T.C.

GEBZE TEKNİK ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

TÜRKİYE'DE ADLİ BİLİŞİMİN GELİŞİMİ VE DİJİTAL DELİL İNCELEMELERİ

Sercan DÜDEN

YÜKSEK LİSANS TEZİ

STRATEJİ BİLİMİ ANABİLİM DALI

GEBZE

2019

T.C.

GEBZE TEKNİK ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

TÜRKİYE'DE ADLİ BİLİŞİMİN GELİŞİMİ VE DİJİTAL DELİL İNCELEMELERİ

Sercan DÜDEN

YÜKSEK LİSANS TEZİ

STRATEJİ BİLİMİ ANABİLİM DALI

Tez Danışmanı

Prof.Dr. Ali Ekber AKGÜN

GEBZE

2019

GEBZE TEKNİK ÜNİVERSİTESİ	YÜKSEK LİSANS JÜRİ ONAY FORMU

GTÜ Sosyal Bilimler Enstitüsü Yönetim Kurulu'nun 24/06/2019 tarih ve 2019/17 sayılı kararıyla oluşturulan jüri tarafından 11/07/2019 tarihinde tez savunma sınavı yapılan Sercan DÜDEN'in tez çalışması Strateji Bilimi Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRİ

ÜYE (TEZ DANIŞMANI)	: PROF.DR.ALİ EKBER AKGÜN
ÜYE	: DOÇ.DR.KURTULUŞ DEMİRKOL
ÜYE	: DR.ÖĞRETİM ÜYESİ VOLKAN POLAT

ONAY

Gebze Teknik Üniversitesi Sosyal Bilimleri Enstitüsü Yönetim Kurulu'nun

...../...../..... tarih ve ...../..... sayılı kararı.

ÖZET

Bu tez çalışmasında adaletin gerçekleşmesine hizmet eden ve teknolojinin gelişmesiyle önemi her geçen gün artan adli bilişim bilim dalının nitel araştırma yöntemleri kullanılarak genel kabul görmüş prosedür ve tekniklerinin ortaya konulması amaçlanmıştır.

Çalışma esnasında hukuksal çerçeve ve tarihsel gelişim süreci incelenmiş, konu hakkında uzmanlaşmış güvenlik güçleri personeli, adli personel ve adli bilişim hizmeti sağlayan firmalar ile bilgi alışverişi yapılmıştır. Uluslararası alanda konu ile ilgili gelişmeler araştırılarak elde edilen bilgiler ülkemizdeki uygulamalar ile karşılaştırılmıştır. Ayrıca adli bilişim ve dijital deliller hakkında önceden yazılan tez konularına Yüksek Öğretim Kurumu vasıtasıyla erişilerek eksik konular belirlenmiş ve özellikle bu eksikliklerin çalışma kapsamında giderilmesine gayret edilmiştir.

Sonuç olarak, adli bilişim ve dijital delil inceleme konularında Türkiye'de ve Dünya'da tam bir standardın oluşturulamadığı, yeterli uzman personelin bulunmadığı ve adaletin yerine getirilebilmesi için teknolojinin yoğun kullanıldığı günümüzde uzman personel ve bu personelin bilgi seviyesinin artırılmasının oldukça önem arz ettiği sonucuna varılmıştır.

Anahtar Kelimeler: Adli Bilişim, Dijital Delil, Bilişim Sistemleri, Bilişim Suçları

SUMMARY

This thesis study aims to reveal the generally accepted procedures and techniques using qualitative research methods for the scientific branch of computer forensics, which serves the realization of justice and whose importance is growing each day with the development of technology.

During the study, the legal framework and historical process of development were examined, and information exchange was performed with security force personnel, judicial personnel, and companies that provide judicial forensic services regarding the issue. Information obtained through research on developments related to the area in the international field were compared with the practices in our country. Incomplete subjects were specified by accessing previously written thesis topics regarding computer forensics and digital evidence through the Higher Education Council, and efforts were shown to resolve these deficiencies in the scope of the study.

As a result, it was concluded that a complete standard has not been created in Turkey and around the World on the topics of computer forensics and the examination of digital evidence, that there are not adequate expert personnel, that technology is used intensely for the fulfillment of justice, and that it is quite important to increase the level of knowledge of expert personnel today.

Keywords: Computer Forensics, Electronic Evidence, Information Systems, Cyber Crimes

TEŞEKKÜR

Çalışmamın her aşamasında önerileri ile beni yönlendiren, bilgi ve tecrübelerini benimle paylaşan değerli danışmanım Sayın Prof. Dr. Ali Ekber AKGÜN'e en içten teşekkürlerimi ve saygılarımı sunarım.

Çalışmam sırasında kişisel görüşmelerde bulunduğum ve ihtiyaç duyduğum bazı kaynakları bana sağlayan, konusunda uzman hâkimler, savcılar, baro mensupları ve emniyet teşkilatı mensuplarına çalışmama yapmış oldukları katkılardan dolayı teşekkür etmeyi bir borç bilirim.

Ayrıca hayatım boyunca beni hep destekleyen, yanımda olan ve başarılı olacağım konusunda beni yüreklendiren ailem ve dostlarıma sonsuz teşekkürlerimi sunuyorum.

İÇİNDEKİLER

KISALTMALAR DİZİNİ

Kısaltmalar	Açıklamalar
ABD	:Amerika Birleşik Devletleri
ACPO	:Association of Chief Police Officers
BGYS	:Bilgi Güvenliği Yönetim Sistemi
BSI	:İngiliz Standart Enstitüsü
CD	:Taşınabilir Disk
CFTT	:Computer Forensic Tool Testing
CMK	:Ceza Muhakemesi Kanunu
DCO	:Device Configuration Overlay
DVD	:Çok Amaçlı Sayısal Disk
EİK	:Elektronik İmza Kanunu
FBI	:Federal Soruşturma Bürosu
FSEK	:Fikir Ve Sanat Eserleri Kanunu
GPS	:Küresel Konumlama Sistemi
HPA	:Host-Hidden Protected Area
IEC	:Uluslararası Elektronik Komisyonu
IP	:İnternet Protokol
IOCE	:Uluslararası Sayısal Delil Organizasyonu
ISO	:Uluslararası Standart Organizasyonu
LAN	:Yerel Alan Ağı
MD5	:Message Digest 5
NIST	:National Institute of Standarts and Technology
NSF	:Amerika Birleşik Devletleri Ulusal Bilim Vakfı
ODTÜ	:Orta Doğu Teknik Üniversitesi
OECD	:Ekonomik Kalkınma ve İşbirliği Örgütü
PDA	:Kişisel Dijital Yardımcı
PVSK	:Polis Vazife ve Salahiyetleri Kanunu
SHA	:Secure Hash Algorithm
SWGDE	:Dijital Deliller Bilimsel Çalışma Grubu
TCK	:Türk Ceza Kanunu
TSE	:Türk Standartları Enstitüsü
TV	:Televizyon
WAN	:Geniş Alan Ağı

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

1. GİRİŞ

Teknolojilerinin gelişmesi iletişimi hızlandırmış ve insan hayatında önemli değişikliklere sebep olmuştur. Bilişim sistemleri aracılığıyla bilginin iletilmesi, işlenmesi ve saklanması ile insanların klasikleşmiş eğitim, kültür, ticaret ve benzeri anlayışları, tamamen farklı bir boyut kazanmıştır. Bu değişimin bu denli hızlı gerçekleşmesinin sebebi bilginin günümüzde daha kolay ulaşılır olması ile açıklanabilmektedir (Boğa, 2011).

Bugün dünya çapında günlük yaklaşık 294 milyar e-posta mesajının gönderildiği değerlendirilmektedir. İnternet üzerindeki video sunucularına her gün 864.000 saatlik video yüklenmekte, Netflix kullanıcıları 22 milyon saat TV seyretmektedirler. 2019 yılı verilerine göre dünya nüfusunun yaklaşık %57'sinin internet bağlantısı bulunmakta olup, %45'sinin sosyal ağlara aktif üyelikleri bulunmaktadır. Dünya nüfusunun %67'si akıllı cep telefonunu kullanmakta ve bu kullanıcıların %55'i cep telefonu üzerinden alışveriş yapmaktadırlar (Hekim & Başıbüyük, 2013).

İnsanlık tarihine farklı bir yön veren bu değişim, yeni suç türlerinin ortaya çıkmasına neden olmuş ayrıca suç işleme yöntemlerinde değişikliğe yol açmıştır. Bu değişimin insanlara sunduğu imkânlarından suçlular da faydalanmakta ve teknolojinin sağladığı kolaylıkları kullanmaktadırlar. Artık bir suçlu için mağdur ile aynı ortamda olmadan suç işleyebilmek mümkün hale gelmiştir. Bununla birlikte teknolojinin gelişmesi, organize suç ve terör örgütlerinin iletişim olanaklarını artırmış, propaganda imkânlarını arttırmış ve yeni faaliyet alanlarının ortaya çıkmasını sağlamıştır (Polat, 2014).

Günümüzde hakaret, müstehcenlik, rüşvet, dolandırıcılık, kumar oynatmak, uyuşturucu madde kaçakçılığı, terör suçları propagandası gibi birçok suç, bilişim sistemleri yolu ile kolaylıkla işlenebilmektedir. Teknolojinin bu hızlı gelişmesi ile hayatımızın vazgeçilmez parçası haline gelen bilgisayar, cep telefonu, hafıza kartları, CD, DVD gibi bilişim sistemleri aynı zamanda birçok suçun işlenmesinde araç haline gelmiştir (Henkoğlu, 2011).

Klasik suç türlerinin bilişim sistemleri kullanarak işlenmesinin yanı sıra, bizzat bilişim sistemleri kullanarak işlenen yeni suç türleri de ortaya çıkmıştır. Bu suç

türlerinin ve bilişim sistemleri ile işlenen diğer klasik suç türlerinin soruşturma ve kovuşturma evrelerinde eski yöntemlerin kullanılması bir takım sorunları ortaya çıkarmıştır.

Klasik adli soruşturma yöntemlerinin suç ve suçlunun tespitinde yetersiz kalması ile yeni yöntemlere ihtiyaç duyulmuş ve bu ihtiyaçlara karşılık adli bilişim bilim dalı ortaya çıkmıştır.

Bu çalışmadaki amaç Türkiye'de adli bilişimin gelişimi ve dijital delil incelemelerinin nitel araştırma yöntemleri kullanılarak araştırılmasıdır. Çalışma sırasında konuyla ilgili olan kitap, makale, konferans, kongre notları, eğitim dokümanları, ulusal ve uluslararası haberler, dergiler ve daha önce hazırlanmış tezler incelenmiştir.

Adli Bilişim kavramının çok boyutlu olması nedeniyle çalışma yalnızca adli bilişim ile sınırlı kalmamıştır. İkinci bölümün birinci kısmında bilişim sistemleri tanımlanmış, bilişim ve hukuk arasındaki ilişki irdelenmiştir. İkinci kısmında bilişim suçları tanımlanarak, bu yeni suç türünün sınıflandırılması yapılmaya çalışılmıştır. Üçüncü kısmında bilişim suçları ile mücadele yöntemleri üzerinde durulmuş, en iyi mücadele yönteminin suç oluşmadan önlenmesi olduğu anlatılmıştır.

Üçüncü bölümde adli bilişim ve dijital delil kavramları derinlemesine ele alınarak, inceleme ve analiz yöntemlerinden bahsedilmiştir. Bununla birlikte birçok ülkenin adli bilişim uygulamaları incelenmiş, Türkiye'deki uygulamalarla farklılıkları ortaya koyulmuştur.

Sonuç ve yorumlar kısmında ise, Türkiye'de adli bilişimin geldiği nokta ile dijital delil kavramının teknik boyutu ve hukuki dayanakları ele alınmıştır. Teknolojinin gelişmesi ile Kıta Avrupası ve ABD'de ortaya çıkan yeni delil inceleme ve analiz yöntemlerinin ülkemizde uygulanabilirliği değerlendirilmiştir.

2. BİLİŞİM SİSTEMLERİ KAVRAMI VE BİLİŞİM SUÇLARI

2.1 Bilişim Sistemleri Kavramı

2.1.1 Bilişim Sistemleri Kavramı, Tanımı ve Önemi

Sistem, ortak bir amaç için birlikte çalışan birbirine bağımlı ve birlikte hareket etme yeteneğine sahip parçaların oluşturduğu bir bütündür (Özkul, 2002). Bilişim ise Türk Dil Kurumu'nun genel sözlüğünde "İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik" (Türk Dil Kurumu, 2016) olarak tanımlanmıştır. Buna göre bilişim sistemi, yöneticilerin karar vermek için ihtiyaç duyduğu bilgiyi değişik kaynaklardan toplayıp, bu bilgiyi işleyen, saklayan ve raporlayan bir bilgi sistemi olarak tanımlanır (Akolaş, 2004).

Bilişim sistemleri ile kastedilen ise; bilginin toplanması, saklanması, işlenmesi, erişilmesi ve dağılmasına hizmet eden tüm teknolojiler (bilgisayar sistemleri, veri depolama araçları, ağ ve iletişim araçları, bilgi bankaları, bilgi erişim hizmetleri, yazılım ve geliştirme araçları) ve sistem içerisinde dönen bilgilerin tümüdür. (Sarıhan, 1998) Bilgisayar ve bilişim sistemi öğretide ve uygulamada bazen aynı anlamda kullanılsa da, bilişim sistemi daha geniş kapsamlı olup bilgisayarı da kapsamaktadır (Eralp, 2011).

Bilişim sistemlerinin çıktısı bilgidir. Günümüzde kişisel ve örgütsel hedeflere ulaşmanın en önemli unsurun bilgi olması göz önüne alındığında, bilişim sistemleri stratejik önem kazanmıştır. Artık ülkeler, askeri güç, sayısal çoğunluk ya da ekonomik büyüklükleri ile değil, bilgi ve bilgiye ulaşmadaki teknolojik gelişmişlikleri dünya sıralamasında yerlerini almaktadırlar (Akolaş, 2004).

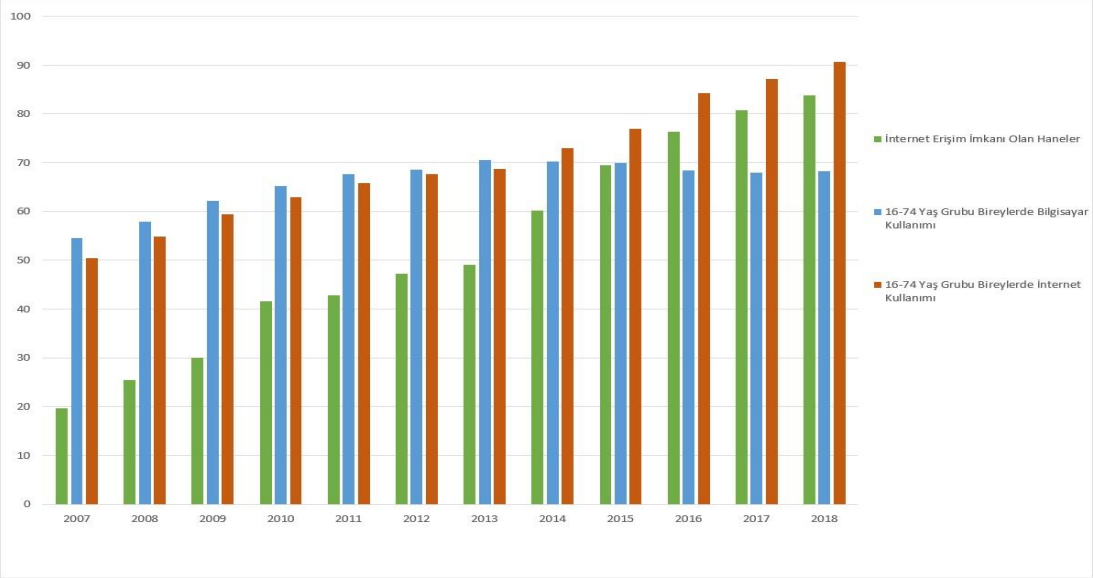
2.1.2 Bilişim Sistemlerinin Günümüzdeki Konumu

Bilişim teknolojilerinin hızla gelişmesi ve bu teknolojilerin giderek insanların günlük yaşamında etkinlik kazanması ile birlikte kamu ve özel sektörün eski düzen kayıt sistemlerini bırakarak, kayıt, işlem ve çıktılarını sanal ortamda düzenlemeleri bilişim sistemlerinin günlük hayatın vazgeçilmez bir parçası olduğunun göstergesidir.

Bilişim sistemleri ve internet sayesinde sesli ve görüntülü haberleşme, sanal ortamda ticari ilişkiler, internet bankacılığı ve cep telefonu gibi birçok teknoloji hayatımıza girmiştir. Özellikle teknoloji devriminin haberleşmede yarattığı olağanüstü gelişme, dünyayı "Küresel Köy" olarak tanımlayacak kadar küçültmüştür (McLuhan, 1962).

Çağımızın en önemli araçlarından birisi haline gelmiş bulunan internet ağının temelleri 1980'in sonlarında atılmış, 1990'ın başlarında kamuoyuna açılmış ve grafik tabanlı internet tarayıcı kullanıma sunulmuştur (Orta, 2015).

Türkiye, internet bağlantısı ile 1993 yılında ODTÜ ile ABD NSF arasında gerçekleştirilen bağlantı ile tanışmıştır (ODTÜ Bilgi İşlem Daire Başkanlığı, 2005). Günümüzde internet kullanımı önemli oranda artmış durumdadır. 2018 yılı verilerine göre Türkiye genelinde evlerin %83,8 internet erişim imkanına sahiptir. 2007 yılı TUİK verilerine göre 16-74 yaş grubundaki bireylerde sırasıyla %54,6 ve %50,4 olan bilgisayar ve internet kullanım oranları 2018 Ekim ayında %68,2 ve %90,7 seviyelerine ulaşmıştır. 2007 yılında hanelerin %87,4'ünde cep telefonu veya akıllı telefon bulunurken, 2018 Ekim ayında bu oran %98,7 olmuştur (TUİK, 2018).



Şekil 2.1.2.1: Temel Göstergeler 2007-2018 (TUİK)

Tablo 2.1.2.1: "Bireylerin Yaş Grubuna Göre Bilgisayar ve İnternet Kullanım Oranları" (TUİK)

Son üç ay içinde bireylerin yaş grubuna ve cinsiyetine göre bilgisayar ve İnternet kullanım oranları, 2007-2018
Individuals using the computer and Internet in the last 3 months by age groups and sex, 2007-2018

(%)

		Yaş grubu - Age group																	
		16 - 24			25 - 34			35 - 44			45 - 54			55 - 64			65 - 74		
	Yıl Year	Toplam Total	Erkek Male	Kadın Female	Toplam Total	Erkek Male	Kadın Female	Toplam Total	Erkek Male	Kadın Female	Toplam Total	Erkek Male	Kadın Female	Toplam Total	Erkek Male	Kadın Female	Toplam Total	Erkek Male	Kadın Female
Bilgisayar Computer	2007	**54,6**	67,3	40,7	**35,1**	44,7	25,5	**26,8**	36,6	17,1	**17,1**	26,8	7,5	**6,0**	9,6	2,0	**1,5**	2,2	0,6
	2008	**57,9**	69,6	47,0	**43,3**	54,8	31,8	**31,6**	41,6	21,5	**20,4**	28,3	12,5	**7,4**	12,6	2,5	**1,8**	3,0	0,9
	2009	**62,2**	76,4	49,1	**46,6**	58,6	34,5	**31,8**	42,1	21,3	**20,2**	28,9	11,6	**6,7**	10,6	3,1	**2,2**	3,2	1,4
	2010	**65,2**	78,5	52,7	**52,0**	62,4	41,6	**36,9**	46,9	26,9	**23,2**	33,6	12,7	**8,3**	13,5	3,4	**2,7**	4,1	1,6
	2011	**67,7**	77,9	58,3	**57,1**	67,5	46,7	**41,7**	52,6	30,6	**24,1**	34,3	13,9	**11,2**	17,2	5,4	**3,0**	5,0	1,4
	2012	**68,5**	81,1	56,4	**59,1**	70,0	48,1	**43,6**	54,3	32,7	**26,7**	36,3	17,0	**12,5**	19,1	6,1	**3,8**	6,9	1,3
	2013	**70,6**	82,0	59,5	**59,6**	70,0	49,1	**47,0**	58,2	35,6	**26,1**	36,2	15,9	**11,9**	18,2	5,8	**4,4**	7,8	1,7
	2014	**70,3**	79,6	61,0	**63,3**	71,3	55,3	**51,0**	61,9	40,0	**30,6**	40,5	20,6	**15,4**	21,9	9,1	**5,0**	8,8	1,8
	2015	**70,0**	78,5	61,4	**62,7**	70,8	54,5	**50,0**	60,7	39,1	**32,0**	41,2	22,8	**15,8**	21,7	9,9	**5,3**	8,2	2,8
	2016	**68,4**	77,0	59,9	**59,3**	67,7	50,8	**48,6**	59,4	37,8	**31,2**	39,7	22,7	**16,1**	22,2	10,1	**6,5**	9,2	4,3
	2017	**68,0**	76,1	59,7	**59,0**	67,9	49,9	**48,0**	57,3	38,7	**31,9**	41,1	22,6	**16,4**	22,9	10,0	**7,5**	11,4	4,2
	2018	**68,2**	75,1	61,0	**61,7**	69,8	53,6	**48,1**	57,4	38,8	**32,6**	42,0	23,2	**19,7**	26,5	13,1	**8,5**	11,5	5,9
İnternet Internet	2007	**50,4**	63,5	36,2	**32,3**	41,5	23,1	**23,8**	33,2	14,4	**14,8**	23,2	6,5	**4,8**	7,5	1,8	**1,4**	2,1	0,6
	2008	**54,8**	67,1	43,4	**41,4**	52,3	30,4	**29,3**	37,7	20,8	**19,4**	27,1	11,6	**6,9**	11,9	2,2	**1,6**	2,5	0,9
	2009	**59,4**	74,1	46,0	**45,1**	57,2	32,9	**30,2**	40,3	19,9	**18,6**	26,7	10,5	**6,2**	9,5	3,1	**2,0**	3,1	1,2
	2010	**62,9**	76,6	49,9	**50,6**	60,9	40,2	**34,7**	43,5	25,7	**22,4**	31,9	12,9	**7,8**	12,6	3,2	**2,7**	4,2	1,6
	2011	**65,8**	76,5	55,9	**55,1**	65,4	44,9	**39,7**	50,4	28,9	**22,7**	32,1	13,2	**10,4**	16,0	5,0	**2,7**	4,5	1,2
	2012	**67,7**	80,6	55,4	**58,5**	69,6	47,2	**42,6**	53,3	31,8	**25,5**	34,8	16,2	**11,9**	18,5	5,6	**3,6**	6,4	1,3
	2013	**68,7**	80,1	57,5	**58,8**	69,1	48,4	**45,6**	56,7	34,4	**24,9**	34,7	15,1	**11,1**	16,8	5,7	**4,2**	7,5	1,5
	2014	**73,0**	82,8	63,2	**67,1**	76,8	57,4	**52,0**	63,7	40,2	**30,4**	40,7	20,0	**15,3**	21,5	9,3	**5,0**	8,8	1,8
	2015	**77,0**	85,1	68,9	**71,7**	81,3	62,0	**55,4**	69,0	41,7	**34,0**	43,7	24,2	**17,2**	22,9	11,6	**5,6**	8,8	2,8
	2016	**84,3**	92,0	76,5	**78,8**	86,7	70,7	**65,4**	77,2	53,5	**41,3**	51,8	30,6	**21,0**	28,9	13,3	**8,8**	12,5	5,8
	2017	**87,2**	91,5	82,9	**85,7**	92,6	78,7	**73,9**	84,0	63,8	**51,7**	62,5	40,9	**27,2**	34,9	19,8	**11,3**	15,6	7,5
	2018	**90,7**	94,7	86,5	**90,1**	94,5	85,6	**80,7**	88,3	73,0	**61,5**	71,8	51,1	**39,2**	47,8	30,8	**17,0**	23,0	11,9

TÜİK, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması, 2007-2018
TurkStat, Survey on Information and Communication Technology (ICT) Usage Survey in Households and by Individuals, 2007-2018
Tablo başlığında bulunan son üç ay ifadesi Ocak-Mart aylarını ifade etmektedir.
In the last three months expression in the table heading refer to the months between January-March
Tablo başlığında bulunan bireyler ifadesi 16-74 yaş grubundaki bireyleri ifade etmektedir.
The individuals expression in the table heading refers to the individuals in the 16-74 age group.

2.1.3 Bilişim Sistemlerinin Sağladığı Yararlar

Günümüzde bilişim sistemleri, örgütsel organizasyon yapılarının ve bireylerin işlerinin yeniden dizaynında çarpıcı bir etkiye sahiptir. Gelişen teknoloji ile bilişim sistemlerine belirli bir sınır çizilememekte, askeri, ticari ve finansal kuruluşlar ile üniversiteler, bilişim teknolojilerini kullanarak hayatımızı kolaylaştırmaktadır (Yaycı, 2007).

Bilişim sistemleri sayesinde bilginin yayılımı hızlanmıştır. Donanım ve yazılımdaki gelişmeler ve bilgisayar ağlarının birbirine bağlanması bu hızı daha çok artırmıştır. Günümüzde kıtalar arası bilgi alışverişi saniyeler içerisinde yapılmaktadır.

Bilişim teknolojileri toplumsal yapıya da etki etmektedir. Gelişen yeni teknolojiler toplumsal yapıyı hızla sanayi toplumundan bilgi toplumuna taşımaktadır. 1950 ve 1960'lı yıllarda Amerika Birleşik Devletleri, Japonya, Batı Avrupa ülkeleri gibi gelişmiş ülkeler bilgi teknolojileri kullanımını artırarak, sanayi toplumundan bilgi toplumuna ilk geçiş yapan ülkeler olmuşlardır. Bilgi toplumunun en önemli özelliği, bilgi teknolojilerinin; tarım, sanayi ve hizmet sektörlerinin yanı sıra eğitim, sağlık, iletişim gibi her alanda kullanılmasıdır. Bilgi toplumlarındaki bu

gelişmeler, diğer ülkeleri kısa zamanda etkisi altına almış, ülkeler bu konuda politikalar geliştirmiştir. Ayrıca ülkeler arasında ekonomik, siyasal, sosyal ve kültürel alanlarda uluslararası bir bütünleşme sağlamıştır (Aktan, 1998).

Ekonomik modernleşme ile bilişim sistemlerinin sağladığı faydalar arasında da sıkı bir ilişki vardır. Bilgiye hızlı bir şekilde erişmek ulusal ve uluslararası pazarlarda "rekabet edebilirliğin" ilk koşulu haline gelmiş, enformasyona ve bilgiye dayalı yeni ekonomik pazarlar ortaya çıkmıştır. Bu sebeple bilginin ekonomik piyasalarda daha etkin kullanılması, sanayi toplumuna geçişte elektriğin keşfedilmesinin yarattığı etkiyle karşılaştırılacak kadar önemli bulunmaktadır (Tonta, 1999).

2.1.4 Bilişim ve Hukuk

Bilişim teknolojileri, sunduğu imkân ve kabiliyetler ile yaşamın her alanına nüfus ettiği gibi sağlık, eğitim, güvenlik, iletişim ve bankacılık gibi birçok sosyal alanın da omurgasını oluşturmaktadır. Bu açıdan bakıldığında bilişim sistemleri teknik bir kavram olmaktan çıkmış sosyal bir kimliğe bürünmüştür.

Bir sosyal kimlikten bahsedildiğinde öne çıkan iki unsur vardır; haklar ve sorumluluklar. İşte bu aşamada hukuk devreye girmektedir. Fakat "toplumu düzenleyen ve devletin yaptırım gücünü belirleyen yasaların bütünü" (Türk Dil Kurumu, 2012) olarak tanımlanan hukukun, bilişim gibi yeni, henüz sınırları çizilemeyen ve devamlı değişim gösteren bir alana uyum sağlayabilmesinin zor olduğu aşikârdır.

Bilişim teknolojilerinin günden güne öneminin artması, buna rağmen denetimin zorlaşması ve karmaşanın büyümesi insanları birçok sıkıntı ile karşı karşıya getirmektedir. Özellikle iletişim kanallarına yetkisiz erişim(telefon dinlemeleri vb.), kişisel verilerin güvenliği ve korunması gibi konular insanların gündelik hayatta karşılaştığı başlıca sıkıntılardır. Bugün hukuk dünyası, bilişim alanında, bilişim suçlarının tanımlanması, sınıflandırılması, sanal toplum yaşamını düzenleme, sosyal ihtiyaçları karşılama ve adalet kavramlarını tüm boyutlarıyla tartışmaktadır. Fakat siber âlem olarak tanımlanan bilişim dünyası üzerine yapılan çalışmalar değişim hızına yetişememekte, hızlı bir şekilde güncelliğini yitirmekte ve yetersiz kalmaktadır (Öztürk, 2007).

Türkiye'de bu konudaki hukuksal boyutta ilk çalışma; Adalet Bakanlığı'nın tarafından oluşturulan komisyonun hazırladığı "Türk Ceza Kanunu Ön Tasarısı" içerisinde yer almaktadır. Bilişim suçları ile ilgili hükümler, "Türk Ceza Kanunu Ön Tasarısı" özel hükümler başlığı olarak tanımlanan ikinci kitabın "Topluma Karşı Suçlar" başlığı altında ikinci kısmında "Bilişim Alanında Suçlar" başlığı dokuzuncu bölüm altında yer alan 342 ile 346'ncı maddeleri arasında düzenlenmiştir. Daha sonra 1991 yılında 3756 sayılı kanunun 20'nci maddesi ile 765 sayılı TCK'da yapılan değişiklikle 525'nci maddesinde "Bilişim Alanında Suçlar" başlığı altında 11'nci bab eklenmiştir. (Eralp, 2011) Ayrıca yine 3756 sayılı kanun ile Türk Ceza Kanununa yeni maddeler eklenmiş, "Bilgileri otomatik işleme tabi tutmuş bir sistem" ile işlenen suçların cezaları tanımlanmıştır.

Bunun yanında kanun koyucu, bilişim sektöründeki gelişmelere paralel olarak 1995 yılında ve 4110 sayılı kanun ile 5846 sayılı FSEK'da değişiklik yapmış ve böylelikle bilişim programları ve bunları oluşturan verileri kanun kapsamına dahil etmiştir. Neticede bir eser olan bilişim yazılımları üzerindeki tüm hakların kasten ihlali durumunda failin cezalandırılmasını öngörmüştür (Yenidüya & Değirmenci, 2003).

Elektronik İmza Kanunu 2004 yılında kabulü ile Türkiye'de hukuksal olarak "Elektronik İmza" geçerliliği kabul edilmiş ve bu yasa ile elektronik imzanın nasıl oluşturulacağı ve geçerliliği ile ilgili düzenlemeler yapılmıştır. Bu kanun ile sahte elektronik imza kullanılması ve sahte elektronik sertifika yapılması ve kullanılması, suç olarak nitelendirilmiştir.

2004 yılında kabul edilen 5237 Sayılı Türk Ceza Kanunu kabul edilmiştir. Bu kanun ile bilişim suçları ile ilgili, "Bilişim Alanında Suçlar" başlığını altında düzenlemeler yapılmıştır. 5237 Sayılı yeni Türk Ceza Kanunu ile kanun koyucu, bilişim alanında suçları bir bölüm altında düzenlemekle kalmamış, diğer başlık altındaki klasik suçlar ile ilgili de bilişim sistemleri ile işlenmesi halinde yeni düzenlemeler yapmıştır. Bu düzenlemeler;

- "Madde 135: Kişisel Verilerin Kaydedilmesi Suçu"
- "Madde 136: Kişisel Verileri Hukuka Aykırı Olarak Verme ve Ele Geçirme Suçu"

- “Madde 138: Verileri Yok Etme Suçu”
- “Madde 163: Karşılıksız Yararlanma Suçu”

Bazı suçlarda ise suçun bilişim sistemleri kullanılmak suretiyle işlenmesi, ağırlaştırıcı sebep sayılmıştır.

- “Madde 142: Hırsızlık”
- “Madde 158: Dolandırıcılık”

Yeni ceza kanunumuzun bilişim suçlarıyla ilgili düzenlemelerinde karşılaşılan en büyük sorun “bilişim sistemi” kavramının açıklanmamasıdır. Eski TCK’da adı geçen “bilgileri otomatik olarak işleme tabi tutan” (Resmi Gazete, 1991) ibaresi çıkarılarak, “verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemlerdir.” (T.C. Adalet Bakanlığı, 2004) şeklinde yoruma açık bir tanımlama yapılmıştır. Bu şekliyle, adli makamlarda bilişim sistemleri tanımı ile ilgili kavram karmaşası yaşanmakta ve bu tip teknolojik sistemlerin dar olarak yorumlaması durumunda uygulamada sorun çıkabilmektedir (Şener, 2012).

2.2 Bilişim Suçlarının Tanımlanması ve Sınıflandırılması

2.2.1 Bilişim Suçlarının Tanımı

Bilişim suçları ile ilgili değişimin çok hızlı olması nedeniyle, kanun koyucu ve hukukçular tarafından herkesin üzerinde anlaştığı bir tanımlama yapılamamıştır., Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu’nun 1983 yılında Paris Toplantısı’nda yaptığı tanımlama en geniş kabul gören tanımlama olarak karşımıza çıkmaktadır. Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu’na göre bilişim suçları; “bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış” olarak tanımlanmaktadır (Boğa, 2011).

Doktrinde farklı tanımlamalar da bulunmaktadır. Örneğin “bilişim suçlarını, bilgisayarın kötüye kullanılması, bilgileri otomatik işleme tabi tutulmuş ve verilerin nakline ilişkin kanuna ve meslek ahlakına aykırı davranışlar” olarak tanımlayan Dönmezer, tanımını kanun ve meslek ahlakına dayandırarak yapmaktadır (Dönmezer, 1989). Başka bir tanım ise, Parker tarafından yapılmıştır. Parker bilişim

suçlarını, “işlendiği takdirde faile çıkar sağlayacak bir şeyler kazandıran ya da kurbana kaybettiren, aynı zamanda bilgisayar kullanımı veya teknolojisi bilgisi içeren herhangi kasıtlı bir davranış” olarak tanımlamıştır (Şen, 2003).

1970’lı yılların başlarına kadar bilinmeyen bir olgu olan bilişim suçları, bilişim teknolojisinin yayılmasıyla hızlı artış göstermiştir. Savcılık tarafından adli takibi yapılan ilk suç 1966 yılında ABD’nin Minneapolis şehrinde bir bilgisayar uzmanının banka hesaplarında bilgisayar marifetiyle tahrifat yapması ile işlenmiştir (Boğa, 2011).

Bilişim suçu, bir bilgisayar ile işlenebileceği gibi daha karmaşık sistemler, yerel veya küresel ağlar üzerinden de işlenebilmektedir. Burada dikkat edilmesi gereken nokta, bilişim suçlarının kapsamının sadece bilgisayar olmadığı, bilgisayar teknolojileriyle beraber, iletişim teknolojilerinin de bu kapsama girdiğidir.

Ortaya çıkan diğer bir sorun ise, gelişmekte olan teknoloji ile birlikte bilişim suçlarında da değişiklikler olmasıdır. Yapılan tanımların farkında da anlaşılabileceği gibi bilişim suçlarının bir sınırı bulunmamaktadır. Bilişim suçlarını bir sınır çizilememesi nedeniyle “bilgisayar suçları”, “internet suçları”, “siber suç”, “ileri teknoloji suçu”, “dijital suçlar”, “sanal suç” gibi kavramların tek bir tanımının yapılmaması, değişimin hızı ile açıklanabilmektedir.

2.2.2 Bilişim Suçlarının Sınıflandırılması

Bilişim suçları kapsamına giren suçların sınıflandırma ve tanımlamasının yapılması bilişim suçları kavramının daha iyi anlaşılmasını sağlayabilecektir. Bilişim suçları; suçun işlenme amacı, suçu işleyen kişiler veya gruplar ve suçun büyüklüğü gibi farklı faktörlere bağlı olarak sınıflandırılabilir. Genel bir sınıflandırma ile Avrupa Ekonomik Topluluğu bilişim suçlarını beş kategoriye ayırmıştır.

- “Bilgisayarda mevcut olan kaynağa veya herhangi bir değere gayri meşru şekilde ulaşarak transferini sağlamak için kasten bilgisayar verilerine girmek, bunları bozmak, silmek, yok etmek,”
- “Bir sahtekârlık yapmak için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek,”
- “Bilgisayar sistemlerinin çalışmasını engellemek için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek,”

- “Ticari manada yararlanmak amacı ile bir bilgisayar programının yasal sahibinin haklarını zarara uğratmak,”
- “Bilgisayar sistemi sorumlusunun izni olmaksızın, konulmuş olan emniyet tedbirlerini aşmak sureti ile sisteme kasten girerek müdahalede bulunmak.”

Avrupa Ekonomik Topluluğu tarafından yapılan bu genel sınıflandırma, teknolojinin değişimi ve gelişmesi ile güncelliğini yitirmiş, günümüzde farklı sınıflandırmalar yapılması ihtiyacını doğurmuştur (Özel, 2001).

Birleşmiş Milletlerin ve Avrupa Birliğinin 1999 yılında hazırladığı “Bilişim Suçları Raporu” ile yeni bir sınıflandırma yaparak bilişim suçlarını altı kategoriye ayırmıştır (Özdemir, 2003).

- “Bilgisayar sistemlerine ve servislerine yetkisiz erişim ve dinleme,”
- “Bilgisayar sabotajı,”
- “Bilgisayar yoluyla dolandırıcılık,”
- “Bilgisayar yoluyla sahtecilik,”
- “Kanunla korunmuş bir yazılımın izinsiz kullanımı,”
- “Diğer suçlar (yasadışı yayınlar, pornografik yayınlar ve hakaret suçları)”

Yukarıda belirtilen sınıflandırmalar haricinde sebep-sonuç ilişkisi göz önünde tutarak bilişim suçlarını dört başlık altında toplayabiliriz.

2.2.2.1 Finansal Unsur Oluşturan Suçlar

Bilişim sistemleri, hayatımızı kolaylaştıran faydalarının yanı sıra kişilere ve topluluklara büyük zararlarda verebilmektedir. Finansal zarar bunun en açık ve net görüldüğü unsurdur. İnternet bankacılığı ve e-ticaret gibi hayatımızı kolaylaştıran sistemler, kötü amaçlı kişilerce menfaat elde etmek amacı ile aleyhimize kullanılabilmektedir. Bununla birlikte sanal dolandırıcılık ve sahtecilik, kişisel veya şirket bilgilerinin çalınarak şantaj amaçlı kullanımı, telif hakkı olan ürünlerin ücretsiz paylaşımı gibi finansal zarar verebilecek faaliyetler bilişim sistemleri yoluyla işlenen suçlar olarak sıralanabilmektedir.

2.2.2.2 Kişilik Haklarını İhlal Eden Suçlar

Bu suçlar kimi zaman finansal zarar veren suçlar ile birlikte işlense de genel olarak kişi hakkında bilgi toplama, izni olmaksızın dijital iletişim kanallarının (telefon, e-mail vb.) takip edilmesi şeklindedir. Bu başlık altında işlenen suçlar hem maddi hem de manevi zarar verebilmektedir. "Bilişim sistemlerinde yer alan verinin ele geçirilmesi suçu", "başkasına zarar vermek amacıyla sistemde yer alan verinin kullanılması, nakledilmesi veya çoğaltılması suçu" bu başlık altına giren suçlardır.

2.2.2.3 Siyasi Suçlar

Bilişim yolları ile işlenen siyasi suçlar incelendiğinde "Siber Terörizm" kavramı ön plana çıkmaktadır. "Siber Terörizm" kavramı yazılı ve görsel medyada, ulusal ya da uluslararası literatürde sıklıkla karşımıza çıkmaktadır. "Belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin, bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılması" olarak tanımlanan siber terörizm, bilişim sistemleri kullanılarak yapılan bir propaganda yöntemidir (Akçadağ, 2012).

Terör örgütleri geçmiş yıllarda kitaplarla, dokümanlarla, broşür gazete dergi ve el ilanları ile yaptığı propaganda faaliyetlerini, örgüt üyeleri ile olan iletişimlerini, yandaş kazanma ve eylemlerini başkalarına haklı gösterme çabalarını artık internet siteleri vasıtası daha geniş kapsamlı yapmaktadırlar. Küresel ağ üzerinde faaliyetlerini daha geniş ve hiçbir sınırlama ve sansüre tabi olmaksızın gerçekleştiren terör örgütleri bu küresel ağ vasıtası ile devlete, kanunlara ve düzene karşı gelmekte, hatta kendi lehlerine toplumu yönlendirme faaliyetlerini gerçekleştirmeye çalışmaktadırlar. Küresel ağ aracılığıyla terörist gruplar ve örgütler; faaliyet gösterdikleri terör örgütünün kuruluşu ve gelişimini ve amaçlarını haklı kılan nedenleri hakkında toplumu bilgilendirmeyi amaçlar. Ayrıca terör örgütleri, deep web ve internet siteleri aracılığı ile faaliyetleri hakkında hazırladıkları kitapları, dergileri, gazeteleri yayımlayarak, örgüte yardım toplamakta ve gelir elde etmektedirler. Terör örgütleri yine aldığı kararları ve izleyeceği politikaları bildirmek, taraftar toplamak ve eleman temin etmek, devletin faaliyetlerini kötülemek, karalamak ve hakaret etmek, terör örgütünün eylemlerini yönlendirmek, terör

örgütünün toplumsal hareketlerini organize etmek ve toplum nazarında sempati oluşturmak için de interneti sıklıkla kullanmaktadırlar (Tulum, 2006).

2.2.2.4 Siber Savaş

Teknolojik açıdan her ilerleme, yapıcı olduğu kadar yıkıcı unsurları da içinde barındırır. Bilgi, bilgi toplumunda güçtür, ama bu gücü kimin hangi amaçla kullanacağı bir sorunsal olarak karşımıza çıkmaktadır.

Günümüz yaşantısının bilgisayar ve ilgili sistemlere olan bağımlılığı ve teknolojinin gelişmesiyle toplum refahının teknolojinin bir çıktısı olarak görülmesi, siber savaş tanımını basit bir etimolojik tartışmanın dışına taşımaktadır. Günlük hayatın teknolojiye bu denli bağımlı olması suç örgütleri ve terörist örgütler kadar hasım bir devletin istismarına da müsait geniş bir alan ortaya çıkarmaktadır (Çakmak & Altunok, 2009).

Bu bölümde ele alınan siber savaş kavramı, siber suç ve siber terörizmden temel unsurları dolayısıyla farklılık göstermektedir. Siber savaş kavramı içinde yer alan savaş, ”hükümetlere bağlı ve hükümet oluşturmaya istekli meşru organize gruplar arasındaki büyük ölçekli şiddetli çatışma durumu” olarak tanımlanabilir. (Yalçınkaya, 2008) Her ne kadar bazı devletler siber suç ya da terör eylemlerinin işlenmesini doğrudan veya dolaylı olarak desteklese de, bireyleri ya da grupları bu doğrultuda yönlendirebilmektedirler. Bunun siber savaş ile karıştırılmaması gerekmektedir. Siber savaşın tarafı devlet ya da örgütlenmiş bir otoritedir. Siber savaş, siber terör ve siber suçların aynı sanal yapıyı kullanmaları bir benzerlik olsa da, motivasyonlar ve amaçlarda farklılıklar bulunmaktadır (Çakmak & Altunok, 2009).

Siber savaşta temel amaç; hedef devletin hayati altyapılarını tahrip etmek, ekonomik zarar vermek ve savunmasız hale getirmektir. Bu yüzden öncelikli hedefler; enerji kaynakları, iletişim altyapısı, finansal altyapı, ulaşım altyapısı ve savunma sistemleri olacaktır. Diğer bir önemli hedef ise muhabere sistemlerinin etkisiz hale getirilmesidir. Bu sayede birimler arasındaki irtibat kesilecek ve koordinasyon sağlanamayacaktır.

Sonuç olarak siber savaş, savunma ya da taarruz amaçlı, bilgi ve iletişim sistemlerinin yok edilmesi, zarara uğratılması ya da manipüle edilmesi eylemlerini içerir.

2.3 Bilişim Suçları ile Mücadele Yöntemleri

Bilişim sistemleri teknolojilerinde yaşanan hızlı gelişmelerin etkileri, Türkiye ve Dünya'da olumlu ve olumsuz yönleri ile kendini göstermektedir. Bu etkiler, ulusal ve uluslararası kanun koyucuları, eksiklerini gelişmeler paralelinde tamamlamak için düzenlemeler yapmaya zorlamaktadır.

Türkiye'de, bilişim alanında yapılan düzenlemeler TCK'da "Bilişim Alanında Suçlar" başlığı altında düzenlenerek bilişim ile ilgili tüm suçların tek bir başlık altında toplanması amaçlanmıştır. Fakat bilişim alanındaki gelişmelerin çok hızlı olması ve internet gibi uluslararası bir ağın söz konusu olması yapılan düzenlemelerin yeteriz kalmasına neden olmuştur.

İnternet kullanımının dünya genelinde artması, verilere erişim kolaylığı ve kazancın büyük olması suç faillerini bilişim suçlarına yöneltmiştir. Bunun yanı sıra suç alanının dinamik olması nedeniyle suç faillerinin bulunmasının güç olması suçlular için caydırıcılığı azaltmış, bu alandaki suç ve suçluların sayısını da arttırmıştır. Bu sebeplerden ötürü bilişim suçlarıyla mücadelede en etkili yöntem suçun oluşmadan engellenmesidir (Boğa, 2011).

2.3.1 Fiziki ve İşlevsel Güvenlik

Bilginin korunmasında yapılması gerekenlerin en başında fiziki güvenlik önlemlerinin alınması gelmektedir. Belirli aşamalardan oluşan fiziki güvenlik tedbirleri, üzerinde titizlikle durulması gereken bir konudur. Fiziksel güvenliğin ilk aşaması; fiziksel güvenlik gereksinimlerinin belirlenmesidir. Öncelikle risk analizi ile hangi bölgenin ne derece güvenliğe ihtiyacı olduğu belirlenmelidir.

Bilgiyi çoğaltabilmek, taşıyabilmek veya arşivleyebilmek amacıyla kullanılan tüm harici hafıza birimleri (disket, CD, harici bellek vb.) mutlaka güvenli bir alanda ve mutlak suretle kilit altında muhafaza edilmelidir. Söz konusu malzemelerin zarar görmesi halinde bir daha kullanamayacak durumda olanlar imha edilmeli, personel

tarafından kullanılan her türlü veri taşıyıcı, yazıcı, tarayıcı vb. donanımlar kayıt altına alınmalıdır.

Sistemlerde lisanssız programların kullanılması suç olduğundan kaynağı ve güvenilirliği bilinen programlar mutlaka lisanslı olarak kullanılmalıdır.

Her bilgisayarda parola koruması mutlaka aktif edilmeli, bilgisayarların kullanılmadığı kısa süreli durumlarda ekranda bulunan bilgilere veya ağ içindeki bilgisayarlarda bulunan bilgilere yetkisiz erişim olmaması için sisteme giriş parolası haricinde ekran koruma parolası da mutlaka belirlenmelidir.

Sisteme erişim için belirlenen parolalar en az sekiz karakterden oluşmalı, bu karakterler harf, rakam ve işaret içermeli, doğum tarihi, isim gibi kolaylıkla tahmin edilebilecek sözcükler parola olarak kullanılmamalıdır. Ayrıca sisteme giriş yetkisi olanların haricinde parolaların bilinmemesi için gerekli önlemler alınmalıdır.

Sistemlerin disket, CD/DVD veya benzeri harici sürücülerle boot edilebilmesi engellenmeli, eğer mümkünse sistemlerde harici aygıt kullanımları engellenmeli, mümkün değilse kontrol altına alınmalıdır.

Bilgisayarların dış tehditlere karşı korunması amacı ile lisanslı virüs programları kullanılmalıdır. Sistem her açıldığında virüs programları aktif olarak çalışmaya başlayarak koruma üst düzeyde tutulmalıdır. Anti-virüs programları güncel olmalı, böylelikle yeni virüslere karşı koruma sağlanmalıdır.

Bilgisayarlar ağ üzerinde kullanılıyorsa, tüm sürücüler paylaşıma kapatılmalıdır. Eğer paylaşım yapılması gerekiyorsa bilgi alış-verişi amacıyla uygun boş bir klasör paylaşıma açılmalı, klasörde gizlilik dereceli dosya paylaşımı engellenmeli ve bu klasöre erişebilecek kullanıcılar tespit edilerek yetkilendirilmelidir (Boğa, 2011).

2.3.2 Kurumsal Güvenlik

Teknolojinin gelişmesinin sağladığı avantajlar ve iş yapma tekniklerinin değişmesine bağlı olarak tüm kurum ve kuruluşlar, iş proseslerini ve bilgi kaynaklarını dijital ortama taşımışlardır. Dijital ortamda saklanan bilginin miktarı arttıkça, bilgi güvenliği stratejik öneme sahip bir konu haline gelmiştir (Eminağaoğlu & Gökşen, 2009).

Sadece fiziksel güvenlik önlemleri alarak stratejik bilgi güvenliğinin sağlanamayacağı göz önüne alındığında konunun kurumsal bir yönetim anlayışıyla ele alınması gerektiği ve üst yönetimden başlayarak tüm çalışanlara konuyla ilgili gerekli eğitimler verilerek, tüm personelin desteğinin alınması ile sonuç alınabileceği açıkça ortadadır.

Tüm fiziksel ve kurumsal önlemleri alan bir kuruluş da dahi, tek bir personelin oluşturacağı bir güvenlik açığı, alınan tüm önlemlerin boşa gitmesine sebep olabilmekte, bilgi güvenliğini zafiyete uğratabilmektedir. Bu sebeple stratejik bilgi güvenliği, kurum ve kuruluşlar için bir öncelikli politika olmalı, tüm kurum personeli için uyulması gereken kurallar bu politika çerçevesinde belirlenmelidir.

Sistemin kesintiye uğramaması, üretilmiş olan veya saklanan bilgilerin bütünlüğünün korunması ve bu bilgilerin kurum dışına izinsiz çıkartılamaması için, bilgi güvenliği mutlaka kurumsal olarak ele alınmalı, kurumlara has tüm iş süreçlerinde olası güvenlik açıkları değerlendirilmelidir. Bu güvenlik açıkları, oluşturulacak bilgi güvenliği politikaları ve bilgi güvenliği standartları ile ivedilikle kapatılmalıdır (Vural & Sağıroğlu, 2008).

2.3.3 Personel Güvenliği

Siber saldırıların artık eski amaç ve yöntemlerle gerçekleştirilmediği, kişisel tatmin yerine para ile motive olan kişilerin bu saldırıları gerçekleştirdiği son dönemde yapılan araştırmalar ile açıkça ortaya konmaktadır. Stratejik bir öneme sahip bilginin, parayla motive olan kötü niyetli kişilerin saldırıları karşısında korunması için alması gereken tedbirlerden biri de personel güvenliğidir.

Bilgisayar son kullanıcıları ve kurum yöneticilerinde stratejik bilgi güvenliği bilincinin oluşturulması personel güvenliğinin en önemli unsurudur. Kurumların bilgi işlem departmanlarında görevli personel, bulundukları konum gereğince sahip olduğu kritik bilgileri kimseyle paylaşmamalıdır. Bilgi işlem departmanlarında mümkün olduğunca bilgi güvenliği konusunda eğitimli, güvenlik tahkikatı yaptırılmış personel görevlendirilmeli, gelişen teknolojiler karşısında personelin kendisini yetiştirebilmesi için gerekli eğitimler personele verilmelidir (Sayıştay, 2013).

Eğer bilişim sistemleri bakım onarım hizmeti kurum dışından sağlanacak ise, hizmet sağlayıcı kuruluş ile kurum arasında imzalanacak sözleşmelerde gizlilik ve

mahremiyet kuralları öncelikli madde olarak bulunmalıdır. Hizmet sağlayıcı firmanın görevlendireceği personel ile ilgili güvenlik tahkikatları titizlikle yaptırılmalı, bu personelin yaptığı iş ve bilgi güvenliği ile ilgili kontroller periyodik olarak yapılmalıdır. Hizmet sağlayıcı firma ile sözleşme şartlarında bir değişiklik oluştuğunda veya sözleşme süresi sona erme aşamasında olduğunda, gizlilik anlaşmaları ve güvenlik politikaları yeniden gözden geçirilmelidir (Orta Doğu Teknik Üniversitesi, 2004).

Bilgi işlem departmanında görevli personel, sisteme dışarıdan müdahale olduğunu fark edebilecek eğitim ve bilgi birikimine sahip olmalı, hızlı bir şekilde sisteme müdahale ederek, gerekli önlemleri alabilecek seviyede olmalıdır. Bununla birlikte dışarıdan yapılabilecek müdahalelerin neler olabileceği ve bu müdahaleler sonucu sisteme ne tür zaralar verilebileceğini, bu kapsamdaki bilişim suçlarının neler olduğu, bu suçlar ile ilgili kendisine düşen görevleri ve bunlar hakkındaki yasal mevzuatı iyi bilmeli ve buna göre daha önce belirlenmiş politikaları yürütebilmelidir. Tüm personel bilgisayar sistemlerinde kullanılan anti-virüs ve firewall gibi güvenlik programlarını kullanmayı çok iyi bilmeli, program tarafından verilen uyarıları anlayabilmeli, oluşabilecek saldırılardan korunabilmelidir (Tulum, 2006).

2.3.4 Bilgi Güvenliği Standartları

Bilgi Güvenliği Standartları, Bilgi Güvenliği Yönetim Sistemleri'nin temel çıkış noktasıdır. Bilgi Güvenliği Yönetim Sistemi ise "kurumun hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşım" olarak tanımlanabilir. Bu sistemin önceliği hassas bilginin korunmasıdır. Bu sistem, iş süreçlerinin ve bilgi teknolojilerinin güvenliğini kapsar (Evrin & Demirer, 2011).

Uluslararası Standartlar Kurumu ISO tarafından kabul edilen ve ISO/IEC 27001:2005 olarak yayımlanan Bilgi Güvenliği Yönetim Sistemi ilk kez 1998 yılında BSI tarafından yayımlanan BS 7799-2 standardında kullanılmıştır. Bilgi güvenliğinin sağlanmasında kullanılacak kontroller ile ilgili standartlar BSI tarafından BS 7799-1 olarak yayımlanmış, yine ISO tarafından kabul edilerek ISO/IEC 17799:2005 olarak yayımlanmıştır. 2007 yılına kadar ISO/IEC 17799:2005 olarak tanımlanan bu standart 2007'den itibaren ISO/IEC 27002:2005 olarak tanımlanmıştır. (Önel & Dinçkan, 2007)

Günümüzde bilgi güvenliği yönetimi ve kontrolü konusunda en yaygın olarak kullanılan standart, "ISO/IEC 27002:2005 Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri" standardıdır. Bu standart, kurumlar içerisinde bilgi güvenliği yönetimi ile ilgili süreçler genel prensipler ve yönlendirici bilgileri ortaya koyar. ISO/IEC 27002:2005 kılavuzluğunda kurulan Bilgi Güvenliği Yönetim Sistemi'nin belgelendirmesi amacı ile "ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler" standardı kullanılmaktadır. Bu standart, kurumun tüm iş süreçlerinde riskleri belirlemek, Bilgi Güvenliği Yönetim Sistemi'ni hayata geçirmek, kontrol etmek ve iyileştirmek için gereksinimleri içermektedir. ISO/IEC 27001:2005 standardı ile ISO/IEC 27002:2005'te belirlenen kontrol hedeflerinin kurum içerisinde nasıl uygulanacağı ve denetleneceği belirlenmektedir (Önel & Dinçkan, 2007).

Her iki standart Türkçe olarak TSE tarafından "TS ISO/IEC 17799:2005" ve "TS ISO/IEC 27001:2005" isimleri ile yayımlanmıştır. Standardın belgelendirmesi konusunda TSE tarafından "TS 13268-1 BGYS Belgelendirmesi İçin Gereksinimler ve Hazırlık Kılavuzu Standardı" yayımlanmıştır (Önel & Dinçkan, 2007).

Kurumlar, karmaşık bir terminoloji içeren bu standartları hem uygulama hem de denetleme sürecinde sorunlar yaşamaktadırlar. Bu sorunlar ile ilgili konuya hakim danışmanlık hizmeti veren firmalar bulunmakta olup, bu firmaların verdiği eğitimler ve hizmetler ile kısıtlı da olsa bilgi güvenliği ile ilgili sorunlar aşılabilmektedir.

2.3.5 Uluslararası Polis İşbirliği

Belirli bir ülkenin sınırlarına bağlı kalmayan ve faaliyet alanlarını sınırlar dışına taşıyan organize suç örgütlerine karşı, ülkelerin ellerindeki tüm imkânları kullanarak soruşturma yürütmeleri günümüzde yeterli olmamaktadır. Ülkelerin bu suç örgütlerine karşı ortak hareket etmeleri ve kararlı bir tutum ile birbirleriyle etkin işbirliği yapmaları, günümüzde bir tercih olmaktan çıkmış adeta bir zorunluluk haline gelmiştir (Ersoy, 2009).

Uluslararası polis işbirliği ile ilgili faaliyetler incelendiğinde, bunun küreselleşme ile ilgili olmadığı, bir gelişim süreci geçirdiği, ulusal polis teşkilatlarının profesyonelleşmeye başladığı 20. yüzyılın başlarından itibaren kendini hissettirmeye başladığı görülmektedir (Emniyet Genel Müdürlüğü, 2009).

Ulusal polis teşkilatlarının yaptıkları ortak çalışmalar, başlarda uyuşturucu ticareti, insan ve göçmen kaçakçılığı, fidye amaçlı adam kaçırma, yasadışı silah ticareti, vergi kaçakçılığı, tarihi eser kaçakçılığı ve uluslararası yolsuzluk gibi konular ile sınırlı iken, teknolojide meydana gelen baş döndürücü gelişmeler ve teknolojinin sınır tanımayan özelliğinin de büyük katkısı ile artık uluslararası polis işbirliği ülkeler açısından dış politikanın ayrılmaz bir parçası haline gelmiştir.

Fakat ulusal kolluk teşkilatları kendilerine verilen yetki çerçevesinde ortak operasyonlar yürütmelerine rağmen ülkelerin ceza yasalarının uyuşmaması yapılan çalışmaların istenilen sonuçları vermemesine neden olmuştur.

1983 yılında OECD ülkeleri, siber suçlar kapsamında karşılaştırmalı olarak ulusal ceza yasalarının birbiri ile uyumlaştırma çalışmalarına başlanmıştır. Bu çalışmalar 1986 yılına kadar sürmüş, sonuç olarak "Bilgisayarla İlgili Suç: Hukuki Politikaların Analizi – Computer Related Crime: Analysis of Legal Policy" raporu yayımlanmış, üye ülkelere bir takım suçların yaptırımlarının uyumlaştırılması için gerekli düzenlemeleri yapmaları tavsiye edilmiştir (Değirmenci, 2003).

Avrupa Konseyi tarafından görevlendirilen bir komite, OECD'nin hazırladığı raporu esas alarak şekilde bir çalışma yapmış, bu çalışma sonucunda OECD'nin raporu doğrultusunda belirtilen suçlar ile ilgili üye ülkelerin ceza kanunlarında uyumlaştırma yapması gerektiği fikri kabul edilmiş, ayrıca OECD raporunda yer almayan bir takım suçlar da bu çalışmada yer verilmiştir. 1995 tarihinde Avrupa Konseyi Bakanlar Komitesi tarafından kabul edilen bir başka bir çalışma ise, bilişim teknolojilerinde yaşanan yeniliklere göre ulusal ceza muhakemesi yasalarındaki soruşturma ve el koymaya, dijital delil ve bilişim suçlarında uluslararası işbirliği başlıklarında yapılması gereken değişikliklere dair tavsiyelerde bulunmuştur (Değirmenci, 2003).

Siber suçlar ile ilgili en geniş kapsamlı uluslararası düzenleme Avrupa Konseyi tarafından hazırlanan "Avrupa Siber Suç Sözleşmesi"dir. Avrupa Konseyi Suç Sorunları Komitesi, 1996 yılında bilişim alanında işlenen suçlar ile ilgili çalışmak üzere bir komite olan "The Committee of Experts on Crime in Cyber-Space" oluşturmuştur. Komite, 1997 yılında çalışmalarına başlamış, sonuç olarak "Siber Suçlar Sözleşme Taslağı" ile ilgili raporunu Avrupa Suç Sorunları Komitesi'ne 2001 yılında sunmuştur. Avrupa Konseyi Bakanlar Komitesi taslağı, 8 Kasım 2001 tarihinde

kabul etmiş ve Budapeşte'de 23 Kasım 2001 tarihinde düzenlenen Siber Suçlar Uluslararası Konferansı'nda imzaya sunulmuştur (Özcan, 2001).

Sözleşme, Ekim 2018 tarihi itibari ile Avrupa Konseyi üyesi ülkeler ile beraber 65 ülke tarafından imzalanmıştır. Türkiye söz konusu sözleşmeyi 10.11.2010 tarihinde imzalamış, 29.09.2014 yılında onaylayarak, 01.01.2015 yürürlüğe sokmuştur (Avrupa Konseyi, 2018).

Avrupa Siber Suç Sözleşmesi, Avrupa Konseyi üyesi ülkeler ile birlikte ABD, Japonya, Güney Afrika dâhil diğer ülkeler tarafından imzalandığından genel kabul görmüş bir sözleşmedir.

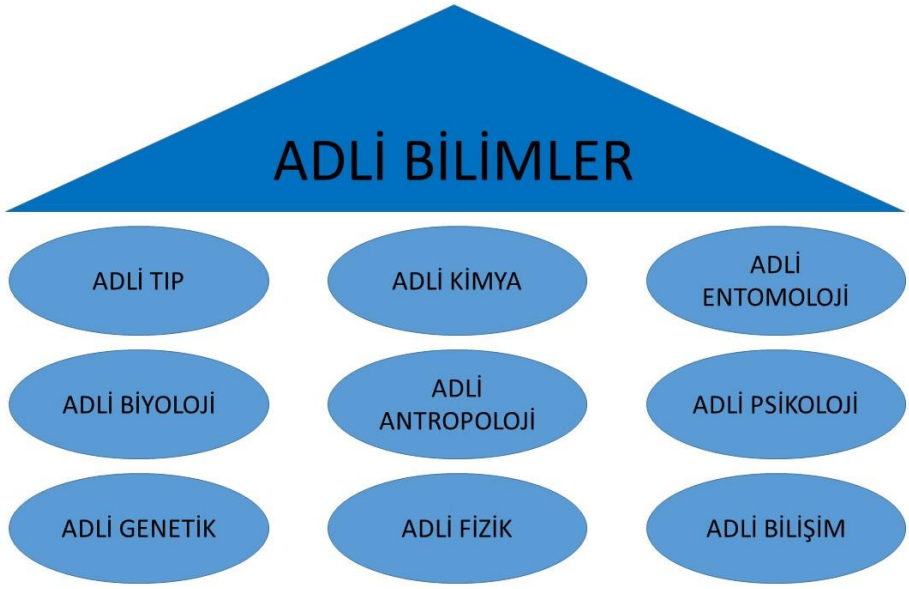
Yapılan tüm bu çalışmalara rağmen ceza kanunlarında düzenlenen birçok klasik suç tipinin aksine bilişim suçlarının dinamik olması, yapılan düzenlemelerin güncelliğini çabuk yitirmesine yol açmaktadır. Bu yüzden, bu konuda yapılan düzenlemeler, gelişen teknolojiyle paralel göstermesi, yeni çıkan ihlal türlerinin ivedilikle suç olarak olarak hüküm altına alınması gerekmektedir. Kanunlaştırma çalışmaları uluslararası hukukla paralel yapılmalı, teknolojik değişim hızı uluslararası çalışmalar yapılırken ile göz önünde bulundurulmalıdır.

3. ADLİ BİLİŞİM VE DİJİTAL DELİL İNCELEMELERİ

3.1 Adli Bilişim Kavramı

3.1.1 Adli Bilişimin Tanımı ve Önemi

Adli bilişim, geniş bir çalışma sahası olan ve genişleme ivmesi teknolojinin hayatımıza girme derecesiyle doğru orantılı bir bilim dalıdır. İngilizce'de "Computer Forensic" diye adlandırılan bu disiplin, Türkçe'ye "bilgisayar incelemesi", "bilgisayar kriminalistiği", "adli bilişim" veya "adli bilgisayar incelemesi" şeklinde çevrilmesine rağmen genel kabul görmüş karşılığı olan adli bilişim ismi ile adli bilimlerin çatısı altında yerini bulmuştur. (Kılıç, 2014)



Şekil 3.1.1.1: Adli bilimler

Yeni ve gelişmekte olan bir disiplin olması nedeniyle adli bilişim ile ilgili birçok tanım ortaya konmuştur. Bir tanıma göre adli bilişim; "işlenen bir suçun aydınlatılabilmesi için varsa dijital verilerin toplanılması, delilleştirilmesi, muhafaza edilmesi ve raporlanması işlemlerini de içinde bulunduran bir bilim dalıdır." Bu bilim dalı sayesinde, suç ve suçlu ile etkin bir şekilde mücadele edilmektedir. Gerçek veya sanal dünyada işlenen suçlar delillendirilerek suç ile ilgisi olmayan masum kişiler korunmaktadır (Çakır & Kılıç, 2013).

Başka bir tanımda ise adli bilişim; “suçun aydınlatılabilmesi için bilimsel metotlar kullanılarak, çeşitli varyasyonlardaki dijital medyalar üzerinde bulunan, suçla ilgili dijital delillerin bozulmadan ve zarar görmeden anlaşılabilir bir şekilde adalet önüne sunulmaya hazır hale getirilmesini sağlayan ve başlı başına bilimsel teknik prensiplerin uygulandığı bir delil inceleme sürecinin bütünü” olarak tanımlanmaktadır (Ekizer, 2014).

Bilgisayar medyaları üzerinde bulunan dijital veriler ile ilgilenen bu adli bilim dalı, kendine özgü yöntemler kullanmaktadır. Elektronik verilerin delil haline dönüşmesi süreci olan adli bilişim, muhakeme konusu olayın açıklığa kavuşturulabilmesi için önem arz etmektedir.

Hukuk alanında yardıma ihtiyaç duyulan teknik konulardaki artış nedeniyle ortaya çıkan adli bilişim bilim dalının temel amacı, elektronik veriler ile olay arasındaki ilişkiyi veya fiil ile eldeki veriler ve kullanıcı arasındaki ilişkiyi ortaya koymaktır. Hem ceza hukuku hem de özel hukuk alanındaki uyuşmazlıklarda adli bilişim tekniklerine başvurulabilmektedir (Henkoğlu, 2011).

Eski zamanlarda el yazısı veya daktilo çıktılarını kapsayan doküman incelemelerine, teknolojinin gelişmesi ve bilgisayarın hayatımıza girmesi ile harddisk, taşınabilir bellek, cep telefonu ve dijital müzik çalarlar gibi dijital veri işleyebilen cihazlarda eklenmiştir. Fakat dijital verilerin narin olması bu tür delillerin güvenilirliği sorununu ortaya çıkarmıştır. Bu delillere özel muamele edilmez ise kolaylıkla silinebilir ya da değişikliğe uğrayabilirler. Adli bilişim teknikleri bu tür sorunlara çözüm olması için geliştirilmiştir.

Bir bilgisayar sisteminde ya da elektronik medya üzerinde var olan elektronik verilerin tespit edilmesi, silinen, şifrelenmiş ya da hasar görmüş dosyaların ve bilgilerin kurtarılması, hem soruşturma hem de kovuşturma aşamasında kolluk kuvvetine ve adli makamlara çok yardımcı olacaktır. Burada dikkat edilmesi gereken en önemli konu, delil bütünlüğünün her şekilde korunması için gerekli önlemlerin alınmasıdır. Bu yüzden olay yeri ya da şüpheliden elde edilecek delil niteliği taşıyan ve veri bulundurma yeteneğine sahip medyanın, tespit edilmesinden başlayarak, üzerinde bulunduğu sistemden ayrılarak, taşınması, kopyasının alınması, muhafaza edilmesi, incelenmesi, rapor hazırlanması ve teslim edilmesi aşamalarında, genel

kabul görmüş uluslararası adli bilişim standartları uygulanmaktadır (EGM KOM Daire Başkanlığı, 2009).

3.1.2 Adli Bilişimin Tarihsel Gelişimi

Bir olayda şüpheli veya sanığın suçlu olup olmadığını belirlemede hayati rol oynayabilen adli bilişim, yeni bir bilişim dalı olup gelişimini henüz tamamlamamıştır. Bu bilim dalının gelişimi teknolojinin gelişimi ile paralel olup, son 15 yıl içerisinde büyük mesafe kat etmiştir. Ayrıca adli bilişim, 21. yüzyılda en fazla gelişme gösteren alanların başında gelmektedir (Orta, 2015).

Kişisel bilgisayarların kullanımının artması ve bununla birlikte bilişim suçlarında olan artış, ülkelerin bu konuda önlem alması ihtiyacını ortaya çıkartmıştır. İlk hukuksal düzenleme 1983 yılında Kanada'da yapılmış, 1984 yılında ABD de FBI bünyesinde, uzmanlardan oluşan bir birim kurarak ilk adım atan ülkelerden biri olmuştur (Wikipedia, 2015). Adli bilişimin ilk kez bir disiplin olarak ele alınması ise 1989 yılında ABD North Texas Üniversitesinde eğitim programı olarak yer alması ile gerçekleşmiştir (Huebner, Bem, & Bem, 2007).

1990'lı yıllarda adli bilişim standartlarının geliştirilmesi konusunda farkındalığın oluşmaya başladığı görülmektedir. 1991 yılına gelindiğinde adli bilişim konuları sıkça tartışılır olmuş ve konu hakkında bir takım toplantılar yapılmaya başlanmıştır. 1991 yılı başlarında ABD'de yapılan ve altı uluslararası kolluk birimi ile pek çok Amerikan Federal kolluk biriminin katıldığı toplantıda, yapılan incelemelerde standart bir yaklaşımın ortaya koyulması gerektiği sonucuna varılmıştır. 1993 yılında FBI'ın ev sahipliğinde elektronik deliller ve adli bilişim konusunda yapılan toplantılar 1995,1996 ve 1997 yıllarında da devam etmiş, sonuç olarak IOCE (International Organization on Digital Evidence) isimli bir kuruluş oluşturulmuştur. (Orta, 2015)

2000'li yıllar standardizasyon üzerinde durulduğu yıllardır. SWGDE (The Scientific Working Group on Digital Evidence) 2002 yılında "Adli Bilişim İçin En İyi Uygulamalar" isimli dokümanı yayınlamıştır. 2004 yılında bilişim suçlarını ve sanal suçlarını kapsayan ilk uluslararası sözleşme olan "Sanal Suçlar Sözleşmesi" imzalanmıştır. Avrupa Konseyi tarafından tasarlanan sözleşme ulusal kanunların harmonisini sağlayarak, araştırma tekniklerini geliştirmeyi hedeflemektedir. 2005

yılında ISO tarafından ISO 17025 “Deney ve Kalibrasyon Laboratuvarlarının Yeterliliği İçin Genel Şartlar” standardını yayımlanmış olup, dijital delil inceleme laboratuvarlarına bir standart getirilmiştir (Wikipedia, 2016).

Türkiye’de yeni sayılabilecek bu bilim dalı, bilişim teknolojilerinin çok daha ileri seviyede olduğu Amerika Birleşik Devletleri gibi gelişmiş ülkelerde daha geniş kullanım alanları bulmaktadır. Öyle ki, adli bilişim analiz yöntemleri artık yalnızca ceza davalarında değil, hukuk itilaflarında hatta özel şirketler dahi adli bilişim tekniklerini de kullanılır olmuştur. Özellikle büyük çaplı özel şirketler, veri kurtarma ve veri imha etme gibi teknik konularda adli bilişim uzmanları ile çalışmakta ya da bu konuda faaliyet gösteren firmalardan destek almaktadırlar (Berber, 2004).

3.1.3 Adli Bilişimin Aşamaları

Adli bilişim, sonuçları hukuk alanında etki oluşturan bir bilim dalıdır. Bu yüzden adli bilişimde elektronik bir bulgunun hukuki bir delile dönüşmesi için takip edilmesi gereken süreçler vardır. Elektronik delillerin tespiti, elde edilmesi, korunması, analizi ve raporlanması yargı mercileri tarafından kabul edilen aşamalardır. Bu aşamalar takip edilmeden elektronik delilin, somut olayın çözülmesinde ve yargılama makamları önünde maddi gerçeğin aydınlatılmasında kullanılması söz konusu olamaz.

3.1.3.1 Delillerin Tespiti ve Olay Yeri İncelemesi

Delil, bir hukuki ihtilafı ispata yarayan bilgi ve bulgulardır. Gerçeğin ortaya çıkartılması ve adil bir yargılama yapılabilmesi için olay yerinin layıkıyla korunması ve delillerin adil bir şekilde olay yerinden elde edilmesinin sağlanması gerekmektedir (Kaygısız, 2005).

Olay yeri incelemesi sırasında yapılan tüm işlemler hukuk kuralları ile düzenlenmektedir. Ülkemizde mevzuata bakıldığında bu konu ile ilgili Anayasa başta olmak üzere, Türk Ceza Kanunu, Ceza Muhakemesi Kanunu ve PVSK gibi kanunları ile birlikte Adli ve Önleme Arama Yönetmeliği, Polis Adli Görevlerinin Yerine Getirilmesinde Delillerin Toplanması, Muhafazası ve İlgili Yerlere Gönderilmesi Hakkında Yönetmelik, Suç Eşyası Yönetmeliği ve Emniyet Teşkilatı Parmak İzi Teknik Hizmetleri Yönetmeliği gibi birçok tüzük ve yönetmeliğin bulunduğu görülmektedir.

Ceza Muhakemesi Kanunu'nda olay yeri incelenmesi ile ilgili ayrı ve açık bir hükme yer verilmemiş, bu konu Ceza Muhakemeleri Kanunu esas alınarak Adli ve Önleme Aramaları Yönetmeliği'nin 9. maddesinde düzenlenmiştir. Bu maddeye göre; "suç işlenen yerlerde, sebep ve sonuç ilişkisini ortaya koyacak delillerin aranması, bulunması ve el koyulması için geliştirilmiş bilimsel ve teknik araştırma işlemlerinin, herkesin girip çıkabileceği kamuya açık alanlarda yapılması için bir emir veya karar gerekmez. Bu yerler dışındaki olay yeri inceleme işlemleri, Hakim veya gecikmesinde sakınca bulunan hâllerde de Cumhuriyet Savcısının, Cumhuriyet Savcısına ulaşılamadığı hâllerde ise konut, işyeri ve kamuya açık olmayan kapalı alanlar dışındaki yerlerde kolluk amirinin yazılı emri üzerine gerçekleştirilir." Bu kural suçüstü durumlar ile şüphelinin talebi veya rızasının bulunması halinde bile geçerliliğini korumaktadır. Bu durum özellikle adliyenin bulunduğu merkezden uzak yerleşim birimlerinde işlenen suçlarda Hakim veya Cumhuriyet Savcısından yazılı emir alınması için geçecek sürede delillerin yok edilmesi, bozulması veya gizlenmesine imkan vermekte, belki de şüphelinin lehine olabilecek delillerin toplanamaması sonucu şüphelinin haklarının yeterince korunamamasına yol açabilmektedir (TCK, m.160/2).

Olay yeri incelemesinde amaç;

- Meydana gelmiş bir olayın bir suç olup olmadığını tespit edebilmek,
- Olayın hangi şartlarda meydana gelip gelmediğini belirleyebilmek,
- Olayın gerçekleştiği yer, şüpheli ve müşteki arasındaki ilişkiyi gösteren suç delillerini bulabilmek,
- İşlenmiş olan suçun aydınlatılabilmesi ve adli makamların doğru kararı verebilmesini sağlamak amacıyla suç mahallini belgelemek,
- Suçun soruşturmasında ve çözümünde olay yeri, şüpheli ve müşteki ilişkisinin ortaya çıkartabilmektir (Kaygısız & Bayer, 2002).

Olay yeri incelemesi temelde bir arama işlemidir. Suç mahallinde her şey delil olabilmektedir. Bu nedenle suç mahallinin ilk incelemesinin gözlem yolu ile yapılması gerekmektedir. Gözlem sonrası olay yerinin her açıdan detaylı bir şekilde video kamera ile kayda alınması ve fotoğraflanması, olay yerinin ilk halinin tespiti açısından önemlidir. Gerekmesi halinde olay yeri ile ilgili notlar alınabilir.

Polis Adli Görevlerinin Yerine Getirilmesinde Delillerin Toplanması, Muhafazası ve İlgili Yerlere Gönderilmesi Hakkında Yönetmeliğe göre "Olay yerinin incelenmesi sırasında elde edilen tüm deliller bulundukları yerde etiketlenerek numaralandırılırlar. Etiketlerin üzerine; delillerin bulunduğu yer, olay dosya numarası, tarih, delillerin izahı, kimden alındığı, emniyet birimin adı, soruşturmacının kimliği ve lüzumlu görülen diğer hususlar yazılır."

Bilişim sistemlerinin suçun aracı veya konusu olması; klasik olay yeri tespit, belgeleme ve delil toplama işlemlerine ek olarak bir takım özel beceri ve uzmanlık gerektiren önlemlerin alınmasını gerektirir. Elektronik delillerin doğası gereği kolayca değiştirilebilmesi, yok edilebilmesi ve bozulabilmesinden dolayı olay yeri inceleme aşamasında bilgisayar medyalarına sadece uzman personel tarafından ve hassasiyetle yaklaşılması gerekir (National Institute of Justice, 2004).

Locard'ın değişim prensibi her failin, suç mahalline bir takım izler bırakacağı ve buradan da kendisine bulaşan bir takım izleri üzerinde taşıyacağına işaret eder. (Wikipedia, 2015) Bu prensipten hareketle ortam, fail ve mağdur arasında olay sonucu mutlaka bir temas gerçekleşir. Bilişim sistemleri marifeti ile işlenen suçlarda bu durum farklılık göstermemektedir. Fail ile mağdurun aynı ortamda bulunmaması işleri zorlaştırmakla beraber bilişim sistemlerinde her hareketin kaydının olmasından dolayı Lacard'ın değişim prensibi bu tip suçlarda da geçerlidir.

Bilişim suçları ile mücadelede ilerleme sağlamış ülkelerde, olay yerinde bulunan teknik ekibin adli bilişim ile ilgili konularda nasıl hareket edeceklerini bağlayıcı hale getiren ve yanlış yapılan işlemlerin bir ihlal olarak değerlendirilerek cezalandırılacağı düzenlemeler bulunmaktadır. Fakat ülkemizde henüz bu konuda hazırlanmış kapsamlı bir düzenleme bulunmamaktadır (Henkoğlu, 2011).

Bilişim suçları ile mücadelede önde gelen ülkelerin olay yerindeki işlemlerin teknik olarak uygulanması ile ilgili benimsediği bir takım hususlar vardır. İngiltere yayımlanan ve 2012 yılında güncellenen "ACPO Good Practice Guide for Digital Evidence" ve ABD'de yayımlanan ve 2008 yılında güncellenen "Electronic Crime Scene Investigation: A Guide for First Responders" bu konuda verilebilecek önemli örneklerdir (Henkoğlu, 2011).

3.1.3.2 Dijital Delillerin Elde Edilmesi

Hukuk devletinin olmazsa olmaz unsurlarında birisi de ceza muhakemelerinde hukuka uygun delil elde edilmesi yöntemidir. Bu nedenle, Anayasa'nın 38'inci maddesini 6'ncı fıkrasında, "hukuka aykırı olarak elde edilen delillerin yargılamada kullanılamayacağı" düzenlenmiştir (Orta, 2015).

Kişiye ait özel bilgiler üzerindeki hak, Anayasa'da koruma altına alınan temel insan haklarındandır. Bu hakkın kısıtlanabilmesi için yasal düzenleme gerekeceği ortadadır. Bilgisayarlarda bulunan verilerin gerçeğin ortaya çıkarılması açısından, ceza davasında delil oluşturacağı kanaat getirilmesi halinde Adli ve Önleme Aramaları Yönetmeliği'ne göre işlem yapılır (Say, 2006). "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma" başlığı adı altında yapılması gerekenler sırasıyla aşağıda sıralandığı gibi anlatılmıştır.

- "Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması hâlinde, Cumhuriyet Savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine Hakim tarafından karar verilir."
- "Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması hâlinde, el konulan cihazlar gecikme olmaksızın iade edilir."
- "Bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır."
- "İstemesi hâlinde, bu yedekten elektronik ortamda bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır."

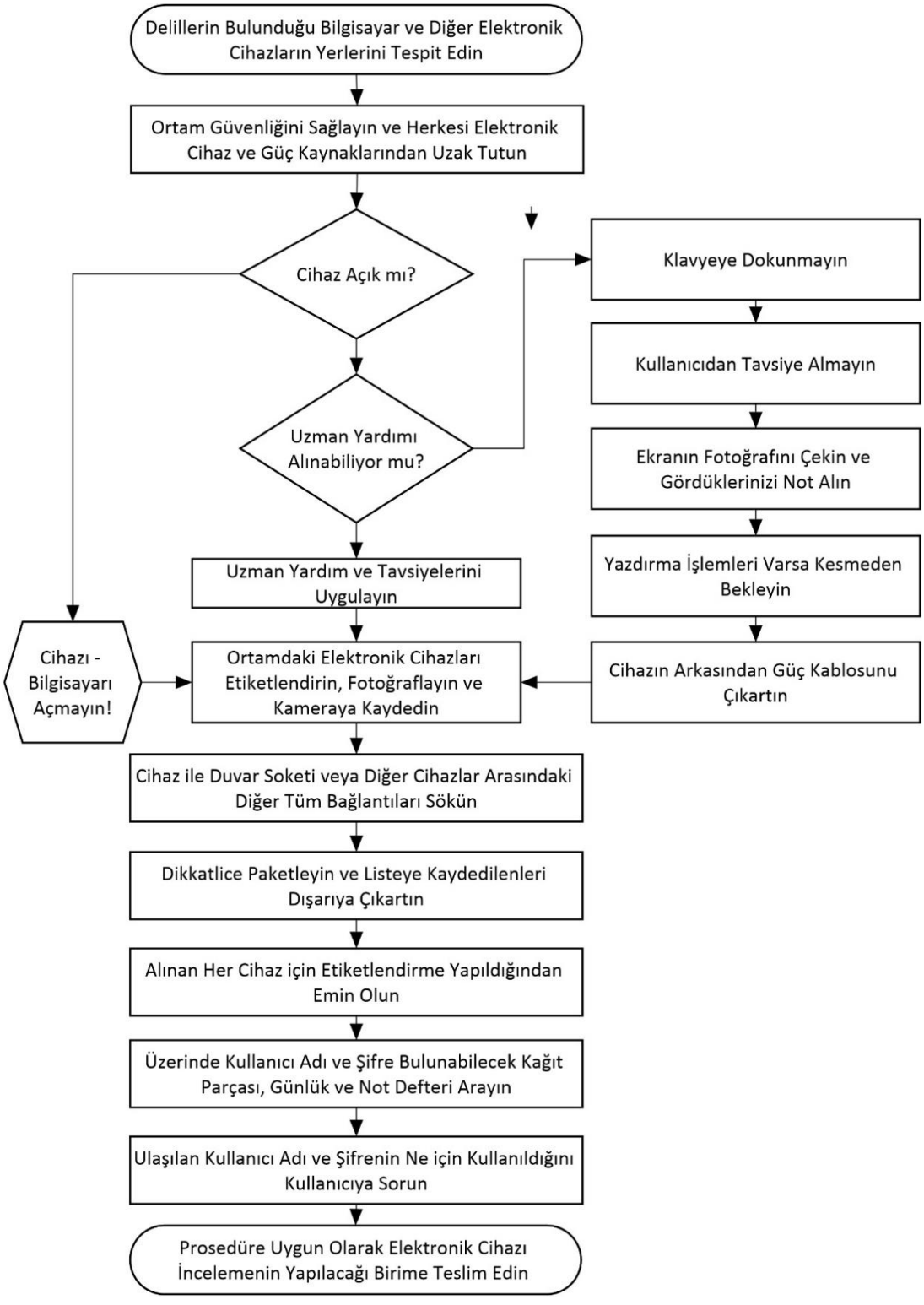
- “Bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir.” (Adlî ve Önleme Aramaları Yönetmeliği, Mad.17)

Birinci fıkrada bahsi geçen “başka surette delil elde etme imkânının bulunmaması hâlinde” şartı; soruşturma esnasında bütün delil elde etme yöntemlerinin uygulanmış olması, ancak başka delil elde etme imkânının artık bulunmaması gerektiği vurgulamaktadır. Bu şart ülkemizde dijital delillere gerekli önemin verilmediğinin açık bir örneğidir.

Ceza ve hukuk mahkemelerinde kullanılan klasik deliller elle tutulabilir, gözle görülebilir, kolayca elde edilebilir somut nitelikteyken, siber suçlarında söz konusu olan dijital deliller, klasik delillerden farklı olarak soyut bir nitelik taşırlar. Dijital delillerin içerisinde yer aldığı somut bir donanım bulunmakta ise de, ceza yargılaması bakımından esas delil teşkil edenler bu donanımın kendisi değil, içerisinde yer alan elektronik verilerdir (Özocak, 2011).

Elektronik delillerin elde edilmesi süreci olay yerinde başlar ve sonrasında devam edecek olan inceleme, analiz ve raporlandırma aşamalarının tümünün geçerliliğini etkileyecek öneme sahiptir (Kiçeci, 2014).

Olay yeri incelemesi ve prosedüre uygun olarak olay yerinden mümkün olan en fazla dijital delilin elde edilebilmesi için akış diyagramlarından yararlanmak işleri biraz olsun kolaylaştırabilmektedir. Bu yol ile basit uygulama hataları yapma ve tüm süreci olumsuz etkileme olasılığı mümkün olan en alt seviyeye düşürülebilir. Bu amaçla hazırlanmış Şekil 3.2: Olay yeri incelemesi faaliyet akış diyagramı (Henkoğlu, 2011) olay yerine müdahale eden ekipler için güzel bir örnektir.



Şekil 3.1.3.2.1: Olay yeri incelemesi faaliyet akış diyagramı

Delillerin orijinalinin bozulmadan elde edilmesi ve elde edilen verilerin değişime uğratılmadan analiz edilmesi, adli bilişimin temelini oluşturmaktadır. Bu nedenle dijital delillerin elde edilmesi veya başka bir ifade ile toplanması aşamasında, olay yerinde bulunan ekiplerin dikkat etmeleri gereken hususlar vardır. Bu hususlar aşağıda sıralanmıştır.

- Elektronik delillere ilk müdahale, mutlaka alanında eğitim almış uzman adli bilişim personeli tarafından yapılmalı, eğer uzman personel bulunmuyor ise, Şekil 3.2'de belirtilen yönlendirmelere dikkat edilmelidir.
- Aramanın yapılacağı alanda delillerin bulunabileceği yerler öncelikle tespit edilmeli, daha sonra delillerin elde edilmesi ve delil arama işlemleri için bir denetleme/gözetim zinciri oluşturulmalıdır. Tüm yapılan işlemler kamera ile kayıt altına alınmalı, grup halinde hareket etme durumu var ise tüm ekibin kameranın görme alanı içerisinde olması sağlanmalıdır.
- Delillere mümkün olduğunca elle dokunulmamaya özen gösterilmelidir. Elektronik cihaz ve veri depolama üniteleri (CD/DVD vb.) üzerindeki parmak izi araştırması gibi kriminal işlemler de ilk aşamada dijital delillerin toplanması işlemi ile birlikte yürütülmelidir.
- İnsan vücudunda oluşan statik elektriğin delillere zarar vermemesi için gerekli tedbirler alınmalıdır.
- Aramanın yapıldığı alan aramaya başlamadan boşaltılmalı, ilgisiz kişilerin el konulacak delillere müdahale edebilecek kadar yakın olmaması sağlanmalıdır.
- Çalışan sistemler tespit edilerek ilk hali fotoğraf çekilmesi suretiyle kayıt altına alınmalı, gerekli notlar alındıktan sonra uçucu delillerin incelenebilmesi için nasıl bir yol izleneceğine kararlaştırılmalıdır. Uçucu veri olmaması durumunda sistemin elektrik bağlantısı kesilmeli ya da bataryası çıkartılmalıdır.
- Olay mahallindeki açık bilgisayarların kapatma işlemi, işletim sisteminin türüne göre yapılmalıdır. Dizüstü bilgisayarlar kapatılırken, işletim sistemine bağlı olarak aynı yöntemler uygulanmakla birlikte, bataryanın da mutlaka çıkartılması gerekmektedir. Bazı dizüstü bilgisayarlarda disket

veya CD/DVD sürücü bölümüne yerleştirilmiş ikinci bataryanın olabileceği de unutulmamalıdır.

- Aramanın yapıldığı yerde imaj alma işlemlerinin yapılması gerekiyor ise, elektrik kesintilerine karşı kesintisiz güç kaynağının olup olmadığı araştırılmalı, kesintisiz güç kaynağı bulunmuyorsa arama tutanağında bu husus belirtilerek el koyma hükümleri uygulanmalıdır.
- İmaj alırken, adli bilişim standartlarına uygun olarak tek yönlü yazma işlemi yapabilen donanım ve programlar kullanılmalı ve orijinal delilin bire bir kopyası ("sector by sector", "bit to bit") alınmalıdır.
- İmaj alınması amacıyla kullanılan donanım araçları ya da yazılımların, bire bir kopya alma, imajı istenen büyüklükte parçalara bölebilme, arızalı disklerin imajını alabilme ve karşılaşılan tüm hataları kaydedebilme yeteneklerine mutlaka sahip olması gerekir. Ayrıca "olayın adı, imaj alınan kişiye ait bilgiler, tarih/saat ve disk etiket" gibi bilgiler mutlaka imaj ile birlikte kaydedilmelidir.
- Arama yapılan yerde imaj alma işlemi yapılmış ise, imaj alınmaya ne zaman başlandığı ve imaj almanın ne zaman son bulduğu ve tespit edilen hash değerleri mutlaka arama tutanağına yazılmalıdır.
- Elektronik delil niteliği taşıyan malzemelere el koyma işlemi yapılıyor ise, imaj alma işlemi yapılmadan şüpheli ya da vekili talep etse dahi, daha sonra yapılabilecek itirazların önüne geçmek adına kesinlikle hash değerleri şüpheli ya da vekiline verilmemelidir.
- Arama yapılan yerde birden fazla bilgisayar veya elektronik delil niteliği taşıyan malzeme var ise, ihlalin gerçekleştirildiği muhtemel bilgisayar veya materyallerin tespiti için tüm elektronik materyallerin kimlere ait olduğu ve kim tarafından kullanıldığı bilgisi öğrenilip, etiketlendirme yapılmalı ayrıca bu hususlar tutanakta belirtilmelidir.
- Bilgisayar ya da dijital materyallere el konulma işlemi yapılacak ise, el konulan malzemenin fiziksel özellikleri, marka, model, seri numarası ve boyut bilgileri mutlaka belirtilmeli ve el konulan tüm malzemeler

etiketlerle numaralandırılıp, ayrı ayrı delil torbasına koyarak ağızları mühürlenip aramada hazır bulunan şüpheli veya yakınına imzalatılmalıdır.

- Arama yapılan alandaki işlemler bitirilerek tutanak işlemine geçirildikten sonra arama yapılan alanı terk etmeden, el konulan elektronik materyallerin kontrol edilmeli ve herhangi bir eksik olmadığından emin olunmalıdır.
- Arama işlemi sonunda, el konulan elektronik malzemeler sıvı madde ve manyetik ortamdan uzak, ısı ve nem kontrolü bulunan bir ortamda muhafaza edilmelidir.
- El konulan elektronik deliller, şeffaf, anti-statik veya kabarcıklı delil torbası içerisinde muhafaza edilerek taşınmalıdır (Başar, 2015) (Henkoğlu, 2011).

Dijital delillerin elde edilme işleminde, diğer delil toplama işlemlerinde olduğu gibi olay yeri aramasının önemi ön plana çıkmaktadır. Delil olabilecek materyallerin yargılama esnasında delil niteliği taşıyıp taşımaması, olay yerinde yapılan ilk müdahalenin usullere uygun yapılıp yapılmamasıyla doğru orantılıdır. Olay yeri inceleme işlemini, "Suçun aydınlatılması amacıyla, Adli Önleme ve Aramaları Yönetmeliği'nde belirtilen usullere uygun olarak uzman personel tarafından, olay yerlerinde her türlü iz, eser, emare ve delil niteliği taşıyabilecek bulguların, çeşitli bilimsel, teknik yöntem ve metot kullanarak araştırılması, elde edilen bulguların tespit edilmesi ve kayıt altına alınması (belgelenmesi), toplanması, muhafazası ve incelenmek üzere ilgili yerlere gönderilmesini sağlayan özel amaçlı bir araştırma işlemi" olarak tanımlamak mümkündür. Klasik suçlar da dahil tüm suç tiplerinde, olay yerinin kontrol altına alınması ve delillerin toplanma işlemi ile ilgisi bulunmayan şahısların olay yerinden uzaklaştırılması büyük önem arz etmektedir. Bu sayede, delil elde edilecek elektronik materyallerin korunabilmesi ve elde edilmek istenen delilin zarar görmemesi sağlanabilmektedir. Bu konuda yapılacak en doğru işlem, delil toplama işleminin bir adli bilişim uzmanı tarafından yapılmasıdır. Elektronik delillerin söz konusu olduğu vakalarda adli bilişim uzmanları delil kaybı ihtimalini asgariye indirerek elektronik delil toplama işlemini yapacaktır (Özocak, 2011).

3.1.3.3 Dijital Delillerin Muhafazası

Toplanan delillerin yapılacak olan duruşmada kullanılabilir durumunu korumak için yapılan işleme delilin muhafazası denilmektedir. Olay mahallinde bulunmasından mahkemeye delil olarak sunulmasına kadar geçen süre içerisinde korunması sağlanamayan delil, ne kadar bilgilendirme potansiyeline sahip olursa olsun geçersiz sayılabilir (Öztürk, 2007).

Suç delili niteliği taşıyan malzemelerin düzgün ve noksansız toplanması, muhafazası ve ilgili makamlara gönderilmesine ilişkin esas ve usuller, "Polisin Adli Görevlerinin Yerine Getirilmesinde Delillerin Toplanması, Muhafazası ve İlgili Yerlere Gönderilmesi Hakkında Yönetmeliği" ve "Jandarma Teşkilatı Görev Ve Yetkileri Yönetmeliği" ile düzenlemektir. Bu yönetmelikler; her iki kolluk kuvvetinin, ceza kanununda suç olarak nitelendirilen fiillerin meydana gelmesi ile başlayan adli görevleri yerine getirmek, suç ve suç sanıklar ile ilgili delilleri tespit etmek, toplamak, muhafazasını sağlamak, ambalajlamak, ilgili yerlere göndermek ve bu konulara ilişkin diğer hususları kapsamaktadır.

Delillerin muhafazası kapsamında öncelikle delillerin durumlarının net bir şekilde ortaya konulması gerekmektedir. Bundan kasıt olay yerinde ele geçirilen delillerin hangi durumda, nerede, hangi koşullar içerisinde bulunduğunun belirtilmesidir. Örneğin, olay yerinde bir taşınabilir belleğin ele geçirilmemesi için fail tarafından kırılmış olması, bu hususun tutanaklarda belirtilmesi ve bütün çalışmaların bu kırık taşınabilir bellekten elde edilen veriler üzerinden yapıldığının belirtilmesi maddi gerçek açısından çok önemli olabilmektedir (Orta, 2015).

Olay yerinde el konulan aygıtların paketlenmesi, taşınması ve muhafazası özel ilgi gerektirmektedir. Elektronik delillerin toz, nem, fiziksel darbe, statik elektrik, manyetik alan, aşırı sıcak ve soğuk ortamlara karşı korunması gerekir. Bu amaçla elde edilen delillerin muhafazasında dikkat edilecek başlıca hususlar şunlardır;

- Tespit edilen her delil paketleme işleminden önce mutlak suretle etiketlendirilmeli ve ilgili tutanaklara kaydedilmelidir. İşlemler esnasında mümkün olduğunca kamera kayıtları ile desteklenmelidir.
- Delillerin yerleştirildiği kutular ve poşetler ayrı ayrı etiketlendirilmeli ve mutlaka açıklayıcı notlar etiket üzerinde bulunmalıdır.

- Çok sayıda bilgisayar olay yerinde bulunması halinde, sistem bütünlüğünün bozulmaması için her bilgisayar ayrı ayrı etiketlendirilmeli, her bilgisayara ait yardımcı donanım birimleri (klavye, fare vb.), kendi grubu içerisinde sınıflandırılarak etiketlendirilmelidir. Bu tür sınıflandırma, ihtiyaç duyulması halinde kriminal işlemlerde (parmak izi alma gibi) önemli rol oynamaktadır.
- Veri depolama ünitelerine ait alınan imajlarda MD5 ve SHA hash değerleri imaj alma ve öncesi ve sonrası mutlaka alınmalıdır. Bu değerler tutanak kayıtlarında belirtilmek suretiyle daha sonra meydana gelebilecek itirazların önüne geçilebilmektedir.
- CD/DVD ve yedekleme ünitelerinde kullanılan kasetlerin hassas veri depolama birimleri oldukları unutulmamalı ve çizilmemesi, bükülmemesi, kırılmaması ve manyetik ortamlara girmemesi için özen gösterilmelidir.
- Delillerin taşınma işlemleri uygun şekillerde yapılmalıdır. Elektronik delilerin yapısı gereği, statik elektrik ve bazı cihazların oluşturduğu manyetik alandan zarar görmemesi için özel toplama ve paketleme poşetlerinin kullanımına özen gösterilmelidir. Bu amaçla plastik yerine sağlam kağıt kılıflar ve zarflar kullanılmalıdır.
- Delillerin yerleştirildiği paketler aşırı ısı, aşırı soğuk ve sıvı temasından uzak tutulmalıdır.
- Deliller taşınma sırasında fiziksel darbelere ve titreşime maruz kalmamalıdır.
- Cep telefonu, tablet ve PDA gibi bazı mobil cihazlar bataryasının tamamen boşalması halinde fabrika ayarlarına dönebilmektedir. Bu tür cihazların güç durumunu muhafaza edecek şekilde gerekli önlemler alınmalıdır (Henkoğlu, 2011).

3.1.3.4 İnceleme ve Analiz

Elektronik delil inceleme, verilerin toplanması safhasında elde edilen tüm verilerin içinden soruşturma konusu olaya ilişkin verilerin çıkarılması işlemidir. İnceleme aşaması, silinmiş veya zarar görmüş verilerin kurtarılması, verinin tasnif edilmesi ve veriler üzerinde içerik araştırmasını kapsamaktadır (Değirmenci, 2014).

İnceleme ve analiz, aygıt üzerindeki verilerin gözden geçirilmesi şeklinde olabileceği gibi veriler içerisinde bir takım yazılımlar kullanarak otomatik arama şeklinde de gerçekleştirilebilmektedir. Bu yazılımlar ile olayın türüne göre şüphe içeren kelime aranması, şifreleme yapılmış ve silinmiş verilerin kurtarılması, disk üzerinde tanımlanmış veya tanımlanmamış bölgelerde bulunan gizli verilerin bulunması gibi işlemler de yapılabilmektedir.

Bu aşamada, bilgisayar ortamında bulunan dijital verilerin hassasiyetine önem verilmeli ve veri elde etme sürecinde problemleri azaltacak araç ve gereçleri kullanmalıdır.

İnceleme ve analiz aşaması, teknik bilginin en çok kullanıldığı ve en uzun süren aşamadır. Adli bilişim uzmanı inceleyeceği medyada ne aranacağını iyi bilmeli ve ona göre yöntem ve usuller kullanmalıdır. Her suç tipi için ayrı bir yöntem geliştirmeli ve üzerinde çalışılan vaka ile ilgili önceden mutlaka bilgilendirilmelidir. Örnek olarak, uyuşturucu ticareti olayı ile ilgili el konulan elektronik materyallerde yapılacak inceleme ile bilişim sistemi yoluyla dolandırıcılık suçu kapsamında yapılan inceleme işlemi farklılık göstermektedir. Bu sebeple üzerinde çalışılan vaka ile ilgili detaylar soruşturma biriminden talep edilmelidir (Başar, 2015).

3.1.3.5 Raporlama

Adli bilişim sürecinin son aşamasını raporlama bölümü oluşturmaktadır. Bu aşama, mahkemelerde görünen kısım olması sebebi ile bir hayli önemlidir. Bu nedenle; rapor teknik bir rapor olsa da anlatılacak hususlar bir herkes tarafından anlaşılabilecek yalınlıkta olmalıdır. Adli bilişim uzmanı, her aşamada karşılaşılan tüm detayları belgelendirmelidir. Bu belgelendirme bazen video kamera ile kaydetme, bazı durumlarda fotoğraf çekme şeklinde olabileceği gibi, bazı durumlarda da not alma şeklinde olabilmektedir. Adli makamlar açısından bir adli bilişim raporunda aşağıdaki detaylar mutlaka bulunmalıdır;

- “Olay tarihi, zaman ve adres bilgileri”,
- “Donanımların üretici, seri numarası, modeli, unsurları gibi sisteme ait bilgiler”,
- “Verilerin toplanması esnasında sistemin durumuna ilişkin bilgiler”,
- “Olaya ilişkin dosya numarası, şikâyetçi veya şüpheli gibi bilgiler”,

- “Verinin analiz edilmesi esnasında tüm aşamalar ve özellikle kullanılan araçlar, süreçler, konular, hata mesajları gibi bilgiler”,
- “Olay yerinden toplanan fotoğraflar ve fiziksel deliller varsa tanık bilgileri” (Özmestik, 2015).

3.2 Dijital Delil Kavramı ve İnceleme Yöntemleri

3.2.1 Dijital Delillerin Tanımlanması

Bir suçun soruşturma ve kovuşturma evresinde en önemli faaliyet, meydana gelen olayla ilgili delillerin elde edilmesidir. Türk Dil Kurumu, delil kavramını “insanı aradığı gerçeğe ulaştırabilecek iz, emare” olarak tanımlarken, Polisin Adlî Görevlerinin Yerine Getirilmesinde Delillerin Toplanması, Muhafazası ve İlgili Yerlere Gönderilmesi Hakkında Yönetmelikte “meydana gelen bir suçun aydınlatılması ve suç sanıklarının tespitine yarayan her türlü ispat vasıtası” olarak tanımlanmıştır (Karabulut, Karapazarlıoğlu, & Tosun, 2015).

Ceza muhakemesinde amaç; “meydana gelen somut olayla ilgili maddî gerçeğe ulaşmak ve hiçbir kuşkuya yer bırakmayacak şekilde olayın delillerle ispat edilmesini sağlamaktır.” Bu sebeple suç olarak tanımlanmış olay ile ilgili olarak elde edilen deliller itiraza mahal vermeyecek şekilde bir takım özelliklere sahip olması gerekmektedir (Parlar, Yüksel, & Hatipoğlu, 2008).

Bu kapsamda delillerde bulunması gereken özellikler şu şekilde sıralanabilir (Kılıç, 2014);

- Kanuna uygun olarak elde edilmiş olmalıdır.
- Maddi gerçeğin ortaya çıkarılmasına aracılık etmelidir.
- Doğruluğu ve geçerliliği konusunda şüphe içermemelidir.
- Delil ve delil ile ilgili rapor herkese açık olmalıdır.
- Mümkünse farklı deliller ile desteklenebilmelidir.

Genel olarak tanımlanmış bu özellikler adli bilişim kapsamında incelenecek olan deliller içinde geçerlidir.

Elle dokunulamayan, ancak bilgisayar sistemleri yardımıyla görülebilen, bilgisayar medyaları üzerine depolanabilen ve bilgisayar medyaları veya sistemleri ile taşınabilen elektronik veriler ile sanal dünyanın parmak izleri, emareleri arasında

tanımlanan IP ve veri trafik bilgisi gibi veriler dijital delillere verilebilecek örneklerdir (Henkoğlu, 2011).

Elektronik delil elde edilmesinin birinci basamağını oluşturan elektronik delillerin tanımlanması, bu delillerin suç tipi ve suç mahalli dikkate alınarak nerelerde olabileceğinin tanımlanması anlamına gelmektedir (Orta, 2015).

Bununla beraber elektronik delil ifadesi hem elektronik cihazı hem de bu cihaz içerisindeki dijital verileri kapsamaktadır. Bu bağlamda elektronik delil tanımlaması yapıldığında, olay yerinden elde edilen dijital medyalar (laptop, masaüstü bilgisayar, hardisk, flash bellek, CD/DVD, mp3 çalar vb.) ile bu elektronik cihazların içerisinde dijital olarak bulunan veriyi ifade ettiği anlaşılmalıdır (Kılıç, 2014).

Elektronik delillerin tanımlanması için bir standart oluşturmak, delillerin somut olmaması sebebiyle kolay olmamaktadır. Bu sebeple elektronik deliller, meydana gelen olayın kendi içinde barındırdığı özel şartlara bağlı olarak değerlendirilmelidir.

3.2.2 Dijital Delillerin Niteliği

Duyu organlarımızla algılayamadığımız, ancak metafizik gibi ispat edilemeyecek bir yapıda da olmayan dijital deliller, kağıt üzerinde bulunan fiziki delillerden yapısal olarak çok farklıdır. Bu delillere ulaşım ancak elektrik enerjisi ve bir takım yardımcı araçlar ile mümkündür. Dijital delillerin sahip olması gereken özellikleri sıralamadan önce, dijital verilerin yapısal özelliklerini incelemekte fayda vardır. Bu özellikler şu şekilde sıralanabilir;

- Dijital veriler, kolaylıkla kopyalanabilir ve çoğaltılabilirler.
- Dijital veriler, manyetik alan, sıcaklık, nem gibi nedenler ile bozulabilirler.
- Dijital veriler, üzerlerinde işlem yapılarak kolaylıkla değiştirilebilirler.
- Dijital veriler, tekrar elde edilemeyecek şekilde silinebilirler.
- Dijital veriler, gizlenmiş veya şifrelenmiş başka verileri üzerinde barındırabilirler (Göksoy, 2017).

Yukarıda belirtilen özellikler ile dijital deliller ile diğer deliller arasındaki yapısal fark ortaya konulmaktadır. Dijital verilerin yapıları gereği manipüle edilmeleri kolay olduğundan dijital delil olarak edilebilmesi için değiştirilmemiş olduklarının ispat edilmesi gerekmektedir. Bununla beraber dijital delilin aşağıda sıralanmış genel kabul gören unsurları da taşıması gerekmektedir.

- Akla uygun ve kabul edilebilir olmalıdır.
- Gerçek ve hakiki olmalıdır.
- Hatasız ve doğru olmalıdır.
- Eksiksiz ve tam olmalıdır.
- Güvenilir ve itimat edilebilir olmalıdır.
- İnandırıcı olmalıdır.
- Tekrar edilebilir olmalıdır.
- Mevcut yasal düzenlemelere uydun olmalıdır (Göksoy, 2017).

3.2.3 Dijital Delil Kaynakları

Dijital delillerin elde edilmesinde, delillerin bulunması muhtemel yerlerin, bu verileri işleyen ve saklayan bileşenlerin neler olduğunun, bunların ne şekilde işlendiğinin, depolandığının ve iletildiğinin bilinmesinin hayati öneme sahip olduğu söylenebilir.

Dijital deliller, elektronik ortamın yer aldığı bilişim sisteminde ve bu sistem ile birlikte kullanılan cihazlar üzerinde yer alır. Verinin iletimi gündeme geldiğinde ise kimi zaman iletim cihazları üzerinde aktarılan verinin kendisi kimi zaman da iletim bilgileri delil olabilmektedir (Orta, 2015).

3.2.3.1 Bilgisayar Sistemleri

Bilgisayar sistemleri ve bileşenleri, dijital delillerin elde edilmesinde kullanılan en önemli kaynaklardan biridir. Belgeler, fotoğraflar, e-postalar, veri tabanları, finansal bilgiler, sohbet kayıtları, internet erişim günlükleri ve sistem olay günlükleri bilgisayar sistemleri üzerinden elde edilebilecek potansiyel delillerden bazılarıdır (Henkoğlu, 2011).

3.2.3.2 Veri Depolama Aygıtları

Dijital verilerin kalıcı veya geçici olarak depolandığı birimler veri depolama aygıtları olarak adlandırılırlar. Kullanım amacına bağlı olarak farklı şekil ve kapasitelerde olabilmektedirler. Bu birimlere örnek olarak; sabit diskler, taşınabilir sabit diskler, ağ diskleri, flash bellekler, bellek kartları, optik diskler (CD/DVD), disketler, veri kasetleri, akıllı kartlar, sim kartla verilebilir. Veri depolama aygıtları

dijital delil elde edebilecek en önemli kaynaklar olup bu aygıtlar üzerinden elde edilen bulgulardan, soruşturma ve kovuşturma evrelerinde her aşamada (olay yeri incelemesi, analiz ve raporlandırma) faydalanılmaktadır (Henkoğlu, 2011).

3.2.3.3 Bilgisayar Ağları

Bilgisayar ağı, iki veya daha fazla bilgisayar sisteminin bilgi paylaşımı amacıyla kablolu veya kablosuz olarak birbirinde bağlantı kurması ile oluşur. Bu ağlardaki veriler akış halinde olan verilerdir. Bu nedenle bu verilerden delil elde edilmek istendiğinde, gerçek zamanlı inceleme yani ağ trafiği gerçekleşirken yapılması gerekmektedir (Değirmenci, 2014).

Bilgisayar ağ sistemleri üzerinde yapılan incelemeler ile ağ üzerinde çalışmakta olan uygulama, hizmet veya kullanıcılar yanında, kullanıcıların bazı ilave bilgilerine (işletim sistemi, tarayıcı programı, bağlantıda bulunulan diğer cihazlara ait diğer yazılımsal ve donanımsal bilgiler) de erişilebilir. Ağ üzerinde yapılan inceleme sonucunda ulaşılabilecek veriler şunlardır (Ercan & Nacak, 2009);

- Ağ yapısı ve altyapısı,
- Ağ üzerindeki çeşitli kaynaklara erişim durumu,
- Bağlantılı bulunan diğer ağlara yetkisiz geçişler.

Bilgisayar ile ağ donanımları arasında tanımlayıcı olan IP adresi ve MAC adresi gibi tanımlayıcı bilgiler kullanılarak önemli dijital delillere ulaşılması mümkün olabilmektedir (Henkoğlu, 2011).

3.2.3.4 Mobil Cihazlar

İletişim teknolojilerindeki gelişmeler, uzak mesafeleri kısaltmış, hatta ortadan kaldırmıştır. Dünyada giderek artan mobil telefon kullanımı, birçok iletişim kolaylığını da beraberinde getirmiştir. Bu durum günlük hayatı önemli ölçüde etkilemiştir. Mobil telefonlar hayatımıza ilk girdiğinde sadece mobil olma özelliği ve iletişim hızını hayatın her alanına taşıyabilme özelliği ile ön plana çıkmışken, günümüzde bilişim teknolojilerinin gelişmesiyle akıllı özelliği taşıyan mobil telefonunlar, birçok farklı özellikleri ile dikkat çekmeye başlamıştır (Karaaslan & Budak, 2012).

Her geçen gün yeni bir gelişmenin kaydedildiği iletişim sektöründe, mobil hatlar üzerinden yalnız ses hizmeti değil, aynı zamanda genişbant data hizmetleri de kolaylıkla sunulur hale gelmiştir (Çakır & Kılıç, 2013).

Teknolojik açıdan hızla gelişmekte olan cep telefonu, PDA ve tablet gibi mobil cihazlar bilişim suçlarında her geçen gün daha fazla kullanılmaya başlanmıştır. Bu nedenle adli bilişimin sık karşılaştığı bir delil kaynağı haline gelmektedir. Mobil cihazlar üzerinde adli bilişim, diğer medya araçları ile karşılaştırıldığında daha zor bir süreci içermektedir. Ancak genel olarak, bilişim sistemlerine uygulanan analiz yöntemleri cep telefonları için de geçerlidir (Orta, 2015).

3.2.3.5 Gömülü Sistemler

Gömülü sistemler; herhangi bir basit sisteme akıllılık özelliğini kazandıran elektronik donanım ve yazılımdan oluşan bir bütünü tanımlamaktadır. Kullanıcı arayüzü bilgisayarlara nispeten kısıtlı olan bu sistemler bir işi yapmaları için tasarlanırlar ve sadece bu işi yaparlar.

Oyun konsolları, MP3 oynatıcılar, faks makineleri, yazıcılar, tarayıcılar ve GPS cihazları gömülü sistemlere örnek olarak verilebilirken teknolojinin ilerlemesi ile buzdolabı, çamaşır makinesi gibi evlerde günlük kullanılan eşyalarda dijital delil bulundurabilecek gömülü sistemler arasında yerlerini almışlardır.

3.2.3.6 Bulut Sistemler

Son yıllarda kullanımı popüler hale gelen bir teknoloji olan bulut teknolojisi, sanallaştırılmış karmaşık bir platform üzerinde büyük miktarda veri depolamaya imkan veren sistemlerdir.

Burada kullanıcı, alt yapı yatırım maliyetine girmeden, kiralama yolu ile hizmet sağlayıcısının sunduğu ortak alt yapıyı kullanarak, ihtiyaç duyduğu yazılım ve donanım servislerini bilişim ağı üzerinden kullanabilmektedir.

Bulut teknolojilerin ve kullanım alanlarının hızlı bir şekilde artması, bu sistemleri suçlular ve suç örgütleri için de cazip hale getirmiştir. İnternetin kullanım alanlarındaki artış ve yüksek hızlı erişim imkanları, kullanıcının her hangi bir bilgisayar, tablet ya da akıllı telefon üzerinden istedikleri internet kaynağına dolayısıyla bulut sistemlere erişimini kolaylaştırmaktadır. Bu durum özellikle siber

suçlar ve sağladığı depolama imkanı ile klasik suç tipleri için bulut bilişimi elverişli yeni bir saha haline getirmiştir (Emekci, Kuğu, & Temiztürk, 2016).

Ancak bulut sistemlerin sanal bir ortamda dağıtık veri işleme modeli, dinamik altyapı topolojisi, farklı ülkelere dağılan veri merkezleri, üzerinde bulunan kaynağın çok sayıda kullanıcı arasında paylaşılarak kullanılması gibi özelliklerinden dolayı bulut sistemlerde yürütülen soruşturmalar daha karmaşık prosedürlere sahiptir. Geleneksel adli bilişim teknikleri ile bulut bilişim ortamlarında karşılaşılan sorunlar tam olarak çözülemeyeceği için; adli bilişime, yeni bir bakış açısı kazandırmaya yönelik çalışmalar yapılmalıdır (Kaya, 2016).

3.3 Dijital Delil İnceleme ve Analiz Yöntemleri

Adli bilişim uzmanları delil elde etmek amacıyla, bilişim sistemlerini, medya aygıtlarını, bilişim ağ cihazlarını, internet ve kapalı ağ sistemlerini araştırması gerekmektedir. Bu işlem yapılırken, deliller cihazların he zaman kullanılan aktif kısımlarında bulunabileceği gibi silinmiş kısımlarında, atık alanlarında ya da gizli yerlerinde açık veya şifrelenmiş şekilde bulunabilmektedir (Orta, 2015).

Tüm bu alanlarda delilleri bulmak ve çıkarmak için adli bilişimin bir takım uygun yöntemler kullanması gerekmektedir. Böylece elde edilen deliller ile suçun aydınlatılması ve maddi gerçeğe ulaşılmasını beklenebilecektir. Dijital delillerin bulunabileceği ortamlardan bozulmadan ve zarar vermeden toplamak, koruma altına almak, incelemek ve nihayetinde yargı makamlarına sunmak gibi işlemler ancak belli teknik prensipler ışında yapılmalıdır (Ekizer, 2014).

Adli bilişim uzmanları bilişim suçunun delillerini ortaya koymak için verileri toplar, analiz eder ve raporlayarak yargı makamlarına sunar. Adli bilişim uzmanları tarafından bütün bunlar yapılırken bilimsel gerçekleri göz ardı etmemeleri beklendiği gibi adli bilişim metodolojilerini de takip etmeleri gerekmektedir (Orta, 2015).

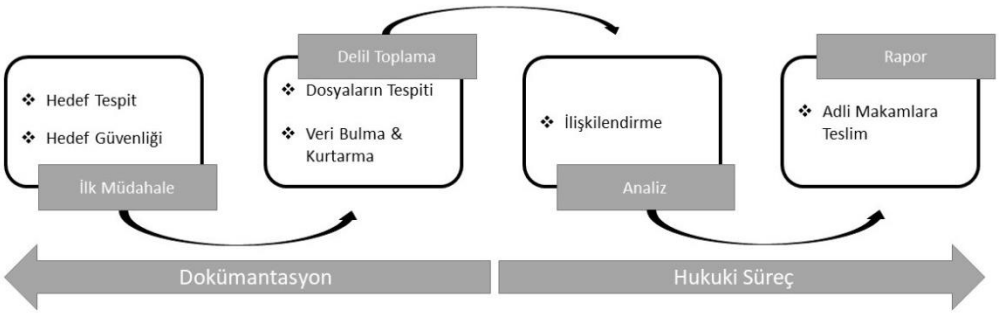
Elektronik delil inceleme aşamasında, verilerin toplanması safhasında elde edilen tüm verilerin içinden soruşturma konusu olaya ilişkin verilerin ayıklanması yapılır. Silinmiş veya zarar görmüş verilerin kurtarılması, verinin tasnif edilmesi ve veriler üzerinde içerik araştırması detaylı olarak yapılır (Değirmenci, 2014).

Elektronik verilerin delil haline getirilebilmesi için bir takım donanımlar ve yazılımlara ayrıca bu donanım ve yazılımı etkili bir şekilde kullanılabilmesi için deneyimli ve yetişmiş insan gücüne ihtiyaç duyulmaktadır (Çakır & Kılıç, 2013).

Adli bilişim donanım ve yazılımları, teknolojideki gelişmelerle birlikte günümüzde oldukça gelişmiştir. Adli bilişim uzmanları silinmiş dosyaları kurtarmak ve elde edilen verilerin üzerinde ileri düzey analiz işlemleri yapabilmek için bu donanım ve yazılımları kullanmaktadırlar. Kullanılan bu donanım ve yazılımlar, sonucu kesin olan, tekrarlanabilir ve tarafsız sonuçlar üretmelidir (Orta, 2015).

3.3.1 Dijital Delil İncelemede Kullanılan Ekipmanlar

Dijital delil incelemede kullanılan ekipmanlar, adli bilişim sürecinde kullanılan araç ve gereçlerden oluşmaktadır. Bu süreç Şekil 3.3'de görülen aşamalardan meydana gelmekte ve ilk müdahale yani olay yerine gidilmesi ile başlayıp, inceleme ve analizler sonucunda elde edilen bulguların ilgili adli makama sunulmasına kadar geçen safhaları içermektedir. Dolayısıyla tanımlama yapılacak olursa "adli bilişim ekipmanları, soruşturma ve kovuşturma ile ilintili olarak, dijital kayıt ortamında veri tutma ve işleme özelliği bulunan medyalardan delil elde etme amacıyla kullanılan yazılım, donanım veya ikisinin bir arada bulunduğu cihazlar ile diğer araç ve gereçlerdir" şeklinde tanımlanabilir (Bakan & Saluk, 2014).



Şekil 3.3.1.1: Adli Bilişim Süreçleri

Bu ekipmanlara tornavida setleri, bağlantı kabloları gibi yardımcı malzemelerden, bire bir kopyalama için kullanılan cihazlar ile inceleme aşamasında kullanılan yazılımlara, hatta teslim alınan maddi bulgunun inceleme sonrası geri gönderilmesi için kullanılacak özel zarf veya paketlere kadar kullanılan tüm araç ve gereçleri dahil etmek mümkündür.

Dijital delillerin toplanmasında, sınıflandırılmasında, paketlenmesinde ve nakledilmesinde kullanılacak araç-gereçlerin güncel olmasına dikkat edilmelidir. Teknoloji geliştikçe kullanılan araç ve gereçlerin gözden geçirilerek yenilenmeleri gerekmektedir (Berber, 2004).

Adli bilişimde kullanılan ekipmanların bazı standartlar taşıması ve testlerden geçirilmiş olması konunun hassasiyeti de düşünülecek olursa büyük öneme sahiptir. Ülkemizde bu konuda TSE bünyesinde yürütülen çalışmalar bulunsa da ekipmanları test edecek bir standart halen bulunmamaktadır. ABD'yi ele alacak olursak, adli bilişim alanında kullanılan yazılım ve cihazların testleri "Ulusal Standartlar ve Teknoloji Enstitüsü" tarafından yürütülen "Adli Bilişim Araç Testi" projesi kapsamında yapılmakta ve sonuçları internet sitesinde yayımlanmaktadır (Bakan & Saluk, 2014).

3.3.1.1 Yazma Koruma Ekipmanları

Dijital delillerin adli analiz sürecinin başlangıcı imaj alma işlemidir. Ancak verilerin depolandığı medyanın hasar görmesi ya da inceleme yapan kişi tarafından bilerek ya da bilmeyerek verilerin değiştirilebilmesi olasılığına karşı imaj alma işlemi esnasında yazma koruma ekipmanları kullanılır. Verilerin depolandığı medya birimi bu ekipmanlar kullanarak bilgisayar sistemine bağlandığında, bu medya üzerinde yazma işlemi gerçekleşmeden sadece okuma işlemi yapılmaktadır (Bakan & Saluk, 2014).

Tüm adli bilim dallarında olduğu gibi adli bilişimde de delillerin incelemeler sırasında değiştirilmemesi esastır. Bu esas doğrultusunda adli bilişim uzmanlarının gerekli tedbirleri alması ve mutlaka yazma koruma ekipmanı kullanması gerekmektedir.

Yazma koruma ekipmanları genellikle bir giriş, bir çıkış bir güç ünitesinden oluşurlar. Giriş kısmına imajı alınacak olan veri depolama birimi, çıkış kısmına ise bir sabit disk ya da bir bilgisayar bağlanır. Güç ünitesi ise giriş ve çıkış kısımlarına bağlanan cihazların çalıştırılmasını sağlar.

Yazma koruma ekipmanının giriş üniteleri genellikle IDE, SATA veya SCSI türünde olabilir. Çıkış ünitesi ise genellikle USB veya Firewire türünde olabilir. Adli

bilişim uzmanı inceleme yapılacak veri depolama birimi ve imajı alacağı veri depolama biriminin türüne göre uygun bağlantıyı yapmalıdır (Say, 2006).

Adli kopya alma esnasında bir donanım kullanmadan yazılımsal yazma koruma teknikleri ile verinin hash değeri değişmeden kopya almak mümkündür. Yazılımsal çözümler, BIOS üzerindeki INT 13h kodunu engelleyerek bunu gerçekleştirmektedir. Ancak, BIOS kontrollerini etkisiz hale getirmek mümkün olduğundan yazılımsal yazma koruma teknikleri pek tercih edilmemektedir (Bakan & Saluk, 2014).

Aşağıda yazma koruma donanım ve yazılımlarına genel özellikleri ile bazı örnekler verilmiştir.

Tableau yazma koruma Cihazları; ABD'de kurulu bulunan Guidance Software firmasının markasıdır. 1997 yılında kurulan Guidance Software, eDiscovery, data discovery ve adli bilişim alanında sunduğu yazılım ve donanım çözümleri ile dünya çapında kolluk kuvvetleri, özel şirketler ve adli bilişim hizmeti veren pek çok özel kuruluşa çözümler sağlamaktadır. Çeşitli modelleri bulunmaktadır (EMT Electronics, 2018).

Tableau T35u, IDE/SATA sabit sürücüler için yazma koruma sağlayan USB 3.0 bağlantısı ile hızlı veri aktarımı yapabilen yazma koruma kiti modelidir. Şekil 3.4'de T35u modelinin genel bir görünümü bulunmaktadır. Model taşınabilir bir modeldir.

Şekil 3.3.1.1.1: Tableau T35u Yazma Koruma Köprü Kiti

Tableau T6u SAS yazma koruma köprü kiti özellikle SAS veri depolama birimlerinden da hızlı veri aktarımına yönelik geliştirilmiştir. Tableau T6es modelinin yerini almıştır. Saniyede 200 MB veri aktarımı yapabilmektedir (Opentext, 2018).

Şekil 3.3.1.1.2: Tableau T6u Yazma Koruma Köprü Kiti SAS Disk Bağlantısı

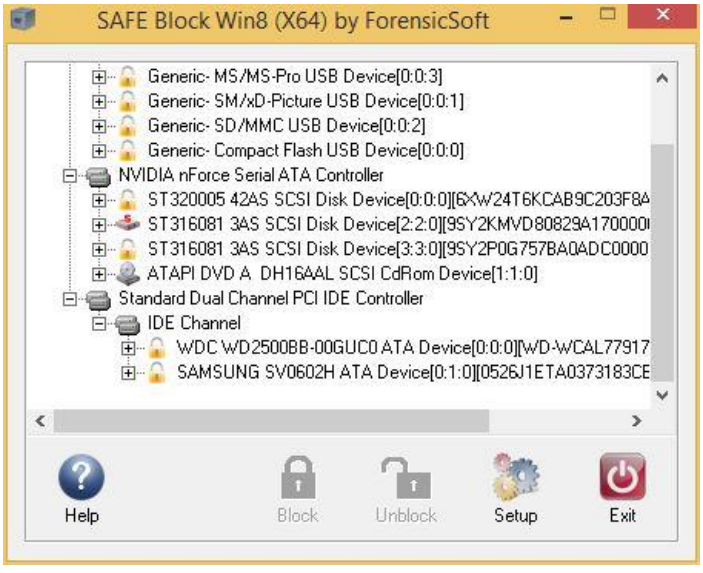
Tableau T356789iu modeli, iş istasyonu tipi bilgisayarlar için OEM olarak üretilmiş yazma koruma donanımıdır. “IDE, SATA, SAS, USB 3.0/2.0/1.1 ve FireWire 800/400” gibi birçok bağlantıya izin vermektedir. T35689iu modelinin yerini almıştır. Bilgisayara USB 3.0 bağlantısı ile bağlanmaktadır (EMT Electronics, 2018).

Şekil 3.3.1.1.3: Tableau T35689iu Forensic SATA/IDE Bridge Modeli

WiebeTech yazma koruma cihazları; Amerika’da kurulu bulunan CRU firmasının bir markasıdır ve çeşitli modelleri bulunmaktadır. Forensic UltraDock v5.5 modeli “PATA/IDE ve SATA diskleri” desteklemekte ayrıca farklı disk modelleri için adaptör desteği sunmaktadır. Üzerinde bulunan ekranda, bağlantı yapılan disk bilgileri görülebilmektedir. Bağlanan disk üzerinde HPA ve DCO alanlarına erişim sağlanabilmekte ve değişiklik yapılabilmektedir. Bilgisayara “USB 3.0/2.0, eSATA, FireWire 400/800 bağlantıları” ile bağlanabilmektedir (CRU, 2019).

Şekil 3.3.1.1.4: CRU WiebeTech Forensic UltraDock v.5.5 Modeli

SAFE Block Yazma Koruma yazılımı; Amerika'da kurulu bulunan ForensicSoft firması tarafından geliştirilmiştir. Windows tabanlı çalışan yazma koruma yazılımı, bilgisayara "IDE (PATA&SATA), SCSI, FC, SAS, USB ve IEEE1394" yolu ile bağlanan tüm medyalar için yazma koruması yapabilmektedir. Windows tabanlı çalışan tüm imaj alma yazılımları ile uyumludur. Aynı anda istenildiği kadar veri depolama birimi için yazma koruması yapılabilmektedir (ForensicSoft, 2016).



Şekil 3.3.1.1.5: SAFE Block Yazma Koruma Yazılımı

Windows XP SP2'den itibaren kayıt defteri ayarlarından USB yazma koruması yapılabilmektedir. Ayrıca bazı USB bellek ve SD kartlar üzerinde "Lock" düğmesi gibi yazma koruma sağlayan düğmeler bulunmaktadır. Bu düğmeler kullanılarak da yazma koruma yapılabilmektedir. Ancak adli bilişim için kullanılan donanımsal

yazma koruma ekipmanlarının kullanılması daha güvenilir bir yol olacaktır (Bakan & Saluk, 2014).

3.3.1.2 İmaj Alma Ekipmanları

Elektronik delillerin hukuken güvenilebilir ve inanılabilir olmaları için elde edilen delil üzerinde doğrudan çalışmamak gerekmektedir. Yapılacak incelemeler delil üzerinden alınan bire bir kopya üzerinden yapılmalıdır. Adli bilişimde yapılan bu bire bir kopyalama işlemine imaj alma işlemi denilmektedir (Duman, 2012).

Bire bir kopya, delil elde edilecek medya üzerindeki bütün verilerin eksiksiz kopyasının alınması anlamına gelmektedir. Alınmış olan bire bir kopya; mevcut ve silinmiş verileri, tanımlanmış ya da tanımlanmamış bölümleri, kısaca veri depolama biriminde bulunan diğer tüm alanları kapsar. Bire bir kopyalama sırasında orijinal medya üzerinde herhangi bir değişiklik meydana gelmemelidir (Bakan & Saluk, 2014).

Aşağıda imaj alma donanım ve yazılımlarına genel özellikleri ile bazı örnekler verilmiştir.

Forensic Falcon Neo; Amerika'da kurulu bulunan LogiCube firması tarafından geliştirilmiştir. Kullanılan disk ve imaj olarak alınacak formata bağlı olarak imaj alma hızı 50 GB/dk kapasiteye kadar çıkabilmektedir. Ham ve bire bir kopya, dd imaj, dmg imaj, e01, ex01 gibi farklı formatları destekler. MD5, SHA1, SHA256 ve dual-hash (MD5+SHA-1) doğrulamalarını destekler. İmaj alma için yazma korumalı iki adet SAS/SATA portu, bir adet USB 3.0 portu ve bir adet PCIe portu bulunmaktadır. İmajın kayıt edileceği hedef için iki adet SAS/SATA portu, iki adet sadece SATA portu, bir adet USB 3.0 portu ve bir adet PCIe portu bulunmaktadır. iki adet 10GbE ağ portu bulunmaktadır. USB portları adaptör ile SATA'ya çevrilebilmektedir. Bir taraftan bir hedef diske wipe işlemi yaparken, diğer taraftan başka bir hedef diske imaj alma gibi 5 işlemi eşzamanlı olarak yapabilmektedir (LogiCube, 2018).

Web tabanlı kullanıcı ara yüzü, kullanıcılara web tarayıcı ile cihaza bağlanabilme ve uzaktan cihazı kontrol edebilme imkanı vermektedir. Ayrıca ağ üzerinde cihaza bağlı kaynağa erişim imkanı veya ağ üzerinde cihaza bağlı kaynağın imajını gönderebilme imkanı bulunmaktadır. Paralel imaj (aynı kaynaktan, farklı hedeflere farklı formatlarda) imaj alınabilmektedir. Örneğin ağ üzerindeki bir hedefe

e01 formatında imaj alırken, aynı anda hedef diske ham halde imaj alınabilmektedir. Ayrıca cihazın imaj alma esnasında eş zamanlı olarak doğrulama işlemi yapması, toplam imaj alma süresini yarı yarıya kadar kısaltabilmektedir (Bakan & Saluk, 2014).

Şekil 3.3.1.2.1: Forensic Falcon Neo İmaj Alma Cihazı

Tableau TD2u; Amerika'da kurulu bulunan Guidance Software firmasının geliştirdiği bir imaj alma cihazıdır. IDE/SATA sabit sürücüler ve USB 3.0 harici sürücüler veya flash medyalardan yazma korumalı olarak ex01, e01, Raw/DD veya dmg formatlarında adli imaj alınmasını veya disk klonlanmasını, ayrıca güvenli veri silme (wipe) işlemlerini sağlayan bir cihazdır (Opentext, 2018).

Şekil 3.3.1.2.2: Tableau TD2u İmaj Alma Cihazı

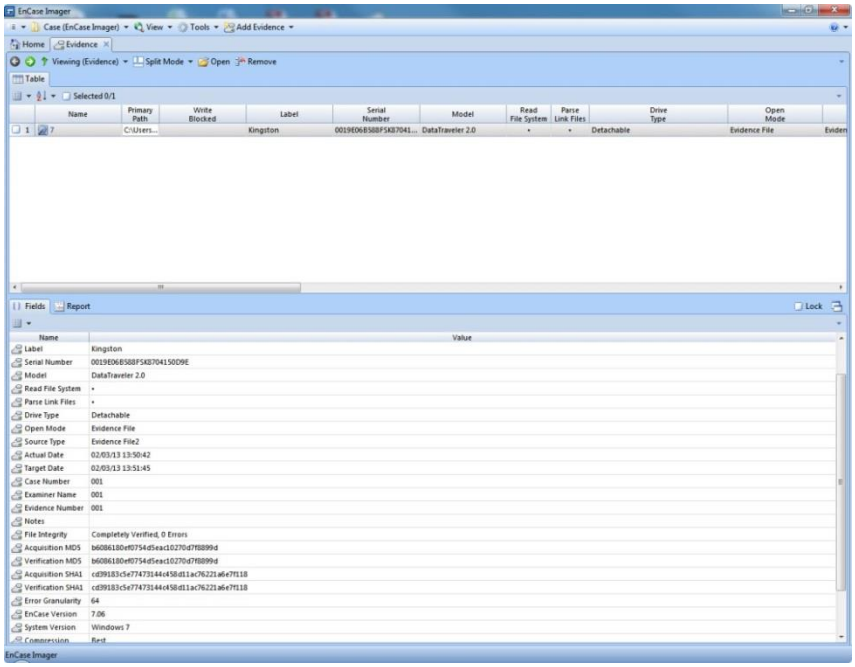
Kullanılan diske ve imaj olarak alınacak formata bağlı olarak imaj alma hızı 15 GB/dk kapasiteye kadar çıkabilmektedir. Tableau TD2 modelinin yerini almıştır. Diskten diske, diskten dosyaya, tek diske veya iki diske imaj alabilmektedir. Disk formatlama, wipe işlemi, MD5 ve SHA hash değeri alma, HPA/DCO tespiti ve boş disk kontrolü yapabilmektedir (Opentext, 2018).

Forensic Toolkit (FTK) Imager imaj alma yazılımı; Amerika Birleşik Devletleri'nde kurulu olan AccessData firması tarafından geliştirilmiş olup, firmanın internet sayfasından ücret ödemeden indirilerek kullanılabilen imaj alma ve ön

izleme yazılımıdır. Bu yazılım ile yerel sabit sürücülerin, flash belleklerin, kompakt disklerin, dizinleri ya da tek bir dosyanın imajı alınabilmektedir. Bununla birlikte bu yazılım ile ortamlardaki dijital delillerin imajını alınmadan ön izlenmesine de yapılabilmektedir.

FTK Imager yazılımı, farklı bir yazılım veya donanım kullanılarak alınan imajın üzerinde analiz yapılmasına da imkân vermektedir. Yazılım disk imaj dosyalarını read-only olarak mount edip, Windows Explorer üzerinden bu imajların bir sabit disk sürücüsüymüş gibi işlem görmesine de ortam hazırlayarak imaj dosyaları içinden dizin ya da dosyaların dışarı kopyalanmasına imkan tanımaktadır (Öztürkci, 2014).

Encase Forensic Imager; Amarika'da kurulu bulunan Guidance Software firmasının geliştirdiği ve sitesinden ücretsiz olarak indirilebilen imaj alma yazılımıdır. Yazılım ile dört temel formatta imaj alınabilmektedir. (ex01, Lx01, e01, L01). ATA-6 ve üstü disklerde HPA ve DCO bölümlerine erişim sağlanabilmektedir. Yazılım, imaj alındıktan sonra imajın doğrulamasını yapmaktadır (Bakan & Saluk, 2014).



Şekil 3.3.1.2.3: Encase Forensic Imager İmaj Alma Yazılımı

3.3.2 Disk İmajı Alma İşlemi

İmaj alma işlemi "orijinal medyada bulunan tüm bilgilerin bit düzeyinde bire bir olarak yeni bir medyaya kopyalanması olarak" tanımlanabilir. Disk imajının alınması işlemi, dijital deliller üzerinde adli analiz sürecinin başlangıcıdır. Disk

imajının usulüne uygun bir şekilde alınması, tüm adli süreci etkileyebilecek kadar önemli bir konudur (Henkoğlu, 2011).

İmaj alma işlemi sonucunda elde edilen kopya "Forensic Duplicate" (adli kopya) olarak adlandırılmaktadır. İmaj alma işlemi, bu işlem için tasarlanmış donanımlarla gerçekleştirilebileceği gibi özel yazılımlarla da gerçekleştirilebilmektedir. Fakat donanım tabanlı sistemlerin kullanımı daha güvenilir olması nedeniyle daha fazla tercih edilmektedir (Kiçeci, 2014).

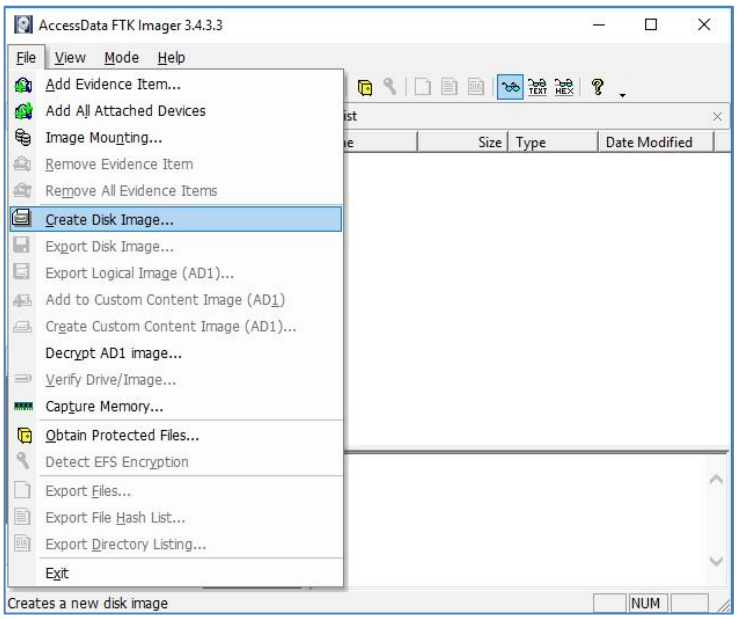
Medya imajının genel kabul görmüş adli bilişim standartlarına uygun olarak alınması, dijital delillerin elde edilebilmesi ve analizi sürecinin doğru başlayabilmesi ve sonuçlandırılması ile yakın ilişki içerisindedir. Bu sürecin doğru işlemesi, mahkemede dijital delillerin niteliklerine gölge düşmeyecek şekilde sunulması ve doğru kararların verilmesine etki edecektir (Henkoğlu, 2011).

Bununla birlikte verilerin elde edildiği kaynak ile imaj olarak alınan kopyanın aynı olduğunun doğrulanması beklenmektedir. Bu nedenle ele geçirilen bütün elektronik verilerin hash değerleri alınmalı ve hazır bulunan taraflara imzalatılmalıdır. Bu işlem daha sonra yapılacak itirazların önüne geçecektir (Orta, 2015).

Disk imajı, diskten diske veya diskten dosyaya şeklinde iki şekilde alınabilmektedir. Diskten diske imaj alma işleminde kaynak disk tamamen hedef diske kopyalanır, diskten dosyaya kopyalama işleminde ise kaynak diskin imajı, mantıksal bir veri dosyasına kopyalanır. Kopyalanan imaj faklı formatlarda olabilmektedir. Bu formatları genel olarak bit-copy ve bit-copy-plus olarak ikiye ayırabiliriz. Bit-copy format ham (raw) formattır ve bu imaj dosyasında sadece diskin imajı bulunur. Bu format tüm yazılımların tanıdığı bir formattır. Ancak bu formatta ekstra bilgi yoktur. Bit-copy-plus formatı ise imaj işlemi ile ilgili üst verilerin de (meta data) oluşturulduğu formattır (Kiçeci, 2014).

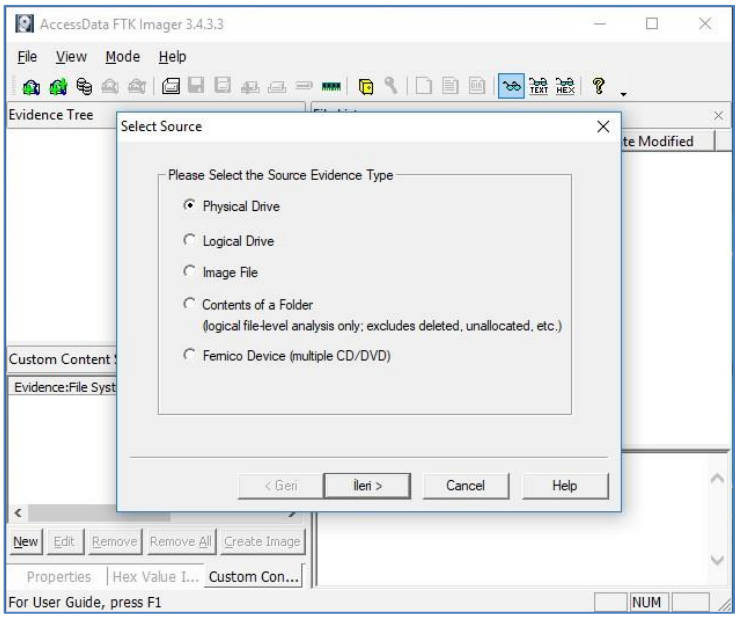
Dünyada yaygın olarak kullanılmakta olan ve üretici firma AccessData'nın internet sitesi üzerinden ücretsiz olarak indirilebilen FTK Imager programının 3.4.3.3 versiyonu üzerinden adli imaj alma işlemi aşamaları aşağıda sıra ile gösterilmiştir.

1. Uygulama yönetici olarak çalıştırılır. "File" menüsünden "Create Disk Image" seçeneğini seçerek disk imajı oluşturma işlemine geçiyoruz. (Şekil Şekil 3.3.2.1)



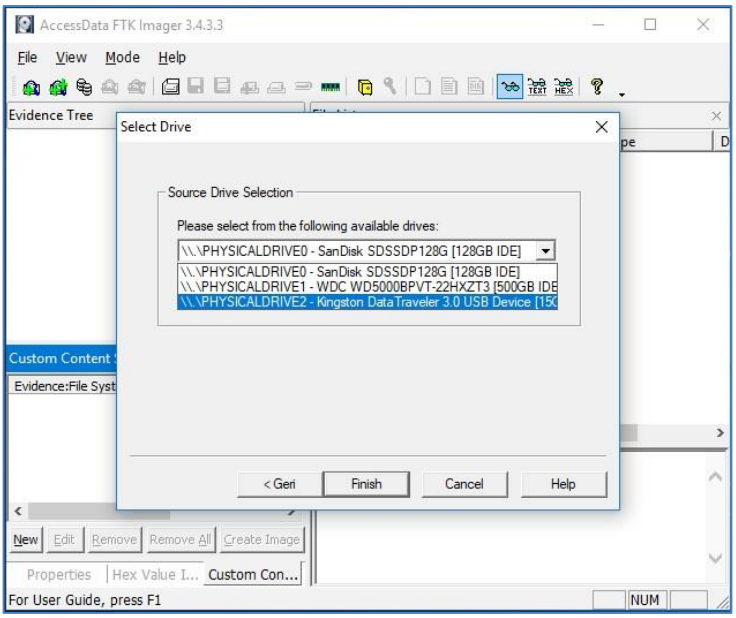
Şekil 3.3.2.1: FTK Imager Disk İmajı Alma Aşama 1

2. Gelen pencereden Physical Drive seçeneği seçilir. (Şekil 3.3.2.2)



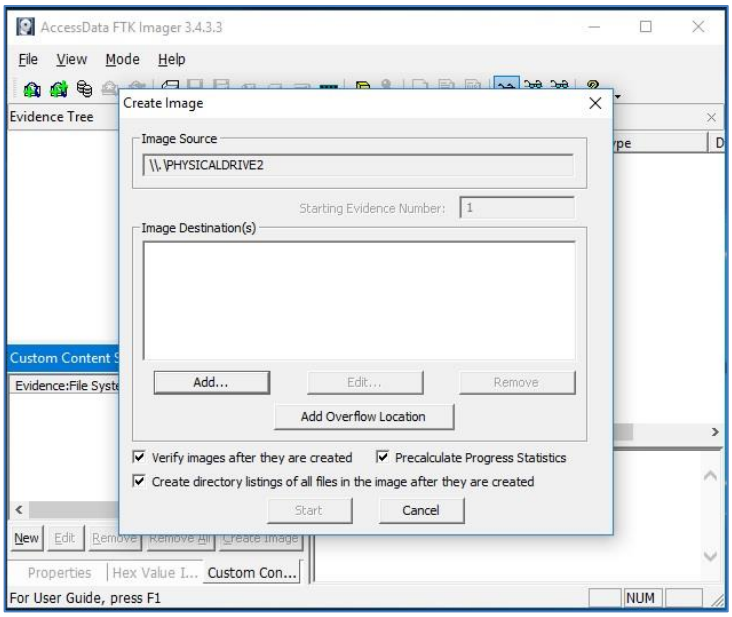
Şekil 3.3.2.2: FTK Imager Disk İmajı Alma Aşama 2

3. Gelen pencerede hangi diskin imajı alınacaksa o disk seçilir. (Şekil 3.3.2.3)



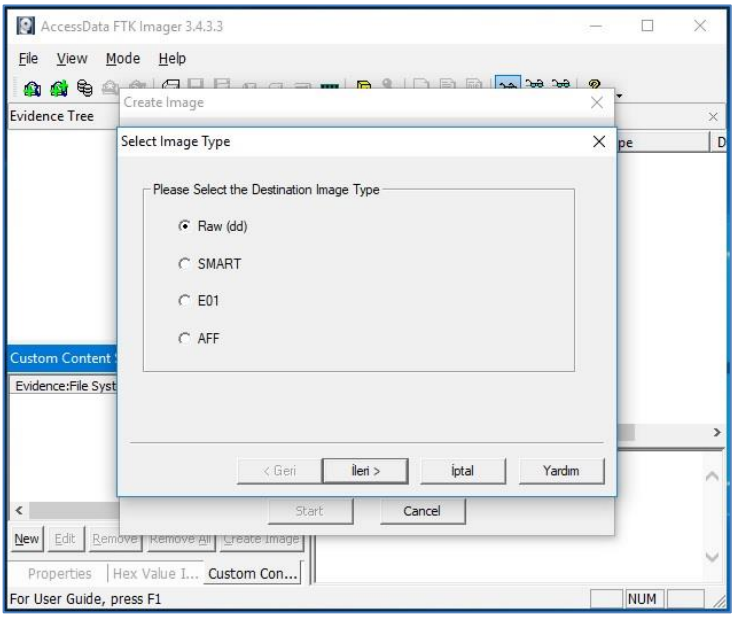
Şekil 3.3.2.3: FTK Imager Disk İmajı Alma Aşama 3

4. Açılan pencerede alınacak imajın nereye kaydedileceği belirlenir. Burada “Verify images after they are created” seçilir ise, imaj oluşturulduktan sonra bir doğrulama işlemi yapılacaktır. Doğrulama işlemi, imaj alma süresini uzatacak bir işlemdir. “Precalculate Progress Statistics” seçeneği seçilmesi halinde yapılacak işlemlerin yaklaşık olarak ne kadar süreceği hesaplatılır. “Create directory listings of all files in the image after they are created” seçeneği seçilir ise, imaj alınacak diskin içinde yer alan dosyaların detayları raporlanır ve imajın kaydedileceği yere kaydedilir. Tercih edilen seçimler yapıldıktan sonra “Add” butonuna basarak oluşturacağımız imaj dosyasının formatını belirtebileceğimiz bir sonraki pencereye geçiyoruz. (Şekil 3.3.2.4)



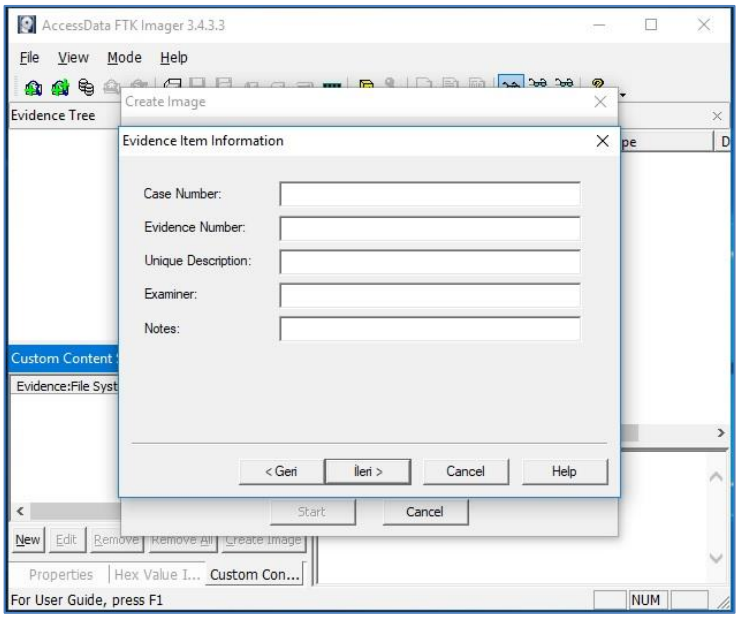
Şekil 3.3.2.4: FTK Imager Disk İmajı Alma Aşama 4

5. FTK Imager yazılımı ile 4 farklı formatta disk imajı oluşturabiliyoruz. Bunlar "Raw (dd) formatı", "SMART formatı", "E01 formatı" ve "AFF formatıdır". (Şekil 3.3.2.5)



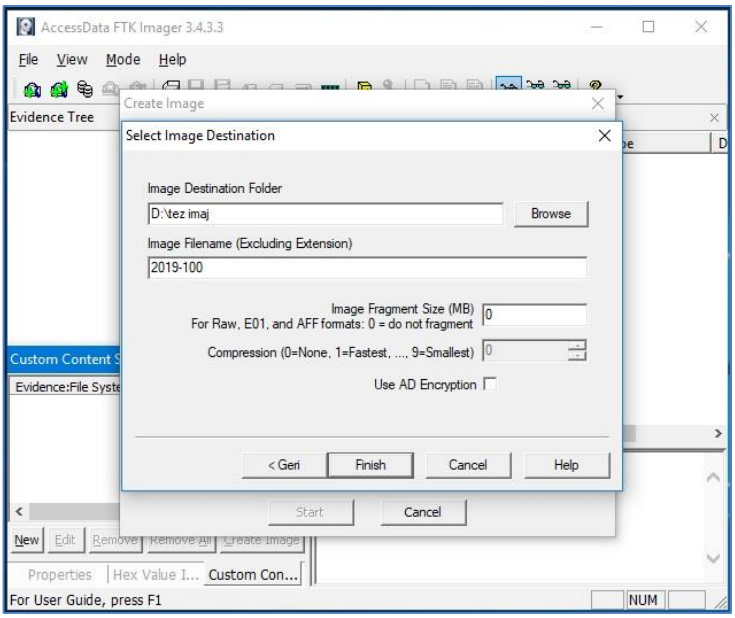
Şekil 3.3.2.5: FTK Imager Disk İmajı Alma Aşama 5

6. Tercih ettiğimiz formatı seçtikten sonra oluşturduğumuz imaj dosyası ile ilgili olarak “soruşturma numarası”, “delil numarası”, “imajı diğer imajlardan ayırt edebilecek bir isim veya numara”, “görevli personele ait bilgiler” ve “açıklama” gibi bilgileri girmemizi isteyen bir pencere karşımıza çıkmaktadır. Girilen bu bilgiler imaj dosyasının kaydedildiği dizinde yer alan ve imaj alma işlemi ile ilgili detayların yer aldığı text dosyasında yer alacaktır. (Şekil 3.3.2.6)



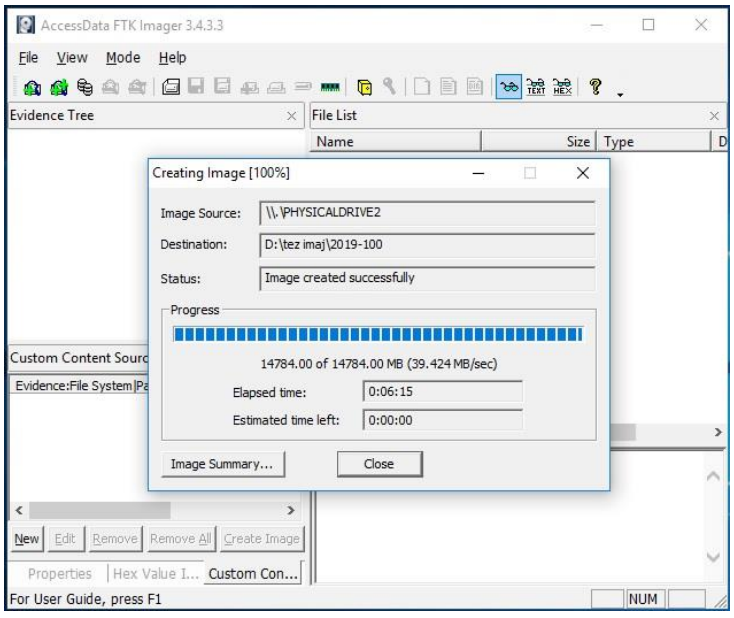
Şekil 3.3.2.6: FTK Imager Disk İmajı Alma Aşama 6

7. Gerekli bilgiler girildikten sonra “Select Image Destination” menüsü ekrana gelecektir. İmaj dosyasının nereye yazılacağını belirleyip imaj dosyasına bir isim verdikten sonra eğer dosya parçalara bölünecekse her imaj dosyasının kaç MB olacağı “Image Fragment Size(MB)” kısmında belirlenir. Ancak imaj tek dosya halinde oluşturulmak isteniyorsa bu durumda “Image Fragment Size(MB)” kısmına “0” olarak belirtilir. “Compression” seçeneği ise sadece imaj sıkıştırma desteği sunan formatlardan birisinin seçilmesi durumunda aktif olur ve sıkıştırma oranını belirler. Alınacak imajın şifrelenmesi isteniyorsa bu durumda “Use AD Encryption” seçeneği ile belirlenir. (Şekil 3.3.2.7)

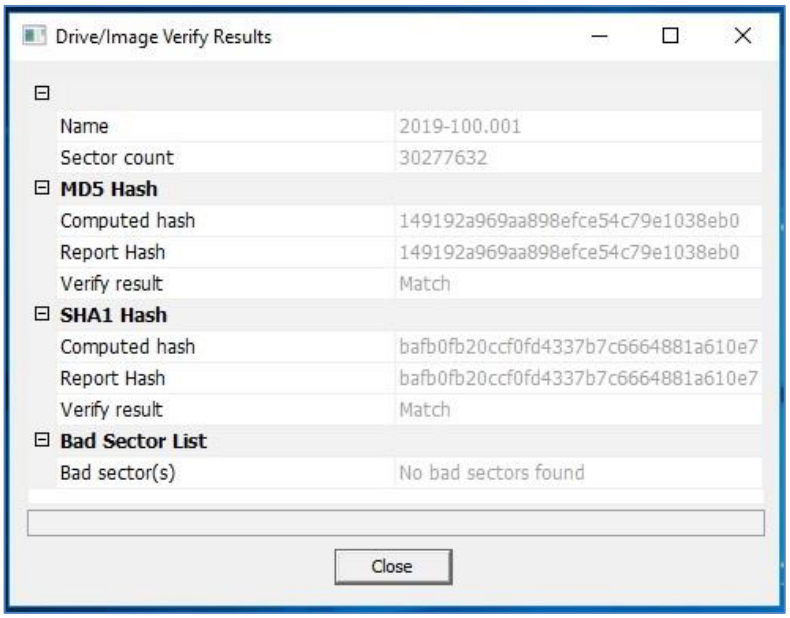


Şekil 3.3.2.7: FTK Imager Disk İmajı Alma Aşama 7

8. “Finish” butonu tıklanarak ilgili adımlar geçildikten sonra imaj alma işlemi başlaması için “Start” butonuna basılır ve imaj alma işlemi başlatılır. İmaj alma işlemi bittiğinde imaj alma işleminin ne kadar sürdüğü, ortalama olarak ne hızla imaj alındığı bilgisinin yer aldığı ve imaj doğrulama sonucunun yer aldığı iki pencere açılır. (Şekil 3.3.2.8 ve Şekil 3.3.2.9)



Şekil 3.3.2.8: FTK Imager Disk İmajı Alma Aşama 8



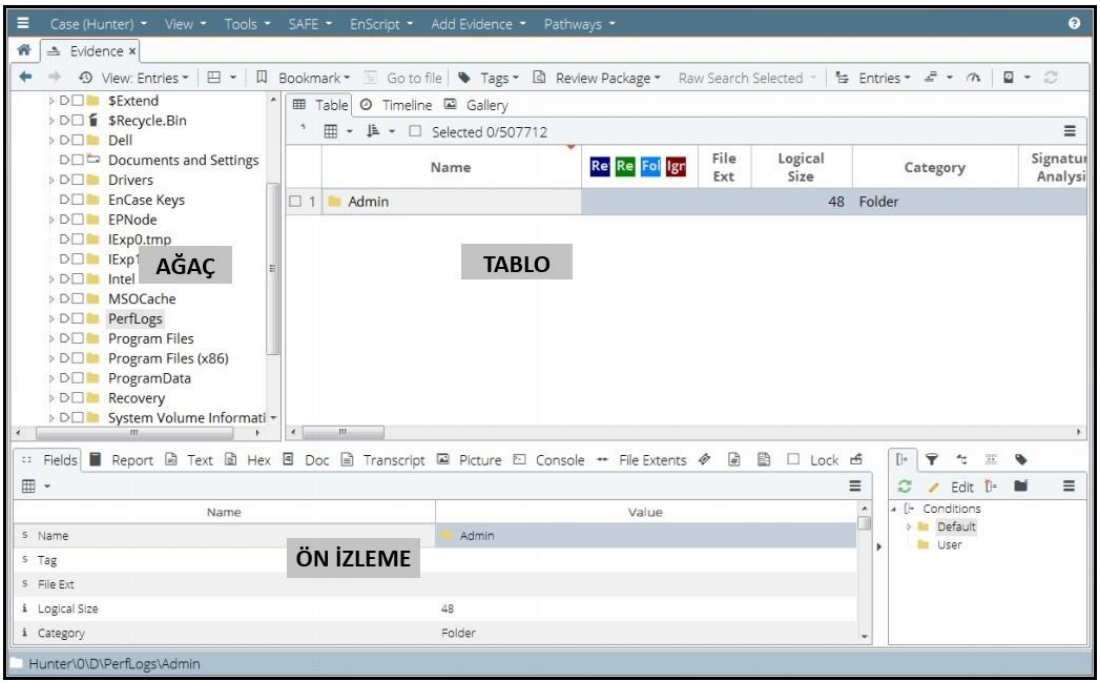
Şekil 3.3.2.9: FTK Imager Disk İmajı Alma Aşama 9

3.3.3 Dosya Analizi

Dosya analiz aşaması, delillerin ortaya çıkartılması noktasında sonuca gidilen en önemli süreçtir. Bu aşamada adli bilişim uzmanı, tam olarak disk veya imaj dosyası üzerinde neyi bulmak istediğini iyi bilmelidir (Henkoğlu, 2011).

Sabit disk, USB bellek, hafıza kartı, CD/DVD gibi veri depolama birimleri imajı alındıktan sonra imaj üzerinden inceleme yapılmalıdır. İnceleme esnasında daha çok adli bilişim yazılımı olarak da adlandırılan yazılımlar kullanılmaktadır. Aşağıda adli bilişim incelemesi esnasında kullanılan yazılımlara genel özellikleri ile bazı örnekler verilmiştir.

Encase Forensic, Amerika'da kurulu bulunan Guidence Software firması tarafından geliştirilmiş çok fonksiyonlu bir adli bilişim yazılımıdır. Windows işletim sistemi tabanlı çalışmaktadır. Yazılım ile doğrudan imaj alınabileceği gibi alınmış imaj dosyaları da incelenebilmektedir. Alınan imajın doğrulaması yapılabilmektedir. Yazılım, kendi imaj formatları olan E01, EX01,L01, LX01 formatlarının yanı sıra VMDK, VHD ve Raw DD gibi farklı imaj formatlarını da desteklemektedir. Ağaç, tablo ve ön izleme menüleri ile etkin bir kullanıcı arayüzüne sahiptir. Arayüzü kullanılarak birçok işlem yapılabilmektedir (Bakan & Saluk, 2014).



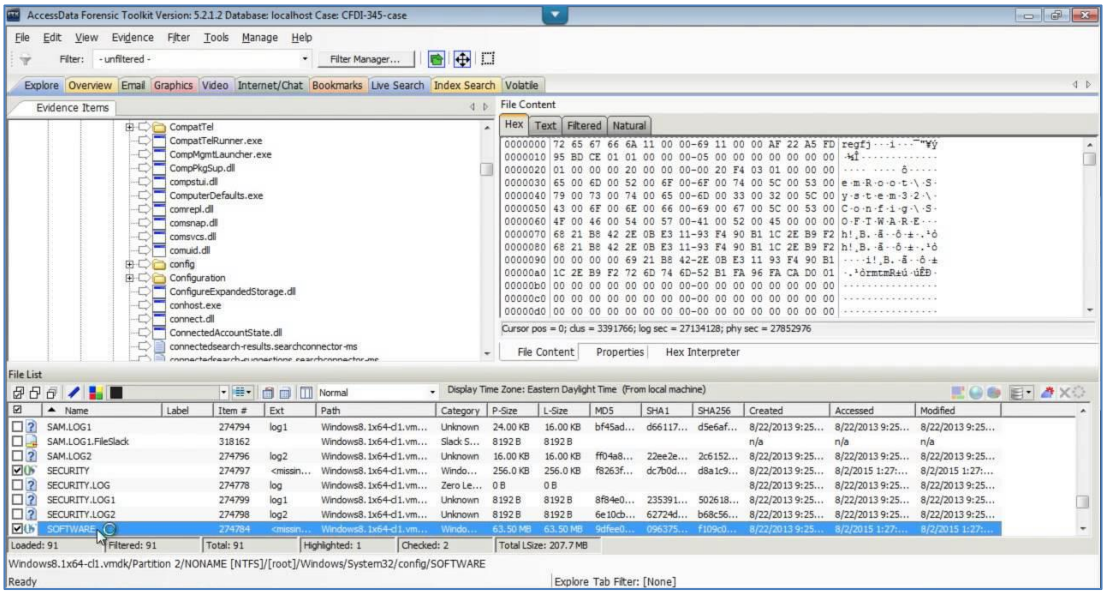
Şekil 3.3.3.1: Encase Forensic v8.07 Kullanıcı Arayüzü

Yazılımın arayüzünde incelenen veri depolama birimi içeriği ağaç görünümünde, hiyerarşik yapıda görüntülenebilmektedir. Tablo bölümünde, ağaç bölümünde seçilen içeriğin detaylı içeriği görülebilmekte ve filtrelenebilmektedir. Ön izleme bölümünde ise dosya içeriği metin, resim, hex gibi farklı formatlarda görüntülenebilmektedir.

Yazılım ile veri depolama biriminde bulunan mevcut ve silinmiş tüm alanlar ile HPA ve DCO bölümleri incelenebilmektedir. İncelenecek alanlarda anahtar kelime araması, veri kurtarma, internet geçmişi analizi, elektronik posta ve sohbet kayıtlarının tespiti ve analizi, şifreli dosya tespiti ve analizi, dosya imza analizi ve hash analizi yapılabilmektedir. Tespit edilen şüpheli veriler üzerinde işaretleme ve etiketleme yapılabilmektedir. Mevcut ve silinmiş tüm veriler indekslenebilmekte, indekslenen veriler içerisinde kelime araması yapılabilmektedir. İncelemeler esnasında istenilen bilgiler raporda yer alması için işaretlenebilmekte ve inceleme sonucunda tüm bilgiler rapor halinde alınabilmektedir. Enscript özelliği ile ihtiyaca yönelik küçük programlar yazılabilmekte ve yazılım içerisinde çalıştırılabilmektedir (Opentext, 2018).

Forensic Toolkit (FTK), Amerika Birleşik Devletleri'nde kurulu bulunan AccessData firması tarafından geliştirilmiş çok fonksiyonlu adli bilişim yazılımıdır. Windows işletim sistemi tabanlı çalışmaktadır. Delil incelemesi ve tespit edilen

delilleri raporlandırma konusunda oldukça başarılı olan bu program, tüm dünyada başta güvenlik güçleri olmak üzere yoğun olarak kullanılmaktadır. Adli makamlar tarafından bu program aracılığı ile mahkemeye sunulan rapor ve verilerin delil niteliğinde olduğu kabul edilir.



Şekil 3.3.3.2: Accessdata Forensic Toolkit (FTK) v5.2 Kullanıcı Arayüzü

Yazılım ile doğrudan medya üzerinde inceleme yapılabileceği gibi farklı bir yazılım tarafından alınan imaj dosyaları da incelenebilmektedir. Yazılım ile medya üzerinde bulunan mevcut ve silinmiş tüm alanlar incelenebilmektedir. İncelenen alanlarda anahtar kelime araması, veri kurtarma, internet geçmişi analizi, e-posta ve sohbet kayıtları tespiti ve analizi, şifreli dosya tespiti ve analizi ile dosya imza analizi yapılabilmektedir. Mevcut ve silinmiş tüm veriler indekslenebilmekte, indekslenen veriler içerisinde kelime araması yapılabilmektedir. Yazılımın zengin bir filtreleme özelliği vardır. Ayrıca kullanıcı tarafından filtre oluşturup uygulanarak inceleme alanı daraltılabilmektedir. Metin, hex ve orijinal görünüm gibi çeşitli formatlarda içerik ön izlemesi yapılabilmektedir. Resim dosyaları grafik sekmesi altında incelenebilmektedir. Video dosyaları üzerinde dönüştürme yapılabilmekte, küçük resimler haline getirerek hızlı bir şekilde inceleme yapılabilmektedir. İncelenen medya üzerinde Cerberus Analysis özelliği sayesinde kötücül yazılım taraması yapılabilmektedir. Yazılımın ayrıntılı raporlama özelliği bulunmaktadır (Bakan & Saluk, 2014).

3.3.4 İşletim Sistemi Üzerinde Yapılan Analizler

Adli bilişim incelemesine konu olan bir bilgisayar üzerinde kurulu işletim sisteminin analizi adli bilişim uzmanına birçok konu hakkında detaylı bilgi vermektedir. Sistem kayıtları, kurulu olan yazılımlar, silinmiş veriler, internet geçmişi, e-posta ve anlık mesajlaşma kayıtları gibi alanlar işletim sistemi üzerinde analiz yapılabilecek alanlardır.

İşletim sistemleri hem kullanıcılar tarafından yapılan her işlemi hem de kendi arka plan işlemlerini zaman ekseninde otomatik olarak kayıt altına alır. Bu kayıtlar işletim sisteminin türü ve özelliğine göre farklı alanlarda saklanır. Bu kayıtlara kayıt kütüğü veya olay günlükleri (log kayıtları) denilmektedir. Adli bilişim incelemesinde işletim sisteminin tuttuğu bu kayıtlar büyük önem taşımaktadır (Durmaz, 2014).

Log kayıtları ile yapılan tüm analiz işlemlerinin sonuçları arasında anlamlı bir bağlantı olması gerekmektedir. Kullanıcın yapmış olduğu tüm işlemler, kurulan ve kaldırılan tüm yazılımlar ve işletim sisteminin tutmuş olduğu kayıtlar arasındaki tutarlılık, medya analiz sonucunu destekler nitelikte olmalıdır (Henkoğlu, 2011).

“Windows Kayıt Defteri”, işletim sistemi ile ilgili işlemlerinin kayıtlarının tutulduğu bir alandır. Windows NT işletim sistemi kurulu bilgisayarlarda “Registry” verisi dört dosyada “Security, Software, SAM ve System” saklanır. Bu dosyalar “C:\Windows\system32\config\” klasörü içerisinde bulunurlar. Kullanıcı ayarları ise “NTuser.dat” dosyasında saklanır. Bu dosya da her kullanıcı için ayrı ayrı “C:\Users\” içerisinde bulunan klasörlerde bulunur (GetData Forensics, 2017).

Kurulu yazılımların tespiti ve analizi, medya incelemesi sonucu tespit edilen verinin işletim sistemi üzerinde kurulu bulunan programlar ile ilişkisinin anlaşılmasına yardımcı olacaktır. Bu tespitler Windows işletim sistemi için Software isimli kayıt defterinin incelenmesi ile yapılabilmektedir. Elde edilen bilgiler sayesinde inceleme esnasında tespit edilen bir verinin, işletim sistemi üzerinde kurulu bulunan programlar ile ilişkisinin anlaşılmasına yardımcı olacaktır (Durmaz, 2014).

İnceleme işleminde depolama aygıtı veya imajının tamamının incelemesi yapılmaktadır. Depolama aygıtında daha önce bulunan ancak verinin silinmesi veya bozulması nedeniyle görülemeyen veriler veri kurtarma işlemi ile kurtarılmakta ve inceleme bu veriler üzerinde de yapılmaktadır. Otomatik veri kurtarma yazılımları ya

da teknik incelemede kullanılan adli bilişim yazılımları, silinen ve bozulan verileri depolama aygıtının silinmiş ve boş olarak işaretlenmiş alanından kurtarmaya çalışır. Silinen bir verinin bulunduğu sektöre yeniden veri yazılması kurtarma işlemini olumsuz etkilemektedir.

İnternet geçmişinin incelenmesi de adli bilişim uzmanına suçun aydınlatılmasında önemli bilgiler verebilmektedir. Yapılan internet geçmişi incelemesi kapsamında, ziyaret edilen internet siteleri, ziyaret saatleri ve kayıtlı parolalar elde edilebilmektedir. Bu veriler, işletim sistemi üzerinde yüklü internet tarayıcılarının dizinleri altında kaydedilmektedir. Tarayıcı dizinine kaydedilen çerezler (cookie) ile bağlantı yapılan internet sitesine ait erişim bilgilerine ulaşılabilmektedir.

İnternetin yoğun olarak kullanılan bir iletişim türü olması nedeniyle, dijital delil incelmelerinde, internet üzerinden iletişimi sağlayan e-posta ve anlık mesajlaşma kayıtlarının incelenmesi önemli bir delil kaynağı olmuştur. Birçok adli bilişim yazılımı inceleme esnasında medya üzerinde kayıtlı e-posta adreslerini bularak, adli bilişim uzmanının bulunan e-posta adreslerine yoğunlaşmasına yardımcı olmaktadır.

3.3.5 Network Analizi

Network analizi, belirli bir sitem içerisinde kurulu olan yerel ağ (LAN), geniş alan ağı (WAN) ya da internet ağ trafiklerinin izlenmesi, analiz edilmesi ve analiz neticeleri doğrultusunda adli makamlara gerekli bilgilerin verilmesi şeklinde tanımlanabilir (Orta, 2015).

Network analizi, bilgisayar ağları kullanılarak gerçekleştirilen suçların aydınlatılması çalışmalarının başında gelmektedir. Fakat ağ trafik kayıtları ham olarak tek başına bir anlam ifade etmemektedir. Kayıt altına alınan ağ trafik verisi; sisteme, kayıt tipine ve analiz edilen olay türüne göre gerçek zamanlı veya önem derecesine göre sınıflandırılarak incelenmesi, ilişkilendirilmesi, raporlanması durumunda ancak bir anlam kazanacaktır (Polat, 2014).

Bir suç araştırmasında, suçun bilişim yolu ile belirli bir network üzerinden gerçekleştirildiği şüphesi olması halinde, şüpheli tarafından kullanılan ağ üzerinden iletilen paketler incelenip analiz edilerek delil toplanması yapılır. Network yapısı,

genel olarak, fiziksel katman, ağ katmanı, taşıma katmanı ve uygulama katmanı olarak dört katmanda incelenir. Her katman elektronik delil anlamında kendine özgü farklılıklar gösterir. Pocket Analyzer (Wireshark, SolarWinds, NetworkMiner vb.) yazılımlar ağ üzerinden iletilen paketlerin yakalanarak analiz edilmesine imkan tanımaktadır.

Bir network üzerinde incelemeye başlamadan önce incelenecek network topoğrafyasının çıkartılması gerekmektedir. Hangi bilgisayar hangisi ile haberleşmiş, kullanılan çevre birimleri ve network cihazlarının (hub, switch, router vb.) neler olduğu tespit edilmelidir (Orta, 2015).

3.3.6 Mobil Sistemlerin Analizi

Mobil sistemlerin kullanımı tüm dünyada hızlı bir şekilde artmaktadır. Mobil sistemler olarak değerlendirebileceğimiz tablet, PDA ve cep telefonları, mobil olarak hizmet veren ve kasası içerisinde bulunan bataryalardan güç alarak çalışan cihazlardır. Günümüzde en yaygın kullanılan aynı zamanda çok hızlı değişim ve gelişim gösteren mobil cihazlardan birisi cep telefonlarıdır.

Cep telefonu hayatımıza ilk girdiğinde sadece mobil olma ve iletişimi yaşamın her alanına her an taşıyabilmesi özelliği ile ön plana çıkarken, günümüzde bilişim teknolojilerinin gelişmesiyle cep telefonları da gelişmiştir. Üzerinde bulunan işletim sistemi ve donanımsal özelliklerine bağlı olarak, bir dizüstü bilgisayar ile yapılabilecek her işlemi yapabilecek duruma gelen cep telefonları her geçen gün daha fazla dijital delilin elde edildiği sistemler olarak karşımıza çıkmaktadır.

Adli bilişim süreçleri ve delillerin geçerliliği ile ilgili kurallar cep telefonları için de geçerli olmakla beraber delillerin toplanması ve analizi cep telefonları için daha karmaşık ve zorlu bir süreçtir. Çok fazla cep telefonu modelinin bulunması ve kullanılan işletim sistemi, dosya sistemi, uygulamalar ve donanımsal farklılıklar adli bilişim incelemesi sürecini zorlaştırmaktadır (Çakır, 2014).

Klasik cep telefonlarında arama kayıtları, telefon rehberi ve kısa mesajlar gibi verilere erişilebilirken akıllı cep telefonları ile birçok multimedya içeriğe ve internet erişimi gibi bilgilere de erişilebilmektedir (Kiçeci, 2014).

Mobil cihazlara el koyma ve muhafaza altına alma işlemi yapılırken, verilerin sağlıklı ele geçirilmesi ve daha sonra da kullanılabilmesi, doğru sonuçlar çıkartabilmesi için belli başlı dikkat edilmesi gereken hususlar vardır (Çakır, 2014).

- Cihaza ait standart dışı data ve şarj kablolarına cihaz ile birlikte el koyulmalıdır.
- Cihaz ekranı fotoğraflanmalı, cihazın kime ait olduğu tespiti içi gerekmesi halinde parmak izi alınmalıdır.
- Mobil cihazlara müdahalede ilk yapılması gereken işlem, eğer cihazlar açık ise, şarj aletleri ile bataryanın devamlılığını sağlamak olmalıdır. Cihazların desteklemesi halinde uçuş moduna geçirilmesi ve açık/kapalı olmasına bakılmaksızın şebeke sinyalleri ve kablosuz ağ sinyalleri ile bağlantısının kesilmesi gerekmektedir. Cihazların sinyal almasını engellemek için sinyal kesici cihazlar, faraday çantası adı verilen koruyucu kılıflar veya alüminyum folyolar kullanılabilir.
- Cihaza ait açılış ve koruma şifreleri öğrenilmeli ve not edilmelidir.

Mobil cihazlara usulüne uygun el koyma yapılıp muhafaza altına alındıktan sonraki adım, verilerin toplanmasıdır. Mobil cihazların incelenmesi için özel donanımlar ve yazılımlar bulunmaktadır. Donanımsal inceleme cihazları daha pratik kullanıma sahip olmakla beraber bu cihazlar daha maliyetlidir (Henkoğlu, 2011).

Adli bilişim uzmanı inceleme yapılacak cihazın ilk önce imajını almalıdır. Olayın türüne göre bu olay mahallinde ya da laboratuvar ortamında olabilmektedir. Diğer mobil cihazlara göre daha karmaşık bir yapısı olan cep telefonlarının imajı alınırken, cep telefonu, sim kartı ve hafıza kartının içerinde veri olabileceği göz önünde tutularak işlem yapılmalıdır.

Cep telefonu, sim kartı ve hafıza kartından elde edilecek veriler; IMEI numarası, telefon sistem bilgisi, ağ bilgisi, GPS konum bilgisi, takvim, hatırlatma ve yapılacaklar listesi, telefon rehberi, arama geçmiş ve süresi, mevcut veya silinmiş SMS mesajları, MMS mesajları, fotoğraflar, videolar, ses dosyaları, e-postalar, dokümanlar, internet geçmişi, anlık mesajlaşma verileri, sosyal medya kayıtları, uygulama bilgileri ve veritabanları şeklinde sıralanabilir (Çakır, 2014).

4. SONUÇ VE YORUMLAR

Delil elde etme konusunda son zamanlarda kullanım alanı hızla artan adli bilişim incelemelerinde, yapılan delillendirmenin klasik delil gibi somut olmaması inandırıcılık ve güvenirlilik açısından toplumda tereddütler oluşturmaktadır. Bu tereddütlerin ortadan kaldırılması için adli bilişim incelemelerinde genel kabul görmüş prosedürlerin izlenmesi büyük önem arz etmektedir.

Türkiye, Avrupa Konseyi tarafından hazırlanmış olan Siber Suçlar Sözleşmesine imza atmış, ulusal düzeyde hukuk düzenlemeleri yaparak bu konuda iradesini göstermiştir. Ancak yapılan hukuki düzenlemeler yeterli olmamakta, teknolojik gelişmelerin ortaya çıkardığı yeni sorunlara cevap verememektedir.

Türkiye'de delillerin toplanması, CMK madde 116 ve gecikmesinde sakınca bulunan hallerde madde 119'a istinaden, usulüne uygun olarak verilmiş bir arama kararı ile mümkündür. Ancak, CMK'nın söz konusu maddeleri, klasik suçlara ilişkin genel bir arama ve el koymaya atıf yapmaktadır. Bilişim sistemlerinin kullanılması suretiyle işlenen suçlarda veya klasik suçlara ilişkin delillerin bilgisayar sistemlerinde bulunma olasılığının söz konusu olduğu durumlarda, bilgisayarlarda yapılacak arama CMK madde 134 ile özel olarak düzenlenmiştir.

Görüldüğü üzere CMK madde 134, Türk ceza muhakemesi hukukunda doğrudan dijital delil elde etme tedbirini konu eden tek maddedir. Bu madde de geçen "başka surette delil elde etme imkânının bulunmaması halinde" şartı dijital delilleri ikinci plana atmakta, aramanın "şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde yapılması" ifadesi ise aramayı kısıtlamaktadır.

Buna karşılık, ABD, Birleşik Krallık ve Kıta Avrupası hukukunda dijital delillerin aranması genel arama hükümlerine tabidir. Ancak dijital delillerin elde edilmesi konusundaki kurallara ilişkin olarak adli makamlar ya da kolluk kuvvetleri tarafından hazırlanan rehberler bulunmaktadır. Mahkemelerde olaylar incelenirken genel olarak bu rehberdeki ilkeler yoluyla dijital delillerin sağlamlığının ve güvenilirliğinin denetimi yapılmaktadır.

Türkiye'de hukuki anlamda dijital deliller gelişmiş ülkelerle karşılaştırmalı olarak ele alındığında, delil teorisinde neyi ifade ettikleri tam olarak bilinmeyen ve anlaşılmayan, ancak ceza yargılamasında bir şekilde kullanılmakta olan bir kavram

ile karşılaşılmaktadır. Üstelik dijital deliller alanındaki gelişmelerle birlikte, bu konudaki tartışmalarda çoğalmaktadır. Dolayısıyla mevcut düzenlemelerdeki yapılacak köklü değişikliklerle bu karışıklığın önüne geçilebilecektir.

Hukuki anlamda yetersizlik yanında Türkiye'de adli bilişim açısından diğer ele alınması gereken konu eğitimdir. Suç ve suçlu ile mücadelede en önemli unsur insandır. Bu nedenle en büyük yatırım insana, dolayısı ile onun eğitimine yapılması gerekmektedir. Adli bilişim ile ilgili hukukçulara ve kolluk kuvvetlerine verilecek eğitim için, eğitim verilecek personelin belli bir eğitim düzeyinde olması gerekmektedir. Bu nedenle eğitim verilecek personelin öncelikle kendi teşkilatı içerisinden seçilmesinde, teknolojiye yatkın ve gelişmelere ayak uydurabilecek personelin tercih edilmesi büyük önem arz etmektedir.

Adli makamlarda görevli hâkim ve savcılar ile kolluk kuvvetinde görevli soruşturmacı personelin, adli bilişim alanındaki hukuki ve teknik gelişmeler ile ilgili belli periyotlarda hizmet içi eğitim almaları sağlanmalıdır. Adli bilişim ile ilgili görev alacak uzmanların belirli sertifikalara sahip olması ve güncel yazılım ile donanımı kullanabilmesi gerekmektedir. Bu şekilde yapılacak olan analizlerin mümkün olduğunca standart hale getirilmesi mümkün olabilecektir.

Ülkemizde kullanılan ve tez çalışması esnasında incelenen adli bilişim, yazılım ve donanımlarının yabancı menşeili ve yüksek maliyetli olması hem uzmanlaşmayı zorlaştırmakta hem de ülkemizi yabancı ülkelere bağımlı hale getirmektedir. Üniversiteler ile yapılacak ortak çalışmalarla ihtiyaca karşılık verecek, dünya standartlarında yazılım ve donanımlar geliştirilerek yabancı ülkelere bağımlılık azaltılarak daha fazla uzman yetişmesi sağlanabilecektir.

Sonuç olarak, her geçen gün hızla gelişen teknoloji ile birlikte bilişim bağlantılı suçlar artmakta ve çeşitlenmektedir. Bu suçlar ile mücadele edebilmek, suç ve suçluyu ortaya çıkartabilmek için adli bilişim sürecine gerekli önemin verilmesi gerekmektedir. Hangi yöntemler kullanılarak, ne şekilde delillerin tespit edileceği, sınıflandırılacağı, raporlanacağı ve yargı makamlarının önüne ne şekilde getirilmesi gerektiği konularında kapsamlı yasal düzenlemeler yapılmalı, bu konuda görev alacak her birimden personele gerekli eğitimler verilmelidir.

KAYNAKLAR

Akçadağ, E. (2012, Temmuz 20). *Sürekli Artan Önemi Işığında Siber Güvenlik.* Ağustos 8, 2012 tarihinde http://www.bilgesam.org/incele/1207/-surekli-artan-onemi-isiginda-siber-guvenlik/#.U8JznLGXDeM adresinden alındı

Akolaş, D. A. (2004). Bilişim Sistemleri ve Bilişim Teknolojisinin Küreselleşme Olgusu ve Girişimcilik Üzerine Yansımaları. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*(12), 29-42.

Aktan, Ç. C. (1998). *Bilgi Toplumunun Doğuşu ve Gelişimi.* Ekim 17, 2012 tarihinde http://www.canaktan.org/yeni-trendler/bilgi-toplumu/bilgi-toplum-dogusu.htm adresinden alındı

Avrupa Konseyi. (2018, Ekim 27). *Siber Suç Sözleşmesi.* Ekim 27, 2018 tarihinde www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures adresinden alındı

Bakan, M., & Saluk, A. (2014). Adli Bilişimde Kullanılan Ekipmanlar. H. Çakır, & M. S. Kılıç (Dü) içinde, *Adli Bilişim ve Elektronik Deliller* (s. 199-267). Ankara: Seçkin Yayıncılık.

Başar, Y. (2015). Siber Suç Soruşturmalarında Adli Bilişim İncelemeleri. Afyon: Yüksek Lisans Tezi.

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

Boğa, U. (2011). Bilişim Suçlarıyla Mücadele Yöntemleri. Ankara: Radyo ve Televiyon Üst Kurulu.

CRU. (2019). *CRU Inc.* 05 09, 2019 tarihinde www.cru-inc.com/products/wiebetech/forensic-ultradock-v5-5/ adresinden alındı

Çakır, H. (2014). Mobil Cihazların İncelenmesi. H. Çakır, & M. S. Kılıç içinde, *Adli Bilişim ve Elektronik Deliller* (s. 371-410). Ankara: Seçkin Yayınevi.

Çakır, H., & Kılıç, M. S. (2013). Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış. *Polis Bilimleri Dergisi*, s. 24.

Çakmak, H., & Altunok, T. (2009). *Suç, Terör ve Savaş Üçgeninde Siber Dünya.* Ankara: Barış Platin Kitapevi.

Değirmenci, O. (2003). Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi. *Legal Hukuk Dergisi*, 11-30.

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

Dönmezer, S. (1989). *Yeni Türk Ceza Kanunu Ön Tasarısı – Ceza Hukuku El Kitabı.* İstanbul.

Duman, E. (2012). Bilgisayarlarda ve Bilgisayar Ağlarında Delil Toplama ve Türkiye'deki Uygulama Sorunları. Ankara: Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü.

Durmaz, Ş. (2014). Elektronik Verilerin Delillendirilmesi. *Adli Bilişim ve Elektronik Deliller* (s. 270-338). içinde Ankara: Seçkin Yayınevi.

EGM KOM Daire Başkanlığı. (2009). *Bilişim Suçları ve Adli Bilişim.* Ankara: Emniyet Genel Müdürlüğü.

Ekizer, A. H. (2014, 02 02). *Adli Bilişim (Computer Forensics).* 1 11, 2016 tarihinde http://www.ekizer.net/adli-bilisim-computer-forensics/ adresinden alındı

Emekci, A., Kuğu, E., & Temiztürk, M. (2016). Adli Bilişim Ezberlerini Bir Düzelem: Bulut Bilişim. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 2*, 8-14.

Eminağaoğlu, M., & Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 1-15.

Emniyet Genel Müdürlüğü. (2009). *Uluslararası Polisiye İşbirliği İhtiyacı.* Ankara: KOM.

EMT Electronics. (2018). *www.emt.com.tr*. 02 14, 2019 tarihinde www.emt.com.tr/tr/markalar/tableau-63 adresinden alındı

Eralp, Ö. (2011, 08). *Türk Ceza Kanunu Madde 243 – Bilişim Sistemine Girme.* 01 09, 2016 tarihinde http://www.ozgureralp.av.tr/web/makaleler/bilisim-suclari-turk-ceza-kanunu-madde-243-bilisim-sistemine-girme-2/ adresinden alındı

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

Ersoy, Ö. (2009, Kasım 10). *Sınıraşan Suçlar.* Mart 17, 2013 tarihinde http://www.sde.org.tr/tr/haberler/350/sinirasan-suclar.aspx adresinden alındı

Evrin, V., & Demirer, M. (2011). Kurumsal Bilgi Güvenliği Süreç Çalışmaları ISO/IEC-27001 Örneği. *IV.Ağ Ve Bilgi Güvenliği Ulusal Sempozyumu.* Ankara: Elektrik Mühendisleri Odası (EMO).

ForensicSoft. (2016). *ForensicSoft*. 5 9, 2019 tarihinde www.forensicsoft.com/safeblock.php adresinden alındı

GetData Forensics. (2017). *The Forensic Explorer User Manual.* 5 18, 2019 tarihinde http://www.forensicexplorer.com/support.php adresinden alındı

Göksoy, R. (2017). Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi Ve Güvenliğinin Sağlanması. İzmir: Yüksek Lisans Tezi.

Hekim, H., & Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Trörizm*, s. 135-158.

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

Huebner, E., Bem, D., & Bem, O. (2007). *Computer Forensics – Past, Present And Future.* 01 11, 2016 tarihinde https://cld.pt/dl/download/a87a98a2-4b85-46b7-8df6-6ac213bbc201/English/Security%20%26%20Hacking/Computer%20Forensics%20-%20Past%20Present%20Future.pdf adresinden alındı

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

Karabulut, F., Karapazarlıoğlu, E., & Tosun, H. (2015). Ceza Muhakemesinde Delil Kavramı ve Kovuşturma Sürecinde Hâkimlerin Delil Algısı. *Türkiye Barolar Birliği Dergisi*(120), 385-422.

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

Kaygısız, M. (2005). *Adli Bilimler* (2 b.). Ankara: Seçkin Yayıncılık.

Kaygısız, M., & Bayer, M. (2002). Olay Yeri İnceleme. Ankara: EGM.

Kaynakçıoğlu, U. (2015, 06). Ceza Muhakemesinde Dijital Deliller. İstanbul: Yüksek Lisans Tezi.

Kiçeci, H. (2014). Bilgisayar Medyalarına İlk Müdahale. H. Çakır, & M. S. Kılıç (Dü) içinde, *Adli Bilişim ve Elektronik Deliller* (s. 161). Ankara: Seçkin Yayıncılık.

Kılıç, M. S. (2014). Elektronik Deliller ve Yapısal Özellikleri. *Adli Bilişim ve Elektronik Deliller* (s. 139-158). içinde Ankara: Seçkin Yayıncılık.

LogiCube. (2018). *https://www.logicube.com/*. 5 11, 2019 tarihinde https://www.logicube.com/shop/forensic-falcon-neo/?v=ebe021079e5a adresinden alındı

McLuhan, M. (1962). Eylül 18, 2012 tarihinde http://en.wikipedia.org/wiki/Global_Village_(term) adresinden alındı

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

ODTÜ Bilgi İşlem Daire Başkanlığı. (2005). *Türkiye'de İnternet.* 01 09, 2016 tarihinde http://www.internetarsivi.metu.edu.tr/tarihce.php adresinden alındı

Opentext. (2018, 5 11). *Encase Forensic User Guide v8.07.* 5 15, 2019 tarihinde http://encase-docs.opentext.com/ adresinden alındı

Opentext. (2018). *Guidance Software*. 02 14, 2019 tarihinde www.guidancesoftware.com/tableau/hardware//t6u adresinden alındı

Opentext. (2018). *www.guidancesoftware.com/*. 11 05, 2019 tarihinde https://www.guidancesoftware.com/tableau/hardware/td2u adresinden alındı

Orta Doğu Teknik Üniversitesi. (2004). *Bilgi Güvenliği ve Standarlar Çalışma Grubu İlerleme Raporu.* Ankara: E-İmza Ulusal Kordinasyon Kurulu.

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

Önel, D., & Dinçkan, A. (2007). *Bilgi Güvenliği Yönetim Sistemi Kurulumu Sürüm 1.00.* Ankara: Tübitak UEKAE.

Özcan, M. (2001). Siber Terörizm ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu. Ankara: Polis Akademisi.

Özdemir, M. (2003, 12 01). *Bilişim Suçları ve Mücadelede Taşra Teşkilatında Karşılaşılan Problemle ve Çözüm Önerileri.* 01 10, 2016 tarihinde http://www.caginpolisi.com.tr/bilisim-suclari-ve-mucadelede-tasra-teskilatinda-karsilasilan-problemler-ve-cozum-onerileri/ adresinden alındı

Özel, C. (2001, Eylül). Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı. *İstanbul Barosu Dergisi*, 863.

Özkul, D. (2002). Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi. *Sayıştay Dergisi*(44-45), 14.

Özmestik, F. Ü. (2015). Bilişim Sistemleri Üzerine Arama ve El Koyma Tedbirine İlişkin Mevzuat ve Uygulamada Yaşanan Sorunlar . İstanbul: Yüksek Lisans Tezi.

Özocak, G. (2011). Ceza Muhakemesinde Elektronik Delillerin Tespiti ve Toplanması. İzmir: İzmir 2. Uluslararası Bilişim Hukuku Kurultayı.

Öztürk, M. İ. (2007). Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri. 6-7. Ankara: Yüksek Lisans Tezi.

Öztürkci, H. (2014, 04 30). *FTK Imager İle Disk İmajı Alma.* 05 11, 2019 tarihinde http://halilozturkci.com/adli-bilisim-ftk-imager-ile-disk-imaji-alma/ adresinden alındı

Parlar, A., Yüksel, E. G., & Hatipoğlu, M. (2008). *Deliller, Çapraz Sorgu ve İspat* (1 b.). Ankara.

Polat, H. (2014). *Adli Bilişim ve Elektronik Deliller* (Birinci b.). Ankara: Şeçkin.

Polat, H. (2014). Bilgisayar Ağları ve Adli Bilişim. H. Çakır, & M. S. Kılıç içinde, *Adli Bilişim ve Elektronik Deliller* (s. 96-135). Ankara: Seçkin Yayınevi.

Resmi Gazete. (1991, 06 14). *20901 sayılı Resmi Gazete.* 01 10, 2016 tarihinde http://www.resmigazete.gov.tr/arsiv/20901.pdf adresinden alındı

Sağıroğlu, Ş., & Karaman, M. (2015). Uluslararası Standartlar Perspektifinde Adli Bilişim Yazılımlarına Ait Test Süreçleri Ve Türkiye İçin Öneriler. Ankara: 3.Uluslararası Adli Bilişim ve Güvenlik Sempozyumu.

Sarıhan, H. İ. (1998). *Rekabette Başarının Yolu Teknoloji Yönetimi* (1 b., s. 167). içinde İstanbul: Beta Yayınevi.

Say, K. (2006). Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi. Ankara: Yüksek Lisans Tezi.

Sayıştay. (2013). *Bilişim Sistemleri Deneim Rehberi.* Ankara: Sayıştay.

Şen, O. N. (2003). Polisin Bilişim Suçlarıyla Mücadelede Yapması Gerekenler. *1. Polis Bilişim Sempozyumu*, (s. 70-71). Ankara.

Şener, K. (2012). http://www.kemalsener.av.tr/bilisim-suclari/bilisim-suclari-ve-turk-ceza-kanunu.html adresinden alınmıştır

T.C. Adalet Bakanlığı. (2004). *Türk Ceza Kanunu Madde Gerekçeleri Madde 243.* 01 10, 2016 tarihinde www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc adresinden alındı

Tonta, Y. (1999). Bilgi Toplumu ve Bilgi Teknolojisi. *Türk Kütüphaneciliği*(13), 363-375.

TUİK. (2018, Ağustos 8). *Hanehalkı Bilişim Teknolojileri Kullanım Araştırması 2018.* Ekim 27, 2018 tarihinde http://www.tuik.gov.tr/PreTablo.do?alt_id=1028 adresinden alındı

Tulum, İ. (2006). Bilişim Suçları İle Mücadele. 45. Isparta: Süleyman Demirel Üniversitesi.

Türk Dil Kurumu. (2012, 07 05). *Büyük Türkçe Sözlük*. www.tdk.gov.tr: http://www.tdk.gov.tr/index.php?option=com_gts adresinden alınmıştır

Türk Dil Kurumu. (2016). *Türk Dil Kurumu Genel Sözlüğü*. 01 09, 2016 tarihinde http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5691169f504259.40664448 adresinden alındı

Vural, Y., & Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendis ve Mimarlık Fakültesi Dergisi*, 507-522.

Wikipedia. (2015, 10 01). *Digital forensics.* 01 11, 2016 tarihinde https://en.wikipedia.org/wiki/Digital_forensics adresinden alındı

Wikipedia. (2015, 11 14). *Locard'ın değişim prensibi.* 10 24, 2016 tarihinde https://tr.wikipedia.org/wiki/Locard'ın_değişim_prensibi adresinden alındı

Wikipedia. (2016). *Wikipedia*. 2 8, 2016 tarihinde https://en.wikipedia.org/wiki/Digital_forensics adresinden alındı

Yalçınkaya, H. (2008). *Savaş: Uluslararası İlişkilerde Güç Kullanımı.* Ankara: İmge Kitapevi.

Yaycı, E. (2007). Bilişim Suçları. Ankara: Yüksek Lisans Tezi.

Yenidüya, A. C., & Değirmenci, O. (2003). *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları.* İstanbul: Legal Yayıncılık.

ÖZGEÇMİŞ

1984 yılında Eskişehir'de doğdum. İlk ve orta öğrenimimi Eskişehir ilinde tamamladım. Anadolu Üniversitesi İşletme Fakültesi İşletme Bölümünden 2006 yılında ve İktisat Fakültesi Uluslararası İlişkiler Bölümünden 2014 yılında mezun oldum. 2009 yılında Emniyet Genel Müdürlüğü bünyesinde Polis Memuru olarak göreve başladım. Halen Biga İlçe Emniyet Müdürlüğü'nde görev yapmaktayım.