ADLİ BİLİŞİMDE DELİLLERİN TOPLANMASI ve İNCELENMESİ

Murat ÖZBEK
110691008

İSTANBUL BİLGİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
HUKUK YÜKSEK LİSANS PROGRAMI
(BİLİŞİM VE TEKNOLOJİ HUKUKU)

Yrd. Doç. Dr. Leyla KESER BERBER

2013

ADLİ BİLİŞİMDE DELİLLERİN TOPLANMASI VE İNCELENMESİ

EVIDENCE COLLECTION AND ANALYSIS IN COMPUTER FORENSICS

Murat ÖZBEK
110691008

Yrd. Doç. Dr. Leyla Keser BERBER :

Öğr. Gör. Dr. Hayretdin BAHŞİ :

Öğr. Gör. İbrahim SARUHAN :

Tezin Onaylandığı Tarih :

Toplam Sayfa Sayısı :125

Anahtar Kelimeler
1) Adli Bilişim
2) Bilişim Suçları
3) Elektronik Delil
4) Delil Toplama ve Analiz
5) Hash Problemleri

Keywords
1) Computer Forensics
2) Cyber Crimes
3) Digital Evidence
4) Evidence Collection and Analysis
5) Hash Issues

ÖZ

Bilişim sistemleri giderek artan bir hızla hayatımıza dahil olması, toplumsal hayatı hızla değiştirerek şekillendirmektedir. Yeni teknolojilerin kullanılması toplumlara büyük yararlar sağladığı gibi, beraberinde birtakım problemler de getirmektedir. Yakın bir zamana kadar daha çok bireysel sorunlara yol açan bilişim suçları, artık suç organizasyonları tarafından kamu ve ülke güvenliğini tehdit edebilecek boyutlara ulaşmıştır.

Bu çalışmada bilişim suçlarının tespit edilmesi ve cezalandırılmasında en önemli hususlardan olan elektronik delillerin, toplanması ve incelenmesi süreci ele alınmıştır.

ABSTARCT

The fact that informatics systems are incorporated in our lives with a gradually increasing speed shapes the changing the public life. Although usage of new technologies has maintained great benefits, it also brought some problems together with it. Cyber crimes, which have caused mostly personal problems until recent periods, now reached to the levels, which can treat the security of public and state by criminal organizations.

In this study, digital evidence collection and analysis process are discussed.

Yoğun mesaiden arta kalan zamanımın da bu çalışmaya ayrılmasına gösterdikleri anlayış ve destekten dolayı müteşekkir olduğum

Sevgili eşime ve biricik kızıma...

İÇİNDEKİLER

KISALTMALAR LİSTESİ

A.B.D.	**:**	Amerika Birleşik Devletleri
A.g.e.	**:**	Adı geçen eser
AÖAY	**:**	Adli ve Önleme Aramaları Yönetmeliği
b.	:	Bölüm
CD	:	Compact Disk
CMK	**:**	Ceza Muhakemesi Kanunu
DVD	:	Digital Video/Versatile Disk
E-delil	**:**	Elektronik delil
FBI	:	A.B.D.'de bulunan (Federal Bureau of Investigation) Federal Soruşturma Bürosu,
Ram	**:**	İşlemci tarafından okunup yazılabilen, üzerinde bilgilerin geçici olarak tutulduğu bellek.
s.	:	Sayfa
S.	:	Sayı
TCK	**:**	Türk Ceza Kanunu

KAYNAKÇA

AccessData. (2013, 03 21). Live Response: http://marketing.accessdata.com/acton/attachment/4390/f-0088/0/-/-/-/-/file.pdf adresinden alınmıştır

Adli Bilişimin Sağladığı Faydalar. (2009). E-Keşif ve Adli Bilişim: http://www.e-kesif.com/2008/05/adli-bilisimin-faydalari.html adresinden alınmıştır

Akalın, P. Ş., Cebeci, P. Z., Bada, Y. E., Mıtış, Y. B., Acar, Y. L., & Tan, D. A. (2012). *Bilgisayar Terimleri Karşılıklar Kılavuzu.* Ankara: Türk Dil Kurumu.

Anderson, M. R. (2012, Eylül 09). *Computer Evidence Processing Step 1 -- Seizure of the Computer.* Government Technology: http://www.govtech.com/magazines/gt/Computer-Evidence-Processing-Step-1---.html?page=1 adresinden alınmıştır

Androulidakis, I. I. (2012). *Mobile Phone Security and Forensics.* New York Heidelberg Dordrecht London: Springer.

Austin, R. (2013). *FORENSIC PROCEDURES MANUAL VERSION 3.5.* Marietta: Department of Information Technology, Southern Polytechnic State University.

Bayraktar, Y. D. (2011, sayı:25). Muhakemelerde Delillerin Önemi. *Sosyal Bilimler Dergisi*, s. 9.

Bolat, M. (2013, Mayıs 05). *Encase Nedir?* Özel Bilirkişilik ve Uzman Mütalaası Hizmetleri: http://www.adlibilirkisi.org/index.php?sayfa=makaleoku&kategori=13&id=444 adresinden alınmıştır

Bolt, S. (2011). *XBOX 360 Forensics.* Burlington: Elsevier Inc.

Borek, J. (2012, 05 20). SANS: http://www.sans.org/reading_room/whitepapers/incident/computer-forensics-weve-incident-investigate_652 adresinden alınmıştır

Bryson, C., Casey, E., Clark, D. F., Frederick, K., Gibbs, K. E., Larson, T., . . . Knijff, R. v. (2004). *Handbook of Computer Crime Investigation Forensic Tools and Technology.* London: Elseiver Academic Press.

Cardwell, K., O'Shea, K., Clinton, T., Reis, K., Cohen, T., Reyes, A., . . . Jean, B. R. (2007). *The Best Damn Cybercrime and Digital Forensics Book Period.* Burlington: Syngress Publishing, Inc.

Carroll, O. L., Brannon, S. K., & Song, T. (2008). *Computer Forensics.* Washington DC: The United States Attorneys.

Casey, E. (2000). *Digital Evidence and Computer Crime.* LONDON: Academic Press.

Chris PROSISE, K. M. (2003). *INCIDENT RESPONSE & COMPUTER FORENSICS, SECOND EDITION.* United States of America: McGraw-Hill/Osborne.

Chris Simpson, A. P. (2012, Eylül 09). *Good Practice Guide for Computer-Based Electronic Evidence.* 7Safe Information Security, eDiscovery, Penetration Testing, Training, PCI DSS, Computer Forensics: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf adresinden alınmıştır

Clarke, N. (2010). *Computer Forensics A Pocket Guide.* United Kingdom: IT Governance Publishing.

Cohen T., C. K. (tarih yok). *Alternate Data Storage Forensics* . United States of America: Syngress Publishing.

Collecting Digital Evidence Flowchart. (2008, Nisan 14). National Institute of Justice: http://www.nij.gov/publications/ecrime-guide-219941/ch5-evidence-collection/collecting-digital-evidence-flowchart.htm adresinden alınmıştır

Cory Altheide, H. C. (2011). *Digital Forensics with Open Source Tools.* Waltham, USA: Syngress.

Craiger, J. (2005). *Computer Forensics Procedures and Methods.* Florida.

Crowley, P., & Kleiman, D. (2007). *CD and DVD Forensics.* Rockland: Syngress Publishing, Inc.

Dave Garza, M. K. (2010). *Computer Forensic Evidence Collection and Preservation.* A.B.D.: Cengage Learning.

Dempsey, L. (1998, Ocak 19). *METADATA: A UK HE PERSPECTIVE.* UKOLN: http://www.ukoln.ac.uk/services/papers/bl/blri078/content/repor~27.htm adresinden alınmıştır

Dokurer, S. (2013, Mayıs 05). *Bilişim Suçlar im Suçları ve Adli Bili Adli Bilişim.* DATA SECURITY, COMPUTER CRIME, COMPUTER FORENSICS AND DATA RECOVERY: http://www.dokurer.net/files/documents/Adli_Bilisim_Wormy.pdf adresinden alınmıştır

Dokurer, S., Saylı, M., & Akdeniz, D. (2001). *Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar.* Bursa: Bursa İl Emniyet Müdürlüğü.

Duman, E. (2013, Nisan 07). *Solıt State Sürücülerin Adli Bilişim Alanında Getirdiği Yenilikler Ve Sorunlar.* DUMAN HUKUK & DANIŞMANLIK: http://www.emrahduman.av.tr/makale/solitstate.pdf adresinden alınmıştır

Dülger, M. V. (2004). *Bilişim Suçları.* Ankara: Seçkin.

Evidence, S. W. (2013, Şubat 11). *SWGDE Best Practices for Computer Forensics.* Scientific Working Group on Digital Evidence: https://www.swgde.org/documents/Released%20For%20Public%20Comment/2013-02-11%20SWGDE%20Best%20Practices%20for%20Computer%20Forensics%20V3-0 adresinden alınmıştır

Forensic Toolkit® (FTK®): Recognized around the World as the Standard in Computer Forensics Software. (2013, Mayıs 05). e-Discovery, Computer Forensics; Cyber Security Software: http://www.accessdata.com/products/digital-forensics/ftk adresinden alınmıştır

Güncel Türkçe Sözlük. (tarih yok). Türk Dil Kurumu: http://tdkterim.gov.tr/bts/ adresinden alınmıştır

Güncel Türkçe Sözlük. (tarih yok). Türk Dil Kurumu: http://www.tdkterim.gov.tr/?kelime=ram&kategori=terim&hng=md adresinden alınmıştır

Henkoğlu, T. (2011). *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi.* İSTANBUL: PUSULA.

Information Security and Forensics Society. (2009). *Computer Forensics Best Practices.* Hong Kong: ISFS.

ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission.

Jain, R. K. (2006). *Cyber Forensics Tools and Practices.* Indiana: The ICFAI University Press.

James Lyle, S. M. (2007). *ADVANCES IN DIGITAL FORENSICS III.* Orlando, Florida: Sprringer.

Johnson, T. A. (2005). *Forensic Computer Crime Investigation.* New York: Taylor & Francis Group.

Jones, D. A., & Vazlli, D. C. (2008). *Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility.* Waltham(United States): Syngress.

Jones, N., George, E., Mérida, F. I., Rasmussen, U., & Völzow, V. (2013). *Electronic evidence guide.* Strasbourg, France: Council of Europe.

Karagülmez, D. D. (2009). *Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri.* Ankara: Seçkin Yayıncılık.

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

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

Keser Berber, L. (2008, Temmuz 09). *BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA KOPLAMAMA EL KOYMA.* Ankara Barosu: http://www.ankarabarosu.org.tr/PANELLER/2008/09.07.2008%20B%C4%B0LG%C4%B0SAYAR%20PROGRAMLARINDA%20VE%20K%C3%9CT%C3%9CKLER%C4%B0NDE%20ARAMA%20KOPLAMAMA%20EL%20KOYMA_PANEL.doc adresinden alınmıştır

Keser Berber, L. (tarih yok). *Adli Bilişim, CMK md 134 ve Düşündürdükleri….* http://www.leylakeser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html adresinden alınmıştır

Kızıltan, M. B. (2007). *5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme Ve Bozma Suçları*. İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi.

Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., & Wright, C. (2007). *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators.* Burlington, A.B.D: Syngress Publishing.

Koltuksuz, A. (2010, Haziran 7). Adli Bilişime Giriş. İzmir.

Kul, D. R. (2009). *Bilişim Sistemleri Temelleri ve Uygulamaları.* İstanbul: Papatya Yayıncılık Eğitim.

Mamun, A. A., Guo, G., & Bi, C. (2007). *Hard Disk Drive Mechatronics and Control.* New York: CRC Press.

Marcella, A. J., & Menendez, J. D. (2008). *Cyber Forensic.* New York: Auerbach Publications.

Mason, S. (2008). *International Electronic Evidence.* London: British Institute of International and Comparative Law.

Michael Wei, L. M. (2013, Nisan 09). *Reliably Erasing Data From Flash-Based Solid State Drives.* The Advanced Computer Systems Association: http://static.usenix.org/events/fast11/tech/full_papers/Wei.pdf adresinden alınmıştır

Middleton, B. (2002). *Cyber Crime Field Handbook.* Florida: Auerbach Publications.

Middleton, B. (2005). *Cyber Crime Investigator's Field Guide.* Florida: CRC Press.

Mueller, L. (2013, Mart 28). *Computer Forensic Hard Drive Imaging Process Tree for Basic Training.* http://www.forensickb.com/2010/12/computer-forensic-hard-drive-imaging_11.html: http://2.bp.blogspot.com/_rX7Jddr9KTM/TQD6GXIOwiI/AAAAAAAAi5Q/Z76iSlXRoJI/s1600/Image+Process+flow+chart.png adresinden alınmıştır

Mukasey, M. B., Sedgwick, J. L., & Hagy, D. W. (2008, Nisan). *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition.* National Institute of Justice: http://www.ncjrs.gov/pdffiles1/nij/219941.pdf adresinden alınmıştır

Optik Disklerin Ömrünü Ne Belirliyor. (2013, Nisan 05). www.chip.com.tr: http://www.chip.com.tr/haber/optik-disklerin-omrunu-ne-belirliyor_34753.html adresinden alınmıştır

Özdilek, A. O. (2002). *İnternet ve HUKUK.* İstanbul: Papatya Yayıncılık.

Öztürkci, H. (2009). Adli Bilişim'e Giriş ve Microsoft Sistemlerinde Adli Bilişim Temelleri. İstanbul.

Philip, A., Cowen, D., & Davis, C. (2009). *Hacking Exposed Computer Forensics Second Edition.* A.B.D.: mhprofessional.

Pogue, C., Altheide, C., & Haverkos, T. (2008). *UNIX and Linux Forensic Analysis DVD Toolkit.* Burlington: Syngress Publishing, Inc.

Pro-G Proje Bilişim Güvenliği ve Araştırma San. (2003). *Bilişim Güvenliği.* Türkiye: Pro-G ve Oracle.

Schweitzer, D. (2003). *Incident Response: Computer Forensics Toolkit.* Indianapolis: Wiley Publishing, Inc.

Shinder, D. L. (2002). *Scene of the Cybercrime: Computer Forensics Handbook.* United States of America: Syngress Publishing.

Shipley, T. G., & Door, B. (2012). *Forensic Imaging of Hard Disk Drives.* Nevada: U.S. Department of Justice.

SIFT Workstation 2.14 Capabilities. (2013, Mayıs 06). SANS Computer Forensics Training, Incident Response: http://computer-forensics.sans.org/ adresinden alınmıştır

Sınar, H. (2001). *İnternet ve Ceza Hukuku.* İstanbul: Beta Basım.

Sırabaşı, V. (2003). *İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz (İNTERNET REJİMİ).* Ankara: Adalet Yayınevi.

Sobey, C. H. (2004). *Recovering Unrecoverable Data.* A.B.D.: ChannelScience.

Sommer, P. (2012). *Digital Evidence, Digital Investigation and E-Disclosure: A Guide to Forensic Readiness.* United Kingdom: IAAC.

Steganography. (2013, Mayıs 06). ÇözümPark Bilişim Sözlüğü: http://sozluk.cozumpark.com/goster.aspx?id=679&kelime=Steganography adresinden alınmıştır

Şirikçi, A. S., & Cantürk, N. (2012, Cilt 5, S.3). Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi. *Bilişim Teknolojileri Dergisi*, 29.

Tamay, G. (2011, Haziran 10). *II. Bilgi Teknolojileri Yönetişim veDenetim Konferansı.* Bilgi Teknolojileri Yönetişim ve Denetim Konferansı: http://www.btyd.org/2011/sunum/tgokturk.pdf adresinden alınmıştır

The Sleuth Kit. (2013, Mayıs 06). The Sleuth Kit (TSK) & Autopsy: Open Source Digital Investigation Tools: http://www.sleuthkit.org/sleuthkit/index.php adresinden alınmıştır

U.S. Department of Homeland Security. (2006). *Best Practices For Seizing Electronic Evidence.* A.B.D.: United States Secret Service.

U.S. Department of Justice Office of Justice. (2001). *Electronic Crime Scene Investigation: A Guide for First Responders.* Washington: PhotoDisc.

US government organization. (2012, 05 10). *Computer Forensics.* www.us-cert.gov: http://www.us-cert.gov/reading_room/forensics.pdf adresinden alınmıştır

Vacca, J. R. (2005). *Computer Forensics - Computer Crime Scene Investigation Second Edition.* Boston, Massachusetts: CHARLES RIVER MEDIA.

Volonino, L., & Anzaldua, R. (2008). *Computer Forensics For Dummies.* Indianapolis: Wiley Publishing, Inc.

Whitcomb, C. M. (Spring 2002). An Historical Perspective of Digital Evidence: A Forensic Scientist's View. *International Journal of Digital Evidence*, 2.

Yavuzcan, A. E. (2010, Nisan 08). *Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma (cmk 134).* http://www.hukuki.net: http://93.187.202.7/entry.php?4-Bilgisayarlarda-bilgisayar-programlarinda-ve-kutuklerinde-arama-kopyalama-ve-elkoyma-(cmk-134) adresinden alınmıştır

ŞEKİLLER DİZİNİ

ADLİ BİLİŞİMDE DELİLLERİN TOPLANMASI ve İNCELENMESİ

1. Giriş

İnsanoğlu var olduğu ilk zamandan beri suç ta var olmuştur. İnsanlığın tarih boyunca gelişiminde yer alan buluşlar iyilere büyük hizmetler ettiği gibi kötülere de yeni olanaklar sunmuştur. İnsanoğlu neyi hangi amaçla kullanacağına kendisi karar vermektedir. İyi insanların mutfakta ekmek keserken kullandığı bıçak kimi zaman kötü insanların elinde suç aleti olarak da karşımıza çıkmaktadır. İnsanlığın tarihi gelişimini gözümüzün önüne getirecek olursak sanayi olarak gelişim sağlandıkça insanların daha rahat ve daha ferah bir hayat sürdüğünü, imkânlarının genişlediğini, hayat standartlarının yükseldiğini çok rahatlıkla göreceğimiz gibi; buna paralel olarak suç işlemenin de kolaylaştığını, yeni imkânlara sahip olduğunu ve yeni suç çeşitlerinin ortaya çıktığını görebileceğiz. Bilgisayarlar veya daha geniş bir tabirle bilişim aygıtları iyi insanların elinde işleri kolaylaştırma amacına hizmet ederken, kötülerin elinde ise suç işleme amacına hizmet edebilmektedir. Gerçek hayatta güncel olarak rastladığımız suç tiplerini artık dijital ortamda da sıkça görmekteyiz[1]. Teknolojinin hızla gelişmesi ve insanların hayatında vazgeçilmez bir şekilde yer alarak iş hayatının ve sosyal hayatın bir parçası olmasına paralel olarak; teknoloji kullanılan, teknoloji hedef alınan veya teknolojiden yardım alınan suç oranlarında artış olmuştur. Bu sebeple de Adli Bilişim'in hukukumuzdaki önemi de hızla artmaktadır. Bu yazıda yeni bir adli bilim dalı olan Adli Bilişim disiplininin uygulama süreci anlatılacaktır.

2. Kavramlar

Adli Bilişim konusunun detaylarına girmeden önce Adli Bilişim ile ilgili bazı kavramları açıklayalım.

---

[1] Dokurer, S., Saylı, M., & Akdeniz, D. (2001). *Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar.* Bursa: Bursa İl Emniyet Müdürlüğü. s. 87

2.1. Bilişim Kavramı

İngilizce "informatics" ve Fransızca "informatique" sözcüklerine karşılık dilimizde enformatik olarak kullanılan bilişim[2] terimi; insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi. Bilgi olgusunu, bilgi saklama, erişim dizgeleri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararı gözeterek inceleyen uygulamalı bilim dalı. Disiplinler arası özellik taşıyan bir öğretim ve hizmet kesimi olan bilişim bilgisayar da içeride olmak üzere, bilişim ve bilgi erişim dizgelerinde kullanılan türlü araçların tasarlanması, geliştirilmesi ve üretilmesiyle ilgili konuları da kapsar. Bundan başka her türlü endüstri üretiminin özdevimli[3] olarak düzenlenmesine ilişkin teknikleri kapsayan özdevim alanına giren birçok konu da, geniş anlamda, bilişimin kapsamı içerisinde yer alır.[4]

Kul bilişimi; işlenmiş ve basit düzeyde de olsa anlam içeren veridir[5] şeklinde tanımlamıştır.

Öğretide bilişim sözcüğünün birçok tanımı yapılmıştır. Bu tanımlarda dikkati çeken ortak yön; bilginin işlenmesi, aktarılması, depolanması ve bunların bilgisayar aracılığıyla yapılmasıdır[6].

---

[2] Türk Dil Kurumu, Bilgisayar Terimleri Karşılıklar Kılavuzu, http://tdkterim.gov.tr/?kategori=bakdetay2&sozid=BTK

[3] Özdevim (veya otomatizm) kendine özgü devinim, hareket anlamına gelip kullanıldığı bağlama göre anlam değişimi gösteren bir sözcüktür.

[4] Türk Dil Kurumu, Bilişim Terimleri Sözlüğü, http://tdkterim.gov.tr/?kelime=bili%FEim&kategori=terim&hng=md

[5] KUL, Bilişim Sistemleri Temelleri ve Uygulamaları, 1. Basım Şubat 2009, s.17

[6] Kızıltan, "5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme

2.2. Adli Bilişim Kavramı

Adli Bilişim; bir olay yeri incelemesi veya bir kurban üzerinde yapılan otopsinin eşdeğeridir.[7] Sayısal verileri elde etme, muhafaza etme ve çözümleme işlemlerinin delilin gereklerine uygun olarak mahkemeye sunulması aşamasına kadar uygulanması[8]; özel inceleme ve analiz teknikleri kullanılarak, bilgisayarlar başta olmak üzere, tüm elektronik medya üzerinde yer alan potansiyel delillerin toplanması amacıyla, elektronik aygıtların incelenmesi süreci kısaca Adli Bilişim (Computer Forensic)[9] olarak açıklanmaktadır. Ancak Adli Bilişim, İngilizce karşılığı olarak dünya genelinde kullanılmakta olan "Computer Forensic" terimine tam olarak karşılık gelmemektedir ve hatta Adli Bilişim Bilimi; Computer Forensic terimini de içine kapsayan ve daha geniş anlama ve uygulama alanına sahip bir bilim dalıdır[10]. "Computer Forensic" anlam olarak adli bilgisayar incelemesi anlamına gelmekte iken Adli Bilişim'in ülkemizde günümüzde uygulama alanları; cep telefonu incelemeleri, databank incelemeleri, ses kayıt cihazı incelemeleri, şifre çözme, stenografi, güvenli veri silme, gizli bilgilerin/belgelerin tespit edilmesi, casus yazılım tespiti… gibi bilgisayar incelemesi dışında birçok inceleme çeşidi sıralanabilir.

Ve Bozma Suçları" başlıklı İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, s.3

[7] BOREK, http://www.sans.org/reading_room/whitepapers/incident/computer-forensics-weve-incident-investigate_652

[8] Türk Dil Kurumu, Kriminal Terimleri Sözlüğü, http://www.tdkterim.gov.tr/?kategori=terimarat2&s3oz5k0t=KRM&kelime=adli+bili%FEim

[9] Keser Berber, Adli Bilişim, CMK md 134 ve Düşündürdükleri…, http://www.leylakeser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html

[10] Whitcomb, C. M. (Spring 2002). An Historical Perspective of Digital Evidence: A Forensic Scientist's View. *International Journal of Digital Evidence*, 2.

3. Adli Bilişim

Adli bilişim bilimi, hukuk bilimi ve bilgisayar bilimi unsurlarını birleştirerek; bilgisayar ağlarından, kablosuz bağlantılardan ve veri depolama aygıtlarından mahkemeler tarafından kabul edilebilir nitelikte deliller toplama ve analiz etme[11] ile ilgilenir. Yani Adli Bilişim, dijital delillerin toplanması ve incelenmesi ile ilgilenmekte ve bununla birlikte diğer adli bilimler gibi adaletin sağlanabilmesine yardımcı olabilmek amacına hizmet etmektedir. Bu hizmeti, suça konu olayların veya uyuşmazlıkların içerisinde yer alan dijital cihazlara delil niteliği kazandırarak yapmaktadır.

Koltuksuz, Adli Bilişimi; elektromanyetik-elektrooptik ortam(lar)da muhafaza edilen ve/veya bu ortamlarca iletilen; ses, görüntü, veri/bilgi veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede sayısal (elektronik-dijital) delil niteliği taşıyacak şekilde:

- Tanımlanması,
- Elde edilmesi,
- Saklanması,
- İncelenmesi ve
- Mahkemeye sunulması çalışmaları bütünüdür[12], şeklinde tanımlamıştır.

Adli konu, ister bilişim sistemleri üzerinde gerçekleşmiş olsun, isterse konu bilişim ile ilgili olmasın; konunun aydınlanmasına yardımcı olabilecek bir bilişim aygıtı varsa, orada Adli Bilişim Biliminin katkısı başlamaktadır. Yani Adli Bilişim sadece bilişim suçlarına özgü bir uygulama alanına sahip değildir.

---

[11] US government organization. (2012, 05 10). *Computer Forensics.* www.us-cert.gov: http://www.us-cert.gov/reading_room/forensics.pdf

[12] Koltuksuz, "Adli Bilişime Giriş" s.43, Adli Bilişim Günü, Yaşar Üniversitesi, 7 Haziran 2010, İzmir

Günümüzde artık birçok adli konuda cep telefonları, taşınabilir bellekler, bilgisayarlar gibi bilişim aygıtlarından alınan verilerle/bilgilerle elde edilen delillerden soruşturma ve kovuşturma aşamasında faydalanılmaktadır.

Adli bilişimin hukukumuzda yeni bir kavram olduğu söylenebilir. Suç profilleri arasına hızlı bir şekilde giren bilişim suçları ile ilgili deliller geleneksel delillerden farklı olarak değerlendirilmeye tabi tutulması gereken bir yapıya sahiptir. Delillerin toplanması ile ilgili geleneksel olarak uygulanan yöntemler ve dikkat edilmesi gerekli hususlar, bilişim aygıtlarını delil olarak toplarken de uygulanmalı ve dikkat edilmelidir. Ancak bunun yanı sıra bilişim aygıtları için ayrıca dikkat edilmesi ve uygulanması gerekli özel yöntemler mevcuttur. Bilişim aygıtlarının delil niteliği kazanabilmesi için çok hassas ve çok teknik işlemlerden geçirilmesi gerekmektedir.

3.1. Adli Bilişim Biliminin Cevap Aradığı Sorular

Diğer adli bilim dallarında olduğu gibi Adli Bilişim Bilimi de konusunu ilgilendiren bazı soruların cevaplarını aramaktadır/vermektedir. Fikir kazandırması açısından Adli Bilişim Biliminin hangi soruların cevabını vermeye çalıştığını aşağıda yazılı olan sorulardan anlayabiliriz.

- Bahse konu olay ile ilgili suç unsuru var mı?
- Hangi bilişim aygıtı/aygıtları delil olabilir?
- Bahse Konu suç hangi bilişlim aygıtı kullanılarak işlendi?
- Adli kopya olay yerinde mi alınmalıdır?
- Hangi bilişim aygıtı/aygıtları e-delil olarak incelenebilir?
- Bilişim aygıtı/aygıtları Wipe'lanmış mı?
- Bilişim aygıtı/aygıtları formatlanmış mı?
- Silinmiş dosyalar ve kaybolan verilerin nelerdir?
- Bilişim aygıtında zararlı/casus yazılım var mı?

- Şifreli klasör/dosya var mı?
- Şifreli verilerin şifresi nedir?
- Verinin üzerine veri yazılmasının engellenmesi için gerekli önlemler alınmış mı?[13]
- Bahse konu e-posta hesabı bu bilgisayarda oturum açtı mı?
- Bilişim aygıtı/aygıtları içeriğinde suç ile ilgili delil var mıdır?
- Müştekinin bilgisayarından şüpheliye ulaşılabilir mi?
- Dijital cihazın kullandığı kablolu/kablosuz modem bilgileri nelerdir?
- Cep telefonlarındaki, navigasyon cihazlarındaki ve diğer bilişim aygıtlarındaki GPS kayıtları nelerdir?
- Bahse konu cihazın kullanıcısı kimdir?
- Cihaz vasıtasıyla en son yapılan görüşme veya yazışmalar nelerdir?
- DVR (Görüntü Kayıt Cihazı)'da silinmiş görüntüler nelerdir?
- Soruşturma konusu bilişim aygıtının içerisinde hangi suç unsurları vardır?
- Cihazın veri gizleme/şifreleme kabiliyeti var mıdır?
- E-delillerin teknik özellikleri ve kapasitesi nelerdir?
- E-delillerin içerisinde suç işlemeye amaç veya araç olarak kullanılabilecek uygun yazılım, uygulama veya kodlar var mıdır?
- İncelenen e-delilde, tespit edilemeyen diğer e-delille/e-delillerle ilgili bilgi var mı?
- İncelenen e-delillerin hangisinde suçun işlendiğine dair bilgi vardır?
- E-delilin veya delillerin adli kopyalarının veri bütünlüğüne zarar gelmiş midir?
- Müştekinin bilgisayarına uzaktan erişim var mı?
- Pos cihazları üzerlerinde kullanılan kredi kartlarının bilgileri kopyalıyor mudur?

---

[13] Information Security and Forensics Society. (2009). *Computer Forensics Best Practices.* Hong Kong: ISFS. s.27

- Mobil cihazların imei numaraları orijinal midir?
- E-delilden alınan adli kopya hangi yazılım veya donanım ile alınmıştır?
- Olay ne zaman oldu?
- Sistem en son ne zaman yedeklendi?[14]
- Sunucu üzerinde yapılan işlemler hangi kullanıcı tarafından yapılmıştır?
- Uçucu belleklerde bulunan kullanıcı adı ve şifreler nelerdir?
- Dijital materyalde bilgi saklama, şifreleme, yok etme, engelleme (anti-forensics) yazılımları var mı?
- Yazıcı içerisinde hafıza birimi var mıdır, hangi bilgilere ulaşılabilir?
- Modem içerisinde IP, MAC ve kullanıcı log kayıtlatı var mıdır, varsa nelerdir?
- Databank içerisinde hafıza birimi var mıdır, varsa hangi bilgiler mevcuttur?
- Oyun konsolu içerisinde hafıza birimi var mıdır, varsa hangi bilgiler mevcuttur?
- Uydu alıcı içerisinde hafıza birimi var mıdır, varsa hangi bilgiler mevcuttur?
- TV içerisinde hafıza birimi var mıdır, varsa hangi bilgiler mevcuttur?
- E-delil içeriğinde değişiklik yapılıp yapılmadığı?
- Sistemin saat dilimi ve BIOS saati, gerçek saati gösteriyor mudur?
- İncelenen sistem üzerinde proxy yazılımları mevcut mudur?
- İncelenen bilgisayarda işletim sistemi mevcut mudur?
- İncelenen e-delil herhangi bir bulut sistemine bağlanıyor mudur?
- İncelenen e-delil üzerindeki yerel kullanıcı hesapları haricinde herhangi bir active directory yapısına dahil bir kullanıcı hesabına bağlanıyor mudur?

---

[14] Middleton, B. (2005). *Cyber Crime Investigator's Field Guide.* Florida: CRC Press. s.6

- E-delil üzerinde 3. şahıslara ait banka hesap bilgileri ve kredi kartı bilgileri var mıdır?
- E-delil üzerinde internet üzerinden yapılan havale veya EFT bilgisi var mıdır?
- E-delil üzerindeki sistemin açma ve kapanma tarihleri nelerdir?
- E-delilde kullanılan işletim sistemi üzerindeki kullanıcı hesapları nelerdir?
- İşletim sisteminin kurulum tarihi nedir?
- E-deliller üzerinde kayıtlı dosyaların metadata bilgileri (oluşturulma, son erişim, değiştirilme, exif vb.) nelerdir?
- E-delilde kullanılan MSN, ICQ, Whatsapp, Skype, Yahoo Messenger, Facebook, Gtalk, Tangoo, Twitter, Viber, MIRC, vb. programlarda kayıtlı kullanıcı adları, takma isimler, telefon numaraları, e-posta adresleri ve anlık ileti kayıtları nelerdir?
- E-delil üzerinde kullanılan internet tarayıcı programlarından ulaşılabilen (explorer, firefox, chrome, opera, safari, yandex vb.) gezinti ve arama geçmişleri, şifreleri, indirilen dosyalar, sık kullanılanlar ve kullanıcı bilgileri nelerdir?
- E-delil içerisinde kullanılan dosya paylaşım programları var mı, bunlara ait bilgiler ve paylaşılan dosyalar nelerdir?
- E-delil ile bağlantı sağlanan FTP adresleri var mı, IP adresi kullanıcı adı ve şifreleri nelerdir?
- Cihazda kullanılmış olan harici bellekler nelerdir, marka, model, seri numarası bilgileri nelerdir?
- Dijital fotoğraf makineleri ve video kameralarında görüntüler var mıdır, görüntülerdeki GPS koordinat bilgileri nelerdir?
- Elde edilen görüntülerin hangi makinede çekildiği, koordinat bilgileri, tarih ve saat bilgileri nelerdir?
- Navigasyon cihazlarındaki ve araç takip sistemlerindeki koordinat ve geçmiş bilgileri nelerdir?

- CD-DVD'lerin yazılma tarihleri, oturum bilgileri ve kullanılan yazma programının bilgileri nelerdir?
- Cihazda uzaktan erişime imkan sağlayan yazılım var mıdır? Erişim sağlanan ya da sağlayan cihazların (IP, kullanıcı adı vs) bilgileri nelerdir?
- E-delil kullanılarak diğer bilişim aygıtlarına virüs bulaştırılmış mıdır?
- E-delil DDOS saldırısında kullanılmış mıdır?
- E-delil içerisinde sahtecilik işlemleri yapmaya elverişli programlar var mıdır, bu programlarla üretilmiş doküman var mı?
- E-delil içerisinde narkotik madde üretimi, tüketimi, dağıtımı ve satışı ile ilgili bilgi veya dokuman var mıdır?
- E-delil içerisindeki log kayıtlarının içerisinde sisteme izinsiz/yetkisiz erişime ait tarih, saat, IP ve kullanıcı bilgileri var mıdır?
- E-delil kullanılarak internet sitesine yorum yazılmış mıdır?
- E-delil içerisinde steaganografi ile gizlenmiş herhangi bir bilgi, belge veya doküman var mı?
- E-delil içerisinde güvenlik yazılımları mevcut mudur, lisanslı mıdır, aktif midir, güncel midir?
- E-delil üzerinde online kumar oynamaya imkan sağlayan yazılım veya donanım var mıdır?
- E-delil üzerinde herhangi bir sanal makine var mıdır?
- E-delil üzerinde kurulu olan programlar ve kurulum tarihleri nelerdir?
- E-delil üzerinden silinen dosyanın hangi kullanıcı tarafından silindiğine dair bilgiler var mıdır?

Yukarıda sıralanan sorular adli bilişim biliminin cevap aradığı soruların neler olabileceği hakkında yüzeysel olarak fikir verecektir. Ancak unutulmamalıdır ki adli bilişim incelemelerinin büyük çoğunluğunda yukarıdaki soruların sadece bir tanesine cevap aranmamakta, bir olay ile ilgili olarak birçok soruya birden cevap verilmesi gerekmektedir. Bu aşamada bir olay ile ilgili olarak

e-delil üzerinde hangi soruların cevaplarının aranması ve bulunması gerekeceğine karar vermede; adli bilişim incelemesini yapan kişinin bilgisine, iş tecrübesine, iş tutuş şekline, analitik düşünce kabiliyetine, uzmanlığına, olaya bakış açısına vb. gibi birçok etkenin önemli olduğunu unutmamak gerekir. Bütünlüğü bozulmamış e-deliller üzerinde yapılan incelemelerde her incelemeci aynı uygulamaları yaptığında aynı sonuca ulaşacaktır, ancak suç konusu ile ilgili yapılacak tespitler için yapılan uygulamalar inceleme yapana göre değişiklik gösterebilecektir. Bazen bir incelemeci kullandığı bir metot ile sonuca ulaşamazken aynı e-delil üzerinde başka bir incelemecinin başka bir metot kullanarak hedeflenen sonuca ulaşabileceği göz ardı edilmemelidir.

3.2. Adli Bilişimin Uygulama Alanları

Ülkemizde bilişimin hızla önem kazanmasıyla birlikte adli bilişim de sürekli artan bir ivmeyle gelişmekte ve her geçen gün uygulama alanlarına yenileri eklenmektedir.

Önceleri özellikle ceza davalarında başvurulan bir uygulama alanı olarak kendini gösteren Adli Bilişim Bilimi şimdilerde hukuk uyuşmazlıklarında da sıkça kullanılır olmuştur. Şirketlerde bu alana sıkça başvurur hale gelmiştir. Adli Bilişimi yakından ilgilendiren veri kurtarma ve veri imha konusunda şirketler bünyelerinde adli bilişim uzmanları çalıştırmakta veya sıklıkla adli bilişim uzmanlarından bu konularda yardım almaktadırlar. İş süreçlerinin her geçen gün bilişimle kesişen kısımlarının artması ve iç içe olan bir hal alması ile Adli Bilişim uygulama alanları da artmaya devam edecektir.

Adli Bilişimin uygulama alanlarına bazı örnekler şu şekilde sıralanabilir:

- Hukuksal uyuşmazlık veya yargılamalarla ilgili incelemeler
- Veri saklama(Koruma)
- Veri silme(Geri getirilemeyecek şekilde imha etme)

- Veri kurtarma(yanlışlıkla silme, veya yazılımsal veya donanımsal arızalardan dolayı veri kaybı gibi durumlarda)
- Şifreleme(verinin güvenli bir şekilde taşınmasını/muhafazasını sağlama)
- Şifre Çözme(şifrelenmiş ve ulaşılamayan veriye ulaşmayı sağlama)
- Gizlenmiş dosya bulma
- Stenografi(Veri altına gizlenen verinin tespiti)
- Suiistimal önleme, tespit ve inceleme çalışmaları
- Soruşturmalar (Yasal / Şirket içi)
- Finansal denetimler
- İç Denetim Çalışmaları
- İç Kontrol Çalışmaları
- Kontrol testleri
- Ticari anlaşmazlıkların incelenmesi ve analizi
- Fikri haklar ile ilgili uyuşmazlıklar
- Performans ölçümleri [15]

3.3. Adli Bilişim Biliminin Faydaları

Bilgisayar yazılım ve donanımlarının çeşitleri konusunda geniş bir yelpazede bilgi sahibi olan adli bilişim uzmanı, Adli Bilişim Bilimini kullanarak keşif sırasında taraflara ve mahkemeye yardımcı olacaktır[16]. Ancak Adli bilimler içerisinde yer alan Adli Bilişim Bilimi sadece adaletin sağlanmasına hizmet etmemekte, başka birçok uygulama alanında Adli Bilişimden faydalanılmaktadır. Adli Bilişimin sağladığı faydalardan bazıları şunlardır:

---

[15] Tamay (2011, Haziran 10). *II. Bilgi Teknolojileri Yönetişim ve Denetim Konferansı.* Bilgi Teknolojileri Yönetişim ve Denetim Konferansı: http://www.btyd.org/2011/sunum/tgokturk.pdf

[16] Keser Berber, L. (2004). *Adli Bilişim (Computer Forensic).* Ankara.s.41

- Bilişim öğelerinin incelenmesi sırasında hiçbir potansiyel delilin kaybedilmemesi,
- Analiz işlemi esnasında analiz edilen bilgisayar sistemlerinin virüslerden etkilenmemesi,
- Delillerden elde edilen bulguların çeşitli sayısal etkilerle kaybedilmesinin engellenmesi,
- Sürekli bir gözlemin kurularak sürdürülmesi,
- Olay yerindeki iş süreçlerinin delil toplama sürecinden çok az veya hiç etkilenmemesinin sağlanması[17],
- Adli inceleme esnasında incelenen materyalin kullanıcısıyla ilgili özel olabilecek verilerin gerektiği hassasiyetle incelenerek ifşa edilmesinin engellenmesi,
- Suçsuz bireyin ceza alarak mağdur olmasına engel olması,
- Suçlu bireyin cezasız kalmasına engel olarak, adaletin sağlanmasına yardımcı olması.

4. Dijital/Elektronik Delil Nedir?

Delil, kelime anlamı olarak: insanı aradığı gerçeğe ulaştırabilecek iz, emare anlamına gelmektedir[18]. Hukuk açısından ise delil: uyuşmazlık konusu olayın gerçekleşip gerçekleşmediği konusunda mahkeme heyetinde bir kanı oluşturmaya yarayan ispat aracıdır[19], bir hukuki ihtilafı çözmeye veya suç fiillini ispata

---

[17] *Adli Bilişimin Sağladığı Faydalar*. (2009). E-Keşif ve Adli Bilişim: http://www.e-kesif.com/2008/05/adli-bilisimin-faydalari.html

[18] Türk Dil Kurumu, Güncel Türkçe Sözlük, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.504cb3d868c040.17628760

[19] Bayraktar, Y. D. (2011, sayı:25). MUHAKEMELERDE DELİLLERİN ÖNEMİ. *Sosyal Bilimler Dergisi*, s. 9.

yarayan ve ikamesi hukuk tarafından yasaklanmamış her şeye (canlı, cansız, yazılı-sözlü) delil veya ispat vasıtaları denilmektedir[20].

Delil toplamak oldukça zordur bir de bu delil elektronik olduğunda araştırmacı bazı ekstra karmaşıklıklarla karşı karşıya gelecektir[21]. Klasik suçların soruşturma evresinde delil, genellikle suç işlenen alandan elde edilir. Bilişim suçlarında delil elde edilecek alan ise çoğunlukla bilişim sistemidir. Bu sistemde ilk akla bilgisayarlar gelmekte ise de, sistemle bir şekilde bağlanabilen ve sistemle ilgili bilgi depolayabilen pek çok unsur da, bilişim sistemi içerisinde değerlendirilmelidir[22]

Bilişim aygıtlarından elde edilen delillerin isimlendirilmesi konusunda yaygın olarak kullanılan veya standartlaşmış olan bir kullanım mevcut değildir. Bu konu hakkında günümüzde genel olarak elektronik delil(e-delil), dijital delil, sayısal delil şeklinde kullanımlar mevcuttur. Bunlar, elektronik aygıtların suçlarda kullanılır olması ve daha sonrasında da uyuşmazlıkları aydınlatmada delil olarak elektronik aygıtlara başvurulmasıyla doğal olarak ortaya çıkmış kullanımlardır[23].

E-deliller fiziksel ve mantıksal şekilde temsil edilirler. Fiziksel şekil, verinin elle dokunulabilir bir cihaz içerisindeki temsilini içerir. Potansiyel e-delilin mantıksal şekli ise bir cihaz içerisindeki verinin sanal olarak varlığına işaret eder[24].

---

[20] Kaygısız, M. (2005). *Adli Bilimler.* Ankara: Seçkin. s. 29

[21] Vacca, J. R. (2005). *Computer Forensics - Computer Crime Scene Investigation Second Edition.* Boston, Massachusetts: CHARLES RIVER MEDIA. s. 217

[22] Karagülmez, D. D. (2009). *Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri.* Ankara: Seçkin Yayıncılık.s. 287-288.

[23] Bu konu hakkında günümüzde genel olarak elektronik delil, dijital delil, sayısal delil, e-delil şeklinde kullanımlar mevcuttur ancak bu yazıda tercihen "elektronik delil" kullanılacaktır.

[24] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre:

E-delil dendiğinde akla sadece bilişim suçlarını aydınlatmada kullanılan deliller gelmemelidir. E-deliller suçun konusu ne olursa olsun, suçun aydınlanmasında faydalanabilecek ve suçu aydınlatmada kullanılabilecek elektronik ortamda kayıtlı olan bilgi anlaşılmalıdır.

E-delil, bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve verilerdir. E-deliller tıpkı parmak izi ve ya DNA delili gibi çoğu kez gizli, görünmeyen bir yapıya sahiptir. Sınırları kolayca ve hızlı bir şekilde geçebilir[25]. Hassastır ve kolayca değiştirilebilir, tahrip edilebilir veya yok edilebilir[26].

Bilgisayar tabanlı E-deliller, belgesel delillere uygulanan aynı kurallara ve aynı kanunlara tabidir[27]. E-deliller, bilginin fiziksel ortamdan elektronik ortama geçmiş hali olarak düşünülebilir. Bu bakımdan E-deliller belgesel delillerle geniş çerçevede yaklaşıldığında ilk aşamada aynı kurallar ve aynı kanunlara tabi olsalar da, delillerin araştırılması, tespit edilmesi ve sunulması yönünden uygulanacak yöntemlerin farklı olması sebebiyle diğer delillerden ayrıca kendine özgü yaklaşım prensipleri mevcuttur.

International Organization for Standardization, International Electrotechnical Commission. s. 8

[25] Keser Berber, L. (2004). *Adli Bilişim (Computer Forensic).* Ankara.s.46

[26] Anderson, M. R. (2012, Eylül 09). *Computer Evidence Processing Step 1 -- Seizure of the Computer*. Government Technology: http://www.govtech.com/magazines/gt/Computer-Evidence-Processing-Step-1---.html?page=1

[27] Chris Simpson, A. P. (2012, Eylül 09). *Good Practice Guide for Computer-Based Electronic Evidence.* 7Safe Information Security, eDiscovery, Penetration Testing, Training, PCI DSS, Computer Forensics: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf, s.4.

4.1. E-Delil Nitelikleri Nelerdir?

E-delillerin soruşturma veya kovuşturma safhasında kullanılabilmesi için klasik delillerin taşıdıkları nitelikleri taşımalıdır.

- **Kabul edilebilir(admissible[28]) olmalıdır.**
  E-delil, dava sırasında hakim veya başka insanlar tarafından kabul edilebilir olmalıdır.

- **Gerçek ve aslına uygun(authentic[29]) olmalıdır.**
  Soruşturma veya kovuşturma altındaki konu ile ilgili doğrudan bir nedensellik bağı veya destekleyici mantıksal bağlar olması gerekir. Nedensellik bağı (illiyet rabıtası) aynı zamanda suçun kanun tanımında yer alan maddi unsurlarındandır ve meydana gelen netice ile fail arasındaki neden-sonuç ilişkisini ifade etmektedir[30]. Adli kopyası alınan e-delilin soruşturmayla ilgili olduğu ortaya konulabilmelidir[31].

- **Eksiksiz ve tam(complete[32]) olmalıdır.**

---

[28] Jones, D. A., & Vazlli, D. C. (2008). *Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility.* Waltham(United States): Syngress. s.10

[29] A.g.e. s. 10

[30] Henkoğlu, T. (2011). *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi.* İSTANBUL: PUSULA. s. 6-7)

[31] [31] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s. 6

[32] Jones, D. A., & Vazlli, D. C. (2008). *Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility.* Waltham(United States): Syngress. s.10

Elde edilebilen tüm deliller toplanmalıdır. Bu deliller yalnızca, failin suçlanmasına ilişkin değil, varsa suçsuzluğuna ilişkin olanları da kapsamalıdır. Nitekim 5271 sayılı Ceza Muhakemesi Kanunu'nun[33] 170. maddesinnin (4) ve (5) numaralı fıkralarına göre, iddianamede, yüklenen suçu oluşturan olaylar, mevcut delillerle ilişkilendirilerek açıklanmalı; iddianamenin sonuç kısmında, şüphelinin sadece aleyhine olan hususlar değil, lehine olan hususlarda ileri sürülmelidir.[34] Sadece maddi olmamalıdır. Şüphelinin suçlu olduğunu veya suçsuz olduğunu kanıtlayan bir delil olmalıdır.

- **Güvenilebilir(reliable[35]) olmalıdır.**

  E-delil güvenilir olmalıdır. Analiz için kabul edilmiş prosedürlere uygunluğuna ve doğruluğuna şüphe edilmemelidir. E-delilin göründüğü gibi olmasını garanti altına almaktır[36]. Başka bir deyişle güvenilirlik, sistemden ne yapmasını bekliyorsak, sistemin de eksiksiz ve fazlasız olarak bunu yapması ve her çalıştırıldığında aynı şekilde davranması olarak tanımlanabilir[37].

---

[33] Ceza Muhakemesi Kanunu yazının devamında CMK olarak anılacaktır.

[34] Karagülmez, D. D. (2009). *Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri.* Ankara: Seçkin Yayıncılık.s. 290.-291.

[35] Jones, D. A., & Vazlli, D. C. (2008). *Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility.* Waltham(United States): Syngress. s.10

[36] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s. 6

[37] Pro-G Proje Bilişim Güvenliği ve Araştırma San. (2003). *Bilişim Güvenliği.* Türkiye: Pro-G ve Oracle. s.11

- **İnanılabilir(believeable[38]) olmalıdır.**

  E-delil, kanıtlama değerine sahip olmalıdır. Sanal yapıda olsa da[39], hakim veya taraflar tarafından açıkça anlaşılabilir ve inanılabilir olmalıdır.

- **Yasaya uygun olmalıdır.**

  E-delil, yukarıdaki özelliklere sahip olsa da, yasaya uygun bir şekilde elde edilmemişse veya her ne kadar yukarıdaki özellikleri taşıyor olsa da yasaya uygun elde edilmediği için delil olarak değerlendirilemeyecektir. Örneğin 5271 sayılı CMK'nın 134. maddesine aykırı olarak bilgisayarlarda arama, kopyalama veya elkoyma[40] işlemi yapılmışsa[41], elde edilenler mahkeme tarafından delil olarak değerlendirilmeyecektir.

4.2. E-deliller ile klasik delillerin karşılaştırılması

- Klasik deliller fiziksel olarak bakıldığında içeriği hemen görülebilen ve değerlendirilebilen bir halde bulunurlar. Ancak e-deliller üzerinde bazı çalışmalar yapılarak veya çeşitli teknik araçlar kullanılarak içeriğine ulaşılabilinir.

---

[38] Jones, D. A., & Vazlli, D. C. (2008). *Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility.* Waltham(United States): Syngress. s.10

[39] Karagülmez, D. D. (2009). *Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri.* Ankara: Seçkin Yayıncılık.s. 291.

[40] "elkoyma" terimi "el koyma" şeklinde ayrı şekilde de kullanılmaktadır. Genel olarak hem birleşik hem de ayrı yazılarak kullanılmakta ise de kanun maddelerinde birleşik yazıldığı görüldüğünden burada da birleşik yazılması tercih edilmiştir.

[41] Karagülmez, D. D. (2009). *Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri.* Ankara: Seçkin Yayıncılık.s. 291.

- Klasik deliller fiziksel durumlarından dolayı hızlıca değişebilecek bir yapıya sahip değildirler, e-deliller ise toplama aşamasında bile yanlış müdahale yapıldığında içerikleri kolaylıkla değişebilir, bozulabilir.
- Klasik deliller yapılarından dolayı dış etkenlerle kolay kolay bozulmazken e-deliller manyetik alan, düşme, çarpa, elektrik dalgalanmaları, aşırı ısınma, aşırı soğuma vb. gibi birçok dış etkenlerden kolaylıkla etkilenerek bozulabilmektedirler. Örneğin klasik deliller taşıma sırasında sarsıntılardan, çarpmalardan etkilenmezken, e-deliller şiddetli sarsıntı veya çarpmalarda tamamen bozulabilmekte ve içerisindeki kayıtlı bilgilere ulaşılamamaktadır.
- Klasik deliller üzerinde yapılan değişiklikler dışarıdan bakılarak kolaylıkla fark edilebilmektedir. Ancak e-deliller üzerinde bir değişiklik yapıldığında değişikliğin fark edilmesi dışarıdan bakılarak mümkün olmamaktadır.
- Klasik deliller ilerleyen zaman içinde yapı olarak pek fazla değişiklik göstermemektedir. Ancak e-deliller, sürekli ve hızla gelişen teknoloji ile daha karmaşık ve daha gelişmiş bir yapıya ulaşmaktadır.
- Klasik deliller ebatlarına göre fazla bilgi tutamazken e-deliller çok küçük hacimde çok fazla doküman saklayabilirler.
- Klasik delil olan kağıt dokümanların çoğaltılıp dağıtılması zaman alırken, e-delillerin çoğaltılıp dağıtılması çok daha kolay ve daha hızlıdır

  Kağıttan farklı olarak;
- Bilgisayar veri/bilgileri, insan müdahalesi olmaksızın da zaman içinde değişebilir.
- Bilgisayar veri/bilgileri; ait oldukları ortamlarından ayrıldıklarında anlaşılamaz hale gelebilmektedir.

- Elektronik dokümanlar, çok farklı formatlarda gelebilir, değişkendirler.
- Elektronik veri/bilgiler, zengin gizli bilgileri (yardımcı verileri) ihtiva edebilir.
- Elektronik dokümanların kaynağını tespit etmek bazı durumlarda güç olabilir [42].

4.3. Delil Olabilecek Bilişim Aygıtları

Adli bilişim konusunda delil olabilecek bilişim aygıtlarından önemli olan bazılarını şu şekilde sayabiliriz:

4.3.1. Bilgisayar

Bilişim denilince akla ilk gelen aygıt bilgisayardır. Bilgisayarlar adli bilişimde delil olabildiği gibi delilleri toplamada ve incelemede de kullanılmaktadırlar. Masaüstü bilgisayar, dizüstü bilgisayar(notebook), internet bilgisayarı(netbook), ekran bilgisayar(monitor pc), sunucu bilgisayar(server), ve günümüzde çok sık kullanılmaya başlanan tablet bilgisayar gibi çeşitli şekillerde tasarlanmış halleri mevcuttur.

Şekil 4.1 Bilgisayar örnekleri

Bir bilgisayar sistemi ve onun bileşenleri bir soruşturmadaki en değerli kanıt olabilir. Donanım, yazılım, belgeler, fotoğraflar, görüntü dosyaları, e-posta ve

---

[42] KOLTUKSUZ, "Adli Bilişime Giriş" s.47,48, Adli Bilişim Günü, Yaşar Üniversitesi, 7 Haziran 2010, İzmir

ekleri, veritabanları, finansal bilgiler, internet tarama geçmişi, sohbet günlükleri, arkadaş listeleri, olay günlükleri, daha önce sisteme takılmış olan harici aygıtlara ait tanımlayıcı bilgiler vb. bilgilere bilgisayarlar üzerinden ulaşılabilir. Günümüz teknolojisinde bilgisayarlar üzerinden, sabit diskler, ram'lar; ağ bağlantıları, çalışan programlar gibi delillere ulaşılabilmektedir[43].

4.3.2. Sabit Disk

Sabit diskler uçucu olmayacak şekilde ve hızlıca veri depolayan ve depolanan veriye tekrar ulaşmayı sağlayan aygıtlardır. Elektrik kesildiğinde üzerinde yazılı olan veri silinmez. Dolayısıyla bilgisayar kapandığında disk üzerinde kayıtlı olan veriler silinmeyecektir[44].

Sabit diskler manyetik olarak veri depolama yaparlar. Veri sabit disklerin içerisindeki cam, seramik veya metal plaka üzerinde kaplı olan özel alaşımlı yüzey üzerinde depolanmaktadır. İlk müdahale sırasında herhangi bir bilgisayarın içerisinde takılı durumda olmayan sabit diskler de bulunabilir. Bu sabit diskler sisteme bağlı olmasalar da değerli kanıtları içerebilir[45].

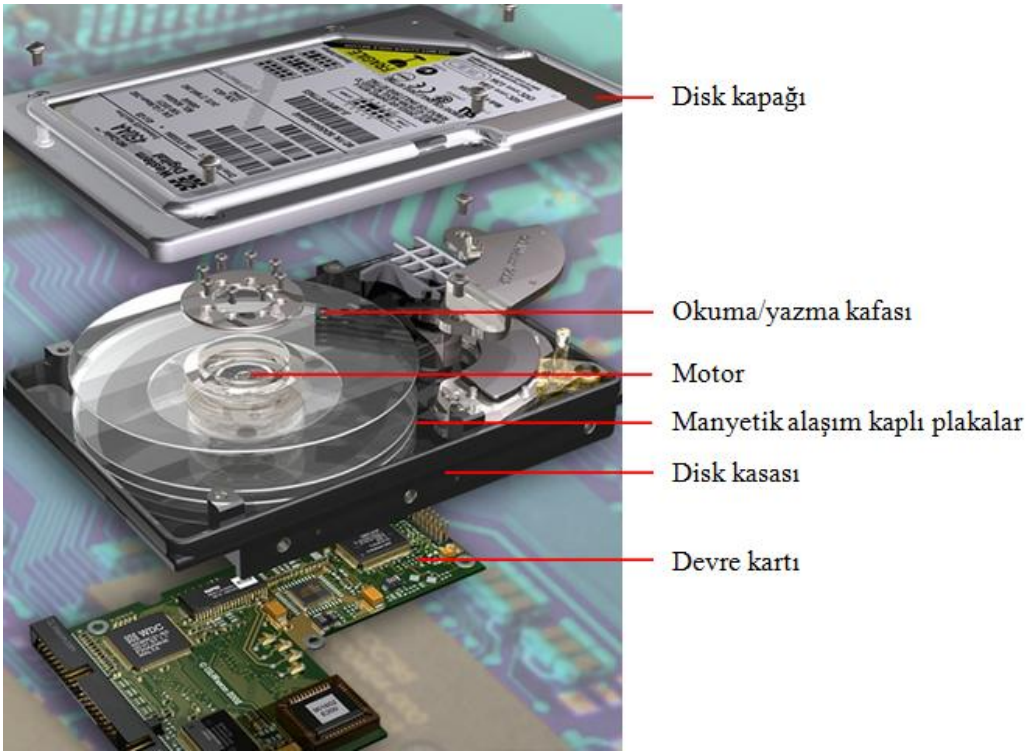
Günümüzde genellikle 2.5" ve 3.5" boyutlu sabit diskler kullanılmaktadır. Sabit diskin içerisindeki ana parçaları gösterir resim aşağıdadır.

---

[43] Mukasey, M. B., Sedgwick, J. L., & Hagy, D. W. (2008, Nisan). *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition.* National Institute of Justice: http://www.ncjrs.gov/pdffiles1/nij/219941.pdf s.2

[44] Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., & Wright, C. (2007). *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators.* Burlington, A.B.D: Syngress Publishing. s.62

[45] Mukasey, M. B., Sedgwick, J. L., & Hagy, D. W. (2008, Nisan). *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition.* National Institute of Justice: http://www.ncjrs.gov/pdffiles1/nij/219941.pdf s.3



Şekil 4.2 Sabit Disk Parçaları[46]

Sabit disklerin sık kullanılan çeşitlerinden örnek resimler aşağıdadır.

Şekil 4.3 Sabit disk çeşitleri[47]

[46] http://www.griffwason.com/images/GriffWason_WesternDigitalCaviar-ExplodedCutaway2.jpg

4.3.3. Harici Disk

Sabit disklerin genellikle plastik veya metal koruyucu kutuların içerisinde bulunduğu ve bağlantıları bu koruyucu kap üzerinden yapılan haline harici diskler denilmektedir. Adli Bilişim delilleri arasında en önemli sayılabilecek bilişim aygıtlarıdır. Önemli olmasının sebebi kullanım amaçlarıyla ilişkilidir. Bu aygıtlar pratik kullanıma elverişli, veri saklama ve taşımayı kolaylaştırdığı için genellikle çok kullanılan ve önemli olan veriler bu aygıtlarda depolanmaktadır. Yani adli bilişim konusu olan ve aranılan bilgi genellikle bu aygıt üzerinde kolaylıkla bulunabilmektedir.

Günümüzde harici diskler ftp sunucu, ağ üzerinden dosya paylaşımı, kablosuz erişim gibi birçok özellikleri üzerlerinde barındırabilmektedir.

Şekil 4.4 Harici Disk örnekleri

4.3.4. USB Bellek

Flash bellek ve parmak disk gibi farklı isimlerle de kullanılan, USB arabirimi üzerinden bilgisayara bağlanan, küçük ve hafif veri depolama aygıtlarındandır[48].

---

[47] Mukasey, M. B., Sedgwick, J. L., & Hagy, D. W. (2008, Nisan). *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition.* National Institute of Justice: http://www.ncjrs.gov/pdffiles1/nij/219941.pdf s.3

[48] Henkoğlu, T. (2011). *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi.* İSTANBUL: PUSULA. s. 228

Taşınması ve gizlenmesi çok kolaydır. Kol saati, İsviçre çakısı, anahtarlık vb. gibi aygıtların içerisine gizlenmiş bir şekilde bulunabilir[49]. Kalem içerisinde gömülmüş usb bellekler kalem olarak kullanılma fonksiyonuna tam olarak sahip olduğu için etrafta usb giriş kısmı açık halde veya bilgisayara takılı halde unutulmadığı sürece fark edilmeyebilir[50]. Farklı görünüme sahip usb belleklerden birkaçı aşağıda gösterilmiştir.

Şekil 4.5 Taşınabilir Bellek örnekleri[51]

Usb bellekler üzerine işletim sistemleri de yüklenebilmektedir. Bir bilgisayarda sabit disk takılı olsun veya olmasın fark etmeksizin usb bellek üzerinden bilgisayar başlatılarak usb bellek üzerindeki işletim sistemi kullanılabilmektedir.

---

[49] Mukasey, M. B., Sedgwick, J. L., & Hagy, D. W. (2008, Nisan). *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition.* National Institute of Justice: http://www.ncjrs.gov/pdffiles1/nij/219941.pdf s.5

[50] Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., & Wright, C. (2007). *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators.* Burlington, A.B.D: Syngress Publishing. s.109

[51] http://www.everythingusb.com/

4.3.5. Hafıza kartı

Şekil 4.6 Hafıza Kartı Örnekleri[52]

Hafıza kartları, bilgisayarlar, dijital kameralar, dijital fotoğraf makineleri, cep telefonları, cep bilgisayarları (PDA/PALM), dijital not defterleri, müzik/video oynatıcılar, oyun konsolları vb. aygıtlarda kullanılan[53], gün geçtikçe kapasiteleri büyürken hacimleri küçülen veri depolama aygıtlarıdır. Hafıza kartları küçük bir dönüştürücü aparatla birlikte USB arayüzünden kullanabilmektedirler. Dolayısıyla USB bellekler gibi kullanılabilmektedirler.

---

[52] http://4.bp.blogspot.com/-DhtWMVeWLeY/TlcxfPUFPmI/AAAAAAAAHX0/P8n4E_1pVQA/s1600/memory-card-128m-8g-.jpg

[53] Mukasey, M. B., Sedgwick, J. L., & Hagy, D. W. (2008, Nisan). *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition.* National Institute of Justice: http://www.ncjrs.gov/pdffiles1/nij/219941.pdf s.6

4.3.6. CD-DVD

CD İngilizce "Compact Disk", DVD ise; "Digital Versatile Disc" kelimelerinin baş harfleri alınarak yapılan kısaltmadır. CD ve DVD'ler optik medya olarak anılırlar çünkü CD ve DVD sürücüleri okuma veya yazma işlemi sırasında lazer ışını kullanırlar[54]. Optik olarak okuma ve yazma işlemi yapılabilen bu aygıtlardan günümüzde Blue-ray olarak adlandırılan modellerin 100GB kapasiteli olanları mevcuttur. Usb belleklerde olduğu gibi CD ve DVD'ler üzerinden de işletim sistemi çalıştırılabilmektedir. Cd ve DVD'ler benzer olarak çalışırlar ancak DVD'ler veri parçalarını daha küçük alanlarda tutabildiği ve hata denetleme metodu için kullanılan alanları daha küçük olduğu için daha çok veri depolayabilirler[55]. Yedekleme amaçlı kullanılan bu ortamlar delil olarak kullanılabilecek veya olayın çözümüne etki edebilecek doküman/veri içerebilirler[56].

Şekil 4.7 CD-DVD örnekleri

4.3.7. Kamera ve Fotoğraf Makinesi

Eski model video kamera ve fotoğraf makineleri şeritler üzerine kayıt yaparken günümüzde üretilen modeller üzerine takılan flash belleklere, sabit

---

[54] Shinder, D. L. (2002). *Scene of the Cybercrime: Computer Forensics Handbook.* United States of America: Syngress Publishing. s.162

[55] A.g.e. s.162

[56] Öztürkci, H. (2009). Adli Bilişim'e Giriş ve Microsoft Sistemlerinde Adli Bilişim Temelleri. İstanbul. s.46

disklere, üzerlerine takılan hafıza kartlarına veya DVD'lere kayıt yapabilmektedir. Ayrıca bunlardan birkaçına birden kayıt yapabilme özelliğine sahip modeller mevcuttur. Bazı kamera ve fotoğraf makinelerinin dahili hafızaları da mevcuttur. Dolayısıyla hafıza kartının delil olarak alındığı bir modelin dahili hafızasının da olabileceği unutulmamalıdır.

Şekil 4.8 Kamera ve Fotoğraf makinesi örnekleri

4.3.8. Yazıcı, Fotokopi ve Faks Makinesi

Yazıcılar, fotokopi ve faks makineleri; üzerlerinde hafızaları olan, internete bağlanabilen, üzerinde yapılan işlemleri hafızasında saklayan bir yapıya sahip olanları günümüzde kullanılmaktadır.

Şekil 4.9 Yazıcı, Fotokopi ve Faks makinesi örnekleri

4.3.9. Cep Telefonu

Cep telefonları küçük fiziksel boyutlarına rağmen, önemli bilgileri hafızalarında tutarlar[57]. Cep telefonları artık bilgisayarların özelliklerini

[57] Sommer, P. (2012). *Digital Evidence, Digital Investigation and E-Disclosure: A Guide to Forensic Readiness.* United Kingdom: IAAC. s.57

taşıyabilmekte ve insan hayatında vazgeçilmez bir yer almış durumdadır. Dolayısıyla adli bilişim incelemesi için gözden kaçırılmaması gereken bir bilişim aygıtıdır.

Şekil 4.10 Cep telefonu örnekleri

4.3.10. Oyun Konsolu

Oyun konsolları 1970'li yıllarda piyasaya çıkmıştır ve günümüzde çok gelişmiş özelliklere sahip bir yapıdadırlar. Bu cihazlar internet sitelerini ziyaret etmek, video, müzik, fotoğraf gibi dosyaları oynatmak ve barındırmak gibi özelliklere sahiptirler ve içlerinde çıkarılabilir hafıza birimleri mevcut olabilmektedir. Ayrıca internet üzerinden sesli ve görüntülü görüşme, içerik indirme, Facebook ve Twitter gibi sosyal ağları kullanabilme gibi özellikleri de mevcuttur[58]. Oyun konsolları göz ardı edilmemelidirler[59].

Şekil 4.11 Oyun konsolları

[58] Bolt, S. (2011). *XBOX 360 Forensics.* Burlington: Elsevier Inc. s.26

[59] Jones, N., George, E., Mérida, F. I., Rasmussen, U., & Völzow, V. (2013). *Electronic evidence guide.* Strasbourg, France: Council of Europe. s.27

5. Adli Bilişim Aşamaları

E-delillerin yapısı, mahkemede kabule şayan bir delil olarak kabul edilebilmeleri için özel bir mücadeleyi gerektirmektedir[60]. Bu mücadele belirli aşamalardan oluşmaktadır. Bu aşamalar bazı kaynaklarda 3'e[61] bazı kaynaklarda 5'e[62] ve hatta 6'ya[63] ayrılmış olsa da aslında yapılan işlerde bir farklılık yoktur. Bu farklılığın sadece gruplandırma ve isimlendirmede olduğu görülmektedir. Bu yazımızda adli bilişimi 4 aşamada ele alacağız. Bunlar:

- Tanımlama/Hazırlık,
- E-Delillerin toplanması,

---

[60] Keser Berber, L. (2004). *Adli Bilişim (Computer Forensic).* Ankara.s.45 p.1

[61] Leyla Keser Berber, *Adli Bilişim (Computer Forensic)* isimli kitabında adli bilişim aşamalarını:
1-Toplama,
2-İnceleme,
3-Analiz etme,
4-Belge Hazırlama,
5-Raporlama; olarak 5 gruba ayırmıştır.

[62] Türkay Henkoğlu, *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi*isimli kitabında adli bilişim aşamalarını:
1-Delillerin tespit edilmesi, toplanması ve muhafazası,
2-Delilleri açığa çıkartma, inceleme ve analizinin yapılması,
3-Delillerin raporlanması; olarak 3 gruba ayırmıştır.

[63] Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., & Wright, C. (2007). *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators* isimli kitabında adli bilişim aşamalarını:
1-Hazırlık,
2-Tespit etme,
3-Muhafaza,
4-Mücadele,
5-Kurtarma,
6-İzlem; olarak 6 gruba ayırmıştır.

- E-Delillerin incelenmesi,
- E-Delillerin raporlandırılması aşamalarıdır.

5.1. **Tanımlama/Hazırlık**

Bir Adli Bilişim süreci başlatılacağında ilk olarak bu iş için bir yol haritası/eylem planı belirlemek gerekir.

- **Verilerin kapsamını ve miktarını belirlemek**

Adli Bilişim Uzmanının ilk planlaması gereken, olay konusu ile ilgili olarak tespit etmesi gerektiğini düşündüğü ve ihtiyacı olacağını düşündüğü verilerin kapsamını belirlemektir.

- **E-delillerin neler olabileceğini belirlemek**

Adli Bilişim Uzmanı olayı aydınlatmak için ihtiyacı olacağını düşündüğü verileri nerelerden elde edebileceğini, olay yerindeki karşılaşabileceği e-delillerin neler olabileceğini, nelerle karşılaşabileceğini belirlemeli veya tahmin etmelidir ki olay yerinde kullanılması muhtemel adli bilişim aygıtlarını yanında bulundurabilsin. Olay yerinde karşısına çıkabilecek olan kişisel bilgisayarlar ile sunucu bilgisayarlara veya akıllı telefonlara aynı adli bilişim aygıtlarıyla müdahale edilemeyeceği gibi; bir kişisel bilgisayarın adli kopyasının alınabilmesi için yanına alınması gereken boş veri depolama birimi miktarı ile bir sunucu bilgisayarın adli kopyasının alınabilmesi için yanına alınması gereken boş veri depolama birimi miktarının aynı olmayacağı aşikardır. Dolayısıyla uygun ve gerekli miktarda boş veri depolama birimi temin edilmelidir.

- **Strateji belirlemek**

Olay ile ilgili yapılacak işlemler için daha sonra sorunlarla karşılaşmayacak şekilde bir strateji belirlenmesi gerekir. Hangi e-delile

nasıl müdahale edileceği, veri bütünlüğünün nasıl korunacağı, dışarıdan müdahalelerin nasıl engelleneceği gibi konularda olay yerinde ve kısa sürede uygulanabilir nitelikte stratejiler belirlemek gerekmektedir.

- **Delil teslim zinciri oluşturmak**

Olay yerinden alınan e-deliller veya bu e-delillerin adli kopyalarının korunması gerekmektedir. Korunma iki yönde olmalıdır.

Birincisi; delillerin fiziksel olarak korunmasından ibarettir. E-deliller çevresel faktörlerden etkilenerek arızalanabilmekte ve böylelikle delil niteliklerini kaybedebilmektedirler. Örneğin içerisinde bir olayla ilgili adli kopyaların bulunduğu bir sabit disk manyetik etkilerin altında olan bir ortamdan geçirilirse sabit disk içerisindeki manyetik veri depolama birimi olan plakaların(platter)[64] üzerinde yazılı olan verilen mıknatıslama etkisiyle mevcut halini koruyamayarak değişecek ve bu şekilde e-delil içerisindeki adli kopyaların da doğru çalışabilirliği kalmayacağından henüz incelenmeyen e-delil kaybedilmiş olacaktır. Dolayısıyla e-delillerin bütünlüğünü kaybetmeyecekleri şekilde bir ortam sağlayacak delil poşetleri/zarfları/odaları hazırlanmalıdır.

İkincisi; e-delillerin, tıpkı diğer tüm delillerde olduğu gibi, el değiştirmelerinin kayıt altına alınmasından ibarettir. Bu kayıtlar sıralı bir şekilde olmalı ve tarih saat gibi bilgileri de içermelidir. Bu şekilde delillerin üzerinde oynama yapılmasının önüne geçilmiş olunur ve herhangi bir sorun olduğunda bu sorunun hangi aşamada olduğunun tespiti yapılabilir hale gelir.

---

[64] Günümüzde halen en yaygın ve en çok kullanılan disk çeşidi içerisinde manyetik olarak bilgilerin yazılıp silinebildiği ve depolandığı bir veya birden çok ***platter***'a sahiptir. Yukarıda plaka olarak bahsedilen platter dairesel yapıda üzerinde özel alaşım bulunan verilerin depolandığı parçaya verilen isimdir.

- **Şeffaflık ve görünebilirlik**

  Tüm bu hazırlıklardan sonra yapılacak olan işlemlerin şüphe uyandırmayacak netlikte ve şeffaflıkta yapılabilmesi için tüm tedbirleri almak gerekir. Olay ile ilgili yapılacak işlemlerden sonra e-delilin değişmeyeceğinin garantisinin olduğu, işlemlerin yazmaya karşı korumalı şekilde yapıldığı anlatılmalı ve böylece işe başlanmalıdır.

5.1.1. Hukuki Dayanak

Teknolojik gelişmeler ve teknolojik gelişmemelere paralel olarak internetin kısa bir sürede olağanüstü gelişerek çok geniş bir kullanım alanına yayılmasına rağmen, ciddi bir yönetim ve denetim altına alınmaması, onun belli bir ölçüde de olsa kontrol altına alınması yönünde bazı düşüncelerin ortaya çıkmasına sebep olmuştur[65]. Elbette kontrol altına almak isteyenlerin bu amaçla kullanmayı düşündükleri en etkin araç ulusal ve uluslar arası ölçekteki hukuki düzenlemelerdir[66]. Bilişim suçlarında delil toplamada başarının birinci alanını (yasal) kurallar ve bu kurallarda gözetilmesi gereken dayanaklar oluşturur[67]. Genellikle adli bilişim personeli denilince, bilişim konusunda teknik bilgiye sahip olan personel akla gelmektedir. Ancak e-delil toplama işlerini yürüten ve teknik bilgiyle donatılmış bir adli bilişim personeli suça müdahale ederken, e-delilleri toplarken teknik bilgilerinin yanı sıra bir de hukuki bilgiye sahip olması gerekmektedir. Aksi takdirde elde edilen e-delillerin bir kısmı veya tamamı, uygunsuz veya usulüne uygun olmayan müdahalelere tabi kaldığında, soruşturma veya kovuşturma aşamasında delil olarak değerlendirilmeyebilecektir. Hukukumuzda e-delillerle ilgili olarak; e-delillerin toplanması ile ilgili yapılacak

---

[65] SIRABAŞI, V. (2003). *İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz (İNTERNET REJİMİ).* Ankara: Adalet Yayınevi. s. 120

[66] Sınar, H. (2001). *İnternet ve Ceza Hukuku.* İstanbul: Beta Basım. s. 45

[67] Karagülmez, D. D. (2009). *Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri.* Ankara: Seçkin Yayıncılık.s. 280.

olan uygulamalar ile ilgili olan "BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA, KOPYALAMA VE ELKOYMA" başlıklı 5271 sayılı CMK'nın 134. maddesi ve Adli ve Önleme Aramaları Yönetmeliği[68]'nin 17. maddesinde diğer delillerden ayrıca düzenlemeler mevcuttur. CMK 134. maddesi şöyledir:

- CMK 134. Madde:

BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA, KOPYALAMA VE ELKOYMA

Madde 134 - (1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır.

---

[68] Adli ve Önleme Aramaları Yönetmeliği yazının devamında AÖAY olarak anılacaktır.

Kısacası;

- CMK madde 134-1'de: Bilgisayarlarda Arama, Kopya Çıkarma, Çözümleme
- CMK madde 134-2'de: Elkoyma
- CMK madde 134-3'te: Yedekleme
- CMK madde 134-4'te: Kopya verme ile ilgili düzenlemeler mevcuttur.

AÖAY 17. maddesi şöyledir:

- AÖAY 17. madde:

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma

Madde 17 - 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 hâkim 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 elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması hâlinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

Bilgisayar veya bilgisayar kütüklerine elkoyma 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 elkoymaksızın 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.

Adli ve Önleme Aramaları Yönetmeliği'nin 17. Maddesindeki içeriğe bakıldığında CMK 134. Maddesi ile paralellik taşıdığı görülmekle birlikte kanunda yazılı olmayan "bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları" ibaresi ile kanun maddesi yönetmelikle genişletilmiştir[69]. Ülkemizde mevcut durumda e-delillerin toplanması ile ilgili tüm uygulamalar bu kanun maddesi ve yönetmelik maddesine göre yapılmaktadır. Yapılmakta olan uygulamalar bu iki madde dayanak alınarak yapılsa da, kanun maddelerinin içeriklerinin dünya standartlarında olan ülkemizdeki uygulamanın gerisinde kaldığı, yeterince belirleyici ve kapsayıcı içeriğe sahip olmadığı ve eksikliklere sahip olduğu söylenilebilir. Bunlardan bir tanesi, maddenin sadece soruşturma evresinden bahsediyor olması ve kovuşturma evresinde bulunan şüpheli bilgisayarın ne olacağı konusunda açıklık bulunmayışıdır. Bir diğeri ise mağdura, müştekiye, tanığa, sanığa, katılana veya şüphelinin kullanımında olmayan diğer kişilere ait olan ve e-delil olabilecek aygıtlar üzerinde yapılacak işlemler için kanun ve yönetmelik maddesinde belirleyici bir metin bulunmamasıdır.

Kanun ve yönetmelikte "başka surette delil elde imkanının bulunmaması halinde" ifadesinin kullanılması ise, birçok suçun doğrudan suç aleti olan veya

---

[69] Keser Berber, L. (2008, Temmuz 09). *BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA KOPLAMAMA EL KOYMA.* Ankara Barosu: http://www.ankarabarosu.org.tr/PANELLER/2008/09.07.2008%20B%C4%B0LG%C4%B0SAYAR%20PROGRAMLARINDA%20VE%20K%C3%9CT%C3%9CKLER%C4%B0NDE%20ARAMA%20KOPLAMAMA%20EL%20KOYMA_PANEL.doc

suçun işlenmesi esnasında vasıta olarak kullanılan elektronik aygıtlardan elde edilecek delillerin ikinci plana atılması olarak algılanmakta ve buna anlam verilememektedir[70]. Bu durumda suç ve suçluların tespiti ve suç konusu olayların aydınlatılmasının büyük derecede zorlaştığı söylenebilir.

Bu kısıtlamanın gerekliliği de göz ardı edilmemelidir. Çünkü bir şahsi bilgisayar incelendiğinde, o bilgisayarın kullanıcısına ait özel verilere ulaşılması kuvvetle muhtemeldir. Dolayısıyla şahsi bilgisayarlar, özel hayatın önemli bir unsuru niteliğindedir[71]. Kullanıcısına ait özel fotoğrafların, videoların, notların, e-posta'ların ve anlık ileti kayıtları gibi birçok özel verinin depolandığı bir bilgisayarı incelemek, o bilgisayarın sahibinin; 1982 Anayasası'nın "Özel Hayatın Gizliliği" başlıklı 20. Maddesi[72] ile korunan hakkına dokunulduğu anlamına

---

[70] Henkoğlu, T. (2011). *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi.* İSTANBUL: PUSULA.s. 17

[71] YAVUZCAN, A. E. (2010, Nisan 08). *Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma (cmk 134).* http://www.hukuki.net: http://93.187.202.7/entry.php?4-Bilgisayarlarda-bilgisayar-programlarinda-ve-kutuklerinde-arama-kopyalama-ve-elkoyma-(cmk-134)

[72] **ÖZEL HAYATIN GİZLİLİĞİ**

Madde 20 - Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. (Mülga cümle: 03/10/2001 - 4709 S.K./5. md.)

(Mülga fıkra: 03/10/2001 - 4709 S.K./5. md.) Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakimin onayına sunulur. Hakim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.

(Ek fıkra: 07/05/2010-5982 S.K./2. md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler,

gelebilmektedir. Aynı madde içerisinde bu haklara hangi hallerde dokunulabileceğinin de sınırları çizilmiştir. Dolayısıyla e-delillerle ilgili yapılacak olan işlemlerle ilgili olarak mevcut olan "başka surette delil elde etme imkânının bulunmaması hâlinde" ifadesinin gerekliliğini de anlıyoruz. Ancak bunun yanında doğrudan bilişim sistemleri üzerinde veya bilişim sistemleri aracı kılınarak işlenen suçlarda başka surette delil elde edilemeyeceği de açıktır.

Ayrıca 5237 sayılı Türk Ceza Kanunu'nun[73] "Bilişim Alanında Suçlar" başlıklı Onuncu Bölümü'nde:

- Madde 243.: Bilişim sistemine girme[74],
- Madde 244.: Sistemi engelleme, bozma, verileri yok etme veya değiştirme[75],

---

ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.

[73] Türk Ceza Kanunu yazının devamında TCK olarak anılacaktır.

[74] *Bilişim sistemine girme*

Madde 243- (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

[75] *Sistemi engelleme, bozma, verileri yok etme veya değiştirme*

Madde 244- (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.

- Madde 245.: Banka veya kredi kartlarının kötüye kullanılması [76];

ve yine TCK'da bilişim ile ilgili suçlar:

- Madde 142.: Nitelikli hırsızlık[77],
- Madde 158.: Nitelikli dolandırıcılık[78],

---

[76] *Banka veya kredi kartlarının kötüye kullanılması*

Madde 245 – (Değişik: 29/6/2005 – 5377/27 md.)

(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

(2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile cezalandırılır.

(3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

(4) Birinci fıkrada yer alan suçun;

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,

c) Aynı konutta beraber yaşayan kardeşlerden birinin,

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

(5) **(Ek: 6/12/2006 – 5560/11 md.)** Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır.

[77] Nitelikli hırsızlık

MADDE 142. - [1] Hırsızlık suçunun;

[2] Suçun;

e) Bilişim sistemlerinin kullanılması suretiyle,

İşlenmesi hâlinde, üç yıldan yedi yıla kadar hapis cezasına hükmolunur. Suçun, bu fıkranın (b) bendinde belirtilen surette, beden veya ruh bakımından kendisini savunamayacak durumda olan kimseye karşı işlenmesi halinde, verilecek ceza üçte biri oranına kadar artırılır.

[78] Nitelikli dolandırıcılık

MADDE 158. - [1] Dolandırıcılık suçunun;

- Madde 135.: Kişisel verilerin kaydedilmesi,
- Madde 136.: Verileri hukuka aykırı olarak verme veya ele geçirme,
- Madde 138.: Verileri yok etmeme,
- Madde 124.: Haberleşmenin engellenmesi,
- Madde 132.: Haberleşmenin gizliliğini ihlal[79],
- Madde 226.: Müstehcenlik,
- Madde 228.: Kumar oynanması için yer ve imkan sağlama başlıkları altında, bilişim sistemleri kullanılarak veya bilişim sistemleri hedef alınarak işlenen suçlarla ilgili bazı cezai yaptırımlar belirlenmiştir.

Ayrıca 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nda, 5070 sayılı Elektronik İmza Kanunu'nda, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele edilmesi Hakkında Kanun'da ve 10 Kasım 2010 tarihinde imzalanan Sanal Suçlar Sözleşmesi yine bilişim ile ilgili olan kanun maddelerindendir.

5.2. E-Delillerin Toplanması

Delil olarak bilişim aygıtlarında bulunmakta olan belgelerle/bilgilerle, klasik deliller farklıdır. Klasik deliller genel olarak gözle görülebilen, mühürlenerek muhafaza altına alınabilen ve değerlendirilebilen bir halde bulunurken e-deliller ise bu şekilde somut gözlem ve değerlendirmelere uygun bir yapıya sahip değillerdir. Örneğin olay yerinde bulunan bir mektup, bulunduğu haliyle taraflara paraflatılıp delil zarfına konulur, mühürlenir ve daha sonra delil

---

f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle,

İşlenmesi hâlinde, iki yıldan yedi yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur. Ancak, (e), (f) ve (j) bentlerinde sayılan hâllerde hapis cezasının alt sınırı üç yıldan, adlî para cezasının miktarı suçtan elde edilen menfaatin iki katından az olamaz.

[79] Dülger, M. V. (2004). *Bilişim Suçları.* Ankara: Seçkin. s.287

niteliği kazanmış olan bu mektup inceleneceği zaman mühürlü olan delil zarfı usulüne uygun olarak açılır ve mektup içeriği yetkililerce okunarak konu ile ilgili değerlendirilebilir. Çünkü mektupta yazılı olan kelimeler/cümleler zaten okunup değerlendirilebilecek bir haldedir. Ancak yine aynı olay yerinde bulunan bir taşınabilir bellek mektup ile aynı şekilde mühürlenip yine aynı şekilde değerlendirilmesi yapılması düşünülemez. Öncelikle taşınabilir belleğin içerisindeki bilgiler gözle görülür halde bulunmadığı gibi taşınabilir belleğin içerisinde silinmiş dosyalar da olabilecektir. Dolayısıyla e-deliller diğer delillerle birebir aynı yaklaşıma tabi tutulmamalıdır.

5.2.1. Olay Yerinde İlk Müdahale

Hukuki olarak olması gereken prosedürlerin eksiksiz olarak yerine getirilmesinden sonra, olay yerine gidildiğinde e-delillere yapılacak ilk müdahalede de uyulması gereken bir takım kurallar mevcuttur. Bu kurallara uyulması olay yerinden elde edilecek olan e-delillerin hukuka uygun olması ve delil niteliğini kaybetmeden kanun önünde değerlendirilebilmesi açısından önemlidir. Olay yerindeki işlemlerin teknik olarak uygulanması, tüm dünyada standart olarak uygulanan ve sadece küçük farklılıkların görüldüğü bir işlem sırasına göre yapılmaktadır[80].

5.2.1.1. Kavramlar

Adli kopya: Adli bilişimde İngilizce kullanımı "forensic image" olan işlem, Türkçe kaynaklarda "bire-bir" kopyalama, yabancı kaynaklarda ise "sector-

[80] Henkoğlu, T. (2011). *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi.* İSTANBUL: PUSULA.s. 18

by-sector" veya "bit-by-bit" kopyalama işlemi olarak ifade edilmektedir[81]. Veri depolama aygıtlarının bit düzeyinde kopyasının oluşturulması işlemidir[82]. Yapılan bu birebir kopyalama işlemine imaj(forensic image) denilmektedir. Kopyalama işlemi sektör-sektör veya bit-bit denilen şekilde hiçbir veri değişmeden, eksilmeden ve artmadan her veri aynı olacak şekilde, dosya halinde bir başka diske yapılmaktadır. İşletim sistemlerinde günlük hayatta yapılan normal kopyalama işleminde kullanıcılar tarafından görülen dosya veya klasörler bir başka bilişim aygıtına aktarılırken bu işlemde bazı bilgilerin(oluşturma tarihi gibi) değişebilmesinin yanı sıra yapılan işlemde sadece görülmekte olan bilgiler kopyalanır. Hatta bazı yeni dosya yapılarında daha detaylı bilgiler tutulabilmekte iken, burada bulunan dosya veya klasör eski dosya yapısıyla formatlanmış bir veri depolama birimine kopyalandığında bazı üstveriler de kopyalanamamaktadır.

Yazma Koruma: bir veri depolama birimi üzerinde yazma işlemi ve değişiklik yapılmasını engelleyen araçtır[83]. Yazma koruma sistemleri veri depolama biriminde değişiklik yapılmasını engellemekte ancak veri depolama birimine erişime izin vermektedir[84].

Hash: Hash tek yönlü bir algoritmik fonksiyondur. Tek yönlü olma özelliği sayesinde hash değerinden geriye dönülerek hash değeri hesaplanan veri parçasına ulaşılamamasını sağlamaktadır. Hash kullanım alanlarından biri de orijinal data ile o datanın adli kopyasının birbirleri ile aynı olup olmadığını karşılaştırmaktır. Hash'ler eşleştiği zaman, bu verilerin tam bir kopyasının

---

[81] A.g.e. s. 48

[82] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s.3

[83] Albert J. Marcella, J. D. (2008). *Cyber Forensic.* New York: Auerbach Publications. s.480

[84] James Lyle, S. M. (2007). *ADVANCES IN DIGITAL FORENSICS III.* Orlando, Florida: Sprringer. s.163

olduğunun kanıtı olarak kabul edilmektedir[85]. Bir verinin veya veri depolama biriminin tamamının ilk sektörden başlanıp, sırayla belirli bir algoritmik fonksiyondan geçirilerek çıkan değer ve bir sonraki sektör tekrar bir algoritmik fonksiyondan geçirilmesi işlemi son sektöre kadar devam eder. Son sektörün de aynı işleme tabi tutulmasıyla ortaya çıkan değere hash değeri denilmektedir. Bu hash değeri verinin değişikliğe uğrayıp uğramadığını kontrolde kullanılmaktadır. Hash değeri, hash'i hesaplanan veriye özel ve parmak izi gibi benzersiz bir değerdir. Hash değeri üzerinden tersine mühendislik yapılarak veriye ulaşılamaz[86]. Veri depolama birimi üzerindeki bir karakterin bile değişmesi durumunda hash değişmektedir. Standart hash algoritmaları:

- **MD2, MD4** ve **MD5:** bu metotların hash değeri(**M**essage **D**igest) 128 bit uzunluğundadır, yani temel olarak hesaplanan değer rakamlardan ve sayılardan oluşan toplam 32 karakterdir[87]. Bu metotlar Ron Rivest tarafından oluşturulmuştur ve çoğunlukla dijital imzalar için kullanılmaktadır.
- **Secure Hash Algorithm (SHA):** bu algoritmanın SHA-1, SHA-256, SHA-384 ve SHA-512 olarak birçok çeşidi bulunmaktadır. Bu çeşitlerin aralarındaki fark hash değerinin bit uzunluklarıdır. SHA hash algoritmaları A.B.D'de varlık gösteren NIST ve NSA isimli iki birim tarafından hazırlanmıştır.[88]

---

[85] Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., & Wright, C. (2007). *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators.* Burlington, A.B.D: Syngress Publishing. s.10

[86] Shinder, D. L. (2002). *Scene of the Cybercrime: Computer Forensics Handbook.* United States of America: Syngress Publishing. s.379

[87] Casey, E. (2000). *Digital Evidence and Computer Crime.* LONDON: Academic Press. s. 59

[88] Shinder, D. L. (2002). *Scene of the Cybercrime: Computer Forensics Handbook.* United States of America: Syngress Publishing. s.380

MD5 ve SHA1 hash değerlerine birer örnek aşağıdadır.

MD5: b8e20611dcc4105286bcf56de754f7a3

SHA1: 9f34ac74f28e6ee9f0ad76d7b39d615722822b4f

Wipe: kelime anlamı olarak silmek ve tamamen ortadan kaldırmak demektir.

Üstveri: Türkçe'de üstveri olarak kullanılan dünyada ingilizce karşılığı olan "metadata" kavramının en basit tanımı "veri hakkında veri" olarak yapılmaktadır. Metadata bir kaynağın öğelerini tanımlayan veridir. Bu nedenle bibliyografik veri olabildiği gibi içerik, kullanım koşulları, kapsam ve teknik ya da erişim özelliklerinde ilişkin diğer tanımlamayı da içerebilir[89].

Uçucu veri: Çalışmakta olan bilgisayar sitemlerinde var olan ancak sistem kapandığında/elektrik kesildiğinde kaybolan[90], fiziksel olarak veri depolama biriminde kayıtlı kalmayan verilerdir. Bu verilere;

- Pano içeriği(clipboard)[91],
- Bağlı olunan ağ aygıtları,
- Açık olan ağ girişleri(ports)[92],
- Bağlı aygıtların listesi,
- Çalışan uygulamalar,

---

[89] DEMPSEY, L. (1998, Ocak 19). *METADATA: A UK HE PERSPECTIVE.* UKOLN: http://www.ukoln.ac.uk/services/papers/bl/blri078/content/repor~27.htm

[90] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s. 16

[91] Bilgisayarda kopyala veya kes komutları kullanıldığında bazı bilgiler ram'e alınır ve asıl veri silinse de ram'deki veri halen yapıştırılarak kullanılabilir.

[92] Yazının devamında İngilizce port kelimesinin karşılığı olarak dilimizde kullanılan "giriş" kelimesi tercihen kullanılacaktır.

- ARP cache (arp)[93],
- Ekran alıntısı(Print Screen),
- İnternet tarayıcıların otomatik tamamlama verileri[94],
- Geçici dosyalar(Temporary cache files),
- Yüklü programlar,
- Ram içeriği,
- Dosya paylaşım programlarına ait anlık paylaşım bilgileri vb. veriler örnek gösterilebilir.

Unallocated alan: sabit disk üzerinde yer alan ve temel hafıza da dahil olmak üzere işletim sistemi tarafından tahsis edilmemiş olan; metadata ve data depolanması için uygun olan alandır[95].

Çerezler(Cookies): internet kullanıcısı, sonradan kullanıcının bilgisayarında yerleşik hale gelen çerez dosyasına bilgi yazan bir siteyi ziyaret eder ve daha sonraki bir zamanda yine bu siteyi ziyaret ederse kullanıcının bilgisayarı içinde yerleşik olan çerez dosyası içinde kayıtlı olan bilgiyi kullanarak siteye ilişkin bilgileri okumaktadır[96].

HPA ve DCO: İngilizce sırasıyla **"**Host Protected Area" ve "Device Configuration Overlay" kelimelerinin kısaltılmışıdır. Her iki metot da sabit disk üzerindeki verinin bir kısmını işletim sisteminden gizlemektir. Bilgisayar üreticilerinin işletim sistemi için kurtarma dosyalarını tuttukları kısımdır. İşletim

---

[93] Craiger, J. (2005). *Computer Forensics Procedures and Methods.* Florida. s. 52

[94] *AccessData.* (2013, 03 21). Live Response: http://marketing.accessdata.com/acton/attachment/4390/f-0088/0/-/-/-/-/file.pdf

[95] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s.4

[96] Özdilek, A. O. (2002). *İnternet ve HUKUK.* İstanbul: Papatya Yayıncılık. s.194

sistemi ve kullanıcı tarafından bu kısımlara doğrudan erişilememektedir. HPA ve DCO ile ilgili kısımlardaki verilere yazılım kullanılarak erişilebilir.

5.2.1.2. Potansiyel e-deliller nelerdir?

Eskiden, bilgisayarın ilk zamanlarında, dijital aygıtlardan elde edilebilecek geçerli deliller; bilgisayarlar, sabit diskler, teyp kaset şeklindeki yedekleme üniteleri ve disketler olarak düşünülmekteydi. Uçucu veri olabilecek donanımların hafıza kapasiteleri oldukça düşük ve sınırlıydı, ayrıca buradan da potansiyel delil çıkartabilecek sistemler yoktu. Günümüz modern dijital aygıtlarında ise delil elde edilebilecek dijital aygıtların çeşitliliği ve sayısı çok geniş ve büyük bir artış göstermiş durumda[97].

E-delil olabilecek bilişim aygıtlardan bazıları şunlardır:

- Sabit Disk(Harici veya Dahili)
- Disket
- CD/DVD
- Flash Bellek
- Hafıza kartı
- Dongle[98]
- Modem
- Router
- Cep telefonu
- Kaset
- Jaz/Zip Kartuşlar[99]

---

[97] Jones, D. A., & Vazlli, D. C. (2008). *Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility.* Waltham(United States): Syngress. s.11

[98] Bilgisayarın bağlantı noktalarından birine takılarak(genellikle usb bağlantı noktasına takılır) kopya yazılım korumasını sağlayan donanım.

- Video Kamera
- Fotoğraf Makinesi
- MP3/MP4 oynatıcı
- Network aygıtları
- Bluetooth aygıtları
- Kızılötesi aygıtları
- WiFi aygıtları
- FM Transmitter[100]
- Televizyon
- Oyun konsolu[101]
- Uydu alıcısı
- Güç kaynağı ünitesi
- PCMCI kart[102]
- GPS aygıtı
- Yazıcı, tarayıcı, fotokopi ve faks makinesi
- Telesekreter
- Databank
- Saat
- E-kitap okuyucu
- Kalem
- Anahtarlık
- Süs eşyaları
- Dijital çerçeve
- Ses kayıt cihazı

---

[99] Kullanımda "Zip kartuşlar" yerine "Zip disketler" de denilmektedir.

[100] FM frekansında radyo dalgaları yayan verici.

[101] Microsoft Xbox, Sony Play Station, Nintendo Wii gibi oyun konsollarının içerisinde 320GB'a kadar kapasiteli sabit diskler bulunabilmekte ayrıca bu sabit disklerin kapasiteleri daha yüksek kapasiteli sabit disklerle değiştirilebilmektedir.

[102] Keser Berber, L. (2004). *Adli Bilişim (Computer Forensic).* Ankara.s.46

Bu listenin amacı, olay yerinde karşılaşılabilecek olan bilişim aygıtlarının hangilerinin e-delil olabileceği hakkında daha kapsamlı düşünülmesini sağlamaktır[103]. Bu liste sadece örnek olabilecek ve sıklıkla karşılaşılabilinen e-delillerden oluşturulmuştur ancak tüm e-deliller bunlardan ibaret olmadığı gibi burada yazılı olup ta ileride kullanım dışı kalacak olanlar da olabilir. Disket kullanım dışı kalacak olanlara örnek gösterilebilir. Önceleri veri taşımada yazılıp silinebilir özellikte olması sebebiyle tekrar tekrar kullanılmaya olanak sağladığından ve çok da pahalı olmamasından dolayı sıkça kullanılan disketlerin yerini günümüzde depolama alanları daha fazla, taşıması daha kolay, veri depolama ömrü daha uzun ve yazma-okuma hızları daha yüksek olan flash bellekler ve harici diskler almış durumdadır.

Teknoloji geliştikçe e-delil olarak değerlendirilebilecek yeni aygıtlar ortaya çıkmaya devam edecektir.

5.2.1.3. Olay Yerinde İlk Müdahalede Genel Kurallar

Olay yerinde yapılacak müdahale için uyulması gereken genel kurallar aşağıda maddeler halinde verilmiştir.

- Olay yeri muhafaza altına alınmalıdır,
- Klasik delillerde de olduğu gibi e-delillerin de karartılmaması için önlem tedbir alınmalı, yazılımsal ve fiziksel olarak zarar görmesi engellenmelidir,

---

[103] Jones, D. A., & Vazlli, D. C. (2008). *Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility.* Waltham(United States): Syngress. s.12

- Olay yerinde görevli olmayan ve olay ile ilgisi olmayan herkes olay yeri dışına çıkartılmalı[104], sadece ilgili kişiler olay yerinde bulunmalı ve yeteri kadarından fazlası olay yerinden çıkartılmalıdır(örneğin olay yeri bir iş yeri ise ve iş yerinde birden fazla bilgi işlem görevlisi çalışıyorsa, sadece bir bilgi işlem görevlisinin sistem hakkında bilgi verecek kadar yeterli bilgisi varsa sadece bir bilgi işlem görevlisi olay yerinde kalmalıdır. Ancak bazı durumlarda bunun tersi bir işlemin yapılması gerekebilir. Diğer bilgi işlem görevlisi olay yerinden ayrıldığında uzaktan sisteme bağlanarak verilere müdahale etmesi gibi bir ihtimal mevcutsa, bu duruma göre gerekli tedbirler alınmalı ve bu duruma göre karar vermek gerekir.)
- Hukuki olarak alınan kararda uygulamayı kısıtlayıcı, uygulamaya yön verici bir içerik mevcut mudur? Karar kontrol edilmeli,
- Olay ile ilgili olarak ne tür e-delillerin olay yerinde aranacağı ve toplanacağı, hangi e-delillerin konu ile ilgili olabileceği hakkında karar verilmelidir. Olay ile ilgili olmayan bilişim aygıtları ayrılmalıdır.
- Olay yeri sistematik olarak aranmalı ve e-delillerin tamamı tespit edilmelidir, küçük boyutlu veya biblo şeklindeki farklı görünümde veri depolama birimleri gözden kaçırılmamalıdır,
- Tespit edilen delillerin toplanması için uygun öncelik sırası belirlenmelidir,
- Olay yerinde herhangi bir müdahale olmadan fotoğraflanmalı veya video kaydı alınmalıdır,

---

[104] Evidence, S. W. (2013, Şubat 11). *SWGDE Best Practices for Computer Forensics.* Scientific Working Group on Digital Evidence: https://www.swgde.org/documents/Released%20For%20Public%20Comment/2013-02-11%20SWGDE%20Best%20Practices%20for%20Computer%20Forensics%20V3-0

- E-deliller üzerinde parmak izi, dna tespiti vb. işlemler yapılması gerekecek ise bu işlemin yapılması için öncelik sırası belirlenmeli ve mümkünse e-delillere dokunmadan önce bu işlemlerin bir an önce yapılması sağlanmalıdır[105],
- Olay yerinde bulunan ve e-delil olarak değerlendirilmesi muhtemel tüm aygıtlar delil etiketleri ile etiketlendirilmelidirler. Etiketlerin üzerinde yeterli açıklayıcı bilgi bulunmalıdır. Bilgisayar kasalarının arka bölümündeki kablo bağlantılarının, mümkünse bağlantı noktasını da (bağlı olduğu port) gösterir şekilde etiketlenmesinde fayda vardır[106]. Aşağıdaki şekilde örnek etiketleme yapılmış bilgisayar kasası görülmektedir.

Şekil 5.1 Örnek etiketleme yapılmış bilgisayar kasası[107]

[105] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s. 18

[106] Henkoğlu, T. (2011). *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi.* İSTANBUL: PUSULA.s. 19

[107] U.S. Department of Homeland Security. (2006). *Best Practices For Seizing Electronic Evidence.* A.B.D.: United States Secret Service. s.4

- Yerinden sökülemeyen, çalışması durdurulamayan (sökülmemesi veya çalışmasının devam etmesi önemli ve gerekli olan) e-delillerin, mümkünse olduğu haliyle çalışırken adli kopyası alınmalıdır,
- E-delil olmayan ancak olay yerinde bulunan ve e-delillerle ilgili olabilecek diğer bilgiler(kullanıcı adları, şifreler, kodlar, ağ bağlantı bilgileri vb. gibi) olabileceği unutulmamalı ve bu bilgiler de toplanmaya çalışılmalıdır. Bazen kullanıcılar bilgisayarlarında bilgi saklamak için kırılması veya bulunması mümkün olmaması için uzun ve karmaşık karakterlerden anlamsız bir şekilde oluşturdukları güçlü şifreler kullanabilmektedirler. Bir de farklı platformlarda, farklı internet sitelerinde farklı şifreler kullanılmakta ve genellikle de kullanılan şifrelerin belirli aralıklarla değiştirilmesi gerekmektedir. Farklı internet sitelerinde aynı kullanıcı adını kullanmanın da pek mümkün olmadığını düşünürsek bu karmaşık şifrelerin bir de farklı kullanıcı isimleriyle eşleştirilmesi gerekecektir. Dolayısıyla karmaşık ve uzun karakterlerden oluşan ve aynı zamanda anlamsız olan bu şifreleri akılda tutmak insan doğası gereği zordur ve bu şifreler ve kullanıcı adları genellikle bir yerlere yazılarak muhafaza edilmektedir. Bu tarz bilgilere olay yerinde her zaman bir kağıt üzerine yazılmış halde ulaşılacağı beklenmemelidir. Kullanıcılar çalışma ortamlarında gözünün önündeki herhangi bir yazıyı, model numarasını, seri numarasını, tarihi, vb. bilgileri de şifre olarak kullanabilmektedirler. Dolayısıyla bu tarz bilgiler de değerlendirilmelidir. Yukarıda yazılan fotoğraf alma işlemi de bu konuda ihtiyacı giderebilecek şekilde olay yerindeki sonradan ihtiyaç duyulabileceği düşünülen olası her şeyin görünebileceği/okunabileceği şekilde detaylıca yapılmalıdır.

- Olay yerinde ilk müdahale sırasında e-delil olabilecek bilişim aygıtlarında anti-forensic[108] sistemleri olabileceği unutulmamalıdır. E-delile yapılacak olan normal bir müdahalede devreye girebilecek şekilde tasarlanmış anti-forensic düzeneği kurulu olan bilgisayar kasası içerisindeki e-delil beklenmedik bir şekilde bir degausser'ın[109] çalışmasıyla manyetik olarak geri getirilemeyecek şekilde manyetik etkiye tabi kalarak bozulabilir.

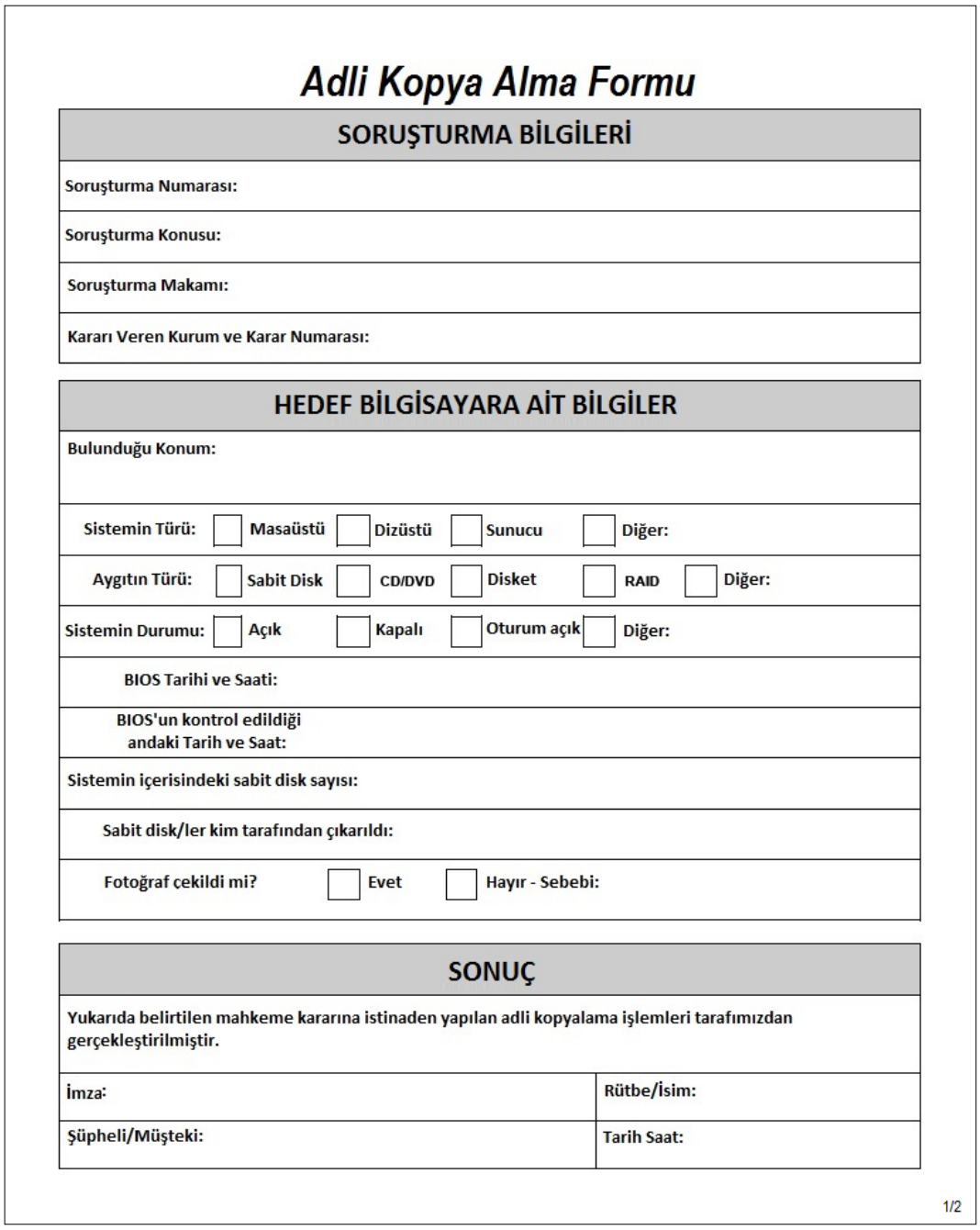
Olay yerinde farklı birçok senaryo ile karşılaşılabilir. Her farklı senaryo farklı müdahaleleri gerektirebilir. Olay yerinde ilk müdahale sırasında nasıl bir senaryoyla karşılaşılabileceği önceden az çok tahmin edilebilse de detayları kestirebilmek zordur. Dolayısıyla olay yerinde ilk anda nasıl müdahale edileceğine ise kısa bir sürede doğru karar vermek çok önemli bir gereksinimdir. İlk müdahale sırasında uyulması ve uygulanması gereken genel kurallar bazı özel durumlarda farklı uygulamaları da gerektirebileceği unutulmamalıdır. Dolayısıyla genel kurallar özel durumlar için de uygulanmak zorunda olan olmazsa olmaz kurallar değildir.

İlk müdahalede olay yerinde kullanmak için formlar hazırlanmalıdır. Örnek olarak "Adli Kopya Alma Formu" aşağıdadır.

---

[108] Anti-forensic: adli bilişim çalışması yapıldığında herhangi bir suç unsuru bulunamaması için bilişim aygıtlarının içerisindeki bilgileri geri getirilemeyecek şekilde yok eden, bilişim aygıtlarına fiziksel olarak çalışamayacak derecede hasar veren donanımlar, programlar ve yöntemler.

[109] Degausser: çok güçlü bir manyetik alan oluşturarak etki alanında bulunan manyetik ortamlar üzerindeki verileri tamamen değiştirerek bozan ve kullanılamaz hale getiren bir donanımdır. Manyetik veri depolama sistemiyle çalışan sabit disklerde verilen geri normal bir silme işlemi sabit diskin kapasitesine doğru orantılı olarak çok uzun süre gerektirmektedir. Ancak degausser kullanılarak bir anda sabit diskin veri yazılı manyetik yüzeylerinin tamamı üzerinde veriler bozularak ulaşılamaz hale getirilebilir.



Adli Kopya Alma Formu

SORUŞTURMA BİLGİLERİ
Soruşturma Numarası:
Soruşturma Konusu:
Soruşturma Makamı:
Kararı Veren Kurum ve Karar Numarası:

HEDEF BİLGİSAYARA AİT BİLGİLER
Bulunduğu Konum:
Sistemin Türü: ☐ Masaüstü ☐ Dizüstü ☐ Sunucu ☐ Diğer:
Aygıtın Türü: ☐ Sabit Disk ☐ CD/DVD ☐ Disket ☐ RAID ☐ Diğer:
Sistemin Durumu: ☐ Açık ☐ Kapalı ☐ Oturum açık ☐ Diğer:
BIOS Tarihi ve Saati:
BIOS'un kontrol edildiği andaki Tarih ve Saat:
Sistemin içerisindeki sabit disk sayısı:
Sabit disk/ler kim tarafından çıkarıldı:
Fotoğraf çekildi mi? ☐ Evet ☐ Hayır - Sebebi:

SONUÇ	
Yukarıda belirtilen mahkeme kararına istinaden yapılan adli kopyalama işlemleri tarafımızdan gerçekleştirilmiştir.	
İmza:	Rütbe/İsim:
Şüpheli/Müşteki:	Tarih Saat:

1/2

Şekil 5.2 Adli Kopya Alma Formu[110]

[110] Jones, N., George, E., Mérida, F. I., Rasmussen, U., & Völzow, V. (2013). *Electronic evidence guide.* Strasbourg, France: Council of Europe. s.265

BİLGİSAYAR		SABİT DİSK/DİĞER
Marka:		
Model:		
Seri Numarası:		

ADLİ KOPYA ALMA BİLGİLERİ				
Adli Kopyayı alanın adı/soyadı:				
Adli Kopyanın alındığı yer:				
Adli kopya alma işleminde kullanılan yazılım	☐ EnCase (v.)	☐ FTK (v.)	☐ Backup (Software):	
	☐ dd Image	☐ Logical File Copy	☐ Diğer:	
Adli kopya alma işleminde kullanılan donanım	☐ Fastblock	☐ Firewire W/B	☐ Bootdisk	☐ Direct Connection
	☐ SCSI-IDE W/B	☐ XOver Cable	☐ Diğer:	
Adli kopyanın alınacağı yer:	☐ Sabit Disk:	☐ Diğer:		
Seri numarası:				
Markası:				
Kapasitesi:	GB	MB		
Adli kopyanın kapasitesi:	GB	MB		
Adli kopya doğrulama işlemi yapıldı mı?	Evet / Hayır	Hata var mı?:	Evet / Hayır	
Hash değeri:				

2/2

Şekil 5.3 Adli Kopya Alma Formu(devamı)[111]

[111] Jones, N., George, E., Mérida, F. I., Rasmussen, U., & Völzow, V. (2013). *Electronic evidence guide.* Strasbourg, France: Council of Europe. s.266

5.2.1.4. Çalışır Durumda Olmayan E-Delillere İlk Müdahale

Olay yerinde tespit edilen ve çalışır durumda olmayan e-delillere müdahale çalışır durumdaki e-delillere göre daha basit işlemlere tabidir.

Bilgisayar sistemlerinde:

- Bilgisayarın çalışır durumda olup olmadığına bakılır. Gösterge ışıkları, soğutma fanları ve ses gibi bilgisayarın açık olduğunu anlamamızı sağlayan durumlar kontrol edilir. Bunlardan herhangi biri mevcut değilse bilgisayarın çalışır durumda olmadığı düşünülebilir ancak bunun teyit edilmesi gerekmektedir. Zira bilgisayar uyku durumuna alınmış olabilir.
- Bilgisayarın ekranı kapalı ise ekranın güç düğmesi, güç kablosuna elektrik gelip gelmediği ve ekranın veri kablosunun bilgisayara takılı olup olmadığı kontrol edilerek bağlantılarda ve güçte sorun olmadığı teyit edilmelidir,
- Ekran halen kapalı ise fare hareket ettirilmeli ancak herhangi bir tuşa basılmamalı ve farenin üzerinde bulunan teker döndürülmemelidir. Bunlar yapıldıktan sonra bilgisayarda ve ekranında bilgisayarın açık olduğuna dair herhangi bir belirti görülmez ise bilgisayarın kapalı olduğu teyit edilmiş olunur.
- Kapalı olan bilgisayar açılmaz,
- Bilgisayarın bağlantı kabloları, bilgisayara bağlı veri depolama aygıtları ve diğer cihazlar etiketlenir. Etiketleme işlemi hangi girişten hangi bilişim aygıtının takılı olduğunu, aygıtlar söküldüğünde belli edecek şekilde hem bilişim aygıtına hem de bilişim aygıtının bağlı olduğu girişe karşılıklı olarak yapılır. Bu işlem pratik olması açısından her iki tarafa da aynı numara ile numaralandırılmış etiketler yapıştırılmak suretiyle olabilir.
- Etiketleme işlemleri yapıldıktan sonra fotoğraf veya video kaydı yapılabilir,

- Güç kablosu sökülür. Dizüstü bilgisayarlarda batarya çıkartılır. Bazı bilgisayarlarda disket sürücüsü, CD/DVD sürücüsü vb. aygıtların takılması için ayrılmış yuvalara batarya takılabildiği de unutulmamalıdır. Varsa bunlarında bağlantısı kesilmelidir.
- Bilgisayara bağlı olan veri depolama üniteleri sökülür. Bazı bilgisayarlarda disket sürücüsü, CD/DVD sürücüsü vb. aygıtların takılması için ayrılmış yuvalara sabit disk gibi veri depolama aygıtlarının takılabildiği de unutulmamalıdır.
- Disket sürücüsünün ve CD/DVD sürücüsünün içi kontrol edilmelidir. Disket veya CD/DVD varsa çıkartılıp nereden hangi e-delilin çıkartıldığı not alınmalıdır.
- Hangi bilgisayarın hangi girişinden hangi bilişim aygıtlarının çıktığına dair bilgiler marka, model ve seri numarası gibi ayırt edici bilgileriyle birlikte not alınır[112],
- Uygun cihaz veya yazılımlarla, veri depolama ünitelerinin adli kopya alma işlemi hash değeri hesaplamasıyla birlikte yapılır,
- Güç kablosu veya batarya tekrar takılarak bilgisayarın açma tuşuna basılır ve BIOS'a girilir. Bilgisayarın ilk açılışı sırasında ESC, DEL, F2, F9, F10 veya F11 tuşlarına basılarak BIOS'a girilebilir[113]. BIOS tarih/saat bilgisi işlemin yapıldığı andaki tarih/saat bilgisiyle birlikte not alınır. BIOS'ta görülen tarih-saat bilgisi o anki tarih/saat bilgisinden farklı olabilir. Bu fark zaman diliminin farklı olmasından olabileceği gibi gerçekte bilgisayar kullanıcısı tarih/saat bilgisi doğru olmayan bir sistemi kullanıyor

---

[112] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s.28

[113] Philipp, A., Cowen, D., & Davis, C. (2009). *Hacking Exposed Computer Forensics Second Edition.* ABD: mhprofessional.s.66

da olabilir. Bu bilgi kasıtlı olarak ta yanlış ayarlanmış olabilir. BIOS üzerinde görülen tarih saat bilgisinin o anki tarih saat bilgisinden farklı olması normal olmayan bir durum olduğu anlamına da gelmemektedir. Bunu konuyu inceleyen adli bilişim uzmanı değerlendirecektir.

- Olay yerinde adli kopya alınacaksa çıkartılan bilişim aygıtlarının kopya alma işlemlerine başlanabilir, adli kopya alma işlemi laboratuar ortamında yapılacaksa kopyası alınmak üzere çıkartılan bilişim aygıtları zarar görmeyecek özel delil torbalarına konularak taşınmalı ve delil torbaların üzerine e-delile ait marka model seri numarası bilgileri yazılmalıdır.

5.2.1.5. Çalışır Durumda Olan E-Delillere İlk Müdahale

Olay yerinde tespit edilen ve çalışır durumda olan e-delillere müdahale detaylı işlemlerin yapılmasını gerektirebilir.

Bilgisayar sistemlerinde:

- Bilgisayarın çalışır durumda olup olmadığına bakılır. Gösterge ışıkları, soğutma fanları ve ses gibi bilgisayarın açık olduğunu anlamamızı sağlayan durumlar kontrol edilir. Bunlardan herhangi biri mevcutsa bilgisayarın çalışır durumda olduğu düşünülebilir.
- Eğer olayın konusu uçucu verilerin toplanmasını gerektirmiyor ise çalışan bir bilgisayarın güç kablosunu çıkartmak genellikle en güvenli seçenektir. Günümüzde bilgisayarların çoğu güç tuşuna basıldığında uyku durumuna geçecek şekilde ayarlanmış durumdadır. Ayrıca bir bilgisayarda güç tuşuna basıldığında, kapanmadan önce sistemdeki verileri değiştirebilen ve/veya silebilen bir komut başlatılacak şekilde ayarlanmış olabilir veya bağlı sistemleri beklenmeyen bir durumun olduğu konusunda uyararak delil değeri olan verileri bulunmadan önce silebilecekleri

alarmı verecek şekilde düzenlenmiş bir yapı devreye girebilecek şekilde ayarlanmış olabilir[114]. Bu durumda bilgisayarın güç kablosu çıkartılır ve kapalı olan bilgisayarlarda uygulanması gereken yöntemler uygulanır.

- Bilgisayarın ekranı açık değilse açılır, ekrana görüntü gelirse ekran; çalışan programları, resimler, internet siteleri, e-posta kayıtları vb. ekrandaki diğer görünenleri anlaşılır ve görülebilir şekilde, fotoğraf veya video ile kayıt altına alınır[115]. Şifre sorma ihtimali olan ekran koruyucu gibi programların devreye girmemesi için gerekli ayarlamalar yapılmalıdır.
- Ekran açık ve ekran koruyucu çalışıyor ise; ekran koruyucuyu devreden çıkartmak için fare hareket ettirilmeli ancak herhangi bir tuşa basılmamalı ve farenin üzerinde bulunan teker döndürülmemelidir. Şifre ekranı gelirse şifre temin edilmeye çalışılır ve temin edilen şifre ile giriş yapılır. Bunlar yapıldıktan sonra ekranda görülen değişimler gözlemlenir ve ekran fotoğraf veya video ile kayıt altına alınır.
- Ekran açık ancak ekranda görüntü yok ise; bilgisayar uyku durumuna girmiş veya ekran tasarruf modundan dolayı kapanmış halde olabilir; her iki modan da çıkartmak için fare hareket ettirilmeli ancak herhangi bir tuşa basılmamalı ve farenin üzerinde bulunan teker döndürülmemelidir. Şifre ekranı gelirse şifre temin edilmeye çalışılır ve temin edilen şifre ile giriş yapılır. Bunlar yapıldıktan sonra ekranda görülen değişimler gözlemlenir ve ekran fotoğraf veya video ile kayıt altına alınır.

---

[114] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s. 28

[115] Johnson, T. A. (2005). *Forensic Computer Crime Investigation.* New York: Taylor & Francis Group. s.12

- Bilgisayarın tarih/saat bilgisi işlemin yapıldığı andaki tarih/saat bilgisiyle birlikte not alınır.
- Olay konusuna göre ihtiyaç var ise öncelikle uçucu veriler toplanmalıdır.
- Açık olan bilgisayarlarda ekranda görülenler çok önemlidir. Çalışan programlar, bağlı aygıtlar, yapılan işlemler, henüz kaydedilmemiş yazılar, anlık ileti kayıtları, notlar, çalışmalar, kodlar, şifreler vb. bilgiler bilgisayar kapandığında elde edilemeyeceği için iyi değerlendirilmeli, her detay not alınmalıdır.
- Eğer varsa ağ bağlantısı kesilmelidir[116].
- Disket sürücüsünün ve CD/DVD sürücüsünün içi kontrol edilmelidir. Disket veya CD/DVD varsa çıkartılıp nereden hangi e-delilin çıkartıldığı not alınmalıdır.
- Açık olan bilgisayarlarda "truecrypt, bitlocker vb." gibi şifreleme yazılımları mevcut ise bilgisayarın ram'inin[117] adli kopyası alınmalı ve sonra bilgisayar açık iken mantıksal olarak adli kopya alınmalıdır. "truecrypt, bitlocker" tarzında şifreleme yöntemi kullanılan bilgisayarlarda fiziksel olarak alınacak adli kopyalar şifreli olacağından imaj üzerinde inceleme yapılabilmesi için şifrenin bilinmesi/bulunması gerekecektir.

5.2.1.6. Güvenlik Kamerası Kayıt Sistemlerine İlk Müdahale

Günümüzde neredeyse her iş yerinde güvenlik kamera kayıt cihazları bulunmaktadır. Olayların aydınlatılmasında güvenlik kamera kayıtlarından alınan görüntüler büyük bir önem taşımaktadırlar. Güvenlik kamerası kayıt sistemleri üzerinden doğrudan olayın aydınlatılmasına yarayan görüntüler elde edilmektedir.

---

[116] Keser Berber, L. (2004). *Adli Bilişim (Computer Forensic).* Ankara.s.52

[117] İşlemci tarafından okunup yazılabilen, üzerinde bilgilerin geçici olarak tutulduğu bellek.

Günümüzde kullanılmakta olan güvenlik kamera kayıt cihazlarının standart bir yapıda olmaması, bu cihazlardan görüntü elde etmeyi zorlaştırabilmektedir.

Güvenlik kamera kayıt sistemlerinden görüntü almak şu yollarla mümkün olabilmektedir:

- Video dosyalarının CD/DVD/Blu-ray diskler yazarak kopyalarının alınması, ancak video dosyasının boyutu büyük ise bu yöntem pratik olmayabilmektedir,
- Video dosyalarını harici bir depolama birimine yazarak kopyalarının alınması,
- Video dosyalarının, varsa ağ bağlantısı üzerinden bağlanarak, kopyalarının alınması,
- Güvenlik kamerası kayıt sisteminin kendisine ait olan program üzerinden, varsa sıkıştırma ve dönüştürme işlemleri yaparak, video dosyalarının alınması işlemi yapılabilir. Ancak bu en son tercih edilmesi gereken seçenektir, çünkü sıkıştırma ve dönüştürme işlemleri orijinal video dosyasının kalitesini düşürebilmekte ve detayını azaltabilmektedir.
- Güvenlik kamerası kayıt cihazındaki video dosyalarının doğrudan alınması mümkün olmadığı durumlarda, uygun bir analog kayıt cihazı kullanılarak, kayıt cihazı üzerindeki analog çıkışı üzerinden ilgili videonun kaydının yapılmasına çalışılmalıdır.
- Herhangi bir şekilde güvenlik kamera kayıt cihazından görüntü almanın mümkün olmadığı durumlarda güvenlik kamera kayıt cihazına bütün olarak olay yerinden alınarak görüntü almak için laboratuar ortamına çalışılabilir[118].

---

[118] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s. 33

Güvenlik kamera kayıt sistemlerinden görüntü alınırken:

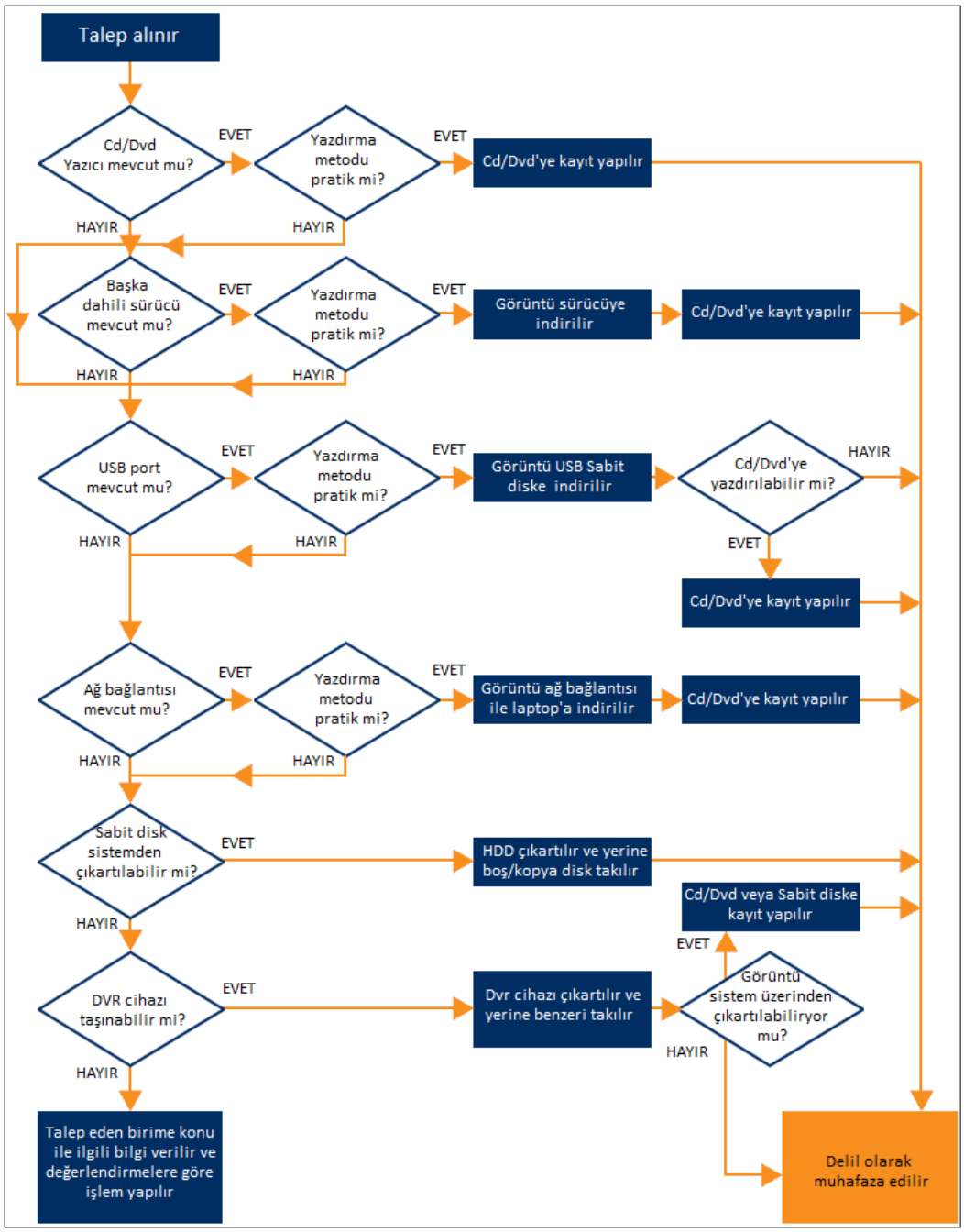
- Güvenlik kamerası kayıt cihazının/sisteminin marka model bilgileri, sisteme bağlı kamera sayıları gibi sistemin yapısına ait bilgiler not alınmalı ve mümkünse fotoğraflanmalıdır,
- Bir değişiklik olması ihtimaline karşın, tekrar eski ayarlara dönülebilmesi için, sistem ayarları not alınmalıdır[119],
- Sistemin tarih saat bilgisi kontrol edilmeli ve tarih saat bilgilerinde yanlışlık varsa bu yanlışlık ayrıntılı bir şekilde not alınmalıdır[120],
- Sistemin ne kadar süre ile eski kayıtların üzerine yazdığı öğrenilmeli veya tespit edilmelidir,
- Mümkünse sadece konu ile ilgili olan kamera görüntüleri alınmalıdır,
- Mümkünse geçmişe dönük kamera görüntüsü alınırken sistemin mevcut anı kaydetmesine devam edilmelidir,
- Alınan güvenlik kamera görüntülerinin diğer işletim sistemlerinde de oynatılabilir olduğundan emin olunmalıdır,
- Güvenlik kamera kayıt sistemine özgü oynatıcı program yardımcı program araçları varsa temin edilmelidir.

Güvenlik kamera kayıt sistemlerinden görüntülerin alınmasıyla ilgili karar ağacı aşağıdadır.

---

[119] Chris Simpson, A. P. (2012, Eylül 09). *Good Practice Guide for Computer-Based Electronic Evidence.* 7Safe Information Security, eDiscovery, Penetration Testing, Training, PCI DSS, Computer Forensics: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf, s.39

[120] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s. 33



Şekil 5.4 Kamera kayıt sistemlerinden görüntülerin alınmasıyla ilgili karar ağacı[121]

[121] Chris Simpson, A. P. (2012, Eylül 09). *Good Practice Guide for Computer-Based Electronic Evidence.* 7Safe Information Security, eDiscovery, Penetration Testing, Training, PCI DSS, Computer Forensics: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf, s.41

5.2.1.7. Cep telefonu ve Taşınabilir Aygıtlara İlk Müdahale

Akıllı/Cep telefonları, tablet bilgisayarlar gibi taşınabilir aygıtlar; bu cihazlarda kullanılan işlemciler, dokunmatik ekranlar, kameralar, vb. donanımların ve bu donanımlar üzerinde yüklenen işletim sistemlerinin de gelişmesiyle son derece kullanışlı hale gelmişlerdir. Bu gelişimin en büyük sebeplerinden birisi de artık günümüzde taşınabilir aygıtlar üzerinden internete ulaşmanın çok kolay olmasıdır. İnsanlar artık bilgisayarlar yerine taşınabilir aygıtları kullanarak işlerini halledebilmektedir. Bu kadar sık kullanılan bu aygıtlarla olayla ilgili olarak da sıkça karşılaşabilmektedir.

Kendilerine özgü yapıları olan bu aygıtlara müdahale edilirken:

- Başkalarının ulaşması ve müdahale etmesi engellenmelidir,
- Ekranında görünenler fotoğraflanmalıdır,
- Aidiyet tespitinde sıkıntı varsa ve gerekiyorsa parmak izi-DNA çalışması yapılmalıdır,
- Sim kartına ait pin kodu ve aygıta ait güvenlik kodu öğrenilmeli ve not alınmalıdır,
- Telefona özel standart dışı bağlantı kablosu, şarj cihazı gibi aygıtlar telefonla birlikte alınmalıdır,
- Aygıtı kapatmadan dış bağlantıyı kesmek gerekiyorsa Faraday çantasına konulmalıdır,

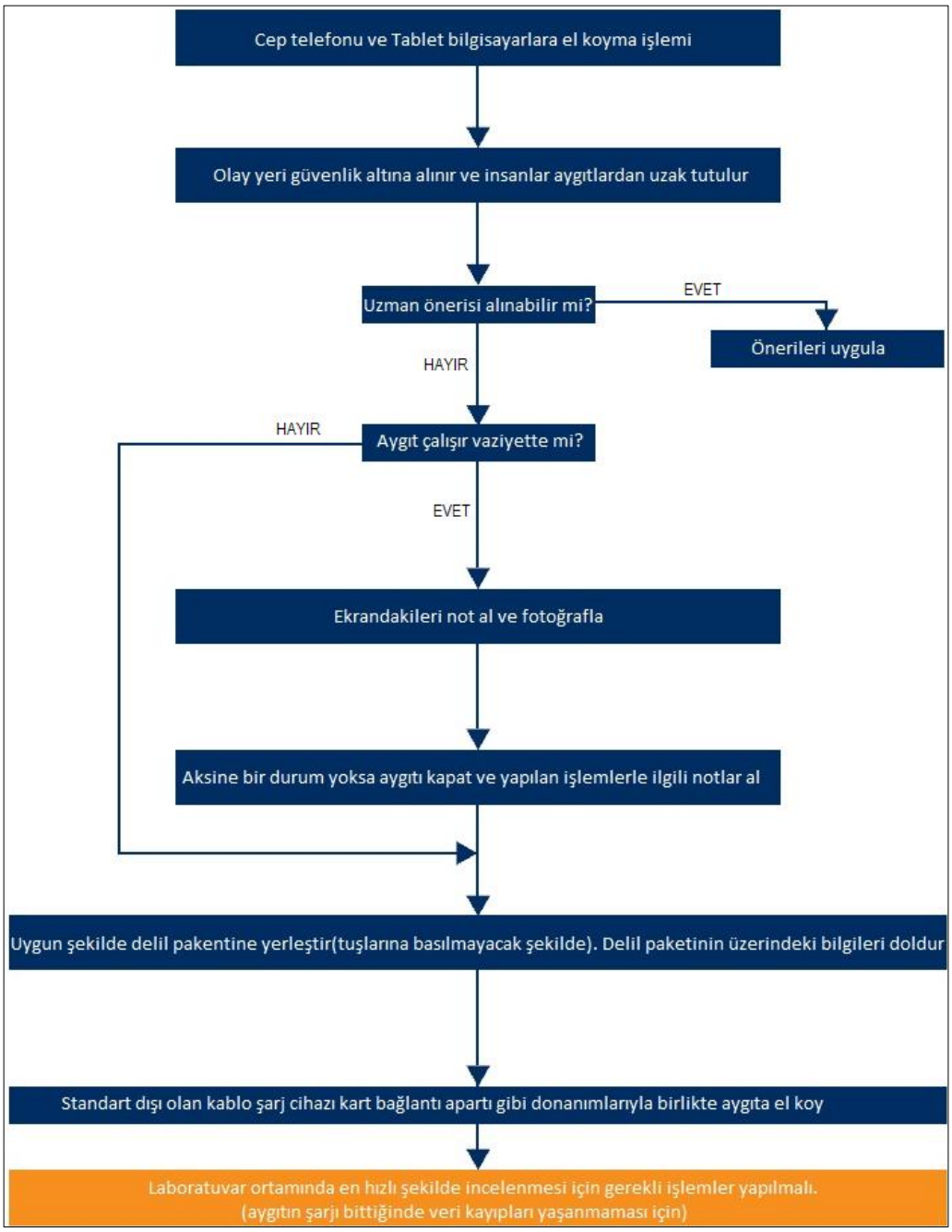
- Sim kart kullanılması gerekiyorsa orijinal sim kartın kopyası olan bir sim kart kullanmak, cihazın ağa erişimini önler. Cihazın sim kartı orijinal sim kart gibi algılamasını sağlar ve cihaz üzerinde yapılandırmada değişikliklerin olmamasını sağlayarak güvenli bir şekilde incelenmesine olanak tanır[122],
- Aygıt açıksa ve pin kodu, puk kodu, güvenlik kodu vb. kodların olduğu düşünülüyorsa, aygıt kapatılmadan önce içeriklerinin çıkartılmasına çalışılmalıdır[123].

Cep telefonları ve tablet bilgisayarlar için olay yerinde karar ağacı aşağıdadır.

---

[122] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s.32

[123] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s.



Şekil 5.5 Cep telefonu ve Tablet bilgisayarların için olay yeri karar ağacı[124]

[124] Chris Simpson, A. P. (2012, Eylül 09). *Good Practice Guide for Computer-Based Electronic Evidence.* 7Safe Information Security, eDiscovery, Penetration Testing, Training, PCI DSS, Computer Forensics: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf, s.51

5.2.1.8. E-delillerin paketlenmesi, taşınması ve muhafazası

E-deliller ve e-delillerin bulunduğu bilgisayar ve bilişim aygıtları; aşırı sıcaklık, soğukluk, nem, fiziksel şok, statik elektrik ve manyetik alanlara karşı duyarlıdırlar[125]. Bu dış etkenlerden sadece birisi, e-delili çalışamaz hale getirebilir.

- E-delil üzerinde parmak izi gibi göremediğimiz biyolojik bir kanıt olabilir. Paketleme işlemi yapılmadan bu çeşit kanıtlar için gerekli çalışma yaptırılabilir, ancak çalışma sırasında kullanılacak kimyasallar e-delile zarar verebilecekse bu çalışma sona bırakılmalıdır.
- E-deliller olay yerinden ilgili kablo, adaptör gibi ihtiyaç duyulabileceği düşünülen parçalarıyla birlikte alınmalıdır.
- Tüm e-deliller antistatik özellikli, çarpmalara karşı(hava balonlu zarf gibi) önlem alınmış, bir defa kapatıldıktan sonra açıldığında açıldığı belli olacak özellikte zarflarda taşınmalıdır.
- Bilgisayar kasaları, tüm parçalarının ekranın arkasında olduğu bilgisayarlar gibi büyük boyutlu e-deliller delil zarflarına sığmayabilirler. Bu gibi e-deliller sarsıntılardan ve manyetik alanlardan(hoparlör, telsiz vb.) uzak kalacak şekilde taşınmalıdır.
- E-delillerin ekran kısımları yumuşak bir yüzeye temas edecek şekilde taşınmalıdır.
- CD, DVD, disket ve microSD hafıza kartı gibi daha hassas yüzeye sahip e-delillerin üzerine etiket yapıştırmadan delil zarflarına

---

[125] *Collecting Digital Evidence Flowchart.* (2008, Nisan 14). National Institute of Justice: http://www.nij.gov/publications/ecrime-guide-219941/ch5-evidence-collection/collecting-digital-evidence-flowchart.htm s.31

konulmalı ve bunların taşınırken kırılması bükülmesi engellenmelidir.

- Cep telefonu, akıllı telefon, cep bilgisayarı olay konusu gerektiriyor ise faraday[126] çantasına konulmalıdır. (Faraday çantasının kullanılması bataryanın bitmesini hızlandırabilir. Eğer kaynaklar izin veriyorsa, faraday çantası içerisindeyken yardımcı bir güç ile bataryanın bitmesi önelenebilir[127].)
- Delil zarflarının üzerindeki bilgiler doldurulmalıdır. Zarflar kapatıldıktan sonra hangi zarfta ne olduğu zarfın üzerinde yazan bilgilere bakılarak anlaşılacak ve delil zinciri bu şekilde devam edecektir.
- Paketlenen delillerin en kısa sürede laboratuar ortamına konulması sağlanmalıdır.

E-deliller ile ilgili, klasik delillerde olduğu gibi, delil teslim zinciri bilgileri tutulmalıdır. Delil teslim zinciri aşağıdaki bilgileri içermelidir:

- E-delilin kimliği ve aidiyeti,
- E-delille yapılan erişimlerin tarih saat bilgileri ve erişimi gerçekleştirenin kimlik bilgisi ve erişimin sebebi,
- E-delilin delil muhafaza dolabına giriş ve çıkış tarih saat bilgileri ve giriş ve çıkışları kontrol edene ait kimlik bilgileri,

---

[126] İngiliz Fizikçi Micheal Faraday'ın buluşu olan Faraday kafesi, elektriksel iletken metal ile kaplanmış veya iletkenler ile ağ biçiminde örülmüş içteki hacmi dışarıdaki elektrik alanlardan koruyan bir muhafazadır. Faraday çantasına konulan cep telefonunun baz istasyonu ile bağlantısı cep telefonu kapatılmadan kesilmiş olur.

[127] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s.17

- E-delil üzerinde zorunlu olarak gerçekleşen değişiklikler ve bu değişikliklerin gerçekleşmesiyle ilgili kişilere ait kimlik bilgileri[128].

E-delillerin paketlenmesi, taşınması ve muhafazasında ana amaç e-delili korumak, kaybı, zarar görmeyi veya değiştirilmeyi engellemek ve denetlenebilirliği mümkün kılmaktır[129].

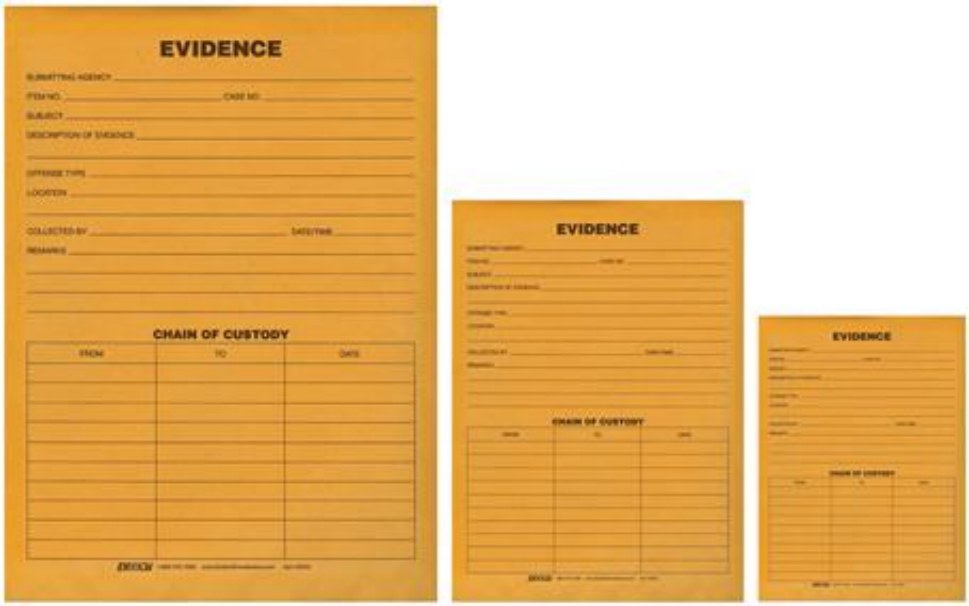
E-deliller, klasik delillerde olduğu gibi, özel ve olumsuz etkenlerden koruyucu delil zarflarında taşınmalıdırlar. Delil zarflarına ve Faraday çantasına örnek resimler aşağıdadır.

Şekil 5.6 Faraday Çantası

[128] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s. 10-11

[129] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s. 17

Şekil 5.7 Antistatik maddeden ve baloncuklu üretilmiş delil zarfları[130]



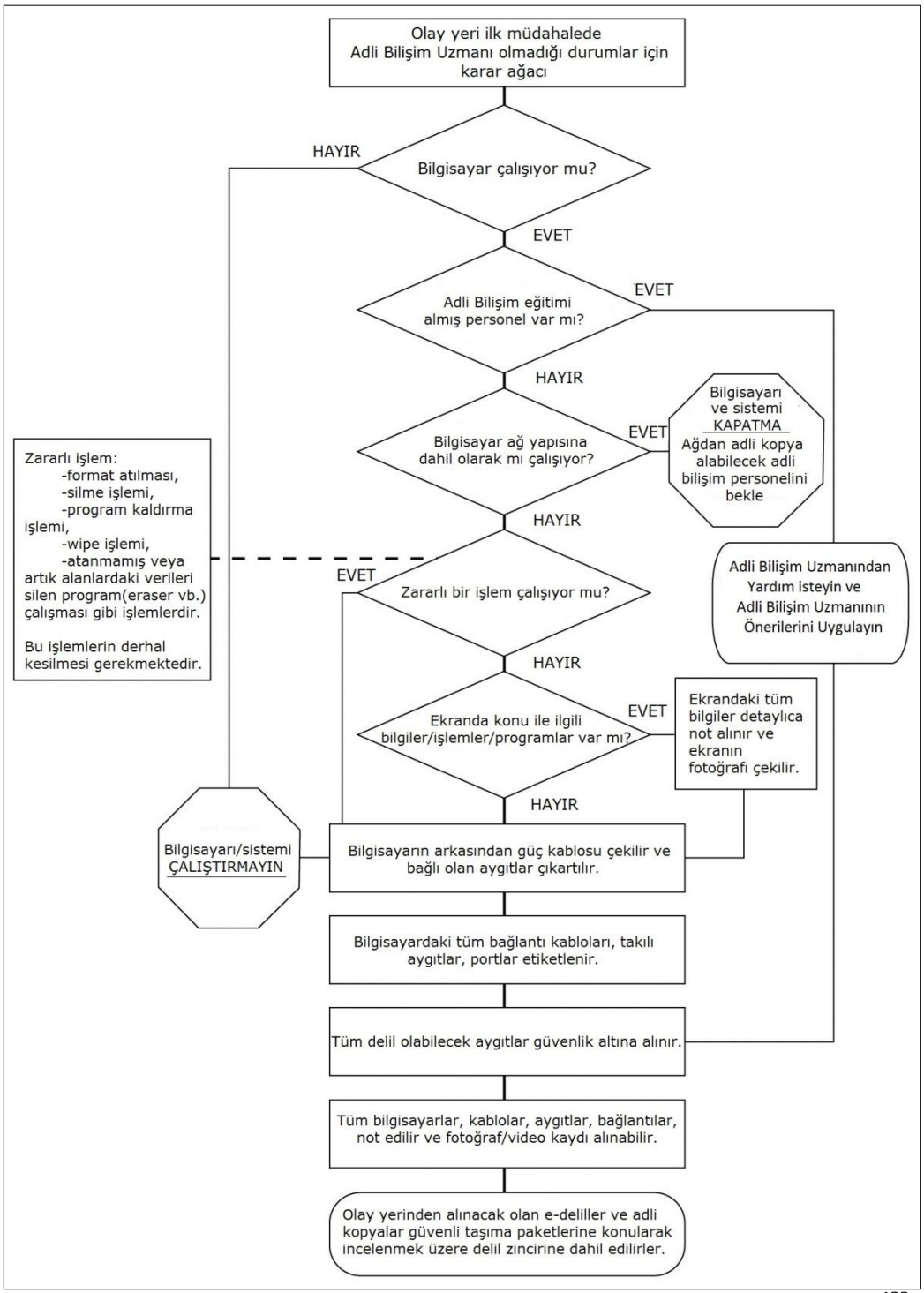
Şekil 5.8 Üzerine delille ilgili bilgilerin yazılabileceği kağıt kaplanmış antistatik ve baloncuklu delil zarfları[131]

[130] http://www.tritechforensics.com/store/product/plastic-evidence-bags-anti-static-bubble/

[131] http://www.evidentcrimescene.com/cata/evid2/evid2.html

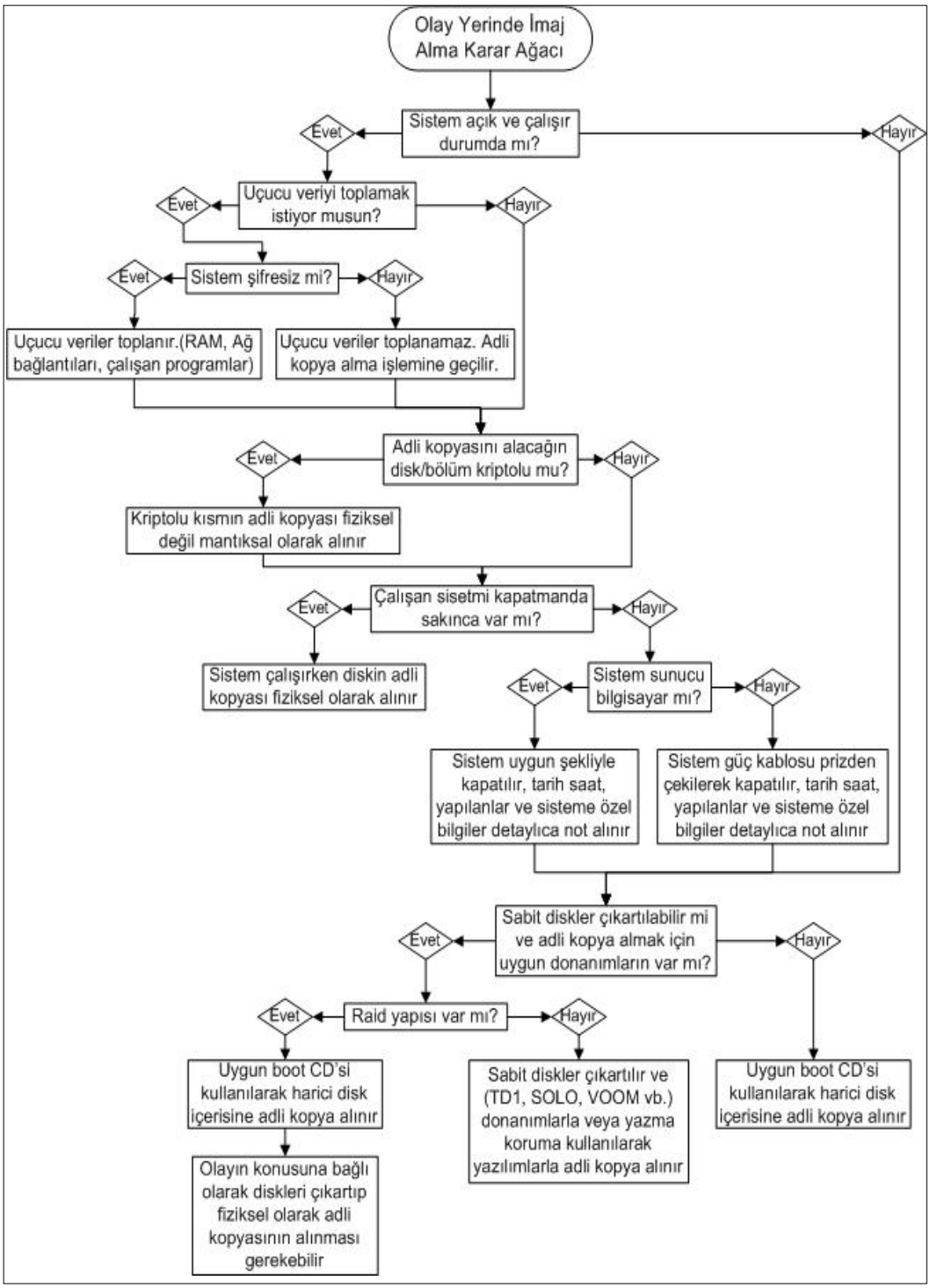
5.2.1.9. Olay Yerinde ilk Müdahalede Karar Alma

Olay yerinde doğru ve yeterli müdahale, çok fazla detaya hakim olmayı gerektirir. İnsanoğlu yeterince bilgili olsa da doğası gereği detaylar arttıkça yanılma payı da artar. Olay yerinde ilk müdahale sırasında faydalanabilmek ve daha doğru karar verilebilmesini sağlamak için şemalar hazırlanmalıdır. Bu şemalar olay yerindeki ihtimalleri ve bu ihtimallerle karşılaşıldığında yapılması gerekenleri belirtecek şekilde, önceden hazırlanmalıdır. Olay yerinde Adli Bilişim Uzmanı olmadığı durum için karar ağacı ve Olay Yerinde Adli Bilişim Uzmanı için karar ağacı aşağıda örnek olarak sunulmuştur.



Şekil 5.9 Olay yerinde Adli Bilişim Uzmanı olmadığı durum için karar ağacı[132]

[132] *Collecting Digital Evidence Flowchart.* (2008, Nisan 14). National Institute of Justice: http://www.nij.gov/publications/ecrime-guide-219941/ch5-evidence-collection/collecting-digital-evidence-flowchart.htm



Şekil 5.10 Olay Yerinde Adli Bilişim Uzmanı için Karar Ağacı[133]

[133] Mueller, L. (2013, Mart 28). *Computer Forensic Hard Drive Imaging Process Tree for Basic Training.* http://www.forensickb.com/2010/12/computer-forensic-hard-drive-

5.2.2. Adli Kopya Alma İşlemi

E-delil üzerinde inceleme yapılırken, orijinal veri üzerinde bozulma, değişiklik vb. durumlar olduğunda, inceleme yapabilecek başka bir alternatifin olmaması önemli bir sorundur[134]. Adli kopya alma işlemi, e-delilin incelenmesi sırasında orijinal e-delil üzerinde değişiklik olmasının engellenmesi için ve e-delilin kopyası üzerinden başkaları tarafından da incelenebilmesi ve inceleme sonucunda aynı sonuca ulaşabilmesi için, uygulanmaktadır[135]. Adli kopya alma süreci, e-delilerin bir kopyasının alınması ve kopya alımı sırasında kullanılan metotların ve yapılan işlemlerin kayıt altına alınması işlemlerinden oluşur[136].

Adli kopya alma işlemi farklı şekillerde yapılabilmektedir.

- Şüpheli bilgisayardan sabit disk sökülür ve başka bir bilgisayara takılarak adli kopyalama işlemi başlatılır.
- Yeterli boş alana sahip olan sabit disk şüpheli bilgisayara takılır ve adli kopyalama işlemi başlatılır.
- Şüpheli bilgisayardan sabit disk sökülür ve adli kopya çıkartmak için üretilmiş olan donanıma takılarak adli kopyalama işlemi başlatılır.

---

imaging_11.html: http://2.bp.blogspot.com/_rX7Jddr9KTM/TQD6GXIOwiI/AAAAAAAAi5Q/Z76iSlXRoJI/s1600/Image+Process+flow+chart.png

[134] Schweitzer, D. (2003). *Incident Response: Computer Forensics Toolkit.* Indianapolis: Wiley Publishing, Inc. s.59

[135] Mason, S. (2008). *International Electronic Evidence.* London: British Institute of International and Comparative Law. s. 48

[136] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s. 9

- Ağ bağlantısı ile şüpheli bilgisayara bağlantı kurularak şüpheli bilgisayarın sabit diskinin adli kopyalama işlemi başlatılır[137].

Bu metotlardan hangisi kullanılarak adli kopya çıkartılacağına eldeki adli bilişim cihazlarının durumundan, e-delillerin hangi tür aygıtlardan oluştuğuna kadar birçok değişkenin belirleyici rolü vardır.

Adli kopyanın kaydedilmesinde kullanılacak olan dijital aygıt daha önce başka bir soruşturmada veya başka bir iş için kullanılmış ise wipe işlemine tabi tutulması gerekebilmektedir[138].

Adli kopya alma işlemi sonunda adli kopyanın doğru bir şekilde kopyalandığının kontrolü için hash hesaplatılarak kontrol edilmelidir. Çalışan sistemlerden adli kopya alınması işleminde olduğu gibi, doğrulama işleminin yerine getirilemediği durumlarda yapılan işlemler sebepleriyle birlikte kayıt altına alınmalıdır[139].

Adli kopyası alınacak olan e-delil hafıza birimi kapasitesi çok büyük olduğu durumlarda sadece belirlenen dosya türlerinde veya sadece belirlenen dosya veya klasörler gibi alanlarda mantıksal adli kopya alma işlemi yapılabilir. Mantıksal adli kopya alma işleminde sadece mevcut(silinmemiş) dosya ve dosya bazlı olmayan veriler kopyalanabilmektedir[140].

---

[137] Shinder, D. L. (2002). *Scene of the Cybercrime: Computer Forensics Handbook.* United States of America: Syngress Publishing. s.560

[138] Austin, R. (2013). *FORENSIC PROCEDURES MANUAL VERSION 3.5.* Marietta: Department of Information Technology, Southern Polytechnic State University. s.12

[139] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s. 9

[140] ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.* İsviçre: International Organization for Standardization, International Electrotechnical Commission. s. 10

5.2.2.1. Yazma Koruma

Adli kopya alma işlemleri e-delil üzerinde değişiklik olma ihtimalini ortadan kaldırmak ve delil bütünlüğünü korumak için yazma korumalı olarak yapılmalıdır. Bu duruma çalışır haldeki sistemlerden adli kopya alma işlemleri dahil değildir. Çalışır durumdaki sistemlerden adli kopya alabilmek için sisteme boş veri depolama birimi takılması gerekmekte ve adli kopyanın bu birim üzerinde kaydedilmesi gerekmekte olduğu için aynı zamanda yazmayı engelleme işlemi yapılamaz.

Yazılımsal olarak yazmayı engellemek mümkündür. Yazılımsal olarak kullanılan yazma koruma sisteminin doğru çalışmadığı durumlar olabileceğinden bu konuda daha dikkatli olunmalıdır. Yazılımsal olarak yazma koruma sisteminin çalışabilmesi için bilgisayar öncelikle doğru bir şekilde başlatılabilmelidir[141]. Windows işletim sisteminde kayıt defterinde yapılacak değişiklikle USB girişinden takılan veri depolama birimlerine yazma koruma yazılımsal olarak yapılabilmektedir. Linux işletim sistemlerinde veri depolama birimini yazma korumalı olarak sistemin kullanımına dahil etmek mümkündür. Microsoft DOS tabanlı ve Linux tabanlı işletim sistemlerini çalıştırıldıklarında veri depolama birimi üzerinde değişiklik yapmayacak şekilde kendi kaynaklarını kullanarak çalışacakları halde tasarlamak mümkündür. Tasarlanan bu sistemler CD-DVD, USB bellek vb. veri depolama birimleri üzerinden çalıştırarak kullanılabilmektedir[142].

Donanımsal olarak hazırlanmış olan yazma koruma aygıtları da mevcuttur. Adli kopya alma esnasında sürekli kullanıldıklarından, yazma koruma aygıtları

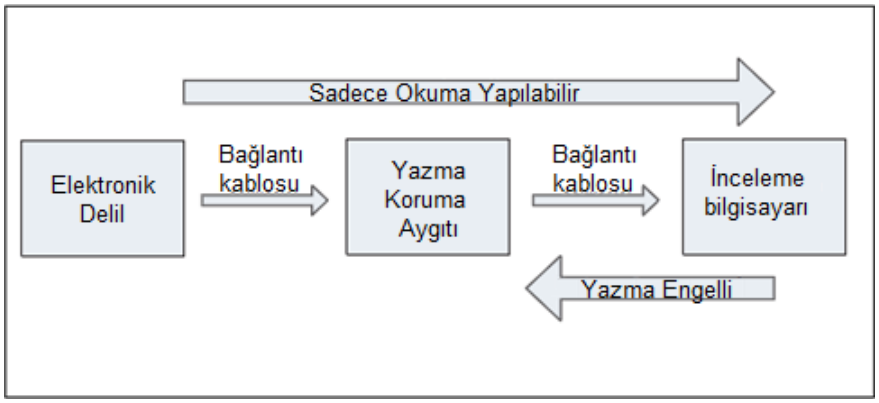
---

[141] Jain, R. K. (2006). *Cyber Forensics Tools and Practices.* Indiana: The ICFAI University Press. s.127

[142] Cardwell, K., O'Shea, K., Clinton, T., Reis, K., Cohen, T., Reyes, A., . . . Jean, B. R. (2007). *The Best Damm Cybercrime and Digital Forensics Book Period.* Burlington: Syngress Publishing, Inc. s.33

adli bilişim laboratuarlarında her masada bulunması gerekli cihazlardandır[143]. Yazma koruma aygıtları genellikle giriş çeşitlerine göre ayrı ayrı tasarlanmaktadırlar. SATA, SCSI, USB, IDE, vb her çeşit giriş için genellikle ayrı yazma koruma aygıtları mevcuttur. Hafıza kartı okuyucuları, disket okuyucuları üzerinde de yazma koruması olan aygıtlar mevcuttur.

Yazma koruma sistemini ve yazma koruma aygıtlarını gösterir resimler aşağıdadır.



Şekil 5.11 Yazma koruma aygıtlarına ait yazma koruması çalışma sitemi[144]

[143] Cardwell, K., O'Shea, K., Clinton, T., Reis, K., Cohen, T., Reyes, A., . . . Jean, B. R. (2007). *The Best Damm Cybercrime and Digital Forensics Book Period.* Burlington: Syngress Publishing, Inc. s.33

[144] Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., & Wright, C. (2007). *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators.* Burlington, A.B.D: Syngress Publishing. s.36

Şekil 5.12 Yazma koruma aygıtlarının bulunduğu takım çantası[145]

5.2.2.2. Adli Kopya Alma Yazılımları

Adli kopyanın adli bilişim standartlarına uygun olarak alınması, dijital delillerin elde edilmesi ve analizi sürecinin doğru başlaması ve sonuçlandırılması ile yakın ilişki içindedir[146]. Delilleri toplarken daima doğru araçlar kullanılmalıdır. E-delillerden adli kopya almak için çok sayıda yazılım ve donanım mevcuttur. Genel olarak kullanımı tercih edilen adli kopya alma yazılımları aşağıdadır.

5.2.2.2.1. FTK Imager

AccessData internet sitesi[147] üzerinden ücretsiz olarak edinilebilecek olan FTK Imager, yaygın olarak kullanılan Windows işletim sistemi tabanlı adli kopya

---

[145] http://www.digitalintelligence.com/products/ultrakit/images/ultrakitiii_medium.jpg

[146] Henkoğlu, T. (2011). *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi*. İSTANBUL: PUSULA.s.59

[147] http://www.accessdata.com/support/product-downloads

alma yazılımıdır[148]. FTK Imager 3.0 ve daha sonraki sürümleri AD1(AD Custom Content), E01(Encase), S01(Smart), AFF(Advenced Forensic Format), 001(RAW/DD) uzantılı adli kopya dosyalarını desteklemektedir[149]. RAM belleğin adli kopyasını alabilme özelliğine de sahiptir. FTK Imager potansiyel e-delil üzerinde verileri önizleme yaparak değerlendirmeyi sağlayacak özelliğe sahip bir yazılımdır. Bu yazılım kullanılarak adli kopya çıkartılırken veya veriler kopyalanırken orijinal veri üzerinde değişiklik meydana gelmez[150].

FTK Imager ile veya başka bir araç ile alınmış adli kopya bu yazılım kullanılarak dosyaları görülebilir[151].

5.2.2.2.2. Encase Forensic Imager

Guidance Software'ın internet sitesi[152] üzerinden ücretsiz olarak edinilebilecek olan Encase Forensic Imager yazılımı ile bilgisayarın üzerinde takılı halde olan veri depolama birimlerinden adli kopya alma, ağ bağlantı kablosu üzerinden çapraz(crossover[153]) kablo kullanılarak bağlanılan diğer bilgisayarın

---

[148] Henkoğlu, T. (2011). *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi.* İSTANBUL: PUSULA. s.49

[149] AccecssData FTK Imager 3.1.2.0 User Guide s.29

[150] Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., & Wright, C. (2007). *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators.* Burlington, A.B.D: Syngress Publishing. s.244

[151] Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., & Wright, C. (2007). *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators.* Burlington, A.B.D: Syngress Publishing. s.244

[152]http://download.guidancesoftware.com/fmD53CUKavaLhjEhqw93o1pMm5fPdnZUTP/Zn5XZGan1zbiKdff0fWvVZuYh3QZTD3ECGLjLvyI%3D

[153] CAT5 kablolarının iki ucunu da 568A yada 568B şeklinde bağlandığı kablolara straight (Düz) kablo denir. Bir ucu 568A diğer ucu 568B olan kablolara Crossover (Çapraz) kablo denir. 568B tipinde bir kabloyu 568A tipinde bir kablo'ya dönüştürmek için kablo pinlerinden 1 ile 3 ve 2 ile 6'nın yerlerini değiştirmek gerekir. Kablonun bir ucu 568A bir ucu 568B olduğu takdirde aynı olan iki cihaz arasında bir switch,hub, yada bridge

adli kopyasını alma, alınmış bir adli kopya üzerinde bütünlük kontrolü yapma, alınmış bir adli kopyayı "e01" formatına dönüştürme, bir veri depolama birimine wipe yapma gibi işlemler yapılabilmektedir. RAM belleğin adli kopyasını alabilme özelliğine de sahiptir. Encase programı olan E01 ve L01 formatlarında ve aynı zamanda bunların daha fazla sıkıştırılmış halleri olan Ex01 ve Lx01 formatlarında da adli kopya alabilmektedir. Ex01 ve Lx01 formatlarında alınmış olan adli kopyalarda yeni şifreleme ve hash seçenekleri desteklenmektedir[154]. Restore menüsü ile de adli kopya disk üzerine yazılabilir.

Encase programının Linux işletim sistemleri için "LinEN" isimli sürümü de mevcuttur. LinEN ile adli kopya alınacağında bazı noktalara dikkat etmek gerekmektedir. Linux, NTFS dosya yapısında kararlı bir şekilde çalışamadığı için adli kopyanın kaydedileceği dijital aygıtın dosya yapısını ext2/ext3 veya FAT32 türlerinden biri ile formatlamak gerekmektedir. Bir diğer husus ise autofs servisinin durdurulması gerekliliğidir. Autofs servisi, sisteme takılan aygıtları mount ederek, otomatik olarak kullanıma açacaktır ve böylelikle yazma korumasında sorun olabilecektir. Birçok Linux sürümünde autofs servisi varsayılan olarak açık halde olmasa da, bu durum kontrol edilerek emin olunmalıdır[155].

---

bulunmadan birbirleriyle iletişim kurabilirler. Bunun nedeni birinin transtmit pininin (Veri ileten pin) diğerinin recieve pinine (Veri alan pin) denk gelmiş olmasıdır.

[154]Encase Forensic Imager v7.06 User's Guide https://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CDEQFjAA&url=http%3A%2F%2Fdownload.guidancesoftware.com%2FKU%252BE%2FU1Ix%2FedkrHovP20INeCqc5ribTB2vJxVDTiToVBaytASWq5Afg5YV%2FsHF1qdzL82L9O9Y%252Bu7j32H3J6pA%253D%253D&ei=vDNpUaDhHpDcsgaO_oC4BA&usg=AFQjCNECCdJrGH_YhvTigZMGp-2d7uOMUA&bvm=bv.45175338,d.Yms

[155] Pogue, C., Altheide, C., & Haverkos, T. (2008). *UNIX and Linux Forensic Analysis DVD Toolkit.* Burlington: Syngress Publishing, Inc. s.64

5.2.2.2.3. Forensic Imager

Getdata internet sitesi[156] üzerinden ücretsiz olarak edinilebilecek olan Forensic Imager, Windows işletim sistemi tabanlı adli kopya alma yazılımıdır. E01, AFF, RAW/DD uzantılı adli kopya dosyalarını desteklemektedir[157]. Desteklediği bu adli kopya türlerini birbirine dönüştürme işlemi yapabilmektedir. MD5 ve SHA1'in yanı sıra SHA256 hash hesaplama yöntemini de desteklemektedir. Ancak Forensic Imager yazılımı HPA ve DCO ile korunan alanlara erişememektedir.

5.2.2.2.4. Tableau Imager

Tableau internet sitesi[158] üzerinden ücretsiz olarak edinilebilecek olan Tableau Imager, Windows işletim sistemi tabanlı adli kopya alma yazılımıdır. E01, RAW/DD ve DMG uzantılı adli kopya dosyalarını desteklemektedir. Desteklediği bu adli kopya türlerini birbirine dönüştürme işlemi yapabilmektedir. MD5 ve SHA1'in hash hesaplama yöntemlerini desteklemektedir. Tableau yazma koruma donanımlarıyla uyumlu ve hızlı bir şekilde adli kopya alabilmektedir. Adli kopya alımı esnasında adli kopya alımını durdurma ve kaldığı yerden devam etme özelliğine sahiptir.

5.2.2.2.5. "dd" komutu

Linux tabanlı işletim sistemlerinde verinin elde edilmesi amacıyla kullanılan çok yönlü bir komuttur. "dd" komutu tüm Linux işletim sistemleri içerisinde yer almaktadır[159]. Unix tabanlı sistemlerde adli kopya almak için kullanılan en çok

---

[156] http://www.getdata.com/download.php

[157] http://www.forensicimager.com/

[158] http://www.tableau.com/index.php?pageid=products&model=TSW-TIM

[159] Henkoğlu, T. (2011). *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi.* İSTANBUL: PUSULA.s.59

kullanılan araçtır[160]. Her ne kadar tüm Linux işletim sistemleri üzerinde bu komutu yer alsa da; adli kopya alınacak bilgisayar Linux işletim sistemine sahip ise ve bilgisayarı kapatmadan adli kopya alma işlemi yapılacaksa; sistem üzerindeki komut kullanılmamalı, güvenilir bir kaynaktan alınmış olan "dd" programı kullanılmalıdır. Şüpheli bilgisayar üzerindeki "dd" komutu değiştirilerek farklı bir şekilde düzenlenmiş olabilir. Dolayısıyla "dd" komutu çalıştırıldığında adli kopyası alınmak istenen veriler değişebilir, silinebilir ve zarar görebilir. Adli kopyasının alındığı sanılan veriler aslında o esnada geri getirilemez şekilde siliniyor olabilir.

"dd" komutu ile birlikte komut parametrelerini kullanarak veri depolama biriminin bir bölümünün veya tamamının adli kopyasını almak mümkündür. "dd" komutunun adli bilişimde kullanımı için geliştirilmiş olan "dc3dd" ve "dcfldd" ismiyle kullanımda olan sürümleri mevcuttur.

"dc3dd" ve "dcfldd" komutları ile;

- Adli kopya alma sırasında[161] hash değeri hesaplatma,
- Adli kopyası alınan verinin miktarını gösterme,
- Verilere istenilen değerleri yazarak wipe atma,
- Adli kopyanın orijinal elektronik delil ile bire bir aynı olduğunun doğrulamasını yapma,
- Adli kopyanın kayıt dosyalarının istenilen boyutlarda parçalar halinde yazılmasını ayarlama,

---

[160] Chris PROSISE, K. M. (2003). *INCIDENT RESPONSE & COMPUTER FORENSICS, SECOND EDITION.* United States of America: McGraw-Hill/Osborne. s.157

[161] "dd" komutu ile adli kopya alımı sırasında aynı zamanda hash değeri hesaplatmak mümkün değildir. "dd" komutu ile adli kopya alındığında hash değeri hesaplatmak için tekrar bir işlem daha başlatmak gerekecektir ve bu işlemin tamamlanma süresi adli kopya alma süresiyle yaklaşık olarak aynıdır. Dolayısıyla zaten uzun süreler alan adli kopya alma işlemi için harcanması gereken süre bu komutun tercih edilmesiyle kazanılacaktır.

- Adli kopya ve adli kopyaya ait kayıt dosyaları istenilen bir uzak bağlantı üzerine kaydedilebilme işlemleri yapılabilmektedir.

Her iki komut ta adli kopya alma işleminin sonunda ekrana hesaplanan hash değerinin sonucunu verdiği gibi aynı zamanda da "haslog" ismiyle bu hash değerini kaydetmektedir[162]. Adli kopya alımı sırasında okuma hatasıyla karşılaştıklarında, okunamayan sektörler için adli kopya içerisine sıfır değerini yazmaktadır. Sadece RAW/DD türünde adli kopya oluşturabilmekte ve sadece bu türdeki adli kopyalar üzerinde çalışabilmektedirler. "dc3dd" komutu MD5, SHA1, SHA256 ve SHA512 hash türlerini desteklemekte iken "dcfldd" komutu bunlara ek olarak SHA384 hash türünü de desteklemektedir.

5.2.2.2.6. Guymager

Linux tabanlı işletim sistemlerinde kullanılabilen bir adli kopya alma yazılımıdır. İşlemci kullanımı, kopyalama süresi ve ortalama kopyalama hızı açısından Guymager yazılımının FTK Imager yazılımına göre başarılı olduğu tespit edilmiştir[163]. RAW/DD, AFF, E01 uzantılı adli kopyaları desteklemektedir. Ayrıca disk klonlama işlemi de yapabilmektedir. MD5 ve SHA256 hash hesaplama yöntemlerini desteklemektedir. Live CD'ler[164] üzerinde genellikle Guymager programı yer almaktadır. Kullanıcı arayüzüne sahip olduğu için kullanımı kolaydır ve komutlar bilmeye gerek kalmadan kullanılabilmektedir.

---

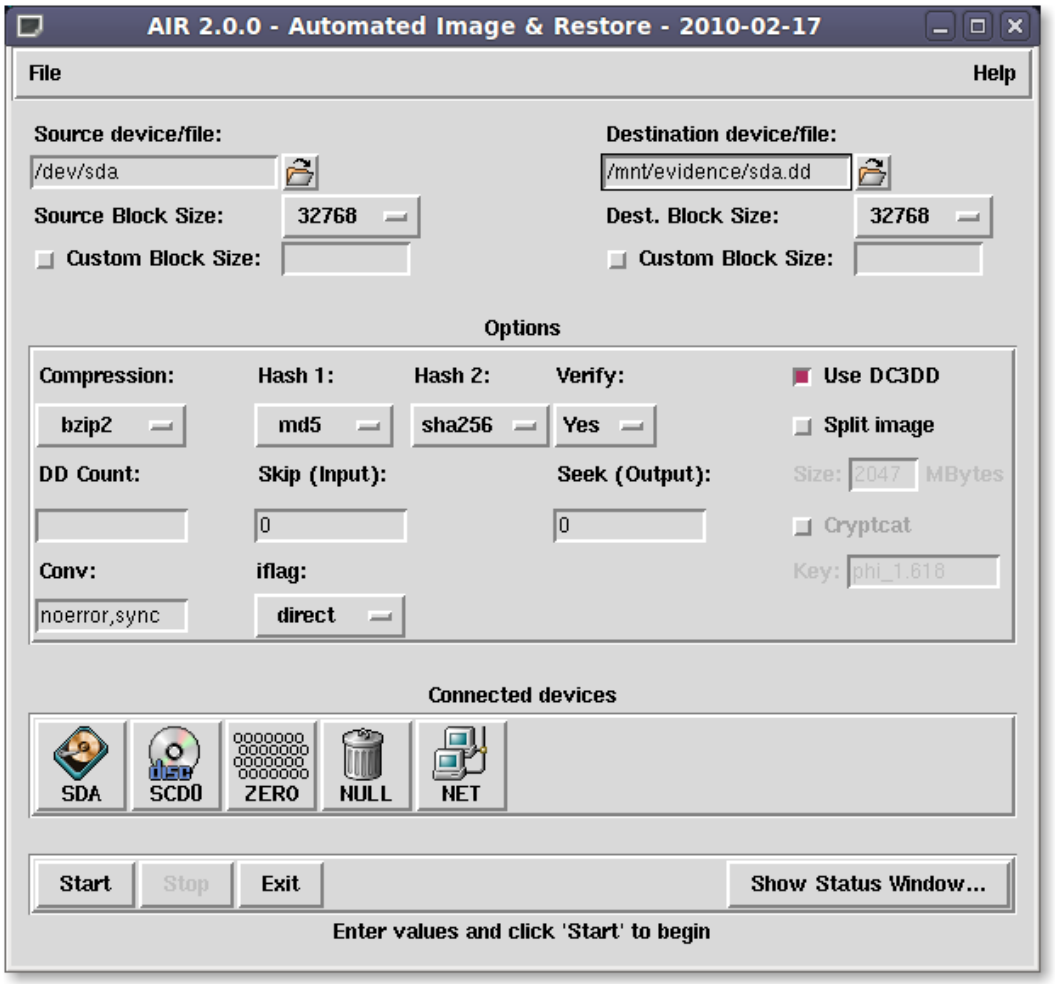
[162] Cory Altheide, H. C. (2011). *Digital Forensics with Open Source Tools.* Waltham, USA: Syngress. s.66

[163] Ahmet Serhat Şirikçi, N. C. (2012, Cilt 5, S.3). Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi. *Bilişim Teknolojileri Dergisi*, s. 29.

[164] Live CD: Bilgisayar sisteminin CD/DVD/USB üzerinde kurulu olan işletim sistemi üzerinden başlatılacak şekilde hazırlanmış olan CD kalıplarıdır.

SIFT, GRLM, DEFT, CAINE, MATRIUX, DFLCD, FORLEX, FORENS*NIX, PERIBR ve FCCU isimli Live CD'lerde Guymager isimli adli kopya alma programı mevcuttur.

5.2.2.2.7. AIR



Şekil 5.13 AIR programına ait görünüm[165]

İsmini İngilizce "**A**utomated **I**mage and **R**estore" kelimelerinin baş harflerinden alan bu program Linux tabanlı işletim sistemlerinde kullanılmaktadır. Kullanıcı arayüzünden kontrol ederek kolayca adli kopya almaya imkan sağlamaktadır. Birçok Live CD içerisinde yer almaktadır.

AIR programı;

- MD5, SHA1, SHA256, SHA384 ve SHA512 hash türlerini,
- CD-ROM, IDE/SATA ve SCSI girişli diskleri otomatik algılamayı,
- TCP/IP ağ bağlantısı üzerinden adli kopya almayı,

---

[165] http://sourceforge.net/apps/mediawiki/air-imager/index.php?title=Main_Page

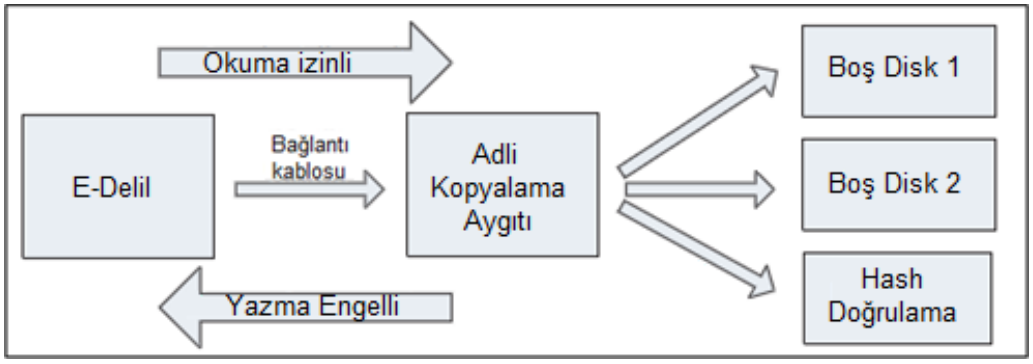
- Adli kopyaları belirli boyutlarda parçalar halinde kaydetmeyi,
- Ayrıntılı iş kaydı tutmayı,
- Adli kopyayı sıkıştırarak almayı desteklemektedir.

AIR arka planında "dd/dcfldd" komutlarını kullanarak adli kopya çıkartmaktadır.

5.2.2.3. Adli Kopya Alma Donanımları

E-delillerden adli kopya almak için çok sayıda donanım mevcuttur. Bu donanımlar adli kopya alma işlemleri sırasında e-delil üzerinde herhangi bir değişiklik yapmamak üzere yazma koruma sağlayacak şekilde tasarlanmışlardır.

Yazma koruma sistemini genel olarak gösterir resim aşağıdadır.



Şekil 5.14 Adli Kopyalama aygıtlarına ait yazma koruması çalışma sistemi[166]

Genel olarak kullanımı tercih edilen adli kopya alma donanımları aşağıdadır.

---

[166] Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., & Wright, C. (2007). *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators.* Burlington, A.B.D: Syngress Publishing. s.38

5.2.2.3.1. Tableau TD2

Şekil 5.15 Tableau TD2 Adli Kopya Alma Donanımı

Şekil 5.15'te fotoğrafı görülen Tableau TD2 donanımı SATA ve IDE/PATA bağlantısıyla çalışabilen veri depolama birimlerinin adli kopyalarını alabilmektedir. İsteğe bağlı olarak alınabilecek olan USB ve SAS dönüştürücüleriyle USB ve SAS bağlantısıyla çalışabilen veri depolama birimlerinin de adli kopyalarını alabilmektedir. Dakikada en fazla 9GB veri transferi yapabilmektedir. HPA ve DCO korumalarını aşarak veriye ulaşabilmektedir. Sabit diski, sabit diske ve sabit diski dosyaya bire bir olarak kaydedebilmektedir. MD5 ve SHA1 türlerinde hash değeri hesaplayabilmektedir. RAW/DD, E01 ve Ex01 uzantılarında adli kopya alabilmektedir. Sabit diskin adli kopyasını bir veya aynı anda iki diske birden alabilmektedir. Adli kopyalama işlemi sona erdiğinde adli kopya üzerinde hash doğrulaması yapabilmektedir. Adli kopya alımı sonrasında işlem ile ilgili bilgileri kaydedebilmektedir. Wipe işlemi yapabilmektedir. İçerisinde yüklü olan yazılım güncellenebilmektedir[167].

Kullanımı kolay ve pratik olarak tasarlandığı için en çok kullanımı tercih edilen adli kopya alma cihazlarındandır.

---

[167] http://www.tableau.com/index.php?pageid=products&model=TD2

5.2.2.3.2. Tableau TD3

Şekil 5.16 Tableau TD3 Adli Kopya Alma Donanımı

Şekil 5.16'da fotoğrafı görülen Tableau TD3 donanımı SAS, SATA, USB 3.0/2.0/1.1, FireWire(1394 A/B) ve IDE/PATA bağlantısıyla çalışabilen veri depolama birimlerinin adli kopyalarını alabilmektedir. Sahip olduğu dokunmatik ekranı üzerinden kontrol edilmektedir. Dakikada en fazla 9GB veri transferi yapabilmektedir. HPA ve DCO korumalarını aşarak veriye ulaşabilmektedir. Sabit diski, sabit diske ve sabit diski dosyaya bire bir olarak kaydedebilmektedir. MD5 ve SHA1 türlerinde hash değeri hesaplayabilmektedir. RAW/DD, E01 ve Ex01 uzantılarında adli kopya alabilmektedir. TD3 donanımının üzerinde gigabit hızlı ethernet bağlantı girişi vardır. E-deliller yazma korumalı olarak Ethernet girişi üzerinden ağ bağlantısıyla paylaşıma açılabileceği gibi e-delillerden alınmış olan adli kopyalar da ethernet girişi üzerinden ağ bağlantısıyla paylaşılabilir. Adli kopyalama işlemi sona erdiğinde adli kopya üzerinde hash doğrulaması yapabilmektedir. Adli kopya alımı sonrasında işlem ile ilgili bilgileri kaydedebilmektedir. FireWire girişi üzerinden Apple MAC bilgisayarların adli kopyasını alabilmektedir. Wipe işlemi yapabilmektedir. İçerisinde yüklü olan yazılım güncellenebilmektedir[168].

Kullanımı kolay ve pratik olarak tasarlandığı için en çok kullanımı tercih edilen adli kopya alma cihazlarındandır.

---

[168] http://www.tableau.com/pdf/en/Tableau_TD3_Users_Guide.pdf

5.2.2.3.3. Forensic Dossier

Şekil 5.17 Forensic Dossier Adli Kopya Alma Donanımı

Şekil 5.17'de fotoğrafı görülen Forensic Dossier donanımı SAS, SATA, USB 2.0/1.1, FireWire(1394 A/B) ve IDE/PATA bağlantısıyla çalışabilen veri depolama birimlerinin adli kopyalarını alabilmektedir. Bir e-delilin bir veya aynı anda iki sabit diske adli kopyasını alabildiği gibi, iki ayrı e-delilin adli kopyasını iki ayrı sabit diske de alabilmektedir. Sahip olduğu dokunmatik ekranı üzerinden kontrol edilmektedir. Dakikada en fazla 7GB veri transferi yapabilmektedir. HPA ve DCO korumalarını aşarak veriye ulaşabilmektedir. Sabit diski, sabit diske ve sabit diski dosyaya bire bir olarak kaydedebilmektedir. MD5 türünde hash değeri hesaplayabilmektedir. RAW/DD ve E01 uzantılarında adli kopya alabilmektedir. Adli kopya alma işlemi sırasında veya sadece adli kopya almaksızın e-delil üzerinde kelime araması yapabilmektedir. Forensic Dossier donanımının üzerinde ethernet bağlantı girişi vardır. Adli kopya ethernet girişi üzerinden ağ bağlantısıyla paylaşıma açılabilir. Adli kopyalama işlemi sona erdiğinde adli kopya üzerinde hash doğrulaması yapabilmektedir. Adli kopya alımı sonrasında işlem ile ilgili bilgileri kaydedebilmektedir. FireWire girişi üzerinden Apple MAC bilgisayarların adli kopyasını alabilmektedir. Wipe işlemi yapabilmektedir. İçerisinde yüklü olan yazılım güncellenebilmektedir[169].

[169] http://www.logicube.com/shop/forensic-dossier/

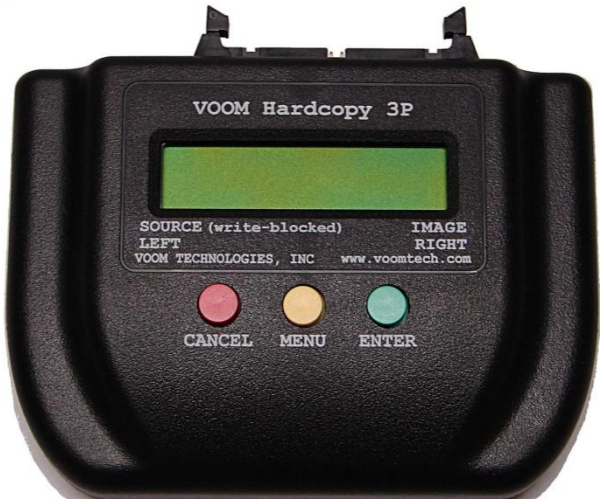
5.2.2.3.4. Image MASSter Solo-4

Şekil 5.18 Image Masster Solo-4 Adli Kopya Alma Donanımı

Şekil 5.18'de fotoğrafı görülen Image Masster Solo-4 donanımı SCSI, SAS, SATA, USB 3.0/2.0/1.1, FireWire(1394 A/B), hafıza kartı ve IDE/PATA bağlantısıyla çalışabilen veri depolama birimlerinin adli kopyalarını alabilmektedir. Bir e-delilin bir veya aynı anda iki sabit diske adli kopyasını alabildiği gibi, iki ayrı e-delilin adli kopyasını iki ayrı sabit diske de alabilmektedir. Sahip olduğu dokunmatik ekranı üzerinden kontrol edilmektedir. Dakikada en fazla 18GB veri transferi yapabilmektedir. HPA ve DCO korumalarını aşarak veriye ulaşabilmektedir. Sabit diski, sabit diske ve sabit diski dosyaya bire bir olarak kaydedebilmektedir. SHA-1, SHA2 ve MD5 türlerinde hash değeri hesaplayabilmektedir. RAW/DD, E01 ve VHD uzantılarında adli kopya alabilmektedir. Adli kopya alma işlemi sırasında adli kopyayı AES256 algoritmasıyla şifreli bir yapıya dönüştürerek kaydedebilmektedir ve yine adli kopya alma işlemi sırasında word, excell, PDF, yazı, resim, video ve ses dosyaları donanımın üzerindeki ekrandan önizleme yapılabilmektedir. Haricen temin edilen cep telefonu adli kopya alma yazılımları bu donanım ile birlikte kullanılabilmektedir. Image Masster Solo-4 donanımının üzerinde ethernet bağlantı girişi vardır. Adli kopya gigabit hızlı ethernet girişi üzerinden ağ bağlantısıyla paylaşıma açılabilir. Adli kopyalama işlemi sona erdiğinde adli

kopya üzerinde hash doğrulaması yapabilmektedir. Adli kopya alımı sonrasında işlem ile ilgili bilgileri kaydedebilmektedir. Wipe işlemi yapabilmektedir. İçerisinde yüklü olan yazılım güncellenebilmektedir[170].

5.2.2.3.5. Hardcopy 3P



Şekil 5.19 Hardcopy Adli Kopya Alma Donanımı

Şekil 5.19'da fotoğrafı görülen Hardcopy 3P donanımı SATA ve IDE/PATA bağlantısıyla çalışabilen veri depolama birimlerinin adli kopyalarını alabilmektedir. Bir e-delilin bir veya aynı anda iki sabit diske adli kopyasını alabilmektedir. Dakikada en fazla 6GB veri transferi yapabilmektedir. HPA ve DCO korumalarını aşarak veriye ulaşabilmektedir. Sabit diski, sabit diske ve sabit diski dosyaya bire bir olarak kaydedebilmektedir. SHA256 ve MD5 türlerinde hash değeri hesaplayabilmektedir. RAW/DD uzantısında adli kopya alabilmektedir. Adli kopyalama işlemi sona erdiğinde adli kopya üzerinde hash doğrulaması yapabilmektedir. Adli kopya alımı sonrasında işlem ile ilgili bilgileri kaydedebilmektedir. Wipe işlemi yapabilmektedir. İçerisinde yüklü olan yazılım güncellenebilmektedir[171].

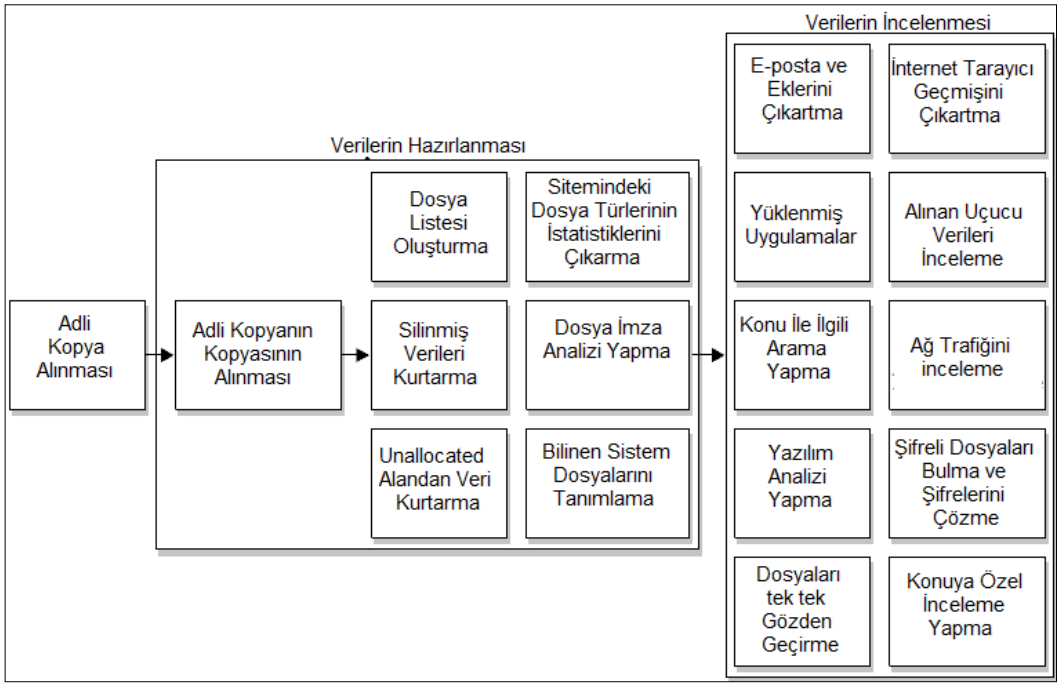
---

[170] http://www.ics-iq.com/v/vspfiles/files/datasheets/Solo-4%20Ruggedized.pdf

[171] http://www.voomtech.com/sites/default/files/HC3P%20Product%20Brief%208-16-12_0.pdf

5.3. E-Delillerin İncelenmesi

E-deliller üzerinde sağlıklı bir inceleme ve bu inceleme sonucunda maddi gerçeğe uygun bir delil elde edilebilmesi için, olay yerinden toplanan materyallerin incelemesini yapacak her türlü cihaz ve konusunda uzman personelin bulunduğu bir laboratuar ortamına gerek duyulmaktadır. Her türlü ihtimale karşı, inceleme yazılımları, birçok dönüştürücü cihaz ve tamir bakım setleri gibi araç gereçlerin her an hazır tutulması gerekmektedir[172]. İnceleme için laboratuarlardaki en önemli gereksinimlerden birisi de adli bilişim için özel olarak kullanıma sunulmak üzere tasarlanmış programlardır. Adli bilişim alanında incelemelerde genel olarak aşağıdaki resimde görülen işlemler yapılmaktadır.



Şekil 5.20 İnceleme sırasında genellikle yapılan işlemler.

Şekil 5.20'de görülen işlemleri yapabilmek ve incelemede hedefe ulaşabilmek için araç olarak kullanılan olan yazılımlar ve donanımlar aşağıdadır.

---

[172] DOKURER, S. (2013, Mayıs 05). *Bilişim Suçlar im Suçları ve Adli Bili Adli Bilişim.* DATA SECURITY, COMPUTER CRIME, COMPUTER FORENSICS AND DATA RECOVERY: http://www.dokurer.net/files/documents/Adli_Bilisim_Wormy.pdf s.43

5.3.1. İncelemelerde Genel Olarak Kullanılan Donanım ve Yazılımlar

Bu alanda en çok bilinen Encase Forensic, Forensic Toolkit ve SIFT gibi yazılımlardır[173]. Encase Forensic ve Forensic Toolkit yazılımları, inceleme konusu e-delil üzerinde son derece tutarlı ve tekrar edilebilir sonuçlar verdiği için, ticari yazılımlar arasında ön plana çıkmışlardır. Ticari yazılımlar, ücretsiz yazılımlara oranla daha fonksiyonel ve gelişiminin daha hızlı olması nedeniyle daha kullanışlıdır. Fakat bunun bedeli olarak, özellikle genel kabul görmüş ticari yazılımlar, bireysel imkanlarla her adli bilişim uzmanının sahip olabilmesinin mümkün olmadığı ücretler karşılığında satın alınabilmekte ve güncellenebilmektedir[174].

Ticari yazılımlar ücretsiz yazılımlara göre;

- Kolay kullanım arayüzüne sahip olma,
- Teknik destek alabilme,
- Hızlı güncellemelerle yeni kabiliyetlere kavuşabilme,
- Eğitim ve sertifikasyon,
- Görsel olarak daha anlaşılabilir sonuçlar,
- Detaylı ve düzenlenebilir raporlama,
- Windows işletim sistemi üzerinde çalışabilme gibi avantajlara sahiptirler.

Ancak bunun yanı sıra:

- Temin sırasında yüksek maliyetlere gerek duyulması,
- Güncellemeler için periyodik olarak yenilenmesi gereken lisans ücretleri,
- Kullanım ve sertifikasyon eğitimleri için istenilen yüksek ücretler,

---

[173] Clarke, N. (2010). *Computer Forensics A Pocket Guide.* United Kingdom: IT Governance Publishing. s.35

Henkoğlu, T. (2011). *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi.* İSTANBUL: PUSULA. s.43

- Programların kaynak kodlarının açık olmaması dolayısıyla program üzerinde değişiklik yapılamaması gibi dezavantajlara da sahiptirler.

5.3.1.1. Encase Forensic Yazılımı

Dünyada en çok kullanılan adli bilişim yazılımlarının ilk sıralarında yer alır. Guidance Software şirketi tarafından ticari olarak kullanıma sürülen ücretli bir yazılımdır. Windows işletim sistemi üzerinden çalışmaktadır. Lisanslı olarak çalışabilmesi için dongle bilgisayara takılı olması gereklidir. Dongle olmadan DOS moda çalışabilir ve adli kopya alabilir[175]. Delil inceleme ve delil ilişkilendirme konunda kendisini kanıtlayan bu program, başta FBI olmak üzere dünyadaki birçok kolluk teşkilatı tarafından mutat olarak kullanılmaktadır. Gösterdiği performansın yanı sıra Avrupa ve A.B.D.'de neredeyse bütün mahkemeler tarafından, bu program vasıtasıyla mahkemeye sunulan rapor ve verilerin delil niteliğinde olduğu kabul edilmiştir. Bu sebepten ötürü son yıllarda Encase Forensic yazılımının Adli Bilişim konularında kullanım oranı ciddi anlamda artış göstermiştir[176].

Encase Forensic yazılımı ile:

- Sabit disk, usb bellek, RAM, dosya, klasör, sunucu gibi e-delillerin yanı sıra; akıllı telefon ve tabletlerin adli kopyası alınarak incelemesi yapılabilmektedir,
- Windows ve Unix işletim sistemli e-deliller üzerinde inceleme yapmayı desteklemektedir,
- E-delil ve adli kopya üzerinden hash hesaplaması yapabilmektedir,
- Veri kurtarma yapabilmektedir,
- Dosyalar üzerinde imza analizi ve hash analizi yapabilmektedir,

---

[175] Middleton, B. (2002). *Cyber Crime Field Handbook.* Florida: Auerbach Publications. s.50

[176] BOLAT, M. (2013, Mayıs 05). *Encase Nedir?* Özel Bilirkişilik ve Uzman Mütalaası Hizmetleri: http://www.adlibilirkisi.org/index.php?sayfa=makaleoku&kategori=13&id=444

- Hash tablosu kullanılarak sistem dosyaları gibi bilinen dosyalar ayıklanabilmektedir,
- Birçok çeşitli uzantılı dosyalar üzerinde önizleme yapılabilmesinin yanı sıra harici dosya göstericileri de programa eklenerek kullanılabilmektedir,
- EnScript[177] düzenlenebilmekte ve hazır olan EnScript'ler kullanılabilmektedir.
- Şablonu düzenlenilebilir raporlama özelliğine sahiptir,
- E-posta içeriğini harici bir programa gerek kalmaksızın gösterebilmektedir,
- İşlemler, kullanıcı tarafından belirlenecek şekilde sırasıyla ve otomatik olarak yapılabilmektedir,
- Dizin oluşturma işlemi yapılabilmektedir,
- Zaman çizelgesi çıkartabilmektedir,
- Kelime veya karakter araması yapılabilmektedir,
- "Passware Kit Forensic" isimli şifre bulma/kırma yazılımı ile birlikte çalışabilmektedir.

Haricen satılan eklentileri ile:

- Dosya, klasör, bölüm, şifreli bölüm vb. e-delil parçalarının yazma korumalı halde sürücü olarak başka programlarla görülebilir hale getirebilmektedir,
- Microsoft BitLocker, GuardianEdge Encryption Plus/Encryption Anywhere/Hard Disk Encryption, Utimaco SafeGuard Easy, McAfee SafeBoot, WinMagic SecureDoc Full Disk Encryption, PGP Whole Disk Encryption, Microsoft Encrypting File System (EFS), CREDANT Mobile Guardian, PST (Microsoft Outlook), şifreli PST dosyaları, NSF (Lotus Notes), NTUSER.dat, Security

[177] EnScript: Adli Bilişim incelemeleri sırasında belirli amaçları daha kolay şekilde gerçekleştirebilmek için ve/veya arananlara daha kolay ulaşabilmek için EnCase üzerinde kullanılmak üzere Java veya C++ dillerinde yazılmış olan küçük programlardır.

Hive, Active Directory 2003 (ntds.dit) gibi şifreli alanların şifrelerinin bulabilme/kırabilme özelliğine sahiptir,

- Yazılımsal olarak yazma koruma kullanılabilmektedir.

5.3.1.2. Forensic Toolkit(FTK) yazılımı

En çok kullanımı tercih edilen yazılımlardan biridir. AccessData Software şirketi tarafından ticari olarak kullanıma sürülen ücretli bir yazılımdır. FTK yazılımı ile yapılan adli bilişim incelemeleri mahkemelerde kabul edilen güvenilirliğe sahiptir[178].

Program arayüzü tüm farklı özellikleri ve seçenekleri ile, ilk bakışta korkutur, ancak program kullanıldıkça, kullanım çok daha sezgisel hale gelir[179].

Forensic Toolkit yazılımı ile:

- Sabit disk, usb bellek, RAM, dosya, klasör, sunucu gibi e-delillerin adli kopyası alınarak incelemesi yapılabilektedir,
- Windows ve Unix işletim sistemli e-deliller üzerinde inceleme yapmayı desteklemektedir,
- E-delil ve adli kopya üzerinden hash hesaplaması yapabilmektedir,
- Veri kurtarma yapabilmektedir,
- Dosyalar üzerinde imza analizi ve hash analizi yapabilmektedir,
- Hash tablosu kullanılarak sistem dosyaları gibi bilinen dosyalar ayıklanabilmektedir,
- Birçok çeşitli uzantılı dosyalar üzerinde önizleme yapılabilmesinin yanı sıra harici dosya göstericileri de programa eklenerek kullanılabilmektedir,
- 100'den fazla uygulamanın şifresi kurtarılabilmektedir,

---

[178] *Forensic Toolkit® (FTK®): Recognized around the World as the Standard in Computer Forensics Software*. (2013, Mayıs 05). e-Discovery, Computer Forensics; Cyber Security Software: http://www.accessdata.com/products/digital-forensics/ftk

[179] Albert J. Marcella, J. D. (2008). *Cyber Forensic.* New York: Auerbach Publications. s.35

- Otomatik analiz yapılabilmektedir,
- Devam eden işlemleri durdurma, duraklatma ve devam ettirme gibi kontrol seçenekleri mevcuttur,
- Şablonu düzenlenilebilir raporlama özelliğine sahiptir,
- Kapsamlı uçucu veri analizi yapabilmektedir,
- E-posta içeriğini harici bir programa gerek kalmaksızın gösterebilmektedir,
- Zaman çizelgesi çıkartabilmektedir,
- Dizin oluşturma hizmeti çok gelişmiş olarak yapılabilmektedir,
- FTK programının hata vererek çalışmayı durdurması gibi bir duruma karşı, veritabanı üzerinde işlemlerin durmaksızın devam edeceği bir yapıda tasarlanmıştır,
- Apple DMG ve DD_DMG çeşitlerindeki adli kopyalar üzerinde çalışabilmektedir,
- SQLite veritabanını desteklemektedir,
- Kelime veya karakter araması yapılabilmektedir,
- Credant, SafeBoot, Utimaco, SafeGuard Enterprise and Easy, EFS, PGP, GuardianEdge, Pointsec and S/MIME gibi şifreli alanların şifrelerinin bulabilme/kırabilme özelliğine sahiptir,

Haricen satılan eklentileri ile:

- Cerberus malware analiz yazılımı ile malware analizi yapılabilmektedir,
- 30.000'den fazla fotoğraf kütüphanesi ile e-delil üzerinde potansiyel pornografik fotoğrafları tespit edebilmektedir,
- FTK programıyla bütünleşmiş bir şekilde çalışabilen Password Recovery Tool Kit(PRTK) programı ile şifreli dosyalar üzerinde çalışmalar yapılabilmektedir[180].

---

[180] Bryson, C., Casey, E., Clark, D. F., Frederick, K., Gibbs, K. E., Larson, T., . . . Knijff, R. v. (2004). *Handbook of Computer Crime Investigation Forensic Tools and Technology.* London: Elseiver Academic Press. s. 47

5.3.1.3. The Sleuth Kit ve Autopsy Yazılımları

The Sleuth Kit yazılımı açık kaynak kodlu ve ücretsiz bir yazılımdır. Unix ve Windows işletim sistemlerinde çalışabilmektedir. Komut satırı üzerinden kullanılabilen bir inceleme yazılımıdır[181]. Bir incelemenin tamamen komut satırı üzerinden yapılmasının sıkıcı olduğu herkes tarafından bilinmektedir. Bu sebeple The Sleuth Kit içerisinde Autopsy isimli grafiksel arayüz üzerinden The Sleuth Kit'e ait komutları kullanmaya imkan veren bir program mevcuttur. Autopsy ile e-delil yönetimi, adli kopya bütünlüğünü kontrol, kelime araması vb. otomatik uygulamalar kullanılabilmektedir.

The Sleuth Kit ve Autopsy yazılımları ile:

- DD, Encase, ve AFF uzantılı adli kopyalar üzerinde inceleme yapılabilmektedir,
- NTFS, FAT, UFS 1, UFS 2, EXT2FS, EXT3FS, HFS, ve ISO 9660 ve bunların türü olan dosya sitemlerini desteklemektedir,
- Kelime veya karakter araması yapılabilmektedir,
- E-delil ve adli kopya üzerinden hash hesaplaması yapabilmektedir,
- Hash tablosu kullanılarak sistem dosyaları gibi bilinen dosyalar ayıklanabilmektedir,
- Zaman çizelgesi çıkartabilmektedir,
- Veri kurtarma yapılabilmektedir,
- Steganography[182] kontrolü yapılabilmektedir,

---

[181] *The Sleuth Kit*. (2013, Mayıs 06). The Sleuth Kit (TSK) & Autopsy: Open Source Digital Investigation Tools: http://www.sleuthkit.org/sleuthkit/index.php

[182] Steganography: Eski Yunanca'da "gizlenmiş yazı" anlamına gelmektedir. Bir resim veya text dosyası arkasına yazı, dosya vb. içerikleri saklama yöntemidir. Bilgiyi gizleme (şifreleme değil) bilimine verilen addır. Steganografi'nin şifrelemeye göre en büyük avantajı bilgiyi gören bir kimsenin gördüğü şeyin içinde önemli bir bilgi olduğunu fark etmiyor olmasıdır, böylece içinde bir bilgi aramaz.

5.3.1.4. SANS Investigative Forensic Toolkit (SIFT)

SANS Enstitüsü, ortak araştırma ve eğitim kuruluşu olarak 1989 yılında kurulmuştur. Adli bilişim alanında araştırma ve eğitim faaliyetlerine devam etmekte olan SANS Enstitüsü SIFT adıyla derleyip geliştirerek, ücretsiz olarak kullanıma sunduğu inceleme araçlarıyla ilgili dünya üzerinde geniş bir yelpazede eğitimlerine devam etmektedir. SIFT Unix tabanlı işletim sistemi üzerinden çalışmaktadır ve Windows tabanlı işletim sistemleri üzerinde sanal bilgisayar üzerinde çalıştırılabilmesi için hazırlanmış sürümü de mevcuttur. İçerisinde Sleuth Kit ve Autopsy de dahil olmak üzere incelemede kullanılacak birçok araç mevcuttur. The Sleuth Kit ve Autopsy yazılımları ile yapılabilenlerin yanı sıra;

SIFT yazılımı ile:

- Windows (MSDOS, FAT, VFAT, NTFS), MAC (HFS), Solaris (UFS), Linux (EXT2/3/4) tabanlı sistemler üzerinde inceleme yapmayı desteklemektedir,
- E01, DD ve AFF uzantılı adli kopyalar üzerinde çalışabilmektedir,
- Malware analizi yapılabilmektedir,
- Şifre kırma/bulma işlemi yapılabilmektedir,
- Ağ bağlantıları üzerinde inceleme yapılabilmektedir,
- Antivirüs taraması yapılabilmektedir,
- Pdf uzantılı dosyaların içerikleri yazıya dönüştürülebilmektedir,
- Skype programına ait yazışmaları RAM üzerinden çıkartabilmektedir,
- Yahoo e-posta sunucusu üzerinden açılmış olan e-postaları RAM üzerinden çıkartabilmektedir,
- Facebook anlık ileti kayıtlarını RAM üzerinden çıkartabilmektedir,
- Gmail üzerinden açılmış olan e-postaları RAM üzerinden çıkartabilmektedir,
- Windows XP işletim sistemine ait kurtarma noktası kayıtları üzerinde inceleme yapılabilmektedir,

- Dosya kurtarma yapılabilmektedir,
- Ağ bağlantılarına ait paketlerin toplanması,
- Resim önizleme ile ilgili sistem tarafından oluşturulmuş dosyaları inceleme(Thumbs.db: Windows 95 işletim sisteminden itibaren, Windows Vista hariç, her önizlemesi yapılan resme ait küçük önizleme resminin depolandığı bir veritabanı dosyasıdır[183]),
- İnternet Explorer'a ait internet geçmişini inceleme,
- Geri dönüşüm kutusu üzerinde inceleme,
- iPhone, Blackberry ve Android cihazları üzerinde inceleme,
- Registery kayıtları üzerinde inceleme,
- Windows işletim sistemi üzerinde bulunun "prefetch, usbstor, event log, vb." sistem tarafından kaydedilen bilgileri inceleme yapılabilmektedir[184].

5.3.1.5. Cellebrite UFED Touch Ultimate

Cep telefonları üzerinden adli incelemeye uygun olarak veri almak, cep telefonu üreticilerinin sayısının fazla olması, ürettikleri telefonların özelliklerinin farklı olması ve veri depolama yapılarındaki farklılıkların fazla olması gibi nedenlerden dolayı standart şekillere sahip değildir. Bu sebeple marka ve model desteği fazla olan bu donanımları adli incelemelerde kullanmak e-delillere zarar vermeden inceleme olanağı verdiğinden ve kısa zamanda e-delillerden içerik çıkartmayı mümkün kıldığından büyük avantaj sağlar. Genel olarak cep telefonu inceleme yazılımları/donanımları, desteklediği modellerden;

- Fiziksel adli kopya alabilmektedir,
- Mantıksal adli kopya alabilmektedir,

---

[183] Carroll, O. L., Brannon, S. K., & Song, T. (2008). *Computer Forensics.* Washington DC: The United States Attorneys. s.13

[184] *SIFT Workstation 2.14 Capabilities*. (2013, Mayıs 06). SANS Computer Forensics Training, Incident Response: http://computer-forensics.sans.org/

- Mevcut dosya içeriğini çıkartabilmektedir,
- Mevcut veya silinmiş; uygulamaları, şifreleri, e-postaları, çağrı geçmişini, mesajları, rehberi, ajanda bilgilerini, gps konum bilgilerini resimleri, video vb. dosyaları çıkartabilmektedir,

Şekil 5.21 Cellebrite Ufed Touch Ultimate donanımı[185]

Şekilde 5.21'de fotoğrafı görülen Cellebrite UFED Touch; sim kartlar, cep telefonları, akıllı telefonlar, GPS cihazları, tablet bilgisayarlar ve bazı müzik çalarlar üzerinden adli incelemeye uygun veriler alınmasını sağlayan bir donanımdır. Desteklediği marka ve model sayısı çok geniştir ve sıklıkla yeni model destekleri eklenmektedir. Dokunmatik ekrana sahiptir.

Desteklediği modellerden;

- Fiziksel adli kopya alabilmektedir,
- Mantıksal adli kopya alabilmektedir,
- Mevcut dosya içeriğini çıkartabilmektedir,

---

185 http://www.baquia.com/system/rich_text_images/000/003/703/original/touch.jpg?1361964126 adresinden alınmıştır.

- Mevcut veya silinmiş; uygulamaları, şifreleri, e-postaları, çağrı geçmişini, mesajları, rehberi, ajanda bilgilerini, gps konum bilgilerini resimleri, video vb. dosyaları çıkartabilmektedir,

UFED Physical Analyzer yazılımı kullanılarak kötücül(malware) yazılım araması yapabilme imkanı sunmaktadır[186].

UFED donanımı bilgisayar gibi başka bir donanım olmadan da kullanılabilmektedir.

5.3.1.6. XRY

Şekil 5.22 XRY donanımı[187]

Şekil 5.22'de fotoğrafı görülen XRY; sim kartlar, cep telefonları, akıllı telefonlar, GPS aygıtları, tablet bilgisayarlar ve bazı müzik çalarlar üzerinden adli incelemeye uygun veriler alınmasını sağlayan bir donanımdır. XRY donanımı Windows işletim sistemi üzerine kurulan programı ile birlikte kullanılabilmektedir.

---

[186] http://www.cellebrite.com/images/stories/brochures/UFED-Touch-Ultimate-ENGLISH-web.pdf

[187] http://www.msab.com/app-data/sidebar-images/xry-physical-2nd.png

XRY yazılımı ile aynı anda 3 farklı girişe sahip model üzerinde içerik çıkartma işlemi yapılabilmektedir.

5.3.2. Genel Olarak Karşılaşılan E-Delil İncelemesi Gerektiren Suçlar ve Bu Suçlarla İlgili İncelemelerde Tespitine Çalışılan E-Deliller

Her suç konusu olayda e-deliller üzerinde tespiti gereken ve tespitine çalışılan noktalar farklılık göstermektedir. Genel olarak hangi suç konusunda hangi konuların tespitinin yapılması gerektiğine dair hazırlanmış tablo aşağıdadır.

	E-delil inceleme türleri										
Potansiyel e-delil türleri	Bilgisayar sahteciliği	Çocuk tacizi ve pornosu	Network ihlalleri	Cinayet	Uyuşturucu	Mali sahtecilik ve dolandırıcılık	Kimlik hırsızlığı	Telekomünikasyon sahteciliği	Aile içi şiddet	E-posta ile tehdit	Online kumar
Online açık arttırma kullanıcı hesapları	x					x					
Yazılım ve dosya kullanıcı hesapları	x					x					
Adres defteri	x		x	x	x	x			x	x	x
Ses dosyaları		x		x	x				x		
Arka plan							x				
Banka günlükleri						x					
Doğum belgesi							x				
Tarayıcı geçmişi		x									
İş çekleri						x	x				
Ajanda	x				x	x					x
Kasiyer fişleri						x	x				
Chat günlükleri ve geçmişi	x	x								x	
Çek ve para ödeme emri fotoğrafları						x					
Çek bozdurma kartları						x	x				

	E-delil inceleme türleri										
Potansiyel e-delil türleri	Bilgisayar sahteciliği	Çocuk tacizi ve pornosu	Network ihlalleri	Cinayet	Uyuşturucu	Mali sahtecilik ve dolandırıcılık	Kimlik hırsızlığı	Telekomünikasyon sahteciliği	Aile içi şiddet	E-posta ile tehdit	Online kumar
Yazılım klonlaması								x			
Yazpılandırma dosyaları			x								
Kişi listesi											x
Çerezler		x									
Sahte mahkeme belgeleri							x				
Sahte para resimleri						x					
Sahte hediye çekleri							x				
Sahte sigorta belgeleri							x				
Sahte kredi belgeleri							x				
Sahte satış gelirleri							x				
Sahte araç tescilleri							x				
Para resimleri						x					
Müşteri veritabanı kayıtları								x			x
Müşteri bilgileri	x					x					x
Veritabanları	x				x	x					
Silinmiş dosyalar						x	x				
Günlükler				x					x	x	
Dijital kamera yazılımı	x	x					x				
Dijital fotoğraflar		x					x				
Sürüce belgeleri							x				

	E-delil inceleme türleri										
Potansiyel e-delil türleri	Bilgisayar sahteciliği	Çocuk tacizi ve pornosu	Network ihlalleri	Cinayet	Uyuşturucu	Mali sahtecilik ve dolandırıcılık	Kimlik hırsızlığı	Telekomünikasyon sahteciliği	Aile içi şiddet	E-posta ile tehdit	Online kumar
İlaç tarifleri					x						
Elektronik para transferleri											x
Elektronik seri numaraları								x			
Elektronik imzalar						x	x				
E-posta ve haber grubu ilanları							x				
E-postalar, notlar ve mektuplar	x	x	x	x	x	x		x	x	x	x
Çalıştırılabilir programlar			x								
Sahte kimlik					x	x					
Mali ve varlık kayıtları	x			x	x	x		x	x	x	x
Sabit ve mobil kimlik numaraları								x			
Oyunlar		x									
Grafik görüntüleme/düzenleme yazılımı		x									
Donanım ve yazılım araçları							x				
Kimlik şablonları							x				
Resimler		x			x					x	
İmza görüntüleri						x					
İnternet aktiviteleri ve günlükleri		x	x	x	x	x	x	x		x	x
Kimlik hırsızlığı ile ilgili internet activiteleri							x				
IP adresleri ve kullanıcı isimleri			x								
İnternet yayınlı chat kayıtları			x								

	E-delil inceleme türleri										
Potansiyel e-delil türleri	Bilgisayar sahteciliği	Çocuk tacizi ve pornosu	Network ihlalleri	Cinayet	Uyuşturucu	Mali sahtecilik ve dolandırıcılık	Kimlik hırsızlığı	Telekomünikasyon sahteciliği	Aile içi şiddet	E-posta ile tehdit	Online kumar
Yasal belgeler				x						x	
Haritalar				x							
Suç bölgesine ait haritalar										x	
Tıbbi kayıtlar				x							
Para transferleri						x	x				
Video dosyaları		x									
Kıymetli evrak/devredilebilir kıymetler							x				
Ağ diyagramları			x								
Çevrimiçi bankacılık yazılımları						x					x
Çevrimiçi siparişler						x	x				
Çevrimiçi ticaret bilgileri						x	x				
Ödeme kartı bilgileri ve numaraları	x					x	x				x
Ödeme kartı okuyucu ve yazıcıları						x	x				
Şahsi çekler						x	x				
PIN girişli cihazlar						x					
Şüpheli/mağdur fotoğrafları				x							
Reçete formu fotoğrafları					x						
E-posta, not ve mektup çıktıları											x
Online kumar sitelerine referanslar											x
Tarayıcı yazılımı							x				

	E-delil inceleme türleri										
Potansiyel e-delil türleri	Bilgisayar sahteciliği	Çocuk tacizi ve pornosu	Network ihlalleri	Cinayet	Uyuşturucu	Mali sahtecilik ve dolandırıcılık	Kimlik hırsızlığı	Telekomünikasyon sahteciliği	Aile içi şiddet	E-posta ile tehdit	Online kumar
Kimlik numaraları							x				
Kaynak kodları			x								
Spor bahis istatistikleri											x
Telefon görüşme kayıtları				x					x	x	
Kullanıcı adı ve şifre içeren metinler			x								x
Ücetsiz numaralar (0800)								x			
Trofe fotoğrafları				x							
Kullanıcı tarafından oluşturulmuş dosya ve klasörler		x									
Mağdur ile ilgili araştırma										x	

Şekil 5.23 Soruşturma türleri ve aranması gereken potansiyel e-delil çeşitleri[188]

Bir elektronik aygıt yapısı itibariyle belirli özelliklere sahiptir. Bu özelliklerin o elektronik aygıta kazandırdığı bir takım kabiliyetler olduğu gibi bununla birlikte o aygıtın özellikleri dışında limitleri de vardır. Dolayısıyla her farklı elektronik aygıt üzerinden elde edilebilecek e-deliller de farklılık göstermektedir. Genel olarak karşılaşılan elektronik aygıtlar ve bu aygıtlar üzerinden elde edilebilecek e-deliller tablosu aşağıdadır.

[188] U.S. Department of Justice Office of Justice. (2001). *Electronic Crime Scene Investigation: A Guide for First Responders.* Washington: PhotoDisc. s.42-44

Elektronik Aygıtlar	**Potansiyel E-deliller**
Bilgisayar Sistemleri	<u>Kullanıcı tarafından oluşturulan dosyalar</u> — Adres defteri — Ses/görüntü dosyaları — Takvim — Veritabanı dosyaları — E-posta dosyaları — Resimler
	<u>Kullanıcı tarafından korunan dosyalar</u> — Sıkıştırılmış dosyalar — Şifre korumalı dosyalar — Kriptolu dosyalar — Gizli dosyalar
	<u>Bilgisayar tarafından oluşturulan dosyalar</u> — Yedekleme dosyaları — Çerezler[189] — Yapılandırma dosyaları — Günlük kayıt dosyaları — Geçmiş kayıtları — Sistem dosyaları — Geçici dosyalar
	<u>Diğer</u> — Bilgisayar tarihi, saati, şifresi — Silinmiş dosyalar — Gizli bölümler — Üstveri bilgileri — Yazılım kayıt bilgileri — Unallocated alan

189

Akıllı kartlar, dongle'lar, biyometrik tarayıcılar	— Karta, kullanıcıya, erişim ve kontrol seviyesine, ayarlara, izinlere ve sahipliğe ait tanımlama ve doğrulama bilgileri içerir
Telesekreter	— Arayan bilgisi — Silinmiş mesajlar — En son aranan numara — Telefon numaraları ve isimleri
Dijital fotoğraf makineleri	— Fotoğraflar — Çıkarılabilir hafıza kartları — Ses kayıtları — Video kayıtları — Tarih saat bilgisi
El cihazları (PDA gibi)	— Radevu/takvim bilgileri — E-posta — Şifre — Telefon defteri — El yazısı — Yazılı mesajlar — Sesli mesajlar
Harici depolama ortamı (Hafıza kartı gibi)	— (Bilgisayar sistemleri ile aynı içerik)
Yerel Alan Ağı (LAN) Kartı veya Ağ Arayüz Kartı (NIC)	— Cihazın kendisi ile ilgili bilgi — MAC adresi
Router, Hub, Switch	— Cihazların kendileri ile ilgili bilgi — Yapılandırma bilgileri(router için)
Çağrı cihazları	— Adres bilgisi — E-posta — Telefon numaraları — Yazılı mesajlar

	— Sesli mesajlar
Yazıcılar	— Dokümanlar — Sabit disk — Ağ kimlik bilgisi — Silindir üzerinde bindirilmiş görüntüler — Tarih saat bilgisi — Kullanıcı kullanım kayıtları
Tarayıcı	— Tarama bilgileri
Telefon	— Randevu takvim bilgileri — Arayan kimlik bilgileri — Elektronik seri numarası — Hafıza — Şifre — Rehber — Telesekreter

Şekil 5.24 Elektronik aygıtlar içerisindeki potansiyel e-deliller[190]

Cep telefonlarından, özelliklerinde mevcutsa, genellikle aşağıdaki içerikler elde edilmektedir:

- Gelen, giden ve cevapsız çağrılar,
- Gelen ve giden yazılı mesajlar[191],
- Rehber,
- Ses kayıtları,
- Fotoğraf, video, resim ve diğer çalışma dosyaları,
- Takvim, ajanda, alarm saati, hatırlatma kayıtları, yapılacaklar listesi,
- Hafızaya kaydedilen notlar,
- E-posta kayıtları,
- İnternet tarayıcısı geçmişi,

[190] http://www.first.org/vendor-sig/isodocs/iso-iec-n7570_wd7934.pdf s.29-31

[191] Volonino, L., & Anzaldua, R. (2008). *Computer Forensics For Dummies.* Indianapolis: Wiley Publishing, Inc. s.222

- GPS bilgileri,
- PIN numarası,
- IMEI numarası,
- Kullanılan kablosuz ağlar ile ilgili bilgi,
- Telefon hafızasına eklenen kelimeler,
- GPRS, WAP ve internet ayarları elde edilebilirler[192].

5.4. E-Delillerin Raporlandırılması

Raporlandırma aşaması diğer tüm aşamalar geçildikten sonra e-delillerin inceleme sürecini tamamlayan en önemli ve en zor aşamadır[193]. E-delil üzerinde yapılan tüm teknik çalışmalar ve bu çalışmalar sonucunda ulaşılan ve değerlendirilen bilgiler incelemeyi yapan tarafından anlaşılır bir yargı ve sonuç belirtse de, raporlandırma işlemi yeterince açık ve anlaşılır olmadığı takdirde; rapor, raporu inceleyen diğer gözler tarafından doğru ve yeterli bir şekilde anlaşılamayacak ve e-delil üzerinde yapılan inceleme söz konusu olayı aydınlatmada, ya hiç yararlı olmayacak, ya da yanlış yönlendirmeler yapılmış olacaktır.

İyi bir raporda bulunması gereken özellikler şunlardır:

- Standart bir yapıda olmalıdır,
- Rapor başından sonuna kadar açık ve net bir şekilde anlaşılır olmalıdır[194],
- Resmi bir dil kullanılmalıdır,
- Yazım kurallarına uyulmalıdır,

---

[192] Androulidakis, I. I. (2012). *Mobile Phone Security and Forensics.* New York Heidelberg Dordrecht London: Springer. s.77

[193]Chris PROSISE, K. M. (2003). *INCIDENT RESPONSE & COMPUTER FORENSICS, SECOND EDITION.* United States of America: McGraw-Hill/Osborne. s.30

[194] Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., & Wright, C. (2007). *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators.* Burlington, A.B.D: Syngress Publishing. s.740

- Mümkün olduğunca yabancı kelimeler kullanılmamalı, mümkün değilse de kullanılan kelimelerin anlamları açıklanmalıdır.
- Sürekli veya sık sık kullanılan teknik terimler veya yabancı terimler var ise, bu terimlerden oluşan bir sözlük hazırlanmalıdır[195],
- Raporda kısaltmalar kullanılıyor ise bu kısaltmalar da, açık halleriyle birlikte, hazırlanan sözlük içerisinde yer almalıdır,
- Çıkartılan sonuçlar mümkün olduğunca kısa ve öz olmalıdır[196],
- İnceleme konusu ile ilgili olarak sadece aleyhte olan sonuçlar değil lehte olan sonuçlar da olmalıdır,
- Gerekmiyorsa detay bilgi içermemelidir,
- Varsayım veya ihtimal değil somut bilgiler içermelidir,
- Tespitler doğru bir sırayla raporda sunulmalıdır,
- Rapor karmaşık bir görünümde olmamalıdır,
- Rapora konulan fotoğraf, anlık ekran görüntüsü vb. görsellerin ne için konulduğu belirtilmelidir,
- Rapor içerisinde fazladan detay bilgi olduğu için konulmak istenmeyen ancak rapor okuyucusu tarafından istenirse bakılabilmesi istenilen bilgiler ek olarak sunulmalıdır,
- Çok uzun raporlarda "içindekiler" bölümü olmalıdır,
- Raporun sayfalarında numaralandırma olmalıdır,
- Rapor, içeriği değiştirilmeyecek veya içeriğinin değiştirildiğinin anlaşılmasına imkan tanıyacak bir formatta sunulmalıdır ve aslı muhafaza edilmelidir[197],

---

[195] A.g.e. s. 740

[196] Henkoğlu, T. (2011). *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi.* İSTANBUL: PUSULA. s.214

[197] Öztürkci, H. (2009). Adli Bilişim'e Giriş ve Microsoft Sistemlerinde Adli Bilişim Temelleri. İstanbul. s.155

- İnceleme konusu ile ilgili olmayan ancak (örneğin: başka bir suç unsuru olduğu için) rapora eklenecek olan bulgular inceleme konusu ile ilgili tespitlerin tamamından sonra ayrı bir başlıkta sunulmalıdır.

Hazırlanacak olan raporda, her konuda aşağıdaki maddelerin tamamının olması zorunlu olmamakla birlikte, aşağıdaki bilgilerin bulunması gereklidir:

- İncelemeyi talep eden kurum/sahış bilgisi,
- İncelemeyi yapan kurum/sahış bilgisi,
- İnceleme konusu ile ilgili bilgiler,
- Özellikle tespiti istenilen bir husus var ise bu hususa ait bilgi,
- İncelemeye başlama-bitiş tarihleri,
- E-delilin aidiyet bilgileri,
- E-delil ile ilgili marka, model, seri numarası, kapasite vb. bilgiler.
- Sisteme ait tarih saat bilgileri[198],
- İncelemede kullanılan donanım ve yazılım bilgileri,
- Adli kopya ile ilgili hash değeri, adli kopya almakta kullanılan program adı ve sürümü vb. bilgiler,
- E-delil içerisindeki bulgulara ait hash değerleri,
- E-delil içerisindeki bulgulara ait dosya veya klasör isimleri, bulundukları konumları, oluşturma tarihleri, değiştirme tarihleri ve son erişim tarihleri[199],
- İnceleme tekniği ve incelemede izlenilen yol[200].

---

[198] Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., & Wright, C. (2007). *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators.* Burlington, A.B.D: Syngress Publishing. s.745

[199] "Oluşturma tarihleri, değiştirme tarihleri ve son erişim tarihleri" İngilizce kısaca "mac times" olarak kullanılmaktadır.

[200] Dave Garza, M. K. (2010). *Computer Forensic Evidence Collection and Preservation.* A.B.D.: Cengage Learning. b.6 s.2

6. Adli Bilişim Sürecinde Teknik Alanda Karşılaşılan Hash Problemleri

Elektronik delillerin depolandığı aygıtlar kısıtlı bir kullanım ömrüne ve karmaşık veri depolama yapılarına sahiptirler. CD-DVD gibi optik veri depolama aygıtları, Sabit diskler gibi manyetik veri depolama aygıtları, SSD diskler gibi flash yongalar üzerinde veri depolama teknolojisine sahip aygıtlar; her birinin kendine ait olan teknolojisine ve maruz kaldığı dış etkenlere göre değişen bir kullanım ömrü vardır. Bu veri depolama birimleri arasında veri okuma/yazma ömrü en uzun olan ve en yaygın kullanıma sahip olanı sabit disklerdir ancak mekanik diskler de bir noktada bozulacaktır. Kevin O'Shea'ye göre; belki günler, aylar veya daha uzun sürecek ancak bir noktada bozulacaklardır[201].

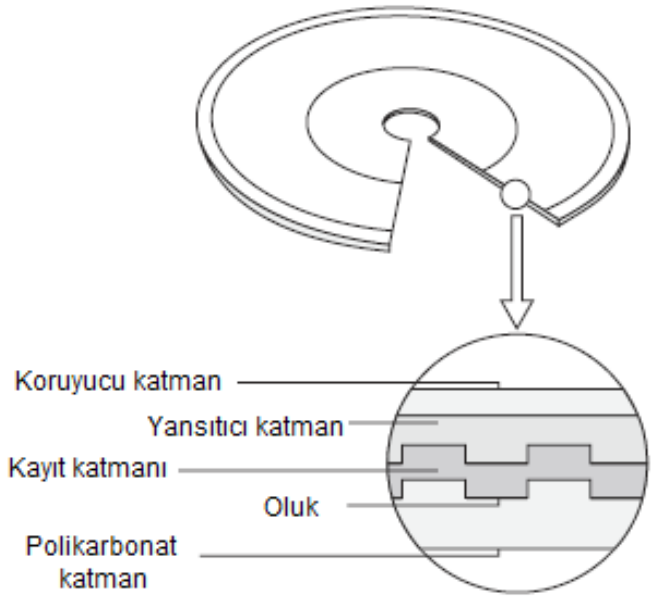
6.1. Optik Disklerde Hash Problemleri

Yaklaşık 30 yıldır kullanımda olan optik diskler(CD-DVD) bu 30 yıl içerisinde büyük bir gelişme gösterdiler. Günümüzde optik diskler için 200 yıla kadar ömür biçilse de onların ne zaman bozulacağını tahmin etmek oldukça güç. Tüm optik diskler, ortak olarak şu dört katmana sahiptirler: koruyucu katman, lazeri yansıtan parlak katman, verileri depolayan alaşımın bulunduğu katman ve polikarbonat katman[202].

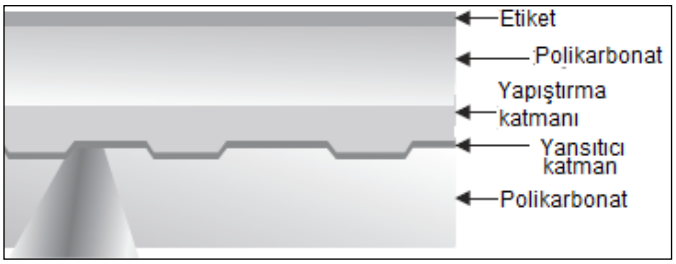
---

[201] Cohen T., C. K. (2007). *Alternate Data Storage Forensics* . United States of America: Syngress Publishing. s.80

[202] *Optik Disklerin Ömrünü Ne Belirliyor*. (2013, Nisan 05). www.chip.com.tr: http://www.chip.com.tr/haber/optik-disklerin-omrunu-ne-belirliyor_34753.html



Şekil 6.1 CD-ROM katmanları[203]



Şekil 6.2 DVD'den kesit[204]

Şekil 5.25 ve 5.26'da görüldüğü gibi farklı optik diskler, farklı katmanlara sahiptirler. Bu katmanlardan özellikle yansıtıcı katman, daha çok hasar görebilmektedir. Standart kompakt diskler, alüminyumdan oluşan bir yansıtıcı katmana sahiptir. Alüminyum, havaya maruz kaldığında oksitlenir. Bu, genellikle diskin kenarlarında gerçekleşir. Ancak diskin bozulmasına tek neden olan, yansıtıcı katmanın bozulması değildir. Kullanım ve muhafaza şartlarına bağlı

---

[203] Crowley, P., & Kleiman, D. (2007). *CD and DVD Forensics.* Rockland: Syngress Publishing, Inc. s.3

[204] Philipp, A., Cowen, D., & Davis, C. (2009). *Hacking Exposed Computer Forensics Second Edition.* ABD: mhprofessional s.37

olarak birçok sebep sayılabilir. Elektronik deliller doğru olmayan şekillerde taşınmaları ve muhafaza edilmeleri sonucunda da bozulabilmektedir.

Adli kopyası alınarak hash bilgisi kaydedilen elektronik delil niteliğindeki bir optik diskten bir süre sonra tekrar adli kopya alma işlemi yapıldığında hesaplanan hash değerleri birbirini tutmayabilmektedir. Bunun sebebi tamamen veya kısmen bozulduğu için okunamayan bir sektör olabildiği gibi daha önceden adli kopya alma işlemi sırasında okunamamış veya yanlış okunmuş ancak sonraki adli kopya alma işleminde doğru şekilde okunabilmiş bir sektörden de kaynaklanabilmektedir. Okunama veya eksik okuma sonucu hash değerlerinin uyuşmaması sorunu sadece optik diskten de kaynaklanmıyor olabilir. Bir optik sürücünün okuyabildiği optik disk üzerindeki veriyi, bir başka optik sürücü okuyamayabilmektedir. Ayrıca bazı adli kopya alma yazılımları arasında optik disk üzerinden okudukları sektör sayılarında fark olabilmektedir. Bu fark aynı programın farklı sürümlerinde de görülebilmektedir.

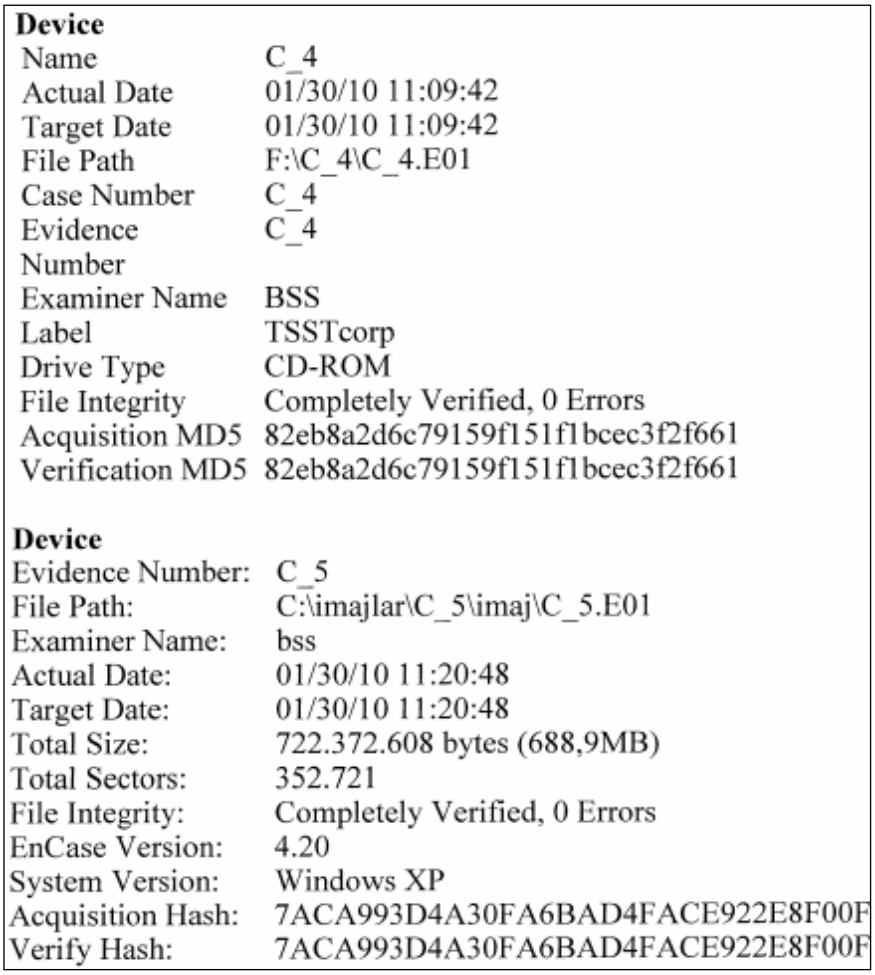
Bir yazılımın x sayıda sektör okuyarak almış olduğu adli kopyanın hash değeri, diğer yazılımın veya aynı yazılımın diğer sürümünün okumuş olduğu x-1 sayıda veya x+1 sayıda sektör okuyarak almış olduğu adli kopyanın hash değeri ile aynı olmayacaktır.

Uygulama	Hash değerleri	Sektör sayısı
Encase 4	A296A352F2C8060B180FFE6F32DE6392 (1 Read error)	1207
Encase 5	7A1366AE9CC3A96FD9BF56B9B91A633B	1206
FTK	44133feb352d37bc365ec210df81d7fd	1208
X-Ways	2211A026EC7F309517050D55CEEE2954(2 Read errors)	1208
MD5sum/readcd	I/O error	1208

Şekil 6.3 Aynı optik diskten farklı programlarla alınan adli kopyalarda okunan sektör sayıları ve hash değerleri

Bir yargılama konusunda elektronik delil olan 16 adet optik disk üzerinde tekrar hash hesaplatılması yaptırılmış ve hesaplanan hash değerlerinden 10 tanesinin daha önce alınan adli kopya sırasında hesaplanmış olan hash değerleriyle uyuşmadığı görülmüştür. Bu uyuşmazlığın kullanılan yazılımın

sürüm farkından kaynaklandığı ilerleyen süreçte tespit edilmiştir.



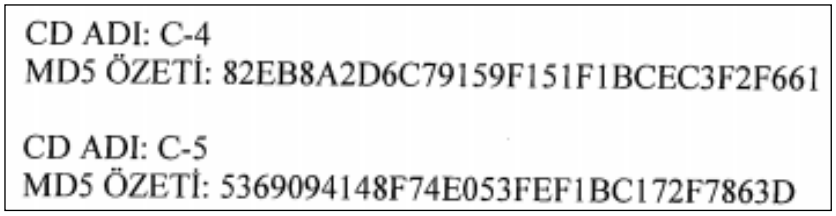
Device

Name	C_4
Actual Date	01/30/10 11:09:42
Target Date	01/30/10 11:09:42
File Path	F:\C_4\C_4.E01
Case Number	C_4
Evidence Number	C_4
Examiner Name	BSS
Label	TSSTcorp
Drive Type	CD-ROM
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	82eb8a2d6c79159f151f1bcec3f2f661
Verification MD5	82eb8a2d6c79159f151f1bcec3f2f661

Device

Evidence Number:	C_5
File Path:	C:\imajlar\C_5\imaj\C_5.E01
Examiner Name:	bss
Actual Date:	01/30/10 11:20:48
Target Date:	01/30/10 11:20:48
Total Size:	722.372.608 bytes (688,9MB)
Total Sectors:	352.721
File Integrity:	Completely Verified, 0 Errors
EnCase Version:	4.20
System Version:	Windows XP
Acquisition Hash:	7ACA993D4A30FA6BAD4FACE922E8F00F
Verify Hash:	7ACA993D4A30FA6BAD4FACE922E8F00F

Şekil 6.4 Bir davada delil olan optik disklerden 2 tanesine ait hash değerleri



CD ADI: C-4
MD5 ÖZETİ: 82EB8A2D6C79159F151F1BCEC3F2F661

CD ADI: C-5
MD5 ÖZETİ: 5369094148F74E053FEF1BC172F7863D

Şekil 6.5 C-4 ve C-5 isimli 2 adet delil olan optik diskten tekrar hesaplanan hash değerleri

Şekil 5.28 ve Şekil 5.29'da görüldüğü gibi C_4 isimli optik diske ait tekrar hesaplanmış olan hash değeri önceki hash değeri ile birebir aynı iken, C_5

isimli optik diske ait hash değerleri birbirini tutmamaktadır. Bunun sebebi ise Şekil 5.28'de görülen ilk adli kopya alımı sırasında C_4 isimli CD'nin Encase v6 sürümüyle adli kopyasının alınması, C_5 isimli CD'nin Encase v4 ile adli kopyasının alınması sonrasında; Şekil 5.29'da görülen işlemlerde her iki CD'nin de adli kopyalarının Encase v6 ile alınmış olmasıdır. C_4 isimli CD'ye ait hash değeri her iki adli kopya alım işleminde Encase'in aynı sürümü kullanıldığından aynı hash değerleriyle sonuçlanmıştır. C_5 isimli CD'de ise ilk adli kopya alımının Encase v4 ile ikinci adli kopya alma işleminin ise Encase v6 sürümüyle yapılması sonucu farklı hash değerleri hesaplanmıştır.

Adli kopyası mevcut olan bir elektronik delil üzerinden tekrar adli kopya alındığında hesaplanan hash değeri daha önceki hash değeri ile uyuşmayabilmektedir.

6.2. Sabit disklerde hash problemleri

Sabit diskler uçucu olmayacak şekilde ve hızlıca veri depolayan ve depolanan veriye tekrar ulaşmayı sağlayan aygıtlardır. Elektrik kesildiğinde üzerinde yazılı olan veri silinmez. Dolayısıyla bilgisayar kapandığında disk üzerinde kayıtlı olan veriler silinmeyecektir[205].

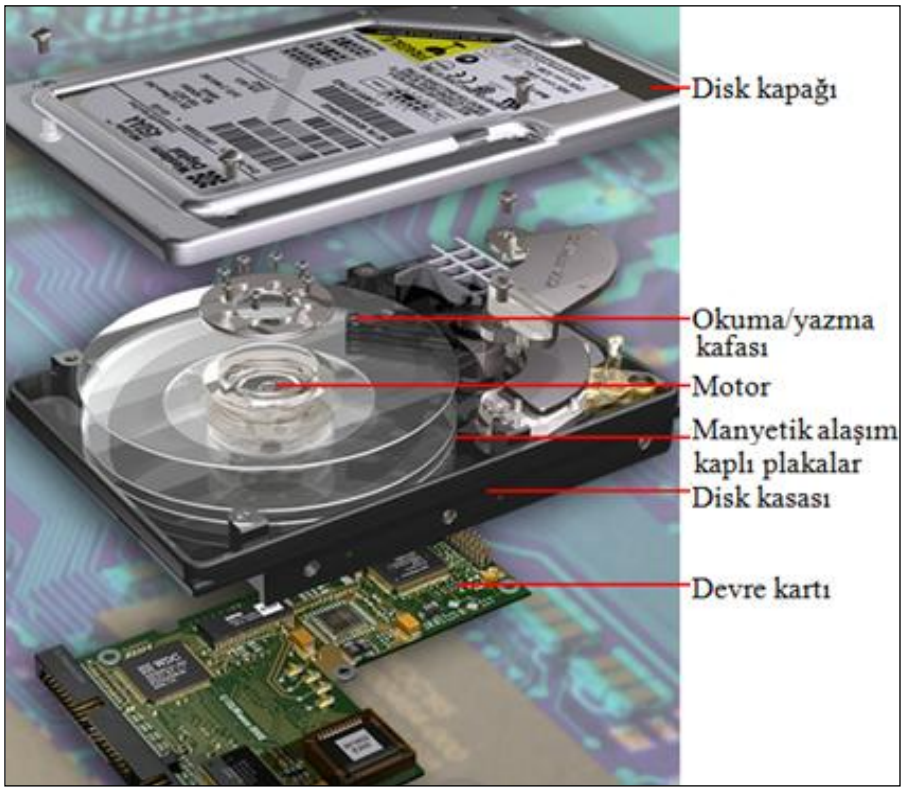
Sabit diskler manyetik olarak veri depolama yaparlar. Veri sabit disklerin içerisindeki cam, seramik veya metal plaka üzerinde kaplı olan özel alaşımlı yüzey üzerinde depolanmaktadır[206].

Günümüzde genellikle 2.5" ve 3.5" boyutlu sabit diskler kullanılmaktadır ve sabit disklerin IDE, SATA, SAS SCSI gibi çeşitli çeşitleri mevcuttur. Aşağıda Şekil 5.30'da Sabit disk parçaları görülmektedir.

---

[205] Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., & Wright, C. (2007). *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators.* Burlington, A.B.D: Syngress Publishing. s.62

[206] Mamun, A. A., Guo, G., & Bi, C. (2007). *Hard Disk Drive Mechatronics and Control.* New York: CRC Press. s. 8



Şekil 6.6 Sabit Disk Parçaları[207]

Sabit diskler üretildikten sonra sabit diskin veri depolama yüzeyindeki sorunlu noktaları belirlemek için üretici tarafından bir yüzey testinden geçirilir. Sabit diskler fabrikadan ilk çıktıklarında bile yüzeylerinde sorunlu noktalar mevcuttur. Ayrıca üzerinde veri depolanan bu mekanik yüzeyler zaman geçtikçe ve kullanıldıkça çevresel etkenlerin de etkisiyle özelliğini kaybedebilerek kullanılamaz hale gelebilmektedir. Hatta hiç kullanılmayan sabit diskler de, üretim maddelerinin ömrü kadar süreyle kısıtlı bir ömre sahiptirler. Fabrikadan çıkmadan önce yapılan yüzey testinde tespit edilen sorunlu noktalar sabit diskler üzerinde bulunan ve normal şartlarda kullanıcıların erişemediği servis alanında bir listede tutulurlar. Bu listede kayıtlı olan alanlara kullanıcı tarafından veri kaydı yapılmamaktadır. Genellikle sabit diskler üzerinde iki farklı bozuk sektör kaydı tutulan liste mevcuttur. Bunlardan birincisi sabit disk fabrikadan çıkmadan önce

[207] http://www.griffwason.com/images/GriffWason_WesternDigitalCaviar-ExplodedCutaway2.jpg

yapılan yüzey testinde tespit edilen bozuk sektörlerin tutulduğu P-List diğeri ise sabit disk kullanılırken bozulan ve sabit disk içerisindeki yazılım tarafından bozulduğu tespit edilen sektörlerin ve bu sektörler yerine kullanım için atanan sektörlerin bilgilerinin tutulduğu G-List'tir[208].

P-List içerisinde tutulan bozuk sektör bilgilerine, atlanacak sektörlere ait kayıt bilgileri de denilebilir. Her sabit diskin farklı sektörlerinde bozukluklar(Bozuk alanlar yada başka birşey) olacağından P-List sabit diske ait benzersiz ve sadece o diske özel bir listedir. Sabit diskin okuma yazma kafası P-list içerisinde kaydı bulunan sektörü daima atlar. Sabit disk içerisindeki adresleme P-List içerisindeki sektörler yokmuş gibi atlanarak yapılmaktadır. Dolayısıyla P-List'ine ulaşılamayan veya P-List'inde sorun oluşmuş bir sabit disk üzerindeki sektörlere ait adresleme P-List'siz bir şekilde yapıldığında verilere doğru bir şekilde ulaşmak mümkün değildir. Bu şekilde ancak küçük boyutlu ve parçalanmadan depolanmış veri parçalarına anlamlı bir şekilde ulaşabilmek mümkündür.

Sabit disk kullanılmaya devam edildiği sürede bozulduğu tespit edilen sektörler ve bu bozuk sektörler yerine kullanıma açılacak olan yedek sektör bilgisi G-List'e eklenir[209]. G-List'e eklenecek bozuk sektörler yerine kullanıma açılacak yedek sektörler belirli bir sayıda olmak üzere sabit diskin veri yazılan yüzeyinde önceden ayrılmışlardır ve bu ayrılmış alana, G-List'e eklenmedikçe, normal şartlarda kullanıcılar erişemezler. G-List'e ekleme işlemleri kullanıcı onayı alınmadan ve kullanıcı fark etmeden olur.

Adli kopya alma işlemi sırasında sabit disk içerisindeki okuma yazma kafası tüm sektörleri okumaya çalışırken sabit diske ait yazılım da bozuk olduğunu tespit ettiği bir sektörü G-List'e ekleyerek onun yerine başka bir sektörü kullanıma atayabilir. Böylelikle sabit disk kullanımı sırasında bozulduğu tespit edilen sektör bilgisi G-Liste eklenerek, yerine yenisi atandığından; bir sabit diskten adli kopya alınması sırasında hesaplanmış olan hash değeri, aynı sabit

---

[208] Sobey, C. H. (2004). *Recovering Unrecoverable Data.* A.B.D.: ChannelScience. s.6

[209] Shipley, T. G., & Door, B. (2012). *Forensic Imaging of Hard Disk Drives.* Nevada: U.S. Department of Justice. s.5

diskten tekrar adli kopya alındığında hesaplanan hash değeri ile uyuşmayabilir.

Adli kopyası alınarak hash bilgisi kaydedilen elektronik delil niteliğindeki bir sabit diskten bir süre sonra tekrar adli kopya alma işlemi yapıldığında hesaplanan hash değerleri birbirini tutmayabilmektedir. Bunun sebebi tamamen veya kısmen bozulduğu için okunamayan bir sektör olabildiği gibi daha önceden adli kopya alma işlemi sırasında okunamamış veya yanlış okunmuş ancak sonraki adli kopya alma işleminde doğru şekilde okunabilmiş bir sektörden de kaynaklanabilmektedir. Okumama veya eksik okuma sonucu hash değerlerinin uyuşmaması sorunu sadece sabit diskten de kaynaklanmıyor olabilir. Adli kopya almakta kullanılan bazı yazılımların veya donanımların okuyabildiği sektörleri diğer yazılım veya donanımlar aynı kararlılıkta okuyamayabilmektedir. Dolayısıyla daha önceden adli kopyası alınmış bir sabit diskin tekrar adli kopyası alındığında hesaplanan hash değerleri farklı olabilecektir.

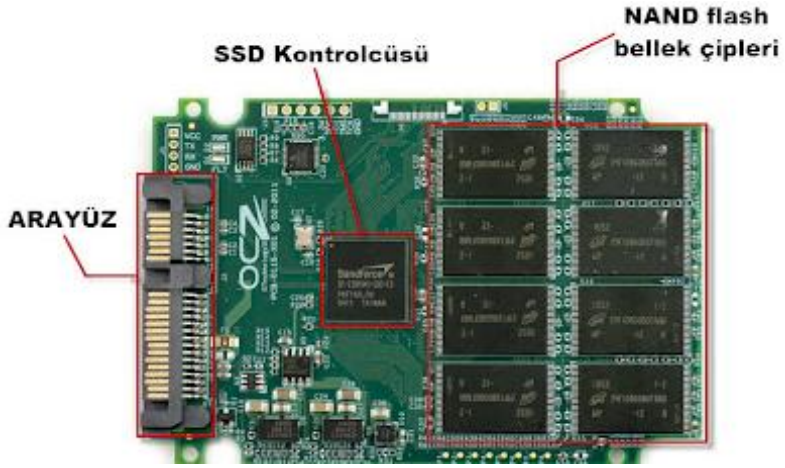
6.3. SSD disklerde hash problemleri

SSD(Solid State Drives) diskler yapısal özellikleri, kendisine bir anlamda ismini de vermiştir. SSD'lerde, diğer manyetik depolama ünitelerinden farklı olarak, herhangi bir hareket eden parça yoktur. Bu da onların Solid State, yani Katı Hal Sürücüsü olarak adlandırılmasına neden olmuştur[210]. Aşağıda Şekil 5.31'de farklı arayüz bağlantılarına ve farklı şekillere sahip SSD diskler görülmektedir.

[210] DUMAN, E. (2013, Nisan 07). *SOLIT STATE SÜRÜCÜLERİN ADLİ BİLİŞİM ALANINDA.* DUMAN HUKUK & DANIŞMANLIK: http://www.emrahduman.av.tr/makale/solitstate.pdf

Şekil 6.7 Çeşitli SSD diskler

Henüz kapasitelerinin düşük ve fiyatlarının yüksek olması sebebiyle yaygın olarak kullanılmasa da zaman ilerledikçe veri okuma/yazma yönünden daha hızlı, daha az enerji tüketimine sahip ve sarsıntı gibi dış etkenlere daha dayanıklı oldukları için daha çok tercih edileceklerdir. Bilgisayar üreticilerinin pazara sunduğu bilgisayarlarda daha yüksek performans için, kullanmayı daha çok tercih etmeye başlamalarına paralel olarak adli bilişim alanında da her geçen gün daha sık karşılaşılan SSD diskler, üzerlerinde bulunan Nand flash yongalarında veriyi depolamaktadır. Şekil 5.32'de SSD disk üzerindeki ana parçalar görülmektedir.



Şekil 6.8 SSD Disk parçaları[211]

SSD disklerin mekanik bir yapıda veri depolamaması ve okuma yazma işlemini sabit disklerdeki gibi hareketli parçalarla yapmamasından dolayı veriye erişim için beklenmesi gereken süre oldukça düşüktür. Sabit disklerde veriye erişmek için öncelikle veri yazılı plakaları döndüren motorun belirli bir hıza ulaşması gerekmekte ve daha sonra okuma/yazma kafası veri yazılı yüzeyi tarayarak okumaya başlamaktadır. SSD diskler ise mekanik tabanlı olmaması yani hareketli parça içermemesi ve flash bellek tabanlı elektronik tümleşik devrelerden

[211]http://4.bp.blogspot.com/-pG1GY9_mH68/UC6jY-HdALI/AAAAAAAAMD4/jwiFKNxlExc/s400/vertex-3-pcb-top.jpg

imal edilmesi, uygulamada pek çok faydayı da beraberinde getirmektedir. Öncelikle, okuma ve yazma işlemleri, sabit disklerdeki başlıkların yaptığı gibi mekanik olarak uygulanmadığı için, erişim süreleri oldukça düşüktür ve günümüzde 0.1 ms'ye kadar düşmüştür[212].

SSD diskler üzerinde veri depolama birimi olarak bulunan flash yongalar üzerine verinin nasıl kaydedileceğini veya silineceğini SSD kontrolcüsü düzenler. SSD disk ömrünü uzatmak ve performansı daha üst seviyelere ulaştırmak için veri flash yongalar üzerine ham olarak sırasıyla kaydedilmemekte, veri değişik algoritmalar kullanılarak ve farklı yongalara dağıtılarak kaydedilmektedir. Bu algoritmik ve dağınık kayıt biçimi diskten diske ve hatta modelden modele değişebilmektedir. SSD üreticileri performansı ve SSD disk ömrünü arttırmak için kullandıkları bu algoritmaları ticari sır niteliğinde olduğu için paylaşmamakta, dolayısıyla SSD disk teknolojisinde veri depolama şekillerinde standartlaşma olmamaktadır.

SSD disk üzerindeki flash yongalara okuma/yazma erişimlerinin tamamı SSD kontrolcüsü üzerinden gerçekleşmektedir. Sabit disklerde yazılabilir, okunabilir ve silinebilir en küçük birim 512byte iken SSD disklerde yazılabilir ve okunabilir en küçük birim 4KB büyüklüğündeki Page'lerden oluşurken; silinebilir en küçük birim ise 512KB büyüklüğündeki Blok'lardır. Page'ler Block'ların içerisinde yer alır. SSD diskler üzerinde veri sadece boş alanlara kaydedilmektedir. Daha önce veri kaydedilmiş ve silinmiş de olsa bir veri daha kaydedileceğinde, silindiği için boşalmış olan alana değil daha önce kullanılmamış olan veya daha az kullanılmış olan bir alana kaydedilir. Bunun sebebi ise SSD disklerdeki flash yongalarına maksimum veri yazma/okuma sayısının sabit disklere göre oldukça düşük olması ve dolayısıyla kullanım ömürlerinin sabit disklere göre kısa olmasıdır. SSD diskler kullanım ömrünü arttırmak için flash yongalar üzerinde mantıksal bir adresleme kullanırlar.

---

[212] Michael Wei, L. M. (2013, Nisan 09). *Reliably Erasing Data From Flash-Based Solid State Drives.* The Advanced Computer Systems Association: http://static.usenix.org/events/fast11/tech/full_papers/Wei.pdf

Kullanılan bu adresleme sisteminde mantıksal olarak tutulan adresler sürekli değişmektedir ancak bu değişimler kullanıcı ve işletim sistemi tarafından fark edilmemekte, bu işlem SSD kontrolcüsü tarafından yapılmaktadır. Mekanik yapıya sahip sabit disklerde bozulan sektör yerine kullanıma açılmak üzere ayrılmış sektörler mevcut iken SSD disklerde ise disk üzerinde yazılı veri depolama kapasitelerinin %25'ine kadar fazla veri depolanabilecek flash yongalara sahip olarak üretildikleri görülebilmektedir[213]. Mekanik yapıya sahip disklerde bulunan yedek sektörler üzerine, bozulan bir sektör yerine kullanıma açılmadıkça, veri kaydedilememekte ve o sektörlere erişilememektedir. SSD disklerde ise fazladan konulmuş flash yongalar mantıksal adreslemenin değişmesiyle sırası geldiğince kullanılmaktadır.

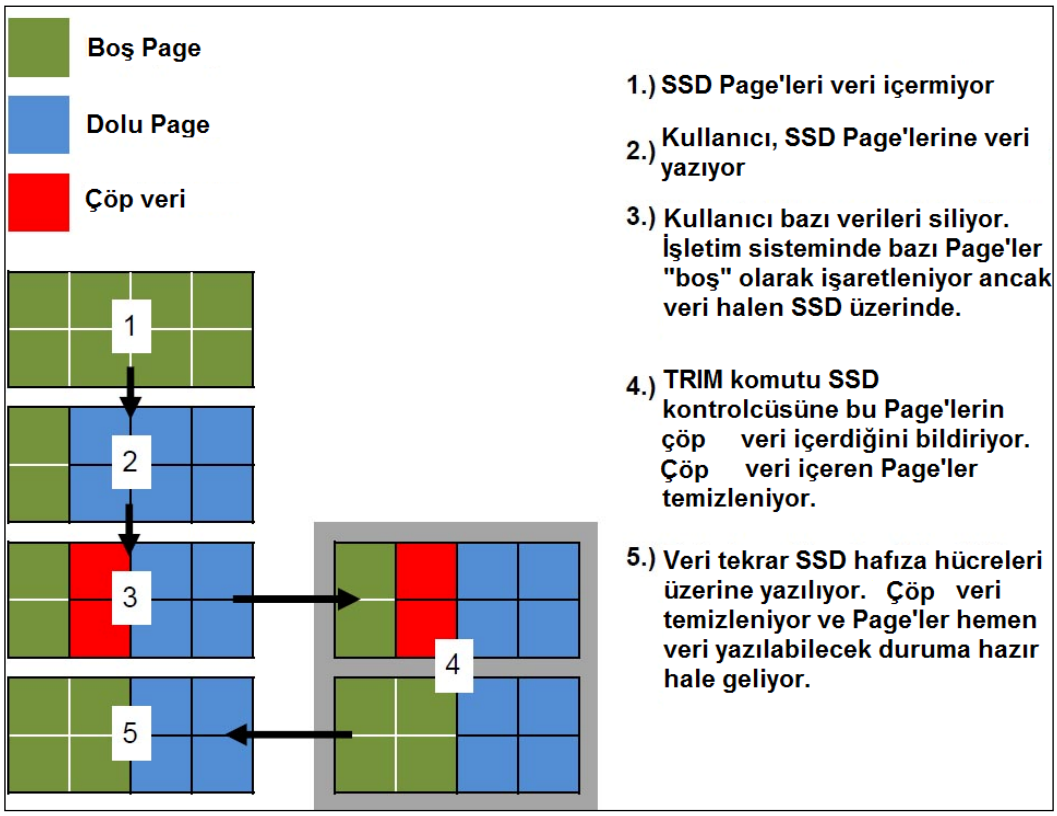
Bir yazma işlemi sırasında mantıksal adresleme içerisinde 100. Sırada olarak görülen bir sektör bir başka yazma işleminde 110. Sektör olarak adreslenebilmektedir.

Yeni nesil SSD disklerde TRIM desteği mevcuttur. "TRIM" bir SATA komutudur. TRIM komutunun kullanılabilmesi için hem işletim sisteminde hem de SSD diskte TRIM desteğinin bulunması gerekir. TRIM desteği olmaksızın bir silme işlemi yapıldığında işletim sistemi silinen dosyayı kendi haritasında silindi olarak işaretler ancak SSD diske ayrıca sil komutu göndermez. Sil komutu gönderilmediği için SSD üzerinde halen bulunan ancak gereksiz olan veri SSD disk üzerinde çalışan Garbage Collection adı verilen yazılım tarafından bir süre sonra tespit edilerek silinirken aynı zamanda defragmantasyon işlemi de yapılarak SSD disk üzerindeki veri bloklarının daha verimli kullanılması sağlanır. Ancak Garbage Collection tarafından gereksiz ve kullanılmayan verinin tespiti ve defragmantasyona tabi tutulması zaman alabilmektedir. TRIM teknolojisi aktif olan bir sistemde ise: işletim sisteminde yapılan silme işlemiyle ilgili olarak silinmiş olarak görünen alanlar işletim sistemi tarafından SSD kontrolcüsüne

---

[213] Michael Wei, L. M. (2013, Nisan 09). *Reliably Erasing Data From Flash-Based Solid State Drives.* The Advanced Computer Systems Association: http://static.usenix.org/events/fast11/tech/full_papers/Wei.pdf

bildirilir. SSD kontrolcüsü kendisine işletim sistemi tarafından silindiği bildirilen alanları çöp olarak işaretler. Daha sonra SSD diskin boşta olduğu zamanlarda çöp olarak işaretlenen alanlar Garbage Collection tarafından silinerek veri blokları düzenlenir. SSD kontrolcüsünü çöp olarak işaretlemesi ve Garbage Collection tarafından işaretlenen alanların silinmesi ve yeniden düzenlenerek bütün halinde Block'lara kaydedilmesi işlemlerinin tamamı işletim sistemi ve kullanıcı tarafından kontrol edilemeyecek bir yapı içerisinde gerçekleşmektedir. Yani eğer bir alan TRIM tarafından gönderilen komutla çöp olarak işaretlenmişse bu alan bir süre sonra geri getirilemeyecek şekilde silinecek ve ideal şekilde Block'lardaki veri düzenlenecektir. Bu işlemler yapılırken aynı zamanda mantıksal adreslemeler de değişebilmektedir. TRIM çalışma sistemi Şekil 5.33'te gösterilmiştir.



Şekil 6.9 TRIM çalışma sistemi[214]

Yazma korumalı olarak adli kopyası alınmak istenen bir SSD disk

[214] http://www.corsair.com/us/blog/how-to-check-that-trim-is-active/

üzerinde daha önce çöp olarak işaretlenmiş ancak henüz silinmemiş veriler olabilmektedir. Garbage Collection programı da çalışmaya devam etmektedir. Yazma koruma sadece işletim sistemi veya kullanıcı gibi dışarıdan diske veri yazılmasını/silinmesini engellemektedir. TRIM ve Garbage Collection sistemleri ise SSD içerisinde çalışan sistemlerdir. Donanımsal yazma koruması veya yazılımsal yazma koruması bu sistemlerin çalışmasını engellememektedir. Adli kopya alınması esnasında bu sistemler çalışmaya devam edeceğinden SSD disk üzerindeki verilerde değişiklikler olmaya devam etmektedir. İlk adli kopya alma işleminde çöp olarak işaretlenen ancak henüz Garbage Collection tarafından silinmediği için sektör üzerinde okunmuş olan bir veri aynı SSD diskten ikinci defa alınacak olan adli kopya üzerinde bulunmayabilmektedir. İki adli kopya alma işlemi süresince çalışmakta olan SSD disk üzerindeki sistemler önceden çöp olarak işaretlenmiş olan alanlarda değişiklikler yapmaya devam etmektedir. Dolayısıyla ilk adli kopya sonucu hesaplanan hash değeri ile ikinci adli kopya işlemi sonucu hesaplanan hash değeri farklı olacaktır.

6.4. Uygulama

Adli bilişim alanında adli kopya ile ilgili uygulamalarda elektronik delillerin orijinali üzerinde tekrar adli kopya alma işlemleri yapılmakta ve sonucunda hesaplanan hash değeri ilk adli kopya alma işleminde hesaplanmış olan hash değeri ile karşılaştırılarak farklılık görüldüğünde elektronik aygıtın delil niteliği kalmadığı değerlendirilmektedir. Bunun yanında açık olan sistemlerden alınan adli kopyalarla ilgili olarak, RAM'lerden alınan adli kopyalarla ilgili olarak ve cep telefonlarından alınan adli kopyalarla ilgili olarak tekrar adli kopya alınması ve hash değerlerinin kıyaslanması gibi bir uygulama söz konusu değildir. Çünkü açık olan sistemler, RAM'ler ve cep telefonları üzerinde kayıtlı olan verilerin adli kopyaları alınırken sistem çalışmaya devam ettiği için, halen sistem tarafından zararsız ufak değişiklikler yapılmakta olduğu bilindiğinden; tekrar bir adli kopya alındığında aynı hash değeri elde edilemeyeceği bilindiğinden, böyle bir tehid yoluna başvurulmamaktadır. Bu sistemlerden alınan ve elde olan ilk adli

kopyalar üzerinden tüm inceleme ve değerlendirmeler yapılmakta, orijinal elektronik delil üzerinde tekrar hash hesaplatılması gibi bir işlem yapılmadan adli kopya delil olarak olayın aydınlatılmasında kullanılmaktadır.

CD-DVD gibi optik diskler, mekanik bir yapıya sahip olan sabit diskler ve katı hal diski olarak adlandırılan SSD disklerde de çeşitli sebeplerden dolayı hash problemleri yaşanabilmekte olduğu görülmektedir. Uygulamada, delil olabilecek elektronik aygıt üzerinden adli kopya alındığı sırada hesaplanan hash değeri ile, alınan adli kopyanın kaydedildiği veri depolama birimi üzerine tam ve doğru olarak kaydedildiğinin tespiti için hesaplanan hash değerleri birbiri ile aynı ise bu aşamadan sonra ilerleyen zamanda delil bütünlüğünün korunup korunmadığının kontrolü için elektronik delilin orijinali üzerinde tekrar adli kopya alma işlemi yapılması gerekmemekte, bu kontrolün eldeki adli kopya üzerinde hash hesaplatılarak yapılması gerekmektedir. Orijinal elektronik delil üzerinde meydana gelen bozulmalar ve değişimler hukuksal açıdan delil bütünlüğünün bozulduğuna anlamına gelmemelidir. Çalışan sistemlerden, RAM'lerden ve cep telefonlarından alınan adli kopyalarda olduğu gibi; diğer elektronik deliller de sadece adli kopyaları üzerinden değerlendirilmelidirler. Elektronik delil üzerinde herhangi bir veri değişikliği olup olmadığı ise orijinal delil üzerinden tekrar adli kopya alınarak ve orijinal delilin hash değeri hesaplatılarak değil, eldeki adli kopya üzerinde tekrar hash hesaplatılarak kontrol edilmelidir. Daha önceden orijinal delilden adli kopya alınırken hesaplanan hash değeri, adli kopya üzerinden tekrar hesaplatılan hash değeri ile birbirini tutuyor ise delil bütünlüğü korunuyor anlamına gelmektedir. Bu aşamada veri bütünlüğünün kontrolü için orijinal delil üzerinde tekrar hash hesaplatılması gibi bir yol izlenmemelidir.

7. Sonuç

Teknolojinin hayatımızın birçok alanında vazgeçilmez bir parça haline geldiği günümüzde, insanlığın ortaya çıkışından bu yana insan olmanın getirdiği

“suç” unsuru da artık içerisinde bilişimden izler bulunan veya tamamen bilişim üzerinden işlenmiş hallerde karşımıza çıkmaktadır. Bilişim aygıtlarının varlığının bulunduğu bir olayda adli bilişim incelenmesi gerekmektedir.

Bu tez çalışmasında Adli Bilişimde e-delillerin toplanması ve incelenmesi süreci teknik boyut ve hukuki dayanak yönlerinden ele alınmıştır. Teknik yönden, ilk müdahale öncesi hazırlık aşamasından başlayarak, raporlandırma aşamasını kapsayan süreç boyunca dünyada standart haline gelmiş olan genel geçerli bilgiler verilerek, bazı özel konularda da dikkat edilmesi gereken hususlara değilmiştir. Dünya üzerinde genel olarak kullanımı yaygın olan ve adli bilişim alanında yeterli kararlılıkta çalışabildikleri için sıkça tercih edilen ve standartlaşmış olan yazılımlar ve donanımlar hakkında detaylı teknik bilgiler verilmiştir. Adli bilişim teknik uygulamaları esnasında karşılaşılan hash problemleri ele alınmıştır. Hukuki dayanak olarak adli bilişim uygulamalarıyla doğrudan ilgili kanun maddeleri ve adli bilişim uygulamalarına başvurulan diğer suçlarla ilgili olan kanun maddeleri ele alınmıştır.

Sonuç olarak; adli bilişimde ilk müdahale, e-delillere zarar vermeden, yeterli teknik bilgiye sahip olan personel tarafından veya yeterli teknik bilgiye sahip personelin yönlendirmeleri doğrultusunda diğer görevliler tarafından yapılmalıdır. Dolaysıyla mutlak ihtiyaç duyulacak olan ilk müdahale yapabilecek bilgi ve tecrübeye sahip yeterince personelin olabilmesi için, adli bilişim ile ilgili ilk müdahale eğitimleri verilmelidir. Adli Bilişim Uzmanlığı sertifikasyonlarının standartları belirlenmeli ve incelemelerin sadece Adli Bilişim Uzmanları tarafından yapılması sağlanmalıdır.

Üniversitelerde adli bilişimin her aşamasıyla ilgili çalışmalar yapılmalı, bu çalışmalar adli bilişim ilk müdahale personelleri ve inceleme personelleri ile irtibat halinde devam ettirilerek, ihtiyaca yönelik gelişmeler sağlanmalıdır. Adli bilişim donanım ve yazılımlarının maliyetlerinin yüksek olması sebebiyle, üniversitelerle işbirliği içerisinde, ihtiyaca karşılık verecek yeteneklere sahip olabilecek özelliklerde ve belirlenen standartları karşılayabilecek donanım ve yazılımlar üretilerek ülke kaynaklarının yurtiçinde kalması ve adli bilişim konusunda uzmanların yetişmesi sağlanmalıdır.

Adliyelerde adli bilişim alanında danışmanlık ve/veya inceleme faaliyetleri sürdüren Adli Bilişim Uzmanı olan personel bulundurulmalıdır.

Adli bilişim incelemeleri gerekli eğitimleri almış ve yeterli tecrübesi olan Adli Bilişim Uzmanlarına yaptırılmalıdır. İlk müdahale personelleri ve adli bilişim incelemelerini yapacak olan adli bilişim uzmanları sadece teknik bilgi içerikli eğitimden geçirilmemeli, bunun yanında hukuki mevzuat hakkında da detaylı bilgi sahibi olmalıdırlar. Sadece teknik bilgiye sahip olunması veya sadece hukuki mevzuata hakim olunması adli bilişim konusunda yeterli olmamaktadır. Hukukçuların adli bilişim konularında bilgi sahibi olmasının gerekliliği her geçen gün, bilişim sistemlerinin kullanımlarının artmasıyla orantılı olarak, artacaktır.

Ülkemizde adli bilişim ile ilgili olarak yürürlükte olan kanun maddelerinin adli bilişim uygulamalarının gerisinde kaldığı ve uygulamalara yeterince cevap veremediği görülmektedir. Adli bilişim çalışmalarının masraflı olması, uzun zaman harcamak gerekliliği göz önünde tutularak; adli bilişim incelemesinin gerekip gerekmediği konusunda doğru bir karar verilebilmesi için gerekli ölçütlerin belirlenmesi ve çerçevenin oluşturulması gerekmektedir. Adli bilişim ile ilgili kanun maddelerinin güncellenmesi ve ihtiyaca cevap verecek niteliklere sahip olması sağlanmalıdır.

Adli bilişim aşamaları ve bu aşamalarda kullanılmakta olan yazılım ve donanımlar ile ilgili olarak standartlar belirlenmeli ve belirlenen standartlara uygunluk kontrolleri yapılarak adli bilişim sürecinin ev adli bilişimde kullanılan donanım ve yazılımların ülkemizde standartlaşması sağlanmalıdır.