



**T.C.
ÜSKÜDAR ÜNİVERSİTESİ
BAĞIMLILIK VE ADLİ BİLİMLER ENSTİTÜSÜ
ADLİ BİLİMLER ANA BİLİM DALI
OLAY YERİ İNCELEME VE KRİMİNALİSTİK BİLİM DALI**

**ADLİ BİLİŞİM VE
TÜRK CEZA MUHAKEMESİ HUKUKUNDA
BİLGİSAYARDA ARAMA**

Yeşim Bucak - 164501017

YÜKSEK LİSANS TEZİ

**Tez Danışmanı
Doç. Dr. Serhat Özekes**

İstanbul-2019

**T.C.
ÜSKÜDAR ÜNİVERSİTESİ
BAĞIMLILIK VE ADLİ BİLİMLER ENSTİTÜSÜ
ADLİ BİLİMLER ANA BİLİM DALI
OLAY YERİ İNCELEME VE KRİMİNALİSTİK BİLİM DALI**

**ADLİ BİLİŞİM VE
TÜRK CEZA MUHALEMESİ HUKUKUNDA
BİLGİSAYARDA ARAMA**

Yeşim Bucak - 164501017

YÜKSEK LİSANS TEZİ

**Tez Danışmanı
Doç. Dr. Serhat Özekes**

İstanbul-2019



T.C.
ÜSKÜDAR
ÜNİVERSİTESİ

YÜKSEK LİSANS TEZ SAVUNMA SINAVI TUTANAĞI
BAĞIMLILIK VE ADLİ BİLİMLER ENSTİTÜSÜ

GENEL BİLGİLER

Öğrenci No	: 164501017
Öğrenci Adı Soyadı	: Yesim Burak
Anabilim Dalı	: Adli Bilimler
Tez Danışmanı	: Doç. Dr. Ferhat Öztepe
Tezin Başlığı	: Adli Bilisim ve Türk Ceza Muhakemesi Hukukunda Dijital Deliller

Toplantı Tarihi	: 10.07.2019	Saati	: 14:30
Öğrenci Savunmaya : <input checked="" type="checkbox"/> Geldi			
<p>Üniversitemiz Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin ilgili hükümleri uyarınca tez bilimsel olarak incelenmiş, adayın tez çalışmasını sunmasının ardından, adaya tez çalışması ile ilgili sorular yöneltilmiştir.</p> <p><input checked="" type="checkbox"/> Yapılan savunma sınavında adayın tez çalışması başarılı bulunarak KABUL edilmesine,</p> <p><input type="checkbox"/> Yapılan savunma sınavı sonunda tez çalışmasının DÜZELTİLMESİNE, düzeltme için adaya ay EK SÜRE verilmesine (en fazla 3 ay)</p> <p><input type="checkbox"/> Yapılan savunma sınavının sonunda tezin REDDEDİLMESİNE</p> <p><input type="checkbox"/> OY BİRLİĞİ <input type="checkbox"/> OY ÇOKLUĞU</p> <p>İle karar verilmiştir.</p>			
Savunmada Tezin Başlığı : <input type="checkbox"/> Değişmedi <input checked="" type="checkbox"/> Değişti			
Tezin Yeni Başlığı : <input type="checkbox"/> Değişmedi <input checked="" type="checkbox"/> Adli Bilisim ve Türk Ceza Muhakemesi Hukukunda Bilisimlerde Arama			
Öğrenci Savunmaya : <input type="checkbox"/> Gelmedi			
<p>Üniversitemiz Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin ilgili hükümleri uyarınca yukarıda belirtilen tarih ve saatte Tez Savunma Jürisi toplanmış ancak ilgili öğrenci savunma sınavına gelmemiştir. Adayın tez çalışmasını Jüri önünde sunmadığı için yapılan değerlendirmeler sonunda adayın tez çalışmasıyla ilgili aşağıdaki kararı,</p> <p><input type="checkbox"/> OY BİRLİĞİ İLE REDDEDİLMİŞTİR.</p>			

Tez Sınavı Jürisi	Unvanı, Adı Soyadı	İmza
Başkan	Prof. Dr. Sevil Atasoy	
Danışman Üye	Doç. Dr. Ferhat Öztepe	
Üye	Doç. Dr. Gülsün A.A. Uğurlubay	
Üye	Dr. Öğr. Üy. Tanıl Başkan	
Üye	Dr. Öğr. Üy. Ümit Tay	

(Tüm durumlarda jüri üyelerinin tez değerlendirme raporları gerekir.)

Sayı No :

Tarih : 10 / 07 / 2019.

Yukarıda kimlik bilgileri belirtilen ve Anabilim Dalımız Yüksek Lisans Programı öğrencisinin Tez Savunma Sınav Tutanağı ve eklerinin Enstitü Yönetim Kurulunda görüşülmesi hususunda bilgilerinizi ve gereğini arz ederim.

Not: Bu forma orijinal raporlar (bir nüsha) eklenecektir.

Prof. Dr. Sevil Atasoy
Anabilim Dalı Başkanı
(Unvanı, Adı Soyadı, İmza)

ÖZET

Hızla gelişen teknoloji sayesinde hayatımıza birçok yeni iletişim aracı girmiş, buna bağlı olarak da farklı suç türleri ortaya çıkmıştır. Yeni nesil iletişim cihazlarıyla çoğunlukla sanal bir dünyada gerçekleştirilen suçların soruşturma ve kovuşturma süreci, günümüzdeki hukuk sistemlerinde birçok açığı ve yetersizliği gündeme getirmektedir. Klasik suçlardan bambaşka bir hüviyete sahip bu sanal suçların işlenme sırasında kullanılan özel cihaz ve yöntemlerin dizginlenemeyen bir hızla değişmesi, yargı sisteminin delil toplama ve değerlendirme sürecinde sayısız zorluklarla karşı karşıya kalınmasına neden olmuştur. Bu tür suçların aydınlatılmasında ve gerçek failin bulunmasında büyük rol oynayan dijital deliller, sahip oldukları farklı yapısal özellikleri nedeniyle delil toplama ve değerlendirme aşamasında özel uzmanlık ve yöntemlere ihtiyaç duymaktadırlar. Bu nedenle adli bilişim disiplini daha da önem kazanmaya başlamış, bu alandaki gelişmeler her geçen gün hem ulusal hem de uluslararası arenada kendini ispatlamıştır. Yeni suç türlerinin aydınlatılmasında kilit rol üstlenen dijital delillerin hukuk sisteminde geçmişinin çok geriye gitmemesi, dijital dünyanın dinamik ve değişken bir yapıda olması, bu alanda kısıtlı sayıda bilimsel çalışmanın karşımıza çıkmasına sebep olmaktadır. Dolayısıyla adli bilişim ve dijital delillere dair ele alınan her bilimsel değerlendirme ve çalışmanın aktif olan bu gelişim sürecine katkısının büyük olacağı aşikardır.

Bu çalışmada adli bilişim kavramı, adli bilişim süreçleri, Türk hukukunda dijital deliller, bilgisayarlarda dijital delillerin aranması, toplanması ve değerlendirilme aşamaları ele alınmıştır.

Anahtar Sözcükler: Adli Bilişim, dijital deliller, Türk Hukuku, Ceza Muhakemesi Kanunu, bilgisayarlarda arama ve elkoyma tedbiri.

ABSTRACT

As a result of rapidly developing technology, various new communication tools entered into our lives and thus different crime types emerged. The investigation and prosecution process of these crimes, which took place mostly in the digital world with the new generation communication devices, reveals many gaps and incompetencies within the current legal systems. The unbridled rapid change in these special devices and methods used to commit these virtual crimes that have a totally different identity than the classical ones causes the judicial system to face numerous challenges in the process of collecting and reviewing evidences. These digital evidences that play a significant role in clarifying such crimes and finding the true perpetrators require special expertise and methods in evidence collection and review phase due to their unique nature. Thus digital forensics began to gain more importance, and the developments in this field proved themselves both in the national and international arena. The facts that the digital evidences playing a crucial role in clarifying these new crime types don't have a long background and that the digital world has a dynamic and changing nature cause scientific studies to be limited in this field. So, each scientific assessment and study regarding digital forensics and digital evidences will certainly have a huge contribution to this development period.

This study examines the concept of digital forensics, the digital forensic processes, the digital evidences in the Turkish legal system, and the phases of collecting and reviewing digital evidences in computers.

Key Words: Digital Forensics, digital evidences in computers, turkish law, turkish code of criminal procedure.

TEŞEKKÜR

Öncelikle Adli Bilimler bölümünü seçmemde büyük etkisi olan Türkiye'nin en müstesna bilim insanlarından saygıdeğer hocam Prof. Dr. Sevil Atasoy'a, tez çalışmam sırasında kıymetli bilgi, birikim ve tecrübeleriyle bana destek olan değerli danışman hocam sayın Doç. Dr. Serhat Özekes'e teşekkürlerimi sunarım.

Bu zorlu süreçte benden desteğini bir an için bile esirgemeyen kıymetli eşim Azimet Bucak'a, varlıklarıyla hayatıma anlam katan biricik kızım Belinay ve bebeğim Ömer Hamza'ya, canım kardeşlerime, tüm eğitim hayatım boyunca zorlukları benimle birlikte göğüsleyen ve bu hayattaki en büyük şansım olan annem Filiz Ceylan'a sonsuz teşekkürlerimi bir borç bilirim.

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum ‘Adli Bilişim Ve Türk Ceza Muhakemesi Hukukunda Bilgisayarda Arama’ adlı çalışmamın, tarafımdan, bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

Yeşim Bucak

İÇİNDEKİLER

Sınav Tutanağı	i
Özet	ii
Abstract	iii
Teşekkür	iv
Yemin Metni	v
Resim ve Tablolar	ix
Kısaltmalar	x
ADLİ BİLİŞİM VE TÜRK CEZA MUHAKEMESİ HUKUKUNDA	
BİLGİSAYARDA ARAMA	1
1. GİRİŞ	1
2. ADLİ BİLİŞİM	2
2.1. Adli Bilişimin Amacı	3
2.2. Adli Bilişimin Türleri	3
2.2.1. Bilgisayar Adli Bilişimi	3
2.2.2. Ağ ve İnternet Adli Bilişimi	4
2.2.3. Gömülü Cihazlara Ait Adli Bilişim	5
2.3. Diğer Adli Bilişim Türleri	5
2.3.1. Mobil Adli Bilişimi (Cell Forensics)	5
2.3.2. GPS Adli Bilişimi (GPS Forensic)	6
2.3.3. Medya Araçları Adli Bilişimi (Media Device Forensic)	6
2.3.4. Sosyal Ağ Adli Bilişimi (Social Network Forensic)	7
2.4. Adli Bilişimin Gerekliliği	8
2.5. Adli Vakalarda Dikkat Edilmesi Gereken Hususlar	8
2.6. Adli Bilişimde Delil Niteliğindeki Bilişim Cihazları	10
2.6.1. Bilgisayar	10
2.6.2. Sabit Disk	11
2.6.3. USB Bellek	12
2.6.4. Hafıza Kartı	13
2.6.5. CD- DVD	13

2.6.6. Kamera ve Fotoğraf Makinesi	14
2.6.7. Yazıcı, Fotokopi ve Faks Makinesi	15
2.6.8. Cep Telefonu	15
2.6.9. Oyun Konsolu	16
2.7. Adli Bilişim Evreleri	16
2.7.1. Hazırlık Aşaması	17
2.7.2. Dijital Delillerin Toplanması	18
2.7.2.1. Adli Kopyalama	19
2.7.2.1.1. Disk Yazma Koruma İşlemi	20
2.7.2.1.2. Uçucu Verilerde Adli Kopyalama (İmaj Alma)	22
2.7.2.1.3. Hash Değeri	24
2.7.2.2. Canlı Analiz	26
2.7.2.3. Dijital Delillerin Taşınması ve Muhafaza Edilmesi	28
2.7.3. Dijital Delillerin İncelenmesi	31
2.7.4. Dijital Delillerin Raporlanması	32
2.8. Adli Bilişim Laboratuvarları Ve Özellikleri	33
2.9. Adli Bilişimde Kullanılan Yazılımlar Ve Özellikleri	35
2.10. Adli Bilişim Uygulamalarına İlişkin Uluslararası Anlaşmalar & Örgütler	38
2.10.1. Birleşmiş Milletler	38
2.10.2. Budapeşte Sözleşmesi - Avrupa Konseyi (Council Of Europe)	39
2.10.3. İktisadi İşbirliği Ve Kalkınma Örgütü	40
(Organisation For Economic Cooperation And Development: Oecd)	
2.10.4. Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization: Nato).....	40
2.10.5. Asya Pasifik Ekonomik İşbirliği Kuruluşu	41
(Asia-Pasific Economic Cooperation: Apec)	
2.10.6. Şangay İşbirliği Örgütü (Shangai Cooperation Organization: Sco)	41
2.10.7. Sanal Küresel Görev Gücü (Virtual Global Taskforce:vgt)	41
2.10.8. Siber Suçlar Çalışma Grubu Stratejik İttifakı	42
3. DİJİTAL DELLİLER	43
3.1. Dijital Deliller	43

3.1.1. Dijital Delillerin Nitelikleri	43
3.1.2. Dijital Delillerin Elde Edilmesi	45
3.2. Ceza Muhakemesi Kanunu'nda Dijital Deliller	50
3.2.1 Türk Ceza Muhakemesi Kanunu'nda Bilgisayarlarda Arama ve Elkoyma	52
3.2.1.1. Genel	52
3.2.1.2. Bilgisayarlarda Arama ve Elkoyma Tedbirlerinin Şartları	55
3.3. Ceza Muhakemesi Kanunu'nda Düzenlenmeyen Arama Türleri	61
3.3.1. Uzaktan Erişimle Arama	61
3.3.2. Bulut Bilişimde Arama	63
3.4. Bilgisayarlara İlişkin Diğer Yasal Düzenlemeler	67
3.4.1. Adli ve Önleme Aramaları Yönetmeliği	67
3.4.2. Suç Eşyası Yönetmeliği	68
3.5. Dijital Delillere Dair Yargıtay Uygulamaları	69
3.6. Dünyadaki Hukuk Sistemlerinde Dijital Delillerin Elde Edilmesine İlişkin	
 Düzenlemeler	71
3.6.1. Amerika Birleşik Devletleri	71
3.6.2. İngiltere	74
3.6.3. Almanya	77
SONUÇ	80
KAYNAKÇA	86
Özgeçmiş	93

RESİM ve TABLOLAR

Şekil-1: TD2 Adli Kopya Alma Donanımı	19
Şekil-2: Image Masster Solo-4 İmaj Alma Donanımı	20
Şekil-3: Yazma koruma cihazlarına ilişkin çalışma sistemi	21
Şekil-4: Yazma koruma cihazlarının bulunduğu takım çantası	21
Şekil-5: Hash Değeri	24
Şekil-6: Hash Değeri	25
Şekil-7: Delil Zarfları	29
Şekil-8: Faraday Çantası	30
Şekil-9: Faraday Çantası	30
Şekil-10: Faraday Çantası	30
Şekil-11: Adli Bilişim İncelemesi sırasında genellikle yapılan işlemler	31
Şekil-12: Adli Bilişim Laboratuvarı	33
Şekil-13: Adli Bilişim Laboratuvarı	34
Şekil-14: EnCase Forensic	36
Şekil-15: AccessData FTKImager 3.1.2.0	37
Şekil-16: Linux dd	37
Şekil-17: UltraEdit	46
Şekil-18: Log Parser	46
Şekil-19: X-Ways Forensics	49
Şekil-20: COMODO Registry Cleaner	49
Şekil-21: Bulut Bilişim	63
Şekil-22: Bulut Bilişim	64

KISALTMALAR

ABD	: Amerika Birleşik Devletleri
ARP	: Adress Resolution Protocol
BIOS	: Basic Input/ Output System
CD	: Compact Disc
CDFS	: CD- ROM file System
CMA	: Computer Misuse Act (Bilgisayarın Kötüye Kullanılması Kanunu)
CMK	: Ceza Muhakemesi Kanunu
CRC	: Cyclic Redundancy Check
DCO	: Device Configuration Overlay
DLT	: Digital Linear Tape
DOC.	: Document
DVD	: Digital Video/ Versatile Disk
DVR	: Digital Video Recorder
E-Delil	: Elektronik Delil
f.	: Fıkra
FAT	: File Allocation Table
FTP	: File Transfer Protocol
FTK	: Forensic Toolkit
GPS	: Global Positioning System
HFS	: Hierarchical File System
HMK	: Hukuk Muhakemeleri Kanunu
İHAS	: İnsan Hakları Sözleşmesi
IP	: Internet Protocol Address
MAC	: Macintosh
m.	: Madde
MSN	: Messenger
NTFS	: New Technology File System

PACE	: Police and Criminal Evidence Act (Polis ve Suç Delili Kanunu)
PCMCIA	: Personal Computer Memory Card International Association
PDA	: Personal Digital Assistant
PDF	: Portable Document Format
RAM	: İşlemci aracılığı ile okunup yazılabilen, üzerinde bilgilerin geçici olarak bulunduğu yer
RIPA	: Regulation of Investigatory Powers Act (Soruşturma Yetkileri Düzenleme Kanunu)
s.	: Sayfa
SHA	: Secure Hash Algorithm
TCK	: Türk Ceza Kanunu
TV	: Television
USB	: Universal Serial Bus

ADLİ BİLİŞİM VE TÜRK CEZA MUHAKEMESİ HUKUKUNDA BİLGİSAYARDA ARAMA

1. GİRİŞ

Birçok canlı türüne ev sahipliği yapan dünya her geçen gün daha da yaşlanmakta, insanoğlu ise bu yıpranmaya paralel olarak bilime ve teknolojiye daha sıkı sarılmaktadır. Geliştirdiği yeni nesil teknolojik cihazlarla yaşlı ve yorgun dünyayı global bir köye çeviren insanoğlu, kurduğu uluslararası ağ ve haberleşme trafiği ile daha önce kendisine de yabancı olan hiç tanımadığı birçok suç alanı yaratmıştır. Teknolojik gelişmeler neticesinde suç işleme sahaları daha da genişlemiş, karmaşık ve uluslararası bir yapıya bürünmüştür. Öyle ki bir ülkede elektronik cihazlarla işlenen bir suç artık dijital veri trafiği nedeniyle kolayca başka bir ülkenin ağ trafiğinde ortaya çıkabilmektedir. Her geçen gün daha fazla kişi klasik haberleşme ve bilgi muhafaza metotları yerine, veri saklama ve iletme konusunda harikalar yaratan dijital cihazları tercih etmektedir. Bu yaygın davranış modeli de doğal olarak dijital ortamda bambaşka suç ve delil türlerinin ortaya çıkmasına neden olmuştur.

Yapısal özellikleri itibariyle fiziksel delillerden çok farklı olan dijital delillerin elde edilme ve inceleme süreçleri zaman içinde gelişerek ceza yargılamasında sıkça karşılaşılan bir konu haline gelmiş, yepyeni bir disiplin olan Adli Bilişimi hukuk dünyasına kazandırmıştır.

Ceza yargılamasında maddi gerçeğe ulaşmak hedeflenmekle beraber, gerek fiziksel gerekse dijital delil elde etme sırasında şüphelilerin bilişim sistemlerine ilişkin ele alınacak koruma tedbirlerinin temel hak ve özgürlükleri ihlal etmemesine özen gösterilmelidir. Zira bu tür uygulamalarda kişilerin özel hayatına doğrudan müdahale söz konusudur.

Bu çalışmada Adli Bilişim ve Türk Ceza Muhakemesi Kanunu'nda dijital deliller, bilgisayarlardan dijital delillerin elde edilmesi ve korunma sürecinde uyulması gereken usul kuralları, mevcut yasal düzenlemeler ve ilgili kanun maddelerinde yapılması gerekli değişiklikler incelenecektir. Mukayeseli hukukta ise ABD, İngiltere ve Almanya'nın

konuya ilişkin hukuki düzenlemeleri, bunların Türkiye'nin iç hukukuna göre nasıl farklılıklar gösterdiği ve konuya ilişkin öneriler ele alınacaktır.

2. ADLİ BİLİŞİM

*Adli bilişim, bilişim sistemleri üzerinde bulunan depolama ünitelerinin, herhangi bir suçu işlemede veya yasaklanmış bir faaliyette kullanılıp kullanılmadığını tespit etmek amacıyla yapılan çalışmaların tümüdür.*¹

Kökeni İngilizceye dayanmakta olan bu kavram, dilimizde Computer Forensic olarak adlandırılmaktadır. Her ne kadar Computer Forensic kelime anlamı itibariyle adli bilgisayar incelemesi olarak bilinse de, günümüzde uygulama sadece bu alanla sınırlı kalmamakta, gerek ceza hukukunda gerekse özel hukukta ortaya çıkan hukuki uyuşmazlıklarda farklı adli bilişim yöntemlerinden faydalanılmaktadır. Delillerin elde edilmesi, ele geçirilen delillerin muhafazası, tahribata uğramış verilerin tekrar kazanılması, buradan çıkan sonuçların analiz edilerek rapor haline getirilmesi ve son olarak bu raporun sunulması adli bilişim uygulamalarında ortaya çıkan aşamalardır.

Tüm bu süreç içinde azami dikkat edilmesi gereken en önemli noktalardan biri de araştırmaların bilimsel ve teknik yöntemlerle yapılması gerektiğidir. Aksi takdirde adli bilişim süreci içinde elde edilen deliller güvenilirlik itibariyle sorgulanacak ve hatta kabul dahi edilmeyecektir. Zira yargılama aşamasında kullanılacak delillerin maddi gerçeğe katkıda bulunabilmesi için öncelikle güvenilir olma kriterini yerine getirmesi beklenmektedir.

1 Henkoğlu Türkay, Adli Bilişim, Dijital Delillerin Elde Edilmesi ve Analizi, İstanbul, Pusula Yayıncılık, 2014, s.1.

2.1. ADLİ BİLİŞİMİN AMACI

Genel anlam itibariyle adli bilişim, soruşturma veya kovuşturma aşamasında önem arz eden elektronik delillerin belirli bir düzen dahilinde toplanması, analiz edilmesi, değerlendirilmesi ve son olarak yargı makamlarına sunulması olarak tanımlanmaktadır. Temelini herhangi bir şahsa suç yüklemek ya da onun masumiyetini kanıtlamak oluşturmaz, elektronik delillerin teknik bir inceleme neticesinde eksiksiz ve tarafsız bir şekilde adli makamlara ulaştırılması esastır.²

2.2. ADLİ BİLİŞİMİN TÜRLERİ

Adli bilişim 4 ana alt başlık altında incelenmektedir, bunlar sırasıyla

- Bilgisayar adli bilişimi
- Ağ ve internet adli bilişimi
- Gömülü cihazlara ait adli bilişim ve
- Sosyal ağ adli bilişimidir.³

2.2.1. Bilgisayar Adli Bilişimi

Son yıllarda artan teknoloji kullanımı ile beraber yargıya intikal eden konularda artık bilgisayar adli bilişiminden de sıkça faydalanılmaktadır. Örneğin “*suçun işlendiği olay yerinde bulunan ya da şüphelinin kullandığı bir bilgisayar - ister masaüstü ister dizüstü ya da netbook olsun- soruşturma organları tarafından tüm teknik yöntemler ve usul kuralları gözetilerek muhafaza altında adli bilişim laboratuvarlarına sevk edilir. Bilgisayarda veri içeren tüm üniteler incelenir ve bu süreçte elde edilen bulgular raporlanarak yargılama makamına sunulur.*”⁴

2 Muharrem Özen ve Gürkan Özocak, “Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve Elkoyma Tedbirinin Hukuki Rejimi (CMK M. 134)”, Ankara Barosu Dergisi 1/1 (Ocak 2015): s. 45.

3 <https://fordefence.com/dijital-delillerde-adli-bilisim/> (Son Er. T.: 30.05.2019).

4 Özen ve Özocak, s.46.

2.2.2. Ağ ve İnternet Adli Bilişimi

İngilizce tabiriyle ‘Network Forensics’ olarak da bilinen ağ ve internet adli bilişimi, ağ trafiğinde ya da sistem hafızalarında işlenmiş olan bir suça ilişkin soruşturma ya da kovuşturmada bilgi ve veri toplama, adli delil elde etme, herhangi bir sızma şüphesi nedeniyle ağ trafiğinin izlenmesi, buradan elde edilen verilerin toplanması, raporlandırılmak suretiyle yargı makamına sunulması sürecini tanımlamaktadır.⁵

Günümüzde bazı kötücül yazılımlar diske herhangi bir şey yazılmaksızın, direkt olarak bellekte çalışabilmektedirler. Örneğin Network ağ saldırılarında güvenlik ihlalini yapan kişi, işini bitirdiğinde arkasında RAM ve ağ dışında bir iz bırakmamaktadır. Bu kişi izinsiz şekilde eriştiği sistemin loglarını ya da eriştiği sistemi tümüyle silebilmekte, ortada hiçbir delil bırakmamaktadır. Böyle durumlarda bilgi/delil ancak ağ/güvenlik kaynaklarından toplanabilmektedir. Gerek Network Forensic gerek Computer Forensic’in hedefi delil toplamaktır. İkisi arasındaki en önemli fark, Network Forensic’te delillerin bilgisayarda ya da RAM’de değil, network paketlerinde aranıyor olmasıdır. Network’a ilişkin delil toplama iki yöntem aracılığı ile sağlanmaktadır. Bunlar ‘Proaktif Delil Toplama ve Reaktif Delil Toplama’dır.⁶

Proaktif Delil Toplama aşamasında gerekli cihaz, donanım ve yazılımlar kurulup, olayın gerçekleşmesi beklenmeden, ilgili hedef izlenmeye alınır. Reaktif Delil Toplama aşamasında ise olayın gerçekleştiği andan itibaren (networkta bir adrese giriş yapılması vs.) izleme yapılır.⁷

Network Forensic’te Full Content (Tam İçerik), Session Data (Oturum Verisi), Alert Data (Uyarı Verisi) ve Statical Data (İstatiksel Veri) olmak üzere 4 ayrı delil türü bulunmaktadır. Full Content (Tam İçerik) delil türünde amaç, içeriğin tümünü elde etmektir. Şayet hedefe ilişkin ayrıntılı bir inceleme yapılmak isteniyorsa, bu delil türüne başvurulmalıdır. Session Data (Oturum Verisi)’nde içeriğe dair değil, oturum hakkında (oturum süresi, oturumun kurulduğu uç noktalar, oturum süresi vs. gibi) bilgiler bulunmaktadır. Alert Data (Uyarı Verisi), Network’taki bot aktivitelerine ilişkin tespitler yapılmaktadır.⁸

5 <https://fordefence.com/dijital-delillerde-adli-bilisim> (Son Er. T.: 30.05.2019).

6 <http://btkultur.blogspot.com/2016/06/network-forensic-nedir.html> (Son Er. T.: 30.05.2019).

7 <http://btkultur.blogspot.com/2016/06/network-forensic-nedir.html> (Son Er. T.: 30.05.2019).

8 <http://btkultur.blogspot.com/2016/06/network-forensic-nedir.html> (Son Er. T.: 30.05.2019).

Belirlenen kriterlerden yola çıkarak, o kriterlerle uyumlu paketlere denk gelindiğinde olmaktadır. Statical data (İstatiksel Veri) ise hedefe ilişkin istatistiksel bilgi (en çok hangi protokolden veri transferi gerçekleşmiş vs. gibi) toplanmasını sağlamaktadır.

WireShark ya da WinDump gibi Network analiz araç ve yazılımları, ağ üzerinde akış halinde olan paketleri tutmayı, onları çeşitli şekilde bölerek, kullanıcının işine yarar hale getirmeyi hedefler.⁹

2.2.3. Gömülü Cihazlara Ait Adli Bilişim

Gömülü cihazlara ait adli bilişim dalında bilinen mobil cihazlar aracılığıyla işlenmiş olan bir suçta, failin kullanmış olduğu bu cihazın ele geçirilmesi, bu cihazlara yönelik spesifik adli bilişim teknikleriyle suçun aydınlatılmasında kullanılabilecek verilerin elde edilme, raporlanma ve yargıya intikal ettirilme süreci söz konusu olmaktadır.¹⁰

2.3. DİĞER ADLİ BİLİŞİM TÜRLERİ

2.3.1. Mobil Adli Bilişimi (Cell Forensics)

Günümüzde mobil cihazların kullanımının artması suç dünyasında da kendini göstermeye başlamıştır. Adli bir soruşturma ya da kovuşturma esnasında mobil cihaz incelemeleri yaygınlaşmıştır.

Mobil cihazlar yapı itibarıyla taşınabilir olduğundan olası bir failin neredeyse tüm hareketleri takip edilebilmektedir. Aynı zamanda birçok veriyi de bünyesinde barındıran cep telefonları bu şekilde adli soruşturmaların vazgeçilmez bir inceleme unsuru haline gelmiştir.

Mobil cihazların içinde bulunmakta olan servis sağlayıcılarının hesap bilgilerini, aranan ve aranılan kişilerin detaylı verilerini elde etmeye yarayan bir disiplin olan mobil

9 <http://btkultur.blogspot.com/2016/06/network-forensic-nedir.html> (Son Er. T.: 30.05.2019).

10 <https://fordefence.com/dijital-delillerde-adli-bilisim/> (Son Er. T.: 30.05.2019).

adli biliřim aracılıęıyla birok suun aydınlatılması iin delil nitelięinde mhim bilgiler elde edilebilmektedir. Geliřmiř cep telefonları sadece arama deęil aynı zamanda e-mail kullanımı, mesajlařma, fotoęraf ekimi ve ses kayıt zellikleri bakımından da yargılama ařamasında son derece nemli deliller sunabilmektedir. Ancak sz konusu bu veriler cep telefonun sabit diskine kayıt edilebildięi gibi kolaylıkla silinebilmektedir. Silinmiř verilerin kurtarılabılme imkanı ortaya ıktıęında mobil adli biliřim de ayrı bir disiplin olarak kabul grmüştür.¹¹

Tařınabilir bilgisayarlar kadar sık kullanılan mobil telefonların bir ok modelinin farklı iřletim sistemlerine sahip olması cihazların inceleme ařamasında bazı sorunlar ortaya ıkarmakta, inceleme iin tek bir yntemin ve tek bir aracın kullanımını imkansız hale getirmektedir.

2.3.2. GPS Adli Biliřimi (GPS Forensic)

Teknoloji dnyasının vazgeilmez unsuru haline gelen GPS sistemleri her geen gn daha da aktif kullanılmakta, bu sistemlere iliřkin geliřmelerde bu kullanıma paralel olarak ilerlemektedir. zel ya da toplu tařımada, nakliyat ya da kiralama aralarında kullanıcıya baęlı olmaksızın birok GPS cihazı bulunmaktadır.

GPS adli biliřimi, son derece yaygın olan GPS sistemlerinin inceleme, analiz ve delil elde etme ařamasını ieren bir alt disiplindir. Bu cihazlar arala gidilmiř olan ya da sıka ziyaret edilen yerleri zaman da dahil olmak zere kayıt altına aldıęı iin zellikle lmle sonulanan trafik kazalarında nemli bir delil tespit kaynaęı olabilmektedir.¹²

2.3.3. Medya Araları Adli Biliřimi (Media Device Forensic)

Teknolojinin hakim olduęu gndelik hayatta ses kayıt cihazları, flash bellekler, tařınabilir harici diskler gibi benzeri elektronik cihazlar sıklıkla kullanılmakta, yine bu cihazlar vasıtası ile su ierikli birok řifreli veri, grnt ve ses kaydı muhafaza edilebilmekte ve

11 <https://fordefence.com/dijital-delillerde-adli-bilisim/> (Son Er. T.: 30.05.2019).

12 <https://fordefence.com/dijital-delillerde-adli-bilisim/> (Son Er. T.: 30.05.2019).

izlenebilmektedir. Ne var ki tıpkı diğer elektronik cihazlarda olduğu gibi bu tip cihazlarda da içerik ve zamana dair veriler failler tarafından silinebilmekte, deliller yok edilebilmektedir. Soruşturma ve kovuşturma aşamasında delil olabilecek, ancak silinmiş bu verilerin tekrar kurtarılabilmesi medya araçları adli bilişimi alt disiplini ile mümkün olmaktadır.¹³

2.3.4. Sosyal Ağ Adli Bilişimi (Social Network Forensic)

Sosyal ağ, en genel tabiriyle kişilerin internet ortamında birbirleriyle etkileşim içinde olduğu ve bilgi paylaşımında bulunduğu bir platformdur. Facebook, Instagram, Twitter, Snapchat gibi sosyal paylaşım sitelerinde paylaşılan herhangi bir yazı, görüntü ya da ses kaydı saniyeler içinde milyonluk kitleler tarafından görülebilmektedir.

Kişiler, sosyal ağ platformlarında aile ya da arkadaş çevresine ilişkin paylaşımlar yapabildiği gibi, sosyal, politik, ideolojik ve kültürel paylaşımlarda da bulunabilmektedir. Bu paylaşımlar kimi zaman bilinçli/bilinçsiz hakaret, tehdit ya da başka bir suç içeriğine sahip olabilmekte, diğer kullanıcıların kişilik hakları zarar görebilmektedir.

Türkiye’de Emniyet Teşkilatı bünyesinde bulunan Siber Suçlarla Mücadele ekipleri, Sanal Devriye ve Suç Önleme Faaliyetleri çerçevesinde internet aracılığıyla yayın yapan tüm sosyal paylaşım platformlarında, suç unsuru teşkil edebilecek paylaşımlarda yapan hesap kullanıcılarını tespit etmekte, gerektiği takdirde adli işlemleri başlatabilmektedir. Emniyete bildirilen ihbarlar en kısa sürede değerlendirilmekte, söz konusu sosyal medya hesapları incelemeye alınmaktadır.¹⁴

Bununla beraber NCMEC (Uluslararası Kayıp ve Sömürülen Çocuk Merkezi) nin emniyete raporladığı Facebook, Twitter, Instagram gibi sosyal paylaşım siteleri aracılığıyla müstehcen fotoğraf ya da video paylaşımında bulunan şüpheliler hakkında adli işlemler uygulanmakta, el konulan dijital materyaller (Harddisk, Cep Telefonu vb.) varsa, bunlar üzerinde adli bilişim personeli tarafından inceleme yapılmakta, elde edilen deliller adli mercilere sevk edilmektedir.¹⁵

13 <https://fordefence.com/dijital-delillerde-adli-bilisim/> (Son Er. T.: 30.05.2019).

14 <https://www.egm.gov.tr/siber> (Son Er. T.: 30.05.2019).

15 <https://www.ozgureralp.com.tr/read-offline/5819/internette-mustehcenlik-sucu-ve-cezasi.print> (Son Er. T.: 30.05.2019).

Sonuç itibariyle sosyal ağ adli bilişimi spesifik alt disiplin olarak söz konusu paylaşımların hangi uygulamalar vasıtasıyla işlendiği, hangi platformda bu verilerin toplandığı, ele geçirilen verilerin incelenmesi, analiz edilmesi ve yargı makamına sunulması aşamalarını içermektedir.¹⁶

2.4. ADLİ BİLİŞİMİN GEREKLİLİĞİ

Gerek dünyada gerekse ülkemizde bilişim teknolojisi büyük bir ivme kazanmış, buna bağlı olarak eski araştırma ve yazılım teknikleri zamanla kullanım dışı kalmış, bu tarz bilgi ve belgeler artık elektronik ortamda muhafaza edilmeye başlanmıştır. Ne var ki elektronik belge ve veriler son derece hassas bir yapıdadırlar ve bundan dolayı çok kolay bir şekilde değişim geçirebilmektedirler. Bu nedenle soruşturma ya da kovuşturma esnasında ortaya konan belgeler üzerinde olası bir değişiklik olup olmadığının tespiti, var olan ve elde edilen verilerin en güvenli şekilde korunması ve yargıya sunulması için özel adli bilişim teknik ve yöntemlerinden faydalanılmaktadır.

Sadece özel ve kişisel alanlarda değil aynı zamanda iş hayatında da tüm kurum ve kuruluşlarda dokümanlar elektronik ortamda saklanır hale gelmiş, mevcut verilere yetkisiz ve onaysız erişim, dolandırıcılık, hacking gibi vakalar ortaya çıkmıştır. Buna bağlı olarak bu alanlarda da adli bilişimin özel tekniklerinden ve kriminal incelemelerden faydalanma gereği doğmuştur.

Elektronik ortamlarda Adli Bilişim çerçevesinde kriminal inceleme yapılırken söz konusu olaya ilişkin suç unsuru olup olmadığı, hangi bilişim cihazların kullanıldığı, bunlarda şifreli dosyaların bulunup bulunmadığı gibi sorulara cevaplar aranmaktadır.

2.5. ADLİ VAKALARDA DİKKAT EDİLMESİ GEREKEN HUSUSLAR

Bilişim sistemleri ile ilgili herhangi bir suç karşısında nasıl bir yol haritası izlenmesi gerektiği bu alan için belirlenmiş güvenlik politikaları sayesinde mümkün olmaktadır. Aynı sürecin hukuki boyutuna bakıldığında, eğer ki delil elde etme süreci hukuka

16 <https://fordefence.com/dijital-delillerde-adli-bilisim/> (Son Er. T.: 30.05.2019).

uygun ilerlemezse, yargılama aşamasında hakim, hukuka aykırı elde edilen bu delilleri dikkate almayacaktır.

Adli olaylarda belirlenmiş olan güvenlik şartlarına uyulmadığının tespiti halinde ilgili kurum, kuruluş ve her türlü organizasyon, bünyesinde barındığı bilişim uzmanları aracılığıyla duruma müdahale etmekte, ancak bu müdahalelerin çoğu zaman yetersiz kaldığı görülmektedir.

Olayların vuku buldukları yere göre 3 farklı inceleme örneği bulunmaktadır. Bunlar *“olay yerine ilişkin incelemeler, kurum ya da kuruluşlarda bulunan birden fazla bilgisayarın dahil olduğu bilgisayar ağlarını da içine alan incelemeler ve kişisel bilgisayarlar üzerinde işlenen suçlara ilişkin dar bir alanda yapılan incelemelerdir.”*¹⁷

Bu tür incelemelerin gerçekleştirebilmesi belli bir suçun mevcudiyetine yahut bu suçun işlendiğine dair bir iddia ya da şüphenin varlığına bağlıdır. Söz konusu suç, kişiye özel bir dijital ortamda olabileceği gibi, uluslararası ya da kurumsal bir dijital ortamda da işlenmiş olabilir. Adli incelemeye konu suçlar arasında kimi zaman bilişim suçları olarak adlandırılan çocuk pornografisi, yetkisiz erişim, dolandırıcılık bulunmakta, kimi zaman da bilişim suçu kategorisine girmeyen suçlar gözlemlenmektedir.

Gerek kişiye özel gerek kurumsal bilişim sistemlerinde yapılacak olan kriminal inceleme esnasında güvenlik açıklığı ortaya çıktığında takip edilmesi gereken süreç ve yöntem ana başlıklarıyla şu şekilde karşımıza çıkmaktadır:

- *“Dijital ya da dijital olmayan kayıt ve belgelerin denetlenmesi*
- *Gerek şüphelilerle gerekse olay yerinde hazır bulunan kişilerle görüşme yapılması ya da sorgulanması*
- *Olayın özellikleri göz önünde bulundurularak arama işlemi için bir plan hazırlanması*
- *Uygun görüldüğü takdirde şüpheliye ait ya da şüphelinin çalıştığı tüm alanlar*

17 Henkoğlu, s.13.

üzerinde arama yapılması

- Soruşturma için gerekli görülen delillere el konulması

- Uygun görüldüğü takdirde gözaltı süreci için harekete geçilmesi”¹⁸

Kriminal incelemeyi yapacak olan kişilerde bulunması gereken niteliklerin başında, görevlinin tarafsız, güvenilir, teknik konularda donanımlı ve tecrübeli, bilişim hukuku ve ağ güvenliğine dair deneyim sahibi; adli bilişim süreci, yazılım, işletim sistemleri ve analiz tekniklerine vakıf olması gelmektedir.

Adli bilişim incelemelerinde takip edilmesi gereken süreç 3 ana başlık altında toplanmaktadır, bunlar sırasıyla:

- “Olay yerinde delillerin tespit edildikten sonra, toplanması ve korunması

- Delillerin ortaya çıkarılması, adli bilişim uzmanlarınca incelenmesi ve analiz edilmesi.

- Delillerin rapor haline getirilmesi”¹⁹

2.6. ADLİ BİLİŞİMDE DELİL NİTELİĞİNDEKİ BİLİŞİM CİHAZLARI

Adli bilişim alanına giren adli vakalarda karşılaşılan ve delil sayılabilecek bilişim cihazlarının en önemlileri şunlardır:

2.6.1. Bilgisayar

Bilgisayar, çeşitli aritmetik ve mantıksal işlemleri yapabilen, gerçekleştirdiği bu işlemlerin verilerini muhafaza edebilen ve arzu edildiğinde tekrar geri getirme kabiliyeti

18 Henkoğlu, s.14.

19 Henkoğlu, s.17.

olan elektronik bir cihazdır.²⁰

“Günümüzde çok yaygın kullanılan bir bilişim cihazı olan bilgisayar, soruşturma ve kovuşturma aşamasında bizzat delil olarak yer alabileceği gibi buradan elde edilen donanım, yazılım, belgeler, fotoğraflar, görüntü dosyaları, e-posta ve ekleri, veri tabanları, finansal bilgiler, internet tarama geçmişi, sohbet günlükleri, arkadaş listeleri, olay günlükleri, daha önce sisteme takılmış olan harici aygıtlara ait tanımlayıcı bilgiler gibi kanıt değeri taşıyan bulguların incelenmesinde de kullanılabilir. ”²¹

2.6.2. Sabit Disk

Sabit diskler, veri depolamaya yönelik manyetik kayıt alanı olup, aynı zamanda veriye tekrar ulaşmayı sağlayan, elektirik akımı kesildiğinde ya da bilgisayar kapatılsa dahi üzerindeki bilgilerin saklı kaldığı ve silinmediği aygıtlardır.

Önceleri büyük boyutları ve yüksek fiyatlarından dolayı yalnızca bilgisayar merkezlerinde kullanılan sabit diskler, cep telefonları ve sayısal fotoğraf makineleri bünyesinde olabilecek kadar küçülen ebatları ile günlük hayatımızda yerlerini almışlardır. Sabit diskler en yoğun bilgisayarlarda kullanılırlar. Ses, görüntü, yazılımlar, veri tabanları gibi çok fazla yer kaplayan bilgiler, ihtiyaç duyulduğunda kullanılmak üzere sabit disklerde muhafaza edilirler.

Sabit diskler günümüz dünyasında oldukça hızlı veri aktarımında bulunsalar da elektromekanik yapıları sebebiyle RAM'lara göre yavaşlardır. Bilgisayarlarda yardımcı ve kalıcı bellek görevi görürler.

Bilgisayar sabit diskleri genellikle bilgisayarların içinde sabitlenmiş bir şekilde bulunurlar, bilgisayarlara haricen bağlanabilen taşınabilir olanları da mevcuttur.²²

Bilgisayar açıldığında sabit disk işletim sistemini ve yazılımları sistem belleğine yükler. Kullanıcı kalıcı olmasını istediği verileri bilgisayar kapalı vaziyette olsa dahi mu-

20 http://www.teknolojide.com/bilgisayar-nedir_4881.aspx (Son Er. T.: 30.05.2019).

21 Murat Özbek, Adli Bilişimde Delillerin Toplanması ve İncelenmesi (Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, 2013), s. 20.

22 <https://www.pcbilimi.com/sabit-disk-nedir/> (Son Er. T.: 30.05.2019).

hafaza etmeye devam eder.

PATA (IDE), SATA (Serial ATA), SCSI (Small Computer System Interface), SSD (Solid State Disk) olmak üzere 4 çeşit sabit disk vardır. Sabit diskler üzerinde cam, seramik ya da metalik kaplı, özel alaşımlı bir alan bulunmaktadır. Veriler bu alan üzerinde depolanmaktadır. Sabit disk üzerinde yazılan verilerin yoğunluğu, diskin veri saklama kapasitesini etkilemektedir.²³

Adli inceleme esnasında olay yerinde herhangi bir bilgisayara takılı olmayan sabit diskler de bulunabilir. Bu durum, söz konusu sabit disklerin kanıt içermediği anlamına gelmez, aksine değerli deliller içermesi mümkündür.

2.6.3. Usb Bellek

USB Bellekler güç kesintisi olsa da, içinde bulunan verilerin kaybolmadığı, üzerinde depolanan bilgilerin isteğe göre tekrar yazılıp silinebildiği depolama aygıtlarıdır. Mekanik değil, elektronik yapıdadırlar. Bünyesinde hareket eden bir parçaya sahip olmadıklarından ‘solid state’ (durağan) olarak adlandırılırlar. Verilerin bellek üzerinde muhafaza edilme süreleri sonsuz değildir. Bu süre genellikle 10 yılı bulabilmektedir. Disketlerin ve kısmen CD-ROM’ların yerine tercih edilmelerinin en büyük nedenleri arasında kapasitelerinin büyüklüğü, daha uzun ömürlü ve boyut olarak küçük olmaları, her geçen gün daha da ucuzlamaları gösterilebilir. Elektrikle yazılıp silinebilen bir bellek özelliği taşırlar. Bazı hafıza türlerinden farkları, yazma ve silme işleminin byte olarak değil daha büyük bloklar hâlinde gerçekleşmesidir.²⁴

CompactFlash, SD (Secure Digital), MultimediaCard, Memory Stick, Smart Media gibi çeşitleri olan USB bellekler tak-çalıştır prensibinden ötürü birçok aygıtın bağlantısında sorunsuz ve kolaylıkla kullanılabilir. Yaygın olarak kullanıldıkları aygıtlar içerisinde cep telefonları, bilgisayarlar, mp3 playerlar, dijital fotoğraf makinaları ve görüntü cihazları bulunmaktadır. Bununla beraber kol saati, anahtarlık gibi nesnelerin içinde de gizlenmiş bir vaziyette bulunmaları da mümkün olabilmektedir.

23 <https://ademocut.com/sabit-disk-nedir-sabit-disk-cesitleri-nelerdir-adem-ocut/> (Son Er. T.: 30.05.2019).

24 <https://teknoprom.com/usb-bellek-nedir-nasil-calisir/> (Son Er. T.: 30.05.2019).

2.6.4. Hafıza Kartı

Hafıza kartı, bünyesine medya dosyalarının depolanabildiği bellek şeklindedir. Bununla beraber elektronik cihazlar tarafından genellikle içerisine fotoğraf, video, müzik ve diğer data türlerini aktarmak üzere kullanılmaktadır. Kapasite ihtiyacına cevap veremeyen cihazlarda depolama alanını artırmaya yönelik belleklerdir.²⁵

Boyutları, entegre oldukları cihazların kullanım amacına bağlı olarak değişebilmektedir. İngilizce Memory Card olarak tanımlanan hafıza kartları esasen bir çeşit flash bellektir. Sadece boyut olarak biraz daha küçük bir yapıdadırlar. Kullanım alanları bilgisayarlar, dijital kameralar, fotoğraf makineleri, cep bilgisayarları gibi günlük hayatta kendisinden sıkça istifade edilen cihazlardır.²⁶

Verimli bir kullanım için hafıza kartı seçiminde fiziksel boyutu, bozulma ömrü, yazma hızı, kapasite, okuma hızı gibi özellikler dikkate alınmalıdır.

2.6.5. CD- DVD

Görüntü, ses ve veri sayısal format muhafaza eden CD (Compact Disc) ve DVD'ler optik medya olarak adlandırılırlar zira okuma ve yazma işlemleri için lazer ışınına ihtiyaç duyarlar.²⁷

CD'lerin 650-720 MB'e kadar değişen kapasiteleri vardır. DVD sürücüler ise 4.7 GB ve üzerinde bir veri depolama alanına sahiptirler. Boyut olarak bakıldığında CD ve DVD arasında herhangi bir fark bulunmamaktadır. 2 katmanlı yapıda olan DVD'lerin depolama alanları, lazerin, ilk katmanda altında bulunan ikinci katmana da ulaşabilmesi nedeniyle 2'ye katlanmaktadır. DVD sürücüdeki diskin dönme hızı ise CD ile karşılaştırıldığında yine 3 kat daha fazladır. USB bellekler de olduğu gibi CD ve DVD'lerin de işletim sistemi üzerinden çalıştırılabilme özellikleri mevcuttur. Bir DVD'nin ortalama 10 katına kadar bilgi depolayabilen (25-50 GB) Blu-Ray'ler gelişen teknolojinin giderek

25 <https://wmaraci.com/nedir/hafiza-karti> (Son Er. T.: 30.05.2019).

26 <https://wmaraci.com/nedir/hafiza-karti> (Son Er. T.: 30.05.2019).

27 <https://bilgihanem.com/cd-dvd-surucusu-nedir-nasil-calisir/> (Son Er. T.: 30.05.2019).

artan kapasite ihtiyacına bir cevap olarak doğmuş yeni sayılabilecek bir ses ve görüntü depolama medyasıdır.²⁸

Çoğunlukla veri yedekleme amacıyla kullanılan bu optik medyalar adli vakalarda maddi gerçeğin ortaya çıkmasına yardımcı olabilecek ve delil olarak kullanılabilecek mühim veriler içerebilirler. Bu nedenle adli bilişim açısından önemli bir dijital delil olarak görülmektedirler.

2.6.6. Kamera ve Fotoğraf Makinesi

Dış kaynaklı görüntülerin kayıt altına alınmasını mümkün kılan teknolojik alete kamera adı verilir. Teknik olarak ise kamera, *‘görüntüden yansıyan ışığı mercek ya da objektiften yararlanarak bir düzlemde toplayan, o düzleme konulan film veya ışığa duyarlı elektronik devre elemanları sayesinde ışık enerjisini elektrik enerjisine çevirdikten sonra çıkış sinyali veren ve gerekirse bunu kaydeden bir sistemdir.’*²⁹

Kamera ile fotoğraf makinesi arasındaki en önemli fark; fotoğraf makinesinin donmuş kareler kadar hareketli görüntüleri de kaydedebiliyor olmasıdır.³⁰

Yaklaşık yüzyıl evvel icat edilen kameralar günümüzde birçok sistemin ana parçasını oluşturmaktadır. Kullanım alanlarına göre birçok türü bulunmaktadır. TV yayıncılığı, kişisel kameralar, binalarda güvenliği sağlayan güvenlik kameraları, su altı kameraları, termal kameralar, tıbbi gözlem kameralar olmak üzere birçok türü bulunmaktadır.³¹

Önceki yıllarda şeritler üzerine kayıt yapan kamera ve fotoğraf makineleri günümüz teknolojisi sayesinde artık flash bellek, sabit disk ya da üzerinde bulunan hafıza kartı veya DVD'lere kayıt yapmaktadırlar. Hafıza kartı hariç dahili hafızaya sahip olan kamera ve fotoğraf makinelerinin mevcudiyeti adli inceleme ve delil toplama aşamasında özellikle göz önünde bulundurulmalıdır.

28 <https://bilgihanem.com/cd-dvd-surucusu-nedir-nasil-calisir/> (Son Er. T.: 30.05.2019).

29 <https://www.elektrikport.com/teknik-kutuphane/kamera-nasil-calisir/14791#ad-image-0> (Son Er. T.: 30.05.2019).

30 <https://www.mailce.com/kamera-nedir.html> (Son Er. T.: 30.05.2019).

31 <https://www.elektrikport.com/teknik-kutuphane/kamera-nasil-calisir/14791#ad-image-0> (Son Er. T.: 30.05.2019).

2.6.7. Yazıcı, Fotokopi ve Faks Makinesi

Bir bilgisayardaki bilgilerin, fotoğrafların ve benzer verilerin hafızadan kağıt üzerine çıkışını mümkün kılan donanım yazıcı olarak adlandırılmaktadır. Bir çok yazıcının bilgisayara bağlanması USB yada RJ45 aracılığıyla sağlanır. Bununla beraber fotoğraf makinasında yada hafıza kartından direkt çıktı alınması mümkündür. Günümüzdeki yazıcıların birçoğunun faks yada fotokopi çekme gibi özellikleri de bulunmaktadır.³²

Tıpkı diğerleri gibi yazıcı, fotokopi ve fax makineleri de adli bilişim incelemesine konu olabilecek donanım araçlarıdır. Üzerlerinde yapılan işlemleri hafızaya alma mekanizmaları olduğu gibi, internete de bağlanabilmektedirler.

Bu tür araçlara ilişkin spesifik bir incelemede bulunan adli bilişim uzmanının dikkat etmesi gereken hususlardan biri de olay yerinde bulunan açık bir yazıcının kağıdının bitmesinden dolayı hafızasına aldığı verileri yazdırıyormuş olabileceğidir. Bununla beraber gelen ve giden faks kayıtları, son yazdırılan belgelerin de hafızada bulunabileceği gözönünde bulundurulmalıdır.

2.6.8. Cep Telefonu

‘Cep telefonu radyo sinyalleri ile çağrı yapabilen ve çağrı alabilen taşınabilir iletişim cihazıdır. Bu çağrı işlemlerini cep telefonu operatörlerinin sunduğu hücresel ağ sistemine bağlanarak yapmaktadır.’³³

Kolayca taşınabilen ve fiziksel olarak küçük boyutlara sahip olan cep telefonları kablolu telefon sistemini kullanmaktadırlar.

Akıllı telefonlar, sesli ve yazılı görüşme ile beraber görüntülü görüşme, görüntülü mesaj, müzikçalar, video oyunları, internet, veri transferi ve hatta ofis uygulamaları gibi tüm diğer bilgisayar fonksiyonlarını kullanıcının hizmetine sunabilmektedir. Aynı zamanda internet

32 <https://www.tech-worm.com/yazici-nedir-yazici-turleri-nelerdir/> (Son Er. T.: 30.05.2019).

33 <https://www.hermesiletisim.net/blog/cep-telefonlari-arasinda-iletisim-nasil-gercekle sir#.XVgPuafBLLZ> (Son Er. T.: 30.05.2019).

ve telefon bankacılığı gibi hizmetlerde de sıkça başvurulanan bir cihazdır. Paypal gibi hesaplar kullanmak suretiyle, sms yoluyla, satın alınan mal ve hizmetlerin ücretlerinin ödenmesi de bu cihazlarla artık mümkün olabilmektedir.³⁴

Son yıllarda yaygınlaşan akıllı telefonlar, normal telefon özelliklerine ek olarak yukarıda zikredilen bilgisayar özelliklerini de taşıdıklarından, bu durum onları adli bilişim incelemeleri açısından son derece önemli bir delil kaynağı haline getirmiştir.

2.6.9. Oyun Konsolu

“Oyun Konsolu, TV veya diğer görüntü ünitelerine bağlanılarak kullanılan birincil amacı ileri seviye oyun deneyimi ve multimedya olan cihazlardır.”³⁵

Günümüzde oldukça gelişmiş bir yapıda olan oyun konsolları ile video, fotoğraf, müzik gibi dosyalar oynatılabildiği gibi muhafaza da edilebilmektedir. Bu özellik içlerindeki çıkarılabilir hafıza üniteleri sayesinde mümkün olmaktadır. Oyun konsolları aracılığı ile aynı zamanda internet üzerinden görüntülü ve sesli iletişim kurma, içerik indirme, çeşitli sosyal medya ağları kullanımı yapılabilmektedir. Dolayısıyla adli bilişim incelemelerinde dijital delil elde edilebilecek önemli araçlardan biridirler.

2.7. ADLİ BİLİŞİM EVRELERİ

Dijital delillerin mahkemece delil olarak kabul görmesi için itina, dikkat ve kurallara uygun elde edilmesi gerekmektedir. Olay yerinden elde edilmesinden mahkemeye sunulma aşamasına kadar geçen aşamalar 4 ana başlık altında toplanmaktadır:

- *“Hazırlık Aşaması*

- *Dijital Delillerin toplanması*

34 <https://www.turkcebilgi.com/cep-telefonu-nedir> (Son Er. T.: 30.05.2019).

35 <https://wmaraci.com/nedir/oyun-konsolu> (Son Er. T.: 30.05.2019).

- Dijital Delillerin incelenmesi

- Dijital Delillerin Rapor Haline Getirilmesi”³⁶

2.7.1. Hazırlık Aşaması

Olay yerine intikal eden bir adli bilişimcinin yapması gereken olayın aydınlanması için hangi verilere ulaşması gerektiği ve bu verileri hangi bilişim cihazlarından/ aygıtlarından elde edebileceğini belirlemesidir. Önceliğin bu olmasının bir nedeni de, adli bilişim uzmanının olay yerinde karşılaşacağı cihazların birbirinden tamamen farklı tekniklerle incelenme ihtimalidir. Zira elde edilmek istenen veriler kişisel bir bilgisayarda bulunabileceği gibi, yazıcı, faks, fotoğraf makinesi ya da bir cep telefonunda da olabilir. Dolayısıyla bilişim uzmanının bu ihtimalleri göz önünde bulundurup, adli kopyalama işlemi için beraberinde ona göre uygun boş veri depolama birimini bulundurması gerekmektedir.

Hazırlık aşamasında dikkat edilmesi gereken noktalardan biri de, adli bilişim uzmanının veri toplama esnasında karşılaşabileceği sorunları asgari düzeye indirgeyecek şekilde önlemler alması, strateji geliştirmesidir.

Olay yerinde elde edilen dijital delillerin her açıdan korunması kusursuz bir adli kopya alımı için vazgeçilmez bir kuraldır. Söz konusu koruma 2 şekilde ele alınmaktadır: Dijital deliller öncelikle fiziksel olarak korunmalıdır. Zira son derece hassas bir yapıya sahip olan elektronik cihazlar birçok çevresel etkene maruz kalabilmekte, kolaylıkla arızalanabilmektedir. Örneğin bünyesinde bir olaya ilişkin adli kopyalar bulunduran bir “sabit disk manyetik etki altındaki bir ortama maruz bırakılırsa, sabit disk manyetik veri depolama ünitesinde yer alan plakaların (platter) üzerinde yazılı şekilde bulunan dataların mıknatıs etkisiyle mevcut halini muhafaza edemeyerek değişecek ve böylelikle e-delil içerisinde ki adli kopyalar da doğru çalışma olanağı bulamayacağından henüz incelenmeyen e-delil yok olacaktır.”³⁷

36 Henkoğlu, S. 17.

37 Özbek, s. 30.

Diğer bir koruma şekli ise elde edilen dijital delil ya da delillerin kaç defa ve tam olarak ne zaman (tarih-saat) el değiştirdiğine dair bilgilerinin belirtilmesi gerektiğidir. Amaç, mevcut deliller üzerinde istenmeyen müdahalelerin yapılmasını engellemektir.³⁸

2.7.2. Dijital Delillerin Toplanması

Dijital deliller, klasik delillerden farklı olarak alışılmış tekniklerle muhafazası mümkün olmayan yapıdadırlar. Örneğin olay yerinden elde edilen taşınabilir bir belleğin ihtiva ettiği verileri gözle görmek mümkün olmadığından farklı yöntemlerle muhafazası söz konusu olacaktır.

Dijital delillerin elde edilmesi aşamasında özen gösterilmesi gereken birçok husus bulunmaktadır. Ele geçirilen deliller öncelikle elle tutulmamalı, dijital aygıtlar ve veri depoları üzerinde parmak izi bırakmamaya dikkat edilmelidir. Arama işlemi yapılırken bir kontrol zinciri çerçevesinde tüm işlemler kamera aracılığıyla kayıt altına alınmalı, böylelikle muhtemel aksaklık ya da eksikliklerin sonradan denetleme imkanı sağlanmalıdır.³⁹

Olay yerinde bulunan delili tahrip edebilecek bir programın aktive edilip edilmediği araştırılmalı, mevcut aktif olan programların ise ekran görüntüsü alınmalıdır. Yapı itibarıyla daha titiz ve yoğun bir araştırma gerektiren programlar (PGB, TruCryp) söz konusu ise, buna dair bir tutanak hazırlanarak, kamera kaydı altında adli bilişim uzmanı tarafından bir inceleme gerçekleştirilmeli, yapılan her bir işlem tek tek raporlanmalıdır. Deliller toplanırken göz önünde bulundurulması gereken bir diğer önemli adım ise, olay yerinde bulunan bilgisayarların kapatma işlemidir. Ancak burada bazı farklılıklar bulunmaktadır. Windows gibi işletim sistemleri bilgisayarın fişinin çekilmesiyle kapatılabiliyorken, Linux ya da Macintosh gibi bilgisayarlar sıradan bir bilgisayarı kapat komutuyla kapatılmaktadır. Dizüstü bilgisayarlarda ise kapatma işlemine ek olarak bataryanın da çıkartılması icap etmekte, kimi zaman CD sürücü kısmında da bataryanın olabileceği ihtimali gözden kaçırılmamalıdır.⁴⁰

38 Henkoğlu, s. 19.

39 Henkoğlu, s. 23.

40 Henkoğlu, s. 24.

Delil toplama işleminin en önemli aşamalarından biri olan imaj alma işlemi için FTK Imager, Encase gibi adli bilişim standartlarına uyan programlar tercih edilmeli, ele geçirilmiş olan orijinal delilin ‘bit to bit’ kopyası alınmalıdır. İmaj almada kullanılan donanım ya da yazılımların bit to bit kopyalama işlemi yapabilme, alınan imajı arzu edilen formata getirebilme, tahrip edilmiş ya da bozulmuş disklerin imajını alabilme, ortaya çıkan yanlışları kaydedebilme gibi spesifik özelliklerinin olması gerekmektedir.⁴¹

2.7.2.1. Adli Kopyalama

Kökeni ingilizce bir terim olan ‘forensic image’ dilimize adli kopya olarak geçmiş, ülkemizde ‘bire-bir’ kopyalama olarak adlandırılmaktadır. Bu işlem, veri depolama cihazlarının bit düzeyinde bire-bir kopyalanması anlamına gelmekte, aynı zamanda imaj alma olarak da nitelendirilmektedir.⁴²

Söz konusu kopyalama, “*sektör-sektör veya bit-bit denilen şekilde hiçbir veri değişmeden, eksilmeden ve artmadan her veri aynı olacak şekilde, dosya halinde bir başka diske yapılmaktadır. İşletim sistemlerinde günlük hayatta yapılan normal kopyalama işleminde kullanıcılar tarafından görülen dosya ve klasörler bir başka bilişim aygıtına aktarılırken bu işlemde bazı bilgilerin (oluşturma tarihi gibi) değişebilmesinin yanı sıra yapılan işlemde sadece görülmekte olan bilgiler kopyalanır. Hatta bazı yeni dosya ve klasör eski dosya yapısıyla formatlanmış bir veri depolama birimine kopyalandığında bazı üst veriler de kopyalanamamaktadır.*”⁴³



Şekil- 1: TD2 Adli Kopya Alma Donanımı⁴⁴

41 Henkoğlu, s. 24.

42 Hüseyin Çakır ve Mehmet Serkan Kılıç, Adli Bilişim ve Elektronik Deliller (Ankara: Seçkin Yayıncılık, 2014), S. 172.

43 Özbek, s. 40.

44 <https://www.adlibilisimuzmani.com/adli-kopya-alma-donanimlari-imaj-alma-donanimlari/> (Son Er. T.: 30.05.2019).



Şekil- 2: Image Masster Solo-4 İmaj Alma Donanımı ⁴⁵

2.7.2.1.1. Disk Yazma Koruma İşlemi

İngilizce Write Protection adı verilen Yazma Koruma mekanizması, bir donanım ya da yazılımın bünyesinde bulunan verileri korumak adına, var olan bilginin üzerine başka yeni bir bilgi eklenmesini engelleme özelliğine sahiptir. Yazma korumasına sahip bir hafıza kartı, disk, flash bellek ya da yazılımda yer alan mevcut veriler korunduğundan dolayı, bunlar üzerindeki dosyaların silinmesi ve içeriğinin değiştirilmesi mümkün değildir. Bu veriler okunabilmekte, ancak üzerine yeni bir veri eklenememektedir.⁴⁶

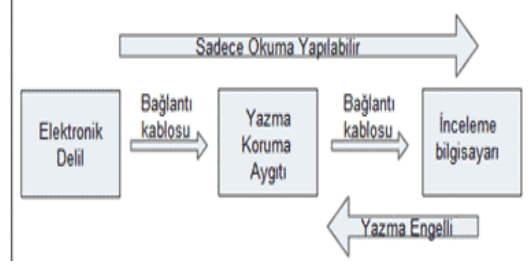
Adli kopyalama işlemi, dijital delil üzerinde herhangi bir değişiklik olma ihtimaline karşı delil bütünlüğüne zarar gelmemesi için yazma korumalı gerçekleştirilmelidir. Ancak bu çalışma vaziyetteki sistemlerden imaj alma işlemlerini kapsamamaktadır.⁴⁷

Çalışır vaziyetteki bir sistemden imaj alabilmek ancak sisteme boş veri depolama ünitesi takıldığı zaman mümkün olduğu için, aynı zamanda yazmayı engelleme işlemi gerçekleştirilemez.

⁴⁵ <https://www.adlibilisimuzmani.com/adli-kopya-alma-donanimlari-imaj-alma-donanimlari/> (Son Er. T.: 30.05.2019).

⁴⁶ <https://wmaraci.com/nedir/yazma-korumasi> (Son Er. T.: 30.05.2019).

⁴⁷ Çakır ve Kılıç, s. 201.



Şekil- 3: Yazma koruma cihazlarına ilişkin çalışma sistemi⁴⁸



Şekil- 4: Yazma koruma cihazlarının bulunduğu takım çantası⁴⁹

Yazma Koruma tedbiri, içerisinde olası delillerin yer aldığı diskin tek yönlü veri akışını sağlayacak ve veri bütünlüğünü koruyacak şekilde tasarlanmıştır. Donanımsal yazma koruma ve yazılımsal yazma koruma olmak üzere iki tür yazma koruma mevcuttur.⁵⁰

Donanımsal yazma koruma, incelenecek olan disk ve bilgisayar arasında bağlantı kuran bir cihaz olup, verilerin okunmasını sağladığı gibi, diske veri yazılmasına da engel olur. Adli kopyalama esnasında sıkça kullanıldığı için, adli bilişim labotuarlarında bulunması gereken temel aygıtlar arasındadır. Yazılımsal yazma koruma ise, bazı yazılımlar aracılığı ile incelemede kullanılacak olan bilgisayarın analiz edilecek diske veri yazma komutlarını engellemektedir.⁵¹

48 <https://www.adlibilisimuzmani.com/adli-bilisim-yazma-koruma-write-blocker/> (Son Er. T.: 30.05.2019).

49 <https://www.adlibilisimuzmani.com/adli-bilisim-yazma-koruma-write-blocker/> (Son Er. T.: 30.05.2019).

50 <https://www.adlibilisimuzmani.com/adli-bilisim-yazma-koruma-write-blocker/> (Son Er. T.: 30.05.2019).

51 <https://www.adlibilisimuzmani.com/adli-bilisim-yazma-koruma-write-blocker/> (Son Er. T.: 30.05.2019).

2.7.2.1.2. Uçucu Verilerde Adli Kopyalama (İmaj Alma)

Uçucu veri çalışıyor durumdaki bir bilgisayar sisteminde bulunan, sistem dışarıdan kapatıldığında ya da elektrik kesintisi olduğunda yok olan, veri depolama ünitesinde sürekli kayıtlı şekilde kalmayan veriler, uygulamalardır.⁵²

İşlemci teknolojilerin zaman içinde gelişmesi ve sabit disklerin hız konusunda ihtiyaca cevap verememesi, uçucu belleğin bilgisayarlardaki veri işleyişi itibarıyla daha da önem kazanmasına neden olmuştur.

Önceden adli bilişim olaylarında uçucu verilerin imajı alınmamaktaydı. İncelemeye tabi olan bilgisayarlar üzerinde güç kaynağı kesildikten sonra çalışma yapılmakta, ancak bu durum uçucu bellekteki verilere ulaşılmasını engellemektedir. Ancak sosyal medya kullanımının, bulut teknolojilerinin ve bilişim suçlarının yaygınlaşması ile kötü niyetli yazılımların artış göstermesi gibi sebepler, bilgisayarlardaki uçucu belleğin imajının alınıp incelenmesini mecburi bir yöntem olarak adli bilişim dünyasına kazandırmıştır.

Uçucu bellekteki incelemeler, adli bilişim vakalarında delillerin ortaya çıkarılması ve olayın süratli bir şekilde aydınlatılması açısından önemlidir, zira sabit diskteki incelemeler tek başına kesin bir sonuç için yetersiz kalmaktadır. Bu nedenle uçucu bellekte bulunan tüm bilgilerin zarar vermeden kopyalanması, bu kopyalamanın hangi yöntemle yapılacağı, ne tür analiz programlarının kullanılacağı adli bilişim vakalarındaki kritik sorular arasındadır.

Uçucu bellekte elde edilebilecek veriler arasında aktif network bağlantılarının durumu, kaydedilmemiş dokümanlar, sisteme oturum açan kullanıcılara ilişkin bilgiler, kayıt defteri bilgileri, en son bakılan fotoğraflar, bulut sistemlerine ilişkin teknik bilgiler, açık ağ bağlantıları ve ARP önbellek, ziyaret edilen adres bilgileri, e-mail üzerinde gerçekleştirilen en son işlemler, sohbet ve sosyal ağ kayıtları gibi veriler bulunmaktadır.⁵³

Günümüzde uçucu bellekte imaj alma işlemi FTK Imager, Belkasoft Live RAM Capturer, Encase V7 ile mümkün olabilmektedir. AccessData firmasının ürettiği

52 Çakır ve Kılıç, s. 311.

53 <https://fordefence.com/ram-analizi-ve-adli-bilisimdeki-yeri/> (Son Er. T.: 30.05.2019).

bir yazılım olan FTK Imager aracılığı ile depolama ünitelerinin içeriği gösterilebilmekte, uçucu belleğin birebir kopyası alınabilmektedir. Ayrıca güncel versiyonları ücretsiz de kullanılabilmektedir.⁵⁴

Bir başka ücretsiz program olan Belkasoft Live RAM Capturer ise uçucu belleğin imajını alabilen, canlı analize imkan sağlayan, aynı zamanda hata düzeltme mekanizmasına sahip adli bir araç olma özelliği taşımaktadır.⁵⁵

Uçucu bellek imajının alınmasında kullanılan bir başka yazılım ise Guidance Software firmasının bir ürünü olan Encase v7 dir. Encase v7 yazılımı sistem üzerinde kurulum yapılarak kullanılmaktadır. Bu nedenle uçucu bellek üzerinde oldukça fazla proses çalıştırmakta ve buradaki verilere kalıcı zarar verme tehlikesi bulunmaktadır. Esasen ücretli bir yazılım olan Encase v7'in imaj alma özelliği kullanıcıların hizmetine ücretsiz olarak sunulmuştur.⁵⁶

Uçucu belleğin imajından alınan kopyanın inceleme aşaması son derece zordur ve uzmanlık gerektirmektedir. Bununla birlikte uçucu belleklerdeki hiyerarşik yapının eksikliği analiz programlarının ne kadar mühim olduğunu ortaya koymuştur. Analiz aşamasında kullanılan yöntemlerden biri Volatility'dir. Canlı analiz yapma özelliği olmayan bu yöntemle, çalışan uygulamalar, açık ağ portları, imajın alındığı zaman bilgileri, uygulama veya proses tarafından açılan dosyalar ve registry anahtarı gibi bilgiler öğrenilebilmektedir.⁵⁷

Belkasoft Evidence Center ise ücretli bir yazılım olmanın yanısıra, IOS, Android, Windows ve Blackberry için uçucu bellek analizi yapabilmektedir.⁵⁸

54 <http://fatihberber.com/adli-bilisim-incelemelerinde-birebir-kopya-alma/> (Son Er. T.: 30.05.2019).

55 <http://fatihberber.com/adli-bilisim-incelemelerinde-birebir-kopya-alma/> (Son Er. T.: 30.05.2019).

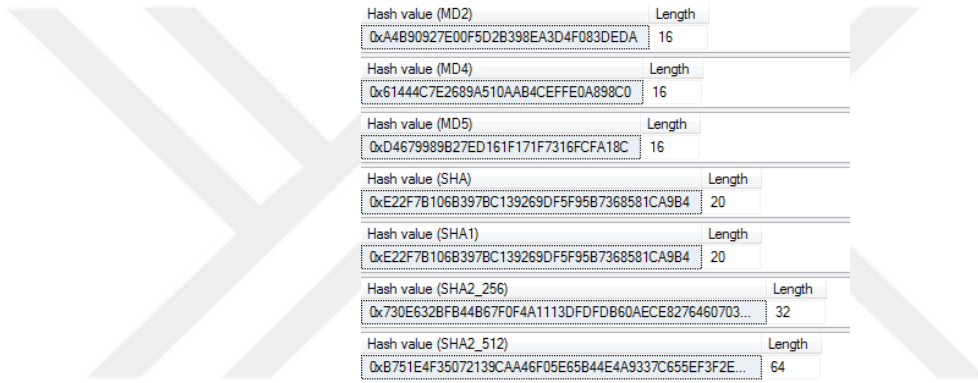
56 <https://www.adlibilisimuzmani.com/adli-kopya-alma-yazilimleri-imaj-alma-yazilimleri/> (Son Er. T.: 30.05.2019).

57 <https://www.slideshare.net/bgasecurity/ram-belleklerinin-adli-biliim-analiz-teknikleri> (Son Er. T.: 30.05.2019).

58 <https://www.adlibilisimuzmani.com/adli-kopya-alma-yazilimleri-imaj-alma-yazilimleri/> (Son Er. T.: 30.05.2019).

2.7.2.1.3. Hash Değeri

Hash fonksiyonu bir algoritmaya bağlı olarak çalışan bir sistemdir. Bu algoritma fonksiyonu aracılığı ile veri tabanında aranmakta olan bir veri süratle bulunabilmekte yahut veri karşılaştırma işlemleri daha hızlı yapılabilir. Bir insanda parmak izi ne ise, adli bilişimde hash algoritması da odur. Tıpkı parmak izi gibi, hash algoritması da ilgili olduğu dosya veya diske özeldir. Öyle ki, bir disk ya da dosya üzerinde hash algoritması oluşturulduğu vakit, bunlar üzerinde gerçekleştirilen en ufak bir değişiklik (1'in 0 yapılması veya 0'in 1 yapılması) ortaya çıkarılan sayı dizinin neredeyse yarısının değişmesine sebep olmaktadır.⁵⁹



Hash value (MD2)	Length
0xA4B90927E00F5D2B398EA3D4F083DEDA	16
Hash value (MD4)	Length
0x61444C7E2689A510AAB4CEFFE0A898C0	16
Hash value (MD5)	Length
0xD467989B27ED161F171F7316FCFA18C	16
Hash value (SHA)	Length
0xE22F7B106B397BC139269DF5F95B7368581CA9B4	20
Hash value (SHA1)	Length
0xE22F7B106B397BC139269DF5F95B7368581CA9B4	20
Hash value (SHA2_256)	Length
0x730E632BF44B67F0F4A1113DFDFB60AECE8276460703...	32
Hash value (SHA2_512)	Length
0xB751E4F35072139CAA46F05E65B44E4A9337C655EF3F2E...	64

Şekil- 5: Hash Değeri⁶⁰

Hash algoritması standardı için fazlasıyla alternatif bulunmasına rağmen, en sık tercih edilen 2 standart 128 bit MD5 (Message – Digest Algoritma) ve 160 bit SHA-1 (Secure Hash Algoritma)'dır. Adli bilişim uzmanları tarafından oluşturulan bilirkişi raporlarında bahsi geçen 2 standarttan ya birinin ya da her ikisinin birden gösterilmesi gerekmektedir.⁶¹

Ne var ki, son zamanlarda bu iki standart için de çakışma ihtimalinin olduğu ve bunun bilimsel olarak ortaya konduğuna ilişkin haberler gündeme oturmuş, bunun üzerine daha gelişmiş standartların oluşturulması için adımlar atılmıştır (SHA-2 ve SHA-3). Ancak bu durumun MD5 ve SHA - 1'in adli bilişim camiasında güvenilirliğine henüz

⁵⁹ Çakır ve Kılıç, s. 176.

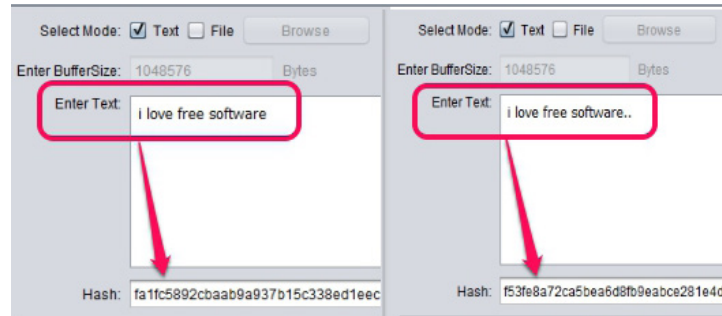
⁶⁰ <https://sqlserverrider.wordpress.com/2013/03/01/generate-hash-value-using-md-and-sha-algorithm-sql-server/> (Son Er. T.: 30.05.2019).

⁶¹ Henkoğlu, s. 56.

olumsuz yönde bir etkisi bulunmamaktadır. Adli bilişim alanına giren bir dosya ya da programın bilgi depolama ünitesinde belli bir zaman diliminde herhangi bir değişiklik yapıp yapılmadığı, yani orijinali ile farklılık olup olmadığı hash değeri kullanılarak anlaşılır. Eğer ki hash değeri işlem ön- cesinde ve sonrasında aynı değeri taşıyorsa, program, dosya ya da belgede herhangi bir değişiklik yapılmadığı, farklı değer söz konusu ise, değişiklik yapıldığı anlamına gelmektedir.⁶²

Adli bilişim uzmanı şüphelinin kullandığı bilgisayarın harddiskinin imajı alınması esnasında hash değerini ortaya koyar ve imajı alınan diskin kullanıcıya da söz konusu hash değerinin bir kopyasını verir. Bu hash değerlerinin inceleme neticesinde hazırlanan raporda yer alan hash değeri ile aynı olması gerekmektedir. Aksi halde adli bilişim uzmanının elde ettiği bu analiz bulgularına itiraz edilmesi ve mahkeme tarafından delil olarak kabul görmemesi kaçınılmaz olacaktır.⁶³

Hash değeri hesaplanırken dikkat edilmesi gereken noktalardan biri, sabit disk üzerinde verilerin yer aldığı kimi sektörlerin manyetik alan, sarsıntı ya da nem gibi faktörlerden dolayı bozulma ihtimalidir. Bu sektörler “bad sector (bozuk alan)” olarak adlandırılmakla beraber üzerlerinde herhangi bir veri kaydedilmediği için hash değeri hesaplanırken dikkate alınmazlar. Bad sector sayısının bilinmesi önemlidir, bu nedenle hesaplanan hash değerleriyle beraber bad sector sayısı da raporda ayrıca belirtilmelidir.⁶⁴



Şekil-6: Hash Değeri⁶⁵

Hash değerine ilişkin ihmallerin en başında gerekli kontrol ve takibin yapılması gelmektedir. Zira bazı davalarda kolluk tarafından elde edilen ve raporlanan hash

62 Henkoğlu, s. 56.

63 Başlar, s.216.

64 Çakır ve Kılıç, s. 149.

65 <http://www.ilovefreesoftware.com/12/windows/portable-sha1-md2-md5-hash-generator-calculate-hash-value-files.html> (Son Er. T.: 30.05.2019).

değerlerinin bilirkşi raporunda bulunan hash değeriyle örtüşmediği görülmektedir. Böyle durumlarda bilirkşinin incelemek üzere ele aldığı imajın orjinalinden farklı olduğu ve buradan elde edilen bulguların adli bilişim kuralları çerçevesinde delil özelliğine sahip olmadıkları aşıkardır.

Adli bilişim uzmanlarının kendilerine incelemeleri için teslim edilen disk imajı üzerinde çalışmak yerine, bu disk imajlarını ilk önce başka bir diske kopyalamaları ve bu disk imajı üzerinde incelemelerini yapmaları gerekmektedir. Aksi takdirde imaj üzerinde herhangi bir sebepten oluşabilecek en ufak bir değişiklik hash değerinin de değişmesine neden olacak ve gerçekleştirilen bütün incelemeleri hükümsüz kılacaktır.⁶⁶

Son zamanlarda hash değerinin hesaplanması veya doğruluğunun denetlenmesi için geliştirilmiş ve adli bilişim uzmanına ihtiyaç duymadan kullanılabilen yazılımlar ortaya çıkmıştır. Bunlardan biri 'HashCalc'dır. Ücretsiz olan bu yazılım kullanılarak 12 farklı algoritma ile Hash değeri hesaplanması ve doğrulaması (SHA-1, SHA-2 (256, 384, 512), PANAMA, TIGER, MD2, MD4, MD5, ADLER32, CRC32) gerçekleştirilebilmektedir.⁶⁷

2.7.2.2. Canlı Analiz

Olay yerine intikal eden adli bilişim uzmanlarının azami dikkat göstermesi gereken en mühim noktalardan biri ortamda bulunan açık halde bulunan bilgisayarların usulüne uygun bir şekilde kapatılması ve muhafaza edilmesidir. Zira izlenilen yöntemdeki en ufak bir dikkatsizlik ya da ihmal son derece hassas bir yapıda olan dijital delillerin yok olmasına sebep olabilmektedir. İçindeki işletim sisteminde delil niteliği taşıyan veri olduğu düşünülen bilgisayarlar üzerinde imaj alma işlemleri yapılır. Ancak bilgisayarları açma ve kapama esnasında sistemde bulunan uçucu verilerin kaybolma riski doğmaktadır. Bu nedenle adli bilişim uzmanı her daim bu risk bilinciyle hareket etmeli, olay yerinde açık bir bilgisayarla karşılaştığında uçucu verileri olası bir sistem kapanmasından önce kayda geçirmelidir.⁶⁸

66 Çakır ve Kılıç, s. 150.

67 Henkoğlu, s. 57.

68 Henkoğlu, s. 29.

Canlı analiz yöntemi, sadece teknik bir uzman aracılığı ile yapılabilen, bellek, ön bellek ya da sistemde bulunan uçucu verilerin elde edilmesini hedefleyen, ancak içinde delilleri değiştirme riski barındıran bir analiz yöntemidir.⁶⁹

İçinde bulunduğumuz dijital çağın en önemli suç araçlarından biri haline gelmiş olan bilgisayarların sistemlerinde bazen içindeki tüm delilleri yok edebilecek zararlı yazılımlar bulunabilmektedir. Dolayısıyla suç mahallinde bulunan uzman ekip, olası her türlü dijital tuzağa karşı bilinçli ve donanımlı olmalı ve buna göre hareket etmelidir.

Teknik ekip için ilk adım, öncelikle olay yerinde bulunan dijital delillerin hiçbir tahribata uğramadan orijinal hali korunmak suretiyle elde edilmesidir. Uçucu karakterdeki verilere değişme ve kaybolma riski yüksek olduğundan öncelik tanınmalıdır. Bu yönüyle ele alındığında bellekte bulunan veriler uçucu karakteri açısından kaybedilme riski en yüksek olan verilerdir. Adli bilişim uzmanı olay yerine ulaştığında, kapalı bilgisayarlar açılmamalı, açık bilgisayarlar ise şifreli programlar içeriyorsa canlı analiz yöntemiyle teknik incelemeye alınmalıdır. Zira açık bilgisayarlarda şüpheli ve delil niteliği taşıyan bir program çalışıyor vaziyette olabilir ve uçucu veriler, sistemin kendiliğinden kapanması halinde geri dönüşümü olmayacak şekilde kaybolabilir. Canlı analiz yöntemi, ancak çok gerekli hallerde başvurulması gereken, sadece bellekteki verilerin elde edilmesi ile sınırlı tutulması gereken bir analiz yöntemidir.⁷⁰

Adli bilişim uzmanı canlı analiz yöntemini kullanırken, bu süreçte bazı aşamaları izler. Olay yerine ulaşan teknik uzman, öncelikle bulunan bilgisayarın fotoğrafını çeker, çalışan programları kayıt altına alır. Burada uygulanan tüm işlemlerin hem yazılı hem de görsel olarak kayıt altına alınması büyük önem taşır, zira yargılama aşamasında ispat gücü açısından gerekli olacaktır. Çalışır vaziyette bulunan bilgisayarda görülen tarih ve zamana dair veriler ile gerçek tarih ve zaman bilgileri yazılı ve görsel kayıt altına alınır. Olay yerinde incelemeye tabi tutulan her bir bilgisayar için yapılan tüm işlemlerin kaydedildiği ayrı bir işlem kayıt dosyası oluşturulur. Bununla beraber bu işlemlerin kim tarafından ve ne zaman yapıldığı, işlemlerin hangi yazılım aracılığı ile gerçekleştirildiği, işlem sırasında sistem üzerinde herhangi bir değişiklik meydana gelip gelmediği kaydedilmelidir. Bu bilgiler, sabit disk üzerinde kalıcı bilgilerin analiz edilme işlemi sonrasında

69 Henkoğlu, s. 26.

70 Henkoğlu, s. 26.

adli bilişim uzmanı ya da bilirkişi tarafından doğru bir delil değerlendirmesi için gerekli olacaktır.⁷¹

Belli bir uçuculuk sırası tespit edilerek ve bu sıraya uyularak veri elde etme işlemlerine geçilmelidir. Bilişim uzmanları tarafından alışlagelmiş olan sıra şu şekildedir:

- “Ana bellekteki veriler, ağ bağlantıları, açık dosyalar ve takas alanları
- Şifrelenmiş ve şifresi bilinmeyen disk bölümleri
- Geçici dosyalar (tmp uzantılı dosyalar)”⁷²

Bunun yanında özel CD’lerden faydalanılarak ve mevcut bilgisayar sistemine entegre olmadan çalıştırılabilen programlar yardımıyla gerekli bilgiler elde edilir. Bu işlem bir kamera kaydı altında gerçekleştirilir ve yazılı halde belge haline getirilir. Bu bilgiler tarih/zaman, kayıt içeriği, kullanılan dosya sistemleri vs. gibi hususları içermektedir.⁷²

2.7.2.3. Dijital Delillerin Taşınması ve Muhafaza Edilmesi

Hassas yapıları itibariyle dijital deliller hiçbir değişikliğe mahal vermeyecek şekilde muhafaza edilmeli, ele geçirilen cihazların barındırdığı verilerde oluşabilecek tüm tahribatlar engellenmelidir. CD, DVD, Flash Bellek, Sabit Disk gibi veri depolama üniteleri ısı, nem, manyetik alan ve dış etmenlere karşı son derece duyarlı olduklarından, bunların toplanması, taşınması ve muhafaza edilmesi özel uygulama ve yöntemlerle sağlanmaktadır.

Deliller, olay yerinde ait oldukları yerden alınmadan önce kendisine ait kablo, adaptör gibi ek parçalarıyla birlikte alınmalıdır. Elde edilen dijital delillerin özel poşetlerle paketlenmeden önce ve sonra (delilin kendisi ve içine konulduğu paket) mutlaka etiketlenmelidir, tüm bu işlemler mümkün mertebe kamera ile kayıt altına alınmalıdır. İmajların MDS ve SHA Hash değerleri özenle alınmalı, sonradan yapılabilecek itirazlar

⁷¹ Henkoğlu, s. 27.

⁷² Henkoğlu, s. 30.

göz önünde bulundurularak bir tutanak aracılığı ile belgelendirilmelidir. Hassas veri depolama ünitelerinin yüzeylerinde çizilme, kırılma olmaması ve manyetik ortama maruz kalmaması yönünde gerekli önlemler alınmalıdır.⁷³

Delillerin taşıma işlemi herhangi bir araç aracılığı ile olacaksa, aracın içi ve delillerin yerleşme düzeni herhangi bir fiziki tahribata yol açmayacak şekilde dizayn edilmelidir. Ebat olarak daha büyük aygıtlar delil zarflarına sığmaları mümkün olmadığından, ekranı aşağıya gelecek ve yumuşak bir yüzeye yaslanacak şekilde emniyet kemeriyle desteklenmelidir.⁷⁴

The image shows three evidence bags (Delil Zarfları) of different sizes, each with a yellow form for recording evidence details and a chain of custody table. The forms include fields for: EVIDENCE, SUBMITTING AGENCY, ITEM NO., CASE NO., SUBJECT, DESCRIPTION OF EVIDENCE, OFFENSE TYPE, LOCATION, COLLECTED BY, DATE/TIME, and REMARKS. Below these fields is a 'CHAIN OF CUSTODY' table with columns for FROM, TO, and DATE. The bags are arranged in a row, with the largest bag on the left and two smaller bags on the right.

Şekil-7: Delil Zarfları⁷⁵

Bir diğer önemli konu ise, batarya ile çalışan dijital aygıtların, batarya tamamen sonlanmadan şarj edilmesidir, zira olası bir batarya bitiminde aygıt üzerinde tüm program ve tarihler sıfırlanmakta, önemli veriler kaybolmaktadır.

Cep telefonları, cep bilgisayarları, akıllı telefonlar söz konusu ise, bu cihazlar özellikle faraday çantası denilen özel bir çantaya yerleştirilmeli ve bununla taşınmalıdır. Faraday kafesi olarak da bilinen Faraday çantası İngiliz fizikçi Michael Faraday tarafından geliştirilmiş,

73 Henkoğlu, s. 25.

74 Henkoğlu, s. 25.

75 <https://www.adlibilisimuzmani.com/elektronik-delillerin-paketlenmesi-tasinmasi-ve-muhafazasi/> (Son Er. T.: 30.05.2019).

elektiriksel iletken bir madde ile evrelenmiř ve aę řeklinde rlmř bir antadır. Bu zel tasarımı antanın yardımı ile antanın iindeki cep telefonu dıřardaki elektrik alandan korunur, baz istasyonu ile baęlantısı manuel kapatılmaksızın kesilmiř olur.⁷⁶



řekil-8: Faraday antası⁷⁷



řekil- 9: Faraday antası⁷⁸



řekil-10: Faraday antası⁷⁹

76 akır ve Kılı, s. 238.

77 <https://mosequipment.com/products/mission-darkness-large-non-window-faraday-bag> (Son Er. T.: 30.05.2019).

78 <https://mosequipment.com/products/mission-darkness-large-non-window-faraday-bag> (Son Er. T.: 30.05.2019).

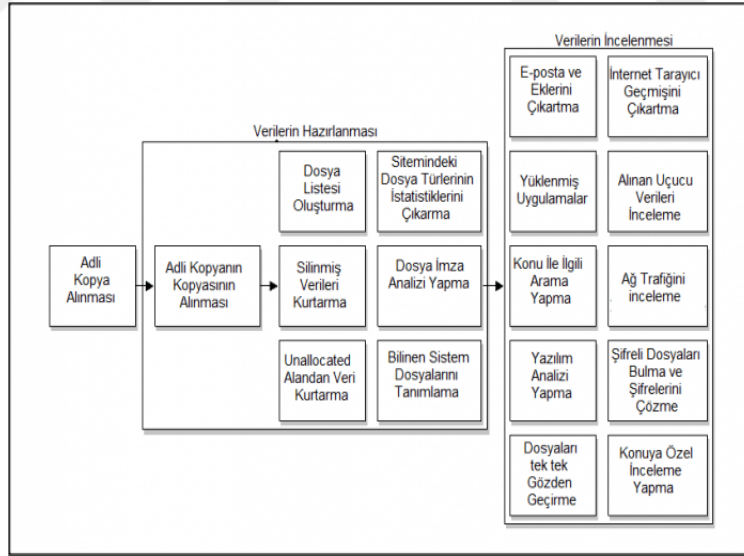
79 <https://mosequipment.com/products/mission-darkness-large-non-window-faraday-bag> (Son Er. T.: 30.05.2019).

İncelenme maksadıyla emanete ya da laboratuvara teslim edilen dijital deliller envanter olarak kayıt altına alınmalı, bulundukları ortamda ısı, nem, statik elektrik ve manyetik alandan etkilenmeyecek şekilde muhafaza edilmeleri gerekmektedir.⁸⁰

Tıpkı klasik delillerin toplanılmasında olduğu gibi dijital deliller toplanırken de delil teslim zinciri bilgileri kayıt altına alınmalıdır. Delil teslim zinciri, dijital delilin kime ait olduğu, bu delille kimlere, ne zaman ve hangi sebeple erişim yapıldığı, delil muhafaza dolabına ne zaman ve kim tarafından konduğu ve son olarak delil üzerinde zorunlu bir değişiklik yapıp yapılmadığı, eğer yapıldıysa kim tarafından yapıldığı bilgilerini içermektedir.⁸¹

2.7.3. Dijital Delillerin İncelenmesi

Dijital deliller toplandıktan sonra inceleme aşamasına geçilmektedir. Ancak bu aşamaya geçmeden önce arama işlemi esnasında elde edilen imajın birebir kopyalanması, imajının alınması gerekmektedir. Bu imaj üzerinde yapılacak olan çalışmalar muhtemel bir hata sonucu delil bütünlüğünün kaybolmasının önüne geçecektir.



Şekil- 11: Adli Bilişim İncelemesi sırasında genellikle yapılan işlemler⁸²

80 Henkoğlu, s. 25.

81 Çakır ve Kılıç, s. 150.

82 <https://www.adlibilisimuzmani.com/adli-bilisimde-elektronik-delillerin-incelenmesi/> (Son Er. T.: 30.05.2019).

2.7.4. Dijital Delillerin Raporlanması

Adli bilişimde delillerin toplanması ve inceleme/analiz aşamalarını raporlandırma işlemi takip etmektedir. Adli bilişim uzmanı, Cumhuriyet Savcısı adına delilleri, delil bütünlüğünü koruyarak toplamakta, delillerin inceleme ve analizini yaparak buradan çıkan sonucu raporlandırmaktadır. Adli bilişim bilirkişisi ise delilleri Cumhuriyet Savcısı ya da Hakim'den, görevlendirme durumunda arama noktasından almaktadır. Delil bütünlüğünün kolluk tarafından korunup korunmadığını kontrol eden adli bilişim bilirkişisi delillerin analiz ve incelemesini gerçekleştirerek adli ubilişim uzmanının raporunun değerlendirmesini yapmaktadır. İnceleme sırasında yapılan tüm işlemler ve elde edilen sonuçlar bilirkişi tarafından adli makamlara sunulur ve teslim edilen mühür altındaki aygıt ve gereçler de bir tutanakla beraber ilgili mercie ulaştırılır.⁸³

Bilirkişi raporunun hazırlanması, bilirkişinin duruşma evresinde karşılaşacağı muhtemel durumlar, bilirkişinin reddi ve bilirkişilikten çekinme ile alakalı hususlar, Ceza Muhakemesi Kanunu'nun 67. ve 68. maddelerinde düzenlenmiştir.

Adli bilişim sürecinde ortaya konan tüm çalışmaların bir neticesi olması hasebiyle raporlama aşaması oldukça önemlidir ve bu nedenle öncelikle anlaşılır, açık, kısa ve öz olmalıdır. Raporlama işlemi, veri toplama, elde edilen sonuçların analiz edilmesi, rapora dair bir taslağın oluşturulması, rapora son şeklini verme ve raporun en son halinin gözden geçirilmesi olmak üzere belirli safhalardan geçmektedir. Söz konusu raporda suça konu olay hakkında bilgiler, incelemenin özeti, üzerinde inceleme yapılan delillere ilişkin bilgiler, istifade edilen kaynaklar, elde edilen delillerin ne zaman ve kime verildiği bilgisi, inceleme neticesinde hangi bulgulara ulaşıldığı ve hash hesaplamaları gibi bilgilere yer verilmesi gerekmektedir. Raporların eklerinde incelenmesi talep edilen video, resim ya da programlara ve işletim sistemine ilişkin olay günlükleri de muhakkak yer almalıdır. Ayrıca rapor teknik açıdan doğru ve bilimsel hazırlanmalı, adli bilişime özel tanım ve terimler sade, herkesin anlayacağı şekilde açıklanmış olmalıdır.⁸⁴

Bilirkişi, yapacağı tarafsız, objektif ve mevcut standartlara uygun bir raporlamanın her daim hakim kararını etkileyebileceği bilinciyle hareket etmelidir. Özellikle taşrada

83 Henkoğlu, s. 241.

84 Henkoğlu, s. 242

yeterli sayıda adli bilişim uzmanı bulunmadığından, mahkemeler özensiz ve standarttan uzak raporlarla karşı karşıya kalmaktadırlar. Kimi zaman da raporun ya sadece sonuç kısmı üzerinden bir hükme varılmakta ya da yetersiz görülen rapor tekrar başka bir bilir-kişiyeye gönderildiği için süreç gereksiz yere uzatılmaktadır.⁸⁵

2.8. ADLİ BİLİŞİM LABORATUVARLARI VE ÖZELLİKLERİ

Olay yerinde ele geçirilen bilişim aygıtları adli bilişim uzmanı tarafından analiz edilirken hedef, güvenilir, yargı makamları tarafından kabul edilebilir deliller elde edebilmektir. Bu hedefe ise ancak tam donanımlı, alanında uzmanların aktif olduğu bir çalışma ortamı ile ulaşmak mümkün olmaktadır.

Türk Polis Teşkilatı içinde adli bilişim laboratuvarları barındırmakta, bu nedenle adli bilişimin tüm evrelerinde kolluk kuvvetleri de yer almaktadır. Her ne kadar kolluk kuvvetleri söz konusu işlemleri görevi dahilinde eksiksiz ve güvenilir bir şekilde icra ediyor olsa da, bu durum aynı işlemlerin dünyadaki örneklerinde olduğu gibi bağımsız bir kuruluş, üniversite birimleri ya da özel şirketler tarafından yapılamayacağı anlamına gelmemelidir. Zira özel kurum ve kuruluşların söz konusu inceleme sürecine katılması, analiz işlemlerinin daha efektif ve hızlı bir şekilde yol almasını sağlayacaktır.



Şekil- 12: Adli Bilişim Laboratuvarı⁸⁶

85 Çakır ve Kılıç, s. 506.

86 <https://www.difose.com.tr/laboratuvar/> (Son Er. T.: 30.05.2019).

İdeal bir adli bilişim laboratuvarında bulunması gereken en önemli özelliklerden biri öncelikle fiziksel olarak güvenli olmasıdır. Toplama aşamasında ele geçirilen delillerin her türlü manipüleden uzak, yüksek güvenli bir ortamda analiz edilmesi delillerin doğruluk ve inanılabilirliğini de yargı aşamasında perçinleyecektir.



Şekil- 13: Adli Bilişim Laboratuvarı⁸⁷

Laboratuvarda analiz için kullanılan yazılımların lisanslı ve denetlenebilir olması gerekmektedir. Adli incelemeye tabi bilişim cihazlarının çok çeşitli olduğu düşünülürse, inceleme esnasında çıkabilecek her türlü komplikasyonu aşabilmek için halihazırda kullanılan yazılımların çeşitleri ve eski sürümleri de mümkün mertebe laboratuvarda bulundurulmalıdır. Laboratuvarda bulunan bilgisayarların kullanım alanlarına ve teknik özelliklerine göre (analiz etme ya da şifre kırma gibi) sınıflandırılması inceleme işleminin hızı ve güvenilirliği açısından önemlidir. Adli inceleme yapılan bir laboratuvarda güvenlik ve analiz konusunda belirli standartların bulunması gerekmektedir. Ne var ki, konuya ilişkin yasal bir çerçeve bulunmamakta, bu alanda faaliyet gösteren özel kuruluşların ne kadar büyük olacağı ya da hangi donanım ve yazılımlara sahip olması gerektiği hususunda herhangi bir düzenleme bulunmamaktadır. Adli bilişimde binlerce yazılım ve donanımın söz konusu olduğu düşünüldüğünde, yasal bir düzenlemenin olmaması mantıklı gibi görünmektedir. Zira bu kadar yazılım ve donanım arasından birinin seçilip zorunlu kılınması, seçim bakımından problemli olacağı gibi, seçim dışı kalan üretici firmaları da muhtemelen bir hukuk mücadelesine itecektir. Bununla beraber bulguların, dünyada doğruluğu ve güvenilirliği kabul görmüş yazılım ve donanımlarla desteklenmesi, bunların mahkemelerce de daha kabul edilebilir bir pozisyona taşıdığı gözlemlenmektedir.⁸⁸

Gerek özel gerek kamuda hizmet veren adli bilişim laboratuvarlarına, belli bir

87 <http://tuncaybesikci.com/adli-bilisim-nedir/> (Son Er. T.: 30.05.2019).

88 Henkoğlu, s. 39.

standart dahilinde değerlendirilmek suretiyle sertifika verilmesi, bu laboratuvarlarda elde edilen bulgulara karşı bir güven oluşmasını sağlayacak önemli bir faktördür. Ancak Türkiye’de adli inceleme yapan laboratuvarlar, ABD’de bulunan ‘American Society Of Crime Lab Directors’ gibi bir kuruluş tarafından derecelendirmeye tabi tutulmamaktadır.⁸⁹

Adli bilişim laboratuvarları meydana gelebilecek doğal afet ya da hırsızlık gibi olaylara karşı fiziksel güvenlik tedbirleri almalıdır. Güvenlik alanında bulunan odalara erişim sınırlı tutulmalı, kapılarda şifreli kilitler kullanılmalı, bu alanlarda sadece yetkili kişilerin giriş ve çıkışlarına müsaade edilmeli, 24 saat aktif kamera ve alarm sistemi bulunmalıdır.

Dikkat edilmesi gereken bir diğer husus ise adli bilişim laboratuvarının hareket kabiliyetine sahip olmasıdır. Örneğin, olay yerinde delil toplamakla görevli kolluk kuvvetlerinin faal oldukları laboratuvarların, veri toplama, analiz ve kopyalama işlemlerini yerine getirebilecek mobil bilgisayarların yanısıra birebir kopyalamada kullanılan tek yönlü yazma cihazları, taşınabilir optik depolama üniteleri, çeşitli bağlantı kabloları ve başkaca donanımları bulundurması gerekir. *“Depolama üniteleri de analiz işlemleri öncesinde ve analiz esnasında en çok ihtiyaç duyulan donanım birimleridir. Bu nedenle, IDE, SCSI sabit diskler, zip sürücüler, teyp üniteleri ve kartuşları, optik sürücüler ve floppy sürücüler gibi çeşitli tür ve kapasitelerde depolama üniteleri laboratuvar ortamında her an hazır bulunmalıdır.”*⁹⁰

Her bir olay yerinin özelliğine göre, bu tür mobil birimlerin varlığı ve donanımsal kalitesi adli sürecin gidişatını, hatta neticesini değiştirebilecek öneme sahiptir.

2.9. ADLİ BİLİŞİMDE KULLANILAN YAZILIMLAR VE ÖZELLİKLERİ

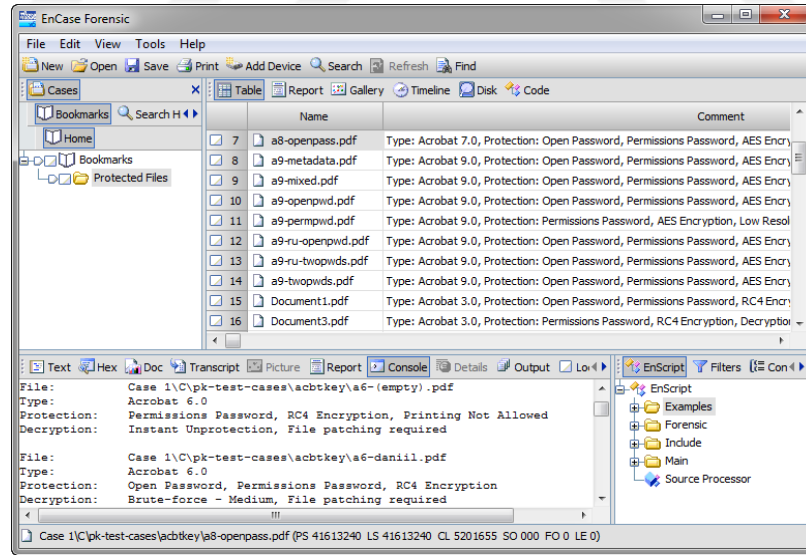
Adli bilişimde genel itibarıyla 2 tür yazılım kullanılmakta, ticari ve ücretsiz olarak sınıflandırılmaktadır. Doğası gereği halihazırdaki teknoloji pazarında sayısı yüzlere varan birçok yazılım çeşidi bulunmakta, ancak adli bilişim uzmanlar tercihini uluslararası

⁸⁹ Henkoğlu, s. 39.

⁹⁰ Henkoğlu, s. 40.

kurum/kuruluşlar ve ulusal mahkemeler nezdinde doğruluğu ve güvenilirliği kanıtlanmış yazılımlardan yana kullanılmaktadırlar.⁹¹

Adli bilişimde yazılımların bazı spesifik özellikleri içermesi tercih edilmeleri açısından önemlidir, öyle ki, yapı ve işleyişlerinin delillerin elde edilmesi sırasında herhangi bir tahribata yol açmaması, verilerin en sağlıklı şekilde toplanmasını mümkün kılması, sahip oldukları işleyiş sisteminin güvenilir olması, analiz sonrasında elde edilen verilerin tekrar edilebilir niteliği taşıması bu özelliklere örnek olarak gösterilebilir. Ticari yazılımlar, ücretsiz yazılımlarla karşılaştırıldığı zaman sahip oldukları kolay kullanım ara yüzü, teknik destek ve detaylı rapor verebilme imkanı, süratli güncellenebilme ve Windows işletim sistemiyle uyumlu çalışabilme kabiliyeti özellikleri sebebiyle tercih edilmektedirler. Ancak ne var ki, söz konusu yazılımlar aynı zamanda hem satın alma hem zorunlu sistem güncellemeleri, hem de sertifikasyon ücretleri yönüyle oldukça yüksek maliyetli olabilmekte, özellikle kullanılan programlar üzerinde teknik sebeplerden dolayı herhangi bir değişiklik yapılamaması nedeniyle de tercih dışı kalabilmektedirler. Encase, Access data Forensics Tool Kit, Paraben gibi yazılımlar sık kullanılan ticari adli bilişim yazılımlarında ön plana çıkmaktadır.⁹²

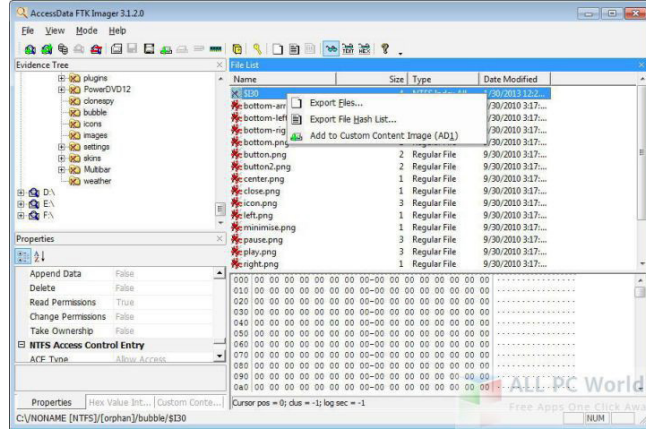


Şekil-14: EnCase Forensic⁹³

91 Henkoğlu, s. 43.

92 Henkoğlu, s. 44.

93 <https://support.passware.com/hc/en-us/articles/221742468-How-to-use-Passware-Kit-Forensic-with-Guidance-Software-EnCase> (Son Er. T.: 30.05.2019).



Şekil-15: AccessData FTKImager 3.1.2.0⁹⁴

Herhangi bir sebepten dolayı ticari bir adli bilişim yazılımı tercih edilmediyse, alternatif olarak yine güvenilir hale gelmiş olan açık kaynak kodlu yazılımlar kullanılabilmektedir. Bu yazılımların özellikleri arasında internet ortamında kolayca indirilebilme, kurulabilme ve çalıştırabilme imkanı yer almaktadır. Çoğu zaman ücretsiz ya da ucuz olan, lisans gereksinimi bulunmayan ve rahat temin edilebilen bu yazılım türleri bir dezavantaj olan kullanım zorluğu yüzünden ise ancak gerçekten uzman ve eğitimli kişilerce çalıştırabilmektedir. Açık kaynak kodlu yazılımlarına örnek olarak Linux dd, Autopsy ve The Sleuth Kit, Helix gibi örnek göstermek mümkündür.⁹⁵

```
ubuntu@ubuntu: ~
ubuntu@ubuntu:~$ sudo fdisk -l /dev/sda
Disk /dev/sda: 60 GiB, 64424509440 bytes, 125829120 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
ubuntu@ubuntu:~$ sudo fdisk -l /dev/sdb
Disk /dev/sdb: 30 GiB, 32212254720 bytes, 62914560 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xfca79835

Device      Boot    Start        End    Sectors    Size Id Type
/dev/sdb1   *            2048    1026047    1024000    500M  7 HPFS/NTFS/exFAT
/dev/sdb2             1026048   44898303   43872256    20.9G  7 HPFS/NTFS/exFAT
ubuntu@ubuntu:~$
```

Şekil- 16: Linux dd ⁹⁶

94 <http://allpcworld.com/forensic-toolkit-ftk-imager-free-download/> (Son Er. T.: 30.05.2019).

95 Henkoğlu, s. 44.

96 <https://www.howtoforge.com/tutorial/linux-dd-command-clone-disk-practical-example/> (Son Er. T.: 30.05.2019).

Bir adli bilişim yazılımından en efektif şekilde faydalanabilmek, doğru ve güvenilir veriler ortaya koyabilmek için, yazılımın bazı temel özelliklere sahip olması gerekmektedir. Disk kopyalama ve imaj alma işlemi yapmanın yanında, imajı alınan diskler üzerinde bulunan tüm dosya sistemlerini vs. okuyabilme özellikleri bu hususta örnek olarak gösterilebilir.

2.10. ADLİ BİLİŞİM UYGULAMALARINA İLİŞKİN ULUSLARARASI ANLAŞMALAR & ÖRGÜTLER

İnternet ağının ulusal sınırları geçerek geniş bir alana yayılması, bu gelişmiş ağ aracılığı ile işlenen bilişim suçlarının rahatlıkla uluslararası alana kaymasına sebep olmuştur. Failler, ülkeler arası yeterli düzeyde teknik ve hukuki bir iş birliği sağlanamadığından geniş bir hareket alanında denetimden uzak farklı iletişim ağlarıyla suç işleyebilmekte, kendi aralarında çeşitli suç örgütleri kurabilmektedirler.

Hatta son yıllarda artan bir oranda siyasi amaçlı organize siber suç örgütleri oluşmaya başlamış, başka devletlerin güvenlik ya da bilişim sistemlerine gönüllü olarak siber saldırılarda bulunmaya başlamışlardır.

Uluslararası platformda büyük bir ivme kazanan tüm bu olumsuz gelişmeler, adli olay incelemelerine de yansımaktadır. Zira diğer hukuki alanlarda olduğu gibi adli bilişim alanında da uluslararası düzeyde ortak adli inceleme, kontrol ve yaptırımların gerekliliği kaçınılmaz hale gelmiş, bu alanda aktif olan türlü resmi kuruluş ve gönüllülerin çabası bazı uluslararası organizasyon ya da örgütlerin oluşumuna katkıda bulunmuştur.

2.10.1. BİRLEŞMİŞ MİLLETLER

Bilişim suçları Birleşmiş Milletlerin Uluslararası Telekomunikasyon Birliği'nin gerçekleştirmiş olduğu düzenlemeler ile kontrol altına alınmaya çalışılmaktadır. Bununla beraber aynı örgütün Uyuşturucu ve Suçlarla Mücadele Bürosu da bu alanda aktif faaliyetlerde bulunmaktadır. Sayısal suçlara ilişkin ilk düzenleme 1988 yılında, ki bu tarihte internet kullanımı 2000'li yıllara kıyasla henüz çok fazla yaygın değildir, ITR tarafından

kabul edilmiştir. Siber suçların kanun düzeyinde düzenlemesi ise 1990 yılında 8. Birleşmiş Milletler Suçun Önlenmesi ve Suçlu Muamelesi kongresinde gerçekleştirilmiştir. 2000’li yıllara gelindiğinde ise BM Genel Meclisi 55/63 numaralı kararı ile üye ülkelerin bilgisayar teknolojisinin bilişim suçu kapsamında kullanılmasının önüne geçecek kanun ve uygulamalarının geliştirileceğini teminat altına almasını, bilişim sistemlerinin ve veri gizliliğinin yetkisiz erişimden korunması için her türlü yasal tedbir ve yaptırımları uygulamasını kararlaştırmıştır.⁹⁷

Bilişim suçlarının önlenmesi hususunda ise 2010 yılında ulusal alanda teknik ve hukuki gelişmelere ilişkin bilgi alışverişi, teknik destek ve uluslararası eş güdümlü çalışma grupları oluşturulması 65/230 numaralı karar ile imza altına alınmıştır. Konuya ilişkin son düzenleme ise 2012 yılında Dubai’deki Dünya Telekomünikasyon Konferansı’nda 89 ülke tarafından imzalanmış ve kabul edilmiştir.⁹⁸

2.10.2 BUDAPEŞTE SÖZLEŞMESİ - AVRUPA KONSEYİ (COUNCIL OF EUROPE)

Öncelikle 1997 yılında Avrupa Konseyi tarafından Siber Uzayda Suç Uzmanları komitesi oluşturuldu. 2001 yılında ise Budapeşte Sözleşmesi imza altına alındı. Haliha-zırda 35 ülke söz konusu sözleşmeyi imzalamış ve kabul etmiştir. Türkiye’de yürürlüğe girme tarihi ise 2004 tür. Sözleşmenin temel hedefi taraf ülkelerde siber suçlara ilişkin iç hukuk düzenlemelerinin yapılması ve elektronik delillerin söz konusu olduğu suç tipleri-nin soruşturma ve kovuşturulmasına ilişkin ulusal usul hukukunun düzenlenmesini sağla-maktır. Bir diğer amaç, siber suçlarla mücadele konusunda etkin ve hızlı bir uluslararası işbirliği ağının kurulmasıdır.⁹⁹

Avrupa Konseyi Siber Suç Sözleşmesi’nin ceza muhakemesiyle alakalı hüküm-leri 14. ve 21. maddeler arasında yer almaktadır. Koruma tedbirlerinin konusunu dijital ortamda depolanmış veya iletişim safhasındaki, trafik, içerik ve abone dataalarını da kap-

97 Gökhan Şengül, “Adli Bilişim Alanındaki Mevcut Problemler, Çözüm Önerileri ve Gelecek Öngörüler”, 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 17-18 Ekim 2014, İstanbul, s. 97.

98 http://www.mfa.gov.tr/no_-299_-ulkemizin-itu-konsey-uyeligi-hk.tr.mfa (Son Er. T.: 30.05.2019).

99 <https://www.sibersan.com/sanal-ortamda-islenen-suclar-sozlesmesi-6533-sayili-yasa/> (Son Er. T.: 30.05.2019).

sayan her türlü bilgisayar verisi oluşturmaktadır.

Bu tedbirler klasik elkoyma tedbirlerinin siber suçlara uyarlanmış hali olmakla beraber, sözleşmede oldukça detaylı bir şekilde düzenlenmiş ve taraf devletlere de bu hükümlerle uyumlu düzenlemeler yapma mükellefiyeti yüklenmiştir.

2.10.3. İKTİSADİ İŞBİRLİĞİ VE KALKINMA ÖRGÜTÜ

(ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT: OECD)

Sayısal suçlar konusunda önemli adımlar atan ilk uluslararası örgütlerden biri de OECD'dir. Anlaşma imzalama yetkisi olmayan bu örgüt tüm dünyada kabul gören bir çalışma politikası oluşturmayı hedeflemektedir. Bu anlamda yaptığı çalışmalar arasında 2002 yılında *Bilgi Sistemleri ve Ağ Güvenliği: Güvenlik Kültürüne Doğru*, 2008'de Çevrim İçi Kimlik Hırsızlığı Raporu, 2009 yılında ise Çevrimiçi Kimlik Hırsızlığı Konusunda OECD Politika Rehberi gibi yayınlar bulunmaktadır.¹⁰⁰

2.10.4. KUZEY ATLANTİK ANTLAŞMASI ÖRGÜTÜ

(NORTH ATLANTIC TREATY ORGANIZATION: NATO)

Kuruluş amacı gereği NATO, uygulamalarını bünyesindeki ülkelere karşı gerçekleştirilen saldırılarla sınırlı tutmaktadır. Bu konudaki çalışmalardan biri Nato Kıdemli Sivil Acil Durum Planlama Komitesi (SCEPC) sivil halkın ve önemli altyapıların kritik saldırılara karşı korunması amacıyla üye ülkelere yaptığı yardımdır. Bunun yanı sıra NATO Sivil İletişim Planlama Komitesi (CCPC) ise genel ve özel iletişim altyapısıyla ilgili çalışmalarda bulunmaktadır. Bu çalışmalar kapsamında ülkemizde Ankara'da 2008 yılında NATO Terörizmle Mücadele Mükemmeliyet Merkezi faaliyete geçirilmiştir.¹⁰¹

100 <http://www.mfa.gov.tr/ekonomik-isbirligi-ve-kalkinma-teskilati.tr.mfa> (Son Er. T.: 30.05.2019).

101 <http://www.mfa.gov.tr/nato-tarihce.tr.mfa> (Son Er. T.: 30.05.2019).

2.10.5. ASYA PASİFİK EKONOMİK İŞBİRLİĞİ KURULUŞU (ASIA-PASIFIC ECONOMIC COOPERATION: APEC)

Bünyesinde ABD, Rusya ve Çin gibi ülkeleri barındıran APEC, 1990 yılında Bilgi ve İletişim adlı bir çalışma grubu hayata geçirmiş, kendi altında Liberalleşme Yönlendirme Grubu, Bilgi ve İletişim Teknolojileri Geliştirme Yönlendirme Grubu ve Güvenlik ve Geliştirme çalışma grubu olmak üzere 3 grup daha kurmuştur. Güvenlik ve Geliştirme Çalıştırma grubu faaliyet alanları içerisinde ağ, altyapı, servis, çeşitli teknolojik uygulamalara ilişkin güvenlik stratejileri bulunmakta, bununla birlikte siber suçların önlenmesinde etkili olan Bilgisayar Acil Durum Müdahale Ekibi ve Bilgisayar Güvenliği Olay Müdahale Ekibi gibi oluşumlara destek vermektedir.¹⁰²

2.10.6. ŞANGAY İŞBİRLİĞİ ÖRGÜTÜ (SHANGAI COOPERATION ORGANIZATION: SCO)

Örgüt 2009 yılında Yaketerinburg Açıklaması ile uluslararası alanda bilgi güvenliğini ön plana çıkarmıştır. 2012 yılında Pekin’de yapılan toplantıda üye ülke liderleri SCO’nun siber suçlarla mücadelede işbirliği yapacağı konusunda mutabık kalmışlardır.¹⁰³

2.10.7. SANAL KÜRESEL GÖREV GÜCÜ (VIRTUAL GLOBAL TASKFORCE:VGT)

Sanal Küresel Görev Gücü, Avustralya, Kanada, İngiltere, ABD, Birleşik Arap Emirlikleri, İtalya, Yeni Zelanda ve hatta İnterpol ve Europol’un üye olarak faaliyet gösterdiği, kanun uygulama noktasında işbirliği yaptığı bir örgüttür. Faaliyet alanları içerisinde çocuk cinsel istismarına ilişkin sivil toplum örgütleriyle gerçekleştirdiği çalışmalar da vardır.¹⁰⁴

102 Şengül, s. 97.

103 Şengül, s. 98.

104 Şengül, s. 98.

2.10.8. SİBER SUÇLAR ÇALIŞMA GRUBU STRATEJİK İTTİFAKI

Siber suçlarla mücadele konusunda aktif olan Siber Suçlar Çalışma Grubu Stratejik İttifakı, ABD, Kanada, Yeni Zelanda, Avustralya ve İngiltere'nin üye olduğu bir örgüttür.

Yukarıda zikredilen uluslararası faaliyetlerin amacı öncelikle bilişim suçlarıyla mücadeledir. Bu hedefi gerçekleştirebilmek için ise gerek suç araştırma ve inceleme gerekse delillendirme aşamalarında uluslararası bir işbirliği sağlanmalıdır.¹⁰⁵



105 Şengül, s. 98.

3. DİJİTAL DELLİLER

3.1. DİJİTAL DELİLLER

Bilişim hukuku çerçevesinde değerlendirildiğinde dijital deliller ceza hukuku ve ceza muhakemesi hukuku yanında usul hukuku gibi birçok hukuk dalıyla yakından bağlantılıdır.

Ceza Muhakemesinde delil, yargılama konusu olayın aydınlatılması, maddi gerçeğin ortaya çıkarılması amacıyla kullanılan araçlara verilen addır.¹⁰⁶

Ceza hukukunda delil serbestisi geçerlidir, ancak buna rağmen ispat aracı olarak hizmet eden delillerin bazı özelliklere sahip olması gerekmektedir. Delil, yargılama konusu olayın tümünü ya da bir kısmını ispat edebilmeli, 5 duyu organıyla algılanabilmeli, elde edilebilir, hukuka uygun, müşterek, akılcı, sağlam ve güvenilir olmalıdır.¹⁰⁷

“Dijital deliller ise, adli bilişim uzmanlarının suçla bağlantılı bilişim cihazlarından birçok teknik yöntemle elde ettiği adli delillere verilen addır.”¹⁰⁸

Dijital delil mahkemelerde sıkça müracaat edilen bir delil türüdür. Ancak bu deliller aynı zamanda üzerinde en çok spekülasyon yapılan, kolayca suistimal da edilebilen özelliktedirler. Her geçen gün değişen ve gelişen teknolojik imkanlarla bu tarz delillere sonradan müdahale imkanı kısıtlanabiliyorsa da, güvenlik testleri ve bilirkişilik kurumunun daha da güçlendirilmesi gerekmektedir.

3.1.1. Dijital Delillerin Nitelikleri

Soruşturma veya kovuşturma aşamasında elektronik aygıt ya da aygıtlardan elde edilen verilerin dijital delil olarak kullanılabilmesi için bazı özelliklere sahip olması gerekmektedir:

¹⁰⁶ Yener Ünver ve Hakan Hakeri, Ceza Muhakemesi Hukuku, (Ankara: Adalet Yayınevi, 2017), s. 596.

¹⁰⁷ Ünver ve Hakeri, s. 597.

¹⁰⁸ Henkoğlu, s.5.

- ***“Dijital delil kabul edilebilir (admissible) olmalıdır.”***¹⁰⁹

Elde edilen elektronik delil hem yargı mensubu otorite hem de diğer kişiler tarafından akla uygun olarak kabul edilebilir olmalıdır.

- ***“Dijital delil gerçek ve akla uygun (authentic) olmalıdır.”***¹¹⁰

Suçla ilişkin mahkemeye sunulacak olan delillerle soruşturma veya kovuşturmayla konu suç arasında bir illiyet (nedensellik) bağı olması gerekmektedir. Elde edilen adli delilin soruşturma ya da kovuşturma ile bağlantılı olduğu kesin ve net bir şekilde ortaya konulabilmelidir.

- ***“Dijital delil tamam ve eksiksiz (complete) olmalıdır.”***¹¹¹

Elektronik cihazda delil niteliğindeki tüm veriler toplanmalıdır. Bu deliller, faile suç yükleyen nitelikte olabileceği gibi, suçsuzluğunu ispatlar özellikte de olabilir.

- ***“Dijital delil güvenilir (reliable) olmalıdır.”***¹¹²

Elektronik ortamdan kazanılan deliller teknik anlamda analiz için kabul görmüş olan prosedürlere uygun olmalı, doğruluğu konusunda hiçbir şüpheye mahal vermemelidir.

- ***“Dijital delil inanılır (believable) olmalıdır.”***¹¹³

Yargıya sunulan dijital deliller kanıt değeri taşımalı, net bir şekilde anlaşılabilir ve inanılabilir olmalıdır.

109 Yusuf Başlar, Ceza Yargılamasında Elektronik Delil (Ankara: Yetkin Basımevi, 2016), s. 88.

110 Başlar, s. 88.

111 Başlar, s. 88.

112 Başlar, s. 88.

113 Başlar, s. 88.

- ***“Dijital delil yasaya uygun olmalıdır.”***¹¹⁴

Dijital deliller de dahil olmak üzere tüm deliller mevcut yasalara uygun elde edilmiş olmalıdır, zira 5271 sayılı CMK’ nın 134.maddesine aykırı olarak bilgisayarlarda, arama, kopyalama veya elkoyma işlemi yapılmışsa, elde edilen deliller mahkemece delil olarak değerlendirilmeyecektir.

- ***“Dijital delil tekrar edilebilir olmalıdır.”***¹¹⁵

Mahkemede ortaya konan dijital deliller aynı yöntem ve tekniklerle farklı kişiler tarafından da elde edilebilir, ulaşılabilir olmalıdır.

3.1.2. Dijital Delillerin Elde Edilmesi

Kullanıcının sistem üzerinde yapmış olduğu her türlü işlem, kullanmış olduğu program ve uygulamalara ait bilgiler ile işletim sisteminin hafızasındaki kayıtlar birbirini ve aynı zamanda dijital delilden elde edilen sonucu doğrular nitelikte olmalıdır.

*“Kullanıcının internet kullanım ve gerçekleştirmiş olduğu işlemlerinin kayıtları ile beraber uzaktan erişim ve ağ kaynakları kayıtları da adli bilişim uzmanına analiz için gerekli olan delil kaynakları arasındadır. Bu kaynaklara, program ve işletim kurulum kayıtları, işletim sistemi olay kayıtları, güvenlik duvarı kayıtları, uygulama kayıtları, ağ cihazları ve hata kayıtları örnek olarak gösterilebilir”*¹¹⁶. Bu kayıtlar öncelikle program ve işletim sistemi kurulum kayıtları, bunlar üzerine kurulmuş olan programların ve kurulumla ilişkin bilgilere sahip kayıt dosyalarıdır. Aynı zamanda kurulum esnasında gerçekleştirilmiş olan işlemlerin başarıyla tamamlanıp tamamlanmadığını, buna ilişkin tarih ve zaman bulgularını da içerir.

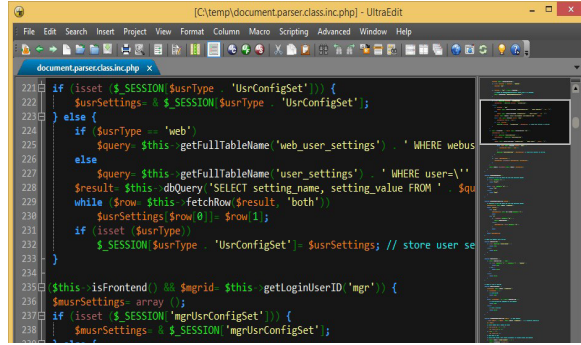
Bilgisayarın bünyesindeki program kayıtlarının incelenmesi özellikle cyber-crime yani bilgisayarlar aracılığı ile işlenen suçların, kriptolu ya da şifrelenmiş dosyaların ana-

114 Başlar, s. 88.

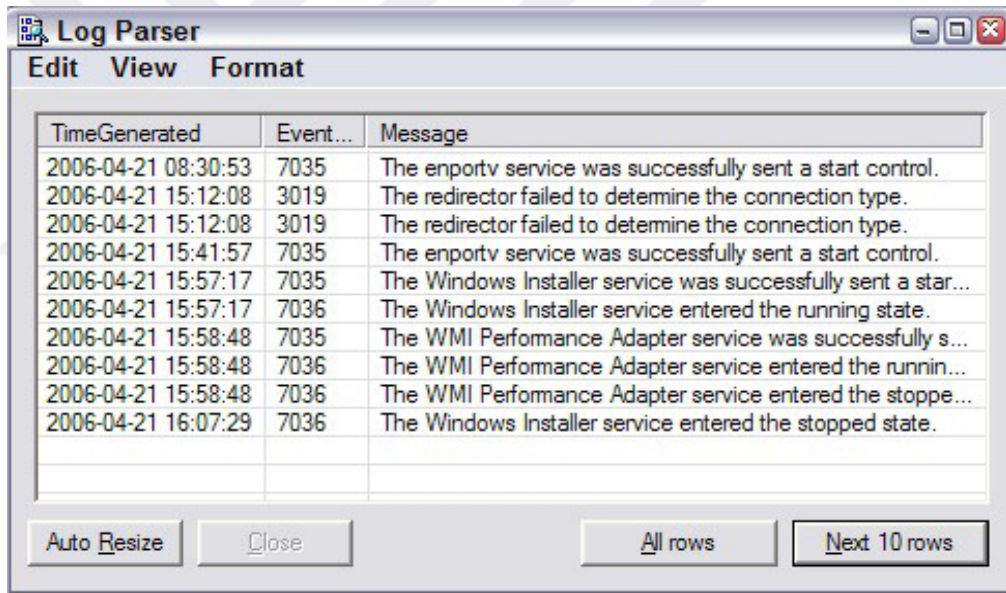
115 Başlar, s. 88.

116 Henkoğlu, s. 95.

lizinden veriler elde edilinceye kadar geçen zamanın (şifreli programlarda şifre kırılması, algoritma kullanılan programlarda algoritmanın çözülmesi) kısaltılması yönüyle büyük önem taşır. UltraEdit, Microsoft Log Parser gibi not defteri şeklinde geliştirilmiş birçok program yardımıyla metin bazlı program kayıtları analiz edilebilir.¹¹⁷



Şekil-17: UltraEdit¹¹⁸



Şekil-18: Log Parser¹¹⁹

Kurum veya kuruluşlarda bilgisayar ağına bağlı bilgisayarlara yetkisiz bir şekilde donanım cihazlarının eklenmesi ya da yabancı programlar kurulması gibi işlemler de program kurulum kayıtları yardımıyla ortaya çıkarılabilir.

117 Henkoğlu, s. 96.

118 <https://www.ultraedit.com/company/blog/products/2015-ultraedit-v22.html> (Son Er. T.: 30.05.2019).

119 <https://www.jasonsamuel.com/2010/01/12/using-log-parser-to-query-huge-log-files-and-only-display-the-results-you-need/> (Son Er. T.: 30.05.2019).

Analiz aşamasında elektronik delil elde edilebilecek bir diğer alan olay günlükleridir. Olay günlükleri işletim sistemi tarafından kayıt altında tutulur. İşletim sistemi olay günlüğü, uygulama, güvenlik ve sistem kayıtları adlı 3 ana bölümü kapsar. *“Uygulama ve sistem kayıtları işletim sistemi tarafından otomatik olarak kaydedilirken, güvenlik kayıtlarının yapılabilmesi için ayrıca denetim ilkelerinin açılması gerekir. Uygulama olayları, hata, uyarı ve bilgi başlıkları altında sınıflandırılarak kaydedilirler.”*¹²⁰

Antivirüs programları işletim sistemi üzerine kurulan uygulamalardan biridir. Antivirüs programına dair güncellemeler ve bu programın sisteme zararlı kodları saptayıp yok etmesi gibi işlemler uygulama olayları bünyesinde kayıt altına alınır. Yetkisiz erişimin söz konusu olduğu durumlarda bir bilgisayara kimin, ne zaman erişim sağladığına ilişkin veriler bu kayıtlarda bulunmaktadır.¹²¹

Sabit disk ya da CD/DVD sürücülerin bünyesinde muhtemel sorunları ortadan kaldırma amacıyla bazı özel alanlar bulunmaktadır. Söz konusu alanlar bilişim suçlarında kullanıcıların veri gizleme alanı olarak kullanılabilmekte, bu yüzden şüpheli bilgi barındırma ihtimali yüzünden adli incelemelerde özellikle taranmaktadırlar.

Günümüzde iletişimin en yaygın olduğu türlerden biri de e-posta kullanımınıdır. İnternet dolandırıcılığından hakaret ve virüs içerikli iletilere kadar birçok bilişim suçunun işlenmesinde önemli bir rol alan e-postalar, işlenen suç hakkında veri elde edilebilecek alanlardan biridir. E-postaların incelenmesi esnasında iletilerin bulunduğu hizmet sağlayıcısı ve kullanıcının bu servisten faydalanırken kullanmış olduğu araçlardan (Web Arayüzü, Outlook) kaynaklı bazı sorunlar ortaya çıkabilmektedir. Öyle ki, eğer kullanıcı Web Arayüzü tercih etmişse, adli bilişim uzmanının e-posta iletişi üzerinden delil elde etme ihtimali de azalabilmektedir. Üzerinde inceleme gerçekleştirilen bilgi depolama birimi e-posta sunucusuna aitse, adli incelemenin yapılabilmesi için çok daha fazla zaman gerekecektir.

Her geçen gün daha da yoğun kullanılan cep telefonları sahip oldukları işletim sistemi ve donanımlar nedeniyle dijital delillerin elde edilebileceği elektronik cihazlardan biridir. Cep telefonlarında tutulan kayıtlar işletmeciler tarafından 9 ay boyunca gerek iz-

120 Henkoğlu, s. 96.

121 Henkoğlu, s. 96.

leme gerekse geriye yönelik fatura kontrolü amacıyla saklanmakta, kullanıcıların kimle, ne zaman, ne kadar süreyle konuştuğu, kaç mesaj yazdığı arzu edildiğinde Telekomünikasyon İletişim Başkanlığı'na verilebilmektedir.

Cep telefonları tıpkı diğer bilişim cihazları gibi analiz edilirken kendileri için özel geliştirilmiş özel donanım ve yazılımlara ihtiyaç duyarlar. Adli bilişim laboratuvarlarında daha çok donanımsal cihazlar kullanılmaktadır.

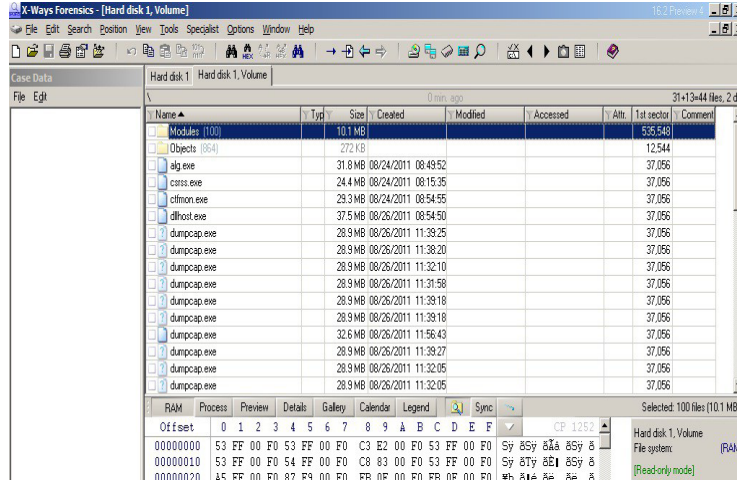
Özel yazılımlar ile incelenen cep telefonlarının analizi esnasında “*adli bilişimciler telefonla bilgisayar arasında gerekli olan bağlantı kablosunu bulmak ya da telefonun bilgisayara tanımlanabilmesi için uygun sürücüyü yüklemek gibi çeşitli problemlerle karşılaşabilmektedirler.*”¹²²

Adli soruşturmada kolluk kuvvetleri arama/elkoyma işlemlerini gerçekleştirirken, sadece cep telefonuna değil aynı zamanda ele geçirilen cep telefonuna ait bağlantı kabloları ve şarj cihazlarına da elkoymaktadır.

Özellikle iş ve eğitim alanında büyük rağbet gören flash bellekler, harici sabit diskler ya da fotoğraf makineleri, video kameraları dijital verilerin, bulguların elde edilebildiği USB depolama birimleridir. USB depolama ünitelerinin incelenmesi 2 şekilde yapılmaktadır. Bu inceleme USB depolama biriminin önceden bilgisayara takılı olup olmaması yönüyle ya da depolama biriminin üzerindeki verilerin kurtarılması açısından birbirinden farklı şekilde gerçekleştirilmektedir. USB depolama üniteleri, bilgisayardaki işletim sistemiyle bağlantısı kurulduğu anda kayıt edilirler. Bu kayıtlar dışarıdan bir müdahale olmadığı takdirde, bu alanda kayıtlı kalırlar ve analiz için detaylı veriler sunabilirler. X-Ways Forensic, Encase ya da FTK gibi inceleme yazılımları aracılığı ile USB belleklerinden veri kurtarma işlemleri yapılabilmektedir.¹²³

122 Henkoğlu, s. 128.

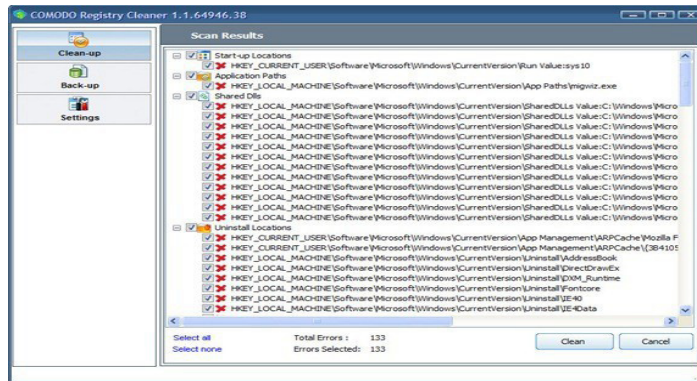
123 Henkoğlu, s. 129.



Şekil-19: X-Ways Forensics¹²⁴

“İşletim sistemi üzerinde yapılan tüm işlem kayıtları ve işletim sistemi konfigürasyonunu barındıran veri tabanı Windows kayıt defteri olarak adlandırılır. Windows işletim sisteminin çalışması bu veri tabanına bağlıdır.”¹²⁵

Bilgisayar analizi yapan adli bilişim uzmanı için Windows kayıt defteri faydalı birçok bulgu ve ipucu içeren, detaylı olarak incelenmesi gereken bir delil alanıdır. Adli bilişim uzmanının Windows kayıt defterinden inceleme sonucunda kazandığı veriler, işletim sistemi üzerindeki başka ek programlar yardımıyla elde edilen bulgularla örtüşüyor ise, bu ortaya çıkarılmış olan sonuçların doğrulandığı anlamına gelmektedir. ¹²⁶



Şekil-20: COMODO Registry Cleaner¹²⁷

124 <https://f-response.com/blog/f-response-live-physical-memory-x-ways-forensic-162-preview-4> (Son Er. T.: 30.05.2019).

125 Henkoğlu, s.133.

126 Henkoğlu, s.133.

127 <https://comodo-registry-cleaner.en.softonic.com/> (Son Er. T.: 30.05.2019).

3.2. CEZA MUHAKEMESİ KANUNU'NDA DİJİTAL DELİLLER

Ceza Muhakemesinde dijital deliller daha çok bilişim sistemlerinde bulunan veri arama, kopyalama ya da elkoyma tedbirleri sonucunda karşımıza çıkmaktadır. Öyle ki, soruşturma evresinin sonunda iddianamenin hazırlanabilmesi için yeterli bir şüphenin varlığı aranır. Kovuşturma aşamasında ise maddi gerçeği arayan hakim karar verebilmek için şüphesini yenebilecek kuvvetli delillere ihtiyaç duyar. Bu tarz deliller bilişim suçlarında bilişim sisteminde bulunan dijital deliller olarak ortaya çıkmaktadır.

Dijital delillere ilişkin arama ve elkoyma tedbirleri Ceza Muhakemesi Kanunu'nun 134. maddesinde yer almaktadır. Buna göre bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkanının bulunmaması halinde, hakim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin haline getirilmesine (...) karar verilir. Bir bilgisayara elkoyabilmek için

- Somut delillere dayanan kuvvetli bir suç şüphesinin varlığı
- İşlenmiş bir suç sebebiyle soruşturmanın başlamış olması
- Delillerin başka türlü elde edilme imkanının olmaması
- Hakim kararı
- Gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararı
- Elkoyulacak bilgisayarın şüpheli tarafından kullanılıyor olması şartları aranmaktadır.

Aynı maddenin 2. fıkrası gereğince bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun süreceği olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında CMK 134 III gereğince sistemdeki bütün verilerin yedeklemesi yapılır. Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

Kimi zaman ilgili maddenin 5. fıkrası uyarınca ‘bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır.

Bazen şüphelinin kullandığı bilgisayardan elde edilen veriler bir başka bilgisayarla bağlantı halinde olabilir. Bu tür durumlarda Ceza Muhakemesi Kanunu 135. maddesi gereği iki sistem arasındaki akış halinde olan veriler, iletişimin tespiti, dinlenmesi ve kayda alınması tedbiri ile toplanır.

“Düzenleme itibariyle bir elkoyma maddesi olarak görünen CMK 134, esasen Ceza Muhakemesi Hukukunda arama önleminin bilgisayar kütük ve programlarına ilişkin spesifik bir hükmü olmakla beraber, bir elkoyma düzenlemesi değil, arama düzenlemesidir. Öyle ki, söz konusu madde arama sonrası bir objeye elkoyma değil, yalnızca elde edilen bulguların çıktı ya da kopyalarının alınarak delil tespiti yapılmasını ihtiva etmektedir. Çok gerekli olduğu takdirde, örneğin bir bilgisayar programı şifrelenmiş ya da şifresi kırılmamış ise ve bundan dolayı istenen verileri elde etmek mümkün olmadıysa CMK 134 uygulanır. Ancak o zaman bile bilgisayara elkoyma amacıyla değil, bilgisayar ya da programlarında sınırlı ve geçici bir süre içinde veri elde etmeye yönelik inceleme yapmak için el konulabilir.”¹²⁸

Yukarıda zikredildiği gibi elkoyma işlemleri esnasında bilgisayar sistemindeki tüm veriler yedeklenir ve bu yedeklerin birer kopyası şüpheli ya da vekiline verilerek, taraflarca imzalanarak tutanak altına alınır. Yalnız adli bir soruşturmada örneğin bir hacker şüpheli konumunda ise, yedeklenen verilerin bir kopyasının şüpheliye teslim edilmesi suç tekrarı açısından sakıncalı hallerin doğmasına sebebiyet verebilir.

128 Ünver ve Hakeri, s. 431.

Bu tür ihtimaller hep var olsa da, düzenlemeyle amaçlanan, elkonulan bilgisayar program ya da kütüklerinin sonradan değiştirildiğine ilişkin ortaya atılabilecek iddiaların önüne geçmektir.

Kolluk kuvvetleri bilgisayar programlarında ya da kütüklerinde arama işlemi yaparken, suç teşkil eden içeriklerle karşılaşabilirler. Örnek olarak bulundurulması, çoğaltılması ya da paylaşılması ceza yasası uyarınca suç kabul edilen çocuk pornografisi verilebilir. Bu durumda Ceza Muhakemesi Kanunu 127. maddesi gereğince bilgisayar programının ya da kütüğünün söz konusu suçta kullanılmış olması sebebiyle ileride müsadere edilebilecek eşya sıfatıyla ilgili kayıtların bulunduğu veya suçun işlenmesinde araç olarak kullanılan cihaza kolluk kuvvetleri tarafından elkonulmalıdır.

Adli bilişimin teğet geçildiği bir suçun olay yeri incelemesi esnasında inceleme ekiplerinin en ihtimam gösterdiği ve en fazla zaman alan kısım, suça ilişkin delillerin sağlıklı, güvenli bir şekilde toplanması ve yine güvenli bir şekilde muhafaza edilmesidir.

Dijital deliller, bilgisayar veri depolama birimleri, GPS cihazları, telesekreter kayıtları, e-posta kayıtları, dijital fotoğraf ve videolar vs. gibi belli başlı alanlarda karşımıza çıkabilmektedir.

Soruşturma organı ilk olarak başkaca delillerin varlığını, başka delil elde etmenin mümkün olup olmadığını araştırmalıdır. Başka delil elde etme imkanı olmadığı anlaşıldığında, bu bildirilmelidir. Ancak bu süreçlerden sonra tedbire başvurulabilme imkanı doğar.

3.2.1 Türk Ceza Muhakemesi Kanunu'nda Bilgisayarlarda Arama ve Elkoyma

3.2.1.1. Genel

Klasik arama ve elkoyma işlemlerinde olduğu gibi bilgisayarlardaki elektronik veriler elde edilirken alınan koruma tedbirleri de şahısların özel hayatının kısıtlanma-

sını gerektirmektedir. Elektronik delillerin elde edilmesine ilişkin getirilen söz konusu koruma tedbirleri ve soruşturma organlarına verilen yetkiler Anayasa'nın 13. maddesi gereğince kanunla ve ayrıntılı bir şekilde düzenlenmiş olmalıdır.

Türk Ceza Muhakemesi Kanunu'nda genel arama ve koruma tedbirlerinin yanında bilgisayarlara dair arama, elkoyma ve kopyalama tedbirleri de ayrıca düzenlenmiş, Anayasa'nın temel hak ve özgürlüklere müdahale konusuna ilişkin 13. maddede belirttiği esasların muhafazası amaçlanmıştır.

Bu bağlamda öncelikle bilgisayarlara ilişkin arama, elkoyma ve kopyalama koruma tedbirlerinin yer aldığı CMK 134. madde, Adli Önleme Aramaları Yönetmeliği'nin 17. maddesi ve Suç Eşyası Yönetmeliği'nin 8. maddesi önem arz etmektedir. Bilişim teknolojisinin her geçen gün daha da gelişmesi kolluk kuvvetlerinin bu alanda işlenen suçlarda delil elde etmede bazı zorluklarla karşılaşmasına neden olmaktadır. Özel şifrelerle korunan, gözle görülmesi mümkün olmayan elektronik verilerin, yenilenen teknolojiyle elektronik medyanın farklı alanlarında çok farklı şekillerde muhafaza edilmesi söz konusu olabilmektedir. Elektronik verilerin ceza yargılamasındaki geçmişi çok eskiye dayanmasa da, artık günümüzde mahkemelerde sıklıkla delil olarak kullanılabilir.

Bilgisayarlardaki elektronik delillerin elde edilmesine ilişkin arama ve elkoyma koruma tedbirleri, elektronik delillerin sahip oldukları özellikler nedeniyle CMK'nın 116. vd. ile 127. maddelerindeki genel arama ve elkoyma tedbirlerinden farklı olarak CMK'nın 134. maddesinde düzenlenmiş, bu şekilde Anayasa ile güvence altına alınan temel hak ve özgürlüklerin korunması hedeflenmiştir.

CMK'nın 134. maddesinde yer alan arama, elkoyma ve kopyalama tedbirinde amaç, şüphelinin yakalanmasından çok, suçun ispatına yarayacak delillerin elde edilmesi ve zarar görmeksizin bir bütün olarak korunmasıdır. Polisin bilgisayarlarda gerçekleştirdiği arama sırasında öncelikli hedefi buradan elektronik bir veri elde etmektir, zira bu veri ya da veriler yargılama aşamasında suçun aydınlatılması bakımından delil olarak kullanılabilme özelliğine sahip oldukları gibi yargıcın davaya konu olayda maddi hakika- te ulaşmasını ve vicdani kanaatinin oluşmasını da sağlarlar.

Şüpheli şahsın kullandığı bilgisayar, bilgisayar programları ve kütükler Ceza Mu-

hakemesi Kanunu'nun 134. maddesinin 1. fıkrası uyarınca arama, elkoyma ve kopyalama koruma tedbiri kapsamındadır. Bilgisayar programları doğası gereği bilgisayarın içinde olabileceği gibi bilgisayar haricinde başkaca veri saklama ünitelerinde de bulunabilmektedir. Dolayısıyla bilgisayarda yapılan aramalar, bilgisayar programları ve veri saklama üniteleri için de geçerli olmaktadır.

Bilgisayar kütüğü, internet kullanıcılarına ait IP numaralarının ve diğer erişim verilerinin İnternet servis sağlayıcıları tarafından saklandığı veri tabanına (database) verilen addır. İngilizcede 'log' olarak adlandırılmaktadır.¹²⁹

CMK 134. maddesine dair dikkat çeken hususlardan biri de, içinde aynı bilişim teknolojisiyle donatılmış cep telefonu, faks makinesi, dijital fotoğraf makineleri, çağrı aygıtları, akıllı kart vb. gibi taşınabilir cihazlara ilişkin herhangi bir düzenleme bulunmamasıdır. Oysa ki, söz konusu cihazlar günlük hayatta oldukça yaygın bir şekilde kullanılmakta ve içlerinde adli bilişim uzmanları tarafından elde edilebilecek son derece önemli veriler barındırabilmektedir. Pratikte bu sorun CMK'nın 116. ve 123. maddelerinde yer alan arama ve elkoymaya dair genel hükümlerin söz konusu cihazlara uyarlanmasıyla çözülmektedir. Ancak ne var ki, CMK'nın 116 ve 123. maddeleri yerine daha spesifik bir düzenleme olan CMK'nın 134. maddesinin söz konusu cihazlara yönelik arama, kopyalama, elkoyma işlemlerinde baz alınması çok daha yerinde bir uygulama olacaktır, zira bu cihazlar esasen yapısal özellikleri itibarıyla bilgisayardan çok da farklı değildir.

Her ne kadar kanun maddesinde bilişim sistemlerine ilişkin tüm bu cihazların tek tek sıralanması yasal açıdan belirlilik ve açıklık prensibiyle bağdaşsa da, böyle bir düzenleme orta ve uzun vadede teknolojik gelişmeler karşısında hukuksal ihtiyaçlara cevap veremeyecektir. Bu nedenle CMK'nın 134. maddesi bilgisayarlar ve benzer donanımdaki tüm cihazları kapsayacak şekilde teknolojik ilerlemelerin hızı da göz önünde bulundurularak tekrar düzenlenmeli, bununla beraber bilişim hukukuna dair tüm konular gerekirse ek bir kanun maddesinde ayrıca yer almalıdır.

“Üzerinde durulması gereken konulardan biri de elektronik postalara ilişkin yapılan aramalarda elde edilmesi beklenen dijital delillerin CMK'nın 134. maddesinde zikredilen tedbire dahil olup olmadığıdır. Bu konuda türk hukuk sisteminde birçok görüş mev-

129 <https://berqnet.com/blog/loglama>. (Son Er. T.: 30.05.2019).

cuttur. Bunlardan birine göre elektronik haberleşme üzerinden dijital delil elde edildiği takdirde CMK m. 134'deki değil, CMK m. 135'te düzenlenen 'telekomünikasyon yoluyla iletişimin denetlenmesi' tedbirine müracaat edilmelidir.”¹³⁰

Bir diğer görüş ise şu şekildedir: *“Elektronik posta ekseriyetle web posta hizmeti altında gönderilmekte olup, bu hizmet türünde kişinin elektronik postalarının muhafaza edildiği bir alan mevcuttur. Elektronik posta, göndericinin sunucusundan alıcının sunucusuna vardığında, bu akış hali sona ermektedir. Bu durumda iletişimin içeriğinin incelenmesi amacıyla iletişimin dinlenmesi tedbiri söz konusu olduğundan CMK m.135'e göre işlem tesis edilebilecektir. Ancak eğer ki elektronik posta, bu hizmeti sunan kurumun bilişim sistemlerinde okunmadan duruyor vaziyette ise, o zaman CMK m. 134'ün uygulanması da mümkün görünmektedir.”¹³¹*

“Burada ortaya çıkan karmaşada kararsızlığa nokta koyacak hukuki bir orta yol mevcuttur. Elektronik posta kutusunda yahut servis sunucusunda saklanan elektronik postalara ilişkin delil elde etme prosedürü CMK m. 134 uyarınca gerçekleştirildiğinde, akışkan durumdaki elektronik postalara dair elde etme işlemi ise CMK m. 135'de yapılan ayrı bir ek düzenleme aracılığı ile yerine getirildiğinde çözüm sağlanabilir.”¹³²

3.2.1.2. Bilgisayarlarda Arama ve Elkoyma Tedbirlerinin Şartları

Bilgisayarlara ilişkin arama, kopyalama ve elkoyma tedbirlerinin hangi suç türleri için geçerli olduğu konusunda kanun koyucu tarafından yasal herhangi bir sınırlama getirilmemiştir.

Söz konusu tedbirler özellikleri itibarıyla sadece bilişim suçlarına uygulanabilir gibi gözükse de, farklı suç tiplerini de kapsamaları mümkündür. Ancak kabahat ya da disiplin eylemlerinden dolayı sürdürülen soruşturmalarda tedbir uygulamasının hiçbir karşılığı yoktur. Yukarıda adı geçen tedbir ancak suça ilişkin bir soruşturma başlatıldığı zaman uygulanabilmektedir. Ceza Muhakemesi Kanun'unun 134. maddesi 1. fıkrası gereğince tedbirin

130 Başlar, s.160.

131 Başlar, s.160.

132 Başlar, s.160.

uygulanabilirliđi somut delillere dayanan kuvvetli bir řüphenin varlıđına bađlıdır. Kuvvetli řüphe iki bakımdan incelenmektedir: Hem suçun řüpheli tarafından işlendiđine ilişkin hem de řüphelinin kendisine ait biliřim sisteminde işlediđi suçla alakalı bir delilin bulunabileceđine dair kuvvetli bir řüphenin bulunması gerekmektedir.¹³³

İlgili kanunda söz konusu tedbire başvurma nın řartlarından bir diğeri de başka türlü delil elde etme imkanının bulunamaması halidir. Kanun koyucu bu řekilde tedbirin uygulanma sahasını ciddi anlamda daraltma yoluna gitmiřtir. Ancak bu uygulama alanının başkaca ilave řartlar ile daha da sınırlandırılması soruşturma sürecini önemli ölçüde yavaşlatma riski taşımaktadır.

Birden fazla tedbirin uygulama alanı bulduđu hallerde oranlılık ilkesinin gözetilmesi temel hak ve hürriyetlerin korunması bakımından son derece önemlidir. Zira bu durumda temel hak ve özgürlüklere müdahalenin en az olduđu tedbire öncelik verilmeli, kısaca söz konusu tedbire en son çare olarak başvurulmalıdır.¹³⁴

Bilgisayarda bulunması muhtemel dijital delillere ulaşabilmek için tabii ki öncelikle bilgisayarın kendisinde arama tedbiri uygulanmalıdır. Bu nedenle bu tür suçlara ilişkin yürütölmekte olan soruşturmalarda ön řartın gerçekteřtiđinden bahisle başka türlü delil araştırmasına gitmeden söz konusu tedbir uygulanabilmeli, ön řart daha geniş yorumlanmalıdır.

Tedbir kararı, Cumhuriyet Savcısının talebi üzerine soruşturma nın yürütölmekte olduđu Sulh Ceza Hakimi tarafından verilir. Gecikmesinde sakınca bulunan durumlarda hem Cumhuriyet savcısının hem de kolluđun tedbiri doğrudan uygulama yetkisine sahip olmaması, söz konusu maddenin temel hak ve özgürlükler bakımından oldukça sıkı řartlarla korunduđunu ortaya koymaktadır.

Hız kesmeden ilerleyen, gelişen ve deđişen biliřim teknolojileri, suçla ilişkin delillerin ivedilikle elde edilmesini zorlařtırmaktadır. Dolayısıyla hızlı delil ele geçirmenin mümkün olmadıđı hallerde tedbirin, sonradan hakim onayına sunulması řartıyla, Cumhuriyet Savcısının vermiř olduđu karara istinaden uygulanabiliyor olması büyük önem arz

133 Başlar, S. 162.

134 Başlar, S. 164.

etmektedir. Bu hususta kanun koyucunun CMK'nın ilgili maddesinde deęişikliğe gitmiş olması yerinde bir adım olmuştur. Zira 25/7/2018 tarihli ve 7145 sayılı Kanunun 16. maddesiyle, bu maddenin birinci fıkrasında yer alan "Cumhuriyet savcısının istemi üzerine" ibaresi "hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından" şeklinde deęiştirilmiş, fıkra da yer alan "hâkim tarafından" ibaresi madde metninden çıkarılmış, ikinci fıkrasına "bilgilere ulaşılammaması" ibaresinden sonra gelmek üzere "ya da işlemin uzun sürecek olması" ibaresi eklenmiştir.

CMK'nın 134. maddesinde zikredilen tedbirin uygulanma şartlarından biri de yürütülen soruşturmada şüpheli sıfatıyla bir kişinin bulunmasıdır. Tedbirin uygulama alanı sadece şüphelinin kullandığı bilgisayarlardır, üçüncü kişiler ya da sanık durumundaki kişiler buna dahil değildir.¹³⁵

Dikkat çeken noktalardan bir diğeri de, söz konusu madde metninde kanun koyucunun bilinçli olarak 'şüpheliye ait' deęil, 'şüphelinin kullandığı' ibaresini tercih etmiş olmasıdır, zira akli başında hiçbir kişi kendi adına satın alma işleminin kolaylıkla tespit edilebileceğı bir bilgisayarda bilerek ve isteyerek suç işlemez. Kanun koyucu metinde tam tersine 'şüpheliye ait' seçeneğine yer vermiş olsaydı, uygulama alanı kısıtlanmış bir tedbirle karşı karşıya kalınılabildi.

Mağdur ya da şikayetçi kişinin kullandığı elektronik medyaya ilgili tedbirin uygulanıp uygulanamayacağı madde metninde yer almamaktadır. Ancak özellikle bilişim suçunun söz konusu olduğı durumlarda şüpheliye ulaşmak bazen mağdurun ya da şikayetçinin bilgisayarında bulunan dijital deliller yardımıyla mümkün olabilmektedir. Bu nedenle mağdur veya şikayetçiye ait bilgisayarda, kendi rızalarını açıkça beyan ettikleri takdirde, CMK m. 134 kapsamında arama, elkoyma ve kopyalama tedbirinin uygulanması yerinde ve akılcı bir yaklaşım olarak deęerlendirilebilir. Son olarak kanun metninde geçen 'şüpheli' sıfatı hem özel kişi hem de kamu tüzel kişisi olarak anlaşılmazdır.

Ceza Muhakemesi Kanunu'nun 134. maddenin 1. fıkrası gereğince bilgisayarlar üzerinde yapılan arama işlemleri, bu işlemler sonucu elde edilen dijital deliller zarar görmeden adli bilişim prensipleri çerçevesinde gerçekleştirilmelidir.

135 Başlar, S. 167.

Bilgisayar, bilgisayar programları ya da kütüklerinde suça ilişkin dijital kayıtlara ulaşıldığında, bunlar öncelikle birebir kopyalanmalı, içeriği çözümlenmeli ve metin haline getirilmelidir. Son olarak ise tüm sistemin hash değeri alınmalıdır.

Aynı maddenin 2. fıkrası uyarınca bilgisayarlar şifrelendiklerinden dolayı giriş yapılamıyor, içerisindeki saklı bilgilere ulaşılması mümkün değilse, şifrenin çözülmesi ve kopyaların alınabilmesi amacıyla bunlara elkonulabilir. Kopyalar alınır alınmaz, bilgisayarların iade edilmesi gerekmektedir. İlgili madde metninde süreye ilişkin herhangi bir sınırlama getirilmemişse de, işlemlerin makul bir süre içinde sonlandırılması beklenmektedir. Bilgisayarın şüpheliye iade edilmesi bazen sorun teşkil edebilmektedir, bunun çözümü hususunda öğretide farklı görüşler mevcuttur. Bunlardan birine göre bünyesinde suç unsuru barındıran bilgisayar şüpheliye tekrar verilmemeli, bunun yerine verilerin kopyası iade edilmelidir. Yalnız bu durumda da iade edilen kopyada suça ilişkin verilerin silinmesi gerekmektedir. Ne var ki bu görüşün çözüm noktasında çok da etkili olmadığı aşıkardır, zira güncel teknolojik gelişmeler göz önünde bulundurulduğunda silinen verilerin geri getirilmesi bugün pekala mümkün olabilmektedir.¹³⁶

Nasıl ki suça konu olayda kullanılan kesici aletin şüpheliye iade edilmesi kulağa mantık dışı geliyorsa, bünyesinde (fıkri mülkiyet haklarını ihlal eden kopya program, çocuk pornografisi vb.) suç öğeleri barındıran elektronik medyanın kendisinin ya da bir kopyasının şüpheliye iade edilmesi de o derece tartışmalıdır. Bu nedenle mevcut yasal düzenlemede değişime gidilmesi yerinde bir adım olacaktır.

CMK m. 134/3 uyarınca bilgisayar ya da bilgisayar kütüklerine elkoyma işlemi devam ederken bilgilerin kaybolmaması ve şüphelinin mağduriyetinin önüne geçilmesi amacıyla sistemde bulunan tüm verilerin yedeklenmesi gerekmektedir. Herhangi bir zarar ya da mağduriyet ihtimali olmasa dahi, yedekleme mutlaka yapılmalıdır. Böylelikle elektronik medyaya karşı yönelebilecek olası bir dış müdahale baştan önlenabilmektedir. Elektronik veriler yapıları itibariyle teknik inceleme sırasında zarara ya da değişime uğrayabilirler, hatta silinme riski taşırlar. Bu nedenle her ne kadar madde metninde ‘elkoyma işlemi sırasında’ ibaresi yer alıyorsa da, yedekleme, elkoyma işleminden önce yapılmalıdır.¹³⁷

136 Başlar, S. 172.

137 Başlar, S. 174.

Yedekleme işlemi tamamlandıktan sonra CMK m. 134/4 e göre bir kopyanın şüpheliye ya da vekiline verilmesi gerekmektedir. Bununla beraber durum tutanağa geçirilmeli ve imza altına alınmalıdır. Nitekim bu düzenlemeyle kanun koyucu olası hukuka aykırılık iddialarının önüne geçmeyi hedeflemiştir.

Söz konusu maddenin 4. fıkrasına ilişkin altı çizilmesi gereken konulardan biri de madde metninde zikredilen ‘vekil’ ibaresidir. Bilişim suçlarının günümüz dünyasında hiç azımsanmayacak bir oranda ‘küçükler’ tarafından da işlenebildiği dikkate alındığında, ‘vekil’ ifadesi, ‘şüpheliyi temsil eden kişi’ biçiminde daha geniş bir yorumlama ile ele alınmalı, bu kavram ‘anne-baba’ ya da müşterek konutta yaşayan yasal temsilciler bakımından da uygulanabilir olmalıdır.¹³⁸

CMK m. 134/5 ile bilgisayarlarda bulunan verilerin tümünün ya da bir kısmının kopyasının alınabilmesi mümkün kılınmıştır. Madde metninde zikredilen kopyalama işlemine boş alanların ve silinmiş verilerin kopyalanması da dahil olduğundan, aslında söz konusu olan birebir bir kopyalama işlemidir.

İşlem tamamlandıktan sonra kopyası alınan veriler kağıda yazdırılır, bu husus bir tutanağa bağlanır ve en son ilgililer tarafından imza altına alınır.

CMK’nın 134. maddesinin 5. fıkrası şüphelilere bilgisayarlarını, program ve data-larını kullanmaya devam etme imkanı tanımaktadır, zira yedeklenen ve de tutanak altına alınan dataların gerçekleştirilen bu işlemlerden sonra değiştirilmesi soruşturmanın seyri açısından pek de bir mana ifade etmeyecektir. Uygulamaya bakıldığında, polisin sonradan çıkabilecek her türlü uyuşmazlığa karşı verilerin üç adet kopyasını çıkartarak önlem aldığı görülmektedir. Nitekim bu kopyalardan biri öncelikle inceleme için adli bilişim uzmanlarına, bir diğeri ise şüpheliye verilmekte, sonuncusu ise ayrı bir birimde muhafaza altına alınmaktadır.

Hash değerinin tutanağa kaydedilmesi gerektiği yönünde madde metninde herhangi bir düzenleme bulunmamasına rağmen delil bütünlüğünün korunması, delil eklenme iddialarının önüne geçmek amacıyla hash değerinin de aynı tutanağa kaydedilmesi büyük önem arz etmektedir. Bu nedenle kanun koyucu mevcut maddede biran önce deği-

138 Başlar, S. 175.

şiklik yaparak hash değerinin alınmasını teknik bakımdan bir zorunluluk olarak düzenleme yoluna gitmelidir. Her ne kadar CMK 134’de zikredilen arama, elkoyma ve kopyalama tedbirleri özel hüküm niteliği taşısa da, madde metnine aykırı düşmediği sürece bazı hususlarda CMK’nın arama ve elkoymaya ilişkin genel hükümleri de uygulama alanı bulabilmektedir.

Arama kararında nelerin yazması gerektiği, arama işlemini gerçekleştiren polis memurlarının kimlik bilgilerinin tutanakta belirtilmesi, arama işleminde hazır bulunması gerekli kişiler ve arama işlemi sonucunda verilmesi gereken dokümanlar vs. gibi hususlar genel hükümlerin geçerli olacağı konulara örnek olarak gösterilebilir.¹³⁹

CMK m.134’de açıkça düzenlenmeyen bir mühim konu da, kişinin bilgisayarlar da, bilgisayar programlarında ve kütüklerinde yapılan arama, kopyalama ve elkoyma tedbirine karşı kullanabileceği yasal itiraz haklarıdır. Burada da genel hükümler geçerliliğini korumakta, CMK m. 267 hükmü gereğince şüpheli ya da müdafii hakim vermiş olduğu tedbir kararına karşı itiraz edebilmektedir.¹⁴⁰

CMK m.122/1 de açıkça belirtilmiştir ki, hakkında arama işlemi gerçekleştirilen kişinin belge ya da kağıtları üzerinde sadece ve sadece Cumhuriyet savcısı ve hakim inceleme yapabilir. Dolayısıyla CMK m. 134’e göre arama yapan polisler bilişim sistemlerinde buldukları ve sonrasında kağıda aktardıkları verileri hiçbir surette inceleme yetkisine sahip değildirler.

Bu bağlamda özellikle kamu tüzel kişiliklerinin bilişim sistemlerinde yapılan ara malar dikkat çekmektedir. Kolluk kuvvetlerinin arama işlemi sırasında ele geçirdiği devlet sırrı niteliğindeki dokümanlar üzerinde incelemeyi CMK m. 125/2 gereğince yalnızca hakim ya da mahkeme başkanı yapabilmektedir. Bu nitelikteki belgelerin kopyası alınmadığı gibi, fotokopisi de çekilemez, sadece suçun aydınlatılmasına yarayacak bilgiler hakim ya da mahkeme başkanı tarafından tutanağa geçirilir.

Elektronik medyada ölçsüz bir şekilde gerçekleştirilen arama işlemlerinde şüpheli bakımından tazminat hakkı CMK’nın genel hükümlerine göre belirlenmekte, şüpheli

139 Başlar, S. 178.

140 Başlar, S. 178.

ya da müdafii CMK m. 141/1-i gereğince tazminat talep edebilmektedir.

Kolluk kuvvetleri bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama yaparken bazen tesadüfen soruşturma ve kovuşturmayla ilgisi olmayan, ancak başka bir suçun işlendiğine işaret eden bir delille karşılaşabilirler. Tesadüfen elde edilen bu deliller kolluk tarafından CMK m. 138/1 uyarınca muhafaza altına alınmalı ve durum biran önce Cumhuriyet savcısına bildirilmelidir. Tesadüfi delil bulunduğu arama işleminin genişletilmesi özellikle sakınılması gereken bir husustur. Nitekim bu tür bir keyfi uygulama tedbirde oranlılık ilkesini zedeleyerek hukuka aykırılıklara neden olabileceği gibi, mevcut soruşturmanın hızını da kesebilir.¹⁴¹

CMK m. 134/'de yer alan tedbir Avrupa Konseyi Siber Suç Sözleşmesi bakımından değerlendirildiğinde, iç hukuktaki bu düzenlemenin sözleşmeyle önemli ölçüde uyumlu olduğu gözlemlenmektedir.

Bununla beraber CMK'nın 134. maddesinin 3. fıkrasında elkoyma nedenlerinin detaylı bir şekilde zikredilmemiş olması önemli bir eksiklik olarak karşımıza çıkmaktadır. Aynı şekilde arama işlemi sırasında kolluk tarafından elkonulan verilerde suç unsuru sayılan içeriğin (örn. Çocuk pornografisi, virüs programları vs.) kopyaları alındıktan sonra silinmemesi, erişilebilir ve kullanılır halde kalması maalesef sözleşmeyle uyumlu bir uygulama değildir. Söz konusu sözleşmede bunun düzenlenmiş olması, ancak CMK m. 134 de hala böyle bir hükmün yer almıyor olması bir diğer eksiklik olarak göze çarpmaktadır.

3.3. CEZA MUHAKEMESİ KANUNU'NDA DÜZENLENMEYEN ARAMA TÜRLERİ

3.3.1. Uzaktan Erişimle Arama

Uzaktan erişimle arama Türk hukukunda düzenlenmeyen hususlardan biridir. Günümüzde internetle iletişim yaygın olmanın ötesinde öyle bir seviyeye ulaşmıştır ki,

141 Başlar, S. 181.

internet bağlantısı bulunan bir bilişim sistemine kullanıcının bilgisi olmadan erişmek, buradaki saklanan verilere ulaşmak son derece kolay bir hale gelmiştir.

“Uzaktan arama yöntemleri aracılığı ile kolluk kuvvetleri internete bağlı bir bilgisayarın sabit diski üzerinde ya da aktif olan diğer hafıza alanlarında arama imkanına sahip olduğu gibi, elektronik haberleşme trafiğinin kontrolü ve ağ tarayıcısının hangi faaliyetlerde bulunduğu da mümkün olabilmektedir.”¹⁴²

Ancak bu yöntem kullanıldığında şüpheli, kendine ait bilişim cihazında uzaktan arama yöntemi kullanılmak suretiyle arama yapıldığından ve bu şekilde delil elde edilmek istendiğinden haberdar değildir. *“Dolayısıyla bahsi geçen delillere ilişkin kişinin gözetleme ve haklarının muhafazasını isteme hakkı bertaraf edilmekte, deliller üzerinde kolluk ya da üçüncü kişilerce gerçekleştirilen hukuka aykırı uygulamalar da söz konusu olabilmektedir.”¹⁴³*

Aksi görüşü savunan Değirmenci’ye göre CMK m. 134’deki hüküm, bir yazılım üzerinden bilişim sisteminde arama yapılmasını, sistemde bulunan tüm verilerin başka bir yere aktarılmasını ve sistemdeki hareketlerin takip edilmesini mümkün olmadığını ortaya koymaktadır. Söz konusu madde Değirmenci’ye göre aynı zamanda sabit verilere ilişkin aramayı hüküm altına alan, arama sırasında ilgili kişinin haberdar olmasını şart kılan, aramanın yasal usul ve esaslarını belirten bir tedbirdir. Dolayısıyla kişinin haberi olmadan, kullandığı bilişim sistemlerinde yazılım üzerinden uzaktan erişimle arama yapmak mevcut yasal düzenleme uyarınca mümkün olmadığı gibi, yazılım yardımıyla veri elde etme de arama olarak görülemez. Zira arama yasal bakımdan zaman sınırı olan bir eylemdir, süreklilik arz etmez. Oysa yazılım yardımıyla bilişim sisteminden veri elde etmek anlık bir eylem olmanın çok ötesinde süreklilik arz eden bir faaliyettir.¹⁴⁴

Değirmenci gibi Ünal da uzaktan erişimle bilişim sisteminde arama yapmanın CMK m. 134’e göre mümkün olmadığı görüşünü benimsemekte, bu tür aramanın temel hak ve özgürlüklere ağır bir müdahale anlamına geldiğini, bu nedenle yeni bir yasal düzenlemeye ihtiyaç olduğunu savunmaktadır.¹⁴⁵

142 Özen ve Özocak, s. 50.

143 Özen ve Özocak, s. 50.

144 Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 364 -365.

145 Başlar Yusuf, Ceza Yargılamasında Elektronik Delil, Ankara, Yetkin Yayınları, 2016.

Mali bakımdan ele alındığında delil elde etmeye yönelik uzaktan arama tedbirleri bilhassa ağır ceza gerektiren suçlar bakımından yerinde bir düzenleme olarak nitelendirilebilir. Elbette bu durumda da özel hayatın gizliliği ilkesine azami ölçüde dikkat edilmeli, temel hak ve özgürlüklere müdahale en asgari seviyede tutulmalıdır.

3.3.2. Bulut Bilişimde Arama

Teknoloji dünyasında geçmişi çok da eski olmayan bulut bilişim ile bilişim sisteminde bulunan kişisel dosya, program ve arşiv vb. gibi veriler internetteki sunucular üzerinde depolanabilme ve tekrar erişilebilir olma özelliği kazanmaktadırlar.¹⁴⁶ Kullanıcılar internete bağlı oldukları her yerden ve her türlü bilgi iletişim cihazıyla (Mac, PC, iPhone, BlackBerry, Android) bu sunuculara ulaşabilmektedirler. Sabit disk ve harici taşıyıcılara gerek kalmadan kişisel veri ve belgelere heryerden ulaşabiliyor olmak bulut bilişim hizmetini giderek daha çok tercih edilen ve avantajlı bir bilgi iletişim teknolojisi haline getirmiştir. Olası dosya ve veri kayıplarının önüne geçmeyi sağlayan bulut bilişim, bu verilere herhangi bir cihaza bağımlı kalmadan ve çok daha ucuza 7/24 ulaşılabilmesini mümkün kılmaktadır.



Şekil- 21: Bulut Bilişim¹⁴⁷

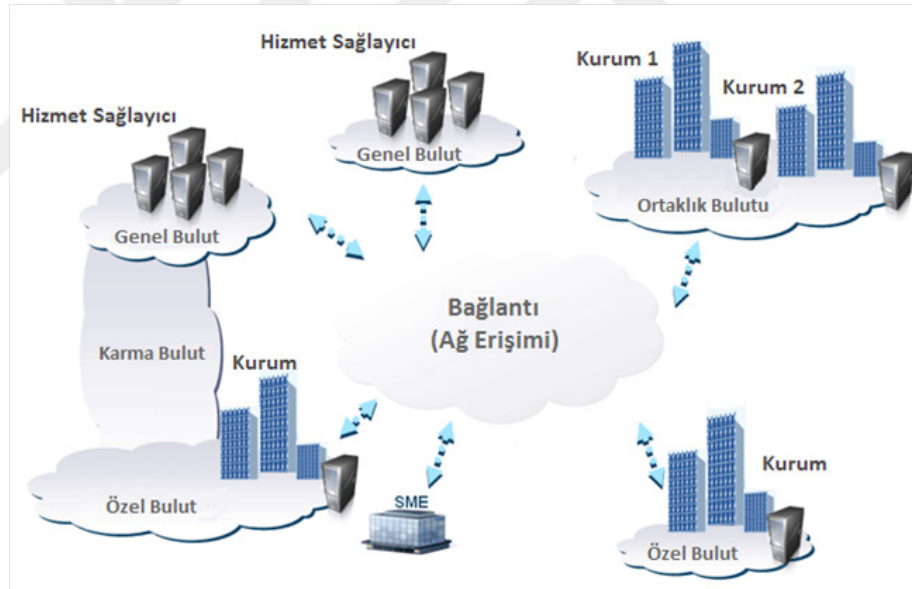
Daha fazla depolama alanı, daha süratli veri transferi, maliyete ilişkin tasarruf im-

¹⁴⁶ <https://www.endustri40.com/bulut-bilisim-cloud-computing-nedir/> (Son Er. T.: 30.05.2019).

¹⁴⁷ <https://bilgisayarbaligi.wordpress.com/2015/10/17/cloud-computing-bulut-bilisim/> (Son Er. T.: 30.05.2019).

kanı bulut bilişim hizmetini şirketler açısından da oldukça cazip hale getirmektedir. Hatta büyük ölçekteki şirketler için iş gücü tasarrufu da bu avantajlar arasına eklenebilmektedir. Bulut bilişim hizmeti veren platformlara Dropbox, Google Drive, SkyDrive, iCloud, Yandex.Disk, Turkcell Akıllı Bulut, TTNET Bulut örnek olarak gösterilebilir.¹⁴⁸

Günümüz dünyasında sıkça gündeme gelen sosyal ağlara bakıldığında, burada kullanılan müzik, fotoğraf, yüklenen videolar gibi birçok verinin de bu internet sitelerinin kendi bulut sistemlerinde depolandığı görülmektedir. Kullanım şekline göre bulut bilişim 4 ayrı çeşidiyle hizmet sağlamaktadır: Public Cloud (Genel Bulut)'ta kullanıcı kendi sistemini, bulut hizmetinden faydalananarak, yani üçüncü şirket üzerinde kiralan kaynaklar üzerinde kurmaktadır. Sıklıkla kullanılan e-mail hizmetleri genel bulut kategorisine girmekte, kullanıcılar elektronik postalara hiçbir ücret ödemeksizin bunların çeşitli özelliklerinden istifade etmektedirler. Küçük ve orta ölçekli şirketlerde kullanılabilen, kullanıldığı kadar ödeme yapılan bir model niteliğindedir.



Şekil- 22: Bulut Bilişim¹⁴⁹

Private Cloud (Özel Bulut) ise belirli kurum veya kuruluşlara sunulan, büyük şirketlerin tercih ettiği, erişim güvenliğinin ve gizliliğin yüksek olduğu bir bulut teknolojisidir. Bulut hizmetini sağlayan üçüncü bir bulut hizmet sağlayıcı olabileceği gibi, kurumun

148 <https://www.endustri40.com/bulut-bilisim-cloud-computing-nedir/> (Son Er. T.: 30.05.2019).

149 <http://yunus.hacettepe.edu.tr/~ceren.bayindir11/webfinal/modelleri.html> (Son Er. T.: 30.05.2019).

ya da kuruluşun kendisi de olabilmektedir. Özel bulut teknolojisinde, kuruma dışarıdan bütün erişim yolları kapatılarak, yalnızca kurum içi hizmet sağlanır.¹⁵⁰

Henüz çok yaygın olmayan bir kullanım biçimi de Melez Bulut (Hybrid Cloud)'tur. Public ve Private Cloud'un birleşmesiyle ortaya çıkmış bir bulut teknolojisidir. Zira bazen güvenlik ve gizliliğin daha fazla önem taşıdığı ve yüksek güvenlik tedbirlerinin gerekli olduğu alanlarda Private Cloud'un, güvenlik tedbirlerinin daha düşük seviyede tutulabileceği yerlerde ise Public Cloud'un tercih edilmesi daha mantıksal bir yaklaşım olabilmektedir. Bununla birlikte söz konusu bulut teknolojilerinin hangi oranda birleşeceği kurum ya da kuruluşun hacmine göre değişim göstermektedir.¹⁵¹

Çok fazla kullanılmayan (Community Bulut) Topluluk Bulutu'nda ise belirli bir grup ya da topluluğa bulut hizmeti sunulmaktadır. Uygulama ve verilere ancak topluluk üyeleri erişebilmektedir.¹⁵²

Günlük hayatta kullanıcılara birçok avantaj sağlayan bulut bilişimin elbette dezavantajları da bulunmaktadır. Bunlardan en göze çarpanı ise sanal alanda depolanan verilere ulaşabilmek için bir internet bağlantısının olması gerektiğidir. Öyle ki internet bağlantısının sağlamadığı durumlarda, durum ne kadar acil olursa olsun, bulut sisteminde depolanmış bilgilere erişmek kesinlikle mümkün olamamaktadır. Bununla beraber düşük bir internet hızı, veri trafiğindeki hızı yavaşlatmakta, kurum ya da kuruluşlarda hizmet bağlamında bir takım aksaklıklara sebebiyet verebilmektedir. Son zamanlarda en dikkat çeken dezavantajlardan biri de güvenlik açıklığı hususudur. Bulut hizmet sözleşmelerinde kullanıcıya ait bilgilere yalnızca kendisinin ulaşabileceğine ilişkin açık ifadeler bulunmamaktadır. Bu tür sözleşmeler sadece hizmet sunucunun lehine olacak biçimde hazırlandığı gibi, sistem çöktüğünde, kendisinin tekrar ne zaman aktif hale geleceği ve hizmet verebileceği hususunda da herhangi açık bir düzenleme yer almamaktadır.¹⁵³

Ayrıca bulut sisteminde depolanan verilerin kime ait olduğu konusu da net değildir. Örneğin kimi hizmet sözleşmelerinde yüklenen verilerin sahibinin kullanıcı olduğu ve bunlardan kullanıcının sorumlu olduğu ifade edilmektedir. Ancak aynı sözleşmenin bir

150 <https://azure.microsoft.com/tr-tr/overview/what-is-a-private-cloud/> (Son Er. T.: 30.05.2019).

151 <http://yunus.hacettepe.edu.tr/~hgamze11/web06/> (Son Er. T.: 30.05.2019).

152 <http://yunus.hacettepe.edu.tr/~ceren.bayindir11/webfinal/modelleri.html> (Son Er. T.: 30.05.2019).

153 Henkoğlu, s. 220

başka maddesinde, hizmeti sağlayanın hizmet kalitesini artırmak için, içeriğin ‘kullanılabileceği, değiştirilebileceği, uyarlanabileceği, kaydedilebileceği, yeniden üretilebileceği, dağıtılabilmesi ve görüntülenebileceği’ belirtilmektedir. Bu geniş çaptaki izin ve yetki sözleşme ile hizmet sağlayıcıya tahsis edildiğinde, malesef içeriğin, kullanıcıyı koruma adına alınacak önlemlerin (kötü amaçlı yazılım tespiti vb.) haricinde kullanımına da imkan sağlanmaktadır.¹⁵⁴

Sanal sunucularda depolanan bilgilerin, kişisel ya da kurumsal, her zaman kötü niyetli kişilerin eline geçerek kötü amaçlar için kullanılma ihtimali bulunmaktadır. Dolayısıyla bu tür suç soruşturmalarında bulut bilişim kullanılarak da elektronik delil elde edilmesi mümkün olabilmektedir. Ancak verilerin üçüncü kişilerin kontrol alanında olması hukuksal açıdan tartışmalara konu olmaktadır.

CMK m. 134’de zikredilen ‘şüphelinin kullandığı’ ibaresi hem fiziki hem de sanal açıdan kullanma olarak nitelendirilmektedir. Bulut bilişime bakıldığında, bu hizmeti sağlayan sunucular, kullanıcılarına veri depolama için belli bir sanal alan alan sağlamaktadır. Bu kişi bu sisteme kullanıcı adını ve şifresini kullanarak erişim sağlar ve verilerini burada depolar. Dolayısıyla kişinin kullanmış olduğu bu sanal alan için CMK m. 134 uyarınca arama kararı verilebilmekte ve bu karara istinaden arama işlemi gerçekleştirilebilmektedir. Yalnız üçüncü kişiye ait olan veya şüphelinin kullanmadığı alanlar için arama işlemi yapılamaz. Hizmet sağlayıcı şüphelinin kullandığı sanal alandaki tüm verilerin mantıksal kopyasını teslim etmelidir. Ancak bu işlemden önce söz konusu verilerin hash değerinin alınması delilin güvenilirliği açısından önemlidir.

Dikkat edilmesi gereken hususlardan biri de, sadece kullanıcının hesabına ilişkin veriler üzerinde arama yapılabilmesidir. Aksi halde bu hizmeti veren sunucuya tahsis edilmiş tüm sanal alanda arama yapılabilmesi söz konusu olur ki, bu da üçüncü kişilerin mahremiyet haklarının zarar görmesi ve CMK m. 134’deki hükmün dışına çıkılması anlamına gelir.

Ne var ki bulut bilişim hizmetini veren hizmet sağlayıcı çok daha geniş bir alanda, yurtdışında hizmet veriyor olabilir, bu durumda bulut bilişimde arama, verilere elkoyma ve söz konusu verilerin mantıksal kopyasının alınması işlemleri adli yardımlaşmaya iliş-

154 Henkoğlu Türkay, s.223.

kin düzenlemeler kapsamında yapılacaktır.

Avrupa Konseyi Siber Suç Sözleşmesi'nin 29. maddesi gereğince hizmet veren sunucu taraf devletlerden birinde bulunuyorsa, diğer taraf devlet verilerin muhafazasını acilen talep edebilir.

Bulut bilişimde muhafaza edilen dosyalar ve veriler açısından Avrupa Konseyi Siber Suç Sözleşmesi'nin 32. maddesinin hükmü önem taşımaktadır. Buna göre taraf devletlerden biri kendi sınırları içindeki bir bilişim sistemi yardımıyla başka bir taraf devlette saklı tutulan bilgisayar verilerine bulut bilişim kullanıcısının onayı da alınarak erişebilir veya alabilir.

“Türkiye’de ikamet eden bir bulut kullanıcısı verilerini/dosyalarını Almanya’daki bir bulut sunucusunda muhafaza ediyorsa, bu durumda türk kolluk kuvvetleri şüpheliye ait kullanıcı adına ve şifreye vakıf olmaları kaydıyla CMK m. 134’e göre Almanya’daki sunucudan söz konusu verileri/dosyaları alabilirler. Ancak şifre bilinmiyor ve çözümü için şifre kırıcı programa ihtiyaç varsa, bu durumda kolluğun kullanıcının bulut hesabına erişim hakkı bulunmamaktadır.”¹⁵⁵

3.4. BİLGİSAYARLARA İLİŞKİN DİĞER YASAL DÜZENLEMELER

Kanun koyucu Ceza Muhakemesi Kanunu’nda yer almayan bazı konuları Adli ve Önleme Arama Yönetmeliği ve Suç Eşyası Yönetmeliği ile düzenleme yoluna gitmiştir.

3.4.1. Adli ve Önleme Aramaları Yönetmeliği

CMK m. 134/3’de yer alan hüküm gereğince bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Adli ve Önleme Aramaları Yönetmeliği’nin 17/3. maddesi CMK m. 134/3’deki bu düzenlemeye ek olarak ‘bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir

155 <https://jurix.com.tr/article/10935>) (Son Er. T.: 30.05.2019).

donanımları hakkında da uygulanır' hükmünü getirmiştir. Böylelikle sadece olay yerinde bulunan bilgisayarlar değil, aynı zamanda CD, disket, çıkarılabilir özellikteki usb memory gibi veri saklama birimleri de yedeklenebilmektedir. Bu ek düzenlemeyle birbirine LAN ya da WAN sistemi üzerinde bağlı olan bilgisayarlardan uzaktan yedekleme yapılabilmesi de mümkün kılınmıştır.

Söz konusu madde yakından incelendiğinde yalnızca 'yedeklemeden' bahsedildiği göze çarpmaktadır. Oysa delil olabilecek dijital verileri elde etmek için öncelikle arama yapılması gerekmektedir ve yedekleme de ancak arama işlemi sonrasında gerçekleştirilebilecek bir eylemdir. Dolayısıyla Adli ve Önleme Aramaları Yönetmeliği'nin 17/3. maddesi bilgisayar ağları, uzak bilgisayar kütükleri ve çıkarılabilir donanımlar üzerinde de arama, kopyalama ve elkoyma işlemi yapılabileceği şeklinde yorumlanmaktadır.

CMK m. 134/5 uyarınca bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kağıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır. Yönetmeliğin 17/5. maddesinde kanun koyucu CMK m.134/5'den farklı olarak 2. cümlede değişikliğe gitmiş, bu kısmı 'kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir.' şeklinde düzenlemiştir. Bu hükümle birlikte CMK m. 134/5 de yer alan sayfalarca belge çıktısı alma işlemi son bulmaktadır.

Ne var ki CMK 134'de yer alan bu koruma tedbirlerinin sınırlarının uygulama bakımından bir yönetmelik maddesiyle genişletilmesi temel hak ve özgürlükler açısından oldukça hassas ve bir o kadar da tartışmalı bir konudur, zira temel hak ve özgürlükler Anayasa'nın 13. maddesine göre ancak yasa ile sınırlandırılabilir. Dolayısıyla bilgisayar ağları, uzak bilgisayar kütükleri ve çıkarılabilir donanımlar bakımından yapılacak işlemlerin yeni bir yasal düzenlemeyle hüküm altına alınması yerinde bir adım olacaktır.

3.4.2. Suç Eşyası Yönetmeliği

Elektronik deliller dijital bir yapıya sahip olmaları sebebiyle, bozulmaları, tahrif edilmeleri ya da kaybolmaları çok kolaydır. Bu tür risklerin önüne geçmek için yapısal

olarak son derece hassas olan bu delillerin muhafazası özen gerektirmektedir. Zira kullanılamaz durumda olan ya da yok olmuş bir elektronik delil soruşturma ve kovuşturmanın seyrini pekala değiştirebilmektedir.

Bu bağlamda Suç Eşyası Yönetmeliği'nin 8. maddesi öne çıkmaktadır. Nitekim Suç Eşyası Yönetmeliği'nin m.8/2 uyarınca bilgisayar, bilgisayar kütükleri ve bu sisteme ilişkin verilerin asıl ya da kopyaları, ses ve görüntü kayıtlarının bulunduğu depolama aygıtları gibi eşya, bozulmalarını engelleyecek, nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak uygun ortamda muhafaza edilir.

Öyle ki Avrupa Konseyi Siber Suç Sözleşmesi m. 16 da, 'saklanan bilgisayar verilerinin hızlı bir biçimde korunması başlığı altında elde edilen bilgisayar verilerinin silinmeden, değiştirilmeden, bozulmadan özgün niteliğinin korunmasını ortaya koymuş, böylelikle taraf ülkelere de bu maddeyle uyumlu yasama işlemlerini gerçekleştirme yükümlülüğü getirmiştir.

Ne var ki, CMK'nın 134. maddesinde bu yönde herhangi bir düzenlemeye yer verilmemiştir. Kanun koyucu CMK m. 134 de bu eksikliği Suç Eşyası Yönetmeliğindeki hükümle gidermeyi hedeflemiştir.

Dijital cihazlar yapıları gereği bir güç kaynağıyla beslenmek zorundadırlar, aksi takdirde sistemde bulunan veriler kaybolma ya da silinme tehlikesiyle karşı karşıya kalırlar. Cihazdaki verilerin en iyi şekilde korunması, delil değeri bakımından herhangi bir zarar görmemesi belli aralıklarla düzenli bir şekilde kontrol edilmesine bağlıdır. Bu nedenle söz konusu Yönetmeliğe bu hassasiyetler de dikkate alınarak kontrol tedbirlerine ilişkin ek hükümler getirilmesi isabetli bir yaklaşım olacaktır.

3.5. DİJİTAL DELİLLERE DAİR YARGITAY UYGULAMALARI

Dijital delillere ilişkin uygulamada karşılaşılan en yaygın sorunlardan biri güvenirlilikleridir. Zira bu tür deliller kolaylıkla değiştirilebilir olmakla beraber, delil değerleri orijinal olup olmadığına göre değişmektedir.

Bu konuda hassas bir yaklaşım sergileyen Yargıtay 2010 tarihli bir kararında “*sa-nığın işyerinde bulunan güvenlik kamerası görüntülerinin orijinalliğinin ve söz konusu kayıtlara sonradan ekleme yapıp yapılmadığının tespiti için bilirkişi raporunun gerekli olduğunu belirtmiş, buna aykırı uygulamaların kabul edilemez olduğundan bahisle yerel mahkemenin kararını bozmuştur.*”¹⁵⁶

Soruşturma evresinde birden fazla dijital delilin bulunduğu bir davada, bu delille-rin tamamının toplanması ve mahkemeye sunulması davanın seyri açısından son derece büyük bir önem taşımaktadır. Bu hususa ilişkin bir kararında Yargıtay, “*uyuşturucu tica-retinin söz konusu olduğu bir davada yerel mahkemenin kararını eksik inceleme sebebiyle bozma yoluna gitmiştir. Zira hem iletişimin tespitine ilişkin verilerin hem de havaalanı güvenlik kamerası ve MOBESE kamerası kayıtlarının dijital delil olarak kullanılması gerekirken yerel mahkeme kararını bunlardan sadece birine dayanarak vermiştir.*”¹⁵⁷

Elektronik delillerin mahkemede delil olarak kullanılabilmesi için öncelikle adli bilişim uzmanları tarafından incelemeye ve değerlendirmeye elverişli hale getirilmesi ge-rekmektedir. İnsan öldürme suçuna ilişkin bir davada Yargıtay, *soruşturma evresinde olay anı ve öncesine ilişkin elde edilen güvenlik kamera kayıtlarının bilirkişi tarafından analiz edilmesinin, çıkan sonuçların duruşma esnasında taraflara bildirilmesin ve tarafların da buna karşı bir beyanı olup olmadığının sorulmasının gerekli olduğu kanaatine varmış, güvenlik kamerası görüntülerinin hangi tarihte ve nerede incelendiğinin mahkeme tara-findan net olarak anlaşılamadığı hallerde mahkumiyet kararı verilemeyeceği sonucuna ulaşmıştır.*¹⁵⁸

“*Bilgisayar hard diski veya cep telefonun belleğinden elde edilen veriler*”¹⁵⁹, *çocuk pornografisi suçunun söz konusu olduğu bir olayda sanığa ait elektronik posta adresinde ele geçirilen kayıtlar*¹⁶⁰; *dava konusunun kasten insan öldürme ve yaralama suçu oldu-ğu olayda MOBESE kamera görüntülerinin çözümleri*”¹⁶¹ Yargıtay tarafından delil olarak kabul görmüş, elde edilen bu elektronik verilerin araştırılmamış olması yerel mahkeme kararlarının bozulmasına neden olmuştur.

156 10. CD, 22.01.2013, 2012/20151, 2013/680.

157 10. CD, 22.01.2013, 2012/20151, 2013/680.

158 1. CD, 16.01.2012, 2008/10249, 2012/48.

159 9. CD, 2010/12773-10407.

160 5. CD, 01.10.2007, 2007/ 9856- 6957.

161 1. CD, 14.05.2008, 2007/9024, 2008/4006.

3.6. DÜNYADAKİ HUKUK SİSTEMLERİNDE DİJİTAL DELİLLERİN ELDE EDİLMESİNE İLİŞKİN DÜZENLEMELER

Bu bölümde dijital delillerin elde edilmesine ilişkin düzenlemeler ABD, İngiltere ve Almanya'daki uygulamaları kapsamaktadır.

3.6.1. Amerika Birleşik Devletleri

Ülkemizde olduğu gibi ABD ceza yargılama sisteminde de dijital delillerin aranması ve elkonulmasına ilişkin mahkeme kararı kolluk güçlerince icra edilmektedir.

23.11.2001 yılında Avrupa Konseyi Siber Suç Sözleşmesini imza altına almıştır. Sözleşme 29.09.2006 tarihinde onaylanmak suretiyle 01.01.2007 yılında yürürlüğe girmiştir. Ancak saklanan dijital verilerin aranması ve elkonulmasına dair imzalanmış olan Siber Suç Sözleşmesi'nin 19. maddesine ilişkin bir iç düzenleme yapılmamıştır. Dolayısıyla bilişim sistemlerinde yapılacak olan arama ve elkoyma işlemlerine ilişkin spesifik bir düzenleme bulunmamakta, uygulamalar normal arama ve elkoyma kurallarına göre tesis edilmektedir.

ABD Anayasa'sına eklenmiş olan Dördüncü Değişiklik soruşturma aşamasında arama ve elkoyma işlemlerine ilişkin yetki sınırlandırılması getirmiştir. Bu konuda iki düzenleme bulunmaktadır. İlk *“olarak arama yapılması için arama kararının bulunması gerekliliği (Johnsan United States Davası, 1948), ikinci olarak ise istisnai durumlarda geçerli bir kararı olmadan da arama yapılmasına imkan verilmesidir (İllinois v. Rodriguez Davası, 1990).”*¹⁶²

Dördüncü Değişiklik taslağıyla beraber Amerikan mahkemeleri arama kararının gerekliliğine dair az sayıda istisnanın uygulanmasına müsaade etmişlerdir. *“Buna ek olarak mevcut arama kararının halihazırdaki olaya uygulanamayacağı, delillerin kaybolma ya da zarara uğrama riski altında olması gibi gerekçelerin bulunma zorunluluğu vardır*

162 Başlar Yusuf, Ceza Yargılamasında Elektronik Delil, Ankara, Yetkin Yayınları, 2016, s.128.

(*Parkhurst v. Trapp Davası*). ”¹⁶³

Arama kararına bağılı olarak yapılan arama ve elkoymada olması gereken şüphenin derecesini Dördüncü Değişiklik makul şüphe olarak tayin etmiştir. Dolayısıyla bir bireyin makul ve meşru özel hayat beklentisi arama ile ihlal edilmiyorsa, anayasal olarak belirlenen sınırlar da korunmuş olmaktadır. Dijital delillere ilişkin yapılan arama ve elkoyma işlemleri esnasında da aynı ‘makul özel hayat beklentisi’ ölçütü dikkate alınmaktadır.¹⁶⁴

Elektronik medyada muhafaza edilen bilgilerin kişinin özel hayatının makul beklentisi sayılıp sayılmadığını belirlemek için, bilişim sistemlerini doküman çantası ya da dosya dolabı gibi kapalı bir kap gibi konumlandırmak icap etmektedir. Böylelikle, *Dördüncü Değişiklik, benzer pozisyonadaki bir kapalı kabın açılması ve muhtevasının incelenmesinin yasaklanabilir olduğu hallerde, ekseriyetle, kolluk kuvvetlerinin elektronik medyada depolanmış verilere ulaşımını ve bunları görüntülemesini men etmektedir.*¹⁶⁵

ABD yargılama sisteminde arama kararı, arama yapılacak yer ve el konulması gereken kişisel eşyaya ilişkin açık ve belirgin olmalıdır. (*Kyllo v. United States Davası, 2001*) *Bu kurallarla hedeflenen amaç, yetkililerin arama kararıyla gerçekleştirdiği arama eylemini genel arama varmışçasına kişisel eşyaları gelişigüzel karıştırma işlemine dönüştürmemektir.*¹⁶⁶

ABD Ceza Muhakemesi Kanunu’nun 41/b maddesinde arama ve elkoymanın hangi makam tarafından talep edilebileceği, kimlerin karar mercii olduğu düzenlenmiştir. Söz konusu madde uyarınca arama ve elkoymaya ilişkin kararlar federal ceza infaz yetkilileri ve de savcı tarafından talep edilebilir. Bu kararlar, il ya da ilçe sınırları içindeki yetkili hakimlerce, bunun haklı nedenlerle mümkün olmadığı durumlarda ise, aynı bölgede buna yetkisi olan başka bir hakim tarafından verilir. Bilişim sistemlerine ilişkin aramalar ABD Ceza Muhakemesi Kanunu 41/e-2-i maddesine göre sulh hakimi tarafından arama kararına dayanarak en geç 14 gün içinde gerçekleştirilmelidir. Söz konusu 14 günlük süre arama işleminin ilk evresini kapsamakta, bilişim sisteminden alınmış imaj üstünde daha

163 Başlar, s. 128.

164 Başlar, s. 128.

165 Başlar, s. 130.

166 Başlar, s. 130.

sonradan yapılacak analiz ve inceleme süreleri bu sınırlamaya dahil değildir.¹⁶⁷

Ne var ki ilgili analiz ve inceleme süresine ilişkin pratikte bazı problemler ortaya çıkabilmektedir. “2010 yılında görülen *United States v. Mutschelknaus* davasında kolluk kuvvetleri hakim tarafından verilen arama kararına dayanarak 10 gün içinde arama ve elkoyma işlemlerini sonuçlandırmış, elektronik medya üzerinde yapılan analiz işlemini ise 60 gün içinde tamamlamışlardır. Her ne kadar 41. maddede bir süre kısıtlaması öngörülmemişse de, davaya konu olayda bilişim sisteminde gerçekleştirilen 60 günlük inceleme süresinin anayasal çerçevede makul sınırları aşıp aşmadığı mahkemece incelenmiş, süre fazla bulunmuş ve kolluk kuvvetlerinin incelemeden elde ettiği verilerin yargılamada delil olarak kullanılamayacağına hükmedilmiştir.”¹⁶⁸

Şartlar gerektirdiği takdirde kolluk kuvvetleri herhangi bir arama kararı ya da makul şüphe sebebi olmaksızın arama yapabilirler. Bu istisnai durumlardan biri kişinin rızasının bulunmasıdır. Örneğin eşlerden birinin rızası alınarak elektronik cihazlar üzerinde yapılan aramalar mahkemeler tarafından çoğunlukla geçerli sayılmaktadır. Ancak rızanın mahkemelerce geçerli kabul edilmediği davalar da görülebilmektedir. Bu duruma 1998 yılında görülen *United States v. Smith* davası örnek gösterilebilir. Davaya konu olayda tacizle suçlanan Smith isimli şahıs, “*Ushman ve iki kızıyla birlikte aynı evi paylaşmakta, kullandığı bilgisayar ise evin ebeveyn odasında bulunmaktadır. Ushman’ın Smith’e ait bilgisayarda kolluk kuvvetlerince gerçekleştirilen aramaya vermiş olduğu rıza mahkemece yerinde ve geçerli kabul edilmiş, verilen bu karara gerekçe olarak da Ushman’ın ebeveyn odasına giriş izninin bulunması ve söz konusu bilgisayara herhangi bir şifre konmaması gösterilmiştir.*”¹⁶⁹

Eşin elektronik medyaya erişim izninin olmadığı hallerde mahkemenin aksi yönde hüküm verdiği davalar da mevcuttur. “*Nitekim 2001 yılında görülmüş olan Trulock v. Freeh* davasında mahkeme kişinin eşine ait bilgisayardaki dosyalar üzerinde kolluk tarafından yapılan aramaya göstermiş olduğu rızayı geçersiz saymış, kararına gerekçe olarak da eşin dosyaya giriş şifresini bilmediğini göstermiştir.”¹⁷⁰

167 Başlar, s. 131.

168 Başlar Yusuf, Ceza Yargılamasında Elektronik Delil, Ankara, Yetkin Yayınları, 2016, s.132.

169 Başlar Yusuf, Ceza Yargılamasında Elektronik Delil, Ankara, Yetkin Yayınları, 2016, s.133.

170 Başlar, s.133.

Ebeveynlerin on sekiz yaşından küçük çocuklarının elektronik medyaları üzerinde yapılan aramalara göstermiş oldukları rıza da mahkemelerce geçerli sayılmaktadır. Şayet çocuk on sekiz yaşından büyükse, bu durumda verilmiş olan rızanın hukuksal geçerliliği mahkemece somut olaya göre değerlendirilmektedir.¹⁷¹

Örneğin “*bilişim sistemlerindeki arama aile konutunun ortak kullanım alanlarında yapılıyorsa, mahkeme bu durumda ebeveynin vermiş olduğu rızayı çocuğun yaşından bağımsız olarak geçerli kabul etmektedir.*”¹⁷²

3.6.2. İngiltere

Bilişim sistemlerinde arama ve elkoymaya ilişkin yasal çerçeveler İngiliz hukukunda üç farklı kanunda düzenlenmiştir. “*Bunlar sırasıyla 1984 tarihli Polis ve Suç Delili Kanunu (PACE), 1990 tarihli Bilgisayarın Kötüye Kullanılması Kanunu (CMA) ve son olarak Soruşturma Yetkileri Düzenleme Kanunu (RIPA) ’dur.*”¹⁷³

Polis ve Suç Delili Kanunu’na göre kolluk kuvvetlerinin arama işlemi yapabilmesi için makul bir sebep ve suç oluşturan bir eylem bulunması zorunludur. Bununla beraber arama işlemi bir bina ya da eklentilerinde gerçekleştirilecekse hukuki yararın varlığı da gözetilmelidir. Arama işleminin çerçevesi ABD’deki düzenlemelerde de öngörüldüğü gibi, kişi, eşya, ev ve eklentiler yönünden mümkün mertebe ayrıntılı bir şekilde çizilmelidir.¹⁷⁴

Elkoymaya dair genel düzenlemeler ise PACE’nin ikinci kısmındaki 19. maddede bulunmaktadır. Buna göre maddenin 2. ve 3. fıkraları uyarınca, “*bina bünyesindeki herhangi bir eşyanın bir suçun işlenmesi neticesinde temin edildiği veya bir soruşturmanın ya da başka herhangi bir suçun delili olduğu konusunda ve bu özellikteki eşyanın gizlenmesi, kaybolması, zarar görmesi, değiştirilmesi veya imha edilmesinin önüne geçilmesi amacıyla gerekli olduğundan bahisle makul nedenler mevcutsa kolluk söz konusu eşyaya*

171 Başlar, s. 132.

172 Başlar, s. 134.

173 Değirmenci, s. 293.

174 Başlar, s. 138.

el koyabilecektir.”¹⁷⁵

Bu maddeye dayanarak kolluk kuvvetleri gerek duyulduğu takdirde dijital medyada gizlenen, korunan veya bina içerisinde ele geçirilen veri ve bilgiye el koyabilir, ancak bunlar hem görüntülenebilir hem de okunabilir olmalıdır. Arama işlemi sırasında ulaşılan veri ve bilgiler sadece teknik cihazlarla okunuyor ya da görüntülenebiliyor olabilir, bu durum kolluk kuvvetlerinin o an için elkoyma işlemini gerçekleştirmesine engel teşkil etmez.¹⁷⁶

Kolluk kuvvetlerinin PACE m. 20 kapsamında genişletilmiş bir yetkiye sahip olduğu söylenebilir, zira kolluk, söz konusu yetkiye istinaden sadece bilgisayardaki verileri değil, bilgisayara bağlı durumdaki diğer üniteleri de araştırabilmektedir.

Polis ve Suç Delili Kanun’unun 19. ve 20. maddelerinde zikredilen makul nedenler var olduğu takdirde, polis kanuni şartları taşıyan bir arama kararı ile arama yapabilir, arama kararı kapsamında yer alan her objeye el koyabilir. Ayrı bir elkoyma kararı gerekmemektedir.

“Dijital ortamda saklanan bilgiler, delillerin kimler tarafından ve nasıl toplanacağına ilişkin PACE’de yer alan tüm hükümler Avrupa Konseyi Siber Suç Sözleşmesi’nin 19. maddesindeki düzenlemelere uyum sağlamaktadır, zira söz konusu uluslararası sözleşme 23.11.2001 tarihinde İngiltere tarafından imzalanmış, 25.05.2011’de onaya sunulmuş, kabul edilmiştir. İç hukukta yürürlüğe girmesi ise 01.09.2011 tarihini bulmuştur.”¹⁷⁷

Elektronik medya üzerinde arama ve elkoymaya ilişkin bir diğer kanun olan Bilgisayarın Kötüye Kullanılması Kanunu (CMA)’nda kasten dijital virüs yayma ve bilgisayar korsanlığı gibi suçlar düzenlenmiş, böylelikle elektronik ortamlarda yaygın olan yetkisiz erişimle sisteme müdahale etmek ve suç örgütlerine bilişim sistemleri aracılığı ile yardım etmek gibi suç teşkil eden eylemlerin engellenmesi hedeflenmiştir.¹⁷⁸

Soruşturma Yetkilerinin Düzenlenmesi Kanunu (RIPA) İngiltere’de dijital medya

175 Başlar, s. 139.

176 Başlar, s. 139.

177 Başlar, s. 139.

178 Başlar, s. 140.

üzerinde arama ve elkoyma hususlarını düzenleyen bir başka kanundur. Kanun, soruşturma yürüten birimlere arama kararı olmaksızın oldukça geniş yetkiler sunmakla beraber, hakim kararıyla verilen yetkilere de yer vermektedir. Örneğin RIPA'nın 49 ile 56. maddeleri arasında şifrelenmiş dijital verilerin açığa çıkarılması ve sunulması için bildirimde bulunma zorunluluğu vardır. *“Eğer ki bir olayda makul nedenler mevcutsa soruşturma yetkilisi hakim kendisine vermiş olduğu uygun izinle şifreyle korunan elektronik medyanın sahibine şifreyi açıklama yükümlülüğünü bildirir. Şifrenin sahibi bu açıklamayı yalnızca hakim uygun izni verdiği ya da söz konusu kararda yetkili olarak gösterilen kişiye yap- makla yükümlüdür.”*¹⁷⁹

Elektronik medyalara ilişkin tedbirlerin yer aldığı PACE'ye nazaran çok daha detaylı bir düzenleme olarak göze çarpan RIPA, şifreyle korunan verilerin çözümüne dair hükümler içermekle beraber, aynı zamanda diğer dijital 'iletişim cihazları' için de kullanılabilir.

İngiliz hukuk sisteminde kanun koyucu RIPA'da bilişim sistemi, bilgisayar gibi genel tanımlamalardan kaçınmış, dikkati daha çok veri tanımına çekerek, verinin saklandığı alanların tarifi konusunda herhangi bir sınırlama getirmemiştir. Bu uygulama son yıllarda gelişim hızının öngörülmesi gittikçe zorlaşan teknolojik gelişmeler yönüyle son derece yerinde ve isabetli bir yaklaşım olmuştur.

Bilişim sistemlerine dair bir diğer önem arz eden husus da uzaktan erişimle aramadır. Her ne kadar İngiltere'de uzaktan arama işlemine, kullanılan cihazların meşruiyetine ve bu aramadan elde edilen delillerin yargılamadaki kullanılabilirliğine dair bir mahkeme kararı mevcut değilse de, Avrupa Konseyi'nin yönlendirmesiyle uzaktan arama resmi olarak bir soruşturma yöntemi haline gelebilmiştir. Bu bağlamda İngiltere İçişleri Bakanlığınca onaylanan bir plana göre kolluk kuvvetleri ve gizli servis, herhangi bir arama kararı olmadan, şüphelilere ait bilişim sistemleri üzerinde uzaktan erişimle arama işlemlerini gerçekleştirebilmiştir. Bu konuyu meşru bir zemine taşıma çalışmaları esasen 1994 yılında başlamıştır. Öncelikle CMA'da bazı hükümler değişmiş, böylece bilişim sistemine uzaktan erişim yapılması yasallaşmıştır. Benzer adımlar bir diğer kanun olan RIPA'da atılmış, yönlendirilmiş gözetim tedbiri adı altında yeni düzenlemeler getirilmiş-

179 Başlar, s. 141.

tir.¹⁸⁰

Geçmiş çok eskiye gitmeyen yönlendirilmiş gözetim tedbirinde kolluk güçleri, gizli bir soruşturma ve izleme faaliyeti içinde ciddi bir suçun işlendiğinden ya da önlenmesi gerektiğinden bahisle, şüpheli hakkında bilgi edinmeye çalışırlar. Soruşturma esnasında RFS olarak adlandırılan spesifik cihazlar yardımıyla belirli kişi ya da kişilere dair bilgi toplanmakta, şüpheliye ait bilişim aygıtında saklanan dijital verilere ulaşılmakta ve çevrimiçi hareketleri izlenebilmektedir.¹⁸¹

3.6.3. Almanya

“Bilişim sistemlerine dair ‘veri’ kavramı Alman Ceza Kanunu’nda ilk kez Avrupa Konseyi Siber Suç Sözleşmesi’nin 23.11.2001’de imzalanması ve 01.07.2009’da iç hukukta yürürlüğe girmesi ile yer almıştır. Buna göre kanunda adı geçen elektronik verilerin muhafaza edildiği ve işlem gördüğü elektronik ortama girmek, burada bulunan verileri elde etmeye çalışmak Alman Ceza Kanunu 202a maddesi gereğince suç teşkil etmektedir.”¹⁸²

Bununla beraber Siber Suç Sözleşmesi’nin elektronik verilerin aranması ve bunlara el konulmasına ilişkin 9. maddesi iç hukukta herhangi bir karşılık bulmamıştır. Sonuç itibarıyla elektronik ortam ve cihazlara yönelik arama ve elkoyma tedbirleri Alman Ceza Muhakemesi Kanunu’nda hususi olarak düzenlenmemiştir. Söz konusu sistemlere ilişkin tedbirler normal arama ve elkoyma kurallarına göre yerine getirilmektedir.

Ceza soruşturması kapsamında suçun aydınlatılması için önem taşıyan ve elektronik medyalarda muhafaza edilen verilere Alman Ceza Muhakemesi Kanunu 94. maddesi gereğince el konulabilir. Söz konusu bilişim sistemi, sahibi tarafından kendi istek ve iradesiyle yetkili organlara teslim edilmediği takdirde, kolluk kuvvetlerinin zorla elkoyma hakkı saklıdır. Elkoyma işlemi aynı kanunun 98. maddesine göre hakim vermiş olduğu karara istinaden, acil müdahale gerektiren hallerde ise savcı ya da diğer adli organlar tarafından verilmiş kararlarla yapılır. Hakim kararı olmaksızın gerçekleştirilen elkoyma işlemi

180 Başlar, s.142.

181 Başlar, s.142.

182 Başlar, s.143.

soruşturma organları tarafından en geç 3 gün içinde hakimın onayına sunulmak mecburiyetindedir. Karar 3 gün içinde verilmelidir. Eşyasına el konulan kişinin bu karara itiraz hakkı her zaman mevcuttur.¹⁸³

*“Soruşturma organlarınca arama işlemi neticesinde elde edilen eşya ya da belgeler Alman Ceza Muhakemesi Kanunu 110. madde gereğince ancak savcılık ya da bu makamca yetki verilmiş organlar tarafından incelenebilir. Kolluğun elde edilen verileri doğrudan inceleme yetkisi bulunmamaktadır.”*¹⁸⁴

Savcılığın bizzat kendisinin ya da kolluk kuvvetlerinin yardımıyla veri toplaması, ilgili organlarla yazışması aynı kanunun 161. maddesinde düzenlenmiş, 163. maddesinde ise kolluğun delillerin elde edilmesine ve karartılmasının engellenmesine ilişkin görev kapsamı belirlenmiştir. Her iki madde aynı zamanda elektronik medya üzerinde gerçekleştirilen arama ve elkoyma işlemleri yönüyle de uygulanabilir özelliği taşımaktadır.¹⁸⁵

Alman hukukunda bir diğer önem arz eden konu elektronik posta trafiğine ilişkin uygulamalardır, nitekim Alman Anayasası’nın 10. maddesine göre bu konuya ilişkin soruşturma tedbirlerinde haberleşmenin gizliliği prensibi esastır.

Ancak ve ancak soykırım, cinayet, hırsızlık vb. gibi ağır ceza gerektiren suçlara ilişkin yapılan soruşturmalarda elektronik haberleşme trafiği polis tarafından izlenebilmektedir. Söz konusu suçlar ise Alman Ceza Muhakemesi Kanun’unun 100. maddesinde açıkça sayılmıştır.¹⁸⁶

Son yıllarda alman hukuk camiasında gündeme gelen bir diğer konu da uzaktan erişimle aramadır. Bilişim sistemleri üzerinde uzaktan erişimle arama yapma işleminin hukuken uygulanabilirliği tartışmalıdır. “25 Kasım 2016’da görülen bir davada Bundesgerichtshof Federal Mahkemesi şüpheli şahsa ait bir bilgisayarın uzaktan erişimle aranmasına ilişkin Savcılık kararının kaldırılmasına hükmetmiştir. Savcılık ise Ceza Kanunu’nun 94, 102 ve 110. maddelerini gerekçe göstererek söz konusu karara itiraz etmiş, ancak Federal Mahkeme polisin şüphelinin evinde yaptığı genel aramayla uzaktan

183 Başlar, s. 143.

184 Başlar, s. 144.

185 Başlar, s. 144.

186 Başlar, s. 144.

erişimle bilgisayarda gerçekleştirdiği aramanın aynı olmadığını öne sürmüş, alman yasalarına göre kolluk kuvvetlerinin uzaktan arama yapmaya yetkisinin bulunmadığından bahisle savcılığın itirazının reddine karar vermiştir.”¹⁸⁷

30 Aralık 2016 yılında Nordrhein–Westfalen eyaleti tarafından Anayasayı Koruma Kanununun 5/2 maddesinde yeni bir düzenlemeye gidilmiştir. “*Bu ilave edilen maddeyle birlikte bilişim sistemleri ağı üzerinden gerçekleştirilen bilgi alışverişlerinde kolluğa gizli araştırma ve izleme yetkisi verilmiş, böylelikle şüpheli kişinin şahsi bilgisayarı veya laptopu üzerinde Anayasa Koruma Kurulunca uzaktan erişimle arama yapılabilmesi bakımından legal bir zemin oluşturulmuştur. Ne var ki, söz konusu yasal düzenleme anayasal şikayet başvurusu kapsamında Alman Federal Anayasa Mahkemesi tarafından ele alınmış ve 27 Şubat 2008 yılında ilave kanun maddesinin anayasaya aykırı olduğu kararı verilmiştir. Hükme gerekçe olarak yeni nesil teknolojik sistemlerinin zaman içinde yeni bir insan hakkının daha doğmasına neden olduğu, bu sebeple bu hak kapsamında da gizliliğin ve dahi bütünlüğün korunması gerektiği gösterilmiştir.*”¹⁸⁸

Sonuç olarak Amerika Birleşik Devletleri ve Almanya’nın Avrupa Konseyi Siber Suç Sözleşmesinin taraf ülkeleri olmalarına rağmen dijital verilerin aranması ve el konulmasına ilişkin Sözleşme’nin 19. maddesi çerçevesinde herhangi bir özel düzenleme yapmadığı, arama ve elkoyma tedbirlerine dair genel düzenlemeleri ve mahkeme içtihatlarını kullanma yolunu tercih ettikleri görülmüştür.

İngiltere ise İngiliz Polis ve Suç Delili Kanunu (PACE) ve Soruşturma Yetkilerinin Düzenlenmesi Kanunu (RIPA) ile Avrupa Konseyi Siber Suç Sözleşmesi’nin 19. maddesiyle uyumlu hukuki düzenlemeler yapma yoluna gitmiştir.

187 Başlar, s.145.

188 Başlar, s.145.

SONUÇ

Genel olarak deliller, hukuki bir uyumsuzluğu ispat etmekte kullanılan bilgi ve bul-gulardır. Dijital deliller ise dijital ortamda bulunan ve dijital cihazlar tarafından iletilen bilgi ve verilerdir. Dijital delillerin en önemli özelliklerinden ve maalesef dezavantajlarından biri kolayca değiştirilebilir, silinebilir ve bozulabilir olmalarıdır. Bundan dolayı suç mahallinde yapılacak olan olay yeri incelemeleri uzman bir ekip aracılığıyla ve hassas teknik cihazlarla yapılmalıdır. Aksi takdirde suçun aydınlatılmasında kullanılabilecek olan dijital deliller çok rahatlıkla kullanılamaz hale gelebilmektedir. Olay yerindeki bilinçsiz her müdahale delil bütünlüğünün bozulmasına ve yargılama aşamasında çok önem arz eden bir delilin tahrif olmasına neden olabilmektedir. Bu süreçte birçok hatanın telafisi mümkünken, dijital delillerin toplanması ve değerlendirilmesi aşamasında yapılan hataların telafisi hiç olmamakta ya da çok zor olmaktadır. Nitekim ülke geneline bakıldığında adli bilişimde delillerin elde edilmesi, analiz ve bilirkişilik hususunda usul ve esaslara ilişkin yerleşmiş bir standart hala mevcut değildir.

Ceza Muhakemesi Kanunu'nda genel nitelikteki arama hükümleri 116. ve 123. maddelerde düzenlenmiştir. 134. madde ise özel nitelikte bir düzenlemedir. Buna göre şüphelinin işyeri veya konutunda CMK 116. madde uyarınca gerçekleştirilen bir arama-da, şüphelinin kullandığı bilgisayar üzerinde bir arama yapılamaz. Bunun için ayrıca CMK m. 134'e göre bir arama kararı alınması gerekmektedir. Aksi takdirde kolluk kuvvetlerinin yapmış olduğu bu arama hukuk aykırı olup, buradan elde edilen deliller de yasak delil niteliğindedir.

Söz konusu düzenleme gerek özel hayatın ve haberleşmenin gizliliği hakları yönünden ve Avrupa İnsan Hakları Sözleşmesi'nin m 8/2 ve 10/2 maddeleri bakımından gerekse Anayasa'nın 20/2, 22/2 ve 26/2 maddelerinde hüküm altına alınan istisnai durumlar ve oranlılık ilkesi açısından uygulanabilir bir hükümdür. Ne var ki uygulama sırasında kolluk kuvvetlerinin usul kuralları takibi noktasında gerekli hassasiyetten uzak yaklaşımları ve madde hükmünün farklı yorumlanması bazı ihlalleri beraberinde getirebilmektedir. Bu nedenle dijital delilleri elde etme aşamasında CMK ve diğer düzenlemelerdeki usul kurallarına uymayan kolluk görevlileri için daha etkin ve sıkı yaptırımlar tartışmaya açılmalıdır. Aksi takdirde toplanan deliller hukuka aykırı hale gelmekte, yargılamada kullanılamamakta ve sonuç olarak maddi gerçeğin ortaya çıkması zorlaşmakta ya

da mümkün olamamaktadır. Soruşturma aşamasındaki tüm şüphelerin eğitimi, uluslararası kabul gören sertifika programlarının ve özellikle adli bilişim uzmanlarının istihdamı bu nedenle büyük önem taşımaktadır.

Ceza Muhakemesi Kanunu'nun 1. fıkrası uyarınca, bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine (...) karar verilir.

Aynı maddenin 2. fıkrasına göre bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşamaması ya da işlemin uzun sürecektir olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

Yasa metnine göre bilgisayara ancak şifreli olduğunda, şifrenin çözülmesinin mümkün olmadığı, gizlenmiş bilgilere ulaşamaması ya da işlemin uzun sürecektir olması halinde elkonulabilir, bunun dışında elkonulmasına olanak yoktur. Bu haliyle söz konusu düzenlemede eksiklik göze çarpmaktadır, zira sadece yasa metninde ifade edilen hallerde değil, ayrıntılı bir incelemenin lüzumlu olduğu her durumda bilgisayarların adli bilişim laboratuvarında incelenmesi gerekmektedir. İlgili kanun maddesinin metnine eklenecek 'ayrıntılı bir incelemenin lüzumlu olduğu her durumda' ibaresi elkoymaya ilişkin tüm halleri kapsayan bir tanımlama olarak bu yönde ortaya çıkabilecek muhtemel problemleri bertaraf edecektir.

Söz konusu yasa metninde 'şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde elkonulan cihazlar gecikmesizin iade edilir' ibaresi yer almaktadır. Burada dikkat çeken husus daha bilirkşi incelemesi tamamlanmadan hard diskin şüpheliye iade ediliyor olmasıdır. Oysa bu durum her şartta doğru bir uygulama olmayabilir. Zira bilgisayarda sadece bulundurulması dahi suç teşkil eden dosyalar, bilgiler olabilir ve bunlar da ancak adli bilişim laboratuvarında yapılan inceleme sonucu anlaşılabilir. Örneğin

kolluk kuvvetlerinin çocuk pornografisi nedeniyle elkoymuđu bir hard diskin CMK m. 134 kapsamında řüpheliye iade edilmesi dođru bir uygulama olmayacaktır. Dolayısıyla hard diskin hangi suç ya da suçlar kapsamında iade edileceđi konusunda da ilgili madde de bir ek düzenlemeye gidilmesi son derece önemlidir.

Üzerinde durulması gereken bir diđer konu ise CMK’nın 134. maddesinin 3. fıkrasıdır. Madde metnine göre bilgisayar ve bilgisayar kütüklerin elkoyma işlemi sırasında, sistemdeki tüm verilerin yedeklemesi yapılır. Ancak büyük boyutlu dolandırıcılık suçlarında el konulan onlarca bilgisayar, cep telefonu, Iphone ve Ipad içeriğinin nasıl yedekleneceđi ve nerede muhafaza edileceđi mühim bir sorundur. Uygulamaya bakıldığında yedekleme için gerekli olan veri depolama birimlerinin (hard diskler) henüz suçluluđu ispatlanmamış řüpheliye aldırıldığı gözlemlenmektedir. Zira ne adliyenin ne jandarmanın ne de polisin elkoyma esnasında boş veri depolama ünitesi aldırıtma hakkı bulunmamaktadır. Dolayısıyla eđer ki yasa metninin dođru şekilde uygulanması isteniyorsa, gerek adliyelerde gerekse polis merkezlerinde geniş çapta adli vakaların ortaya çıkma ihtimaline binaen yüzlerce ya da binlerce boş hard diskin hazır bekletilmesi gerekmektedir.

Ayrıca yasa metninde ‘yedek alma ve kopyalama’ terimlerine yer verilmekte, ancak ‘imaj alma ya da hash değeri’ zikredilmemektedir. Halbuki bir veri taşıma aracının kopyasının ya da yedeğinin alınması işlemi ile imajının alınması ve bunun neticesinde hash değerinin elde edilmesi işlemi arasında fark vardır. Zira yedekleme ve kopyalama işleminde boş veriler kopyalanmamakta, veri bütünlüğünün ve güvenliğinin korunması bu şekilde riske girmektedir. Bu da dijital delillerin güvenilir olma özelliklerini kaybetmelerine neden olmaktadır. İmaj alma ve hash değeri ibarelerinin kanun metninde yer almaması, hatta bir yönetmelikle dahi düzenlenmemesi önemli bir eksiklik olarak göze çarpmaktadır.

Bu eksik düzenlemeye rağmen kolluk kuvvetleri yürütülen soruşturmalarda yüksek görev bilinciyle hareket ederek, uluslararası standartlar dahilinde yine de imaj ve hash değeri alma işlemlerini yerine getirmektedirler. Ne var ki, bu işlemleri yapmayan bir soruşturma görevlisi bu konuda yasal bir düzenleme olmadığı için kimseye hesap vermek zorunda kalmamaktadır. Bu nedenle CMK ya da yönetmelikte konuya ilişkin bir düzenlemenin bir an önce hayata geçirilmesi gerekmektedir.

İlgili maddenin 5. fıkrasına göre bilgisayar ve bilgisayar kütüklerine elkoymaksızın da sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kağıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır. Yasa metninde geçen ‘sistemdeki verilerin tamamının veya bir kısmının kağıda yazdırılarak...’ hükmünün her vakada hayata geçirilmesi mümkün değildir, zira yüzbinlerce satır bilginin kağıda bastırılmak suretiyle hakim önüne konması imkan dahilinde değildir.

Her ne kadar arama, elkoyma ve kopyalama işlemleri CMK’nın 134. maddesinde düzenlenmiş olsa da, taşra ve merkez olmak üzere farklı yerlerde gerçekleştirilen işlemler konusunda uzman personelin yetersizliği ya da kolluk kuvvetlerinin sahip olduğu teknik imkanlar hala ciddi farklılıklar göstermektedir. Bu hususta öncelikle ülke çapında belli bir standardın belirlenmesi ve bu standardın her yerde uygulanması gerekmektedir, zira bu durum kolluk kuvvetlerinin yapmış olduğu işlemlere duyulan güveni artıracak, delillerin bütünlüğü ve doğruluğunu perçinleyecek ve suç soruşturmasının sağlıklı bir şekilde yürütülmesine yardımcı olacaktır. Bu nedenle kolluk kuvvetlerinin ve bilişim aygıtları üzerinde inceleme yapan uzmanların kullandıkları teknikler, analiz işlemlerini nerede ya-pacakları, hazırlayacakları ve sunacakları rapor konusunda CMK’nın 134. maddesinde ek bir düzenlemeye gidilmesi yasal bir standardın oluşturulmasına katkı sağlayacaktır.

Olay yeri incelemesinde uzman kişi tarafından elde edilen dijital delillerin değişime uğramadan analiz edilmesi ve değerlendirilmesi aynı zamanda adli bilişimin de temelini oluşturmaktadır. Zira adli bilişim uzmanlarının amacı mahkemeye sunulan dijital delillerin kabul edilmesini sağlamak ve bu hedefe ulaşmak için incelemenin her aşamasında delillerin orijinalliğinin korunması yönünde azami bir dikkat göstermektir. Delil koruma ve gözetim zincirine özen göstermek aynı zamanda suçun aydınlatılmasında ve maddi gerçeğe ulaşma yolunda atılan ilk adımdır.

2016 yılında Olağanüstü Hal Kapsamında çıkarılan 674 sayılı Kanun Hükmünde Kararnameye istinaden Adli Tıp Kurumu bünyesinde ‘Adli Bilişim İhtisas Dairesi’ kurulmuş, daireye, mahkeme, hakimlik ve savcılık tarafından bir talep geldiğinde bilişimle alakalı hususlarda gerekli incelemelerde bulunma, analiz etme ve raporlama yetkisi tahsis edilmiştir.

Bu bağlamda üniversitelerin hukuk fakültelerinde veya enstitülerinde de adli bilişim derslerinin zorunlu ders kapsamına alınması, konuya yönelik eğitim müfredatının uluslararası standartlara uygun şekilde hazırlanması yerinde olacaktır. Bununla beraber yazılı, görsel, işitsel ve dijital medyada adli bilişim ve dijital delillere ilişkin bilimsel ve eğitici yayınların yaygınlaşması sağlanmalı, bilimsel incelemelere finansal kaynak desteklenmeli, ülke çapında bir ‘adli bilişim farkındalığı’ oluşturulmalıdır. Farkındalığın artması, ilgili hukuk alanlarına talebi artıracak gibi, açılan yeni enstitülerde istihdam konusunu da ortadan kaldırmış olacak, Avrupa’da genç ve dinamik nüfusuyla öne çıkan Türkiye’nin bu alanda öncülük etmesine katkıda bulunacaktır.

Dijital delillerin özellikleri, neleri kapsadığı, araştırma sürecinde ihtiyaç duyulan yöntem ve cihazlar, incelemenin hangi teknik uzmanlar tarafından gerçekleştirileceği ve elde edilen delillerin yargılama aşamasında nasıl kullanılacaklarına dair kuralların hukuk sisteminde özel bir şekilde düzenlenmesi gerekmekte, bu düzenlemelerin mümkün mertebe dünyadaki diğer hukuk sistemleriyle uyumlu olması gerekmektedir. Zira bilişim suçları mevcut sanal dünyada sadece bir ülke ile sınırla kalmamakta, aksine birçok ülke hukukunu teğet geçmekte, dolayısıyla suç yolunun farklı hukuk sistemleriyle kesişmesi kaçınılmaz hale gelmektedir. Bu nedenle yeni nesil olan dijital delil türlerine ilişkin ortaya çıkan sorunların diğer hukuk sistemleriyle karşılaştırılarak yorumlanması ve gerekirse yeniden tanımlanarak çözümler üretilmesi gerekmektedir. Bu noktada özellikle cep telefonlarına ilişkin elkoyma koruma tedbiri dikkat çekmektedir. Günümüz teknolojisinde cep telefonları normal bir bilgisayarın neredeyse tüm özelliklerini taşımaktadırlar. Öyle ki, elektronik posta ile haberleşme, internet bağlantısı, verilerin muhafazası vb. gibi kullanıcıların sıklıkla başvurduğu işlemler bilgisayarlardan çok cep telefonları aracılığı ile yapılmaktadır. Ancak uygulamaya bakıldığında cep telefonları ve benzer nitelikteki birçok elektronik cihaz hala bilgisayar tanımı altında konumlandırılmamıştır. Nitekim bilgisayar dışındaki eşyalara ilişkin tüm arama ve elkoyma işlemleri hala CMK m. 116-129 de düzenlenen hükümlere göre gerçekleştirilmektedir. Ortada bir suçun işlendiğine ilişkin makul bir şüphe bulunduğu takdirde CMK m. 127 uyarınca kolluk amirinin yazılı emriyle cep telefonuna elkonulabilmekte, ancak şüphelinin haklarını güvence altına alan yedekleme gibi bir önlem maalesef söz konusu olmamaktadır. Uygulamada ortaya çıkan bu problem temel hak ve özgürlükler bakımından tartışmalı olup, kişisel veriler ve özel hayatın gizliliği ilkesiyle de hiçbir şekilde örtüşmemektedir. Üzerinde arama işlemi gerçekleştirilen cep telefonlarının bilgisayarla aynı kanun maddesi içinde yer alması bu

ihlalleri bertaraf edecektir.

Tüm bu nedenlerden dolayı yapılacak yasal düzenlemenin öncelikle hızla ilerleyen teknolojik gelişmelere uyum sağlayacak geniş bir kapsamda ele alınması, bilişim sistemlerinin bağlantılı olduğu tüm donanımlarıyla birlikte değerlendirilmesi ve bilişim hukukuna dair tüm hususların ayrı bir kanunda, örneğin Bilişim Suçları Kanunu'nda, düzenlenmesi gerekmektedir.

Nitekim dijital delillerin dinamik yapısı, onları sadece bizim değil dünyadaki tüm hukuk sistemlerinde değişime ve gelişime açık bir hale getirmektedir. Birkaç yıl öncesine kadar varlığı dahi bilinmeyen suç türlerinin bugün en fazla işlenen suçlar arasına girmesi dijital dünyanın ve bu dünyada işlenmekte olan suçların toplumdaki gidişatı konusunda endişeleri her geçen gün artırmakta, Ceza Muhakemesi Hukuku'nda dijital delillere ilişkin yeni düzenleme ve yaptırımların yukarıda değindiğimiz üzere gerekliliğini her geçen gün daha fazla gündeme getirmektedir.

Son olarak adli bilişim ve elektronik deliller artık sadece ulusal değil küresel güvenlik bakımından da hayati önem taşımaktadırlar. Bu alanda bilgi, teknik donanım ve bilimsel çalışmalarını sürekli güncel tutan, yenileyen ülkeler diğerlerinden bir adım önde olacak, uluslararası siber platformlarda dijital çağın en etkin söz sahipleri olarak yer alabileceklerdir.

KAYNAKÇA

APAYDIN, Cengiz. Bilişim Suçları ve Ceza Hukuku. İstanbul: Acar Matbaacılık, 2017.

AYDIN, Devrim. Ceza Muhakemesinde Deliller. Ankara: Yetkin Yayınları, 2014.

BAŞLAR, Yusuf. Ceza Yargılamasında Elektronik Delil. Ankara: Yetkin Basımevi, 2016.

CENTEL, Nur ve **ZAFER**, Hamide. Ceza Muhakemesi Hukuku. 13. Baskı. İstanbul: Beta Yayınları, 2016.

ÇAKIR, Hüseyin ve Kılıç, Mehmet Serkan. Adli Bilişim ve Elektronik Deliller. Ankara: Seçkin Yayıncılık, 2014.

DEĞİRMENCİ, Olgun. Ceza Muhakemesinde Sayısal (Dijital) Delil. Ankara: Seçkin Yayıncılık, 2014.

DEMİRBAŞ, Timur. Soruşturma Evresinde Şüphelinin İfadesinin Alınması. 4. Bası. Ankara: Seçkin Yayıncılık, 2015.

DİNLER, Veysel. Ceza Muhakemesinde Delillerin Toplanması. Polis Akademisi Güvenlik Bilimleri Enstitüsü, 2009.

DÜLGER, Murat Volkan. Bilişim Suçları ve İnternet İletişim Hukuku. Ankara: Pusula Yayıncılık, 2015.

GÖKSOY, Resul. Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenilirliğinin Sağlanması. Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, 2017.

GÖKŞEN, Elif. Türk Ceza Muhakemesinde Dijital Verilerin Delil Değeri. Yüksek Lisans Tezi, İstanbul, 2014.

HENKOĞLU, Trkay. Adli Biliřim, Dijital Delillerin Elde Edilmesi ve Analizi,

İSTANBUL: Pusula Yayıncılık, 2014.

ÖZBEK, Murat. Adli Biliřimde Delillerin Toplanması ve İncelenmesi. Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, 2013.

ÖZTRK, Bahri (Editr). Ana Hatlarıyla Ceza Muhakemesi Hukuku. 4. Baskı. Ankara: Seçkin Yayıncılık, 2017.

ÖZEN, Muharrem ve **ÖZOCAK**, Grkan. ‘Adli Biliřim, Elektronik Deliller ve Bilgisayarlarda Arama ve Elkoyma Tedbirinin Hukuki Rejimi (CMK M. 134)’. Ankara Barosu Dergisi, s.1. (Ocak 2015).

ŞENGL G, **ATSAN F.K**, **BOSTAN A** (2014). Adli Biliřim Alanındaki Mevcut Problemler, Çzm nerileri ve Gelecek ngrleri. 7.Uluslararası Bilgi Gvenlięi ve Kriptoloji Konferansı, İstanbul, 17-18 Ekim, 97-98.

NVER, Yener ve **HAKERİ**, Hakan. Ceza Muhakemesi Hukuku, Ankara: Adalet Yayınevi, 2017.

YURTCA, Erdener. CMK Şerhi. Ankara: Adalet Yayınevi, 2017.

İNTERNET SİTELERİ

<https://fordefence.com/dijital-delillerde-adli-bilisim/> (Son Er. T.: 30.05.2019).

<http://btkultur.blogspot.com/2016/06/network-forensic-nedir.html>
(Son Er. T.: 30.05.2019).

<https://www.egm.gov.tr/siber> (Son Er. T.: 30.05.2019).

<https://www.ozgureralp.com.tr/read-offline/5819/internette-mustehcenlik-sucu-ve-cezası.print> (Son Er. T.: 30.05.2019).

http://www.teknolojide.com/bilgisayar-nedir_4881.aspx (Son Er. T.: 30.05.2019).

<https://www.pcbilimi.com/sabit-disk-nedir/> (Son Er. T.: 30.05.2019).

<https://ademocut.com/sabit-disk-nedir-sabit-disk-cesitleri-nelerdir-adem-ocut/>
(Son Er. T.: 30.05.2019).

<https://teknoprom.com/usb-bellek-nedir-nasil-calisir/> (Son Er. T.: 30.05.2019).

<https://wmaraci.com/nedir/hafiza-karti> (Son Er. T.: 30.05.2019).

<https://bilgihanem.com/cd-dvd-surucusu-nedir-nasil-calisir/> (Son Er. T.: 30.05.2019).

<https://www.elektrikport.com/teknik-kutuphane/kamera-nasil-calisir/14791#ad-image-0>
(Son Er. T.: 30.05.2019).

<https://www.mailce.com/kamera-nedir.html> (Son Er. T.: 30.05.2019).

<https://www.tech-worm.com/yazici-nedir-yazici-turleri-nelerdir/> (Son Er. T.: 30.05.2019).

<https://www.hermesiletisim.net/blog/cep-telefonlari-arasinda-iletisim-nasil-gerceklesir#.XVgPuafBLLZ> (Son Er. T.: 30.05.2019).

<https://www.turkcebilgi.com/cep-telefonu-nedir> (Son Er. T.: 30.05.2019).

<https://wmaraci.com/nedir/oyun-konsolu> (Son Er. T.: 30.05.2019).

<https://www.adlibilisimuzmani.com/adli-kopya-alma-donanimlari-imaj-alma-donanimlari/>
(Son Er. T.: 30.05.2019).

<https://wmaraci.com/nedir/yazma-korumasi> (Son Er. T.: 30.05.2019).

<https://www.adlibilisimuzmani.com/adli-bilisim-yazma-koruma-write-blocker/>
(Son Er. T.: 30.05.2019).

<https://fordefence.com/ram-analizi-ve-adli-bilisimdeki-yeri/> (Son Er. T.: 30.05.2019).

<http://fatihberber.com/adli-bilisim-incelemelerinde-birebir-kopya-alma/>
(Son Er. T.: 30.05.2019).

<https://www.adlibilisimuzmani.com/adli-kopya-alma-yazilimleri-imaj-alma-yazilimleri/>
(Son Er. T.: 30.05.2019).

<https://www.slideshare.net/bgasecurity/ram-belleklerinin-adli-biliim-analiz-teknikleri>
(Son Er. T.: 30.05.2019).

<https://sqlserverrider.wordpress.com/2013/03/01/generate-hash-value-sing-md-and-sha-algorit hm-sql-server/> (Son Er. T.: 30.05.2019).

<http://www.ilovefreesoftware.com/12/windows/portable-sha1-md2-md5-hash-generator-calculate-hash-value-files.html> (Son Er. T.: 30.05.2019).

<https://www.adlibilisimuzmani.com/elektronik-delillerin-paketlenmesi-tasinma-si-ve-muhafazasi/> (Son Er. T.: 30.05.2019).

<https://mosequipment.com/products/mission-darkness-large-non-window-faraday-bag>
(Son Er. T.: 30.05.2019).

<https://www.adlibilisimuzmani.com/adli-bilisimde-elektronik-delillerin-incelenmesi/>
(Son Er. T.: 30.05.2019).

<https://www.difose.com.tr/laboratuvar/> (Son Er. T.: 30.05.2019).

<http://tuncaybesikci.com/adli-bilisim-nedir/> (Son Er. T.: 30.05.2019).

<https://support.passware.com/hc/en-us/articles/221742468-How-to-use-Passwa-re-Kit-Forensic-with-Guidance-Software-EnCase> (Son Er. T.: 30.05.2019).

<http://allpcworld.com/forensic-toolkit-ftk-imager-free-download/> (Son Er. T.: 30.05.2019).

<https://www.howtoforge.com/tutorial/linux-dd-command-clone-disk-practical-example/> (Son Er. T.: 30.05.2019).

http://www.mfa.gov.tr/no_-299_-ulkemizin-itu-konsey-uyeligi-hk.tr.mfa (Son Er. T.: 30.05.2019).

<https://www.sibersan.com/sanal-ortamda-islenen-suclar-sozlesmesi-6533-sayili-yasa/> (Son Er. T.: 30.05.2019).

<http://www.mfa.gov.tr/ekonomik-isbirligi-ve-kalkinma-teskilati.tr.mfa> (Son Er. T.: 30.05.2019).

<http://www.mfa.gov.tr/nato-tarihce.tr.mfa> (Son Er. T.: 30.05.2019).

<https://www.ultraedit.com/company/blog/products/2015-ultraedit-v22.html> (Son Er. T.: 30.05.2019).

<https://www.jasonsamuel.com/2010/01/12/using-log-parser-to-query-huge-log-files-and-only-display-the-results-you-need/> (Son Er. T.: 30.05.2019).

<https://f-response.com/blog/f-response-live-physical-memory-x-ways-forensic-162-preview-4> (Son Er. T.: 30.05.2019).

<https://comodo-registry-cleaner.en.softonic.com/> (Son Er. T.: 30.05.2019).

<https://berqnet.com/blog/loglama>.

<https://www.endustri40.com/bulut-bilisim-cloud-computing-nedir/> (Son Er. T.: 30.05.2019).

<https://bilgisayarbaligi.wordpress.com/2015/10/17/cloud-computing-bulut-bilisim/> (Son Er. T.: 30.05.2019).

<https://www.endustri40.com/bulut-bilisim-cloud-computing-nedir/>
(Son Er. T.: 30.05.2019).

<http://yunus.hacettepe.edu.tr/~ceren.bayindir11/webfinal/modelleri.html>
(Son Er. T.: 30.05.2019).

<https://azure.microsoft.com/tr-tr/overview/what-is-a-private-cloud/>
(Son Er. T.: 30.05.2019).

<http://yunus.hacettepe.edu.tr/~hgamze11/web06/> (Son Er. T.: 30.05.2019).

<http://yunus.hacettepe.edu.tr/~ceren.bayindir11/webfinal/modelleri.html>
(Son Er. T.: 30.05.2019).

<https://jurix.com.tr/article/10935> (Son Er. T.: 30.05.2019).

DERS NOTLARI

ÖZEKES, Serhat. Sayısal Delil İle İlgili Temel Kavramlar (2017) (Power Point Sunumu). Alıntı:<https://stix.uskudar.edu.tr/login> (Son Erişim Tarihi: 30.05.2019)

ÖZEKES, Serhat. Bilgisayar Ağları ve Adli Bilişim (2017) (Power Point Sunumu). Alıntı:<https://stix.uskudar.edu.tr/login> (Son Erişim Tarihi: 30.05.2019)

ÖZEKES, Serhat. Elektronik Deliller ve Yapısal Özellikleri (2017) (Power Point Sunumu).

Alıntı:<https://stix.uskudar.edu.tr/login> (Son Erişim Tarihi: 30.05.2019)

ÖZEKES, Serhat. Bilgisayar Medyalarına İlk Müdahale (2017) (Power Point Sunumu). Alıntı:<https://stix.uskudar.edu.tr/login> (Son Erişim Tarihi: 30.05.2019)

ÖZEKES, Serhat. Adli Bilişimde Kullanılan Ekipmanlar (2017) (Power Point Sunumu). Alıntı:<https://stix.uskudar.edu.tr/login> (Son Erişim Tarihi: 30.05.2019)

ÖZEKES, Serhat. Elektronik Verilerin Delillendirilmesi (2017) (Power Point Sunumu).

Alıntı:<https://stix.uskudar.edu.tr/login> (Son Eriřim Tarihi: 30.05.2019)

ÖZEKES, Serhat. Adli Biliřim (2017) (Power Point Sunumu). Alıntı:<https://stix.uskudar.edu.tr/login> (Son Eriřim Tarihi: 30.05.2019)

ÖZEKES, Serhat. Dijital Deliller (2017) (Power Point Sunumu). Alıntı:<https://stix.uskudar.edu.tr/login> (Son Eriřim Tarihi: 30.05.2019)



ÖZGEÇMİŞ

Kişisel Bilgiler:

Doğum Tarihi	10.08.1978
Doğum Yeri	KASIMPAŞA/İSTANBUL
Medeni Hali	evli
Ehliyet	B sınıfı
Vatandaşlık	Türk vatandaşlığı, İsviçre vatandaşlığı

Eğitim durumu:

1992-1997	Schulhaus Luberzen
1997-2001	Kantonsschule Riesbach Kantonale Maturitaetsschule
2004-2010	Zürich Üniversitesi Hukuk Fakültesi
2012-2016	İstanbul Ticaret Üniversitesi/Hukuk Fakültesi
2016	Üsküdar Üniversitesi/ Adli Bilimler Enstitüsü/Olay Yeri İnceleme ve Kriminalistik Yüksek Lisans

Yabancı Dil (ler) ve Düzeyi

Almanca	anadil seviyesinde
İsviçre Almancası	anadil seviyesinde
İngilizce	çok iyi
Fransızca	çok iyi
İtalyanca	orta seviye

İş Deneyimi

2002-2004	Zürich Kantonu tarafından desteklenen Kick-Off projesinde başarılı yabancı öğrenci sıfatıyla devlet okullarında seminer faaliyeti
2004-2010	İngilizce, Almanca, Fransızca dillerinde özel dersler
2016-2017	World Law Hukuk Bürosu Staj
2017-2018	Ali Yüksel & Hilmi Özalp Hukuk Bürosu Staj

Bilimsel Yayınlar ve Çalışmalar

2002-2004	Zürich kantonu destekli Kick-Off Çalıştayları
2003	Seminer; İsviçre Anayasa Mahkemesi'nde Uygulamalı Dava Seminer; Akıl Hastalarının Cezalandırılma Usulleri, Zürich Hapishanesi
2017	Kadın Adli Bilimciler Konferansı, Adli Arama
2017	Şiddet Sempozyumu, Çocuğa Şiddet