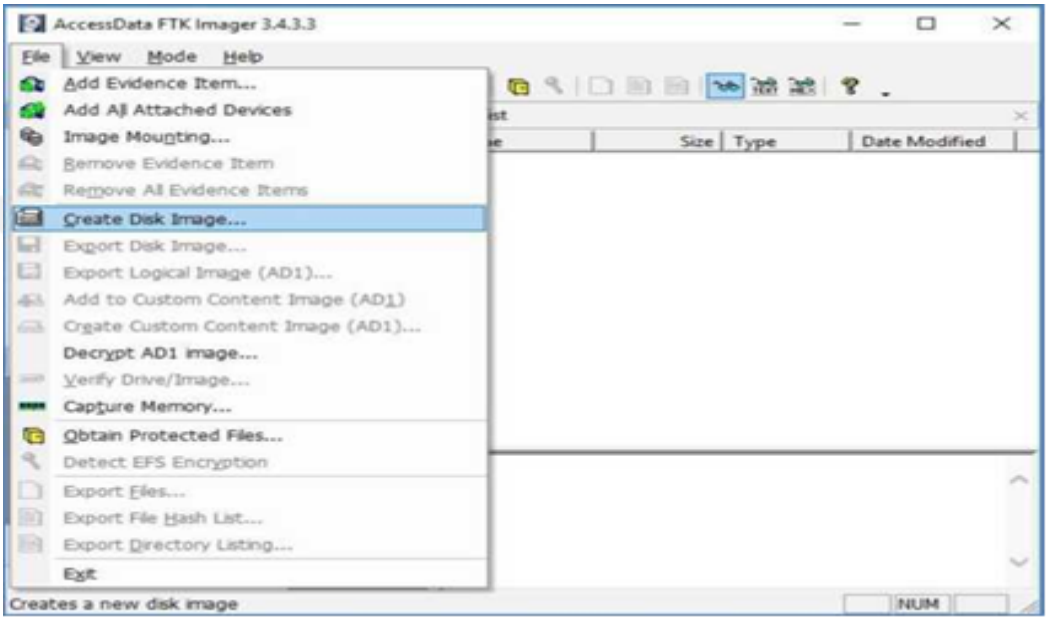
Şekil 17. SAFE Block yazma koruma yazılımı

Windows XP SP2'den başlayarak, kayıt defteri ayarlarında USB yazma koruması etkinleştirmiştir. Ayrıca, bazı USB belleklerde ve SD kartlarda "Kilitle" düğmesi gibi yazmaya karşı koruma düğmeleri bulunmaktadır. Bu butonlar ile yazma koruması da yapılabilmektedir. Ancak adli bilişimde kullanılan donanımlarda okuma koruma cihazlarının kullanılması daha güvenilir bir yoldur (Bakan ve Saluk 2014).

Disk imajı alma işlemi

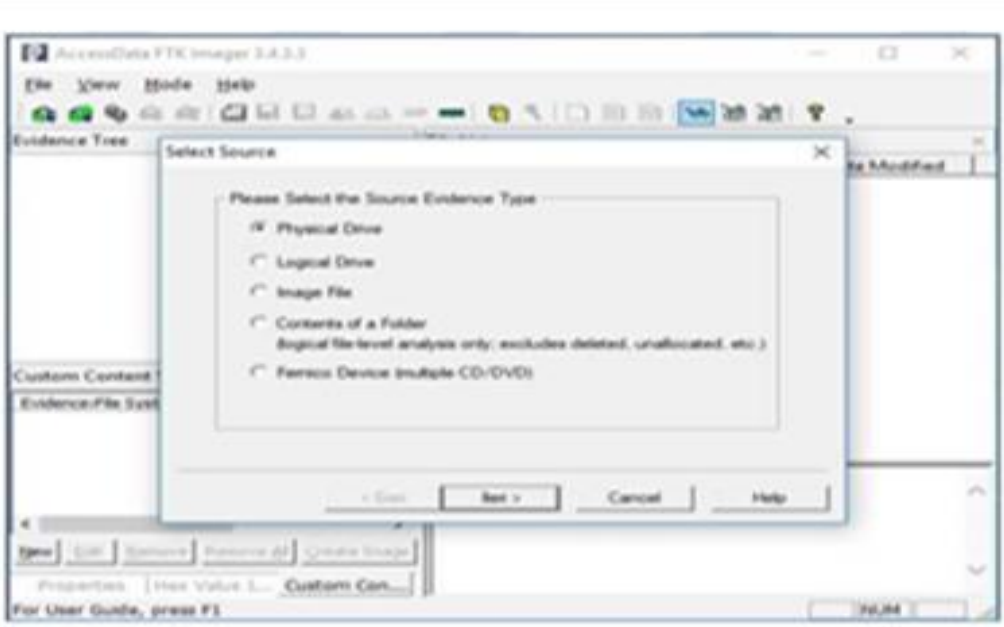
İmaj alma, "orijinal ortamda yer alan bütün verilerin kısmen yeni bir ortama kopyalanması" olarak açıklanmaktadır. Bir disk görüntüsünün alınması, dijital kanıt adli analiz sürecinin başlangıcıdır. İmaj görüntüsünün doğru olması bütün hukuki süreci etkileyecek mühim bir konudur (Henkoğlu 2011). İmaj işlemi neticesinde elde edilen kopyaya "adli kopya" adı verilmektedir. İmaj alma işlemi bu işlem için tasarlanmış donanımlar veya özel yazılımlar ile yapılabilmektedir. Ancak donanım tabanlı sistemlerin kullanılması daha güvenilir olduğu için tercih edilmektedir (Kiceci 2014). Görüntülerin genel kabul görmüş adli tıp standartlarına göre medya tarafından edinilmesi, dijital kanıtların elde edilmesi ve analizi ve sürecin uygun şekilde başlatılması ve sonlandırılması ile yakından ilgilidir. Bu sürecin doğru işlemesi, dijital delillerin mahkemede özelliklerini gölgeleyemeyecek biçimde sunulmasını ve doğru karar verilmesini etkilemektedir (Henkoğlu 2011). Ancak bilginin alındığı kaynak ile imaj olarak alınan kopyanın aynı olduğunun teyidi beklenmektedir. Bu nedenle, hazır bulunan taraflar, yakalanan tüm elektronik verilerin hash değerlerini almalı ve imzalamalıdır. Bu süreç sonraki itirazları engellemektedir (Orta 2015). Disk görüntüsü oluşturmanın iki yolu vardır: diskten diske ya da diskten dosyaya. Diskten diske imaj aramada, kaynak disk tamamen hedef diske kopyalanırken, diskten dosyaya kopyalamada kaynak disk görüntüsü mantıksal bir veri dosyasına kopyalanmaktadır. Kopyalanan görüntü farklı biçimlerde olabilmektedir. Genel olarak bu formatları bit copy ve bit copy plus olarak

ikiye ayrılabilmektedir. Bitmap biçimi ham bir biçimdir ve bu görüntü dosyası yalnızca disk görüntüsünü içermektedir. Bu format, tüm yazılım programlarının tanıdığı formattır. Ancak, bu formatta ek bilgi yoktur. Bit-copy-plus formatı ise görüntü işleme ile ilgili metadataların oluşturulduğu bir formattır (Kiceci 2014). Aşağıda, üreticinin AccessData web sitesinden ücretsiz olarak indirilebilen global FTK Imager sürüm 3.4.3.3'ün kullanıldığı adli veri toplama sürecinin adımları yer almaktadır. 1. Uygulama yönetici olarak çalışır. "File" menüsünden "Create Disk Image" seçerek disk imajı oluşturma işlemine devam edilmektedir (Şekil 18).



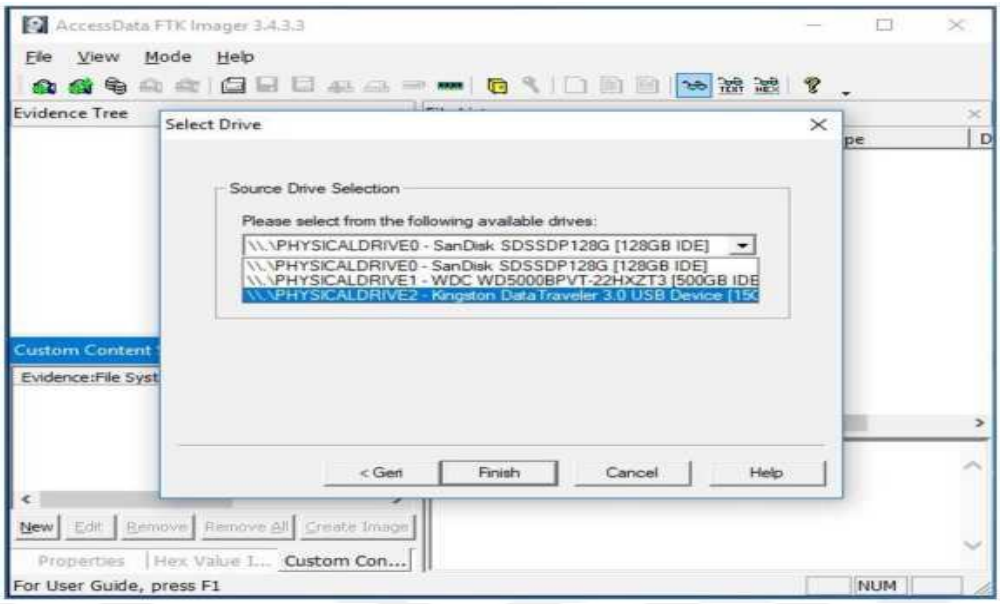
Şekil 18. FTK Imager disk imajı alma aşama 1

Gelen pencereden Physical Drive seçeneği seçilir (Şekil 19).



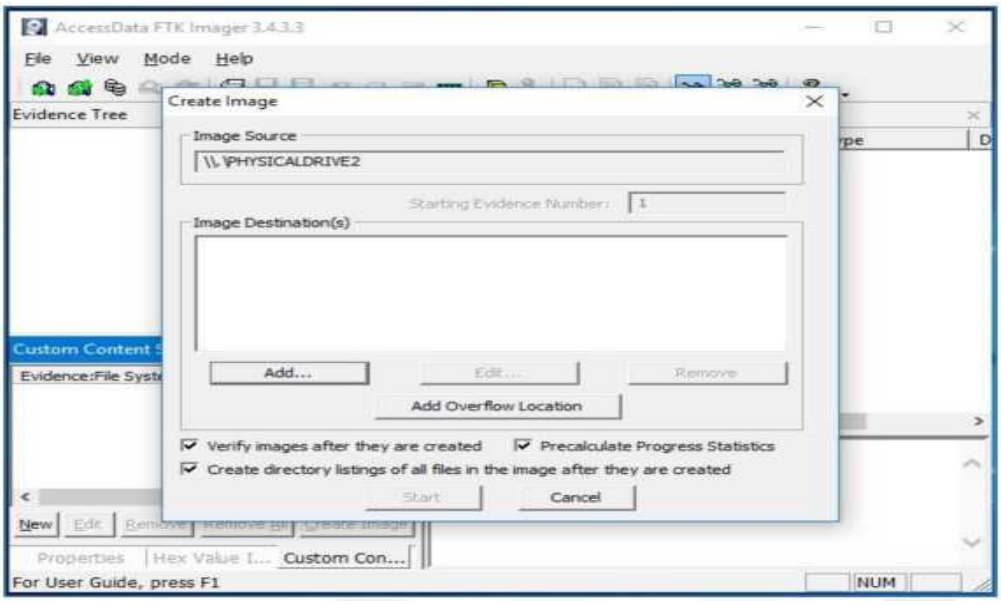
Şekil 19. FTK Imager disk imajı alma aşama 2

Gelen pencerede hangi diskin imajı alınacaksa o disk seçilir (Şekil 20).



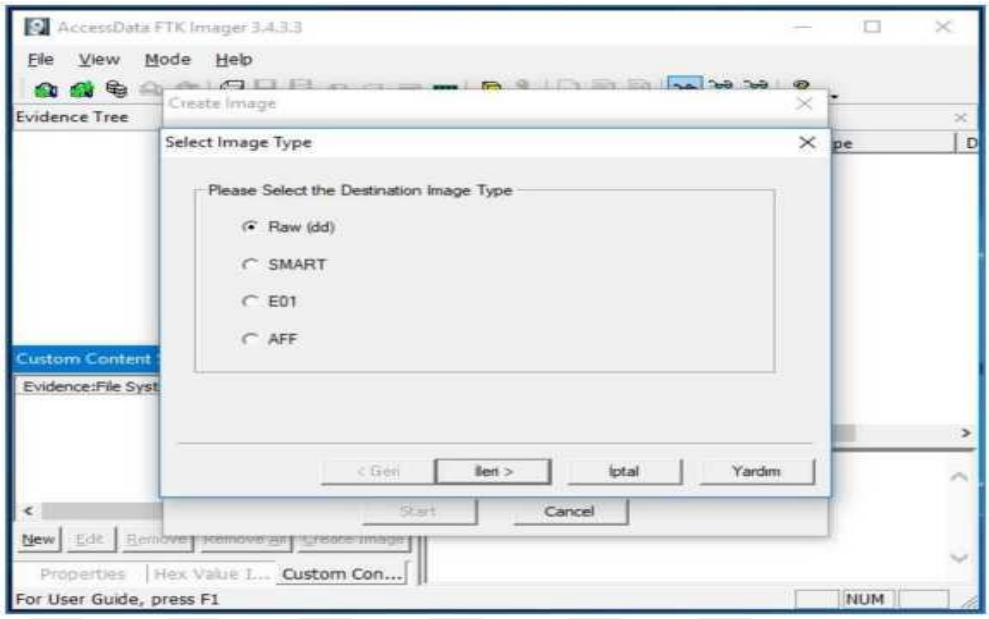
Şekil 20. FTK Imager disk imajı alma aşama 3

Açılan pencerede, kaydedilen görüntünün nereye kaydedileceğini belirtilir. Burada "imajı oluşturduktan sonra doğrula" seçilirse, imaj oluşturulduktan sonra doğrulama işlemi gerçekleştirilir. Yakalama işlemi, bir imajın yakalanması için geçen süreyi artıran bir işlemdir. "Ön İlerleme İstatistikleri" seçilirse, gerçekleştirilen faaliyetlerin yaklaşık süresi hesaplanacaktır. "Oluşturduktan sonra tüm görüntü dosyaları için klasör oluştur" seçeneği seçilirse, görüntülenen diskin dosya bilgileri görüntünün kaydedildiği konuma aktarılacak ve kaydedilecektir. İstenilen seçenekler gerçekleştirildikten sonra "Ekle" butonuna tıklayarak oluşturulan imaj dosyasının formatını belirtebileceğimiz bir sonraki pencereye geçilmektedir (Şekil 21).



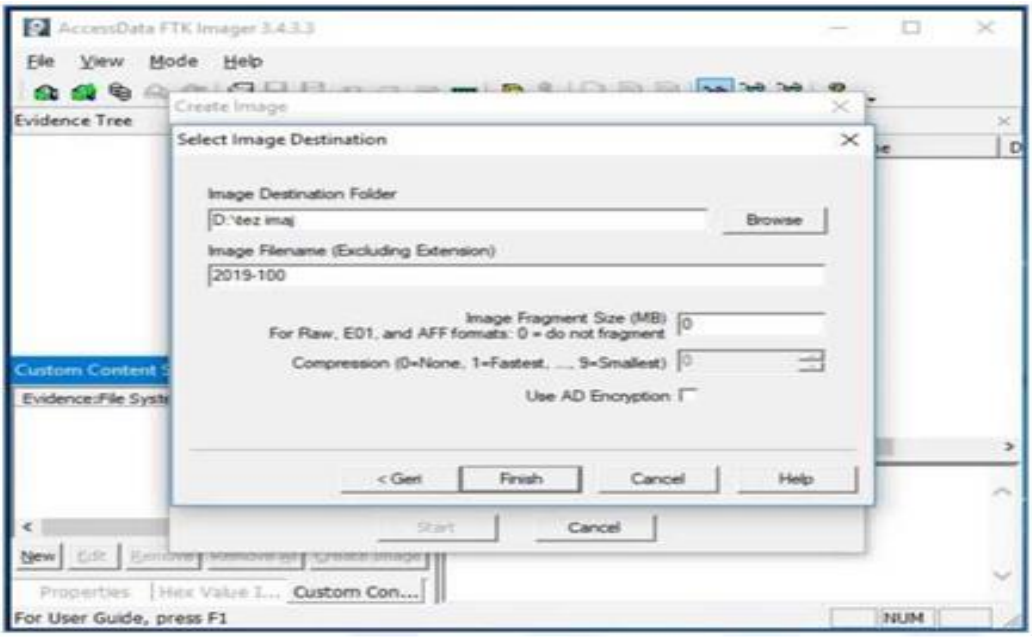
Şekil 21. FTK Imager disk imajı alma aşama 4

FTK Imager yazılımı ile 4 farklı formatta disk imajı oluşturabiliyoruz. Bunlar Raw (dd) formatı", "SMART formatı", "E01 formatı" ve "AFF formatıdır" (Şekil 22).



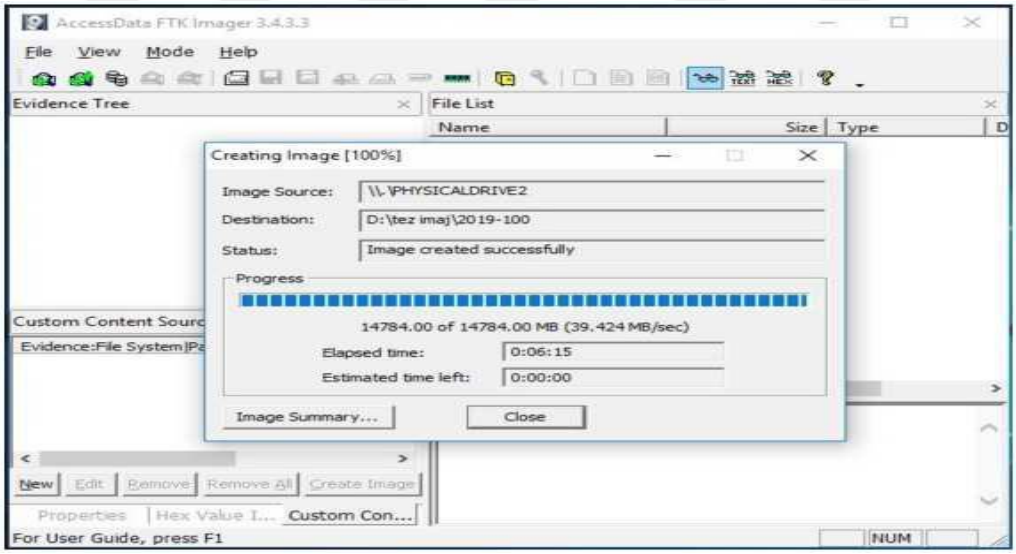
Şekil 22. FTK Imager disk imajı alma aşama 5

İstenilen format seçildikten sonra "anket numarası", "sertifika numarası", "resmi diğer resimlerden ayıran isim veya numara", "kişisel bilgiler" gibi bilgileri girmemizi isteyen bir pencere açılmaktadır. Bu girdi bilgisi imaj dosyasının saklandığı klasörde bir metin dosyasında yer almaktadır ve görüntünün elde edilme süreci ile ilgili bilgileri vermektedir. Gerekli bilgileri girdikten sonra "Görüntü Hedefi Seç" menüsü görünecektir. İmaj dosyasının yerini belirleyip imaj dosyasına isim verdikten sonra "Image fragment (MB)" kısmında dosya parçalara bölündüğünde her bir imaj dosyasının kaç megabayt olduğunu görülecektir. Ancak imaj tek dosya olarak oluşturulacak ise "Image Fragment Size (MB)" değeri "0" olarak alınmaktadır. "Sıkıştırma" seçeneği, yalnızca görüntü sıkıştırmayı destekleyen formatlardan biri seçildiğinde etkindir ve sıkıştırma derecesini belirtir. Yakalanan görüntü şifreliyse, "AD şifreleme kullan" olarak ayarlanmaktadır (Şekil 23).

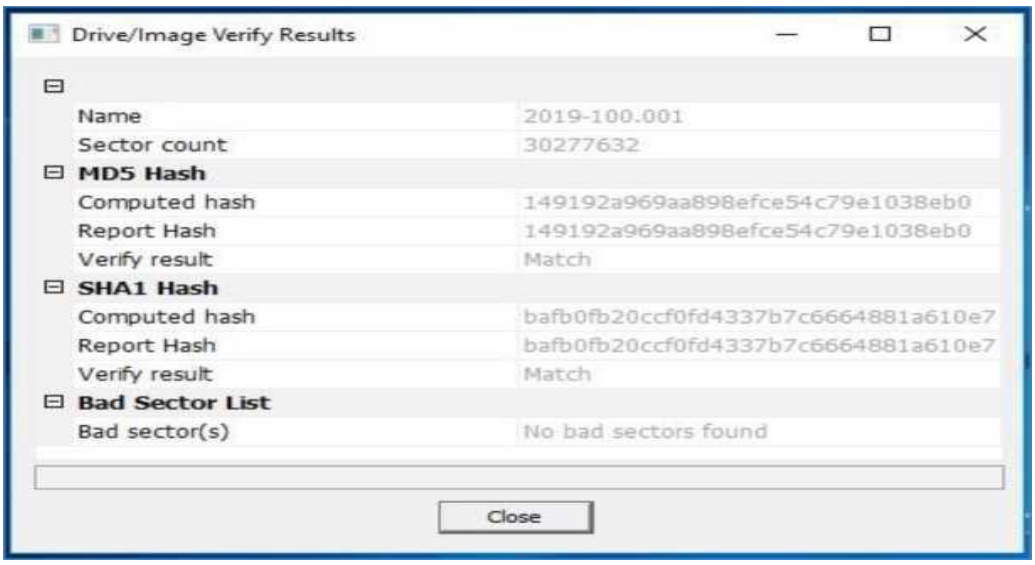


Şekil 23. FTK Imager disk imajı alma aşama 6

"Bitir" butonuna tıklandıktan sonra ilgili adımlar tamamlandığında "Başla" butonuna basılarak imaj yakalama işlemi başlatılır. İmaj alma işlemi tamamlandığında, görüntü alma işleminin ne kadar sürdüğü, görüntünün ortalama olarak ne kadar hızlı çekildiği ve görüntü doğrulamanın sonucu hakkında bilgi veren iki pencere açılacaktır (Şekil 24 ve Şekil 25).



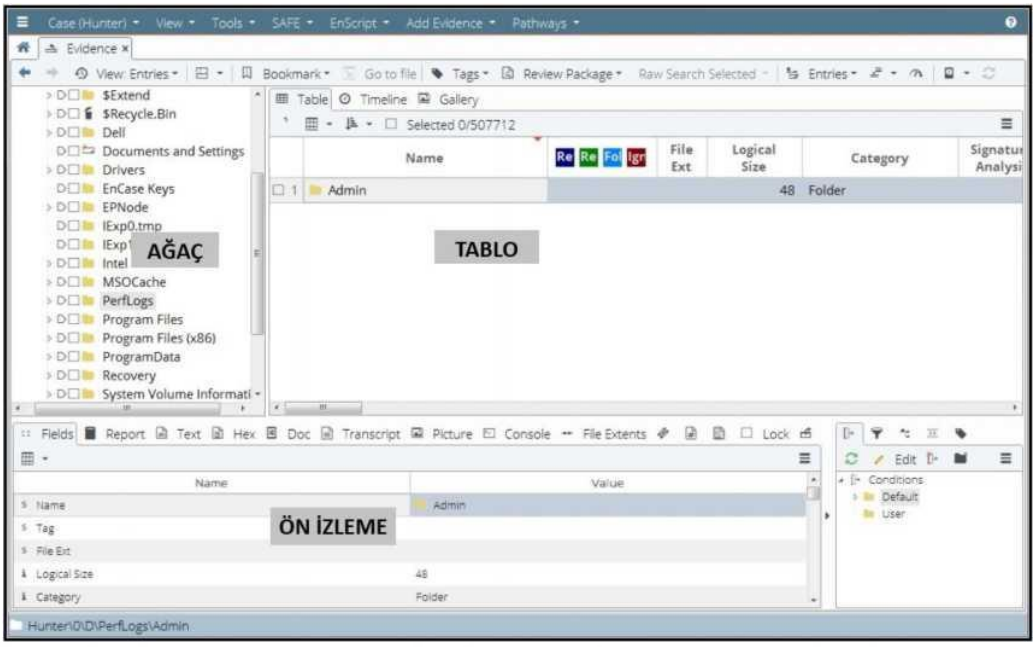
Şekil 24. FTK Imager disk imajı alma aşama 7



Şekil 25. FTK Imager disk imajı alma aşama 8.

Dosya analizi

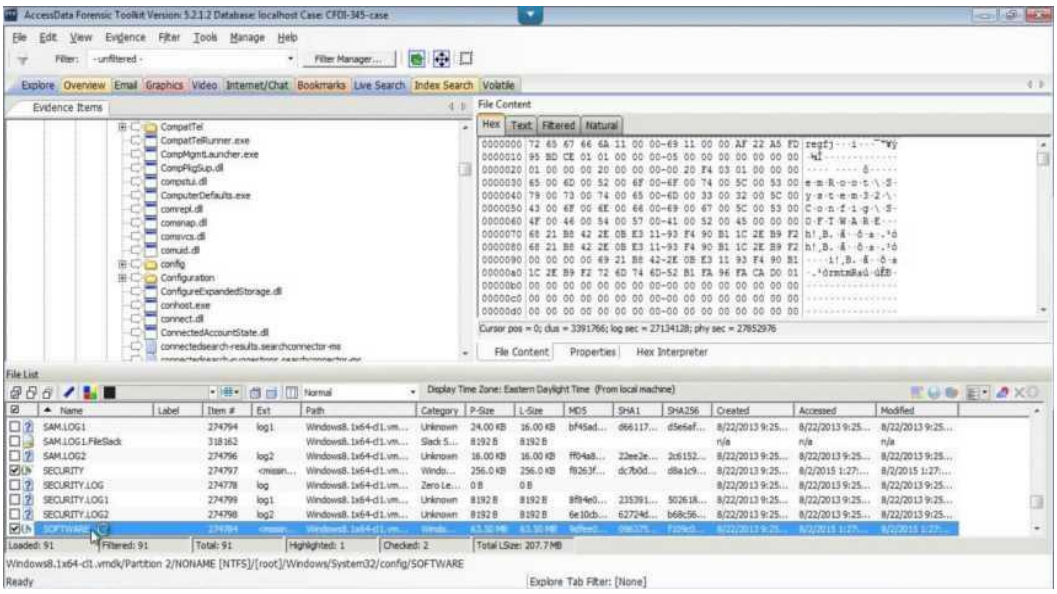
Dosya analizi aşaması, bir sonuca varmak için kanıtları ortaya çıkarmak için en önemli süreçtir. Bu noktada adli tıp uzmanı disk ya da görüntü dosyasında ne bulmak istediğini tam olarak bilmelidir (Henkoğlu 2011). Hard disk, USB bellek, hafıza kartı, CD/DVD gibi bir veri depolama aygıtından görüntü alınmışsa görüntü incelenmelidir. Soruşturma sürecinde ağırlıklı olarak adli yazılım olarak da isimlendirilen yazılımlar kullanmaktadır. Aşağıda adli soruşturmalarda kullanılmakta olan yazılım örnekleri ve genel nitelikleri verilmiştir. Encase Forensic, Amerikan şirketi Guidance Software tarafından geliştirilen çok işlevli bir adli bilişim yazılımıdır. Windows işletim sisteminde çalışmaktadır. Yazılım, doğrudan fotoğraf çekmek veya görüntü dosyalarını görüntülemek için kullanılabilmektedir. Alınan görüntü kontrol edilebilir. Yazılım, VMDK, VHD ve Raw DD gibi çeşitli görüntü formatlarını ve ayrıca kendi E01, EX01, L01, LX01 görüntü formatlarını destekler. Ağaç, tablo ve önizleme menüleri ile güçlü bir kullanıcı arayüzüne sahiptir. Bu kullanıcı ara yüzü kullanılarak çok sayıda fonksiyon gerçekleştirilebilmektedir (Bakan ve Saluk 2014).



Şekil 26. Encase Forensic v8.07 kullanıcı arayüzü

Yazılımın kullanıcı arayüzünde görüntülenen veri depolama birimi içeriği, ağaç görünümünde, hiyerarşik bir yapıda gösterilebilmektedir. Tablo bölümü, ağaç bölümünde seçilen içeriğin ayrıntılı içeriğini görüntüler ve filtrelemektedir. Önizleme bölümünde dosyanın içeriğini text, image, hex gibi farklı formatlarda görülebilmektedir.

Yazılım, veri depolama cihazının tüm mevcut ve silinmiş alanlarının yanı sıra HPA ve DCO bölümlerini görüntülemek için kullanılabilmektedir. Keşfedilecek alanlar arasında anahtar sözcük arama, veri kurtarma, internet geçmişi analizi, e-posta ve sohbet algılama ve analizi, şifreli dosya algılama ve analizi, dosya imza analizi ve hash analizi yer almaktadır. Tespit edilen şüpheli veriler işaretlenebilmektedir. Mevcut ve silinmiş tüm veriler indekslenebilir ve indekslenen veriler kelime bazında aranabilmektedir. İnceleme sırasında istenen bilgiler protokole eklenmek üzere işaretlenebilir ve inceleme neticesinde bütün bilgiler rapor halinde elde edilmektedir. Enscript işlevi, yazılım içinde küçük programların yazılmasına ve yürütülmesine olanak tanımaktadır (Opentext 2018). Forensic Toolkit (FTK), Amerikan şirketi AccessData tarafından geliştirilen çok işlevli bir adli yazılımdır. Windows işletim sisteminde çalışmaktadır. Bulunan delillerin araştırılması ve raporlanması konusunda oldukça başarılı olan bu program, başta güvenlik güçleri olmak üzere dünya genelinde yaygın olarak kullanılmaktadır. Bu program aracılığıyla kolluk kuvvetleri tarafından mahkemeye gönderilen raporların ve bilgilerin kanıtları düzenlenmektedir.



Şekil 27. Accessdata Forensic Toolkit (FTK) v5.2 kullanıcı arayüzü.

Yazılım sayesinde, değişik yazılımlarla gerçekleştirilmiş medya ve görüntü dosyalarını doğrudan görüntüleyebilmek mümkündür. Yazılım, ortamın tüm mevcut ve silinmiş alanlarını görüntülemek amacıyla kullanılabilmektedir. Çalışma sahaları içerisinde anahtar kelime araştırması, veri kurtarma, internet geçmişi analizi, e-posta ve sohbet kaydı tespiti ve analizi, şifreli dosya tespiti ve analizi ve dosya analizi yer alabilmektedir. Mevcut ve silinmiş tüm veriler indekslenebilir ve indekslenen veriler kelime bazında aranabilmektedir. Yazılım zengin bir filtreleme niteliğine sahiptir. Ayrıca kullanıcı tarafından filtre oluşturularak ve kullanılarak inceleme alanı daraltılabilmektedir. İçerik, metin, onaltılık ve yerel görünüm gibi birkaç değişik ön izlenebilmektedir. Görüntü dosyaları, grafikler sekmesi altında görüntülenebilmektedir. Video dosyaları, hızlı inceleme için dönüştürülebilir ve küçük resimlere dönüştürülebilmektedir. Cerberus Analysis işlevi neticesinde, araştırılan veri taşıyıcılarında kötü amaçlı yazılım aramak mümkündür. Yazılımın ayrıntılı bir raporlama işlevi vardır (Bakan ve Saluk 2014).

İşletim Sistemi Üzerinde Yapılan Analizler

Adli inceleme konusu olan bilgisayarda kurulu olan işletim sisteminin araştırılması, adli tıp uzmanına birçok konuda detaylı bilgi sağlamaktadır. Sistem logları, kurulu yazılımlar, silinen veriler, internet geçmişi, email ve anlık mesajlaşma logları gibi alanlar işletim sisteminde analiz edilebilecek alanlardır. İşletim sistemleri, hem kullanıcının işlemlerini hem de kendi arka plan işlemlerini zaman çizelgesine otomatik olarak kaydetmektedir. Bu girişler, işletim sisteminin çeşidine ve fonksiyonuna bağlı olarak farklı alanlarda saklanmaktadır. Bu kayıtlara günlükler veya olay günlükleri denmektedir. İşletim sistemi tarafından idare edilen bu kayıtlar, adli incelemelerde oldukça mühimdir (Durmaz 2014).

Günlük girişleri ile tüm analiz işlemlerinin sonuçları arasında anlamlı bir ilişki olmalıdır. Kullanıcı tarafından gerçekleştirilmekte olan tüm işlemlerin, kurulan ve kaldırılan tüm yazılımların ve işletim sistemi tarafından stoklanan verilerin tutarlılığı, ortam analizi sonucunu desteklemelidir (Henkoğlu 2011). "Windows Kayıt Defteri", işletim sistemi ile ilgili işlemlerin depolandığı alandır. Windows NT bilgisayarlarda, kayıt defteri verileri "Güvenlik, Yazılım, SAM ve Sistem" olmak üzere dört dosyada saklanmaktadır. Bu dosyalar "C:\Windows\system32\config\" konumunda bulunmaktadır. Kullanıcı ayarları "NTuser.dat" dosyasında saklanmaktadır. Bu dosya da her kullanıcı için ayrı ayrı "C:\Users\" klasörlerinde yer almaktadır (GetData Forensics 2017). Yüklü yazılımların algılanması ve incelenmesi medya analizi neticesinde algılanan bilgiler ile işletim sisteminde yüklü programlar arasındaki ilişkinin anlaşılmasına yardımcı olmaktadır. Bu belirlemeler, Windows işletim sistemi için Yazılım adlı bir kayıt defterine bakılarak yapılabilmektedir. Elde edilen bilgiler sayesinde çalışmada gözlemlenen bilgiler ile işletim sisteminde yüklü olan programlar arasındaki ilişkinin anlaşılmasına yardımcı olmaktadır (Durmaz 2014). Tarama işlemi esnasında tüm depolama aygıtı veya görüntü taranmaktadır. Veri kurtarma işlemi, veri silinmesi veya bozulması nedeniyle görüntülenemeyen daha önce depolama aygıtında yer alan verileri geri yükler ve bu veriler üzerinde de inceleme yapılmaktadır. Bültende kullanılmakta olan otomatik veri kurtarma ya da adli tıp yazılımı, depolama cihazının silinmiş ve boş olarak işaretlenmiş bir alanından silinen ve bozulan verileri kurtarmaya çalışmaktadır. Silinen verileri içeren bir sektöre verilerin üstüne yazılması, kurtarma sürecini olumsuz yönde etkilemektedir. İnternet geçmişini incelemek de bir adli bilişim uzmanına bir suçu çözerken önemli bilgiler sağlayabilmektedir. İnternet geçmiş analizi kapsamında, ziyaret edilen web sayfaları, ziyaret süreleri ve kayıtlı şifreler elde edilebilmektedir. Bu bilgiler, işletim sisteminde yüklü olan internet tarayıcılarının klasörlerinde saklanmaktadır. Bağlantı verilen sitenin erişim bilgilerine, tarayıcı klasöründe saklanan çerezler aracılığıyla erişilebilmektedir. İnternetin yaygın olarak kullanılan bir iletişim şekli olması nedeniyle internet üzerinden iletişime olanak sağlayan e-posta ve anlık mesajlaşma kayıtlarının incelenmesi sayısal delil incelemelerinde önemli bir delil kaynağı olmuştur. Birçok adli tıp programı, adli tıp uzmanının, soruşturma esnasında kaydedilen e-posta adreslerini medyada arayarak bulunan e-posta adreslerine odaklanmasına yardımcı olmaktadır.

Network analizi

Ağ analizi, belirli bir sistemde kurulu bir yerel ağ (LAN), geniş alan ağı (WAN) ya da internet ağının trafiğinin izlenmesi, analiz edilmesi ve analiz neticelerine göre gerekli bilgilerin sağlanması olarak açıklanmaktadır (Orta 2015). Ağ analizi, bilgi ağları kullanılarak

işlenen suçların incelenmesinde ön plandadır. Ancak ağ trafiği günlükleri tek başına anlamsızdır. Kayıtlı web trafiği verileri; sadece analiz edildiğinde, bir araya getirildiğinde ve gerçek zamanlı olarak sunulduğunda ya da sistem, kayıt çeşidi ve analiz edilen olayın türüne göre önceliklendirildiğinde anlamlıdır (Polat 2014).

Bir ceza soruşturması, belirli bir ağ üzerinden bilgi yoluyla suç işlendiğinden şüpheleniyorsa, şüphelinin kullanmış olduğu ağ üzerinden iletilen paketler incelenerek analiz edilmektedir ve deliller toplanmaktadır. Ağ yapısı çoğunlukla dört basamak olarak kabul edilmektedir: Fiziksel katman, ağ katmanı, taşıma katmanı ve uygulama katmanı. Her katman, elektronik kanıtlarda benzersiz farklılıklar göstermektedir. Ağ üstünde gönderilen paketleri yakalamak ve incelemek için Packet Analyzer (Wireshark, SolarWinds, NetworkMiner vb.) kullanılmaktadır. Ağda incelemeye geçilmeden önce araştırılan ağın topografyasını çıkarmak gereklidir. Hangi bilgisayarın kiminle iletişim kurduğunu, hangi harici cihazların ve ağ cihazlarının (hub, switch, router vb.) kullanıldığının belirlenmesi gerekmektedir (Orta 2015).

Mobil sistemlerin analizi

Mobil iletişim sistemlerinin kullanımı dünya çapında hızla artmaktadır. Cep telefonu sistemleri olarak düşünebileceğimiz tabletler, PDA'lar ve cep telefonları, muhafazalarının içinde pil gücü ile çalışan mobil cihazlardır. Günümüzde cep telefonları en yaygın kullanılmakta olan ve hızla değişen ve gelişen mobil cihazlardan biridir. Cep telefonu yaşamımıza ilk girdiğinde yalnız mobil olma ve hayatın her alanında her an iletişim kurabilme özelliğiyle öne çıkmıştır ancak çağımızda bilgi teknolojilerinin gelişmesiyle birlikte cep telefonları da değişime uğramıştır. İşletim sistemine ve donanım niteliklerine bağlı olarak bir laptopun yapabileceği her şeyi yapabilen cep telefonları, her geçen gün daha fazla dijital ekran kazanan sistemler olarak kabul edilmektedir. Adli tıp süreçleri ve delillerin kabul edilebilirliği kuralları cep telefonları için de geçerli olsa da cep telefonları için delillerin toplanması ve incelenmesi daha karmaşık ve çetrefilli bir süreçtir. Çok fazla cep telefonu modeli ve işletim sistemi, dosya sistemi, uygulama ve donanım farklılıkları adli incelemeleri zorlaştırmaktadır (Çakır 2014).

Klasik cep telefonlarında ses verisi, telefon defteri ve metin mesajları gibi verilere erişilirken, akıllı telefonlarda birçok multimedya içeriğine ve internet erişimi gibi bilgilere ulaşılabilmektedir (Kiceci 2014). Mobil cihazları edinirken ve yönetirken, verileri doğru bir şekilde toplayıp kullanmak ve doğru sonuçlara varmak için dikkate alınması gereken bazı hususlar vardır (Çakır 2014):

• Cihazla birlikte standart dışı cihaz verilerine ve şarj kablolarına el konulmalıdır.

- Cihazın ekranının fotoğrafı çekilmeli ve gerekirse parmak izi alınarak cihazın kime ait olduğu tespit edilmelidir.
- Cihazlar açılırken taşınabilir cihazlardan kaynaklanan parazit nedeniyle ilk yapılması gereken şarj cihazları ile batarya devamlılığının sağlanmasıdır. Cihazlar destekliyorsa açık/kapalı olmasına bakılmaksızın uçak moduna alınmalı ve ağ sinyallerinden ve kablosuz ağ sinyallerinden bağlantısı kesilmelidir. Cihazların sinyal almaması için sinyal bariyerleri, faraday torba denilen koruyucu örtüler veya alüminyum folyo kullanılabilmektedir.
- Donanım önyükleme parolaları ve güvenlik parolaları öğrenilmeli ve yazılmalıdır. Mobil cihazları ve uygun güvenliği ele geçirdikten sonraki adım, veri toplamadır. Mobil cihaz araştırması için özel cihazlar ve yazılımlar bulunmaktadır. Donanım inceleme cihazları daha pratik kullanımlara sahip olsa da bu cihazlar daha pahalıdır (Henkoğlu 2011).

Adli tıp uzmanı öncelikle incelenmekte olan cihazın fotoğrafını çekmelidir. Olayın türüne göre yerinde veya laboratuar ortamında gerçekleşebilir. Diğer mobil cihazlara göre daha karmaşık bir yapıya sahip olan cep telefonlarında fotoğraf çekilirken cep telefonunda, SIM kartta ve hafıza kartında veri olabileceği göz önünde bulundurulmalıdır. Cep telefonu, SIM kart ve hafıza kartından alınan bilgiler; IMEI numarası, telefon sistem bilgisi, şebeke bilgisi, GPS konum bilgisi, takvim, hatırlatıcı ve görev listesi, telefon defteri, arama geçmişi ve süresi, mevcut veya silinmiş metin mesajları, MMS mesajları, fotoğraflar, videolar, ses dosyaları, e-postalar, belgeler internet geçmişi, anlık ileti verileri, sosyal medya kayıtları, uygulama verileri ve veri tabanlarıdır (Çakır 2014).

Ceza Muhakemesi Hukukunda Delil Kavramı

Ceza muhakemesinin amacı, şüpheli ve sanığın haklarına saygılı bir biçimde maddi gerçeğe ulaşılmasıdır (Centel ve Zafer 2021). Maddi gerçek her ne pahasına olursa olsun araştırılıp bulunmalıdır diye bir kural hiçbir hukuk devletinde söz konusu değildir. Bu bağlamda ceza muhakemesi, insan hakları ihlallerine yol açmadan maddi gerçeğin araştırılıp bulunması, adaletin gerçekleştirilmesi ve hukuki barışın sağlanması amaçlarını hedeflemektedir (Öztürk vd 2020).

Görülmekte olan bir ceza uyuşmazlığına konu olan maddi olay, kronolojik olarak muhakemenin duruşma safhasından önce gerçekleşmiştir. Bu sebeple o olaydan günümüze kalanlar ile olay hakkında bir sonuca ulaşmak gerekecektir. Geçmişte yaşanan olay ile ilgili olan ve günümüze devrolunan her şey delil kavramı altında incelenmektedir. Elde edilen

deliller ile maddi olay, mahkeme önünde yeniden oluşturulacak ve suça konu olan olay yeniden yapılandırılacaktır (Centel ve Zafer 2021).

Ceza muhakemesinde hukuk düzenince kabul edilen araçlarla maddi gerçeğe ulaşma çabası, *"ispat"* olarak anılacaktır. Fiilin, fail tarafından işlendiği veya işlenmediği konusunda tam bir kanaate ulaştıran şeyler ise delil olarak anılacaktır. İspat çabası, sabit oluşu gerektirir (Öztürk vd 2020). Bu bakımdandır ki kişinin suç işlediğinin sabit olup olmadığı konusunda tam bir kanaate ulaşılmadığı müddetçe kişi hakkında mahkûmiyet kararı verilemeyecektir. Ceza muhakemesinde ispat bakımından belirli delillere başvurulması zorunluluğu söz konusu değildir. Aksine ceza muhakemesinde bir olay, her türlü delille ispat edilebilecektir. Öyle ki herhangi bir şey, kabul edilebilirlik sınırları içerisinde kaldığı sürece, delil olarak kabul edilebilecektir. Belirli bazı delillere öncelik tanımak ve diğerlerini kabul etmemek düşüncesi yahut delilleri, ispat gücü bakımından bir derecelendirmeye tabi tutmak düşüncesi maddi gerçeğe ulaşma amacı ile uyuşmamaktadır ve neticesinde ceza muhakemesini işlemez kılacaktır. Bu bakımdandır ki ceza muhakemesinde *"delilserbestisi"* esastır (Centel ve Zafer 2021).

Anayasa'nın 138. maddesi 1. fıkrası uyarınca *"Hakimler... vicdanı kanaatlerine göre hüküm verirler."* Ek olarak Ceza Muhakemesi Kanunu'nun (CMK) 217. maddesinin 1. fıkrası uyarınca *"... deliller hâkimin vicdanî kanaatiyle serbestçe takdir edilir."* Bu açıklamalar sonrasında diyebiliriz ki hukukumuzda *"delil serbestisi"* ve bunun neticesinde *"vicdani ispat"* sistemi kabul edilmiştir ve sonuç olarak bir nesne veya açıklamanın delil olarak kabul edilmesi, yargıçta vicdani kanaat oluşturmasına bağlı kılınmıştır (Centel ve Zafer 2021).

Şu husus belirtilmelidir ki *"delil serbestisi"* ne kadar maddi gerçeğe ulaşmak için her yolun mubah olduğu anlamına gelmiyorsa, *"vicdani delil sistemi"* de o kadar hâkimin keyfi olarak delilleri takdir edeceği anlamına gelmemektedir. Zira yukarıda bahsi geçen maddeler incelendiğinde Anayasa m. 138/1 hükmüne göre hâkimlerin *"... Anayasaya, kanuna ve hukuka uygun..."* olarak karar verebileceklerini ve CMK m. 217/1 hükmüne göre hâkimlerin, kararlarını *"ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere"* dayandırabileceklerini görmekteyiz (Özen ve Özocak 2015).

İlgili maddeler ışığında diyebiliriz ki hâkim, bilime, maddi gerçeğe ve hukuka uygun şekilde elde edilen delilleri, keyfi bir biçimde değil, akla ve mantığa uygun olarak serbestçe değerlendirmeli, akıl yürütme faaliyeti yoluyla değerlendirdiği deliller aracılığıyla maddi meseleye ilişkin sonuca ulaşmalıdır (Toroslu ve Feyzioğlu 2018).

Aynı şekilde Yargıtay da çeşitli kararlarında, ceza yargılamasının amacının:

"hiçbir duraksamaya yer bırakmadan maddi gerçeğin ortaya çıkarılması" olduğunu, "gerçeğe ulaşmada mantık yolunun izlenmesi ve delillerin gerçekçi ve akılcı" olması gerektiğini belirtmiştir.

Ceza Muhakemesi Hukukunda Delillerin Özellikleri ve Dijital Deliller

Delil özgürlüğü ilkesi, delilin özel nitelikler olmaksızın kabul edilebilir olduğu anlamına gelmez. Delilin taşıması gereken bu nitelikler, söz konusu delilin delil sayılabilmesi için gereklidir ve bu bağlamda, tanımlanmış şartları taşımayan deliller ceza davalarında delil olarak kullanılamaz (Değirmenci 2014).

Akılcılık

Deliller, akılcı ve bilimsel olmalıdır. Nitekim yukarıda Yargıtay kararlarında da bu husus defaatle belirtilmiştir. Başka bir ifadeyle deliller, bilimsel açıdan kabul edilebilir yöntemle elde edilmiş ve bilimsel olarak kabul edilebilir olmakla birlikte akla uygun olarak ifade edilebilmelidir. Konumuzla bağlantısı çerçevesinde burada dijital delillerin bilimselliği konusuna da kısaca değinmek gerekir. Bilimsel delil kavramından farklı olarak dijital delilin bilimsel oluşu, delilin elde edilmesi anından hükme esas teşkil ettiği ana kadar geçen süreçte bilimsel yöntemlerin uygulanması anlamına gelmektedir. Bu bağlamda ileride daha ayrıntılı değinilecek olmakla birlikte dijital delillerin elde edilmeleri bakımından hukuki gerekliliklerin yanında bazı teknik gerekliliklerin de sağlanması gerektiğini ve bu çerçevede adli bilişim biliminin karşımıza çıktığını söyleyebiliriz (Swanson 2012).

Temsil edicilik/ gerçekçilik

Delillerin öncelikle ilgili cezai uyuşmazlığın bir kısmını ispatlayabilmesi yani olayı temsil edebilmesi ve beş duyu organıyla algılanabilecek maddi ve gerçekçi bir yapıda olması gerekmektedir. Ancak kısaca ele alacağımız dijital delil, klasik delilden farklı olarak soyut bir yapıya sahiptir ve varlığını anlamak için farklı araç veya cihazlara ihtiyaç duyulmaktadır (Toroslu ve Feyzioğlu 2018). Delilin kabul edilebilirliği ile ilgili şartlardan biri de delilin ilgili olması gerektiğidir. Delillerin yargılamaya katılan taraflar açısından yani olayı temsil etmesi açısından önemli olması gerekmektedir. Dijital delillerin soyut doğası, delillerin bir olayı temsil etmesi ve bu bağlamda beş duyu ile algılanabilen maddi bir yapıda olması gerektiği konusunu gündeme getirebilmektedir (Swanson 2012).

Mahkemeye sunulduğunda dijital delilin basılı olması halinde dijital delilin hukuki özelliğinin ne olacağı tartışılmaktadır. Bununla birlikte, genel olarak, dijital verilerin bir çıktısının mahkemeye sunulması zorluklara neden olabilmektedir. Zira dijital bilgiler

yazdırılırken, suçun koşulları hakkında çok önemli bilgilerin kaybolması mümkündür (Miller 2014). Bu noktada bilgiye ilişkin bilgi olarak tanımlanan metadata kavramından bahsetmek yerinde olacaktır. Metadata, dijital olarak saklanan verilerin kim, ne zaman, nerede, neden ve nasıl karakterize edildiği, karakterize edildiği, değiştirildiği, kontrol edildiği veya var olduğu gibi o verilerle ilgili soruların cevabıdır. Özellikle, yazdırma işleminin bir sonucu olarak, dizinden görünen meta veriler çıktıda görünmez. Bu nedenle, bir bilgi sistemi vasıtasıyla görüntülenebilen ve alınabilen dijital kanıtlar, doğası gereği soyut olsa bile, doğruluğu tesis edilene kadar olayı temsil ettiği düşünülmelidir. Çünkü dijital delil, basılan ve somutlaşan veri değil, bilgi sisteminin kendisinde yaratılan, iletilen, saklanan, değiştirilen ve nihayetinde soyut bir biçimde olan bilgidir. Bu bağlamda temsil kavramı dijital bir ekrana göre farklı değerlendirilmelidir. Öte yandan aynı verinin çıktısı ile dijital ortamda saklanan verinin birebir aynı olması durumunda; Çıktının dijital delil olarak kaldığı ve hukuki niteliği itibariyle gerçekliğini ve temsiliyetini kaybetmediği konusunda hemfikiriz (Değirmenci 2004).

Hukuka uygunluk

Suçlayıcı delil sisteminin sınırını oluşturan hukuka aykırı deliller, ceza yargılamasının hiçbir basamağında kullanılamaz ve dolayısıyla mahkûmiyet ve yargılamaya esas teşkil edemez (Khalil 2021). İlk olarak, deliller hukuki delil olmalıdır. İkincisi, deliller yasal yollardan elde edilmelidir. Delil ilgili usul kurallarına göre toplanmadığı takdirde yargılamaya esas olamaz. Ayrıca CMK md. Yönetmelik 148'e aykırı olarak elde edilen deliller de yasa dışı kabul edilir ve cezaya esas teşkil etmez (Centel ve Zafer 2021). İleride daha detaylı olarak ele alınacak olan dijital delilleri ilgilendiren bu bağlamda, bazı teknik gerekliliklerin ve kanuni zorunlukların tesis edilmesi delillerin hukuka uygunluğuna ilişkin şüpheleri ortadan kaldırmaktadır. Bilhassa dijital delil elde etme şartlarının ihmal edilmesi, CMK m 134 “Bilgisayarlarda, bilgisayar programlarında ve loglarda arama, kopyalama ve el koyma” tedbiri veya bu çerçevede delil elde edilmesinde uluslararası adli tıp yöntemlerinin uygulanmaması toplanan kanıtları yasadışı hale getirmektedir (Swanson 2012).

Önemlilik

Delilin kabul edilebilirliği de önemlilik testine tabidir. Belirli delillerin ilgili olduğu varsayılsa bile, önemi davanın kararını etkilemeyecek kadar önemsiz ise kabul edilemez. Başka bir deyişle ilgililik, ilgili kanıtın kararı etkileyip etkilemeyeceği ile ilgilidir.

Müştereklik

Deliller müşterek olmalıdır. Bir başka ifadeyle delilin içeriği sadece hâkim tarafından değil, taraflar tarafından da bilinmeli ve tartışmaya açılmalı ve hüküm yalnızca hâkimin

kişisel bilgisine göre tesis edilmemelidir. Nitekim CMK m. 216/1 uyarınca deliller *"ortaya konmalı* ve *tartışmaya"* konu olmalıdır. Ek olarak CMK m. 217/1 uyarınca *"hâkim kararını huzurunda tartışılmış delillere..."* dayandırabilecektir (Centel ve Zafer 2021).

Dijital delillerin bütünlüğü, şüpheli ya da sanığın kullandığı bilişim sistemine el konulması ve el konulan bilgi sisteminin adli incelemesi sonucunda düzenlenen adli tıp raporunun ibraz edilmesiyle sağlanmaktadır. Bu kapsamda hazırlanmakta olan raporun, raporu okuyanların anlayabileceği sade bir dille yazılması ve teknik terimlerle dolu olmaması önemlidir (Değirmenci 2004).

Güvenilirlik

Deliller sağlam ve güvenilir olmalıdır. Yani deliller değiştirilmemeli, kopyalanmamalı ve asılları duruşmada kullanılmalıdır. Dijital kanıtlar bu işlevde farklılık göstermektedir. Diğer bir deyişle, orijinal dijital delilin dijital ortamda aranması, delilin hiç kullanılmaması ile sonuçlanabilmektedir. Zira doğası gereği soyut olan ve bu nedenle çıplak gözle görülemeyen dijital deliller, gerekli araç ve gereçler yardımıyla görülebilmektedir. Bu nedenle, dijital kanıtlarla ilgili araç ve gereçleri içeren durumlar, kanıt temeli olarak kabul edilmelidir. Ek olarak, dijital ekran tamamen yeniden üretilebilir. Bu nedenle, prova bozulma olasılığını ortadan kaldırmak için bu kopyalar kontrol edilebilmektedir. Tamamen yeniden üretilebilir özellikler nedeniyle, bazı durumlarda hangi belgenin orijinal olduğunu belirlemek imkânsız bile olabilmektedir. Bu itibarla, dijital delillerin gerçekliği tespit edilirken, asıl belgenin değil, o delili içeren sistemin tam ve doğru çalıştığı tespit edilerek, o belgenin gerçekliği doğrulanmaktadır (Nigel vd 2014).

Dijital delilin bazı nitelikleri, doğası gereği, delilin sahip olması gereken genel özelliklere karşılık gelemez. Bu itibarla dijital delilin doğası gereği bu çelişkilere bakmak gerekir ve bu nedenle dijital delilin delilde bulunabilecek özelliklerine bakılmalıdır (Miller 2014). Örneğin, delilin hassas doğası göz önüne alındığında, değiştirmenin, tahrif etmenin, yok etmenin kolay olması ve soyutluğu, yani dijital kanıtları fiziksel bir nesneye bağlamanın zorluğu, çeşitli endişeler doğurabilmektedir (Nigel vd 2014).

Bu endişelerden kaçınmak için, dijital delillerin ilk elde edildiği andan itibaren delilin bir parçası haline gelene kadar ve son olarak mahkemede sunulduğu zamana kadar belgelenmesi önemlidir, böylece delil zinciri bu belgelere dayandırılır. Dijital delili kimin elde ettiği ve kabul edilebilirliğinin nasıl korunduğu gibi detaylar önemlidir (Başlar 2020).

Elde edilebilirlik

Bir olayı temsil etmek için, ona erişilmeli, geri alınmalı ve sonunda iade edilmelidir. Bu nedenle, somut kanıtlar mahkemeye getirilmez veya tartışılmaz. Dijital kanıtların elde edilmesi, bunları içeren bilgi sistemlerinin aranmasının veya belirli durumlarda, dijital kanıt içeren bilgi sistemlerinin maddi mülkünün istisnai olarak müsadere edilmesinin ve adli tıp laboratuarında yapılan bir aramanın sonucudur (Toroslu ve Feyzioğlu 2018).

Ceza Muhakemesi Hukukunda Delil Türleri ve Dijital Delillerin Yeri

Deliller çeşitli şekillerde elde edilmektedir. Deliller, önemli olayın sunumuna dayalı olarak yapılan ayrım temelinde direk ve dolaylı kanıtlara (belirtiler) ayrılmaktadır. Benzer şekilde, doğrudan deliller ana olayı ispat ederken, ikinci derece deliller ana olaya bağlı ikincil olayları ispat etmektedir. Örneğin, bir suç mahallinde bir zanlının DNA'sının bulunması, zanlının olay mahallinde olduğunu kanıtlar, ancak fiili olayı işlediğini kanıtlamaz. İkinci farka göre deliller şahsi deliller (ifade beyanları, şüpheli, sanık, tanık, mağdur, bilirkişi) ve fiziki deliller (belgesel deliller ve referanslar) olarak ikiye ayrılmaktadır. En sık kullanılan ayrım doğrudan kanıt ile semptomatik kanıt arasında olduğu için burada sadece bundan bahsedilmektedir (Nigel vd 2014).

Doğrudan deliller

Çoğunlukla, sanığın suçu işlediğini kesin olarak kanıtlayabilen görgü tanığı ifadesi gibi, sanığı suçun işlenmesiyle direk ilişkilendiren kanıtlardır. Bir tanım gereği, dolaylı kanıt, şüpheli ya da sanığı suçla mantıksal olarak ilişkilendirdiği sürece, direk kanıt dışındaki her şeyi ifade etmektedir. Dolaylı kanıtlar, bir suçu kanıtlayan kanıt zincirindeki bir halka ile karşılaştırılabilir. Çünkü bu tek başına suçu ispatlamaya yetmez, başka delillerle desteklenirse mahkûmiyete esas teşkil edebilmektedir (Miller 2014).

Beyan

Beyan, bir kişinin veya kurumun belirli bir konu hakkında resmi ve yazılı olarak yaptığı açıklama veya bildirimdir. Beyan, genellikle bir durumu, olayı, niyeti, ya da gerçeği açık bir şekilde ifade etmek amacıyla kullanılır ve hukuki veya idari süreçlerde önemli bir rol oynar. Beyan, genellikle resmi bir belge veya yazılı bir açıklama şeklinde yapılır. Resmiyet, beyanın doğruluğunu ve ciddiyetini artırır. Beyanın içeriği açık ve net olmalıdır. Yanlış anlaşılmalara mahal vermemek için beyanın anlaşılır bir dilde ifade edilmesi gerekir. Beyan, belirli bir konuyu veya durumu açıklamak amacıyla yapılır. Bir olayın, niyetin, görüşün veya gerçeğin bildirilmesi amacıyla kullanılabilir. Beyanlar, hukuki ve idari süreçlerde önemli delil

veya belge olarak kabul edilebilir. Mahkemeler, resmi kurumlar ve diğer otoriteler beyanları değerlendirebilir ve kararlarında kullanabilir. Beyanda bulunan kişi veya kurum, beyanın doğruluğundan sorumludur. Yanlış veya yalan beyan vermek, hukuki yaptırımlara neden olabilir. Beyanlar, çeşitli belgeler ve formlar aracılığıyla yapılabilir (örneğin, beyanname, dilekçe, yeminli ifade). Belirli bir formata ve içeriğe sahip olabilirler.

Belge

Belgesel delil, olay anında doğrudan nesne üstünde kaydedildiğinde ortaya çıkmaktadır. Belgesel kanıt, belirli bir olayı doğru bir şekilde yansıtan kanıtlardır. Bir olayı kaydederken, yazılı belge olayın sahibidir; olay bir zil sesi olarak algılanırsa ses kaydı; olay hem biçim hem de ses olarak aktarılıyorsa, ortam dar anlamda bir film şeridi ya da bir CD vb. olabilmektedir (Aksamitowska 2021).

Belgeyi CMK (CMK m. 214-215), içeriği okumanın dar yorumlayıcı işlevi yerine görerek ve işiterek öğrenilen teknik araçların belgesel kanıt olmayabileceği, ancak keşfedilebilir semptomatik kanıt olabileceği ve bu nedenle kanıtlarla desteklenmesi gerektiği ileri sürülmüştür. Ancak hukuki edinim ve teknik inceleme sonucunda görüntü ve ses algılama cihazlarından elde edilenlerin diğer delillerden bir farkı yoktur; bir şeyi delil olarak kabul etmek ile vicdani kanaat oluşturmak için onu başka delillerle desteklemek farklı şeylerdir. Dijital delillerin görüntü ya da sese dönüştürüldüğünde semptomatik delil olduğu, fakat okunabilir hale getirildiğinde belgesel delil niteliği taşıdığı tespit edilmiştir (Ayözger 2016).

Belirtiler

Semptomlar, olayın geride bıraktığı izler ve eserlerdir. Belirtilerin temsili, tek başına maddi bir olayı kanıtlamasa da, ifadeler ve belgeler gibi doğrudan kanıtlarla elde edilen bir görüşü destekler niteliktedir. Semptomlar doğal ve yapay semptomlar olarak ikiye ayrılmaktadır. Eylemi yapanın iradesi dışında olayın bıraktığı iz ve nesnelere (örn. tabanca, bıçak) yapay (insan yapımı) işaretler olarak adlandırılır. Semptomlar genellikle direk altta yatan çatışmaya işaret etmek için yeterli değildir. Bu bağlamda, genellikle belirli bir olayla ilgili diğer kanıtları değerlendirmekten faydalanırlar ve çoğu zaman diğer kanıtları desteklemeye ihtiyaç duyarlar. Ancak bu destekleyici koşul, kural olarak belirtiler dışındaki tüm kanıtlar için geçerlidir (Börekçi 2020).

Zira delil hürriyetinin kabul edildiği ceza muhakemesi hukukunda hâkim, vicdanı ile ilgili bir kanaat oluşturarak, belgede veya konuşmada verdiği delilleri başka delil ve niteliklerle desteklemeye çalışılmaktadır. Ayrıca hiçbir delilin olayı kesin olarak

ispatlayamayacağı da söylenememektedir. Hem direk hem de dolaylı kanıtların her zaman bir hata payı vardır. Ancak, deliller mahkûmiyete dayanak teşkil edecek şekilde temize çıkarıcı bulunursa, kişi sadece bu delile dayanarak mahkum edilemez. Bilimsel delil olarak da adlandırılan belirtiler, kriminoloji bilgilerine göre bilimsel metotlarla elde edilmekte ve bunların elde edilmesi sonucunda oluşturulan raporlara da bilimsel delil adı verilmektedir. Bu bağlamda, semptom kanıtı için hata payının tanığınkinden daha az olabileceği tespit edilmiştir. Dijital kanıtlara dayalı bir inceleme yapılırken, dijital kanıtların çoğunlukla bazı dijital nesne ya da olayların soyutlanması olduğu söylenebilir. Örneğin, birisi bir bilgisayara e-posta göndermek gibi bir görevi gerçekleştirmesini söylediğinde, ortaya çıkan eylemler gerçekte ne olduğunun yalnızca kısmi bir resmini sağlayan veri kalıntılarıdır. Bu nedenle, dijital gösterge çoğunlukla bir semptom göstergesi olarak kabul edilmektedir. Çünkü bilgisayar faaliyetini yalnızca dijital kanıtlara dayanarak bir bireye atfetmek her zaman basit değildir. Bu nedenle dijital kanıt genellikle bir soruşturmanın parçası olarak kabul edilir. Suç işlendiğinde bilgisayarı başka birinin kullanıyor olması gerçekten mümkündür. Bu bağlamda sayısal delillerin kanıtlayıcı gücünü artırmak için bilişim sistemine bir bütün olarak bakmak gerekmektedir (Buskirk vd 2006).

Fiziksel kanıttan farklı olarak, dijital kanıtın tek başına görüntülenmesi, dijital ekranın sunum kalitesinde kayıp veya önemli kayıpla sonuçlanabilir. Bu nedenle, bilgileri içeren bilgi sisteminin bir bütün olarak incelenmesi ya da elde edilen bilgilerin başka kanıtlarla desteklenmesi, dijital kanıtların doğrulanmasına ve kanıtsal değer elde edilmesine katkıda bulunmaktadır (Casey 2011).

Dijital Delillerin Hukuki Geçerliğinin İncelemesi

Dijital delillerin hukuki geçerliliği incelenirken kanunun temel gereği olan pratiklik, akıl, erişilebilirlik, temsil edilebilirlik, her yerde bulunabilirlik ve kanuna uygunluk özellikleri aranmakta ve diğer delillerde de bulunması gerekmektedir (Başlar 2016). Delil topluluğunun gerektirdiği şekilde, bir ceza davasında sunulan dijital deliller, davanın tüm tarafları tarafından bilinmeli ve sorgulanmalıdır. Dijital delil, delil topluluğu ilkesi açısından diğer delillere göre avantajlıdır. Çünkü soruşturma safhasında bile dijital delil içermekte olan ve bir kopyası sanığa verilen elektronik verinin bir kopyasıdır. Bu, tekrarlanabilir elektronik kanıtın bir avantajıdır. Nitekim fail veya mağdur, fiziki delilleri soruşturma ya da kovuşturma makamına sunamayacak ve kendi seçeceği bir bilirkişiye incelettiremeyecek durumdaysa, dijital delil anlamında böyle bir olanak mevcuttur. Örneğin, aleyhine delil olan bir bilgisayar disketi, zanlı tarafından başka bir bilirkişi tarafından incelenebilir ve oradan elde edilen yeni bilgiler, zanlı lehine kullanılabilir (Akarslan 2012).

Dijital delil makul, açıklayıcı ve izah edilebilir olmalıdır. Bu sebeple tahminler ve zihin okuma araçları ile elde edilen elektronik veriler delil olarak kabul edilemez. Deli kişinin zekâsı, bilimsel olarak kabul edilebilir bir özellik taşımaktadır. Gerçek şu ki, bilimsel kanıtların, bilhassa bilgi sistemlerinden elde edilen elektronik kanıtlar için bir özelliği vardır. Adli tıp uzmanları bilgi sistemindeki verileri alıp analiz ederek suçla bağlantısını ortaya çıkarır. Bu bağlamda, bilirkişi olduğundan şüphelenilmeyen adli bilişim uzmanının dijital delil toplama ve yorumlama yöntemi mahkemeyi etkilemekte ve karar verilmesine katkı sağlamaktadır. Adli tıp uzmanının delil toplama sürecini takip ederek elde ettiği deliller mahkemeyi bağlamamakla birlikte önemli gerçekleri ortaya çıkarması bakımından önemlidir (Değirmenci 2014).

Dijital delil bilimi, delil toplama sürecinde genel kabul görmüş yöntemlerin kullanılmasının yanında araştırmacıların dijital delil elde edebilmesi ile direk alakalıdır. Dijital delil toplayacak çalışanın, kolluk kuvvetinin ya da savcılık/mahkemenin atadığı bilirkişinin, sertifika ile desteklenen adli bilgileri anlayacak düzeyde olması gerekmektedir. Ancak, dijital delillerin bilimsel yöntemlerle toplanması, ispat değeri olması için gerekli değil, yeterli bir özelliktir. Bilimsel metotlarla elde edilmeyen dijital deliller, geçerliliği konusunda şüphe uyandırmaktadır. Yargı makamları bu tür delilleri kabul ederken dikkatli olmalı, varsa bilirkişi raporlarının ilmi araştırılmalı, delil elde etmek için kullanılan bilimsel/teknik araçlar belirlenmeli ve bu araçların güvenilir kabul edilip edilmediği belirtilmelidir (Sarsıkoğlu 2015).

Ceza yargılaması açısından delillerin en önemli özelliği olan “hukuka uygun elde edilmiş olma” sorunu dijital deliller için de büyük önem arz etmektedir. Nitekim dijital delillerin hassas yapısı, toplu tespit imkânı ve elektronik toplumsal yaşamın gereği olarak dijital delillerin ceza yargılamalarında kullanılması gerekliliği, kişisel bilgilerin gizliliği ve kişisel bilgilerin ifşası gibi bazı hak ihlallerine sebep olabilecektir. Bu itibarla elde edilen dijital delillerin hukuka aykırılığı, kanun değişikliği yapıldığında, belirtilen şartlara uyulmaması veya bahsi geçen şartların sınırlarının aşılması halinde ortaya çıkacaktır. Bu durumda dijital delillerin hukuki değerinden bahsetmeden geçmek mümkün değildir.

Elektronik imza bilgisi

Dünyanın pek çok ülkesindeki kanun koyucular, belirli kanuni koşulları sağlayan elektronik imzaların delil niteliğini düzenlemişlerdir. Türkiye’de 5070 Sayılı Elektronik İmza Kanunu, Elektronik İmza Kanunu’nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmzaya İlişkin Süreç ve Teknik Kriterler Hakkında Duyuru ve Elektronik İmzaya İlişkin Diğer Yönetmelikler gibi elektronik imzaların taşıması gereken

standartlar gibi düzenlemeler bulunmakta ve geçerliliklerinin kabul edilmesi için gerekli koşullar belirlenmiştir.



Şekil 28. Elektronik imza

Dijital imza, bir belgeye gömülü olan elektronik parmak izi sürümünüzdür. Süreç, benzersiz bir dijital sertifika oluşturmak için imzayı şifreleyen bir algoritma içermektedir. E-imza olarak da bilinen elektronik imza, belgelerinizi dijital olarak imzalamanın etkili bir yoludur. Dijital belgeler üzerinde onay veya rıza almak yasal olarak geçerli bir yöntemdir. Elektronik imza, fiziksel imzanızın kullanılacağı her durumda kullanılabilir ve imzanızın çevrimiçi eşdeğeridir.

Dijital imzalar, veri bütünlüğünü, doğrulamayı, kimlik doğrulamayı ve reddedilmemeyi sağlamaktadır. Öte yandan, dijital imza araçları, gerekli verileri dijital imza ile imzalamanızı sağlamakta olan yazılım ya da donanımlardır. Bir dijital imza aracının güvenli sayılabilmesi için ürettiği dijital imza oluşturma verilerinin kendi aralarında kopyalanmaması, içinde saklanan dijital imza oluşturma verilerinin her koşulda araçtan dışarı çıkamaması ve güvenliğinin garanti altına alınmış olması ve dijital imzayı oluşturan veriler, üçüncü şahıslar tarafından elde edilemeyecek bir yerde saklanmaktadır. Dijital imza kullanılmaz ve kurcalamaya karşı korunur, imzalanan veriler yalnızca imzalayan tarafından değiştirilebilir ve imzalayan, imza oluşturulmadan önce bu verileri görebilmektedir.

Kanunlarımıza göre elektronik imzalar, elle atılan imzalarla aynı hukuki neticeleri doğurmaktadır. Ancak, kanunen özel bir şekle ya da törensel şekle tabi olan hukuki işlemler ve kefalet sözleşmeleri, güvenli elektronik imza kullanılarak gerçekleştirilemez. Elektronik imza; kamu kurumları, yargı sistemleri, kurumlar arası iletişim, vergi işlemleri, elektronik oylama, internet bankacılığı, sigortacılık hizmetleri, satış elektroniği ve daha birçok alanda

başvurularda kullanılmaktadır. Elektronik imza için gerekli olan sertifikalar, ancak Telekomünikasyon Kurumu tarafından yetkilendirilen kamu kurum ve kuruluşları ile özel gerçek veya tüzel kişiler tarafından dağıtılabilmektedir.

Taşınabilir elektronik imza (veya kısaca mobil imza), bir mobil cihaz ile oluşturulan elektronik imza olarak tanımlanabilmektedir. Mobil dijital imza ile dijital imza arasındaki fark, dijital imzanın oluşturulması için yüklenmesi gereken sertifikayı içeren SIM kartın, operatör üzerinden iletişime olanak sağlayan 128K 4G LTE SIM kart ile birleştirilmesi ve imzanın bir operatörden yapılmasıdır. Elektronik imza mevzuatı taşınabilir elektronik imzaları da kapsadığından taşınabilir elektronik imzalar da elektronik ortamda güvenli dijital imzaların sağladığı hukuki geçerliliği sağlamaktadır.

Tüm bu açıklamalar bağlamında, dijital imzaya sahip dosyaların ya da dijital imza ile oluşturulmuş olan kayıtların dijital delil teşkil edebileceği kesindir. Ancak dosyadaki dijital imzanın geçerliliği ve imzanın nitelikli bir elektronik sertifika veya dijital imzanın zaman damgası kullanılarak üretilip üretilmediği doğrulanmalıdır. Bir dosyayı dijital imzayla imzalarken, imzalama araçları imzalandıktan sonra nitelikli sertifikanın geçerliliğini kontrol etmektedir. Bu sertifikaların süresi dolduğundan, hala sona erme riski altındadır. Ek olarak, kullanılan imza algoritmasının değiştirilmesi, sertifikanın yeniden dağıtılmasına ve eski algoritma kullanılarak sertifikanın geçersiz kılınmasına neden olabilmektedir. Bu gibi durumlarda, dijital imzaların verilmesini önlemek için imza araçları, bir internet bağlantısı aracılığıyla sertifikanın geçerliliğini kontrol etmektedir. Elektronik sertifika hizmet sağlayıcıları dağıttıkları dijital imzaların geçerlilik ve iptal bilgilerini sertifika iptal listesinde (SİL-Sertifika İptal Listesi) ve sertifika durum protokolü sunucularında, Çevrimiçi Sertifika Durum Protokolü (OCSP) üzerinde tutarlar. Araçlar, imzalama için kullanılan sertifikanın CRL'de kayıtlı olup olmadığını ve OCSP sunucusundan sertifikanın geçerliliği hakkında bilgi isteyip istemediğini soran istekleri bu sunuculara depolar. Bu sunucular, istenen bilgileri imzalama motoruna geri gönderir ve son olarak, imza geçerliyse imzalama yürütülür, aksi takdirde imzalama başarısız olur. Sertifika doğrulaması da benzer şekilde yapılır. Bu işlemler internet üzerinden yapıldığından giriş yapılırken ve ödeme yapılırken internet bağlantısı gerekmektedir. Aksi halde imza gerçekleşmez veya geçerli bir dijital imza ile imzalanan dosyadaki imzanın geçersiz olduğu sonucuna varmak yanlış olabilir.

Ek olarak, dijital olarak imzalarken imzalama zamanı olarak sistem saatini kullanmanın, veri imzalama tarihinin ileri ya da geri olma riskini beraberinde getirdiğini, bu nedenle dijital imza araçlarının sertifika hizmet sağlayıcıları tarafından alınan imzalara zaman damgaları ekleyeceğini hemen belirtmeliyiz. Bu sayede imza zamanı, imzalayan tarafından

kullanılan sistem saatinden bağımsızdır. Bu süre, verilerin ne zaman oluşturulduğunu belirlemede de önemlidir (Topcan 2011).

Karma İşlevi (Hash Function) bilgisi

Verilerin bütünlüğünü kontrol etmek için kullanılan tek yönlü bir hashing algoritması olarak da tanımlanabilen karma işlevi, adli soruşturmada uygulanmakta olan yöntemlerin ispatı değiştirmediğini göstermek için kullanılmaktadır (Şekil 29).



Şekil 29. Hashing algoritması

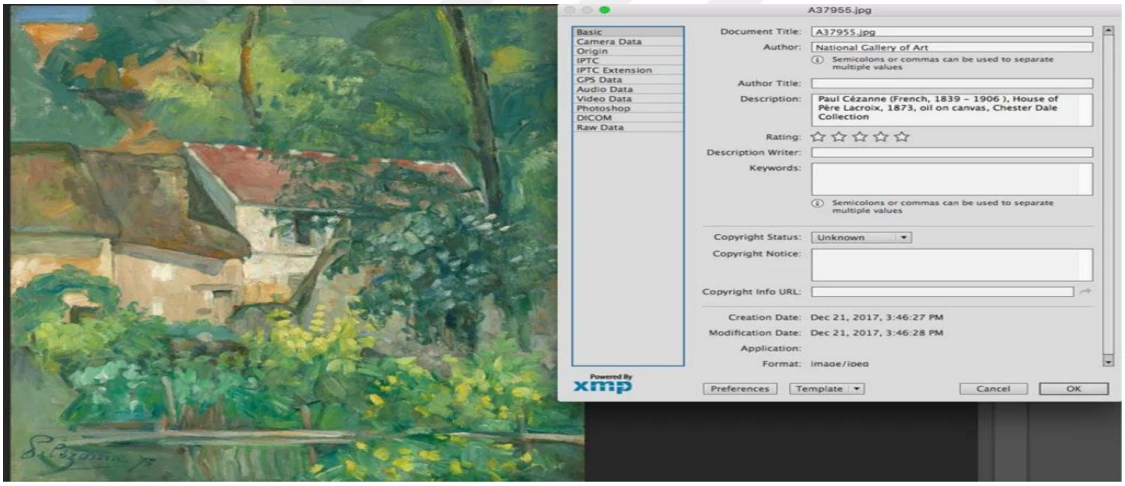
Dijital kanıtın tüm '0'ları ve '1'lerinin belirli bir algoritma ile birlikte işlenmesiyle elde edilen bu değer, veriler üzerinde gerçekleştirilen tespit edilen en küçük değişikliklerin bile ortaya çıkarılmasında faydalıdır. Bilgi karma, dijital kanıtın değerini belirlemek için mevcut teknolojide en sık kullanılan tekniklerden biridir. Bununla birlikte, hash bilgisinin, dijital veri ilk defa ortaya çıkana kadar değişimi temsil etmediğine dikkat edilmelidir. Ancak hash alındıktan sonra dijital verilerin çalışır durumda olup olmadığı ile mahkemeye ya da adli nüshaya sunulan durum arasında bir değişiklik olup olmadığı belirtilecektir. Özetle hash bilgisi, dijital veri elde edildikten sonraki süreçte herhangi bir değişiklik olup olmadığını gösterir. Örneğin, bu bilgi, sisteme eklenen verilerin alınmadan hemen önce algılanması için yararlı değildir. Bu sebeple hash bilgisi tek başına yüzde yüz güvenilir olmamalı, ileride ele alınacak dijital delil toplama adımlarında bir bütün olarak değerlendirilmesi gerekmektedir.

Süreç bilgisi

Süreç bilgisi, delillerin ilk elde edildiği andan, mahkemeye sunulması anına kadar geçen zaman içerisinde kaç kez el değiştirdiğinin, tarihlerle ve kişilerin kimlikleri ile tespit edilip kayıt altına alınmasıdır. Delil zinciri de denilen süreç bilgisi, dijital delil ile kurulan tüm temasların kaydedilmesi sayesinde tüm sürecin izlenmesine imkân sağlamakta ancak bu kayıtların insan eliyle tutulması süreç bilgisine şüpheci yaklaşılmasına sebep olmakta bu yönüyle de süreç bilgisinin geçerliliği eleştirilmektedir (Topaloğlu vd 2014).

Üst veri bilgisi

Meta veri veya gömülü veri olarak da bilinen meta veri bilgisi, kullanıcı tarafından doğrudan görülemeyen ancak ilgili olduğu veri hakkında ek bilgi sağlayan verilerdir. Fotoğrafın çekildiği tarih, fotoğrafı çeken kameranın marka ve modeli, fotoğraf verisine gömülü GPS bilgisi, e-postayı gönderirken izlenen yol ve veriyi oluşturan bilgisayar gibi bilgiler meta veri olarak kabul edilir (Şekil 30). Meta veriler üç kategoriye ayrılabilir: kapalı meta veriler, açık meta veriler ve türetilmiş meta veriler. Kapalı meta veriler, sayısal verilerin kendisinde bulunan ve talep üzerine değiştirilemeyen meta verilerdir. Verinin doğası gereği oluşturulmuş sistemlerdir. En önemli üst veri bilgilerinden biri Zaman damgasıdır. Zaman damgası, bir elektronik verinin üretildiği, değiştirildiği, ne zaman gönderilip alındığını, ne zaman kaydedildiği vb. bilgilerin zamanının tespit edilmesini sağlayan elektronik verilerdir. Zaman damgasının bu özelliği, dijital delilin doğruluğunu ispatlama da ve delilin herhangi bir manipülasyona uğrayıp uğramadığını kanıtlamada çok önemli bir bilgi olarak karşımıza çıkmaktadır.



Şekil 30. Bir fotoğrafın gömülü meta verileri

Açık meta veriler, bireylerin ya da yazılımların verilere atadığı veya manuel olarak girilen değerleri içermektedir. Türev meta veri ise bağlı olduğu verinin içeriğinden elde edilen meta veridir. Elektronik verilerin geçerliliğini belirlemek için en yararlı meta veriler, kapatma meta verileridir. Elektronik kanıtın doğrulanmasına kendi katkılarını yaptıkları için daha önemlidir. Meta veri bilgilerinden, dosyayı en son düzenleyen en fazla on kullanıcıya ulaşılabilir. Bu bağlamda meta veri bilgisi, dijital kanıtın geçerliliğini kontrol etmeye yardımcı olabilecek bir göstergedir

İlişki bilgisi

Dijital delillerin toplanmasıyla beraber delillerin mülkiyeti ve suçla bağlantısı da ifşa edilmelidir. Bu bilgiyi elde etmek için suç mahalli, delili elde eden birim, delili saklayan birimin parmak izi, delilin ulaşım araçları ile ilişkisi, diğer bilgisayarlar, metadata arasında mantıksal bir ilişki kurmak gerekir. Delil bilgileri, delilin bulunduğu ortamdaki güvenlik kameralarından alınan kayıtlar ve delilin içeriği bu ilişkiyi açıklarken tanıkların ifadelerinden de yararlanmak mümkündür. İlişki bilgisi masum insanları korumak için de önemlidir. Bu nedenle delillerin bulunduğu birimlerin sahipleri ile doğrudan ilgili olunmamalı, elde edilen deliller ile ilişkisi şüpheye yer bırakmayacak biçimde açıklanmaya çalışılmalıdır. Ancak bu biçimde sunulan ilişki bilgilerinin, delillerin geçerliliği hakkında doğru sonuçlara yol açması mümkündür. Aynı bilgisayarı birden çok insanın kullanıyor olabileceğini düşündüğünüzde, ilişki bilgilerinin önemi daha da netleşir.

Dijital Delillerin Hukuka Uygunluk Bakımından Değeri

Ceza muhakemesi hukukunda belirli hususların, belirli bazı delillerle ispat edilmesi gibi bir zorunluluk bulunmamaktadır. Benzer şekilde delillerin ispat gücü bakımından da bir derecelendirme söz konusu olmamakla birlikte tüm deliller, delil değeri bakımından eşittir. Bu bağlamda bir nesnenin yahut açıklamanın delil olabilmesi bakımından, delil kurallarını sağlamasının yanında belirli bir hususu ispat bakımından hâkimde vicdani kanaat oluşturabilecek düzeyde olması önem arz etmektedir (Centel ve Zafer 2021).

Bu bakımdan öncelikli hedefin, maddi gerçeğin ortaya çıkarılması olduğu ceza muhakemesi hukukunda hâkim, taraflarca ileri sürülen delillerle bağlı olmayacak ve delil olarak kabul edilebilme kurallarını taşımaları koşuluyla her şeyi delil olarak kabul edilebilecek ve bu şekilde her şeyin, her şeyle ispatı mümkün olabilecektir. Elbette ki her şeyin delil olabileceği gerçeği, her şeyin muhakeme sürecinde ileri sürülebileceği, incelemeye sunulabileceği ve tartışılabileceği anlamlarına da gelecektir (Toroslu ve Feyzioğlu 2018).

Bu bağlamda ispat edilecek hususun, geçmişteki olaylara ilişkin olması ve bu olayların da ortaya çıkacağı zamanın ve şartların önceden bilinememesi, sonuç olarak da delillerin önceden hazırlanamayacak oluşu nedeniyle ceza muhakemesinde delil serbestisi ilkesi benimsenmiştir (Toroslu ve Feyzioğlu 2018).

Her olayın her delille ispatlanabilmesi olanağını sağlayan "vicdani delil sistemi"nden önce "kanuni delil sistemi"nin geçerli olduğu zamanlarda kişiler, yargılama konusu suçla ilgili kanunun aradığı delillerin bulunması durumunda, suçsuzluklarına inanılsa dahi mahkûm edilebiliyor yahut suçu işledikleri farklı delillerle ortaya konulmasına karşın kanunun aradığı

delillerin elde edilemeyişi sebebiyle beraat edebiliyorlardı. Örneğin zina ancak ikrar yahut belirli sayıda tanık beyanı ile ispat edilebilmekteydi. Bu sebeple zinaya yönelik ikrar yahut yeterli sayıda tanık beyanı elde edildiğinde hâkimin bunlara dayanarak karar verme ve sanığı mahkûm etme zorunluluğu bulunmaktaydı (Gedik 2019).

Günümüzde, henüz tam olarak bilimsel delil sistemine geçilmemekle birlikte kanuni delil sisteminin olumsuz sonuçlarını gidermek amacıyla ortaya çıkmış olan vicdani delil sistemi geçerlidir. Delillerin serbestliği ve delillerin serbest değerlendirilmesi ilkeleri, vicdani delil sistemi ile açıklanabilmektedir (Tezcan vd 2022).

Bununla birlikte delillerin serbestçe değerlendirilebilmesi hususu hâkimin keyfi bir şekilde hüküm tesis edebileceği anlamına gelmeyecektir. Söz konusu değerlendirme akla ve mantığa dayalı bir değerlendirme olarak gerçekleştirilmelidir. Ek olarak yukarıda bahsedilen ve bir şeyin delil olarak kabul edilebilmesi için gereken koşulların da taşınması gerekecektir (Centel ve Zafer 2021).

Gerçekleştirilen ceza muhakemesinin sonunda, yargılamaya konu fiilin sanık tarafından işlendiğinin veya işlenmediğinin sabit olduğu sonucuna varılamazsa sanık ilgili fiil sebebiyle mahkûm edilemeyecektir. Bu durum ise *şüpheden sanık yararlanır* ilkesi olarak anılmaktadır. Nitekim Yargıtay da şüpheden sanık yararlanır ilkesini şu ifadelerle açıklamaktadır;

"sanığın bir suçtan cezalandırılmasının temel koşulu, suçun kuşkuya yer vermeyen bir kesinlikle ispat edilmesine bağlıdır. Şüpheli ve aydınlatılamamış olaylar ve iddialar sanığın aleyhine yorumlanarak hüküm tesis edilemez. Ceza mahkûmiyeti bir ihtimale değil, kesin ve açık bir ispata dayanmalıdır."

Türk Hukukunda Dijital Delillere İlişkin Düzenlemeler

Türkiye'de ceza muhakemesi hukukunda delil hürriyeti olduğu söylenmektedir. Dolayısıyla mahkemede her türlü delilin sunulabileceği ve dolayısıyla mahkemede dijital delillerin kullanılabileceği söylenebilir. Ek olarak, 2014 yılında Siber Suçlar Sözleşmesi'nin (SSS) onaylanması nedeniyle, dijital delillerin toplanmasına ilişkin ulusal mevzuatın SSS ile uyumlu bir çerçevede gelişmeye devam edeceğini söylemek güvenlidir. Var olan durumda, SSS uyumunun tam olarak düzenlendiği söylenemezken, önemli düzenlemelerin olduğu da inkâr edilemez. Ancak, bu düzenlemelerin tam durumu açıklanmadan boşluğun nerede olduğunu tespit etmek mümkün olmayacaktır. Bu nedenle dijital delillere ilişkin düzenlemeler tek tek gözden geçirilecektir. Bu itibarla, her şeyden önce, delile ilişkin herhangi bir hükmün dijital delille de doğrudan ilgili olacağı söylenebilir.

CMK kapsamındaki düzenlemeler

Ceza yargılamasında dijital delillere ilişkin araştırma hükümleri bakımından ilk bakılması gereken kanun, Anayasa'dan sonra Türk Ceza Muhakemesi Hukukunun temel kaynağı olan Ceza Muhakemesi Kanunu (CMK)'dır. Bu nedenle, önce CMK kontrol edilecektir. Dijital delilin ne olduğu düşünüldüğünde, CMK 134'ün kanunun diğer hükümlerine göre daha dikkat çekici bir hüküm olduğunu belirtmek gerekir. Nitekim CMK 134 dışında sayılan yollarla da dijital olmayan delil elde edilebilirken, CMK 134 doğrudan dijital delil elde edilmesine yardımcı olan bir hükümdür. Bu hükümler dışındaki uygulamalarda özel kanunlar bulunmadığı sürece CMK genel hükümlerine başvurularak boşluklar doldurulacaktır. Ceza Muhakemeleri Usulü Kanunu (CMUK)'ta dijital delillere ilişkin hiçbir özel hüküm yürürlükten kaldırılmamıştır. Bu nedenle ortaya çıkan sorunlara genel düzenlemelere başvurularak çözüm aranmıştır. CMK taslak halindeyken bilgisayarla ilgili dijital delil yönetmeliği ihtiyacı doğmuş ve bununla ilgili bir madde CMK'da yer almıştır. Bilgisayarların, bilgisayar programlarının ve gazetelerin aranması, kopyalanması ve el koyması başlıklı CMK 134, esas taslakta belirtildiği üzere başlıkta belirtilen hususlara ilişkin arama ve el koyma tedbirinin özel bir halidir. Bu durumda, önce maddenin başlığı dikkate alınacaktır. Bu maddenin başlığı, bilgisayarları, bilgisayar programlarını ve dosyaları aramak, kopyalamak ve ele geçirmektir. Maddenin başlığından da anlaşılacağı gibi, maddenin içeriğinin tüm dijital kanıtları içermediği açıktır. Bildirinin başlığı ve içeriği sadece bilgisayarlar için belirtildiğinden konunun dar anlamıyla anlaşıldığında bu maddenin bilgisayar dışı cihazlara uygulanması mümkün olmayacaktır (Dülger 2014).

Bu sorun, kanunun veri odaklı değil bilişim odaklı olmasından kaynaklanmaktadır. Böyle bir durumda CMK 134 bilgisayar dışında herhangi bir cihaz üzerinde işlem yapmayacak ve bu cihazlar için dijital delil arama ve girme metotları genel yasalara göre uygulanacaktır. Dolayısıyla, bilgisayar dışı cihazlar gibi mükerrer tedbirler kullanılarak var olmayan bir düzenleme kapsamında tedbir alınmaya çalışılacağından, bu şekilde elde edilen dijital deliller açısından hukuka aykırılık oluşturmak mümkündür. Fakat genel olarak bakıldığında bilgisayar dışındaki araçlar için CMK 134 hükümlerinin tam olarak uygulandığı görülmektedir (Tanrıkulu 2014).

Ayrıca CMK 116-123 genel hükümlerine göre bilgisayarların, bilgisayar programlarının ve logların aranması ve bunlara el konulması yapılamaz. Bu tür aramalarda CMK 134 çerçevesinde alınan kararların da bulunması gerekmektedir (Dülger 2014).

Maddenin ilk fıkrasının içeriği ise şu şekildedir: “Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette

delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir."

İçerikten de anlaşılacağı üzere bilgisayar, bilgisayar programı ve bilgisayar loglarının aranması ancak inceleme safhasında yapılabilecek gibi görünmektedir. Ayrıca yazıda sanıktan bahsedilmeden tek sanıktan bahsedilmesi de bu izlenimi pekiştirmektedir. Edebi yorumun tercih edildiği bu durumda sanki kovuşturma aşamasında araştırma yapılamaz gibidir (Centel ve Zafer 2021).

Ayrıca yazının ilerleyen kısımlarında da değinildiği üzere suç kategorisi bulunmamaktadır. Bu sebeple, bu maddenin herhangi bir suç soruşturmasında kullanılması mümkündür. Ancak taslakta yer alan bu hükmün dayanağı açıklanırken, bu hükmün iki sene ya da daha çok hapis cezası gerektiren suçlara uygulanması önerilmektedir. Ayrıca bu tedbirin uygulanmasını isteyebilmek için somut delillere dayalı sağlam şüphenin bulunması gerekir. Getirilen bu yeni şartla, özel deliller toplanmadan bu yöntemin bir ceza soruşturmasında uygulanamayacağı hükme bağlanmıştır. Yani tutuklamada olduğu gibi bu tedbirin getirilmesi zorlaşmış ve daha katı bir şart olan kuvvetli şüphenin bulunması zorunlu hale getirilmiştir. Bu tedbirin alınması için gerekli diğer bir şart da başka bir şekilde delil toplanamamasıdır. Hatta son çare ve gerekli bir koşul olarak da bilinen bu şartın bulunmasının özellikle zor olduğuna dikkat çekilmektedir. Dijital delillerin geleneksel delillere göre değiştirilmesi, bozulması ve yok edilmesi daha kolay olduğundan ve kolayca tahrif edilebildiğinden, başka yollarla delil elde etmeye çalıştıktan sonra dijital kanıtın son çare olarak kullanılması gecikmiş bir önlem olur ve bu da faillere ulaşabilmek amacıyla delilleri zorlaştırır (Dülger 2014).

Bunların yanı sıra şüphelinin kullanmış olduğu ifade de maddede yer almaktadır. Bu temelde arama ve kopyalamanın yapılacağı elektronik cihazların mutlaka şüpheliye ait olmadığı söylenebilmektedir (Dülger 2014). Dolayısıyla zanlının mal sahibi olması şart değildir, yalnız kullanması yeterlidir. Bu nedenle, üçüncü taraf bilgisayarların tetikte olması gerekebilir. Aslında zanlının kullandığı, kısıtlama oluşturan ve zanlının delillere ulaşmak için kullanmadığı bilgisayarların düzenlenmesi gerekmektedir.

Bu yöntemin bir diğer özelliği de savcının talebi ve hakim kararı olmadan uygulanamamasıdır. Yani bu önlem alınırken herhangi bir tatsız gecikmenin varlığı dikkate alınmamıştır Dolayısıyla bu tedbir için hakim kararı gerekli hale gelmiştir. Ancak aramanın sonuç vermemesi, yani verinin yapısından dolayı arama sürecinde engeller olması durumunda

bu engellerin aşılması için bilgisayar çalışması gerekmektedir. Bu gibi haller için maddenin ikinci fıkrası hükmü getirilmiştir.

Maddenin ikinci fıkrasının içeriği şu şekildedir: "Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilir."

Burada dikkat edilmesi gereken ilk nokta, bilgisayar müsadere eyleminin ancak şifrenin çözülememesi veya gizli bilgilere ulaşılamaması nedeniyle bilgisayar, bilgisayar programları ve bilgisayar günlüklerine ulaşılamaması halinde talep edilebileceğidir. Sonuçlara göre, bilgisayara ancak bu koşullar altında el konulabileceği düşünülebilir. Bu şekilde kanun, şifrenin çözülemediği veya gizli bilgilere ulaşılamadığı haller dışında, olay mahallinde de bir suretinin isteneceğini öngörmüştür. Ancak, bir bilgisayarı adli bilişim laboratuvarında test etmek sadece şifrenin kırılamadığı veya gizli bilgilere ulaşılamadığı durumlarda değil, ileri test gerektiren her durumda da mümkündür.

İkinci fıkranın son cümlesinde ise, el konulan ve şifresi çözülerek gerekli nüshaları elde edilen cihazların derhal iade edilmesi gerektiği belirtilmektedir. Bir yandan, burada gecikmesiz hüküm büyük bir belirsizlik oluşturmaktadır. Geribildirim düzenlemesinin yanlış sonuçlara yol açabilecek tek sonuç olduğu açıktır. Örneğin, suç verileri içeren cihazlarda bulunan verilere erişimin engellenmesi veya bu tür verilerin imhasına yönelik hükümlerin bulunmaması önemli bir eksikliktir. Ayrıca makale içeriğini deşifre edemeyen cihazların iade edilmeyeceği kanaatine varılmıştır. Böyle bir durumda mülkiyet hakkının ihlali yolu açılmıştır. Maddenin üçüncü fıkrasının içeriği şöyledir:

"Bilgisayar veya bilgisayar günlüğü girişi sırasında, tüm sistem verileri kaydedilir."

Bu paragrafta ortaya konulan sorunun algılanması, delillerin doğruluğunun ve bütünlüğünün sağlanması açısından makul görünmektedir. Aslında, test yedeklerle yapılırsa orijinal verilerin bozulması önlenebilir. Ayrıca veri içeren bir cihazın fotoğrafının çekilmesi, hash elde edilmesi gibi yedekleme sağlayan tüm işlemlerin şüpheli veya vekilinin gözü önünde yapılması gerekmektedir. Aksi takdirde, sistem verilerinin değiştirildiğini belirten bir mesaj görünecektir (Centel ve Zafer 2021).

Maddenin dördüncü fıkrasının içeriği ise şu şekildedir: "Üçüncü fıkraya göre alınan, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır."

Bu fıkranın değişiklikten önceki versiyonu haklı olarak eleştirilmiştir. Yapılan değişiklikle bir nüshanın şüpheliye veya avukatına verilmesi seçeneği ortadan kaldırılarak zorunlu hale getirildi. Böylece, yedeklenmiş bir sistemdeki verileri değiştirdiği iddia edilen bir bilgi olması durumunda, şüpheli veya savunmaya verilen yedek ile elde edildiği iddia edilen kopya arasında karşılaştırma yapılabilmektedir. Ancak bu aşamada, suç verilerinin şüpheliye iade edilmesinin doğruluğu başka bir tartışma konusu olacaktır.

Maddenin beşinci ve son fıkrasının içeriği ise şu şekildedir: "Bilgisayar veya bilgisayar kütüklerine el koymaksızın da sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır."

Bu fıkrada, ilgili verilerin müsadere olmaksızın çoğaltılabileceği belirtilmiştir. Ancak, kopyalanan verilerin kâğıda kaydedilebileceği ve dakikalar içinde kaydedilebileceği daha da açıklığa kavuşturulmuştur. Ancak, bu hüküm yalnızca az yer kaplayan içerik veya harf ve rakam gibi kâğıt üzerine yazılabilen bazı içerikler için geçerli olabilir. Örneğin, bir videoyu kâğıda yazdıramazsınız. Ayrıca yazılı içeriği aktarmak kadar mantıklı olmayan modası geçmiş bir yöntem çok yer kaplar ve milyonlarca sayfa içerebilir (Tanrıkulu 2014). Genel olarak, CMK 134'ün içeriğine bakıldığında, ölçümün yalnızca beklemede bulunan depolanmış bilgisayar verileriyle ilgili olduğu görülecektir. Ancak dijital ispatın temel değeri olan veri bu durumda her zaman mevcut değildir. Bu nedenle CMK 134, verilerin hareket halinde olduğu, yani gerçek zamanlı bir akışta olduğu durumları karşılayamaz. Türk hukukundaki bu boşluk, CMK 135 ile getirilen medya denetimleri ile doldurulmaktadır.

CMK 135'te temas tespiti, telefon dinleme ve iletişimlerin kaydedilmesi, sinyal bilgilerinin değerlendirilmesi gibi önlemler bulunmaktadır. Yazıdaki bir diğer önlem olan cep telefonu konum tespiti ise sadece fotoğraf amaçlı yapılabiliyor. Dolayısıyla bu ölçümle kanıt elde edilemez. Ayrıca tanımlar incelendiğinde, saklanan veriler üzerinde iletişim dinleme ve kaydetmeye ek olarak ölçümlerin yapıldığı, bu nedenle sadece dinleme ve kaydetme ölçümlerinin mevcut olduğu söylenebilir.

CMK 135 içerisinde bahsedilen tedbirlerin uygulamasının nasıl gerçekleşeceği CMK içerisinde düzenlenmemiştir. Bu konudaki düzenleme de 5397 sayılı kanun tarafından getirilen "5271 sayılı Kanunun 135 inci maddesi kapsamında yapılacak dinlemeler, Telekomünikasyon Kurumu bünyesinde, Kurum başkanına doğrudan bağlı "Telekomünikasyon İletişim Başkanlığı" adıyla kurulan tek bir merkezden yürütülür." hükmünün, şu anda (2559 sayılı Polis Vazife Salahiyet Kanunu) PVSK ek 7/10 olarak adlandırılan hükmü içerisinde bulunmaktadır. Kanun hükmünde kullanılan dinlemeler

kelimesi yerine tedbirlerin açık bir şekilde tek tek yazılması kanun yapma tekniği açısından daha doğrudur.

Maddenin arama ve el koymayı ilgilen birinci fıkrası şu şekildedir: “Arama veya elkoyma koruma tedbirlerinin uygulanması sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ancak, diğer bir suçun işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhâl bildirilir.”

Görüldüğü üzere, arama ve el koyma tedbirlerinin uygulanması sırasında başka bir suçun işlendiğine dair şüphe uyandıran deliller arızi delil kapsamına alınacaktır. Bu kapsamdaki deliller saklanacak ve durum savcılığa bildirilecek. Bu maddenin "Arama ve el koyma önlemleri uygulanırken" bölümündeki ifade dar olarak yorumlanmamalıdır. Aksi takdirde, yalnızca genel arama ve el koyma kararları uygulanacaktır. Ancak bu yazıda CMK 134 kapsamındaki aramalar da arama ve el koyma tedbirine dahil edilecektir (Yaşar ve Dursun 2013).

Maddenin ikinci fıkrası ise şöyledir:

“Telekomünikasyon yoluyla yapılan haberleşmelerin incelenmesi sırasında, bir delil soruşturma veya devam eden yargılama ile ilgili değilse ve 135 inci maddenin altıncı fıkrasında sayılan suçlardan yalnızca birinin işlenmiş olduğuna dair şüphe uyandırıyorsa; bu deliller koruma altında toplanır ve durum derhal savcılığa bildirilir.”

CMK 135 kapsamındaki iletişim kontrollerinin uygulanması sırasında bu kez tesadüfen elde edilen deliller üzerinde fikir birliğine varıldığı görülse de bu kez bir önceki paragraftan farklı olarak sorgulanması gereken bir sınırlama getirilmiştir. CMK 135'te listelenen suçlardan biri işlenmiş, tesadüfen ve bu sınırlamaya uygun olarak elde edilen deliller alıkonulacak ve savcıya bilgi verilecektir.

ARAŞTIRMA BULGULARI ve TARTIŞMA

Çağımızda, bilgi ve teknolojideki gelişmeler, dijitalleşmeye bağlı olarak yeni bir devrim yaratmaktadır. We Are Social'ın Digital 2024 raporuna göre dünya, günlük kullanıcı başına ortalama 400 dakika interneti kullanarak toplam 780 trilyon dakika harcıyor. Türkiye'de internet kullanılarak geçirilen süre incelendiğinde 6 saat 57 dakikayla dünya sıralamasında 20. sırada yer alıyor. Bu rakam dünya ortalamasının 17 dakika üzerindedir. Gün geçtikçe küreselleşen dünyada sınırlar ortadan kalkmış, daha fazla zaman geçirdiğimiz ve muazzam bir bilgi akışının olduğu sanal bir dünya ortaya çıkmıştır. Dijital dünyada bu kadar fazla süre geçirilmesi siber saldırılara maruz kalma riskinin artmasını da beraberinde getirmiştir.

Türkiye'de 4.5G ile ulaşılan daha hızlı mobil internet hizmeti, kullanımı da artırmıştır. 2022 yılı Eylül ayı itibariyle bir önceki yılın aynı dönemine göre aylık ortalama mobil kullanım %31 artışla 14,8 Gigabaytı, sabit internette ortalama aylık kullanım ise %18,1 artışla 243 Gigabaytı bulmuştur (BTK 2022). Dünyada her an internet kullanımı artmakta olup, akıllı mobil cihazlar aracılığıyla internete erişim yaygınlaşmakta ve internet erişim için öncelikli hal almaktadır.

2019 yılından itibaren tüm dünyada etkisi gösteren, dünya ekonomisini olumsuz etkileyen pandemi, ülkelerin uyguladığı pandemi kuralları çerçevesinde insanların hayat tarzlarında önemli değişikliklere sebep olmuş, özellikle insanların evlerinde daha fazla vakit geçirmesi dijital devrimi daha da hızlandırmıştır.

Büyük veri çağı olarak adlandırılan bu dönemde hayatımızın her alanına nüfuz eden teknoloji, bu ortamlarda yaptığımız her işlemi kayıt altına almaktadır. Teknolojinin hayatımıza getirdiği yenilikler ve kolaylıkların yanında birçok riskide beraberinde getirmiş, kötü niyetli kişilerin suç işleyerek belli menfaatler elde etmesine ve mağduriyetlerin yaşanmasına yol açmıştır. Hızla gelişen bilişim dünyası, suç ve suçlu için bir kaynak olmuştur. Bu bilimsel gelişme bir yandan bilgiye erişimi hızlandırıp verimliliği artırırken diğer taraftan yasa dışı faaliyetleri ve suç unsuru içermekte olan her türlü bilgi ve belgenin önüne geçerek belgenin sanal ortama aktarılmasını mümkün kılmıştır.

Teknoloji geliştiricileri tarafından insanlığın hizmetine sunulan yeni ürünlerin artması, insanların bireysel ve toplumsal hayatında köklü ve evrensel değişimlere yol açan bilişim

teknolojilerinin yarattığı bu yeni dünya düzeni, bilişim sistemleri üzerinden işlenen suçlarında çeşitliliğini arttırmış, bu yeniliklere paralel olarak suçla mücadele de yeni yöntemlerin keşfedilerek suçla daha etkin mücadele edilmesini elzem hale getirmiştir.

Yapay zeka, nesnelerin interneti, bulut bilişim gibi yeni teknolojik alanların çeşitliliğinin artması ve internetin hemen her alanda kullanılabilir olması siber saldırıların yaygınlığını da arttırmaktadır. Türkiye Bilişim Derneği 2023 yılında 9 milyar verinin siber saldırıya uğradığını ve küresel ekonomilere maliyetinin 8 trilyon dolar olduğunu söylemektedir. Bu sebeple bilişim sistemleri üzerinden işlenen suçlarla mücadele edebilmek için yeni soruşturma yöntemlerinin geliştirilmesi, gelişen teknolojiye paralel olarak üretilen teknik cihazlarla bu mücadelenin desteklenmesi gerekmektedir.

İnternet ve elektronik cihazların kullanımının hızla artması, kullanılan teknolojik cihazların boyutlarının küçülürken veri kapasiteleri ve sayılarının ciddi oranda artmaya devam etmesi ve yukarıda bahsettiğimiz teknolojik devrimlerin neticesinde, bu sistemler üzerinde suç işlenmesini hızlandırması ve suç delillerinin önemli bir kısmının bilişim sistemleri üzerinde bulunması dijital verilerin keşfedilme ihtiyacını doğurmuş, en yaygın delil bulma yöntemi haline gelen adli bilişimin ortaya çıkarak çok önemli bir alan haline gelmesini sağlamıştır.

Adli bilişim, bir soruşturma kapsamında bilişim sistemlerinde bulunan dijital delile, ilk temas edildiği andan itibaren çeşitli bilimsel ve teknik yöntemler uygulanarak, suçla ilgili dijital delilin herhangi bir değişikliğe uğramadan, anlaşılır bir metin halinde yargı makamlarına sunulma anına kadar devam eden bir delil inceleme sürecini ifade etmektedir. Adli bilişim uygulamalarıyla ceza yargılamaları ve özel hukuk alanındaki ihtilaflarda, dijital veriler ile olay ve kullanıcı arasındaki bağlantı ortaya koyulmaktadır.

Adli bilişim süreci, klasik olay yeri inceleme sürecine benzemektedir. Bilişim sistemleri veya veri depolama cihazları üzerinden belirli teknikler kullanılarak elde edilen, görünmez nitelikteki dijital veriler, laboratuvar ortamında çözümlenerek anlaşılır ve görünür hale getirilir. Süreç içerisinde manipülasyona ya da tahribata uğrayıp uğramadığı tespit edilerek, soruşturma için kritik bilgiler bu süreç içerisinde tespit edilmektedir.

Adli bilişimin dijital delile ilk temas edildiği andan mahkemede delil olarak kabul edilmesine kadar ki sürecin bütünü olarak ifade edilmesi adli bilişimi bir disiplin haline getirmektedir. Delillerin toplanması, incelenmesi, analiz edilmesi ve raporlanması sürecinin ceza ve hukuk yargılamalarında kabul görmesi, adli bilişimi adli bilimlerin bir alt disiplini olduğunu ortaya koymaktadır.

Adli bilişimin teknik boyutu hukuki boyutuna göre daha ön plandadır. Bilişim sistemleri üzerindeki verilerin analiz edilerek hukuki delile dönüştürülme süreci, teknik bilgi gerektiren ve uzmanlık isteyen bir süreçtir. Aynı zamanda adli bilişim uygulamalarını sadece delil toplama ve raporlama süreci olarak ele almayıp bilişim sistemleri üzerinde yapılan sistematik ve kapsamlı bir inceleme süreci olarak değerlendirilmelidir. Ayrıca dijital delillerin hukuka uygun bir delil olarak kabul edilebilmeleri için dijital delil kavramının bilinmesi, dijital delilin adli prosedüre uygun olarak toplanması ve değerlendirilmesi gerekmektedir.

Günümüz teknolojisinde hemen hemen her suçun bilişim sistemleri aracılığıyla işlenebilir hale gelmesi, kağıt ve benzeri fiziki kanıtların dışında bilgisayarlardan ve bilişim sistemlerinden elde edilen dijital delillerin gün yüzüne çıkmasını ve hukuk sistemlerinde yer almasını sağlamıştır. Kısaca dijital delil, "Elektronik bir cihazda saklanan, alınan veya bu cihaz tarafından iletilen bir soruşturma için değerli bilgi ve verilerdir." Bu bağlamda dijital deliller, bilişim sistemleri kullanılarak işlenen suçların soruşturulmasında çok önemli bir unsur haline gelmiştir.

Teknolojik gelişmeler ve suç işlenmesinde bilişim sistemlerinin yoğun bir biçimde kullanılmaya başlanmasıyla birlikte, kağıt ve benzeri fiziki kanıtların dışında, bilişim sistemlerinde ve bunların parçalarında yapılan incelemelerle elde edilen dijital deliller gün yüzüne çıkmıştır. Kısaca dijital delil, "Elektronik bir cihazda saklanan, alınan veya bu cihaz tarafından iletilen bir soruşturma için değerli bilgi ve verilerdir."

Dijital deliller klasik delillerle karşılaştırıldığında daha hassas oldukları söylenebilir. Ceza yargılamalarında en çok kullanılan delil türü haline gelen dijital delil, hassas, kolayca değiştirilebilir ve silinebilir yapıdadır, değişiklik yapıldığında ilk anda fark edilmesi zordur, toplanması ve korunması aşamasında dahi bozulabilme ihtimaline sahiptir, yanlış müdahale nedeniyle deliller zarar görebileceği, yok edilebileceği veya değiştirilebileceği için delil bütünlüğü ilkesinin sağlanması ayrı bir önem arz etmektedir.

Bilişim sistemlerinde ürün çeşitliliğin artması nedeniyle dijital delil, sadece bilgisayar sistemlerinin veri depolama birimlerinde yer almamakta, çok değişik elektronik veri depolayan sistemlerde de bulunabilmektedir. Bu dijital delilin bilişim suçlarının yanı sıra klasik suçlar açısından da önemli bir yere sahip olmasına neden olmuştur. Depolama aygıtlarının delil saklama aracı olarak kullanıldığı klasik suçların soruşturmasında hayati öneme sahip olan bir dijital delilin usule uygun olmayan teknik, prensip ve yasal prosedürlere aykırı biçimde elde edilmesi önemli bir ispat aracının yok olmasına yol açabilecektir.

Adli bilişim açısından bakıldığında teknolojik ürün çeşitliliğin artmasıyla birlikte dijital verilerinde sayısı ve çeşitliliği de artmış, olay yerinde delil olabilecek dijital verinin

toplanması, tasnif edilmesi, paketlenmesi, laboratuvar ortamına gönderilmesi, incelenmesi analiz edilmesi ve raporlama işleminin yapılması, uzun zaman kayıpları ve maliyet oluşturmaya başlamıştır.

Dijital delillerin mahkemelerce delil vasfı taşıyabilmesi için yasal prosedürlere uygun bir şekilde toplanıp, muhafaza edilmesi ve uygun koşullarda incelenerek dijital delillerin bütünlüğüne ve güvenirliliğine özen gösterilmesi gerekmektedir. Günümüzde pek çok soruşturma dosyasında dijital deliller yerini almış ve davanın seyrini değiştirebilmektedir.

Dijital deliller elektronik ve fiziksel olmak üzere iki şekilde korunabilmektedir. Elektronik koruma, delillerin ilk alındığı andan itibaren değişmediğini, bütünlüğünün bozulmadığını ispatlayacak kriptografik işlemler sayesinde, fiziksel koruma ise, delillerin laboratuvara bozulmadan taşınması, mahkemeye sunulacağı ana kadar uygun ortamlarda saklanması ve yine mahkemeye götürülüş sırasında herhangi bir bozulmaya uğramamasını sağlayan tedbirler olarak ifade edilebilir.

Dijital delillerin yeniden ele alınabilirlik, kabul edilebilirlik, gerçeklik, bütünlük ve güvenilirlik gibi özelliklere sahip olması gerekmektedir. Dijital delillerin mahkemeye sunulmadan önce, olayla bağlantısı, gerçekliği ve özgünlüğünün tespit edilmesi hayati önem taşımaktadır.

Dijital deliller kolaylıkla manipüle edilebildiğinden, dijital delillerin toplanmasından yargı makamlarına sunulma anına kadar olan ki sürecin, sistemli, zamanında ve her işlemin kayıtlı olacak şekilde gerçekleştirilmesi yani sürecin her adımının kontrol edilebilir olması kanıt bütünlüğü ve güvenilirliği adına gereklidir, çünkü dijital delillerin yargıda kabul edilebilirliği büyük ölçüde delillerin gerçekliğine bağlıdır.

Ülkemizde adli bilişim uygulamaları en çok kolluk birimlerince uygulanmaktadır. Bu sebeple dijital delil elde edilebilmesi için adli bilişime hakim olan prensip ve prosedürlere uygun olarak bilişim sistemleri ve diğer cihazlara el konulması, yedeklemelerin yapılması, yedeklerin incelenmesi, mahkemeye sunulmak üzere rapor hazırlanması ve uygun şekilde paketlenmesi, taşınması ve saklanması en nihayetinde adli bilişim uzmanı tarafından incelenmesi gerekmektedir. Klasik ya da dijital fark etmeksizin hiçbir delil yasal prosedürlere uygun olarak elde edilmedikçe mahkemede delil olarak kabul edilemeyeceği için adli bilişim sürecinin usulüne uygun olarak yürütülmesi gerekmektedir.

Adli bilişim ilk yıllarında sadece bilgisayar ve donanımları üzerinden veri toplamak suretiyle yapılırken günümüzde mobil akıllı cihazlar, bulut bilişim, nesnelerin interneti başta olmak üzere geniş bir yelpazeye yayılmış bulunmaktadır. Bu durum klasik adli bilişim

yöntemlerinin farklı bir bakış açısına sahip olunmasını gerektirmektedir. Yeni teknolojik cihazlar üzerinde klasik adli bilişim yöntemlerinin uygulanması başta insan haklarıyla ilgili uluslararası sözleşmeler olmak üzere anayasa ve kanunlarca koruma altına alınmış temel hak ve hürriyetleri kullanılamaz hale getirebilmektedir.

İnsan Hakları Evrensel Beyannamesi'nin 12. maddesi ve BM Uluslararası Medeni ve Siyasi Haklar Sözleşmesi'nin 17. maddesi ile birlikte özel hayatın gizliliği ve kişisel verilerin korunması güvence altına alınmıştır. Usulüne uygun olarak imzalanmış uluslararası sözleşmeler kanun hükmünde sayılmaktadır. Hukuksuzluk kavramı bir bütün olduğundan bir kanuna göre hukuksuz sayılan şey başka bir kanuna göre değerlendirilemez. Tüm bu hususlar çerçevesinde dijital delillerin elde edilmesinde uyulacak kurallar Ceza Muhakemesi Kanunu ile düzenlenmiştir. CMK hükümlerine aykırı bir şekilde elde edilen dijital delillerin, delil niteliği kazanması mümkün olmayacaktır. Bu sebeple uluslararası sözleşmelere paralel olarak düzenlenmiş CMK hükümlerine uyulmaması, özel hayatın gizliliği ve kişisel verilerin korunması gibi evrensel insan hakları metinleriyle güvence altına alınmış ilkelerin ihlali sonucunu ortaya çıkarabilmektedir.

Avrupa Birliği'nin 24 Ekim 1995 tarihli ve 95/46/EC sayılı yönergesi uyarınca, dijital verilerin yalnız açıkça ve hukuka uygun olarak belirlenmiş bir amaç için toplanması ve işlenmesi yani illiyet bağının bulunması gerekmektedir. Ayrıca elde edilen verilerin saklama süresi de bu amaç doğrultusunda belirlenmelidir.

Adli Bilişim alanında tüm uygulayıcıların uyması gerekli olan ve kabul edilen bazı standartlar bulunmaktadır; Dijital delillerin tanımlanması, toplanması ve muhafazası için yol gösterici olan ISO/IEC 27037, soruşturmalarda uygun yöntem ve araçların kullanılması konusunda yol göstermek amacıyla oluşturulan ISO/IEC 27041, dijital delillerin sağlıklı ve kontrol edilebilir şekilde analizi ve yorumlanması konusunda ISO/IEC 27042, soruşturmalarda daha geniş bir perspektifle olay incelemesine ilişkin prensipler ortaya koyan ISO/IEC 27043, adli bilişim alanında elektronik keşifle ilgili standartları belirlemek üzere ISO/IEC 27050.

Adli bilişim uygulamaları yapılırken bu standartların ve uluslararası sözleşmelerin göz önünde bulundurularak temel hak ve özgürlükleri zedeleyecek yaklaşımlardan kaçınılması son derece önemlidir.

Bazı ülkeler spesifik dijital delil kanunları çıkarırken, bazı ülkeler kendi ceza muhakemesi kanunlarına birkaç madde ekleyerek bu problemi çözmeye çalışmaktadır. Türk Hukukunda bilişim sistemleriyle ilgili olarak suç soruşturmalarının ana kaynağını Ceza Muhakemesi Kanunu oluşturmaktadır. Ceza Muhakemesi Kanunu'nun 116. maddesinde

“Yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabilir.” şeklinde düzenlenmiştir. Eğer söz konusu yasal şart somut olayda mevcutsa bu durumda CMK m. 119’a göre arama kararı verilmesi gerekmektedir. Arama kararı verilebilmesinin şartları CMK m. 119. Maddesinde düzenlenmiştir.

Bilgisayarda Arama ve Elkoyma tedbirinin amacı, bilişim sistemlerinde bulunan dijital delillerin elde edilmesidir. Dijital delillerin hassas yapısı ve elde edilmesindeki zorluk, verilerin kolayca değiştirilip yok edilebilme ihtimali, uygulanan tedbirin ağırlığı gibi nedenler, bu tedbirin genel arama ve el koyma tedbirlerinden ayrılarak, ayrı bir hüküm ile düzenlenmesini gerektirmiştir. Ceza Kanunu'nun 134. maddesine göre, savcının talebi üzerine hâkimin, somut delillere dayanan kuvvetli şüpheye dayanarak suçu işleyen kişinin bilgisayar, bilgisayar dosyaları ve programlarının aranmasına ve bu takdirde bunlara el konulmasına karar vermesi gerekir. Bunları başka şekilde aramak mümkün değildir. Gecikmenin zararlı olduğu kaçınılmaz hallerde CMK 119'a göre savcının arama kararı yeterli, CMK 134'e göre ise hakimin kararı bağlayıcıdır. Dolayısıyla acil durumlarda dahi bu cihazlara el konulması ve incelenmesi için hâkim kararı alınması kanunen zorunlu olduğundan, suçluların adalet önüne çıkarılmasına yönelik hukuki tedbirler delillerin hukuki kalitesini güvence altına almaktadır.

Ceza Kanunu'nun 134. maddesi ve Yargıtay kararına göre, el konulan materyalin dijital verilerinin şüpheliyle birlikte birer kopyasının alınarak kendisine teslim edilmesi gerekmektedir. Bunun suç mahallinde yapılması mümkün değilse, el konulan malzemenin mühürlenmesi, mührün şüphelinin huzurunda açılması ve soruşturma yerinde fotoğrafının çekilmesi gerekmektedir. Bunun mümkün olmaması durumunda fotoğrafın, arama ve el koyma kararını veren hâkimin gözetiminde çekilmesi gerekmektedir. Bu süreçte davalıyı temsil eden müvekkilin hazır bulunması, dijital verilerin daha sonra değiştirilmesine yönelik itirazları engellemektedir. Ancak bazı durumlarda bilgisayar görüntülerinin alınmasının saatler alması bu uygulamanın ihtiyacı karşılayamayacağını göstermektedir.

Dijital delillere itirazların ana kaynağı, şüphelinin ele geçirilen dijital verilerin tamamını veya bir kısmını kabul etmemesi ve bu verilerin manipüle edildiğini, değiştirildiğini veya eklendiğini iddia etmesidir. Dolayısıyla arama ve el koymanın kanun koyucunun CMK 134. maddesinde öngördüğü süreler içerisinde gerçekleştirilmesi, arama ve elkoyma işlemlerinin yasal prosedürler çerçevesinde yürütülmesi ve yazma korumalı cihaz, hash fonksiyonu gibi işlemlerin mutlak suretle uygulanması tüm problemi çözer ve kötü kişi veya kişilerin delilleri saklamaya çalışmasını veya masum insanları suçlu göstermeye çalışmasını engeller.

Türk Ceza Mahkemesi Kanunu son 10 senede özellikle Ergenekon, Balyoz ve askeri casusluk davalarında dijital delillerin değerlendirilmesinde önemli sorunlar yaşamıştır. Ergenekon ve Balyoz davalarında müebbet hapis cezası alan sanıkların bilgisayarında yapılan işlemler ve dijital delil olarak ele geçirilen elektronik veriler, işlemin maddeye aykırı yapıldığı, delillerin değiştirildiği ya da eklendiği yönündeki itiraz nedeniyle suçlamalar düşürülmüş, 2015-2016'da sanıklar beraat etmiş ve tazminat kararları verilmiştir.

Dijital delillerin toplanması ve değerlendirilmesinin hukuki uygunluğunun yanı sıra, delilleri incelerken bilgi teknolojisi ve dijital adli tıp ilkelerine uymak da önemlidir. Ayrıca bilgisayar kullanımının değerlendirilmesi, failin psikolojisini değerlendirerek kriminolojik açıdan suçla ve faille ilgili olanın belirlenmesine yardımcı olmaktadır. Avukatların dijital adli bilimi yönetmesi gibi, kriminolojik değerlendirmeler ve bilgisayar uzmanları da verilerin doğruluğu hakkındaki şüpheleri ortadan kaldırmaktadır.

Adli Bilişim günümüzün suç olgusuna bakıldığında hayati bir öneme sahip olmuştur. Bu sebeple kolluk kuvvetleri, savcı, hâkim ve avukatlar bu alanda kendilerini geliştirmeli ve gerekli bilgi birikimine sahip olmalıdır. Bilişim teknolojisi her geçen gün değişen ve gelişen bir disiplindir. Kişi, kurum ve devletlerin yeniliklere kısa sürede uyum sağlaması gerekmektedir. Avukatların, savcıların, hakimlerin ve kolluk kuvvetlerinin dijital adli bilimin gelişimi ve dijital delillerin doğal yapıları konusunda ki bilgisi, bilimsel ve adil sonuçlara ulaşmak açısından önemlidir.

Uluslararası hukukta, dijital delillerin toplanmasında dikkat edilmesi gereken önemli hususlardan olan, kişisel verilerin korunması ilkesi ve mahremiyet hakkı düzenlenmiş olduğundan özellikle kolluk kuvvetlerinin delil toplama aşamasında bu hususlara son derece dikkat etmesi, adli bilişime egemen olan ilke ve prensipler ışığında hareket etmesi, adil yargılanma ve hukukun üstünlüğünün korunmasına yardımcı olacaktır.

Ülkemizde savcılık makamları suç türlerine göre belirli kategorilere ayrılmıştır. Gelişen çağın bir gereği olarak siber suçlar konusunda özel bir savcılık biriminin kurularak bu birimde görev alacak savcıların eğitilerek siber suça konu olan soruşturmaların bu savcılar vasıtasıyla yürütülmesi gerekmektedir.

Türk Ceza Hukukunda bilişim sitemleri üzerinden işlenen suç ve suç türlerinin artması bilişim teknolojileri konusunda uzmanlaşmış mahkemelerin oluşturulmasını zorunlu kılmaktadır. Siber suçlara özel mahkemelerin kurularak yargılamaların bu mahkemelerde iyi yetiştirilmiş hakimler vasıtasıyla yapılması, yargılamanın adil ve bilimsel ilkeler ışığında yapılarak hukukun üstünlüğünün korunmasını sağlayacaktır.

Ülkemizde adli bilişim alanında çalışacak yetişmiş insan gücü açığı oldukça fazladır. Bilişim suçlarıyla mücadelede hem adli tıp laboratuvarlarına hem de uzman personele ihtiyaç duyulmaktadır. Her ne kadar özel şirketler kurumsal açıdan personel yetiştirse de, adli bilişim alanında akademik anlamda yeteri kadar ilerleme sağlanamamıştır. Ülkemizde halihazırda lisans ve lisansüstü olmak üzere adli bilişim alanında eğitim veren üniversite sayısı oldukça azdır. Bu sebeple lisans, yüksek lisans ve doktora bölümleri açılmalı, öğrencilerin bu bölümleri tercih etmesi teşvik edilmeli, üniversitelerin ilgili bölümlerinin eğitim müfredatlarına adli bilişim alanında dersler eklenmelidir. Bu alanda devlet ve sivil toplum kuruluşlarının desteğiyle seminer ve konferanslar düzenlenmelidir.

Araştırma kapsamında dikkat edilmesi gereken bir diğer önemli husus da; İnternet ortamında yaygın olarak kullanılan Facebook, X (Twitter), Instagram, Skype, Youtube, Google gibi hosting firmalarının genel merkezleri Amerika Birleşik Devletleri'nde olması, ABD ve diğer ülkelerin iç hukukta ki farklılarının sebep olduğu bilgi paylaşımında yaşanılan sıkıntılardır. Dünya genelinde bilişim teknolojilerinde ürün geliştirme çalışmaları, ülkelerin siyasi amaçlarının veya politik güç savaşlarının gölgesinde kalmaktadır. Teknoloji geliştiren ülkelerin bu durumu diğer ülkeler üzerinde bir baskı unsuru olarak kullanması, siber güvenlik tehditlerine karşı uluslararası bir birlikteliği mümkün kılmamaktadır. Bu sebeple siber suçlarla ilgili olarak ülkelerin uluslararası standartların belirlenerek, dijital dünyada işlenen suçların soruşturulmasında bilgi paylaşımı mekanizmasının oluşturulması gerekmektedir.

Teknolojinin hayatımızın her hücresine nüfuz ettiği sanal bir dünyada yaşıyoruz. Bu sanal dünyada meydana gelen suçların soruşturulması için gerekli olan adli bilişimin uygulamalarının sağlıklı bir şekilde yürütülmesi için dinamik dijital dünyaya göre sıklıkla güncellenen yasa, yönetmelik veya standartlara ihtiyaç vardır. Verilerin doğruluğunu ve güvenilirliğini, yeni ürün, yazılım veya teknolojilerin günlük olarak tanıtılmasını, personelin seçimi ve yetkilendirilmesini, adli bilişim alanında çalışan çalışanların uzmanlaşmasını ve bilimin ışığında değerlendirilmesini sağlayacak şekilde adli analizlerde belli bir standardın belirlenmesi daha kaliteli sonuçların elde edilmesi sağlayacaktır.

Devletlerin, kurumların ve kişisel bilgilerin korunması için adli süreçlerin iyi anlaşılması gerekmektedir. Ayrıca bir suç işlendiğinde bu suçla ilgili karar verirken doğru kararı vermek büyük bir sorumluluk ve özen gerektirir. Bu çalışma kapsamında adli bilişim ve sayısal deliller ile ilgili yayınlanan ulusal ve uluslararası kitap, tez, makale, internet siteleri detaylı bir şekilde incelenerek literatür taraması yapılmış olup bu alanda fikir oluşturacak bir yaklaşım ortaya koymaya çalışılmıştır.

SONUÇ ve ÖNERİLER

Teknolojik gelişmeler bir taraftan bilgiye ulaşımın hız kazanmasını ve teknolojik üretkenliğin artmasını, diğer taraftan yasadışı faaliyetlerin ve suç faktörü her türdeki belgelerin ve bilgilerin dijital ortamda aktarılmasını sağlamıştır. Bunun haricinde dijital dünyanın kısa sürede önemli bir güç durumuna gelmesi, devlet politikalarını zayıflatmış, ekonomik ve siyasi yetersizliğin oluşmasına neden olmuştur. Sosyal platformlar aracılığı ile kişilerin haklarına saldırı gerçekleştirilmesi, özel yaşamın ihlali vb. çeşitli suç faktörünün de akıllı telefon ve bilgisayarlar ile işlenmesi, dijital deliller ve cihazların hukuk açısından geçerliliği ile ilgili uluslararası ve ulusal düzenlemelerin yapılmasını zorunlu duruma getirmiştir.

Suçun bilişim sistemleri kullanılarak işlenebilir olması nedeniyle ceza usul hukukunda kağıt delillerin yerini çoğunlukla dijital deliller almıştır. Bilgisayar ve benzeri cihazlardan toplanan ve dijital delil olarak adlandırılan bu delilleri tespit etmek ve toplamak son derece hassastır ve teknik uzmanlık gerektirir.

Dijital deliller doğası gereği karışık ve kaygan bir formda olup, işlenmesi zordur. Bu tür deliller genellikle dolaylı niteliktedir; ayrıca bilgisayar aktivitelerini bir bireye atfetmek zordur. Bu tür deliller kolayca manipüle edilebilir ve yok edilebilir.

Suçluların yeni teknolojileri kullanması bir zorluktur çünkü adli laboratuvarların da bu teknolojilerle başa çıkmak için aynı derecede güncel ve donanımlı olması gerekir. Bu nedenle, yeni zorluklarla başa çıkmak için düzenli güncellemeler gereklidir. Ancak, yeni teknolojik araçların temini uzun bir süreçtir çünkü farklı seviyelerde bürokratik kurum içi onayı gerektirir. Ayrıca, daha iyi bir soruşturma sağlamak için uzmanların kendilerini düzenli olarak güncellemeleri gereklidir. Araçların temini için bu tür protokollerin uygulanması, adli sürecin amacını bozar.

Delil toplama, sadece teknik bilgi birikimini değil; aynı zamanda delil ile ilgili yasaların da bilgisine sahip olmayı gerektirir. Bu yasaların ihlali, delilin teknik kalitesine ve sanığın suçunu kesin olarak ispatlamasına bakılmaksızın, delilin mahkemece geçersiz sayılmasına yol açabilir. Bilgisayar tabanlı delillerle ilgili her suç mahalli benzersiz zorluklar sunar ve dijital araştırmacılar, adli bilişim ilkelerini yeni durumlara yaratıcı bir şekilde adapte edebilmelidir. Aynı zamanda, soruşturma birimleri çeşitli suçların soruşturulmasıyla ilgili standart prosedürler geliştirmiştir. Bu tür prosedürler, delillerin tutarlı bir şekilde

toplanmasını, korunmasını ve analiz edilmesini sağlamak için adli bilimin temel ilkelerine uygun olmalıdır.

Dijital delillerin mahkemede kabul edilmemesinin başlıca nedenlerinden biri, genellikle kolluk kuvvetlerinin bilgisizliği nedeniyle kırılmış olan zincir idaresidir. Zincir idaresi, delilin bütünlüğünü korumak ve delilin güvenilir olduğunu, yani el konulmasından mahkemeye sunulana kadar müdahale edilmediğini sağlamak için gereklidir.

Siber suçlarla başa çıkmak için mevcut kaynaklar da çok sınırlıdır ve bu durum hızlı ve verimli soruşturmanın önünde bir engel teşkil eder. Örneğin, soruşturmanın bir kısmının uzak bir yerde yürütülmesi gerektiğinde mesafe kritik bir sorun haline gelir. Delil toplamak için bu yere ulaşmak zordur çünkü çoğu durumda kolluk kuvvetleri sıradan ulaşım araçlarını kullanır ve bu da süreci geciktirir. Bu nedenle, ilgili birimlere daha hızlı soruşturma için yeterli mali kaynak sağlanmalıdır.

Bilgisayarlar ve diğer dijital cihazlarla ilgili suçların doğası gereği küresel nitelikte olması nedeniyle, bu tür suçları soruşturma yetkisi büyük bir sorun haline gelmektedir. Suçlar siber uzayda işlendiğinde, suçta kullanılan elektronik cihazın sunucusu Türkiye'nin yargı yetkisinin ötesinde bulunabilir. Bir suçla ilgili olarak diğer ülkelerle ciddi işbirliği ve koordinasyon eksikliği nedeniyle birçok soruşturma tamamlanamamaktadır. Örneğin, Facebook, WhatsApp gibi platformlar, şiddet ve diğer suç teşkil eden faaliyetlere yol açan aktiviteler için kullanılabilinmektedir. Bu forumda paylaşılan mesajların uçtan uca şifrelenmesi nedeniyle, kolluk kuvvetleri de bu tür suçların soruşturmasını yaparken bu mesajlara erişemez. Sunucu ABD'de bulunduğundan, Türkiye'deki kolluk kuvvetleri WhatsApp sunucusunda bulunan bilgilere erişemez. Ancak, bu tür bilgiler yalnızca hizmet sağlayıcı/şirketin takdirine bağlı olarak paylaşılabilir. Bu durum, mesajların uçtan uca şifrelenmesiyle ilgili gizlilik sorunlarını da ihlal etmektedir. WhatsApp'ın sahte mesajları izlemek için bir altyapı kurma taleplerini reddettiğini ve bunu yapmanın uçtan uca şifrelemeyi bozacağını iddia ettiğini belirtmek gerekir. Soruşturma sürecini akamete uğratan bu tür sorunların çözümü için ilgili platformların ülke içinde temsilcilik açmasına ve yerel yasalara uygun, uluslararası standartlar ve temel insan haklarıyla uyumlu olacak şekilde işbirliği içerisinde bulunmasını sağlamak gerekmektedir.

İnternetin temel özelliklerinden biri, kullanıcıyı anonim tutma yeteneğidir; bu, failler için kimliklerini görünürde gizli tutabilecekleri için avantajlı olduğu düşünülmektedir. Siber uzaydaki herhangi bir faaliyetle ilgili olarak suçlunun kimliğinin gizli tutulması, herhangi bir kişinin kimliğinin belirlenmesi ve misilleme korkusu olmadan siber dünyada fikirlerini veya kişisel görüşlerini özgürce ifade edebilmesi nedeniyle, temel ifade özgürlüğü hakkını

güçlendirmiştir. Ne yazık ki, anonimlik, kolluk kuvvetlerinin yanı sıra siber suç mağdurları için de yeni zorluklar yaratmaktadır; zira bu tür eylemlerin arkasındaki kişilerin izini sürmek ve tespit etmek zor olacaktır.

Dijital delillerin dinamik yapısı, onları sadece bizim değil dünyadaki tüm hukuk sistemlerinde değişime ve gelişime açık bir hale getirmektedir. Yakın zamana kadar varlığı dahi bilinmeyen suç türlerinin günümüzde en fazla işlenen suçlar arasına girmesi, dijital dünyanın ve bu dünyada işlenmekte olan suçların toplum üzerinde yarattığı endişeyi her geçen gün arttırmakta, Ceza Muhakemesi Kanunu'nda dijital delillere ilişkin yeni düzenleme ve yaptırımların gerekliliğini her geçen gün daha fazla gündeme getirmektedir.

Bazı devletler dijital delillere yönelik özel yasalar çıkarmakta bazı devletlere de ceza muhakeme kanunlarına ekledikleri birtakım madde ile problemi çözmeye çalışmaktadır. Mahremiyet, özel hayatın gizliliği ve kişisel verilerin korunmasına ilişkin kurallara uyulmaması, evrensel insan hakları belgeleriyle güvence altına alınan ilkelerin ihlal edilmesine yol açabilmektedir. Bu sorunların çözümü için yasa koyucu bilişim suçları üzerinde çalışan özellikle avukatlar ve bilgi teknolojileri uzmanları, insan hakları savunucuları ve bu konudaki diğer hukuk uzmanlarıyla görüşmeli, kalkınma alanı da dahil olmak üzere bu hususlarla alakalı bütün yasal belgelerde, teknolojik ihtiyaçların karşılanması ve bireysel mahremiyetin sağlanması için acilen yeni düzenlemelerin geliştirilmesi gerekmektedir.

Siber suç oranındaki endişe verici artışa rağmen, mevcut personelin etkin bir soruşturma yapabilmesi için gerekli güç artırılmamıştır. Eğitim eksikliği, kolluk görevlilerinin herhangi bir suçu bilimsel olarak soruşturmasını da engeller. Bilimsel soruşturma teknikleriyle donatılması gereken "özel" departmanlar bile genellikle eski teknoloji ve tekniklerle doludur. Her ilçede siber hücreler kurulmamıştır. Mevcut birimlerde ciddi derecede eğitimli personel eksikliği bulunmaktadır. Ayrıca, siber adli laboratuvarların yetersizliği nedeniyle bu tür durumlarda adli uzmanların acil müdahalesi mümkün değildir. Kolluğun ilgili birimleri hariç diğer birimlerinde bilgisayar ile ilgili suçları ele alabilmeleri için yeterli eğitim verilmemektedir. Kolluk görevlileri geleneksel suçlarla uğraşırken bilgisayar tabanlı delilleri göz ardı etme eğiliminde olduğu görülmektedir. Çoğu durumda, kolluk güçlerinde bu tür suçlarla başa çıkmak için farkındalık ve hazırlık eksikliği bulunmaktadır. Bu sebeple ülke genelinde her il ve ilçede siber suçlarla ilgili birimler kurularak gerekli personel, donanım eksikliği giderilmeli, laboratuvarlar kurulmalı, tüm kolluk personeline eğitim verilmelidir.

Adli davaların uzun süre devam etmesi göz önünde bulundurulduğunda, adli laboratuvarlar, inceleme için korunan delillerin güvenli depolanması için yeterli korumaya sahip olmadığı görülmektedir. Dijital delillerin kırılgan yapısı aşırı sıcaklıklara, neme, fiziksel şoka, statik elektriğe ve elektromanyetik alanlara karşı oldukça hassastır. İlk müdahalede bulunan kişi, dijital delilleri belgelemek, fotoğraflamak, paketlemek, taşımak ve depolamak sırasında verileri değiştirmemek, zarar vermemek veya yok etmemek için önlemler almalıdır.

Devlet adli laboratuvarlarının aşırı yüklenmesi veya kaynak eksikliği nedeniyle, soruşturma birimleri adli inceleme için davaları özel adli laboratuvarlara devreder, burada sonuçların manipüle edilmesi veya değiştirilmesi olasılığı yüksektir. Bu tür durumlarda, ceza adalet sistemi amacını yitirmiş olur. Ayrıca, kolluk kuvvetlerinin hesap verebilirliği de tehlikeye girer. Çoğu adli laboratuvar işlevlerini yerine getirecek yeterli insan gücüne sahip değildir. Bu, laboratuvarlarda sonuçlandırılması gereken çok sayıda birikmiş dava bulunmasına ve davaların geç sonuçlandırılması, adaletin sağlanması amacını bozmaktadır. Adli uzmanlara göre, davaların %50'si uygun araç ve teknolojinin eksikliği nedeniyle beklemektedir. Ayrıca ülkemizde yeterli sayıda adli bilişim laboratuvarı olmaması sebebiyle, birçok dijital materyal posta yoluyla laboratuvar olan şehirlere gönderilmektedir. Bu durum inceleme süresini artırıp soruşturma hızını yavaşlatmaktadır. Bu sebeple adli bilişim uzmanı sayısının ve adli bilişim laboratuvar sayısın artırılmasına yönelik çalışmaların ivedilikle yapılması gerekmektedir.

Dijital delillerin güvenliğinin sağlanmasına yönelik teknik hususların madde kapsamına alınması gerekmektedir. İkinci ve en önemli görev ve sorumluluk kolluk görevlisine yani kolluk kuvvetine aittir. Bir ülkede kanunların uygulanması, hukukun üstünlüğü ve adaletin tecelli etmesi için temel yoldur. Bu konuyla ilgili olarak, belirli bir durumda sanığın ya da müdafinin size hatırlatma yapması beklenmemeli, kanunların öngördüğü hukuki prosedürlere harfiyen uyulmalı, uluslararası standartları titizlikle uygulamalı ve yetkilerini hukuka uygun olarak kullanmalıdır. İnsanlığın evrensel başarılarını kötüye kullanmamalı veya bunlara zarar verilmemelidir. Gerekirse şüpheliye karşı şüphelinin haklarını savunarak söz konusu işlemi yapmak gerekmektedir. Dünyanın en modern ve ileri teknolojisi ile uygun yasal belgeler hazırlanmış olsa bile, kötü uygulayıcıların elinde bunlar, açıkçası bu kağıt üzerinde yazılan anlamsız sözlerden öteye geçmeyecektir.

Son olarak adli bilişim ve dijital deliller artık sadece ulusal değil küresel güvenlik bakımından da hayati önem taşımaktadırlar. Adli Bilişim alanında bilgi birikimini, teknik donanım ve bilimsel çalışmalarını sürekli güncel tutan, gelişen teknolojiye paralel olacak

şekilde yenileyen ülkeler diğerlerinden bir adım önde olacak, uluslararası siber platformlarda dijital çağın en etkin söz sahipleri olarak yer alabileceklerdir.

Bu sebeple adli bilişime konu olan, dijital delil aramaları, elektronik keşif vb uygulamalar yapılırken yukarıda belirtilen uluslararası standartlar ve sözleşmeler göz önünde bulundurarak, insanlığın doğası olan temel hak ve özgürlüklerin zedelenmemesi gerekmektedir.

Demokratik ve hukuk devletinde bu tür problemlerin yaşanmaması adına öncelikle yasaların gelişim gösteren teknoloji doğrultusunda güncellenmesi hususunda geç kalınmaması gerekmektedir. İnsanların ev ve işyerlerinde yer alan ve yaşamın bir parçası durumuna gelen bilgisayar, tablet, akıllı telefon gibi teknolojik araçlar günlük olarak gerçekleştirilen çeşitli faaliyetlerin izlerini taşıyan önemli araçlardır. Bu tür teknolojik araçların dijital veriler ile çalışması doğrultusunda klasik delillere göre farklılık gösteren bir yapısının yer aldığı açıkça görülmektedir. Bu sebeple değerlendirme faaliyetlerinin adli bilişim uzmanlarınca gerçekleştirilmesi mecburidir. Bu cihazların yaşamımızın tüm alanında kullanılması, kişisel veriler içermesi ile beraber özel yaşamın gizliliği ve iletişim özgürlüğü bakımından el koyulması ve arama işlemlerinin de klasik suçlar doğrultusunda farklılaştırmıştır.

Türk Hukuk sistemi bazı suçlarda uzmanlık birimlerine nasıl ayrıldıysa, bilişim suçlarında da ayrı ve özel birimlerin kurulması zorunlu hale gelmiştir. Soruşturma ve kovuşturma işlemleri özel eğitimli ve bu alanda bilgili yargı mensupları tarafından yapılmalıdır.

Bir diğer önemli husus, depolama cihazlarından kurtarılan veriler analiz edilmeden önce doğrulanmalıdır. Doğrulama, orijinal verilerin kopya veya görüntülenen verilerle karşılaştırılması ve her ikisinin de aynı veriler olduğunu doğrulama sürecidir. Verilerin doğrulanması, bir karma algoritması kullanan yazılımlar aracılığıyla gerçekleşir. Karma, bir veri kümesini girdi olarak alır ve buna belirli bir sayısal çıktı atar, bu da karma değeri olarak bilinir. Karma değeri, dijital delilleri tanımlamak ve doğrulamak için önemli bir araçtır. Bu tür araçlar, verilerin değiştirildiğine dair karşı tarafın meydan okumasını aşmak için mahkemede kullanılabilir. Dijital delil elde etme süreçlerinde mutlak surette yazılım korumalı cihazlar ve dijital delilin değişmediğini kanıtlayan hash işlevi kullanılmasının zorunlu hale getirilmesi ve madde metnine eklenmesi gerekmektedir. Bu durum oluşabilecek ihlallerin önüne geçilmesini sağlayacak ve insan haklarının zedelenmesini en aza indirecektir.

Bir diğer önemli husus da siber dünyada bu tür istismarlardan korunma önlemi olarak, internette kişisel bilgilerin uygunsuz forumlarda ifşa edilmemesi için yeterli güvenlik önlemlerinin alınması gereklidir. Şifreler, failler tarafından kolayca kırılmamalıdır. İnternet

kullanıcılarının sosyal medya ve diğer sitelerde gizlilik ayarlarını mutlaka yeterli güvenlik seviyesinde ayarlamaları gerekmektedir. Ayrıca devlet veya ilgili kurumlar vatandaşlarının siber saldırılara veya diğer istismarlara karşı koruyucu ve uyarıcı kamu spotlarıyla bilgilendirme faaliyetleri yapması gerekmektedir.

Ülkeler, özellikle internete ve teknolojik cihazlara erişim yaşının ilköğretim seviyesine düştüğü şu zamanlar da; milli eğitim müfredatlarına siber güvenlikle ilgili dersleri koymalı, dijital dünya içerisinde farkındalığı yüksek, bilinçli nesiller yetiştirilmesi sağlamalıdır.

Sonuç olarak, dijital delillerin kabul görmesi açısından hukuki nitelik taşıması gerekmektedir. Bu amaçla toplanan dijital delillerin bütünlüğünün bozulmaması, kanıtlanabilir niteliğinin arttırılması açısından kanunlar doğrultusunda elkoyma ve arama işlemlerinin gerçekleştirilmesi, özel yaşama saygı çerçevesinde kişisel verilerin korunması, adli bilişimin dönemin gerekleri kapsamında personele ve teknolojiye sahip olması gerekir. Bununla birlikte, hukuk alanında hizmet sunan kişilerin tek hedefinin hukukun üstünlüğünü, adil yargılanmayı, mahkemelerin bağımsızlığını, insan haklarını gözeten adil ve hakkaniyet ölçüsünde hareket eden bir niteliğinin olması önem arz etmektedir. Bu yüzdendir ki CMK'nun bilişim sistemleri üzerinden işlenen suçların soruşturulması açısından kapsayıcı ve detaylı bir şekilde güncellenmesi gerekmektedir.

KAYNAKLAR

Akbal,S. and Dogan, E.,2018. Forensics Image Acquisition Process of Digital Evidence, I. J. Comput. Netw. Inf. Secur. 5(12), 1-8.

Akyürek, G.,2012. Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu, Türkiye Barolar Birliği Dergisi, 101, 61-70.

Arslan, Ç.,2015. Dijital Delil ve İletişimin Denetlenmesi, Ceza Hukuku ve Kriminoloji Dergisi, 3(2), 253-266.

Ayers,R., Jansen,W., Brothers,S. 2014. Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1), NIST Spec. Publ, 1(5), 85-100.

Bakan, M., ve Saluk, A. (2014). Adli Bilişimde Kullanılan Ekipmanlar, Adli Bilişim ve Elektronik Deliller, Seçkin Yayıncılık.Ankara, 199-267.

Barmpatsalou,K., Damopoulos,D., Kambourakis,G. and Katos,V. 2013. A critical review of 7 years of Mobile Device Forensics, Digit. Investig, 1(0), 323–349.

Bem, D., Feld, F., Huebner, E. and Bem, O., 2008. Computer forensics-past, present and future. Journal of Information Science and Technology. 5(1), 43-59.

Berber, L. K., 2004. Adli Bilişim (Computer Forensic), (1. b.). Ankara: Yetkin Yayınevi.

Bıçak,V.,2011. Suç Muhakemesi Hukuku, 2. Baskı, Seçkin Yayıncılık, Ankara, 423.

BTK.,2022. Dijitalleşen Dünyada Bilişim Suçları ve Mücadele Yöntemleri, Ankara.

Bulut Bilişim. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 2, 8-14.

Conlan,B.K. and Baggili,L., 2016. Anti-forensics: Furthering digital forensic science through a new extended, granular taxonom, Digit. Investig., 1(8), 66-75.

Çakır, H., ve Kılıç, M. S., 2013. Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış. Polis Bilimleri Dergisi, 1(5), 24-40.

Çelik, Ö., 2022. Dijital Delillerin Toplanması ve Aralarındaki İlişkilerin Bağ Analizi Kullanılarak İncelenmesi. Y.Lisans Tezi, Sağlık Bilimleri Enstitüsü, Ankara Üniversitesi.

Değirmenci, O., 2014. Ceza Muhakemesinde Sayısal (Dijital) Delil (Birinci Baskı b.) Seçkin Yayınevi, Ankara,25.

Değirmenci, O.,2020. Adli Bilişimde Önceliklendirme (Triyaj) Yönteminin Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi. Bilişim Hukuku Dergisi, 47-79.

Dimitriadis,A., Ivezic,N., Kulvatunyou,B. and Mavridis,I.(2020). Digital forensics framework for reviewing and investigating cyber attacks, Array, 5(10),1-15.

Düden, S., 2019. Türkiye'de Adli Bilişimin Gelişimi ve Dijital Delil İncelemeleri. Gebze Teknik Üniversitesi.15-22.

Ekim, A., 2013. Bilişim Suçlarında Sayısal Delillerin Toplanması, Muhafaza Edilmesi, İncelenmesi ve Raporlanması. Y.Lisans Tezi, Sosyal Bilimler Enstitüsü, Marmara Üniversitesi.

Ekizer, A. H. (2014). Adli Bilişim (Computer Forensics). 06. 04. 2023 tarihinde

http://www.ekizer.net/adli-bilisim-computer-forensics/ adresinden alındı.

Emekci, A., Kuğu, E. ve Temiztürk, M., 2016. Adli Bilişim Ezberlerini Bir Düzelem

EMT Electronics. (2018). www.emt.com.tr. 06. 04. 2023 tarihinde www.emt.com.tr/tr/markalar/tableau-63 adresinden alındı.

Ercan, T., ve Nacak, D., 2009. Kablosuz Ağlardaki Paket Trafiğine Adli Bilişim Yaklaşımı. Journal of Yaşar University, 4(13), 1909-1921.

Feyzioğlu,M.,2020. Ceza Muhakemesinde Vicdani Kanaat, Yetkin Yayınları, Ankara, 109.

Forensic Soft, 2016. Forensic Soft. 5.4. 2023 tarihinde www.forensicsoft.com/safeblock.php adresinden alındı.

Göksal, N., Öztürk M., 2022. Adli Bilişim: Güncel Yaklaşım ve Uygulamalar, Polis Akademisi Yayınları, Ankara.

Henkoğlu, T., 2011. Adli Bilişim, Dijital Delillerin Elde Edilmesi ve Analizi (1. b.). Pusula, İstanbul.

Henkoğlu,T.,2014. Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi, İstanbul: Pusula Yayıncılık, 2. Baskı, 5.

Jerry C.W., Brent E. Turvey, and Jodi Freeman (2011).Crime Scene Investigation, California

Jones, et al, Bilişim Suçları Eğitim Modülü, 143- 144; Jeanne Pia Mifsud Bonnici, Melania Tudorica and Joseph A. Cannataci, "The European Legal Framework on Electronic Evidence: Complex and in Need of Reform," Law, Governance and Technology Series, ed. Maria Angela Biasiotti, v.d., vol. 39, Cham, Switzerland: Springer, (2018): 189; Leyla Keser Berber, Adli Bilişim (Ankara: Yetkin Yayınları, 2004), 46. Aktaran: Kaynakçıoğlu, "Dijital Deliller," 23.

Karaaslan, İ., ve Budak, L., 2012. Üniversite Öğrencilerinin Cep Telefonu Özelliklerini Kullanımlarının ve Gündelik İletişimlerine Etkisinin Araştırılması. Journal of Yasar University, 7(26), 4548-4525.

Kaya, M.B.,2019. Hukuki Açıdan Bilişim Suçları: Siber Güvenlik ve Adli Bilişim, 1.Baskı, Grafiker Yayınları, Ankara.

Kaya, Y., 2016. Bulut Temelli Adli Bilişim. İstanbul Bilgi Üniversitesi. İstanbul.

Kent,K., Chevalier,S., Grance,S. and Dang,H.,2006. Guide to Integrating Forensic Techniques into Incident Response, Natl. Inst. Stand. Technol.

Kılıç,S., 2019. Adli Bilişim Nedir?. Erişim Adresi: [https://kernelblog.org/2019/11/adli-bilisim-nedir/]. Erişim Tarihi: 5/4/2023.

Kunter,N.,1981. Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 7. Baskı, Kazancı Matbaacılık Sanayi, İstanbul, 456.

Mohammed, S., 2015. An Introduction to digital crimes, Int. J. Found. Comput. Sci. Technol., 2(5), 13-24.

Murphy, C.A.,2012. Developing Process for Mobile Device Forensics, 1–9.

National Institute of Justice. 2004. Forensic Examination of Difital Evidance: A Guide for Law Enforcement.

Novak,M.,2021.Improving the Collection of Digital EVİDENCE, Natl. Inst. Justice, 284,23-45.

Opentext. (2018). www.guidancesoftware.com/. 06, 04, 2023 tarihinde https://www.guidancesoftware.com/tableau/hardware/td2u adresinden alındı.

Orta,M., 2015. Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim) (1.Baskı.). Yetkin Yayınları, Ankara.

Öztürk, İ.M., 2007. Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri. Y.Lisans Tezi, Sağlık Bilimleri Enstitüsü, Ankara Üniversitesi.

Sachowski, J.(2018). Digital Forensics and Investigations,People, Processes, and Technologies to Defend the Enterprise, by Taylor & Francis Group.

Sadiku, M. N. O., Tembely, M., & Musa, S. M. 2017. Digital Forensics. International Journal of Advanced Research in Computer Science and Software Engineering, 7(4), 274-276.

Sarsikoğlu, Ş.,2015. Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı, Türkiye Adalet Akademisi Dergisi, 6(22), 427-454.

Say, K., 2006. Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi. Y.Lisans Tezi, Ankara.

Shakeel, I., 2003. Introduction to Computer Forensics & Digital Investigation. InfoSec Institute. 1-79.

Şimşek, M.A.,2001. Delalet Kavramı Çerçevesinde Lafız ve Anlam İlişkileri, Nüsha Şarkiyat Araştırmaları Dergisi, 1(2),82-90.

Topaloğlu, N., ve diğerleri, (2014). Adli Bilişim ve Elektronik Deliller, 1. Baskı, Seçkin Yayıncılık, Ankara, 25.

Tosun,Ö.,1984. Türk Suç Muhakemesi Hukuku Dersleri, 4. Baskı, Acar Matbaacılık Tesisleri, İstanbul, 707.

Ünver, Y. ve Hakeri, H.2016. Ceza Muhakemesi Hukuku, 12. Baskı, Adalet Yayınevi, Ankara, 581.

Whitcomb,C.M.,2002. An Historical Perspective of Digital Evidence: A Forensic Scientist's View", Int. J. Digit. Evid., 1(1), 1-30.

Wiles,J. And Reyes,A.,2007. Computer Forensics in Today's World, in: Best Damn Cybercrime Digit. Forensics B. Period.

Zuev,S.,2019. Traditional Values of Criminal Procedure in Terms of IT Development, Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT, 1(9), 420-440.

ÖZGEÇMİŞ

Kişisel Bilgiler
Adı Soyadı: Umut DEMİRCİ **Doğum tarihi:** **Doğum Yeri:** **Uyruğu:** **Adres:** **Tel:** **E-mail:**
Eğitim
Lise: **Lisans:** **Yüksek Lisans**
Yabancı Dil Bilgisi
Üye Olunan Mesleki Kuruluşlar
Emniyet Genel Müdürlüğü
Tezden Üretilmiş Yayınlar
Durak, R. ve Demirci, U., 2024. Adli Bilişim ve Sayısal Deliller. Abant 3RD International Conference on Current Scientific Researches, Abant.