MOBILE FORENSICS

Mesut UKŞAL
112692044

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

Yrd. Dç. Dr. Leyla KESER BERBER

2015

MOBİL CİHAZLARDA ADLİ BİLİŞİM

MOBİLE FORENSICS

MESUT UKŞAL
112692044

Yar. Doç. Dr. Leyla BERBER KESER	:
Yar. Doç. Dr. Mehmet Bedii KAYA	:
Dr. Bülent ÖZEL	:
Tezin Onaylandığı Tarih	:
Toplam Sayfa Sayısı	: 145

Anahtar Kelimeler	**Keywords**
a) Mobil Dünya	a) Mobil World
b) Dijital Adli Analiz	b) Digital foerensics
c) Akıllı Telefon	c) Smart Phones
d) Mobil uygulama	d) Mobile Application
e) Mobil adli Analiz	e) Mobile Forensics
f) Kanıt	f) Evidence
g) Akıllı Telefon Analizi	g) Smart Phone Forensics

MOBİLE FORENSICS

TEZİ HAZIRLAYAN: Mesut UKŞAL

ÖZET

Bilişim teknolojileri dünyasında yaşanan gelişmeler yaşantımıza birçok kolaylık sunmuş olmasına rağmen güvenlik ihtiyacını ve ahlaki, sosyal sorumlulukları da beraberinde getirmiştir. Özellikle mobil teknoloji alanındaki gelişmelere paralel olarak akıllı telefon kullanımının yaygınlaşması, akıllı telefonlar üzerinden işlenen bilişim suçlarının artmasına sebep olmuştur. Bilişim suçlarının akıllı telefonlar üzerinden işlenmesindeki artış ise bu konudaki bilişim suçlarının incelenmesi gerekliliğini doğurmuş ve birçok analiz yazılımları/metotları üretilmiştir, adli bilişim suçları alanında akıllı telefon ve cep telefonlarının incelenmesi alt başlığı oluşmuş, yalnızca bu konuyu inceleyen uzmanlık alanları doğmuştur. Bu çalışmada akıllı telefonların adli bilişim kapsamında incelenmesi ile ilgili önemli detaylar çeşitli telefon, yazılım, uygulama ve çalışmalar karşılaştırılarak anlatılmıştır.

Presented by: MESUT UKŞAL

ABSTRACT

The advancements in Information Technology presents comfort in our daily lives. On the other hand these advancements brings with it the need for security and social responsibilities. Especially in parallel with these advancements, proliferation of smart-phone usage increased the Information Technology Crimes committed using smart-phones. The increase in the Information Technology Crimes created the need for investigation of such crimes and many different analysis techniques/devices have been developed for fighting against them. In addition, Forensic Investigation of Smart-Phones became an area under Forensic Investigation and an expertise called “Smart-Phone Forensic Investigation” is born. In this study, the Smart-Phone Forensic Investigation has been explored by delving into the details of several smart-phones, forensic application/software and studies.

İÇİNDEKİLER

İÇİNDEKİLER **4**

KISALTMALAR **6**

KAYNAKÇA / ELEKTRONİK AĞ ADRESLERİ **9**

ŞEKİLLER LİSTESİ **15**

TABLOLAR **17**

1. GİRİŞ **1**

A. AMAÇ 2

2. ADLİ BİLİŞİMİN TANIMI VE SAFHALARI **2**

A. ADLİ BİLİŞİM KAVRAMI VE BİLİŞİM SUÇLARI 2

1. Bilişim Kavramı *2*

2. Bilişim Suçu Kavramı *2*

3. Adli Bilişim Kavramı *3*

B. ADLİ BİLİŞİM SAFHALARI 5

1. Delil Toplama (Acquisition/Collection) *7*

2. İnceleme/Tanımlama (Identification /Examination) *9*

3. Çözümleme/Değerlendirme (Evaluation/Analysis) *10*

4. Raporlama/Sunum (Reporting/Presantation) *10*

3. MOBİL CİHAZLAR VE GSM TEKNOLOJİSİ **11**

A. MOBİL GSM TARİHİ 11

B. MOBİL CİHAZ DONANIM VE İŞLETİM SİSTEMLERİ 15

1. Mobil Cihaz Donanım Yapısı *15*

2. Mobil Cihaz İşletim Sistemleri *24*

4. MOBİL CİHAZLARDA GÜVENLİK HUSUSLARI **31**

A. MOBİL CİHAZLAR VE GÜVENLİK 32

B. MOBİL CİHAZLARDA GÜVENLİK TEHDİTLERİ 34

1. Kötücül Yazılımlar (Malware) *35*

2. Doğrudan Saldırı (Direct Attacts) *37*

3. Veri iletişimi Dinleme (Data İnterception) *39*

4. Sosyal Mühendislik ve İstismar (SocialEngineering&Exploitation) *40*

C. MOBİL CİHAZLARDA İNCELEME YAPMANIN ZORLUKLARI 41

5. MOBİL ADLİ BİLİŞİM YAZILIM/DONANIMLARININ GENEL ÖZELLİKLERİ **43**

A. ÜCRETSİZ ADLİ BİLİŞİM YAZILIM VE DONANIMLARI 43

1. Caine *43*

2. Deft *44*

3. Bitpim *44*

4. Osaf "Open Source Android Forensics" *45*

5. Pilot-Link *45*

6. TULP 2G *45*

B. ÜCRETLİ ADLİ BİLİŞİM YAZILIM VE DONANIMLARI 46

1. Cellebrite *46*

2. XRY *46*

3. Tarantula *47*

4. Mobiledit *48*

5. Faraday *48*

6. Paraben's Device Seizure *49*
7. Oxygen Forensics Suite *50*
8. EnCase Neutrino *50*
9. Flasher box *51*

6. MOBİL CİHAZLARDA ADLİ BİLİŞİM SAFHALARI 51

A. CEP TELEFONUNDAN DELİL ÇIKARTMA SÜRECİ 53
B. DELİL TOPLAMA "EVİDENCE INTAKE COLLECTİON" SAFHASI 54
1. Veri Alanları *55*
2. Dâhili Hafıza *56*
3. Hafıza Kartında Bulunabilecek Veriler *57*
4. Sim Kart Verileri *58*
C. TANIMLAMA (IDENTİFİCATİON) SAFHASI 58
1. Adli Makam/Yasal Merci *59*
2. İnceleme Amacı *60*
3. Cihazın Tanımlanması *61*
4. CDMA Cep Telefonları *62*
5. GSM Cep Telefonları *62*
6. Çıkarılabilir Hafıza *63*
D. HAZIRLIK (PREPARATİON) SAFHASI 63
1. Uygun Araçların Seçimi ve kapasiteleri *64*
2. Obje Çıkarımı *64*
3. Mantıksal Çıkarım *64*
4. Fiziksel Çıkarım *65*
5. Cihaz Analiz Seviyeleri *65*
E. İZOLASYON (ISOLATİON) SAFHASI 66
F. İŞLEM (PROCESSİNG) SAFHASI 67
G. DOĞRULAMA (VERİFİCATİON) SAFHASI 68
1. Çıkartılan Verinin Telefondaki veri ile Karşılaştırılması *69*
2. Birden Fazla Araç Kullanılarak Sonuçların Karşılaştırılması *69*
H. BELGELENDİRME/RAPORLAMA (DOCUMENTATİON/REPORTİNG) SAFHASI 70
1. Saat Dilimi Ayarları *70*
İ. SUNUM/ARŞİV (PRESENTATİON/ARCHİVİNG) SAFHASI 71

7. MOBİL CİHAZLARIN ADLİ BİLİŞİM YAZILIMLARI İLE ANALİZ EDİLMESİ (ÖRNEK CİHAZ İNCELEMELERİ) 73

A. ARAŞTIRMA METODOLOJİSİ 73
1. Mantıksal İmaj *73*
2. Fiziksel İmaj *73*
3. Test Ortamı ve Gereksinimler *73*
4. Analizler Esnasında Yaşanan Sıkıntılar *79*
5. Rooting and Jailbreaking *79*
6. Senaryo *79*
B. ARAŞTIRMALAR (ÖRNEK SIM, DÂHİLİ/HARİCİ HAFIZA VE UYGULAMA ANALİZLERİ) 80
1. XRY Analizleri *80*
2. MobilEdit Analizleri *92*
3. OXYGEN Suite Analizleri *107*
C. ARAŞTIRMA BULGULARI 118

8. SONUÇ, YORUM VE ÖNERİLER 121

KISALTMALAR

PHONE Mobile phone or device

HASH The fixed-size value, or “digital fingerprint” produced by a

BOME Bilgisayar Olaylarına Müdahale Ekibi

TCK Türk Ceza Kanunu

API Application process Interface

GNU General Public License

AP Application processor

BP Baseband Processor

OP Open source Açık Kaynak

CDMA Code Division Multiple Access

CDR Call Detail Record

CF Compact Flash

CNIC Cellular Network Isolation Card

CSIM Subscriber Identity Module

EDGE Enhanced Data for GSM Evolution

EMS Enhanced Messaging Service

ESN Electronic Serial Number

ETSI European Telecommunications Standards Institute

eUICC Embedded Universal Integrated Circuit Card

FCC ID Federal Communications Commission Identification Number

GPRS General Packet Radio Service

GPS Global Positioning System

GSM Global System for Mobile Communications

http HyperText Transfer Protocol

ICCID Integrated Circuit Card Identification

IDE Integrated Drive Electronics

iDEN Integrated Digital Enhanced Network

IM	Instant Messaging
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IrDA	Infra Red Data Association
JTAG	Joint Test Action Group
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LND	Last Numbers Dialed
MD5	Message Digest 5
MEID	Mobile Equipment Identifier
MMC	Multi-Media Card
MMS	Multimedia Messaging Service
MSC	Mobile Switching Center
MSISDN	Mobile Subscriber Integrated Services Digital Network
NFC	Near Field Communication
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
PIM	Personal Information Management
PIN	Personal Identification Number
PPI	Pixels Per Inch
POP	Post Office Protocol
RAM	Random Access Memory
ROM	Read Only Memory
SD	Secure Digital
SDK	Software Development Kit
SHA1	Secure Hash Algorithm, version 1

SHA2	Secure Hash Algorithm, version 2
SIM	Subscriber Identity Module
SMS	Short Message Service
SSD	Solid State Drive
TDMA	Time Division Multiple Access
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System

KAYNAKÇA / ELEKTRONİK AĞ ADRESLERİ

Ekim Ahmet : Ahmet EKİM, Mobil Cihazlarda adli Bilişim ve Malware Analizi, http://www.bilgisayardedektifi.com/mobil-cihazlarda-adli-bilisim-ve-malware-analizi/206,

Paul McCarty Paul McCarthy, School of Computer and Information Science Mawson Lakes Forensic Analysis of Mobile Phones October 2005 s.3 http://www.8051projects.net/files/public/1236046309_9698_FT19075_forensic_analysis_of_mobile_phones.pdf,

İnternet : TDK "Güncel Türkçe Sözlük" www.tdk.gov.tr,

İnternet : Bilişim Suçları Kapsamında Dijital Deliller, http://ab.org.tr/ab05/tammetin/134.pdf/

İnternet : İstanbul Barosu Dergisi Sayı: "Bilişim Suçu" Mart-Nisan 2014 http://www.istanbulbarosu.org.tr/proje/dergi/19/files/assets/basic-html/page241.html

Dülger : DÜLGER, Murat Volkan. "Turk Ceza Kanunu'nda Yer Alan Bilisim Sucları ve Elestirisi" http://www.dulger.av.tr/pdf/ytkbilisimsucelestrisi.pdf

Berber : Keser Berber, Adli Bilişim, CMK md 134 ve Düşündürdükler, http://www.leylakeser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html 17/05/2014

İnternet : Interpol Computer Crime Manuel 2. Officer, İnterpol, s.10

Uzunay : UZUNAY, Yusuf; BICAKCI, Kemal. A3D3M: Açik Anahtar Altyapisi DESTEKLI DIGITAL Delilleri Doğrulama Modeli http://www.emo.org.tr/ekler/4843973f9b66701_ek.pdf./

Casey : Casey, E. (200s4). Digital Evidence and Computer Crime: Forensic Science, Computers,and the Internet, 2nd Ed., Academic Press. http://www.google.com.tr/books?hl=tr&lr=&id=DQdWRitMcyAC&oi=fnd&pg=PP2&dq=Digital+Evidence+and+Computer+Crime&ots=t4uH0Y4WsI&sig=TLAsvz-Vh3k7pOTQmUVzyWBOKJE&redir_esc=y#v=onepage&q=Digital%20Evidence%20and%20Computer%20Crime&f=false

Hüseyin Çakır Ercan SERT : Hüseyin ÇAKIR / Ercan SERT, Bilişim Suçlarını Delillendirme Süreçi http://utsam.org/images/upload/attachment/utsas_2010_secilmis/Bili%C5%9Fim%20Su%C3%A7lar%C4%B1%20ve%20Delillendirme%20S%C3%BCreci.pdf/

Keser Berber : KESER BERBER, L.(2004). Adli Bilisim. Ankara, Yetkin Yayınları, s.:56-60 ISBN 975-464-299-0

Ekizer : Ekizer, A. H. (2014). Adli Bilişim - Computer Forensics, http://www.ekizer.net/adli-bilisim-computer-forensics/ (Et: 18.09.2014)

İnternet : Adli Bilişim, http://edirnebarosu.org.tr/incelemeler/adli-bilisim-computer-forensic/

İnternet : http://www.hukuksokagi.com/kaynak/adli-bilisim-computer-forensic/

Yusoff,Yunus,Ismail,Roslan,Hassan : YUSOFF, Yunus; ISMAIL, Roslan; HASSAN, Zainuddin. Common phases of computer forensics investigation models. International Journal of Computer Science & Information Technology, 2011, 3.3: 17-31.

http://airccse.org/journal/jcsit/0611csit02.pdf

İnternet : Ekizer, http://www.ekizer.net/adli-bilisim-computer-forensics/

Saudi-Madihah Mohd : SAUDI, Madihah Mohd. An overview of disk imaging tool in computer forensics. *SANS Institute*, 2001. http://www.sans.org/reading-room/whitepapers/incident/overview-disk-imaging-tool-computer-forensics-643

Casey,Eoghan : CASEY, Eoghan; TURNBULL, Benjamin. Digital evidence on mobile devices. *Eoghan Casey, Digital Evidence and Computer Crime. Third Edition. Forensic Science, Computers, and the Internet, Academic Pres*, 2011. http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf

Kruger : Kruger, 2011). Krueger, C. (2011, February 11). Man found guilty of lesser charge in murder recorded on cellphone http://www.tampabay.com/news/courts/criminal/man-found-guilty-of-lesser-charge-in-murder-recorded-on-cell-phone/1150957

Cas,Eoghan : CASEY, Eoghan. *Handbook of digital forensics and investigation*. Academic Press, 2009. http://www.google.com.tr/books?hl=tr&lr=&id=xNjsDprqtUYC&oi=fnd&pg=PP2&dq=van+der+Knijff,+Handbook+of+Digital+Forensics+and+Investigation+2009%3B+&ots=X2tNE-aCtL&sig=4yZF_a2v_D1AQfl8OHC5QGabw2c&redir_esc=y#v=onepage&q=van%20der%20Knijff%2C%20Handbook%20of%20Digital%20Forensics%20and%20Investigation%202009%3B&f=false

Nist : National Institute of Standards and Technology. "Guidelines on Cell Phone and PDA Security (SP 800-124)." http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

Symantec : Symantec. "Symantec Report Finds Cyber Threats Skyrocket in Volume andSophistication." http://www.symantec.com/about/news/release/article.jsp?prid=20110404_03

Hassell,Lewis : HASSELL, Lewis; WIEDENBECK, Susan. Human factors and information security. *Manuscript. Available at: http://repository. binus. ac. id/content A*, 2004, 334. http://repository.binus.ac.id/content/A0334/A033461622.pdf

Huang,Ding-Long-Rau-Pei-Luin Patrick : HUANG, Ding-Long; RAU, Pei-Luen Patrick; SALVENDY, Gavriel. A survey of factors influencing people's perception of information security. In: *Human-Computer Interaction. HCI Applications and Services*. Springer Berlin Heidelberg, 2007. p. 906-915. https://books.google.com.tr/books?id=BVy5BQAAQBAJ&pg=PA107&dq=Human-Computer+Interaction.+HCI+Applications+and+Services&hl=tr&sa=X&ei=UxshVYKTJ4X5UtaOg6AH&ved=0CB4Q6AEwAQ#v=onepage&q=Human-Computer%20Interaction.%20HCI%20Applications%20and%20Services&f=false

İnternet : https://www.bilgiguvenligi.gov.tr/mobil-cihaz-guvenligi/mobil-cihazlarda-guvenlik-android-ve-ios-karsilastirmasi.html

Juniper Networks : Juniper Networks, 2011, Inc. Mobile Device Security Emerging Threats, Essential Strategies http://www.adtechglobal.com/Data/Sites/1/marketing/juniperwhitepapermobiledevicesecurity.pdf

İnternet : Mobile Malware Evolution: An Overview,Part1" http://www.viruslist.com/en/analysis?pubid=200119916

Sağıroğlu, Şeref Bulut, Hülya : SAĞIROĞLU, Şeref; BULUT, Hülya. Mobil Ortamlarda Bilgi Ve Haberleşme Güvenliği Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, 2009, 24.3 s:501-505 http://www.mmfdergi.gazi.edu.tr/article/viewFile/1061000183/1061000154

İnternet : https://www.usom.gov.tr/dosya/1418807372-USOM-SGFF-004-Akilli%20Telefonlar%20ve%20Guvenlik.pdf/

İnternet : https://www.bilgiguvenligi.gov.tr/mobil-cihaz-guvenligi/mobil-cihazlarda-guvenlik-android-ve-ios-karsilastirmasi.html

İnternet : SMS DOS attack on cellular networks", http://www.kenneyjacob.com/2007/08/23/sms-dos-attack-on-cellular-networks/

İnternet : http://www.techopedia.com/definition/5045/bluejacking

İnternet : http://en.wikipedia.org/wiki/Bluesnarfing

İnternet : The Bluetooth Spam FAQ", http://www.mulliner.org/bluetooth/bluespamfaq.php

İnternet : Bluebug, http://trifinite.org/trifinite_stuff_bluebug

Marks, Lary : MARKS, Larry. Blackjacking: Security Threats to Blackberry Devices, PDAs and Cell Phones in the Enterprise, by Hoffman, Daniel V. New York: Wiley, 2007, 292p.ISBN 978-0-470-12754-4. Information Security Journal: A Global Perspective, 2012, 21.6: 355-356. https://books.google.com.tr/books?id=vRpRNp37xngC&pg=PA3&dq=Understanding+the+threats%E2%80%9DBlackjacking,+ch.1,&hl=tr&sa=X&ei=fyIhVeSpCInZU4DVgNgM&ved=0CBIQ6AEwAA#v=onepage&q=Understanding%20the%20threats%E2%80%9DBlackjacking%2C%20ch.1%2C&f=false

İnternet : https://www.bilgiguvenligi.gov.tr/mobil-cihaz-guvenligi/mobil-cihazlarda-guvenlik-android-ve-ios-karsilastirmasi.html

İnternet : http://www.wi-fi.org/news_articles.php?f=media_news&news_id=969

İnternet : http://threatcenter.smobilesystems.com/?p=1587

İnternet : http://www.cyberbullying.us/research.php/

Sun j-Howie D-Koiviso A-Sauvola J : Sun J, Howie D, Koivisto A & Sauvola J "A hierarchical framework model of mobile security." Proc. 12th IEEE International Symposium on Personal, Indoor and Mobile Radio Communication, San Diego, CA, 2001. http://www.mediateam.oulu.fi/publications/pdf/76.pdf

Jones A. : Jones, A. (2008, January 21–23). Keynote speech. In: First International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia, Adelaide, Australia. http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf

Ayes, Rick-Brothers, Sam, Jansen : AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. Guidelines on Mobile Device Forensics (Draft). NIST Special Publication, 2013, 800: 101. http://www.engistudio.it/wordpress/wp-content/uploads/NIST.SP_.800-101r1.pdf/

İnternet : http://tr.wikipedia.org/wiki/GSM/

İnternet : http://www.teknokulis.com/Yazarlar/hasan_genc/2011/06/30/gsmden-ilk-alonun-uzerinden-20-yil-gecti

İnternet : http://tr.wikipedia.org/wiki/GSM

İnternet : http://www.elektrikport.com/teknik-kutuphane/gsm-nasil-calisir-1-bolum/10192#ad-image-1

İnternet : http://tr.wikipedia.org/wiki/Plmn

İnternet : ETSI TR 102 216". Retrieved 25 June 2014 http://www.etsi.org/deliver/etsi_tr/102200_102299/102216/03.00.00_60/tr_102216v030000p.pdf

İnternet : http://tr.wikipedia.org/wiki/SIM_kart/

İnternet : http://en.wikipedia.org/wiki/Universal_Integrated_Circuit_Card

İnternet : http://blogs.strategyanalytics.com/WSS/post/2014/07/30/Android-Captured-Record-85-Percent-Share-of-Global-Smartphone-Shipments-in-Q2-2014.aspx

İnternet : http://www.log.com.tr/mobil-isletim-sistemlerinin-2013-kullanim-oranlari-yayinlandi

İnternet : Android Inc. (n.d.). *What is Android|Android Developers*. Retrieved May 23, 2010, from Android Developers: http://developer.android.com/guide/basics/what-isandroid.html

İnternet : https://gelecegiyazanlar.turkcell.com.tr/konu/android/egitim/android-201/android-mimarisi-ve-sistem-ozellikleri

İnternet : Apple Inc(n.d) *iPhone Technologies Overview*.Retrieved May 22,2010,from iPhone Referenceibrary:http://developer.apple.com/iphone/library/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/iPhoneOSTechnologies/iPhoneOSTechnologies.html#//apple_ref/doc/uid/TP40007898-CH3-SW1

İnternet : https://developer.apple.com/library/ios/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/Introduction/Introduction.html

Topgül : http://www.oguzhantopgul.com/2014/01/guvenlik-arastrmalar-odakl-ios-temelleri.html

Patterson : Patterson, D. (2004). eForensic Solutions: Cell Site Analysis. Latency lags bandwith, Communications of the ACM, (pp. v.47 n.10, p.71-75,). http://www.caine-live.net/ Et:24.12.2014

İnternet : http://www.deftlinux.net/deft-manual/

İnternet : http://www.concise-courses.com/security/mobile-forensics-tools/

İnternet : https://www.nowsecure.com/blog/2010/02/25/viaforensics-announces-release-android-forensics-application/

İnternet : Additional information on pilot-link can be found at: http://www.pilot-link.org

İnternet : http://www.forensicswiki.org/wiki/Cellebrite_UFED

İnternet	:	http://www.cellebriteusa.com/images/stories/brochures/UFED-Booklet-New-Format-Web_June_2013_v2.pdf
Rick Ayer-Wayne Jansen	:	Rick Ayers - Wayne Jansen - Ludovic Moenner - Aurelien Delaitre,*Cell Phone Forensic Tools: An Overview and Analysis Update*,(2007), National Institute of Standards and Technology http://csrc.nist.gov/publications/nistir/nistir-7387.pdf
Paraben Corporation	:	Paraben Corporation. (n.d.). Device Seizure. Retrieved May 29, 2010, from Paraben Corporation http://www.parabenforensics.com/device-seizure.htm
Oxygen Forensics	:	Oxygen Forensic . (n.d.). Oxygen Forensic Suite 2010. Retrieved May 15, 2010, from Oxygen Forensic: http://www.oxygen-forensic.com/
EnCase Neutrino	:	Guidance Software. (n.d.). *EnCase Neutrino.* Retrieved May 28, 2010, from Guidance Software: http://www.guidancesoftware.com/product.aspx?B=Product &Product_S=AccordianTwo&menu_id=117&id=348&terms=mobile+devices
Meyers,matthew,Rogers Marc	:	MEYERS, Matthew; ROGERS, Marc. Computer forensics: the need for standardization and certification. *International Journal of Digital Evidence*, 2004, 3.2: 1-11 http://www.slideshare.net/lisajarrett1972/computer-forensics-35134495
Murphy, Cynthia	:	Murphy, Cynthia. "Cellular Phone Evidence Data Extraction and Documentation". Retrieved 4 August 2013. https://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf
İnternet	:	http://www.theosecurity.com/pdf/Fiorillo.pdf
Somasheker Akkaladevi	:	Somasheker Akkaladevi Virginia State University Department of Computer Information Systems Petersburg, Virginia 23806, USA efficient forensic tools for handheld devices: a comprehensive perspective http://www.swdsi.org/swdsi08/paper/SWDSI%20Proceedings%20Paper%20S406.pdf
Mellars	:	Mellars, B. (2004). Forensic Examination of Moblie Phones. Digital Investigation. The International Journal of Digital Forensics & Incident Response , 1(4), 266-272.
İnternet	:	https://www.packtpub.com/books/content/introduction-mobile-forensics/
İnternet	:	https://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf
Wikipedia	:	‘‘Vikipedi Özgür Ansiklopedi’’, 2014 http://en.wikipedia.org/wiki/Electronic_serial_number
Murphy, Cynthia	:	Murphy, Cynthia. "Cellular Phone Evidence Data Extraction and Documentation". Retrieved 4 August 2013. https://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf
Wikipedia	:	‘‘Vikipedi Özgür Ansiklopedi’’, 2014 http://en.wikipedia.org/wiki/Mobile_identification_number
Wikipedia	:	‘‘Vikipedi Özgür Ansiklopedi’’, 2014 http://tr.wikipedia.org/wiki/IMEI

Wikipedia : Ramabhadran, Anup. Forensic İnvestigaiton process model for Windows mobile devices .s—16 http://www.forensicsfocus.com/download/windows-mobile-forensics-process-model.pdf

Murph, Cynthia : Murphy, Cynthia. "Cellular Phone Evidence Data Extraction and Documentation". Retrieved 4 August 2013. https://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf

Katz, Eric : KATZ, Eric. A field test of mobile phone shielding devices. 2010.page 1-3 http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1033&context=techmasters

Ayers, Ric-Brothers, Sam-Jansen : AYERS,Ric; BROTHERS,Sam; JANSEN, Wayne.Guidelines on mobile device forensics.NIST special Publication,2013 800:101.page 46-48 http://www.nist.gov.tr/forensics/research/upload/draft-guidelines-on-mobile-device-forensics.pdf

İnternet : http://fdset.org/cms/images/Computer%20Forensics.pdf

İnternet : https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Wikipedia : ‘‘Vikipedi Özgür Ansiklopedi’’, 2014 http://tr.wikipedia.org/wiki/Exchangeable_image_file_format

İnternet : http://www.bilgiguvenlik.net/2012/05/ios-forensic.html/

İnternet : http://www.andropedi.com/root-nedir-android-telefonda-root-ne-ise-yarar/

Wikipedia : ‘‘Vikipedi Özgür Ansiklopedi’’, 2014 http://tr.wikipedia.org/wiki/Jailbreak_%28iOS%297

İnternet : http://www.mobiledit.com/downloads.htm?show=14

İnternet : http://www.androiddunya.com/samsung-galaxy-note-ii-n7100-nasil-root-yapilir/

Wikipedia : ‘‘Vikipedi Özgür Ansiklopedi’’, 2014 http://fdset.org/cms/images/Computer%20Forensics.pdf

Wikipedia : http://fdset.org/cms/images/Computer%20Forensics.pdf

SAĞIROĞLU, Şeref; BULUT, Hülya. : *SAĞIROĞLU, Şeref; BULUT, Hülya. Mobil ortamlarda bilgi ve haberleşme güvenliği üzerine bir inceleme.* Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, *2009, 24.3. http://www.mmfdergi.gazi.edu.tr/article/viewFile/1061000183/10610001574*

ŞEKİLLER LİSTESİ

Şekil 1 GSM Nesilleri 12
Şekil 2-GSM Frekanslarının Kullanım Haritası 13
Şekil 3-Örnek GSM Şebekesi 14
Şekil 4-Mobil Cihaz Donanım Görüntüsü 16
Şekil 5-Akıllı Telefon Hafıza Yapısı 20
Şekil 6-SIM Kart IMSI Kod Şeması 22
Şekil 7-SIM Kart Çeşitleri ve Boyutları 23
Şekil 8-SIM kart Dosya Sistemi 23
Şekil 9-2013 -2014 Akıllı Telefon Satış Oranları 24
Şekil 10-Akıllı Telefonların Pazardaki Oranları 24
Şekil 11-Android Mimarisi 25
Şekil 12-IOS Mimarisi 27
Şekil 13-IOS üzerinde çalışan uygulamalar 30
Şekil 14-Android zararlı yazılım istatistiği 37
Şekil 15-Tarantula Donanım ve Çantası 48
Şekil 16-Faraday Çantası 49
Şekil 17-Flasher Box Cihazı 51
Şekil 18-Mobil Cihazlarda Delillendirme Süreci 54
Şekil 19-Mobil Cihaz Üzerindeki Veri Alanları 55
Şekil 20-Akıllı Telefon Analiz seviyeleri 66
Şekil 21-Samsung GT-N7100 XRY bağlantısı 80
Şekil 22-XRY ile tespit edilen Samsun GT-N7100 cihaz bilgisi 81
Şekil 23 XRY ile Tespit Edilen Samsung GT-N7100 SMS kaydı 82
Şekil 24-XRY ile Tespit Edilen Samsung GT-N7100 Tespit Edilen Arama Kaydı 82
Şekil 25-XRY ile Tespit Edilen Samsung GT-N7100 Web History Kaydı 83
Şekil 26-XRY ile Tespit Edilen Samsung GT-N7100 Web Kaydı 84
Şekil 27-Nokia 6300 XRY ile Bağlantısı 84
Şekil 28-XRY ile Tespit Edilen Nokia 6300 Cihaz Bilgisi 84
Şekil 29-XRY ile tepsit edilen Nokia 6300 analizin son ekran görüntüsü. 85
Şekil 30- XRY ile tespit edilen Nokia 6300 Harici bellek verileri 87
Şekil 31-XRY ile tespit edilen Nokia 6300 Dâhili hafıza verileri 87
Şekil 32- XRY ile tespit edile n Nokia 6300 Arama kaydı 87
Şekil 33-XRY ile tespit edilen Nokia 6300 Sim hafıza Arama Kaydı 88
Şekil 34-XRY ile tespit edilen Nokia 6300 Mesaj Kaydı 88
Şekil 35-XRY ile tespit edilen Nokia 6300 SMS kaydı. 88
Şekil 36-XRY tarafından Nokia 6300 desteklenen Analiz Özellikleri 89
Şekil 37- XRY tarafından desteklenen Nokia 5800 Analiz özellikleri 90
Şekil 38-XRY ile tespit edilen Nokia 5800 SMS kaydı 90
Şekil 39- XRY ile tespit edilen Nokia 5800 Tespit Edilen Resim Kaydı 90
Şekil 40-XRY ile tespit edilen Nokia 5800 Ses kaydı. 91
Şekil 41-Mobiledit ile tespit Samsung GT-N7100 cihaz bilgisi. 93
Şekil 42-Mobiledit Samsung GT-N7100 Sim Kart bilgisi 94
Şekil 43-MobileDit ile tespit edilen Samsung GT_N7100 Arama Kaydı 94
Şekil 44-Mobiledit ile tespit edilen Samsung GT-N7100 SMS kaydı 95
Şekil 45-Mobiledit ile tesit edilen Samsung GT-N7100 Ses Kaydı 95
Şekil 46-Samsung GT-N7100 Root Yazılımı Yükleme Ekranı 96
Şekil 47-ODIN Uygulama Ekranı 97
Şekil 48-Mobiledit ile tespit edilen Samsung GT-N7100 Cihaz bilgisi 97
Şekil 49-Mobiledit ile tespit edilen Samsung GT-N7100 Web kaydı 99
Şekil 50-Mobiledit ile tespit edilen Samsung GT-N7100 resim dosyası bilgisi. 99
Şekil 51-Mobiledit ile tespit edilen Samsung GT-N7100 Cihaz Bilgileri 99

Şekil 52-Mobiledit ile tespit edilen Samsung GT-N7100 mail Adresi kaydı 100
Şekil 53-Mobiledit ile tespit edilen Samsung GT-N7100 Uygulama Kaydı..... 100
Şekil 54-Mobiledit ile tespit edilen Samsung GT-N7100 Arama Kaydı. 100
Şekil 55-Mobiledit ile tespit edilen Samsung SIM GT-S5620 SIM kart bilgisi. 101
Şekil 56-Mobiledit ile tespit Samsung S5620 SMS kaydı 102
Şekil 57-Mobiledit ile tespit edilen Samsung GT-S5620 Rehber Kaydı 102
Şekil 58-Mobiledit ile tespit edilen Samsung GT-S5620 mesaj kaydı 102
Şekil 59-Mobiledit ile tespit edilen Nokia 5800 Cihaz Bilgisi. 103
Şekil 60-Mobiledit ile tespit edilen Nokia 5800 Mesaj Kaydı..... 104
Şekil 61-Mobiledit ile tespit edilen Nokia 5800 Resim Kaydı 104
Şekil 62-Mobiledit ile tespit edilen İphone 4S Cihaz Bilgisi..... 105
Şekil 63-Mobiledit ile tespit edilen İphone 4S Mesaj Kaydı 105
Şekil 64-Oxygen Suite ile tespit edilen Samsun GT-N7100 Cihaz Genel Bilgisi 108
Şekil 65-Oxygen Suite ile tespit edilen Samsung GT-N7100 Ses Kaydı..... 108
Şekil 66-Oxygen Suite ile tespit edilen Samsung GT-N7100 SMS Kaydı 108
Şekil 67-Oxygen Suite Samsung GT-N7100 Web Sayfası Erişim Kaydı..... 109
Şekil 68-Oxygen Suite ile tespit edilen Samsung GT-N7100 Bookmarks Kaydı..... 109
Şekil 69-Oxygen Suite ile tespit Samsung GT-N7100 Google Hesap Şifresi kaydı..... 109
Şekil 70-Oxygen Suite ile tespit edilen Samsung GT-N7100 Google Maps Kaydı..... 110
Şekil 71-Oxygen suite Samsung GT-N7100 Google lokasyon kaydı..... 110
Şekil 72-Oxygen Suite Samsung GT-N7100 Google Drive Kaydı..... 110
Şekil 73-Oxygen Suite SQL lite Samsung GT-N7100 Google Drive Kaydı 111
Şekil 74-Oxygen Suite SQL lite GT-N7100 Ibbceptrafik kaydı..... 111
Şekil 75-Oxygen Suite Samsung GT-N7100 Flipboard Uygulama Kaydı 112
Şekil 76-Oxygen Suite Samsung GT-N7100 Flipboard Metadata Kaydı 112
Şekil 77-Oxygen Suite Samsung GT-N7100 Cihaz Bağlantı bilgisi 112
Şekil 78-Oxygen Suite Samsung GT-N7100 Fiziksel İmaj başlatma Ekranı..... 113
Şekil 79-Oxygen Suite ile tespit edilen Samsung GT-N7100 Genel Analiz verileri 113
Şekil 80-Oxygen Suite ile tespit edilen Samsung GT-N7100 Dropbox Kaydı 114
Şekil 81-Oxygen Suite ile tespit edilen Samsung GT-N7100 Youtube Kaydı 115
Şekil 82-Oxygen Suite Samsung GT-N7100 Uygulama Zaman bilgisi..... 115
Şekil 83-Oxygen Suite ile tespit edilen Samsung GT-N7100 Google Mail Kaydı 115
Şekil 84-Oxygen Suite ile tespit edilen Samsung GT-N7100 Facebook Kaydı..... 116
Şekil 85-Oxgyen Suite İphone4S Cihaz Bağlantı Bilgisi 116

TABLOLAR

Tablo 1-Normal telefon ile Akıllı Telefon Donanım Özellikleri 17
Tablo 2-Normal telefon ile Akıllı telefon yazılım Özellikleri 18
Tablo 3-İncelenecek Cihaz ve Yazılım tablosu gösterilmiştir 75
Tablo 4-Yazılımların özellikleri gösterilmiştir 75
Tablo 5-XRY Analiz Sonuçları 76
Tablo 6-Mobiledit Analiz Sonuçları. 77
Tablo 7-Oxygen Suite Analiz Sonuçları 78

1.GİRİŞ

Günümüzde akıllı telefonlar, sadece iletişim aracı olmanın dışına çıkmış, gün geçtikçe ilerleyen donanım ve yazılım özellikleri sayesinde bilgisayarlara alternatif hale gelmiştir.

Günümüz teknoloji dünyasında kullanıcılar bilgisayar ile yapabildikleri her türlü işlemi rahatlıkla akıllı telefonlar vasıtasıyla yapabilmektedir. Mobil teknolojinin sağladığı kolaylıklar beraberinde yeni güvenlik risklerini de getirmiştir.

Akıllı telefonlar ile sosyal medyanın kullanımı artmış, bu artış bilişim suçlarının ve mağdurlarının artmasına neden olmuştur. Akıllı telefonlara yönelik üretilen zararlı yazılımlar ile kişilerin banka hesap bilgilerine ulaşılabilmekte, kişiye özel (resim, video) verilerine izinsiz şekilde erişilebilmekte ve kişinin elektronik posta adresi ele geçirilerek başka kullanıcılara elektronik posta atılabilmektedir.

Günümüzde işlenen suçların %70'den fazlasını mobil cihazlarla ilişkili suçlar oluşturmaktadır. Akıllı telefonlar, işlenen suçların bu kadar büyük bir yüzdesi ile yakından ilgiliyken bilişim suçlarının incelenmesi de bir o kadar önem kazanmıştır.[1]

Tüm akıllı telefon kullanıcıları bilinçli ya da bilinçsiz bir şekilde işlenen bilişim suçunun bir parçası haline gelebilmekte olduğundan akıllı telefonları kullanırken daha çok dikkatli olunması gerekmektedir.

Bu çalışmada anlam kargaşasına mahal vermeden sade ve anlaşılır bir anlatım kullanılabilmesi amacıyla "mobil cihazlar" ibaresi "akıllı telefon ve cep telefonları" manasında kullanılmıştır.

---

1 Ahmet EKİM, Mobil Cihazlarda adli Bilişim ve Malware Analizi, http://www.bilgisayardedektifi.com/mobil-cihazlarda-adli-bilisim-ve-malware-analizi/206 Et:17.05.2014

A. AMAÇ

Mobil cihazların yaşantımızın her alanına girmesi hayatımızı kolaylaştırması ve diğer olumlu sonuçlarının yanısıra kontrol edilmesi güç sorunları da beraberinde getirmiştir. Özellikle 2005 yılı itibariyle akıllı telefonların kullanımındaki süratli artış adli bilişim suçlarının diğer işlenen suçların içerisinde büyük bir pay sahibi olmasına sebep olmuştur[2].

Bu çalışmada mobil cihazlarda bilişim suçları kapsamında delillerin nasıl araştırılması gerektiği ve araştırmanın hangi süreçlerden oluşacağı anlatılmıştır. Mobil cihazlarda adli bilişim inceleme süreçleri için çözümler önerilmiştir.

2.ADLİ BİLİŞİMİN TANIMI VE SAFHALARI

A. Adli Bilişim Kavramı ve Bilişim Suçları

1. Bilişim Kavramı

Bilişim, insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin dayanağı olan bilginin özellikle günümüzde elektronik cihazlar aracılığı ile düzenli ve akla uygun bir biçimde işlenmesi olarak tanımlanmaktadır.[3]

2. Bilişim Suçu Kavramı

Teknolojideki gelişmeler sağlık, eğitim, ticaret, ekonomi ve sanayi gibi birçok alandaki işleyiş modellerinde değişikliklere sebep olmuş, hayatımızı kolaylaştırırken öte yandan çeşitli güvenlik önlemleri almaya zorunlu hale getirmiştir. Günümüzde bilgi çok daha değerli bir hale gelmiş, kültürel, ekonomik, sosyal, siyasal vb. her alanda yeni "güç" ölçü birimi "bilgi" haline gelmiştir. İnternetin yaygınlaşması bilgiye erişim ve paylaşımın çok daha süratli ve kolay hale getirmesinin yanısıra bilginin doğruluğu, bütünlüğü ve gizliliği gibi çeşitli sorunları da beraberinde getirmiştir.

"Bilgi" kavramı çok daha değerli ve hassas hale geldiğinden, kötü niyetli kişilerin hedefi haline gelmiş, bilginin muhafazası ve paylaşımında güvenlik daha ciddi bir unsur olmuştur. Artık "suç" ve "suçlu" olguları sınırlarını genişleterek

---

2 Paul McCarthy, School of Computer and Information Science Mawson Lakes Forensic Analysis of Mobile PhonesOctober2005s.3 http://www.8051projects.net/files/public/1236046309_9698_FT19075_forensic_analysis_of_mobile_phones.pdf Et:18.05.2014

3 TDK "Güncel Türkçe Sözlük" www.tdk.gov.tr, E.t: 17.05.2014

küresel bir boyuta ulaşmış, bilişim suçları çok çeşitlilik kazanarak farklı şekillerde tanımlanmaya başlanmıştır.

Çeşitli kaynaklardan alınan tanımlar aşağıda sunulmuştur;

- "Ceza kanununu ihlal eden, işlenmesinde veya araştırılmasında bilgisayar teknolojisi bilgilerini içeren her suç bilişim suçu" olarak tanımlanmaktadır.[4]
- "Bilişim suçları genel olarak, verilere veya veri işleme bağlantısı olan sistemlere veya sistemin düzgün ve işlevsel işleyişine karşı, bilişim sistemleri aracılığıyla işlenen suçlar" şeklinde tanımlanmaktadır. Türk ceza Kanunu'nda ise bilişim suçları "Bilişim alanında suçlar" ve Özel hayata ve hayatın gizli alanına karşı suçlar" bölümünde düzenlemiştir.[5]
- Dülger, "bilişim suçunu, verilere karşı ve veri işlemlerine bağlantısı olan sistemlere karşı bilişim sistemleri aracılığıyla işlenen suçlar" olarak tanımlamıştır.[6]

3. Adli Bilişim Kavramı

Adli Bilişim özel inceleme ve analiz teknikleri kullanılarak bilgisayarlar başta olma üzere, tüm elektronik medya üzerinde yer alan potansiyel delillerin toplanması amacıyla, elektronik aygıtların incelenmesi süreci olarak açıklanmaktadır.[7]

Bilişim suçlarını çeşitli kategorilerle sınıflandırmak ve farklı şekillerde tanımlamak mümkündür. Türk Ceza Kanunu içerisinde "bilgisayar suçları" "bilişim suçları" olarak tanımlanmaktadır.

---

4 Bilişim Suçları Kapsamında Dijital Deliller, http://ab.org.tr/ab05/tammetin/134.pdf/ Et: 17/05/2014

5 İstanbul Barosu Dergisi Sayı: "Bilişim Suçu" Mart-Nisan 2014 http://www.istanbulbarosu.org.tr/proje/dergi/19/files/assets/basic-html/page241.html Et: 17.05.2014

6 DÜLGER, Murat Volkan. "Turk Ceza Kanunu'nda Yer Alan Bilisim Sucları ve Elestirisi" http://www.dulger.av.tr/pdf/ytkbilisimsucelestrisi.pdf Et:17.04.2014

7 Keser Berber, Adli Bilişim, CMK md 134 ve Düşündürdükler, http://www.leylakeser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html Et:17.04.2014

Bilişim suçlarının en büyük özelliği suçun zaman ve mekân açısından sınırlı olmayacak şekilde meydana gelmesidir. Teknolojinin süratle gelişmekte olması ve bilişim suçlarının uluslararası yapısı karşısında hukuk sistemimiz ve kanunlarımız hem şekil hem de içerik bakımından yetersiz kalmaktadır.

Bilişim suçları dışındaki davalarda deliller elle tutulabilir niteliktedir. Bilişim suçlarında ise delilleri sabit disk sürücülerinden elde edilen veri, akıllı telefon veya bilgisayarların geçici hafızalarından tespit edilen veri gibi sanal nitelikteki ve kompleks araştırma yöntemleriyle sağlanabilen argümanlar oluşturur. Delillerin bu şekilde sunulması dava olaylarına yeni bir boyut kazandırmış ve "Adli Bilişim" (Computer Forensics) biliminin ortaya çıkmasına neden olmuştur.[8]

Adli bir olayın en temel yapı taşlarını "suç faktörünün tespiti" ve "suçlunun belirlenmesi" oluşturur. Bir olgunun "suç" olarak değerlendirilebilmesi için öncelikle kanunen "suç" teşkil edecek şekilde tanımlanmış olması gerekmektedir. Adli bilişim alanında "suç" olarak değerlendirme yapabilmek için dahi büyük bir bilgi birikimine sahip çeşitli uzmanlar tarafından geniş çaplı araştırmalar yapılması ihtiyacı olup tanımların teknolojiye ayak uydurabilecek şekilde belirlenmesi gerekmektedir. Teknolojinin süratli gelişimi adli bilişimin kanununu belirleme noktasında zorluklar yaratmaktadır.

Bir suç işlendiğinde suçu işleyen kişi arkasında mutlaka iz/delil bırakır.[9] Bırakılan iz/delil kolayca fark edilebilir yapıda da, fark edilmesi zor bir yapı da olabilir. Adli bilişim alanında bahse konu deliller farklı şekil ve formatlarda olabilmektedir. LOCARD değişim prensibine göre bir şey veya kişi olay yerinden bazı şeyleri alırken, bazı şeyleri de olay yerinde bırakır.[10] Buradan anlaşıldığı gibi bir suçu iz bırakmadan işlemek neredeyse imkânsızdır.

Dijital deliller dünya içinde yeni bir kavram olup bilimsel alanda çok yoğun tartışmaların odak noktası olmuş ve birçok tanımın yapılmasına neden olmuştur. Türkiye'de bilişim suçlarıyla ilgili gerekli çalışmalar ve bu suçlar için ceza kanunlarında tanımlamalar yapılmıştır.765 sayılı TCK'nin 1991 yılı

---

8 Interpol Computer Crime Manuel 2. Officer, İnterpol, s.10 Et:14.05.2015

9 UZUNAY, Yusuf; BICAKCI, Kemal. A3D3M: Açik Anahtar Altyapisi DESTEKLI DIGITAL Delilleri Doğrulama Modeli http://www.emo.org.tr/ekler/4843973f9b66701_ek.pdf./ Et:10.05.2014

10 Casey, E. (200s4). Digital Evidence and Computer Crime: Forensic Science, Computers,and the Internet, 2nd Ed., Academic Press. http://www.google.com.tr/books?hl=tr&lr=&id=DQdWRitMcyAC&oi=fnd&pg=PP2&dq=Digital+Evidence+and+Computer+Crime&ots=t4uH0Y4WsI&sig=TLAsvz-Vh3k7pOTQmUVzyWBOKJE&redir_esc=y#v=onepage&q=Digital%20Evidence%20and%20Computer%20Crime&f=false Et:10.05.2014

değişiklikleri ile birlikte bilişim alanında suçlar başlıklı 11.babında çeşitli suçlar ve 5237 sayılı TCK'nın ilgili maddelerinde bilişim suçları düzenlemiştir.[11]

Ülkemizde de bilişim suçlarıyla ilgili tanımlamaları belirlemek için yapılan yoğun çalışmalara rağmen hukuksal ve teknik bazı sorunlar yaşanmaktadır. En önemli unsur dijital delillerin tespiti, toplanması, incelenmesi saklanması ve ilgili yerlere aktarılması/sunulması işlemleri esnasında veri bütünlüğünün korunmasıdır. Bu da dijital delilleri inceleyen kurum/kuruluş ve kişilerin belli başlı kalite standartlarına göre işlemlerini yapması gerektiğini dikte eder.[12]

B. Adli Bilişim Safhaları

Dijital delil "Bilişim sistemlerinin veya bilgileri otomatik olarak işleme tabi tutma yetisine sahip elektronik cihazların veri depolama medyaları üzerinde bulunan yahut bu medyalar üzerinden geçen, suç ile ilgili delil niteliği taşıyabilecek ve suçun aydınlatılmasını sağlayacak verilerdir"[13] şeklinde tanımlanmaktadır.

Sayısal deliller normal klasik delillerden farklıdırlar. Klasik deliller olay mahallinde çok rahatlıkla tespit edilebilirken dijital deliller için bunu söylemek pek mümkün olmamaktadır. Olay mahallindeki en ufak ayrıntı ciddi kayıplara yol açabilmektedir. Bu alandaki tüm elektronik cihaz ve medyaların olaya ilişkin bir parça olabileceği unutulmamalı ve her bir cihaza ve ortama nasıl yaklaşılması gerekiyorsa o şekilde yaklaşılmalıdır.

Muhafaza altına alınarak incelemeye başlanmış bir klasik delil ortamında deliller çok rahatlıkla görülebilmektedir. Dijital deliller ise bu kadar somut bir yapıya ve özelliğe sahip değillerdir. Elde edilmesi ve muhafazası çeşitli işlemler gerektirmektedir[14].

---

11 Hüseyin ÇAKIR / Ercan SERT, Bilişim Suçlarını Delillendirme Süreçi http://utsam.org/images/upload/attachment/utsas_2010_secilmis/Bili%C5%9Fim%20Su%C3%A7lar%C4%B1%20ve%20Delillendirme%20S%C3%BCreci.pdf/ Et:10.05.2014

12 Hüseyin ÇAKIR / Ercan SERT, Bilişim Suçlarını Delillendirme Süreçi http://utsam.org/images/upload/attachment/utsas_2010_secilmis/Bili%C5%9Fim%20Su%C3%A7lar%C4%B1%20ve%20Delillendirme%20S%C3%BCreci.pdf/ 19.06.2014

13Ekizer, A. H. (2014). Adli Bilişim - Computer Forensics, http://www.ekizer.net/adli-bilisim-computer-forensics/ (Et: 18.09.2014)

14 Adli Bilişim, http://edirnebarosu.org.tr/incelemeler/adli-bilisim-computer-forensic/ Et: 19.06.2014

Sayısal ortamda doğru bir şekilde analiz yapmak düşünüldüğü kadar kolay değildir. Adli bilişim analizinde delillerin incelenmesi ve analizi klasik adli incelemelere göre karmaşık, teknik ve pahalıdır.

Dijital delil olarak elektronik aygıtlardan elde edilebilecek ve delil oluşturabilecek bulgular şunlar olabilir:[15]

- Video görüntüleri
- Fotoğraflar
- Yazı dosyaları (word, excell, open office vb. dosyaları)
- Çeşitli bilgisayar programları
- İletişim kayıtları (SMS, MSN Messenger, GTalk vb. kayıtları)
- Gizli ve şifreli dosyalar / klasörler
- Dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları
- Son girilen ve sık kullanılan internet siteleri
- İnternet ortamından indirilen (download) dosyalar
- Ve bu türden olup, silinmiş dosya/klasörler

Adli bilişim incelemesinde delillerin tespitinden sonra en önemli aşama hukuki bir delil haline dönüştürülmesidir. Dönüşüm işlemi çeşitli aşama ve işlemlerden oluşmaktadır. Bu aşamalar adli bilişim safhaları olarak tanımlanmakta olup farklı kaynaklarda birbirinden farklı şekillerde belirlenmiştir. Her ne kadar farklı kaynaklarda farklı aşamalar "4 veya 5" belirlenmiş olsa da temelde adli bilişim safhalarını dört bölüme ayrılarak [16] incelemektedir.

- Elde Etme/Toplama (Acquisition/*Collection*)
- Tanımlama/İnceleme (Identification/*Examination*)
- Değerlendirme/Çözümleme (Evaluation/*Analysis*)

---

15 http://www.hukuksokagi.com/kaynak/adli-bilisim-computer-forensic/ Et: 19.06.2014

16 Ekizer, A. H. (2014). Adli Bilişim - Computer Forensics, http://www.ekizer.net/adli-bilisim-computer- forensics/ Et:17.07.2014

- Raporlama/Sunum (*Reporting/Presentation*)

1. Delil Toplama (Acquisition/Collection)

Delillerin elde edilmesi safhasıdır. Olay yeri incelemesi hukuk kurallarına ve yasalara (CMK m 116'ya) uygun olması gerekir. Olay yerindeki delillerin sağlıklı bir şekilde toplanması olay yerine müdahale şekliyle ilgilidir.[17]

Digital deliler doğası gereği bozulmaya veya değiştirilmeye müsait oldukları için elde edilen delillerin yetkili makamlar tarafından kabul olması gerekmekte olup bu aşama bu yüzden önem arz etmektedir.[18]Delil elde etme işlemi esnasında klasik adli bir olayda olduğu gibi olay yerinin güvenlik alanının belirlenmesi ve bu alana yetkisi olmayan kişilerin müdahalesinin engellenmesi gerekmektedir. Ancak bu şekilde delillerin sağlıklı bir şekilde toplanması sağlanabilir.

Olay yeri güvenli hale getirildikten sonra bu alana "Adli Bilişim" uzmanından önce kimsenin girmemesi sağlanmalıdır. Böylece bu ortamda delillerin zarar görmesi ya da kaybolması önlenmiş olacak ve adli bilişim uzamanı uygun şekilde delilleri toplayabilecektir. Unutulmamalıdır ki adli bilişim kapsamında önem arz eden delillerin yanı sıra klasik adli bir olay kapsamında önemli olan ve kriminalistik inceleme gerektiren delillerin(örneğin şüpheliye ait eşyalar üzerinde parmak izi vs.) de bütünlüğü korunmalıdır. Kriminalistik incelemede bir kimyasalın dijital ve elektronik delillere zarar verileceği göz önünde bulundurulmalı, kriminal ve adli bilişim verileri birbirini etkilemeyecek şekilde toplanmalıdır.

Öncelikle olay yerinin fotoğrafları çekilmeli, ortamda bulunan bilgisayar, yazıcı ve diğer donanım aygıtlarının konumları belirtilecek şekilde notlar ve krokiler hazırlanmalıdır. Özetle, bu aşamaya kadar uygulanan yöntemler açısından, kriminalistik ve adli bilişim yöntemlerinin bir arada yürütüldüğünü söylemek mümkündür.[19]

Sonrasında ise işlemler cihazların çalışma durumlarına göre sıralı bir şekilde yapılmalıdır. Çalışmakta olan bir bilgisayarın kapatıldığı zaman tekrar açmak için şifreye ihtiyaç duyulabileceği unutulmamalı veya bilgisayar imajının

---

17 http://www.hukuksokagi.com/kaynak/adli-bilisim-computer-forensic/ Et:03.10.2014

18 YUSOFF, Yunus; ISMAIL, Roslan; HASSAN, Zainuddin. Common phases of computer forensics investigation models. *International Journal of Computer Science & Information Technology*, 2011, 3.3: 17-31. http://airccse.org/journal/jcsit/0611csit02.pdf ET:05.08.2014

19 http://www.hukuksokagi.com/kaynak/adli-bilisim-computer-forensic/ ET:05.08.2014

ve delillerin bütünlüğünün korunabilmesi açısından kapalı bir bilgisayar (veya bilişim aygıtı) imajı alındıktan sonra adli bilişim incelemesine uygun şekilde açılmalıdır. Örneğin bilgisayar sistemlerinin işletim sistemleri açılırken birçok yapılandırma dosyasına erişim sağlamakta ve ileride suç delili olabilecek verilerin zarar görmesine yol açabilmektedir. Dosyaların erişim tarihleri bile bazı durumlarda delil niteliği taşıyabileceği için bu durum oldukça sakıncalıdır. Aynı zamanda işletim sistemlerinin açılırken oluşturabileceği geçici dosyalar ve geçici hafıza disk alanları daha önceden silinmiş olan veri alanlarının üzerine yazılabileceği için silinmiş verilerin delil niteliğinde kurtarılabilme olasılığını ortadan kaldırmış olacak ve dolayısı ile delilin bütünlüğünü bozmuş olacaktır. Bu yüzden incelemesi yapılacak bilgisayar sistemleri ve bazı ağ cihazları kapalı durumda iseler kesinlikle açılmamalıdır.[20]

Yukarıda verilen örneğin aksine, çalışmakta olan bir bilgisayarda delil toplanırken delillere zarar verilebilir. Örneğin sistem kapatıldığında delil olarak nitelendirilebilecek verileri özellikle silen bir uygulama mevcut olabilir ve bu uygulama bahse konu delilleri tekrar bulunması mümkün olmayacak şekilde ortadan kaldırabilir, buna karşı tedbir olarak sistem normal kapanma prosedürünü uygulamak yerine elektriği doğrudan kesilerek kapatılabilir. Bunun yanı sıra sistem kapatıldığında geçici hafızadaki(RAM) veriler silineceği için herhangi bir işlem yapmadan veya sistemi kapatmadan önce RAM'in imajı alınması da gerekebilir.

Bilgisayarların olay muhalinden alınıp inceleme alanı olan "Adli Bilişim Laboratuvarı'na ulaştırılması hassas bir konu olup,

- Ortam şartlarından (sıcaklık, nem, elektromanyetik dalgalar vs.) etkilenmeyecek ve arızalanmayacak bir şekilde muhafaza edilerek nakil edilmeli,
- Olay mahallinden alınan her şeyin bir listesinin tutanak altına alınmasına dikkat edilmeli,
- İncelemenin bitimini müteakip aynı şartlar göz önünde bulundurularak muhafaza edilmelidir.

Adli bilişim kapsamında icra edilecek incelemeler doğrudan el koyulan donanımlar üzerinde veya alınan ilk orijinal imaj üzerinde değil, orijinal imajdan oluşturulan kopya imaj üzerinde yapılmalıdır. İmaj alınması hususunda imajın

20 Ekizer, http://www.ekizer.net/adli-bilisim-computer-forensics/ Et:05.08.2014

doğru yazılım/yazılımlar kullanılarak alınması ve inceleme işlemlerinin veri bütünlüğü bozulmadan yapılması önemlidir. Adli Bilişimde tüm diskin bu şekilde bire bir kopyasının alınması işlemine imaj(forensics image) denilmektedir.[21]

Orijinal imajın üzerinde çalışılmak yerine bahse konu imajın bir kopyası üzerinde çalışılmalı. Çünkü üzerinde çalışılan imajın bozulması durumunda verinin bütünlüğünü bozmadan ve donanıma zarar vermeden tekrar imaj almak gerekir ve imajı alınacak sistemin çalışması devam eden bir sistem olması durumunda yeni alınacak imaj eskisinden farklı olur, çalışması sonlandırılmış bir sistem için ise imaj alma amaçlı olarak donanım her kullanıldığında donanıma zarar verme riski tekrar ortaya çıkmış olur.

İmaj alma işleminde alınan imajlar yazma korumalı olan başka özel bir sisteme yerleştirilmelidir. Kullanılacak yazılım ve donanıma incelenecek cihazın marka ve modeline göre karar verilmelidir. Diğer bir deyişle inceleme yapacak uzman personelin tüm delilleri kayıp olmayacak şekilde toplayabilecek bilgi ve donanıma sahip olması gerekmektedir.

2. İnceleme/Tanımlama (Identification /Examination)

Delil elde etme (Toplama) aşaması imaj alınması ile sona ermekte olup inceleme aşaması ile birlikte çalışmanın teknik yönü başlar. Bu aşamada birtakım delillerin suça dair olup olmadığı araştırılmaktadır. Araştırılacak veriler karşılaştırılan suça ve suç ile ilgili verilerin bulunduğu veri depolama birimlerine göre değişiklik gösterebilmektedir[22]

Bu safhada elimizde birtakım bulgular vardır. Bunların bazıları görünmekte, bazıları henüz görünmemektedir. Görünmeyen bulgular gizli ve silinmiş dosyalardır. İnceleme ile tüm bu bulgular üzerinde çeşitli işlemler yapılarak olası suç unsurları ortaya konacaktır. Örneğin; fotoğraflar, grafik dosyaları, videolar, çeşitli yazı dokümanları (word, excell, openoffice vb.), konuşma kayıtları (chat, MSN, GTalk vb.), e-postalar, ziyaret edilmiş web siteleri, şifreli dizinler, silinmiş klasör ve dosyalar ile dosyaların oluşturulma, değiştirilme ve erişim kayıtları örnek gösterilebilir.[23]

Bu aşama bulunan verilerin anlam kazandırıldığı aşamadır diyebiliriz. İnceleme aşaması delilin gözle görülür kılınmasını sağlamaya ve delilin orijinin

---

21 SAUDI, Madihah Mohd. An overview of disk imaging tool in computer forensics. SANS Institute, 2001. http://www.sans.org/reading-room/whitepapers/incident/overview-disk-imaging-tool-computer-forensics-643/ Et:05.08.2014
22 Ekizer, http://www.ekizer.net/adli-bilisim-computer-forensics/ Et:10.09.2014
23 http://www.gelarabul.com/adli-bilisim-inceleme-surecleri Et:10.09.2014

ve öneminin açıklanmasına yardımcı olmaktadır. Bu aşama pek çok şeyin tamamlanmasını sağlamaktadır.[24] Bu aşamada da birtakım ücretli ve açık kaynak yazılımlar kullanılabilir ve bu yazılımlara FTK *ve* EnCase örnek gösterilebilir.

3. Çözümleme/Değerlendirme (Evaluation/Analysis)

Verilerin "Alınan imajın" görülebilir ve incelenebilir hale getirilmesinden sonra ki analiz edilip incelendiği aşamadır.[25] Bu aşamada, yapılacak analizler sonucunda bulunan veri türleri ayıklanarak hangi verilerin hangi sebeple ve hangi ölçü de yetkili makamlara sunulacağı belirlenir ve bir ayıklama işlemi yapılır. Bu aşamanın bir tür ayrıştırma ve temizleme aşaması olduğunu söylemek mümkün olacaktır. Bu işlemin sonucunda gerekli tutanaklar tutularak yapılan işlemler kayıt altına alınır. Bu aşama aynı zamanda bir nevi adli bilişim biliminin söz konusu olay ile ilgili kurallarına uygun olarak yapılıp yapılmadığının da kontrolü yapılmaktadır. KISACA: Doğru ve öz veriler, bütünlüğü bozulmadan ve anlaşılabilir ölçüde suçu aydınlatacak şekilde delil olarak ortaya konulmalıdır.[26]

4. Raporlama/Sunum (Reporting/Presantation)

İnceleme ve analiz aşamaları bitmiş olup artık adli bilişimin son aşaması olan raporlama bölümüne geçilmiştir. Artık yapılan tüm işlemlerin neticesinde ortaya çıkartılan sonuçların adli makamlara sunulma işlemi gerçekleşir. Adli bilişim uzmanı inceleme aşamasından geçmişe ait verilerden hangilerinin delil olabileceği, soruşturmada görevli güvenlik birimlere iletir ve adli makamlara hangi metotların kullanıldığını, olayla ilgili bilgiler, incelemenin yapıldığı tarih ve zaman dilimi, kullanılan yazılım ve donanım bilgilerini de içerecek rapor hazırlar ve sunar ilgili göreceli kolluk ise değerlendirip adli makamlara sunacaktır.

Bu aşamada ayrıca ayrıntılı olarak dijital delillerin nasıl elde edildiğine ilişkin teknik boyutu ve adli bilişimin hangi metotların kullanıldığı da anlaşılır bir dille belirtecek açıklayıcı bir rapor hazırlanacaktır.[27]

---

24 Keser Berber, Leyla. Adli Bilişim, 1. Basım, Ankara 2004 s. 45 ISBN:975-464-299-0

25 YUSOFF, Yunus; ISMAIL, Roslan; HASSAN, Zainuddin. Common phases of computer forensics investigation models. *International Journal of Computer Science & Information Technology*, 2011, 3.3: 17-31. http://airccse.org/journal/jcsit/0611csit02.pdf Et:15.10.2014

26 Ekizer; http://www.ekizer.net/adli-bilisim-computer-forensics/ Et:15.10.2014

27 Ekizer; http://www.ekizer.net/adli-bilisim-computer-forensics/ Et:15.10.2014

3.MOBİL CİHAZLAR VE GSM TEKNOLOJİSİ

A. Mobil GSM Tarihi

GSM öncelikle Ericsson ve Nokia tarafından, Avrupa'da tasarlanmış dünya çapında kullanılan bir hücresel sistemdir.[28]Mobil iletişim teknolojisinin temeli 1980li yıllarda atılmaya başlanmış olup Global System for Mobile Communications (Mobil İletişim Küresel Sistemi), olarak adlandırılmış bir iletişim protokoldür.

Küresel iletişim ağı dediğimiz mobil iletişim protokolü 1982 yılında AB "Avrupa Birliği" tarafından onaylanmıştır. Önceleri Avrupa Telekomünikasyon Standartları Komitesi-Group Speciale Mobile (mobil iletişim Özel Ağı) alt kuruluş ismini taşımış sonra ise küresel bir isim olarak anılmıştır.[29]

GSM Bugün itibariyle en yaygın cep telefonu iletişim standardı olarak 212 ülkede 2 milyar insan tarafından kullanılmaktadır.[30]

1988 yılında AB tarafından standartları belirlenmiş ve 1990 yılında İngiltere'nin önerisi ile 1800 Mhz frekansı GSM şebekesine adapte edilmiştir. GSM teknolojisi ile ilk defa 1 Temmuz 1991 yılında Finlandiya başbakanı Harri Holkeri Nokia tarafından sağlanan ekipmanlarla ilk GSM görüşmesini yerel GSM operatörü Radiolinja üzerinden gerçekleştirdi.[31]

1989 yılında bu teknoloji AB tarafından uluslararası küresel iletişim ağı standardı olarak kabul edilmiştir. ABD, Japonya ilk zamanlarda bu standardı kabul etmemiş olsa da ABD daha sonra geri adım atmıştır. 1995 yılında Kuzey Amerika'nın ilk hücresel telefon şebekesi ABD Başkan yardımcısı Al Gore ile GSM 1900 frekansı üzerinden yapılan görüşme ile başladı. 800 ve 900 Mhz GSM bantlarına ABD tarafından 1900 bandı eklenmiş oldu.[32]Japonya bu gelişmelere rağmen GSM teknolojisi ile uyumlu olmayan kendi sistemlerini kullanmıştır.

---

28 AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. Guidelines on Mobile Device Forensics (Draft). NIST Special Publication, 2013, 800: 101. http://www.engistudio.it/wordpress/wp-content/uploads/NIST.SP_.800-101r1.pdf/

29 http://tr.wikipedia.org/wiki/GSM/ Et:30.01.2015

30 http://tr.wikipedia.org/wiki/GSM/ Et:30.01.2015

31 http://www.teknokulis.com/Yazarlar/hasan_genc/2011/06/30/gsmden-ilk-alonun-uzerinden-20-yil-gecti Et:15.01.2015

32 http://www.teknokulis.com/Yazarlar/hasan_genc/2011/06/30/gsmden-ilk-alonun-uzerinden-20-yil-gecti/ Et:15.01.2015

Ülkemizde ise 1G(NMT) ve 2G yaygın olarak kullanılmış olup ilk GSM görüşmesi 23 Şubat 1994 tarihinde Başbakan ile Cumhurbaşkanı arasında yapılmıştır.[33]

Ülkemizde ilk olarak hizmet vermeye TURKCELL başlamıştır. O tarihten itibaren Çeşitli nesil GSM teknolojileri kullanılmış olup 10 Eylül 2007 tarihinde Ulaştırma Bakanlığı tarafından 3G ihalesi açılmış ve lisansı satın alınmıştır. 3G'nin kullanılmasıyla akıllı telefonlar kullanılmaya başlanmış olup operatörler "TURKCELL, AVEA ve VADOFONE" arasında numara aktarım işlemi yapılmaya başlanmıştır.

Mobil Telefon Sistemlerinin nesilleri ve özellikleri aşağıda verilmiştir.[34]

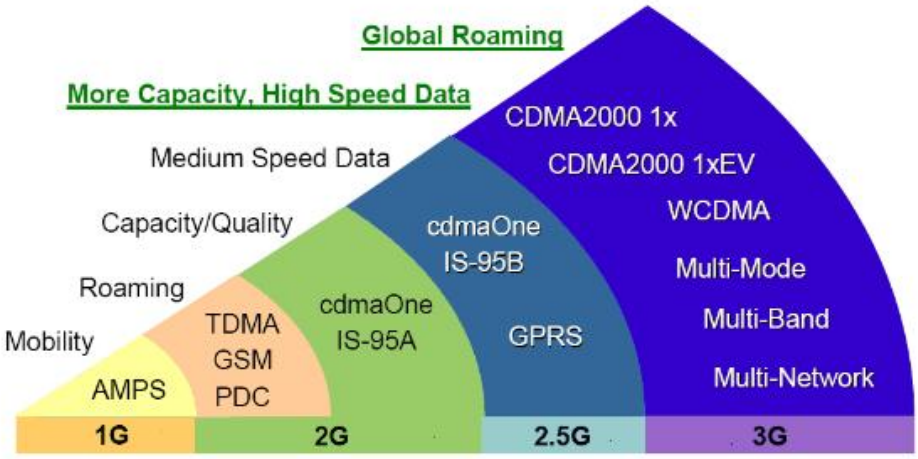
1G olarak adlandırılan ilk nesil sistemlerde, analog veri akışı kullanılır.

2G olarak adlandırılan ikinci nesil sistemlerde sayısal veri akışı kullanılır.

2.5G olarak adlandırılan ikinci nesil sistemlerde devre anahtarlamalı sistemlere ilave olarak paket bazlı veri iletişimin eklenmesini (GPRS, EDGE) içeren şebekeleri ifade eder. GSM 2G ve 2.5G kategorisine giren ikinci nesil bir sistemdir

3G olarak adlandırılan üçüncü nesil sistem ile daha hızlı veri transferi ve bant genişliğinin daha verimli kullanımı mümkün olmuştur.

4G olarak adlandırılan dördüncü nesil sistem ile kapsama alanı başta olmak üzere 3G ile çözülememiş olan sorunların çözülmesi beklenmektedir.



Şekil 1 GSM Nesilleri[35]

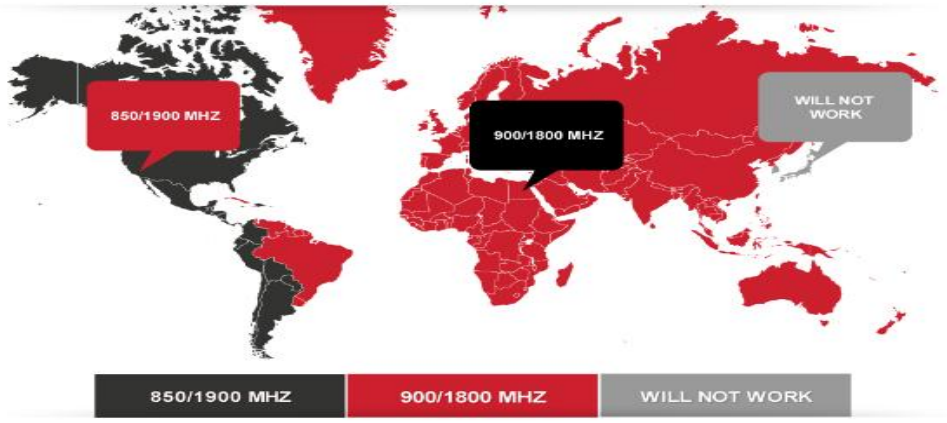
33 http://www.teknokulis.com/Yazarlar/hasan_genc/2011/06/30/gsmden-ilk-alonun-uzerinden-20-yil-gecti Et: 30.01.2015
34 http://tr.wikipedia.org/wiki/GSM Et:30.01.2015

Kullanılmakta olan 4 çeşit GSM sistemi aşağıda sıralanmıştır.

GSM 900 (900 Mhz): GSM900 Mhz bandı Türkiye'de mobil haberleşme için ayrılmış olup 124 kanaldan oluşmaktadır.915-917 MHz arasındaki 2 MHz'lik kısım koruma bandı için bırakılmıştır. Bu 2 MHz'lik koruma bandı, alışveriş frekansları arasındaki elektromanyetik dalgalar arasında oluşabilecek girişimi (enterferans) önlemek amacıyla oluşturulmuştur.[36]

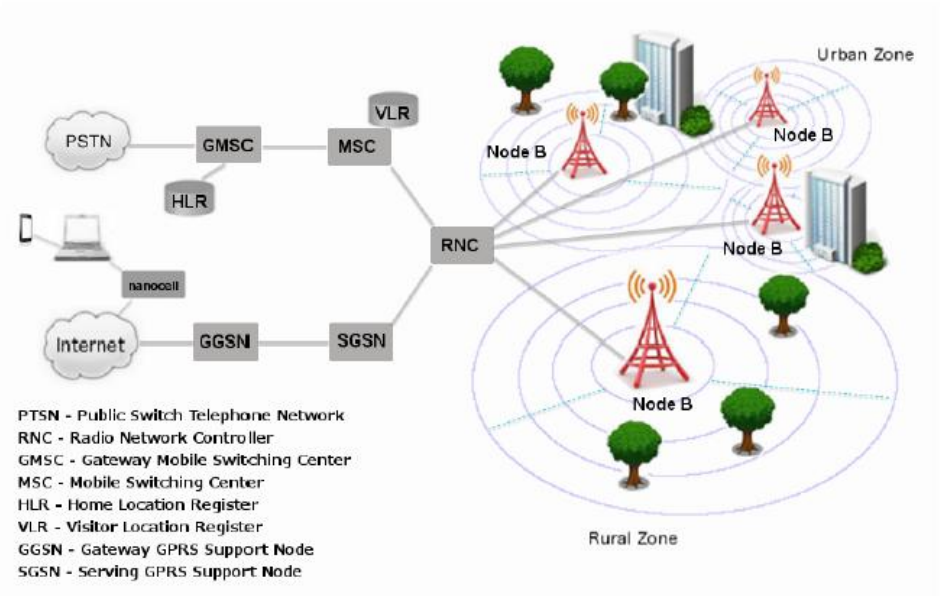
GSM 1800 (1800Mhz): Band iletişim taşıma kapasitesi daha yüksek olduğu için genellikle kentleşmenin çok yoğun olduğu alanlarda kullanılmaktadır. GSM 1800 bandında 75 kanal vardır. Türkiye'de bu bandı yalnızca AVEA A.Ş. kullanmaktadır.

GSM 1900 (1900Mhz) GSM 2100 (2100Mhz): Taşıma kapasitesi daha yüksek olup Amerika Birleşik Devletleri'nde kullanılmaktadır.



Şekil 2-GSM Frekanslarının Kullanım Haritası[37]

35http://www.elektrikport.com/teknik-kutuphane/gsm-nasil-calisir-1-bolum/10192#ad-image-1 Et:01.02.2015
36http://www.elektrikport.com/teknik-kutuphane/gsm-nasil-calisir-1-bolum/10192#ad-image-1Et:01.02.2015
37http://www.elektrikport.com/teknik-kutuphane/gsm-nasil-calisir-1-bolum/10192#ad-image-1 Et:02.02.2015



Şekil 3-Örnek GSM Şebekesi[38]

Genel olarak GSM sistemi iki temel bileşenden oluşur. Bu bileşenlerden biri Baz İstasyonu (BSS-Base Station Subsystem) diğeri ise Şebeke Anahtarlama Sistemidir(NSS-Network Switching System). Mobil İstasyon(MS-Mobile Station) aboneler tarafından kullanılan ve içinde SİM kartı bulunduran cihazdır.

Baz istasyonu; BTS alıcı verici ünitesi ve BSC(Baz İstasyonu Kontrol Ünitesi-Base Station Controller) adı verilen iki kısımdan oluşmaktadır. BTS'ler mobil istasyondan gelen sinyalleri BSC'lere aktarırlar BSC'ler de BTS ile Mobil Anahtarlama Merkezi (MSC-Mobile Switching Center) arasında haberleşme kanalı açarlar.[39]

Şebeke Anahtarlama Sistemi; Abone Kütüğü (HLR-Home Location Register), Ziyaretçi Abone Kütüğü (VLR-Visitor Location Register), Onay Merkezi (AUC-Authentication Center) ve Cihaz Kimlik Kaydı (EIR-Equipment Identiy Register) birimlerinden oluşur. HLR abonelere ait bilgilerin ve abone yönetiminin tutulduğu veritabanıdır. VLR bilgileri ise abonelerin konum bilgilerinin tutulduğu veritabanı olup bu bilgileri HLR'ye bildirir ve bu kayıtlar HLR de tutulur.

---

38 AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. Guidelines on Mobile Device Forensics (Draft). NIST Special Publication, 2013, 800: 101 http://www.engistudio.it/wordpress/wp-content/uploads/NIST.SP .800-101r1.pdf

39 http://tr.wikipedia.org/wiki/Plmn Et: 02.02.2015

Her bir MSC birimi şebeke üzerindeki tüm iletişimi, kayıtları, kimlik otantikasyonunu, alan bilgilerini, bir hücresel ağ içinde bir hücreden diğer hücreye geçiş ve yönlendirme işlemlerini yapmaktadır[40]. MSCde güvenlik ile ilgili bilgilerin tutulduğu iki bölüm mevcuttur. Bu bölümlerden EIR kısmında mobil cihaz istasyon cihaz bilgileri Mobil İstasyonlardaki IMEI(International Mobile Equipment Identity) numarasına göre tutulmaktadır. AUC ise kullanıcı doğrulaması için gerekli olan abone bilgilerini sağlar.

Bir çağrı başlatılacağı zaman MSC Mobil anahtarlama merkezi çağrıyı alır ve Hizmet Kontrol Noktasına(SCP-Service Control Point) iletir. SCP gerekli işlemlerden sonra tekrar MSC'ye bilgi verir. MSC de gerekli talimata göre yönlendirme yapar ya da çağrıyı iptal eder.

B. Mobil Cihaz Donanım ve İşletim Sistemleri

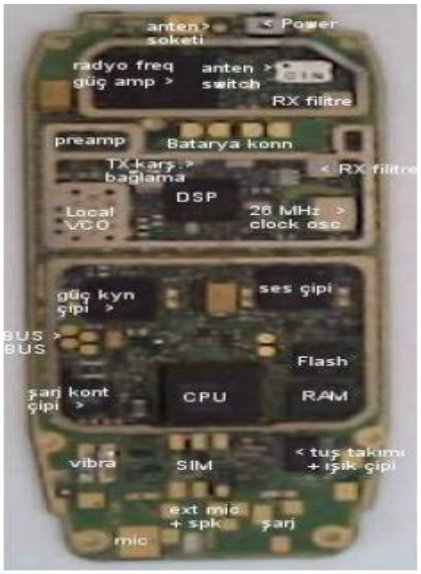
1. Mobil Cihaz Donanım Yapısı

Akıllı telefonlar Mobilete için tasarlanmış olmasından ötürü boyutları küçük, batarya ile çalışabilen hafif cihazlardır. Birçok mobil cihaz bir dizi karşılaştırılabilir özelliğe sahiptir. İçlerinde Mikro işlemci, salt okunur bellek (ROM),rastgele erişim belleği (RAM), Radyo modülü, dijital sinyal işlemcisi, mikrofon ve hoparlör, çeşitli donanımsal tuşlar/anahtarlar ile arayüzler ve LCD ekran mevcuttur.[41]

---

40 AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. Guidelines on Mobile Device Forensics (Draft). NIST Special Publication, 2013, 800: 101 http://www.engistudio.it/wordpress/wp-content/uploads/NIST.SP_.800-101r1.pdf

41 AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. Guidelines on Mobile Device Forensics (Draft). *NIST Special Publication*, 2014, 800: 101. http://www.engistudio.it/wordpress/wp-content/uploads/NIST.SP_.800-101r1.pdf



Şekil 4-Mobil Cihaz Donanım Görüntüsü

Bir mobil cihaz işletim sistemi NAND ve NOR hafızasında saklanabilirken, işlem yürütme ve işlevsellik RAM üzerinde gerçekleşir. Dâhili SD bellek kartı yuvaları sayesinde çeşitli kapasitelere kadar çıkabilen bellek desteği mevcut olabilmektedir. Hücresel olmayan kablosuz iletişim(kızılötesi, bluetooth, Nfc) ve kablosuz ağ (Wi-Fi) kabiliyetinin olması sayesinde çok çeşitli veri tiplerinin (grafik, ses, video ve çeşitli dosya formatları) paylaşımı mümkün olabilmektedir.

Farklı mobil cihazlar farklı teknik ve fiziksel özellikleri barındırır (boyut, ağırlık, işlemci hızı ve bellek kapasitesi. Mobil cihazlar ek işlevsellik sağlamak adına çeşitli genişleme yetenekleri sunabilir. Ayrıca mobil cihazlar küresel konumlandırma sistemi (GPS), kameralar (foto-kamera, video kamera) veya kişisel bilgisayarların imkân kabiliyetlerini de içerebilir. Genel olarak mobil cihazların birincil amaçları ses ve mesaj iletişimi olsa da özellikli telefon ve ya çok daha ileri seviyede özelliklere haiz ve kişisel bilgisayarlardakine benzer multimedya servislerini içeren akıllı telefonlar olarak sınıflandırılabilir.

Tablo-1'de akıllı olmayan (feature Phone) ile akıllı telefon (smart Phone) arasındaki genel donanım özelliklerini bahse konu çeşitliliği vurgulayacak şekilde listelenmiştir.[42]

Donanım Karşılaştırılması		
	Normal Telefon	**Akıllı Telefon**
İşlemci	Limitli 52 Mhz	1 Ghz ve Yukarısı
Bellek (RAM)	Limitli 5 Mb	128 GB
Ekran "Display" Ölçüleri	Küçük Ekran (4k-260k -12 bit 18 bit	Geniş Ekran 5,5 inç
Kart Girişi "Card Slot"	_	microSD, 64GB
Kamera "Camera"	_	HD (Video Kamera)
Klavye "Text Input"	Sayısal Klavye	Dokunmatik Multitouch Ekran
Ses Girişi "Voice Input	_	+
Hücre Arabirimi "Cell Interface"	Ses ve Data Limitli	Yüksek kapasiteli Ses ve Data (4G LTE)
Konum Bilgisi "positioning"	_	GPS
Wifi "Wireless"	Irda, Bluetooth	Bluetooth, Wifi,Nfc
Pil "Battery"	Li-Ion	Li-Ion

Tablo 1-Normal telefon ile Akıllı Telefon Donanım Özellikleri[43]

Akıllı telefonlar ses ve mesaj iletişim protokollerine ek olarak, temel kişisel bilgi yönetimi (PIM-Personal Information Management) uygulamaları olan telefon rehberi ve takvim gibi uygulamalarını da desteklemekte olup kişisel bilgisayarlardakine benzer olarak çok geniş yelpazede genel ve çok özel amaçlara hizmet eden uygulamaları çalıştırabilmektedir. Akıllı telefonlar fiziksel olarak biraz daha büyük olmakla birlikte daha yüksek video çözünürlüğünü desteklemekte ve dokunmatik ekran özelliğine sahip olmaktadır. Akıllı telefonlar bir uygulama mağazası araçlığıyla indirilebilen çok çeşitli uygulamaları çalıştırmayı desteklemektedir. Örneğin (Google Play vs.)

42 AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. Guidelines on Mobile Device Forensics (Draft). NIST Special Publication, 2013, 800: 101 http://www.engistudio.it/wordpress/wp-content/uploads/NIST.SP_.800-101r1.pdf

43 AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. Guidelines on Mobile Device Forensics (Draft). NIST Special Publication, 2013, 800: 101 http://www.engistudio.it/wordpress/wp-content/uploads/NIST.SP_.800-101r1.pdf

Tablo-2'de normal telefon ile akıllı telefon arasındaki uygulama yazılım yetenekleri listelenmiştir.[44]

Yazılım Karşılaştırılması		
	Normal Telefon	**Akıllı Telefon**
İşletim Sistemi	–	Android, İOS, BlackBeryy, Windows Phone, Symbian
Kişisel Bilgi Yönetimi	Rehber, Takvim	Gelişmiş Rehber, Takvim, Hatırlatıcı
Uygulama Yönetimi	–	Gelişmiş uygulama, Oyun, office desteği
Arama türü	Ses	Ses, Video
Mesaj	Text	Text, Çok
Web	_	http,https

Tablo 2-Normal telefon ile Akıllı telefon yazılım Özellikleri[45]

Normal telefonlarda genellikle dokümantasyonu yayınlanmış kapalı işletim sistemleri kullanılır. Gömülü yazılımlar üzerine uzmanlaşmış birkaç şirket, mobil cihaz üreticileri için gerçek zamanlı çalışabilen işletim sistemleri sunmaktadır. Akıllı telefonlar tescilli veya açık kaynak kodlu bir işletim sisteminden herhangi birini kullanabilirler. Yaygın olarak akıllı telefonlarda kullanılan işletim sistemlerini şu şekilde sıralayabiliriz: Android**,** IOS, Windows Phone, Blackberry, Symbian, WebOs. Normal telefondan farklı olarak bu işletim sistemleri ileri seviye mobil cihazların imkân kabiliyetlerini yakalayabilecek şekilde ileri seviye eş zamanlı çoklu iş yapabilme kabiliyetine(multitasking) haiz ve çok yönlü (full-featured) sistemlerdir. Birçok akıllı telefon işletim sistemi üreticisi yazılım geliştirme kiti (SDK-Software, Development KIT)'nide beraberinde sunmaktadır.

44 AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. Guidelines on Mobile Device Forensics (Draft). NIST Special Publication, 2013, 800: 101 http://www.engistudio.it/wordpress/wp-content/uploads/NIST.SP_.800-101r1.pdf

45 AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. Guidelines on Mobile Device Forensics (Draft). NIST Special Publication, 2013, 800: 101. http://www.engistudio.it/wordpress/wp-content/uploads/NIST.SP_.800-101r1.pdf

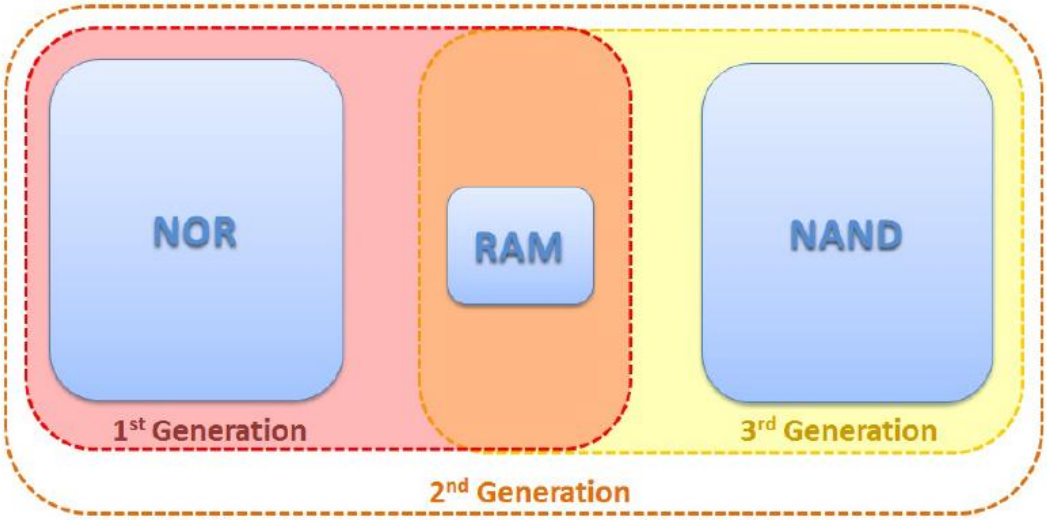
a) Hafıza hususundaki değerlendirmeler:

Mobil cihazlar hem kalıcı hem de geçici bellek içerebilir. Geçici bellek(RAM) dinamik depolama için kullanılan ve işlem sonunda içeriği kaybolan bellektir. Kalıcı bellek ise mobil cihazda mevcut güçten ve telefon açılırken boot işlemi esnasındaki işlemlerden etkilenmeyen hafızadır.

Mobil cihazlar genel olarak iki farklı kalıcı bellek içerir(NAND ve NOR). NOR daha yavaş okuma/yazma özelliği sunarken neredeyse veri bozulmalarına ve disk blok hatalarına karşı bağışıklık gösterir ve herhangi bir hafıza alanına rastgele erişime müsaade eder. NAND bellek ise daha büyük kapasiteli ve daha az istikrarlıdır. Sadece sıralı erişime müsaade eden bir yapı sunmaktadır. Mobil cihazlar arasında bellek yapılandırmaları zamanla gelişmiştir. Normal telefonları NOR flaş ve RAM bellek içeren ilk türler arasındadır. Sistem ve kullanıcı verileri NOR da saklanır ve daha hızlı kod çalıştırma ve erişim için önyükleme esnasında RAM'e kopyalanır. Bu bellek yapılandırmaları arasında ilk nesil olarak bilinir.

Akıllı telefonların buluşu ile birlikte bellek yapılandırmaları da gelişmiştir ve NAND flaş bellek yapısına geçilmiştir. NOR, NAND ve rastgele erişim bellek (RAM) yapısının birlikte kullanılması 2.nci jenerasyon olarak bilinir. Bu jenerasyonda sistem dosyaları NOR flaş da saklanırken, kullanıcı dosyaları NAND yapıda saklanır ve işlemler ise RAM üzerinde yapılır.

Son sürüm akıllı telefonlar ise sadece NAND ve RAM hafızasına sahiptir. Çünkü bu yapılar daha yüksek işlem süratine ve bellek kapasitesini daha ucuza sunar. Mobil cihazın alakartında bulunan düşük hafıza kapasitesi sorununu çözmek ve daha yüksek boyutlu alan (2- 128 Gb) ile kullanıcıları desteklemek için gömülü multimedya kartları (EMMC) tipinde çipler günümüz akıllı telefonlarındaki yerini almıştır. Aşağıdaki şekilde mobil cihaz bellek yapısı gösterilmiştir.



Şekil 5-Akıllı Telefon Hafıza Yapısı

Kalıcı olmayan yapısından ötürü RAM, doğru bir şekilde yakalanması, sabit şekilde muhafaza edilmesi en zor olan hafıza tipidir. RAM işlemlerin icrası maksadıyla kullanıldığıdan içerdiği bilgi (yapılandırma dosyaları, şifreler vb.) inceleme yapan kişi için çok önemli olabilir.[46]

NOR flaş belleği işletim sistemi, kernel, cihaz sürücüleri, yazılım kütüphanesi, uygulamalar ve kullanıcı çalıştırma talimatları gibi verileri içerir. 1.nci nesil hafızaya sahip olan cihazlarda NOR flaş bellek kanıt toplamak için en iyi alandır. **Şekil 3-6'da** görüldüğü üzere 2.nci nesil belleklerde de kanıt maksatlı bilgilere NOR tarafından ulaşılabilir.

NAND flaş bellek de grafik, ses, video ve diğer veri dosyalarını içermektedir. İnceleme yapan kişi için çok faydalı bilgiler içermekedir. Çok çeşitli verilerin kopyalarını işlem tabanlı dosyaları (örneğin veritabanı ve günlük kayıtlarını) muhafaza edebilmektedir.[47]

---

46 AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. Guidelines on Mobile Device Forensics (Draft). *NIST Special Publication*, 2013, 800: 101. http://www.engistudio.it/wordpress/wp-content/uploads/NIST.SP_.800-101r1.pdf

47 AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. Guidelines on Mobile Device Forensics (Draft). *NIST Special Publication*, 2014, 800: 101. http://www.engistudio.it/wordpress/wp-content/uploads/NIST.SP_.800-101r1.pdf

b) SIM Hakkında değerlendirmeler:

SIM kart, cep telefonlarının GSM servis sağlayıcısının telefon hizmetinden yararlanmasını sağlayan, abone kimlik bilgilerini ve telefon defterini barındıran bir mikroçiptir. SIM sözcüğü, İngilizce **S**ubscriber **I**dentity **M**odule (Abone Kimlik Modülü) sözcüklerinin baş harflerini temsil etmektedir[48]. Abone hakkında önemli bilgiler içerir. İki ayrı bileşen ile ifade edilir: Evrensel Entegre Devre Kartı(UICC-Universal Integrated Circuit Card) ve Mobil Ekipman (ME-Mobile-Equipment)[49].

UICC'nin resmi tanımı The European Telecommunications Standards Institute (ETSI) tarafından 25 Haziran 2014'te yapılmıştır[50.] UICC'nin üzerinde telefon defteri, mesajlar, son aranan numaralar ve servis sağlayıcı bilgileri yer almaktadır. Ayrıca UICC'nin cihazdan ayrılabilmesi GSM standartlarına bir portatiftik katmıştır. UICC'nin başka cihaza takılması ile kullanıcı ile ilişkili kimlik bilgileri otomatik olarak diğer cihaza taşınmaktadır.

Bir UICC üç farklı tip uygulama içerebilir: SIM, USIM ve CSIM. GSM ve UMTS cihazlarda SIM ve USIM kullanırken CDMA cihazlar ise CSIM uygulamalarını kullanmaktadır.

UICC 16 ile 128 Kb arasında kalıcı olarak elektriksel silme yapılabilen ve programlanabilen salt okunur belleğe ve bir işlemciye haiz özellikli kart tipidir[51]. Ayrıca uygulamaların çalışabilmesi için RAM ve IOS, kullanıcı doğrulama işlemleri, veri silme algoritmaları ve diğer uygulamalar için ROM'a sahiptir. Mobil cihazın türüne bağlı olarak UICC üzerinde bulunan bilgiler aynı zamanda mobil cihazın hafızasında bulunabilir. Bu veriler UICC'nin dosya sisteminde olabileceği gibi tümüyle mobil cihazın hafızasında olabilir. **GSM** özellikli cep telefonları SIM **Kart** ile çalışırlarken CDMA cep telefonları **SIM** Kartı olmadan çalışabilirler. GSM özelliğine sahip cihazlar SIM kartsız arama yapamaz, internete bağlanamazlar. SIM kartlar (subscriber identy modüle card-abone kimlik modülü)

---

48 ETSI TR 102 216". Retrieved 25 June 2014 http://www.etsi.org/deliver/etsi_tr/102200_102299/102216/03.00.00_60/tr_102216v030000p.pdf

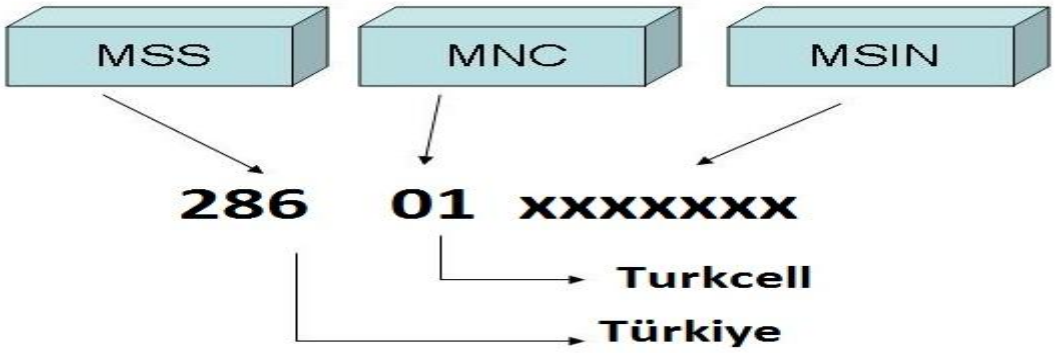
49 http://tr.wikipedia.org/wiki/SIM_kart/ Et:01.02.2015

50 http://en.wikipedia.org/wiki/Universal_Integrated_Circuit_Card Et:01.02.2015

51 AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. Guidelines on Mobile Device Forensics (Draft). NIST Special Publication, 2013, 800: 101. http://www.engistudio.it/wordpress/wp-content/uploads/NIST.SP_.800-101r1.pdf

telefon numarası ve güvenlik gibi kritik bilgilerini üzerindeki küçük bir çip sayesinde barındırır.

SIM kart üzerinde Uluslararası Mobil Abone Kimliği (IMSI-International Mobile Subscriber Identy) SIM kodu ve IMSI kodunun doğrulanmasını sağlayacak **doğrulama anahtarı** bilgisi bulunmaktadır. IMSI telefon numaranızın SIM Kartınızdaki tanımlamasıdır. Mobil sistemlerin üzerindeki bu temel numara 15 karakterdir ve numaralandırma mantığı aşağıda belirtilmiştir:



Şekil 6-SIM Kart IMSI Kod Şeması

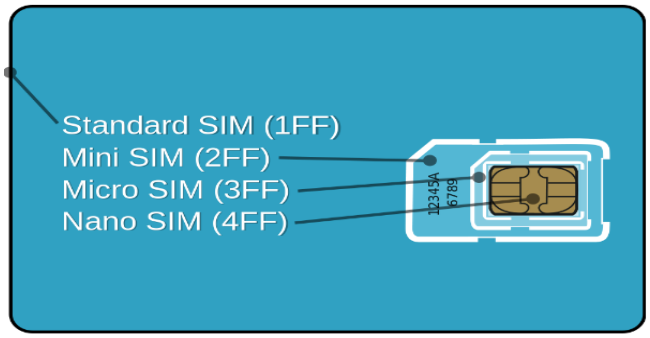
İlk 3 rakam: Ülke Mobil Arama Kodu (MCC-Mobile Calling Code) – Türkiye için 286

Diğer 2 rakam: Mobil Ağ Kodu (MNC-Mobil Network Code): GSM operatörünün ülke içindeki kodu– Avea=03

Sonraki 10 rakam: Operatörün kendisinin belirlediği bir değişken **Sonuç:** MCC – MNC – değişken => 287 05 xxxxxxxxxx

UICC'ler Mini SIM (2FF), Mikro SIM (3FF) ve Nano SIM (4FF) olmak üzere 3 çeşittir. Mini SIM şu anda dünya çapında kullanılan en yaygın biçimdir. Mikro (12mm x 15mm x 76mm) ve Nano (8,8 mm'lik x 12.3mm x. 67mm) SIMS yeni mobil cihazlar (örneğin, Iphone 5 4ff kullanır) bulunur.[52]

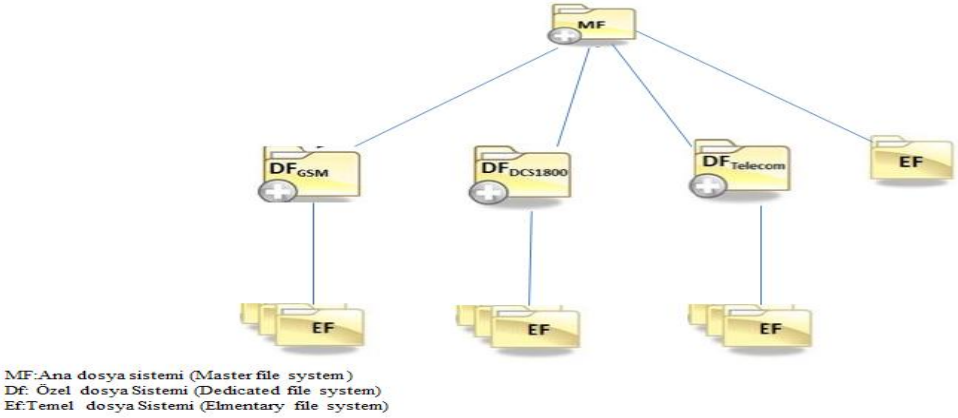
52 http://www.elektrikport.com/teknik-kutuphane/sim-kart-nasil-calisir/14617#ad-image-3/ Et:03.02.2015



Şekil 7-SIM Kart Çeşitleri ve Boyutları[53]

Akıllı telefonlardan önce 25x15 mm boyutlarındaki Mini SIM Kartlar kullanılmaktaydı. Fakat sürekli değişime tabi olan SIM kartlar akıllı telefonların yaygınlaşması ile boyutları küçülerek 15 x 12 mm boyutlarında ve standart 0.76 mm kalınlığında Nano SIM olarak kullanılmaya başlanmıştır.

Ayrıca UICC üzerinde mobil cihazlardaki gibi kalıcı ve kalıcı olmayan bellek mevcuttur. SİM kartlarda hiyerarşik bir dosya sistemi mevcut olup örnek bir SIM kart dosya sistemi aşağıda sunulmuştur.



Şekil 8-SIM kart Dosya Sistemi[54]

53 http://www.elektrikport.com/teknik-kutuphane/sim-kart-nasil-calisir/14617#ad-image-0 Et:03-02.2015

54 AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. Guidelines on Mobile Device Forensics (Draft). *NIST Special Publication*, 2014, 800: 101. http://www.engistudio.it/wordpress/wp-content/uploads/NIST.SP_.800-101r1.pdf

Ana Dosya Sistemi (MF-Master File System) kök dosyalarının olduğu en tepedeki klasördür. Altında şekilde görüldüğü gibi üç farklı ana Özel Dosya Sistemi(DF-Dedicated File System) barındırır. MF ve DF'lerin her birinin altında ise Temel Dosya Sistemi(EF-Elementary File System) bilgileri bulunmaktadır.

2. Mobil Cihaz İşletim Sistemleri

Bütün elektronik cihaz üzerinde donanımın kontrolünü sağlayan ve komutları yerine getiren bir yazılım bulunmaktadır. Teknolojisi gelişmekte olan bu cihazların da daha gelişmiş bir yazılım teknolojisi ile kontrol edilmesi gerekir. Zamanla çok basit yazılımlar ile çalışan cihazlar artık daha gelişmiş yazılım sistemlerine dönüşmüştür.

Strategy Analytics tarafından yayınlanan rapora göre 2014'ün ikinci çeyreğinde 295 milyon adet cihaz satışı gerçekleştirilmiştir[55].

Global Smartphone OS Shipments (Millions of Units)	Q2 '13	Q2 '14
Android	186.8	249.6
Apple iOS	31.2	35.2
Microsoft	8.9	8.0
Blackberry	5.7	1.9
Others	0.5	0.5
		295.2

Şekil 9-2013 -2014 Akıllı Telefon Satış Oranları[56]

Global Smartphone OS Marketshare %	Q2 '13	Q2 '14
Android	80.2%	84.6%
Apple iOS	13.4%	11.9%
Microsoft	3.8%	2.7%
Blackberry	2.4%	0.6%
Others	0.2%	0.2%
Total	100.0%	100.0%

Şekil 10-Akıllı Telefonların Pazardaki Oranları[57]

a) Android

Open Handset Allience (OHA) ve Google tarafından yazılmış açık kaynak kodlu bir işletim sistemi olup, Linux (2.6 kernel) çekirdeğine dayanmaktadır[58].

---

55 http://blogs.strategyanalytics.com/WSS/post/2014/07/30/Android-Captured-Record-85-Percent-Share-of-Global-Smartphone-Shipments-in-Q2-2014.aspx Et:13.12.2014

56http://www.log.com.tr/mobil-isletim-sistemlerinin-2013-kullanim-oranlari-yayinlandi/ Et:13.12.2014

57http://www.log.com.tr/mobil-isletim-sistemlerinin-2013-kullanim-oranlari-yayinlandi/ Et:13.12.2014

Tam manasıyla Linux sistemlerde bulunan özellikleri ve parçaları tam barındırmadığı için tam manasıyla bir Linux işletim sistemi olarak sayılmaz.

(1) Android mimarisi.

Android İşletim sistemi versiyonları android Market ile piyasa sürülmekte olup, çoklu dokunuş (multitouch),çoklu- görev (multitasking) ve flaş desteği ile birlikte birçok uygulama üzerinde çalıştırabilmektedir. Android işletim sistemi sistem kütüphaneleri, çekirdek (kernel), uygulama geliştirme (frameworks) ve yerleşik uygulamalardan oluşmaktadır. Aşağıda Şekil-12 de Android mimarisi gösterilmiştir.

Şekil 11-Android Mimarisi[59]

(2) Temel yapısı

Android işletim sistemi kernel olarak Linux çekirdeğini kullanmaktadır. Android için eklenen kodlar ve kütüphaneler Genel Kamu Lisansı (GNU) altında özgür/bedava bir şekilde dağıtılmaktadır.

Linux çekirdeği doğrudan cihaz sürücülerine ve temel yapılar olan güvenlik, süreç ve hafıza dosyalama kontrolü ile bağlantı için girdi-çıktı işlemlerine doğrudan kaynak sağlamaktadır. Android çekirdeği için özelleştirilmiş başlıca alanlar ise paylaşılan hafıza ve güç kontrolüdür.

(3) Kütüphaneler (Libraries)

Android mimarisinin en önemli yapısı olan kütüphaneler C programlama dili ile yazılmıştır. Sistem kütüphaneleri aşağıda belirtilmiştir;[60]

---

58 Android Inc. (n.d.). *What is Android|Android Developers*. Retrieved May 23, 2010, from Android Developers: http://developer.android.com/guide/basics/what-isandroid.html

59https://gelecegiyazanlar.turkcell.com.tr/konu/android/egitim/android-201/android-mimarisi-ve-sistem-ozellikleri Et:13 Aralık 2014

- İnternet tarayıcısı motorlarının çalışması için Webkit,
- Görüntüleme yapması için oluşturulan **Surface Manager**,
- Grafik işlemleri yapan OpenGL,
- Ses ve video işlemleri yapan **Media Framework**,
- Veri yapıları kontrolü ve düzenlenmesi yapan SQLite

gibi yapılar bu katmanda bulunmaktadır.

(4) Android Runtime:

Bu katman Linux çekirdeği kütüphanelerinin Java ile birleştiği katman olup önemli iki bileşeni vardır. Bunlardan biri temel Java kütüphaneleri ve diğeri de çalışan Dalvik Sanal (virtual) Makinesidir.

Cep telefonu üzerindeki tüm uygulamalar sanal "Dalvik Sanal Makinesi" tarafından çalıştırılır. Java ile yazılan uygulamalar alınır, Java kodları derlenerek bytecode dosyalarına çevrilir ve bu dosyalar dex dosyasına çevrilerek Dalvik Sanal Makinesi'nin anlayacağı/çalıştırabileceği şekilde derlenir.[61]

Android işletim sistemi veri depolama amaçlı SQLite, mobil iletişim olarak GSM, 3G, Bluetooth, EDGE ve Wi-Fi bağlantılarını desteklemektedir. Android açık kaynak kodlu WEB KİT application framework üzerine kuruludur. Birçok multimedya, ses, resim ve video dosya formatını (MPEG-4, MP4, MP3, H.264 ve AAC, AMR, JPEG, PNG, GIF vb.) destekler.

Android işletim sistemleri gelişmiş Uygulama Programlama Arayüzleri (API -Application Programming İnterface) sayesinde uygulama geliştirmek isteyenlere kolaylıklar tanımaktadır. Uygulama geliştirme dili Java olan Android API'lerine örnek olarak yüz tanımlama ve çeşitli uygulamalar gösterilebilir. Java'nın Android İşletim sistemine başarılı bir şekilde entegre olması nedeniyle java geliştiricileri rahatlıkla android uyumlu uygulama geliştirebilmektedir. Android Geliştirici KİT'i(SDK), Java Geliştirici KİT'i (JDK), Eclipse için

---

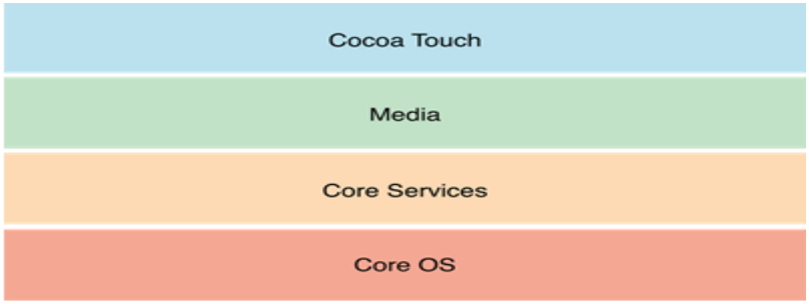
60https://gelecegiyazanlar.turkcell.com.tr/konu/android/egitim/android-201/android-mimarisi-ve-sistem-ozellikleri Et:13 Aralık 2014

61https://gelecegiyazanlar.turkcell.com.tr/konu/android/egitim/android-201/android-mimarisi-ve-sistem-ozellikleri Et:13.12.2014

Android Geliştirici Araçları Yongasının(ADT-Android Devolopment Tools Plugin) yüklü olması yeterlidir.

b) IOS

Apple firması tarafından geliştirilmiş olan Mac OS X (Unix türevli) işletim sistemidir[62]. Yalnızca Apple ailesi içinde üretilmiş cihazlar tarafından kullanılabilmektedir. İlk sürümlerinde üçüncü tarafların geliştirdiği uygulamaları desteklenmiyordu. Ardından üretilen sürümlerde bu katı kapalı tutumdan vazgeçilmiştir. Çekirdeği ve sistem kütüphaneleri ARM işlemciye göre modifiye edilmiştir. iOS temelde 4 katmandan oluşmaktadır. Bu katmanlar **Core OS**, **Core Services**, **Media ve Cocoa Touch** katmanlarıdır.



Şekil 12-IOS Mimarisi[63]

(1) Core OS katmanı:

İşletim sisteminin temel katmanıdır. Diğer katmanlar bu teknolojilerin üzerine inşa edilir. Donanım katmanına en yakın olan katman[64]. Çekirdek (Kernel), sürücüler, alt seviye arayüzler (low-level interface), güvenlik yapıları, cihaza bağlanabilen tüm cihazlar, aksesuarlar Core OS katmanına yönlendirilir.

(2) Core Services katmanı:

Uygulamaların çalışması için gerekli servisler bu katmandadır. Kullanıcı oturum açma işlemlerini yöneten Accounts Framework, depolama kütüphanesi

62 Apple Inc(n.d) *iPhone Technologies Overview*.Retrieved May 22,2010,from iPhone Referenceibrary:http://developer.apple.com/iphone/library/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/iPhoneOSTechnologies/iPhoneOSTechnologies.html#//apple_ref/doc/uid/TP40007898-CH3-SW1 Et:13.12.2014

63https://developer.apple.com/library/ios/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/Introduction/Introduction.html Et:25.12.2014

64 http://www.oguzhantopgul.com/2014/01/guvenlik-arastrmalar-odakl-ios-temelleri.html Et:25.12.2014

olan SQLite, alan yer bilgisi ve lokasyon işlemlerini yöneten Core Location Framework, adres defterini yöneten Address Book Framework, temel telefon işlemleri için API sunan Core Telephone Framework, telefon ayalarını yönetmek için API sunan System Configuration Framework gibi işlemlerin gerçekleşmesini sağlayan katman **Core Services** katmanıdır.

(3) Medya katmanı:

Telefon üzerinde ses, görüntü ve video işlemleri ile alakalı kütüphanelerin olduğu katmandır. iOS için önem arz eden Core Graphics, Media Player, Core Media, Core Audio, Core Video, OpenGL gibi kütüphaneler bu katmanda bulunur.

(4) Cocoa Touch katmanı:

Yüksek seviyeli sistem servislerinin yer aldığı, dokunmatik ekran, geri-bildirimler, eş zamanlı çoklu işlemler gibi önemli servislerin yer aldığı uygulama katmanıdır[65].

(5) İşlemciler:

Akıllı telefonlarda iki adet işlemci bulunmaktadır. Bunlardan biri telefonun bilgisayar gibi özelliklerini; diğeri de telefonun baz istasyonu ve operatör ile ilgili işlemlerini yönetmek için kullanılmaktadır. Akıllı telefonları, telefon ve bilgisayarın birleşmiş hali olarak değerlendirmek gerekirse hem telefon özelliği hem de bilgisayar özelliği için birer işlemciye ihtiyacı vardır. Bu işlemciler Uygulama İşlemcisi(**Application Processor)** ve Baz İşlemcisi(**Baseband Processor)** olarak adlandırılırlar.

Uygulama İşlemcisi telefon haberleşmesini ve GSM dışındaki işlemleri yürütmek için kullanılmakta olan işlemcidir. Bütün uygulamaları ve işletim sisteminin kontrolü bu işlemci tarafından sağlanmaktadır.

Baz İşlemcisi aynı zamanda İletişim İşlemcisi (Communication Processor) olarak da bilinir. GSM-anten gerektiren işlemleri yürüten işlemcidir. Bu işlemcinin kendi RAM'i ve NOR flaş depolama kısmı bulunmaktadır. SIM kilidi bulunan bir cihazın kilidini açmak için Baseband firmware 'ine işlem yapmak gerekmektedir.

65http://www.oguzhantopgul.com/2014/01/guvenlik-arastrmalar-odakl-ios-temelleri.html Et:25.12.2014

Depolama (Storage) iOS üzerinde NAND flaş olup bu alanda iki adet bölüm vardır: Birinci bölümde kullanıcı dosyaları ikinci bölümde ise sistem dosyaları mevcuttur.

Sistem Bölümü: iOS işletim sistemi ve işletim sistemine ait uygulamaların bulunduğu kısımdır. Sistem bölümü salt okunurdur. Bir iOS cihaza SSH yapılıp **kök** dizin altına gidildiğinde bir **Applications(uygulama)** dizini görülür[66]. Bu dizinin içerisindeki uygulamalar sistem bölümündeki uygulamaları kapsar. Mesajlaşma, telefon, haritalar vs. gibi işletim sistemi uygulamaları bu dizinde bulunmaktadır.

Kullanıcı Bölümü: Cihazlarda **/private/var** dizini altındaki yazılabilir bölüm kullanıcı bölümü olarak bilinmektedir. **User** dizini (**/private/var/mobile** dizini) altında da uygulama "**Applications"** dizini vardır. Bu dizinde ise kullanıcının yüklemiş olduğu uygulamalar mevcuttur. Üçüncü taraf uygulamalar burada tutulmaktadır[67]. Telefona yüklenen her uygulama **UUID** adı verilen eşsiz bir dizine yüklenmektedir. **/private/var/mobile/Applications** altına erişildiğinde bu dosyalar görülebilir. Uygulamaların kurulduğu bu dizinin/klasörün ismi dinamik olarak her yüklemede, yükleme sırasında oluşturulmaktadır. Bu uygulamalar cihazdan kaldırılıp tekrar kurulduğunda bu dizin ismi değişmektedir. Böylece saldırganların uygulamalar hakkında bir çıkarım yapmalarının önüne geçilmeye çalışılmıştır.

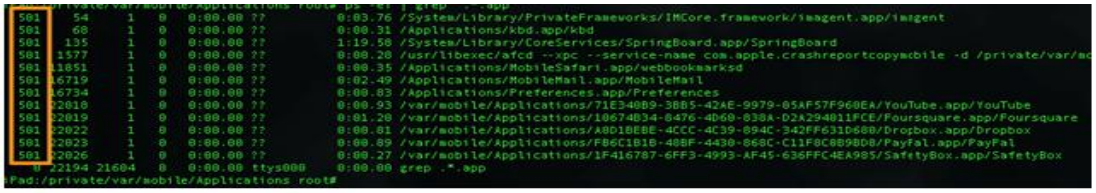
Kullanıcılar: iOS işletim sisteminde temelde iki adet kullanıcı vardır. Bunlar **root** ve **mobile olarak tanımlanmaktadır.**[68] **Root** iOS daki yetkili kullanıcı hakkı ile çalışmaktadır. **Mobile isimli kullanıcısı ise root** kullanıcısının yürüttüğü işlemler dışındaki tüm işlemlere mobile adı verilen düşük yetkili bu kullanıcı ile yapılmaktadır. Çalıştırılan tüm uygulamalar mobile gurubuna ve mobile kullanıcısına atanmaktadır. iOS 'ta bütün uygulamalar mobile kullanıcısı ile çalıştırılır. Aksine Android uygulamaların her bir yeni bir kullanıcı ile çalıştırılmaktadır. Ancak bu sebeple "sandbox" mekanizmasının düzgün çalışması çok önemli olup Sandbox mekanizmasında oluşabilecek bir problemde tüm uygulamaların mobile kullanıcısı ile oluşturulması durumu nedeni ile diğer bir

---

66http://www.oguzhantopgul.com/2014/01/guvenlik-arastrmalar-odakl-ios-temelleri.html Et:05.01.2015
67http://www.oguzhantopgul.com/2014/01/guvenlik-arastrmalar-odakl-ios-temelleri.html Et:05.01.2015
68http://www.oguzhantopgul.com/2014/01/guvenlik-arastrmalar-odakl-ios-temelleri.html Et:05.01.2015

uygulamanın bütün uygulamalara erişim sonucunu doğuracak ve telefon güvenlik noktasında tehlikeye sokacaktır.

Aşağıdaki örnekte görüldüğü gibi çalışan bütün uygulamaların 501 id'li mobile kullanıcısı ile çalıştığı görülebilmektedir[69]. Hatta iOS'un graphical user interface'i SpringBoard'un bile mobile kullanıcısı ile çalıştığı görülmektedir.



Şekil 13-IOS üzerinde çalışan uygulamalar[70]

Her uygulama mobile kullanıcısı ile çalışmakta ancak her uygulamanın sandbox'u farklıdır. Uygulamalar erişmek istedikleri kaynaklara göre yetki verilmekte ve yetkilendirme mekanizması sayesinde hangi uygulamanın nerelere erişebileceği belirtilebilmektedir.

IOS işletim sistemi çoklu görev (multitasking), çoklu dokunma özelliği ve parmak etkileşimi ile çalışacak biçimde tasarlanmıştır. Çok amaçlı uygulama geliştirme ortamı (Iphone SDK) sayesinde uygulamalar yönünden zengin platform sağlamaktadır. Uygulama geliştirmek amaçlı Mac OS yüklü bir bilgisayar gerekmektedir. Flash ve Java desteği yoktur. Çoklu görev (multitasking) özelliği ilk sürümlerde yok iken iOS'un 4.0 sürümü ile bu özellik de eklenmiştir.[71]

c) Windows Mobile

Kavramsal olarak iOS ile benzerlik göstermektedir. Mobil cihazlar için üretilen Windows Mobile Compact Edition (CE) çok gelişmiş bir altyapıya sahip

---

69http://www.oguzhantopgul.com/2014/01/guvenlik-arastrmalar-odakl-ios-temelleri.html Et:05.01.2015
70http://www.oguzhantopgul.com/2014/01/guvenlik-arastrmalar-odakl-ios-temelleri.html Et:05.01.2015
71http://www.oguzhantopgul.com/2014/01/guvenlik-arastrmalar-odakl-ios-temelleri.html Et:05.01.2015

olmasına rağmen Windows tabanlı masaüstünde kullanılan Windows uygulamalarını çalıştıramamaktadır. [72]

İlk sürümünde çoklu dokunuş özelliği bulunmamakla birlikte bu özelliğe 7.nci sürümünde kavuşmuştur. Tek bir cihaza özgü yazılmadığı için optimizasyonu diğer yazılımlara göre düşüktür. Multitasking özelliğini destekler ve C++ tabanlıdır.

Microsoft Office programlarıyla sorunsuz bir uyum içinde çalışmaktadır. Ayrıca multimedya özelliğinin çok gelişmemiş olması nedeniyle rakiplerinin gerisinde kalmıştır**.**

4.MOBİL CİHAZLARDA GÜVENLİK HUSUSLARI

Mobil cihazlar günlük hayatımızın ayrılmaz bir parçası olmuş durumdadır. Bu cihazlar birçok kişi tarafından kullanılmasına rağmen genellikle tek bir kişiye aittirler. Diğer bir deyişle cihazı birçok kişi kullanır fakat bir problem yaşanması durumunda sorumluluk o cihazın sahibine aittir.

Mobil cihazlar arama geçmişi, kısa mesaj, e-posta, dijital fotoğraf, video, takvim öğesi, hatırlatıcı not, adres bilgisi, şifre, kredi kartı numarası vb. birçok kişisel bilgi içermektedir. Bu cihazlar iletişim kurmanın yanısıra; fotoğraf paylaşımı, sosyal ağ ve bloglara bağlanmak, not almak, video ve ses kaydı tutmak, internete bağlanmak vb. için kullanılabilir. Bu cihazlar yaşantımızın ayrılmaz bir parçası haline geldikleri için herhangi bir zaman diliminde kişinin nerede bulunduğu bilgisini belirlemek bu cihazlar vasıtasıyla sağlanabilir.

Mobil cihazlarda hafızasında sürekli olarak kayıt altına alınan bazı bilgiler (örneğin arama ve aranma kayıtları, zamana bağlı mevkii bilgileri, kısa mesajlar vs.) bu kişilerin kimlerle iletişim halinde olduklarını, ne hakkında iletişim kurduklarını ve nerede bulunduklarını ortaya çıkararak bir araştırma sürecinde önemli bazı soruların irdelenmesinde ve çözümlenmesinde yardımcı olabilirler.[73]Örneğin Teröristler tarafından keşif yapmak ve koordinasyon kurmak amacıyla, sınır ötesinde kaçakçılık yapmak için kullanılabilen ve yasak olmasına

---

72 Casey, E., Bann, M., & Doyle, J. (n.d.). Introduction to Windows Mobile Forensics. Digital Investigation Volume 6, Issues 3-4, Pages 136-146, May 2010 http://www.famu.edu/cis/p156-yates.pdf Et:05.01.2015

73 CASEY, Eoghan; TURNBULL, Benjamin. Digital evidence on mobile devices. *Eoghan Casey, Digital Evidence and Computer Crime. Third Edition. Forensic Science, Computers, and the Internet, Academic Pres*, 2011. http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf Et:25.10.2014

rağmen hapishanelerde de bulundurulan mobil cihazlar, cinayetlerin çözümünde de etkili olmaktadırlar. Mobil cihazların bu kadar çok kayıt barındırdıklarının farkında olmayan kişiler şüpheli duruma düştüklerinde mobil cihazlarındaki bilgiler suçlayıcı dijital deliller barındırabilir ve bahse konu bilgiler ciddi suçlarda etkili olabilmektedirler.

Yaşanmış Örnek Vaka: Yanlışlıkla Yapılan Aramayla Çözülen Cinayet

Karısının başka biriyle ilişkisi olduğunu öğrenen Ronald Williams hiddet anında karısı Mariama'yı öldürdü. William'ın cep telefonu, suçun işlendiği anda kendisi fark etmeden karısının cep telefonunu aradı ve arama sesli mesaja düştü. Karısının sesli mesaj kaydı, William'ın karısını öldüreceğini söylediğini, karısının çığlıklarını ve 2 yaşındaki kızın durması için babasına yalvarışını kaydederek William'ın yakalanmasına yardımcı oldu[74]

Akıllı cihazların kontrolsüz olarak kullanımının artması bu cihazların her geçen gün daha çok güvenlik açığı yaratacak bir şekilde kullanılmasını da doğurmaktadır. Örneğin, bazı mobil cihazlar kredi kartı taraması ve bilimsel ölçümler (ör. Voltaj, sıcaklık, hız) gibi veriler elde edilmesi amacıyla uygun hale getirilirler. Bu esneklik üreticilerin amaçlarının ötesinde dallanıp budaklanır ve mobil cihazlar kredi kartlarının çalınması ve bombaların patlatılması için kullanılabilir.[75]

Bu bölümde akıllı telefonların delil kaynağı olarak nasıl kullanılabileceği anlatılacak olup, bu kapsamda kullanılan donanım/yazılımlar ve bu donanım/yazılımların temel işlemleri tanımlamakta, bu cihazlar üzerinde dijital delillerin elde edilmesinde ve incelenmesinde kullanılan donanım, yazılım ve teknikleri sunulmaktadır.

A. Mobil Cihazlar ve Güvenlik

Her alanda olduğu gibi bu alanda da gelişmenin pozitif yönünün yanı sıra doğurduğu riskler de mevcuttur. Mobil cihazlar artık yalnızca telefon rehberi,

---

74 Kruger, 2011). Krueger, C. (2011, February 11). Man found guilty of lesser charge in murder recorded on cellphone http://www.tampabay.com/news/courts/criminal/man-found-guilty-of-lesser-charge-in-murder-recorded-on-cell-phone/1150957

75 CASEY, Eoghan. *Handbook of digital forensics and investigation*. Academic Press, 2009. http://www.google.com.tr/books?hl=tr&lr=&id=xNjsDprqtUYC&oi=fnd&pg=PP2&dq=van+der+Knijff,+Handbook+of+Digital+Forensics+and+Investigation+2009%3B+&ots=X2tNE-aCtL&sig=4yZF_a2v_D1AQfl8OHC5QGabw2c&redir_esc=y#v=onepage&q=van%20der%20Knijff%2C%20Handbook%20of%20Digital%20Forensics%20and%20Investigation%202009%3B&f=false

arama kaydı, kısa mesajlar, fotoğraflar, takvim verileri, notlar ve medya gibi düşük kapasiteli verilerin saklanması için kullanılmanın ötesinde, daha çok veri alanına ihtiyaç duyan e-posta, internet, bankacılık, navigasyon gibi uygulamalar için de kullanılabilmektedir. Bu durum bilgisayarlar için alınan güvenlik önlemlerinin bu alanda da aynı titizlik ve detayda alınması gerektiğini ortaya koymaktadır. Akıllı telefonlar güvenlik noktasında bilgisayar güvenliğini de yakalamış durumda olmayıp, teknik güvenlik önlemleri, firewall (güvenlik duvarı), antivirus ve şifreleme mobil cihazlarda yaygın değil ve bilgisayarlardaki gibi kadar sık bir şekilde güncellenememektedir.[76]

Ne yazık ki pek çok mobil cihaz kullanıcısı mobil güvenlik tehlikelerini bilmemekte ya da güvenlik kurallarını çok fazla önemsememektedir. Hatta kullanıcılar kendi telefonları ile gelen güvenlik yazılımını dahi etkinleştirmekte başarısız olmakta ve bununla birlikte mobil cihazlar ile internette dolaşmanın bilgisayar ile internette dolaşmaktan daha güvenli olduğuna inanmaktadırlar. Bir çalışmada 2009 ve 2010 arası mobil işletim sistemlerindeki güvenlik açıklıklarının yüzde 42 oranında arttığı tespit edilmiştir. Mobil cihazlar üzerindeki çok yönlü saldırı sayıları arttığı ve karşı önlemler alınmakta yavaş kalındığı tespit edilmiştir.[77]

Mobil cihazların donanım ve yazılım olarak gün geçtikçe işlevselliklerinin artması onları saldırıların ve saldırganların hedefi haline getirmektedir. Bu noktada suçun ve suçlunun olduğu bir ortamda mobil cihazların adli bilişim incelemelerinde de kullanılması da daha önemli hale gelmektedir.

Akıllı cep telefonları ve diğer mobil cihazlar arasında "bluetooth, kızılötesi ve kablosuz ağlar" üzerinden bilgi alışverişi imkân ve kabiliyeti olduğundan bu cihazlar üzerindeki veriyi yetkisiz erişimlere karşı izole etme(koruma) ihtiyacı doğmuştur.

Mobil cihazlar çok çeşitli yöntemlerle(dâhili, çıkarılabilir medya aracılığı, çevrimiçi vs.) üzerinde veri saklama ve işleme imkân kabiliyetine sahiptirler. Birçok durumda, mobil cihazdan ve bağlı bulunduğu/ilişkilendirildiği veri

---

76 National Institute of Standards and Technology. "Guidelines on Cell Phone and PDA Security (SP 800-124)." http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf
77 Symantec. "Symantec Report Finds Cyber Threats Skyrocket in Volume andSophistication." http://www.symantec.com/about/news/release/article.jsp?prid=20110404_03

depolama medyasından veriyi elde etmek için birden çok yöntem/cihaz/program kullanılabilmektedir.

B. Mobil Cihazlarda Güvenlik Tehditleri

Mobil iletişim kullanımı kendinden önceki tüm iletişim ve bilgisayar teknoloji sistemlerini geride bırakarak her geçen gün kullanımı artmakta olup basit bir iletişim aracı olmaktan çıkmıştır. Ayrıca bilgi güvenliğinin sadece bir teknoloji sorunu olmadığı fark edilmiş, son yıllarda siber alandaki insan faktörleri de bilgi güvenliği araştırma konusu olmuştur.[78]

Mobil cihazların donanım ve işletim sistemleri neredeyse bilgisayarlarla ile aynı kapasite ve özelliklilere ulaşmış, bu cihazların işlevselliklerinin ve kapasitelerinin artması bilgisayar ortamında yapılan birçok işlemin bu cihazlar ile yapılmaya başlanmasını sağlamış ve kişisel/kurumsal verilerin yetkisiz erişimlerden korunması ihtiyacını beraberinde getirmiştir. Bu nedenle, özellikle mobil bilgi güvenliği alanında, insan faktörünü ve algısını araştırmaya büyük bir talep olmasına neden olmaktadır.[79]

Mobil cihazlar alanında başlıca tehdit yöntemlerini; **kötücül yazılım (malware), doğrudan saldırı (direct attacks), araya girme (data interception), zafiyeti kullanma (exploitation) ve sosyal mühendislik (social engineering)** başlıkları altında toplayabiliriz. Bunların dışında asıl ve en önemli olan kullanıcıların yeterli teknolojik bilgiye sahip olmamasından kaynaklanan güvenlik zafiyetleridir.

Teknolojilerin gelişip yaygınlaşması, günlük işleri elektronik ortamlara taşınmakta ve bilgilerin kolay erişilebilir olmalarını birinci öncelik haline getirmeye başlamaktadır. Netice olarak sayısal ortamlarda bulunan bilgilerin

---

78HASSELL, Lewis; WIEDENBECK, Susan. Human factors and information security. *Manuscript. Available at: http://repository. binus. ac. id/content A*, 2004, 334. http://repository.binus.ac.id/content/A0334/A033461622.pdf

79 HUANG, Ding-Long; RAU, Pei-Luen Patrick; SALVENDY, Gavriel. A survey of factors influencing people's perception of information security. In: *Human-Computer Interaction. HCI Applications and Services*. Springer Berlin Heidelberg, 2007. p. 906-915. https://books.google.com.tr/books?id=BVy5BQAAQBAJ&pg=PA107&dq=Human-Computer+Interaction.+HCI+Applications+and+Services&hl=tr&sa=X&ei=UxshVYKTJ4X5UtaOg6AH&ved=0CB4Q6AEwAQ#v=onepage&q=Human-Computer%20Interaction.%20HCI%20Applications%20and%20Services&f=false

güvenliğinin önemi ve tehditler, gerek sayı gerekse çeşitlilik yönünden artmıştır. Başlıca tehdit yöntemlerini aşağıda başlıklar halinde anlatmaya çalışacağız.

1. Kötücül Yazılımlar (Malware)

Akıllı cihazları tehdit eden malware ve spyware yazılımları üretilmektedir. Kullanıcılar tarafından bu yazılımların ve etkilerinin iyi bilinmesi ve tanınması em önemli korunma tedbiri olup gerekli önlemlerin alınması gerekmektedir.

Malicious software, diğer bir deyişle kötücül yazılım (malware): v**irüs, worm** (*solucan*), **trojan** ve **spyware** (*casus yazılım*) olarak bilinen zararlı yazılımların tümüne verilen isimdir.[80] Bulaştığı sistemlere ağ üzerinden ulaşarak sistemlerin çalışmasını aksatabilmekte veya hiç çalışamaz duruma getirebilmektedir.

Bu yazılımların isimleri "solucanlar (worm) , Truva atları (trojan horse), virüsler, gereksiz mesajlar (spam), rootkitler, klavye girişlerini kayıt edebilen (keylogger)'lar, casus yazılımlar (spyware), tarayıcıyı ele geçirme (browser hijacking) en bilinen genel kötücül yazılımlardır. Neredeyse her programlama dili ile yazılabilmekte ve birçok dosya türü ile sistemlere bulaşabilmektedirler.

2009 ve 2010 yılları arasında, tehditlerde %250 artış olmuş. Neredeyse tüm büyük platformlar kötü amaçlı yazılım hedefleri olmuştur. Örneğin kötücül yazılım içeren SMS kısa mesajlar atmak, arka planda uygulamaları çalıştırılarak faturaların yüksek gelmesi, keylogger ile şifreleri elde etmek ya da kendine kötücül yazılım bulaşan cihazın adres defteri ve diğer bilgilerini göndermesi verebileceğimiz örnekler arasındadır.81

Özellikle internet ve ağ sistemlerinin gelişerek karmaşık hale gelmesi ve kullanımının yaygınlaşarak sistemlerin değişik sebeplerle birbirlerine bağlanması ile bahse konu kötücül yazılımların yazılımlar her geçen gün daha süratli yaygınlaşmaktadır. Sistemlere bulaşan bu yazılımlar bulunup temizlenebilmelerine rağmen verilerin kaybedilmesi, kişisel ve kurumsal itibarlara verilen maddi ve manevi zararlar geri döndürülemeyecek seviyelerde olabilmektedir.

80https://www.bilgiguvenligi.gov.tr/mobil-cihaz-guvenligi/mobil-cihazlarda-guvenlik-android-ve-ios-karsilastirmasi.html Et: 02.09.2014

81 Juniper Networks, 2011, Inc. Mobile Device Security Emerging Threats, Essential Strategies http://www.adtechglobal.com/Data/Sites/1/marketing/juniperwhitepapermobiledevicesecurity.pdf

Sistemlerin bu yazılımlardan korunması konusunda; profesyonel güvenlik uzmanları ve şirketler tarafından yazılan ve geliştirilen; bu tür zararlı öğeleri belirleyip temizleyen; güvenlik açıklarını konusunda tespit/koruma/önleme işlevsellikleri olan yazılımların kullanılmasına rağmen, saldırı yöntemleri de her geçen gün artmakta ve çeşitlenmektedir.

Hâlihazırda kötücül yazılımların doğurabileceği sonuçların farkında olunmaması ve mobil kullanım ortamlarının çok hızlı bir şekilde yaygınlaşması bu cihaz ve sistemlerin büyük bir tehdit altında olmasını gerekliliğini ortaya koymaktadır.

İlk kötücül yazılım olan cabir 2004 yılında ortaya çıkmış olup o dönemin en yaygın Symbian serisi işletim sistemine bluetooth vasıtasıyla zarar vermeyi başarmıştır.[82]

Cabir 29 adlı uluslararası bir grup tarafından geliştirilmiş, bluetooth üzerinden cihazlara bulaşıp kendi kopyalarını oluşturup bulaştığı cihazın pilini bitirme ve etrafındaki cihazları arayarak meşgul etme gibi zararlar vermiştir. Virüsleri bir cihazdan diğerine bulaştırmada Bluetooth ’tan yararlanıldığı gibi diğer yöntem ise MMS kullanılmaktadır. MMS yoluyla bulaşan virüs Commwarrior’dir.[83]

Diğer bir virüs ise Cardtrap olup telefonun hafıza kartına Windows işletim sistemi virüsü bulaştıran kötücül bir yazılımdır hem cep telefonlarda hem de Windows işletim sistemine bulaşan bir virüstür.[84]

Mobil ortamlarda en çok türevi olan ve bulaştığı sistemlere en çok zararı veren diğer bir virüs Skulls virüsüdür. Bulaştığı mobil cihazlarda ikonları

---

82 Mobile Malware Evolution: An Overview,Part1 http://www.viruslist.com/en/analysis?pubid=200119916 Et:18.11.2014

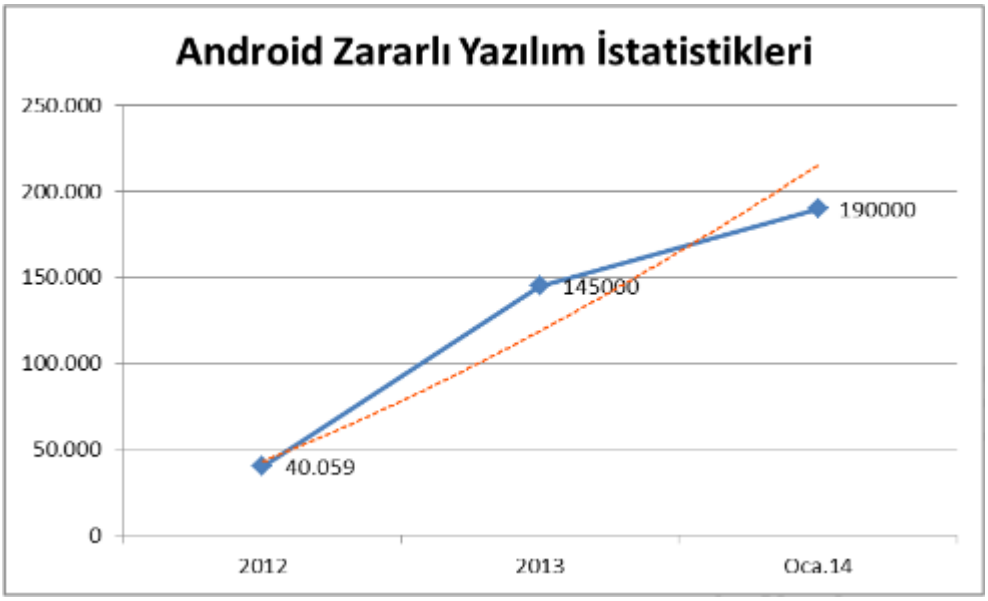
83 SAĞIROĞLU, Şeref; BULUT, Hülya. Mobil Ortamlarda Bilgi Ve Haberleşme Güvenliği Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, 2009, 24.3 s:501-505 http://www.mmfdergi.gazi.edu.tr/article/viewFile/1061000183/1061000154 Et:19.11.2014

84 SAĞIROĞLU, Şeref; BULUT, Hülya. Mobil Ortamlarda Bilgi Ve Haberleşme Güvenliği Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, 2009, 24.3 s:501-505 http://www.mmfdergi.gazi.edu.tr/article/viewFile/1061000183/1061000154 Et:19.11.2014

değiştirerek kafatası ikonu ile değiştiren, uygulama dosyalarını silen Symbian trojanıdır.[85]

Mobil sistemlere bulaşan kötücül yazılımlar incelendiğinde kullanılmakta olan işletim sistemlerinin popüleritesi ile doğru orantılı bir şekilde o platforma yönelik kötücül yazılımların daha yoğun bir şekilde geliştirildiği görülmektedir.

Günümüz itibariyle mobil telefonda kullanılan en yaygın işletim sistemleri Android ve iOS'dur. Bu sebeple özellikle Android ve iOS tabanlı sistemleri etkileyecek virüs ve çeşitleri çok sayıda fazladır. Aşağıdaki tabloda yıllara göre Android zararlı yazılım istatistikleri oranı verilmiştir.



Şekil 14-Android zararlı yazılım istatistiği[86]

2. Doğrudan Saldırı (Direct Attacts)

Doğrudan Saldırı olarak adlandırılan bu yöntemde saldırgan bilinen bir uygulama açıklığını (application vulnerability) ya da işletim sistemindeki açıklığı (OS vulnerability) kullanarak yetkisiz erişim sağlamayı ve bilgi elde etmeyi hedefler.[87]

---

85 SAĞIROĞLU, Şeref; BULUT, Hülya. Mobil Ortamlarda Bilgi Ve Haberleşme Güvenliği Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, 2009, 24.3 s:501-505 http://www.mmfdergi.gazi.edu.tr/article/viewFile/1061000183/1061000154 Et:19.11.2014

86https://www.usom.gov.tr/dosya/1418807372-USOM-SGFF-004-Akilli%20Telefonlar%20ve%20Guvenlik.pdf/ Et:20.O2.2015

87https://www.bilgiguvenligi.gov.tr/mobil-cihaz-guvenligi/mobil-cihazlarda-guvenlik-android-ve-ios-karsilastirmasi.html Et:20.O2.2015

Bu saldırı türünde en fazla **SQL (***SQL injection*) **enjeksiyonu** ve dışarıdan gelen bağlantıları kabul eden servis zafiyetleri yöntemleri kullanılır. Mobil cihazlar genel kullanıma açılmış bir wi-fi ağı üzerinden internete bağlıyken bir de hotspot gibi bir yazılım ile internete çıkıyorsa çok rahatlıkla bir saldırgan tarafından ip' si tespit edilerek saldırganların hedefi olabilir.

Bu cihazlara hizmet aksatması olarak bilinen Dos (Denial of Service) saldırısı yapmak mümkün olabilmekte ve cihaz kullanılmaz hale getirilebilmektedir. Ya da cihazın arka plan da kullandığı kullanıcının farkında olmadığı bir uygulamayı çalıştırarak fazla güç harcaması sağlanabilmektedir.

SMS hizmet aksattırmak DoS saldırısına örnek olarak verilebilir. Bunun için için belirli mobil telefon numaralarının elde edilmesi gerekmekte olup bu atağı yapmanın farklı yolları da mevcuttur.

Örneğin bir operatörün müşteri bilgi bankasına erişilerek ya da sosyal ağ sitelerinden erişim için oluşturulan profil bilgilerine ulaşılarak telefon numaraları elde edilebilir. Yeterince numara elde edildikten sonra, gerçek numaralar filtrelenir ve sahte müşteri id'si ile tüm numaralara eş zamanlı sahte SMS işlemleri gerçekleştirilebilir ve hizmet aksatılması gerçekleştirilir. Bu tip bir saldırı için bir SMPP (Short Message Peer-to-Peer Protocol) ağ geçidi gereklidir.[88]

Bluetooth teknolojisi kullanılarak da(bluetooth sinyalleri sniffing aracı ile tespit edilip) DoS saldırısı gerçekleştirilebilir. Aşağıda bluetooth vasıtasıyla gerçekleştirilebilecek saldırı tipleri açıklanmıştır.

BlueJacking: Kapsama alanı içindeki başka bir kullanıcıya isimsiz olarak mesaj veya veri göndererek cihazı ele geçirmek. Amaç zarar vermek değildir.[89]

BlueSnarfing: Amaç kullanıcının haberi ve izni olmadan bluetooth vasıtasıyla telefon rehberi, e-posta ve metin mesajlarını ele geçirmektir.[90]

BlueSpam: Bluetooth üzerinden gereksiz reklam mesajları gönderilme işlemidir. Gönderme işlemi OOP (Obex Object Push) ve/veya OBEX-FTP (OBEX File Transfer Protocol) kullanılarak yapılır[91]

---

88 SMS DOS attack on cellular networks", http://www.kenneyjacob.com/2007/08/23/sms-dos-attack-on-cellular-networks/ Et:02.02.2015
89 http://www.techopedia.com/definition/5045/bluejacking Et:02.02.2015
90 http://en.wikipedia.org/wiki/Bluesnarfing Et:02.02.20155
91 The Bluetooth Spam FAQ", http://www.mulliner.org/bluetooth/bluespamfaq.php Et:02.02.2015

BlueBug: Bluetooth ile haberleşen cihazlardaki Bluetooth güvenlik açığının adıdır. Mobil cihaz üzerinde çeşitli komutlar çalıştırılmasına imkân sağlar. Çağrı yapılabilir kısa mesaj atılabilir, diğer tüm verilere erişilebilir.[92]

BackDoor: Bu işlemde cihaz arka planda başka bir cihaz ile eşleştirilir ve mobil cihaza erişim sağlanır.[93]

3. Veri iletişimi Dinleme (Data İnterception)

Mobil cihazlar alanında başlıca tehdit yöntemlerinden bir diğeri ise veri iletişiminde araya girmektir(*data interception*). Bu yöntemde ağ üzerindeki paketler toplanarak analiz edilir, ağa sızma işlemi gerçekleştirilir ve veri ele geçirilir.[94]

Bazı durumlarda bir mobil cihaza saldırmanın en kolay yöntemi dolaylı yoldan saldırı gerçekleştirmektir. Bütün mobil cihazlar artık diğer cihazlar ile Wi-Fi, 3G,bluetooth vb. teknolojiler ile iletişime geçebilmektedir. Wi-Fi bağlantısı akıllı cihazlar için tehdit oluşturmaktadırlar. Wi-Fi imkân ve kabiliyetlerine sahip akıllı telefonların yaklaşık %90'da Wi-Fi sniffing ve araya girme de bilinen artan bir tehlike oluşturmaktadır.[95]

Bu teknolojiyi kullanan kişiler ve kurumlar bağlantıları güvenli olmadığından tüm bilgilerinin kriptolu olması gerekmektedir. Çalışmalar göstermiştir ki mobil bir cihaz Wi-Fi ağına bir kez bağlanması onu man-in-the-middle (MITM) araya girme işlemine duyarlı hale getirmektedir.[96]

Özellikle ortak Wi-Fi alanlarında iletişimde araya girme tehdidi daha yüksek ihtimal dâhilindedir. Wi-Fi ağı bağlantısında güvenliği sağlamanın en

---

92 "Bluebug", http://trifinite.org/trifinite_stuff_bluebug. Et:02.02.2015

93 MARKS, Larry. Blackjacking: Security Threats to Blackberry Devices, PDAs and Cell Phones in the Enterprise, by Hoffman, Daniel V. New York: Wiley, 2007, 292p., $39.99. ISBN 978-0-470-12754-4. Information Security Journal: A Global Perspective, 2012, 21.6: 355-356. https://books.google.com.tr/books?id=vRpRNp37xngC&pg=PA3&dq=Understanding+the+threats%E2%80%9DBlackjacking,+ch.1,&hl=tr&sa=X&ei=fyIhVeSpCInZU4DVgNgM&ved=0CBIQ6AEwAA#v=onepage&q=Understanding%20the%20threats%E2%80%9DBlackjacking%2C%20ch.1%2C&f=false

94https://www.bilgiguvenligi.gov.tr/mobil-cihaz-guvenligi/mobil-cihazlarda-guvenlik-android-ve-ios-karsilastirmasi.html Et: 02 Şubat 2015

95 http://www.wi-fi.org/news_articles.php?f=media_news&news_id=969 Et:02.02.2015

96 http://threatcenter.smobilesystems.com/?p=1587 Et:02.02.2015

yöntemi WPA2 (Wi-Fi Protected Access 2) gibi teknolojileri kullanmaktır. Bu şekilde ağa güvenli bağlanılabilir ve veriler şifrelenerek güvenli iletişim sağlanır.

Mobil ağalara bağlanırken genellikle karmaşık olmayan basit şifreler kullanılmakta olup, bu durum saldırganlar için istenen saldırı altyapısını oluşturmakta ve uygun donanım ve yazılımlar kullanılarak ortam dinlenmesi yapılmasına imkân sağlamaktadır.

4. Sosyal Mühendislik ve İstismar (SocialEngineering&Exploitation)

Mobil cihazlarda yapılan açıklık kullanma (*exploitation*) yöntemleri ile sosyal mühendislik uygulamaları sayesinde bilgilerin ele geçirilmesidir. **Oltalama** (*phishing*) saldırısı ile saldırgan kişisel/gizli bilgileri ele geçirebilir.[97]

2004 senesinde Siber Araştırma Merkezi çocukların çevrimiçi olduklarında karşı karşıya kaldığı tehlikeleri araştırıp rapor olarak sunmak amacıyla kurulmuştur. Önemli çalışmalardan bir diğeri ise cep telefonlarının gençler arasında kullanımının popüler olması ve haftalık en az kullanımının % 83 olarak en popüler teknolojik cihaz olduğu bildirilmiştir.[98]

Teknik anlamda teknoloji dünyasında oluşabilecek saldırı türleri maddeler halinde anlatılmış olup, akıllı cihazların kullanımında bireylerin şahsen alması gereken önlemleri aşağıda maddeler halinde sunulmuştur.

- Mobil cihaz üzerinde mutlaka parola ve PIN koruması olmalıdır,
- Herhangi bir virüs ve kötücül yazılıma karşı Anti Virüs yazılımı yüklenmelidir,
- Kullanılmadığı zaman tüm kablosuz bağlantı özelliklerinin kapalı olması, kullanılacağı zaman da güvenli şeklinde kullanılması sağlanmalıdır,
- Akıllı cihaza yüklenecek uygulamaların bilinen kaynaklardan yapılması güvenilir olduğundan emin olunmadıkça uygulamaların yüklenmemesi gereklidir,
- Cihazın çalınma ve kaybolma riskine karşı önemli veriler şifreli bulundurulmalıdır

---

97https://www.bilgiguvenligi.gov.tr/mobil-cihaz-guvenligi/mobil-cihazlarda-guvenlik-android-ve-ios-karsilastirmasi.html Et : 02.02.2015
98 http://www.cyberbullying.us/research.php/ Et:03.11.2014

- Cihaz üzerinde kullanılan gerek işletim sistemi gerekse de diğer yazılımlar güncel bulundurulmalıdır,
- Akıllı cihazlar halka açık alanlarda kullanılırken parola ve kimlik doğrulama işlemlerinin yapılmasını müteakip kullanılmalıdır.[99]

C. Mobil Cihazlarda İnceleme Yapmanın Zorlukları

Mobil cihazlar adli açıdan zorluklar çıkartan dinamik sistemlerdir. Buna ek olarak, her hafta beş yeni telefon modelinin piyasaya sunulduğunu varsayan bazı uzmanlarla birlikte dünya çapında yeni telefon modelleri geliştirilmektedir.[100] Mobil cihazların sayılarının ve çeşitlerinin giderek artış göstermesi, tüm olası sonuçlara değinecek tek bir süreç ya da alet geliştirilmesini zorlaştırmaktadır. Android sistemler, Blackberry, Apple Iphone ve Windows Mobile dâhil olmak üzere akıllı telefon ve platform türlerinin giderek artış göstermesine ek olarak eski sürüm işletim sistemlerini kullanan en telefonların sayısı da oldukça fazladır.

Farklı marka model cihazlar farklı adli bilişim yazılımları tarafından desteklenebilmekte bazıları ise hiç desteklenmeyebilmektedir. Bu durum mobil adli bilişim uygulamalarının piyasaya yeni çıkan akıllı telefonları yeterli seviyede desteklemesi için uzun bir zaman geçmesini gerektirmektedir. Mobil cihazlarda depolanan/işlenen veri ve bunun kullanım/inceleme şekilleri sürekli olarak gelişmekte ve değişmektedir.

Sayısı her geçen gün süratle artan yazılımların ürettiği veriler çok değerli bilgiler içerebilmekte fakat bunları inceleyebilecek adli bilişim yazılımları da hemen bulunmayabilmektedir.

Akıllı telefonlarda adli bilişim analiz işlemlerin neden zor olduğunun temel sebepleri aşağıda maddeler halinde belirtilmiştir.

- Akıllı telefon marka/model sayısının çok olması ve her gün bu cihazlara yenilerinin eklenmesi,
- İşletim sistemi, uygulama ve firma çeşitliğinin fazla olması,

---

99 Sun J, Howie D, Koivisto A & Sauvola J "A hierarchical framework model of mobile security." Proc. 12th IEEE International Symposium on Personal, Indoor and Mobile Radio Communication, San Diego, CA, 2001 http://www.mediateam.oulu.fi/publications/pdf/76.pdf

100 Jones, A. (2008, January 21–23). Keynote speech. In: First International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia, Adelaide, Australia. http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf

- İnceleme yapılan ücretli ve ücretsiz adli bilişim yazılım ve donanımlarının sürekli güncellenmesinin gerekmesi, ya da yazılım/donanımların bütün marka ve model cihazları desteklememesi,
- Şarj kablo ve bağlantı aparatlarının çok çeşitli olması,
- Akümülatör (Batarya) problemlerinin olması,
- Her veri tipini her telefonun kaydetmemesi,
- Verilerin, mesajların şifreli "kriptolu" olması
- Açılış şifreleri ve güvenlik kilidi

gibi belli başlı sorunları söyleyebiliriz. Bahsedilen bu sebeplerden dolayı mobil cihazlara özel adli bilişim yazılımları ve donanımları üretildiğini görmek mümkündür.

5.MOBİL ADLİ BİLİŞİM YAZILIM/DONANIMLARININ GENEL ÖZELLİKLERİ

Bu bölümde dijital adli bilişim olaylarında kullanılabilecek ücretli ve ücretsiz adli bilişim inceleme yazılımlarını ve özelliklerini anlatacağız.

Bir sistemine yapılan yetkisiz giriş ve veya girişimlerin dışardan mı yoksa içerden mi ya da bir problem var ise sistemden mi yoksa insan kaynaklı mı olup olmadığını, bu alanda her gün yeni beceriler ve deneyimler kazanan yazılımlar aracılığı ile "hafıza analizi, harddisk analizi, Log analizi, mobil adli bilişim incelemesi ve imaj inceleme" yaparak çözmemize yardımcı olabilmekte ve telefonlardaki kişisel bilgiler sesli aramalar ve rehber bilgileri bir adli bilişim incelemesinde delil olabilir.[101]Bir sistem başlığı altında neleri geriye dönük olarak geriye getirebileceğimiz yeteneğini görmemize imkân sağlayacak olup bu tabi olarak tüm delilleri görebileceğimiz ve kurtarabileceğimiz manasına gelmiyor.

Her zaman ücretsiz yazılımalar ile istediğimiz sonucu elde edemeyebiliriz bu noktada bunlara ilave olarak ücretli bazı yardımcı yazılımlara," dosya göstericiler, hash değeri üreticiler ve yazı editörlerine" ihtiyaç olabilir. Bu yazılımlardan bazıların daha önce duymuş olsan dahi bu liste içinde bir veya birkaç yararlı yazılım görebileceksiniz.

A. Ücretsiz Adli Bilişim Yazılım ve Donanımları

Aşağıda başlıkları belirtilen yazılımların birçoğu (BackTrack and the SysInternals Suite or the NirSoft Suite of tools) yazılımı veya diğer açık kaynak yazılımlar olup internet ortamında kullanıcıların kullanımına sunulmaktadır.

1. Caine

CAINE (Computer Aided INvestigate Environment) zengin Adli Bilişim araçlarına sahip İtalyan dağıtımı Linux tabanlı bir yazılımdır[102]Çeşitli özelliklere sahip kullanıcı dostu Web ara yüzlü, otomatik rapor oluşturabilen Mobil, Ağ ve Veri kurtarma adli bilişim yazılımıdır.

---

101 Patterson, D. (2004). eForensic Solutions: Cell Site Analysis. Latency lags bandwith, Communications of the ACM, (pp. v.47 n.10, p.71-75,).
102 http://www.caine-live.net/ Et:24.12.2014

CAINE Linux adli bilişim yazılımı boot edilip açıldığı zaman, CAINE adli bilişim araçlarına ait masaüstünde ve görev çubuğunda bulunan kısa yolları ile başlatabiliriz.

2. Deft

Digital evidence ve Forensics Toolkit"DEFT" de caine gibi diğer bir popüler bir İtalyan açık kaynaklı Linux tabanlı adli bilişim yazılımdır.[103] Buradaki amaç siber istihbarat ve adli bilişim senaryolarında olaylara müdahalede yardımcı olmaktır. Diğer adli bilişim yazılımları içinde Mobil Adli Bilişim, Network adli bilişim, veri kurtarma ve hash değerleri alma araçları mevcuttur.

DEFT çalıştırıldığı zaman, DEFT araçlarını yüklemek isteyip istemediğiniz sorulur, eğer yüklerseniz ihtiyaç duyulan araçlar başlat çubuğundaki kısayollardan başlatılabilir. DEFT adli bilişim yazılımı ile aşağıda belirtilen işlemler yapılabilmekte olup bunlar;

a. Hash hesaplama (md5,Sha1,Sha2 ve Dhas) hesaplama
b. Depolama birimi "RAM" inceleme "capture storage media"
c. Zaman bilgisi oluşturma "Timeline ve SüperTimeline"
d. Dosya ve klasör arama işlemi "SEARCH FILES AND FOLDERS"
e. Dosya kurtarma "Carving of Files"

3. Bitpim

BitPIM, Windows, Linux ve Mac OS üzerinde çalışan ve cep telefonları üzerinde veri bir mobil adli bilişim incelemesi yapılacak ise BitPim bunun için değecek bir yazılımdır.[104]İndirimi kullanımı ücretsiz olan bitpim CDMA telefonları üzerindeki verileri görmek için değiştirmemize olanak sağlar. BitPim hangi model telefonları desteklediği telefonları özel durumları ne tür kablolar kullanılacağını ayrıntılı olarak yardım dosyasında yer almaktadır. BitPIM "GNU" Genel Kamu Lisansı altında açık kaynak yazılım olarak dağıtılmaktadır.

---

103 http://www.deftlinux.net/deft-manual/ Et:24.12.2014
104 http://www.concise-courses.com/security/mobile-forensics-tools/ Et:28.12.2014

4. Osaf "Open Source Android Forensics"

OSAF toolkit Cincinnati Üniversitesinde bulunan bir grup Bilişim öğrenci grubu tarafından Android telefonlarda Malware analizi yapmak ve standardizasyon sağlamak için proje olarak geliştirildi.[105]

5. Pilot-Link

Pilot-link linux bilgisayarlar ile Palm Os cihazlar arasında veri transfer işlemi gerçekleştirmek maksadıyla geliştirilmiş açık kaynak yazılım paketidir.[106] Linux yanı sıra diğer birçok masaüstü işletim sistemleri "Windows ve Mac OS" dâhil olmak üzere üzerinde çalışmaktadır. Yaklaşık otuz komut satırı programını kapsayan yazılım paketidir. Fiziksel ve mantıksal analiz işlemi gerçekleştirmek için, pilot-link HotSync protokolü yardımıyla cihaza bağlantı kurar. Adli bir inceleme işleminde RAM ve ROM fiziksel içeriğini almak için iki adet pi-getram ve pi-Getrom yazılım aracı kullanabilir. Diğer bir faydalı yazılım aracı olan pilot-xfer yüklü yazılımların veritabanı yedek alma ve geri yükleme işlemi yapılabilmesidir. Yazılım ile Mantıksal çıkarım yapılabilmektedir. Bu araçlar ile alınan veri içeriği manuel, Palm OS Emulator (POSE) ile ya da EnCase veya hex editör yazılım aracı ile incelenebilir. Pilot-link yazılımı ile hash değeri alınma işlemini sağlamamakta olup farklı bir yazılım ile hash değeri alınmalıdır.

6. TULP 2G

TULP2G (2nd generation) açık kaynaklı bir adli bilişim yazılımı olup mobil cihazlar ile SIM üzerinde adli bilişim analizi yapmamızı sağlayan Netherlands Forensic Institute "Hollanda Adli Tıp" kurumu tarafından geliştirilmiştir. TULP2G'nin çalışması için Windows2000 veya Xp işletim sistemi ve bu sistemlerin güvenlik hizmet paketlerinin güncellenmesi gerekmektedir. TULP2G mobil cihazlara kablo, bluetooth veya kızılötesi arabirimi ile bağlanabilmektedir. SIM kartları analiz edip okumak için bir kart okuyucuya ihtiyaç duymaktadır.

105https://www.nowsecure.com/blog/2010/02/25/viaforensics-announces-release-android-forensics-application/ Et:28.12.2014

106 Additional information on pilot-link can be found at: http://www.pilot-link.org Et:28.12.2014

B. Ücretli Adli Bilişim Yazılım ve Donanımları

Bu kısımda hatırı sayılır adli bilişim alanında isim yapmış ücretli yazılımlara değinilecek olup bunlar aşağıda belirtilmiştir.

1. Cellebrite

Son derece deneyimli bir ekip tarafından 1999 yılında kurulan Telekom ve mobil cihaz teknolojileri ile sektörde büyük atılımlar yapan bir şirkettir. The **Cellebrite 'Universal Forensic Extraction Device' (UFED) yazılımı hem** donanımsal hem de yazılımsal kullanılabilen ürün fiziksel ve mantıksal çıkarım yapabilmektedir. Kablo desteği sağlamaktadır. Cellebrite Eylül 2010 itibariyle (GSM, TDMA, CDMA, iDEN dâhil) 2.500 üzerinde cep telefonu marka/modeli desteklemektedir.[107]

On yılı aşkın bir zaman diliminde cellebrite'in mobil cihazlarda analiz işlemlerinde sağladığı teknoloji pazarda söz sahibi olan bir teknolojiye sahiptir. Öyle ki art arda sektör uzmanları tarafından piyasadaki "En iyi Telefon Adli Bilişim İnceleme Donanım/Yazılımı": 2009, 2010, 2011, 2012 olarak kabul edilmiştir.[108]Cellebrite mobil adli bilişim sektöründe sağladığı yazma korumalı işlevselliği ile adli bilişim bütünlüğü garantisi sağlayan bir yazılımdır. 200'den fazla Android cihazda ilk defa fiziksel ve dosya sisteminden pin ve şifre kilidini bypas ederek adli bilişim işlemi yapabilen yazılım ünvanına sahiptir.

Gelişmiş uygulama çözüm yeteneklerine sahip olmakla "Facebook, WhatsApp, Viber, Fring, Tiger Metin, Waze, Skype, Google+ ve daha fazla uygulamanın analizi ile malware analizi gerçekleştirebilmektedir. Ayrıca cep telefonları için üretilen chipsetlerin birçoğu Çin'de üretilmekte olup bu noktada cellebrite diğer adli bilişim yazılımlarından ayıran özelliklerden biride birçok Çin de üretilen marka model telefona uyumlu olup adli bilişim işlemi gerçekleştirmesi sağlamasıdır. 100 ülkede konuşlanmış 30000 binden fazla birimleri ile UFED Serisi kolluk birimleri "asker, Polis, istihbarat" teşkilatları ile diğer kurumlar ve adli bilişim uzmanları tarafından kullanılmaktadır.

2. XRY

XRY adli bilişim yazılım araçları "GSM, CDMA,UMTS,IDEN ve 3G telefonları dahil olmak üzere 5000 den fazla farklı marka model mobil cihaz ile

---

107 http://www.forensicswiki.org/wiki/Cellebrite_UFED Et:28.12.2014
108http://www.cellebriteusa.com/images/stories/brochures/UFED-Booklet-New-Format-Web_June_2013_v2.pdf Et:28.12.2014

SIM / USIM kartlarından veri çıkarımı ile fiziksel ve mantıksal çıkarım yapabilmektedir. Kablo desteği sağlamaktadır. XRY birimine Infrared (IR) bağlantı noktası, Bluetooth veya kablo arabirimi üzerinden cep telefonu bağlanabilmektedir. Bağlantı kurulumu gerçekleştikten sonra, bağlı telefonunun modelini belirten bir resim, cihaz adı, üreticisi, modeli, seri numarası (IMEI), Abone Kimliği (IMSI), üretici kodu, cihaz saati ve PC saati vs. bilgiler ile cihaz tanımlanması ile gerçekleşir. Cep telefonu cihazlarından elde edilen veriler. XRY formatında saklanır ve değiştirilemez, ancak export edilerek üçüncü parti uygulamalar ile görülebilir. Başarılı bir incelemeden sonra, aşağıdaki alanlar telefonun işlevselliğine bağlı olarak, bulunabilecek bilgi alanları olabilir: Ekran özeti, vaka verileri, genel bilgiler, rehber bilgileri, Aramalar, Takvim, SMS, Resimler, Ses, Dosyalar, Notlar, Görevler, MMS, Ağ Bilgi, Video, vb. veri alan içerikleri görülebilir. Ayrıca, telefonda bulunan grafik dosyaları, ses dosyala Ve diğer veriler incelemeden sonra muhafaza daha detaylı bir araştırma için ihraç edilip saklanabilmektedir. XRY 60 ülkede Polis, Asker, Devlet İstihbarat birimler ile Adli bilişim Laboratuvarları tarafından kullanılmaktadır. Bu sistem ile veri analizi yapmak için bir PC, yazılım ve telefonları bağlamak için bir donanım aygıtından oluşmaktadır.[109]

3. Tarantula

Tarantula: Mantıksal ya da fiziksel çıkarım yapılabilen ürün yazılımsal olarak da kullanılabilmektedir. Şu anda, dünya çapında cep telefonlarının % 30'u olarak Çin'de üretilen yonga setlerini kullanmakta olup dayanmaktadır.[110] Bu eğilim, sonraki yıllarda daha da artması beklenmiş ve öylede olmuştur. Tarantula diğer yazılımlardan farkı yeteneği piyasada bulunan ve Çinli dört firma tarafından üretilen yonga setli cep telefonları üzerinde inceleme yapmayı desteklemektedir. " Mediatek, Spreadtrum, Infineon ve Mstar."

109https://www.nowsecure.com/education/white-papers/iphone-forensics/micro-systemation-xry/#viaforensics/ Et:28.12.2014

110 **EDEC Digital Forensics** 1805 E Cabrillo Blvd. Suite F Santa Barbara, Ca 93108 "Tarantula Chinese Cell Phone Analysis Tool General Overview" http://www.cfi.co.th/uploads/1/0/6/0/10606523/tarantula_product_overview.pdf Et:28.12.2014

Şekil 15-Tarantula Donanım ve Çantası

4. Mobiledit

MOBILedit! GSM / CDMA / PCS cep telefonlarından hem yazılımsal hem de fiziksel ürün analizi yapmamızı sağlayabilen bir uygulamadır. Cep telefonu ile Infrared (IR) port, a Bluetooth ve Kablo desteği ile bağlantı sağlayabilmektedir. Yazılım cihaz ile bağlantı kurduktan sonra cep telefonu üreticisi, model numarası, seri numarası (IMEI) ve cihaz resmi ile donanım tanımlanmaktadır. Cep telefonundan elde edilen veriler *.MED dosya biçiminde saklanır. Başarılı bir incelemeden sonra, aşağıdaki veri alanları bulunur: Cihaz özellikleri, rehber bilgileri, sim rehber bilgileri, cevapsız aramalar, son aranan ve gelen çağrılar, silinmiş öğeler, silinmiş sms/mms'ler, video ve ses dosyaları elde edilebilmektedir. Ayrıca myPhoneSafe.com adresinden adresinden IMEI adresi ile sorgulama yaparak telefonun çalıntı olup olmadığı kontrolünü yapabilmektir.[111]

5. Faraday

Bulunduğu ortamda bir sinyal kesici görevi yapan ve Cep telefonlarının açık kalması gereken durumlarda operatörle iletişimi kesen özel bir çantadır.

---

111 Rick Ayers - Wayne Jansen - Ludovic Moenner - Aurelien Delaitre,*Cell Phone Forensic Tools: An Overview and Analysis Update*,(2007), National Institute of Standards and Technology http://csrc.nist.gov/publications/nistir/nistir-7387.pdf

Şekil 16-Faraday Çantası

6. Paraben's Device Seizure

Paraben's Device Seizure ile "CDMA, TDMA ve GSM şebekeleri üzerinden çalışan cep telefonlarına adli bilişim inceleme olanağı sağlayan adli bilişim yazılım aracıdır. Paraben ile inceleme yapılacağı zaman telefona uygun kablo tipi seçilmelidir. Paraben vasıtasıyla cep telefonları üzerinde aşağıdaki veriler bulunabilir:

•SMS/MMS : Gelen/Giden

•Telefon ve SIM rehber bilgileri.

• Arama kayıtları: Gelen Giden aramalar ile cevapsız çağrılar.

• Takvim Bilgileri: Görev, ajanda ve diğer notlar.

• Video, resim ve ses verileri

• WAP: WAP Settings, WAP Bookmarks

• SIM: GSM Şebeke bilgileri.

Paraben's **Device Seizure** ile MPE deki gibi ya da Oxygen suite aksine cep telefonun bellek analizi yapılarak döküm alınabilmektedir. Mantıksal çıkarımdan ziyade fiziksel çıkarım ile daha çok veri elde edilebilmeyi sağlamaktadır.[112]

112 Paraben Corporation. (n.d.). Device Seizure. Retrieved May 29, 2010, from Paraben Corporation https://www.paraben.com/device-seizure.html Et:24.12.2014

7. Oxygen Forensics Suite

Oxygen: Bu ürün fiziksel ve mantıksal çıkarım yapabilmektedir. Eğer bir dava için mobil cihazdan delil toplanacak ise size yardımcı olacak ve bu işlemi başaracak olan yazılım Oksijen Adli Bilişim yazılımı gerçekleştirebilir. Oxygen suite bir çok avrupa ülkesinde İngiltere Almanya Avustralya İsveç ve Finlandiya da bir çok acenta,kolluk kuvveti, vergi ve gümrük ile diğer hükümet birimleri tarafından en çok tercih edilen adli bilişim yazılımdır.[113]İçerdiği özelikleri ile cihaza ait üreticiyi, işletim sistemini, imei ve seri numarası, rehberi, mesajları (e-mail,sms.mms),silinmiş mesajları, arama kayıtlarını, takvim bilgilerini ve zamanlanmış görevleri toplama ve bulma yeteneğine sahiptir. Aynı zamanda dosya izleme özelliği ile resim, video, doküman ve veritabanlarına erişim ve analiz etmeye imkân verdiği birçok formatta veri elde etmeye imkân ve yeteneği mevcuttur.

Oksijen Adli Bilişim yazılımı çalıştırıldığı zaman; Menu çubuğundaki 'Yeni cihaza bağlan' butonuna tıklanıp çalıştırıldığında bir yardımcı sihirbaz aracı çıkarak cihaz tipi seçilerek adli bilişim inceleme süreci başlatılır.

8. EnCase Neutrino

Mobil cihazlar için adli soruşturma analizi yapabilmek maksadıyla tasarlanmış olan EnCase güçlü bir endüstri lideri olmaya başlayan encase yazılımının 30.000 üzerinde lisanslı kullanıcısı bulunmaktadır. Gelişmiş donanım özelliklerine sahip olan Encase ile Motorola, Nokia, Siemens, Samsung, LG, Palm, BlackBerry, HTC, Sony Ericsson, UTStarcom markaların hatta daha fazlasını içeren en yaygın mobil cihaz üreticilerinin donanımların adli bilişim analizleri yapılabilmektedir. Mobil cihazların adli bilişim işlemleri yapmak maksadıyla dizayn edilen Encase çözümleri endüstri lideri olmuştur. Diğer yazılımların aksine işlem önce SIM ile başlar daha sonra cihaz ile devam eder.[114]

---

113 Oxygen Forensic . (n.d.). Oxygen Forensic Suite 2010. Retrieved May 15, 2010, from Oxygen Forensic: http://www.oxygen-forensic.com/ Et:24.12.2014

114 Guidance Software. (n.d.). *EnCase Neutrino.* Retrieved May 28, 2010, from Guidance Software:http://www.guidancesoftware.com/product.aspx?B=Product &Product_S=AccordianTwo&menu_id=117&id=348&terms=mobile+devices

9. Flasher box

Flasher Box: Cep telefonlarının sim ve güvenlik kilitlerini kırmak maksadıyla kullanılmaktadır. Çok fazla marka ve modeli destelemekte olup adli bilişim incelemelerinde kullanılabilmekte ve dikkatli kullanılmadığı takdirde ciddi zararlar verebilmektedir.

Şekil 17-Flasher Box Cihazı

6.MOBİL CİHAZLARDA ADLİ BİLİŞİM SAFHALARI

Mobil cihazların üzerinde adli bilişim, inceleme alanı olarak 1990'ların sonlarında ve 2000'li yılların başına dayanmaktadır. Mobil cihazların bir suç aracı olarak kolluk kuvvetleri tarafından tanımlanması uzun bir süreç olmuştur. Bu cihazların kullanılabilirliğinin artması adli inceleme sürecini de gerekli kılmıştır.[115]

Mobil cihazlar ve cep telefonları üzerinde inceleme yapma çalışmalarının artması ile birlikte bu cihazlar üzerinde yürütülen adli bilişim sürecine dair ilke ve prensip gereksinimlerinin ortaya çıkmasına neden olmuştur.

Piyasada bulunan her marka ve model cihazın incelemesinin spesifik detaylarının birbirinden farklı olma ihtimali olup cihazların düzenli inceleme işlemlerine tabi tutulması, inceleme yapan kişiye her telefondan çıkan delilin uygun bir şekilde belgelendirilmesi ve bu sonuçların tekrarlanabilir ve savunulabilir olmasını ve ilerleme sağlamasına bu işlerde standartların oluşturulmasında yardımcı olacaktır.

Geçtiğimiz birkaç yıl içinde dijital adli bilişim uzmanları, cep telefonlarının ve diğer mobil cihazların incelenme isteği konusunda gözle görülür bir artışla karşılaşmışlardır. Bu cihazların incelenmesi ve onlardan bilgi elde edinilmesi, adli bilişim uzmanlarına çok sayıda zorluk çıkarmakta olup inceleme

---

115 CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the internet*. Academic press, 2011 http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf

için verilen mobil cihazların giderek artan bir oranını temsil eden akıllı telefonlar ve tabletlerle birlikte, karşılaşılan zorlukların sayısı gün geçtikçe artmaya devam etmektedir.

Piyasada satılan mobil cihazlar çeşitli tescilli işletim sistemleri, gömülü dosya sistemleri, uygulamalar, servisler ve yan birimler kullanmaktadırlar. Bu eşsiz cihazlardan her biri mevcut farklı adli bilişim yazılım araçları tarafından desteklenebilir ya da desteklenmeyebilir.

Mobil cihazlarda bulunan veri türleri ve bu verilerin kullanılma şekilleri sürekli olarak değişmektedir. Akıllı telefonların yaygınlaşması ile birlikte, sadece telefon defterini, arama geçmişini, metin mesajlarını, fotoğrafları, takvim girişlerini, notları ve medya depolama alanlarını belgelendirmek artık yeterli gelmemektedir. Çünkü bu cihazlar bütün yönleriyle mini bilgisayarların fonksiyonlarını yerine getirmekte ve imkân dâhilinde daha fazla ilgili veri içermektedirler. Sürekli sayı ve çeşitliliği artan uygulamaların kullanılmasıyla üretilen veriler, mevcut adli bilişim yazılımları tarafından otomatik olarak çözümlenemeyen bol miktarda bilgi içerebilmekte. Mobil cihaz incelemesi yapmak için geleneksel dijital adli bilişim becerileri ve yeni teknikleri giderek daha da gerekli hale gelmektedir.

Cep telefonları ve diğer mobil cihazlar radyo, Bluetooth, kızılötesi ve kablosuz (WiFi) ağ yapıları aracılığıyla cep telefonu ve diğer ağlarla iletişim kurmak amacıyla tasarlanmıştır. Telefondaki verileri en iyi şekilde korumak için cihazı çevredeki ağlardan izole etmek gerekir. Bu her zaman mümkün değildir. İzolasyon metotları başarısızlıkla sonuçlanabilir.

Mobil cihazlar çeşitli dâhili, harici ve çevrimiçi veri depolama kapasitesi olarak kullanılmakta ve çoğu durumda mobil cihazdan istenilen veriyi ve cihazla özdeşleşen veri depolama ortamını çıkartmak için ve belgelendirmek için birden fazla araç kullanmak gerekir. Belirli durumlarda cep telefonlarını işlemden geçirmek için kullanılan araçlar tutarsız ya da hatalı bilgi üretebilir. Bu yüzden mobil cihazlardan elde edilen verinin doğruluğunu teyit etmek son derece önemlidir. Sıradan bir bilgisayardaki sabit diskin depolama kapasitesine oranla telefonlarda depolanan veri miktarı daha düşük olmasına rağmen, bu cihazların depolama kapasitesiler de giderek artmaktadır.

Cep telefonlarından veri elde etmek için kullanılan teknikler çok çeşitli olabilir. Cep telefonundaki veri genellikle istihbaratı amaçla istenir ve bu alanda telefonları işleme tabi tutmak ilgi çekicidir. Bazen sadece belirli veriler bir inceleme için önem arz ederler. Diğer durumlarda, gömülü dosya sisteminin ve/veya telefonun fiziksel belleğinin tamamen çıkartılması tam teşekküllü adli inceleme ve silinen verinin kurtarılma olasılığı için de istenebilir.

Bu faktörler sebebiyle mobil cihazlardan veri çıkartılması ve bu verilerin belgelendirilmesi için yapılan işlemlerin ve kılavuz ilkelerin gelişimi oldukça önemlidir. Ayrıca mobil cihaz teknolojisi değişmeye ve gelişmeye devam ettiği için bu işlemlerin ve kılavuz ilkelerin periyodik olarak gözden geçirilmesi gerekir.

A. Cep Telefonundan Delil Çıkartma Süreci

Elde edilen elektronik verilerin delil olarak geçerli sayılabilmesi ve işlem sırasının yerine getirilmesi, uluslararası kabul görmüş standartlarda olmalıdır. Dijital veriler üzerinde yapılacak en ufak hata, verilerin zarar görmesi ve yok olmasına neden olabilir.

Dijital deliller yapıları sebebiyle diğer suç mahallinde bulunan ve elde edilen fiziksel delillere göre daha hassas ve kolay bozulabildikleri için birçok zorluğu beraberinde getirmektedir. Bu amaçla olaya müdahalenin başlangıç anı ile laboratuvarlarda yapılan işlemin sonuna kadar her aşama büyük önem taşımaktadır.

Bulunan delillerin mahkeme esnasında kabul edilebilirliğini sağlamak için sadece doğrulamada kullanılacak teknik yöntemler yeterli olmayıp delillerin incelendiği laboratuvarın, kullanılan araç, gereç ve yöntemlerinin de uluslararası standarda uygun olması gerekmektedir. Bu yüzden bilişim suçlarıyla mücadele eden birimler için uluslararası standartların belirlenerek, bu standartların uygulamaya konulması da oldukça önemlidir.[116]

Günümüz Türkiye'sinde bilişim suçlarının soruşturulması sürecinde adli kolluk birimleri, bu dava olaylarına bakan hâkim ve savcılara kadar birçok kamu görevlisi görev almaktadır. Bu süreçlerin kanunlara uygun ve bu suçla mücadele süreci içerisinde çalışan birimlerin uyum içerisinde çalışması gerekmekte olup, bu süreçlerin gelişen teknoloji ve bilişim suç türlerine karşı sürekli yenilemesi gerekmektedir.

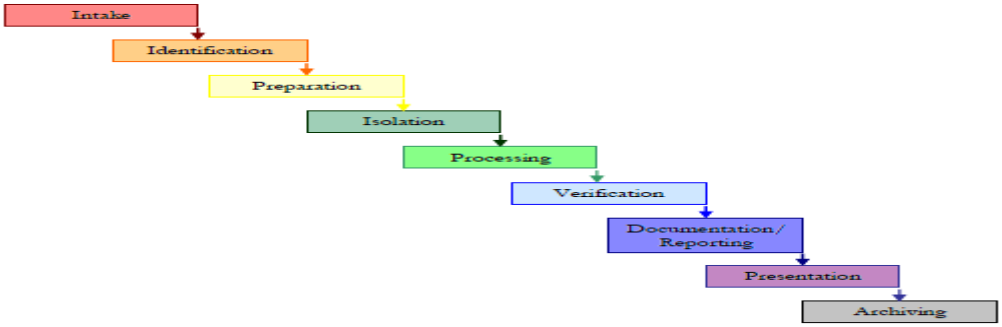
Bu nedenle dijital delilleri belirli metot ve prosedürlere uygun olarak araştırmak ve dillendirmek için birtakım ortak süreçlere ihtiyaç vardır. Aşağıda

---

116 MEYERS, Matthew; ROGERS, Marc. Computer forensics: the need for standardization and certification. *International Journal of Digital Evidence*, 2004, 3.2: 1-11 http://www.slideshare.net/lisajarrett1972/computer-forensics-35134495

Murphy, Cynthia'ın (2013) oluşturduğu 9 basamaklı süreç modeli görülmektedir.[117]

Girdi – Tanılama – Hazırlık – İzolasyon (Ayrıştırma) – İşleme tabi tutma – Doğrulama – Belgelendirme/Raporlama – Sunum – Arşivleme olarak tanımlanmaktadır.



Şekil 18-Mobil Cihazlarda Delillendirme Süreci[118]

B. Delil Toplama "Evidence Intake Collection" Safhası

Delil toplama safhası inceleme isteklerinin ele alındığı aşama olarak tanımlanmaktadır. Delil toplama safhası delil zincirini, mülkiyet bilgisini ve mobil cihazın dâhil edildiği vaka türünü belgelendirmek için genellikle istek formları doldurulmasını, giriş evrakı işlerinin yapılmasını ve başvuran kişinin aradığı bilgi ya da veri türüyle ilgili genel bilgilerin ana hatlarıyla belirtilmesini kapsar.

İncelemenin bu noktasında önemli olan her bir inceleme için belirli amaçların geliştirilmesidir. Bu işlem yalnızca inceleme yapan kişinin amaçlarını netleştirmek ve belgelendirmekle kalmaz, aynı zamanda incelemelerin özelliklerine göre ayrılmasına yardımcı olur ve incelenen her bir cihazın incelenme işleminin belgelendirilmesini başlatır. Çoğu kuruluş ve organizasyon mobil cihazın inceleme için alındığını belgelemek için form kullanmaktadır.

---

117 Murphy, Cynthia. "Cellular Phone Evidence Data Extraction and Documentation". Retrieved 4 August 2013. https://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf

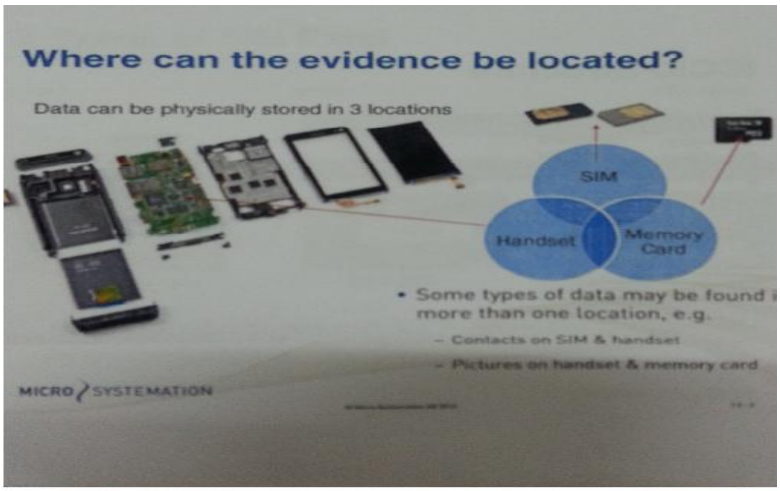
118 Murphy, Cynthia. "Cellular Phone Evidence Data Extraction and Documentation". Retrieved 4 August 2013. https://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf

Bu bölümde, incelemenin diğer aşamalarına geçmeden önce, mobil cihazlar üzerindeki delillerin nerede ve hangi alanlarda olabileceği detaylandırılacaktır.

1. Veri Alanları

Mobil cihazlar 3 farklı alanda veri bulundurabilirler. Bu alanlar, mobil cihazın dâhili hafızası, harici hafızası (Hafıza kartı) ve SIM kartından oluşur.[119]

Cep telefonları içindeki kanıt olarak değerlendirebilecek bilgiler şunlar olabilir: SIM bilgisi, mobil cihaz dâhili hafızası ve servis sağlayıcı bilgileridir. Çok çeşitli yapıdaki hafıza kartları (SIM, SD, MMC, microSD, Memory Stick Duo vs.) akıllı mobil cihazlar tarafından desteklenmekte ve bu kartlar gün geçtikçe çeşitlilik kazanmaktadır.



Şekil 19-Mobil Cihaz Üzerindeki Veri Alanları

Hafıza kartları yüksek kapasiteye sahip olmak ile birlikte bilgisayar uyumlu dosya özelliğine sahiptir. Bu kartların adli bilişim için bir kopyası alınabilmesi için bir kart okuyucuya ihtiyaç vardır. Ancak mantıksal yazılımlar kullanılarak hafıza kartı telefon içinde iken canlı veri kurtarma da yapabilir.

Hafıza kartları dikkatli bir şekilde analiz edilirse adli bilişim teknik ve yazılımları kullanılarak kurtarılması mümkün olabilecek silinmiş veriler ve

---

119 Ahmet EKİM, Mobil Cihazlarda adli Bilişim ve Malware Analizi, http://www.bilgisayardedektifi.com/mobil-cihazlarda-adli-bilisim-ve-malware-analizi/206 Et:17.05.2014

mesajlar tespit edilip kurtarılabilir. Hafıza kartındaki silinen verilerin geri döndürülebilmesi için doğrudan erişilebilir olması gerekir. Bir dosya FAT formatında bir karttan/dosya sisteminden silindiği zaman sadece o dosyanın nerede kayıtlı olduğuna dair bilgi değiştirilir. Bu silme operasyonunda dosyanın içerisinde hiçbir değişiklik yapılmaz yani silinmiş dosyalar başlık bilgisinin yer aldığı alana bakmak yerine dosya bilgisi okunarak bulanabilir.

Servis sağlayıcılar aracılığı ile de çok büyük ve önemli bilgilere erişilebilmektedir. Örnek olarak arama, mesaj, abone(isim, adres, numara vs.) bilgileri verilebilir.

Kolluk kuvvetleri servis sağlayıcılardan elde edilen verileri incelemek için çeşitli uygulama/yazılımları kullanır. Bu yazılımlar iz sürüm/tarama yöntemleri kullanarak mobil telefonların numaraları, IMEI numarası ve bağlantılarını bularak grafiksel raporlar oluşturulabilmektedir. Arama kayıtları ve arama esnasında bağlanılan baz istasyonu bilgileri ceza davasında bilgi olarak sunulabilir. Bu tip analizler analizi yapan kişiye sadece bir adres veya sınırlı bir coğrafi alan değil aramanın yapıldığı bölge ile alakalı bir fikir sunmaktadır. Tespit edilen bilgiler suçlunun suç anında başka yerde olduğu iddiası ortadan kaldırabilir veya destekleyebilir.

2. Dâhili Hafıza

Günümüzde çoğunlukla mobil cihazlar üzerinde NAND veya NOR olarak adlandırılan flaş bellek tipi kullanılmaktadır[120]. Mobil cihazlar birer dijital medya olarak düşünebilir ve diğer veri depolama ortamlarında mümkün olduğu gibi veriler kurtarılabilir. Mobil cihazların bu alanda mantıksal ve fiziksel inceleme türlerinden bahsedebilir. Cihazın ekranında görüntülenen verileri elde etme yöntemi Mantıksal inceleme ile elde edilebilir. Fiziksel incelemede ise bit by bit denilen görüntü alma metodu ile cihazın içerisindeki tüm verilere ham haliyle ulaşılması mümkündür. Bu alanda silinmiş veriler de elde edilebilir.

Mobil cihazların dâhili hafızası içerisinde olabilecek ve adli bilişim incelemesi sonucunda bulunabilecek potansiyel veri türleri aşağıda maddeler halinde sıralanmıştır.[121]

- Gelen aramalar

120 http://www.theosecurity.com/pdf/Fiorillo.pdf Et:05.01.2015

121 Ahmet EKİM, Mobil Cihazlarda adli Bilişim ve Malware Analizi, http://www.bilgisayardedektifi.com/mobil-cihazlarda-adli-bilisim-ve-malware-analizi/206 Et:17.05.2014

- Giden aramalar
- Cevapsız aramalar
- Kişi listesi (kişisel telefon rehberi)
- Metin mesajları (SMS)
- Sohbet kayıtları
- Fotoğraflar
- Video klipler
- Takvim
- E-postalar
- Özel bir zil sesi (Ayırt edici zil sesi, bir soruşturmada tanık tarafından hatırlanabilir)
- Yer ve konum bilgisi
- Yüklü Uygulamalar ve kayıt bilgisi

3. Hafıza Kartında Bulunabilecek Veriler

Şu an piyasada olan çoğu cep telefonu, Trans Flash Micro SD bellek genişletme kartı gibi çıkarılabilir bir depolama cihazına veri depolama özelliğine sahiptir. Böyle bir kartın inceleme için sunulan bir cep telefonuna takılması durumunda, inceleme uzmanının kartı çıkartması ve geleneksel adli bilişim teknikleri kullanarak işlem yapması gerekir. Kart telefona takılı durumdayken cep telefonu adli bilişim araçları kullanılarak yapılan veri depolama kartı işlemi, veri kartında bulunan dosyaların tarih ve zaman damgasının değişmesi ile sonuçlanabilir.

Buna ek olarak cep telefonları, telefon kullanıcısının bilgisayarla ulaşabileceği şebekeye dayalı depolama alanları içindeki verinin harici olarak depolanmasına ya da iOS temelli cihazlar için iCloud, Android temelli cihazlar için Google hesabı gibi telefondaki verinin internet merkezli bir hesapla senkronize olmasına imkân sağlayabilir. Bu veriye erişim yasal yetki gerektirebilir ve genellikle cep telefonu incelenmesi kapsamı dışındadır. Bununla birlikte, şebeke temelli veri depolama işleminin potansiyel varlığı inceleme uzmanı tarafından göz önünde bulundurulmalıdır.

Belirleyici niteliği olan çoğu telefon ve akıllı telefonlar, cep telefonundan bilgisayara veri transferi yapılmasını ve bilgisayardan cep telefonuna veri transferi yapılmasını kolaylaştırmak amacıyla kullanıcı bilgisayarıyla senkronize olacak şekilde tasarlanmıştır. Bir telefondaki verinin tamamen ya da kısmen yedeklemesinin yapılması özelliği, telefonun senkronize edildiği telefon sahibinin bilgisayarında ya da herhangi bir bilgisayarda bulunabilir. Bu alternatif depolama alanlarının var olma potansiyeli, cep telefonlarından gelen ek veri kaynakları olarak inceleme uzmanı tarafından göz önünde bulundurulmalıdır.

4. Sim Kart Verileri

SIM kartlar telefonun ve/veya akıllı cihazların ilgili operatör ile iletişime geçmesini sağlayan mini kartlardır. Aboneye ait kişisel bilgilerden oluşan, abone bilgilerini taşırlar. Boyut olarak gittikçe küçülmekle birlikte kapasiteleri tam tersi oranda artmaktadır. Hiyerarşik bir yapıya sahip olan SIM dosya sisteminin içinde bulunan isimler ve numaraları, gönderilen ve alınan mesajları ve GSM şebeke bilgilerini organize bir şekilde SIM kartlar içerisinde bulmak mümkündür[122].

Sim kartta bulunacak veriler aşağıda sıralanmıştır[123]

- Gelen arama bilgileri
- Rehber Bilgisi.
- Metin mesajları (SMS)
- Giden arama bilgileri (Last numbers Dialed)
- Cevapsız arama bilgileri
- Uluslararası Mobil Abone Kimliği (IMSI)
- Yerleşim bilgisi (Location Area Information LAI)

C. Tanımlama (Identification) Safhası

Bir mobil cihaza yapılan her incelemede, inceleme uzmanı aşağıdakileri bilgileri belirler ve ona göre işlemler yapar[124];

- Cihazı inceleyecek adli makam/yasal merci
- İncelemenin amacı
- Cihaz(lar)ın yapım, model ve tanımlama bilgisi
- Çıkarılabilir & harici veri depolama
- Diğer olası delil kaynakları

---

122 Somasheker Akkaladevi1 1 Virginia State University Department of Computer Information Systems Petersburg, Virginia 23806, USA efficient forensic tools for handheld devices: a comprehensive perspective http://www.swdsi.org/swdsi08/paper/SWDSI%20Proceedings%20Paper%20S406.pdf

123 Mellars, B. (2004). Forensic Examination of Moblie Phones. Digital Investigation. The International Journal of Digital Forensics & Incident Response, 266-272.

124 Murphy, Cynthia. "Cellular Phone Evidence Data Extraction and Documentation". Retrieved 4 August 2013. https://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf

1. Adli Makam/Yasal Merci

Mobil cihazlardan alınan veri araştırmasını çevreleyen içtihat hukuku sürekli güncellenmektedir. İnceleme uzmanının cihazın incelenmesi için hangi yasal merciin var olduğunu belirlemesinin yanı sıra inceleme öncesinde araştırmaya getirilebilecek sınırlandırmaları da belirlemesi ve belgelendirmesi zorunludur.

Ülkemizde mobil cihazlarda adli bilişim yöntemlerine dair ceza hukukumuzda özel bir durum yoktur. Normal Adli Bilişime ilişkin olan hükümler de CMK 134 maddesine göre "Kişisel Verilerimiz üzerinde sahip olduğumuz hak, ulusal ve uluslararası normlarda bireyin temel hak ve özgürlükleri arasında yer almakta ve korunmaktadır. Bu nedenle bilgisayarlar gibi elektronik aygıtların aranması veya bu aygıtlara el konulması söz konusu olduğunda bu müdahalenin ancak hâkim kararı ile yapılması gerektiği vurgulanmaktadır." [125]

Bu kapsamda inceleme yapılacağı zaman aşağıda dikkat edilmesi gereken hususlar aşağıda belirtilmiştir;

- Eğer cep telefonu bir arama izini belgesine istinaden araştırılıyorsa, inceleme uzmanının araştırmayı o belgenin limitlerine göre sınırlandırmaya dikkat etmesi gerekir.
- Eğer cep telefonu birinin rızası/izni gereği araştırılıyorsa, araştırma onay verilen limitlerle sınırlandırılmalıdır (örneğin sadece arama geçmişi incelenir). İnceleme uzmanının telefon incelenmeden önce verilen iznin hala geçerli olup olmadığını belirlemesi gerekir.
- Telefonun tutuklama vakası için araştırıldığı durumlarda, inceleme uzmanı özellikle dikkatli olmalıdır. Çünkü bu alandaki içtihat hukuku karmaşıktır ve sürekli güncellenmekte ya da yetersiz gelebilmektedir.

Bir cep telefonunun araştırılması konusunda yasal merci ile ilgili özel sorular bilgili bir savcıya ya da inceleme uzmanının bölgesindeki bir hukuk danışmanına yöneltilmelidir.[126]

---

125 Leyla KESER BERBER, Adli Bilişim, CMK md. 134 ve Düşündürdükleri. http://www.leylakeser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html Et:10.07.2014

126 CASEY, Eoghan; TURNBULL, Benjamin. Digital evidence on mobile devices. Eoghan Casey, Digital Evidence and Computer Crime. Third Edition. Forensic Science, Computers, and

Bazı durumlarda, arama kararı veya birinin rızası ile icra edilen bir araştırmada, araştırmanın özelliği konusunda belirtilen gerekliliklerin, var olan adli bilişim araçlarının kapasitesinin ötesine geçtiğini görebiliriz. Örneğin bir arama izni, bir cep telefonunun ya da başka bir mobil cihazın araştırılmasını belirli bir tarih aralığındaki arama geçmişi ve mesajlarla sınırlandırıyor olabilir. Çoğu adli bilişim aracı, inceleme uzmanının veri çıkartma işlemini sadece o tarih aralığındaki verilerin çıkartılması ile sınırlandırmasına izin vermemektedir. Bu durumda bir telefondaki tüm veriyi elde etmek ve bu veriden arama emrinde belirtilen veriyi ayıklamak geniş çaplı bir arama gibi gözükebilir. Dolayısıyla arama emirleri hazırlanırken ya da bir cihazı araştırmak için izin alınırken bu tarz kısıtlamaları ifade etmek önemlidir.

2. İnceleme Amacı

Herhangi bir cep telefonunu incelemek için kullanılan genel sürecin mümkün olduğu kadar istikrarlı olması gerekir. Bunun yanısıra her bir telefonun inceleme amacı birbirinden çok farklı olabilir. Bilinen her adli bilişim laboratuvarının her durumda delil niteliği taşıyan veri içeren her bir cep telefonunun inceleyecek kaynağının, imkânının ya da kapasitesinin olması pek mümkün değildir. Bu sebeple, verilen herhangi bir cep telefonu için ne seviyede incelemenin uygun olduğunu belirlemek yararlı olacaktır.[127]

Burada iki temel husus vardır; birincisi veriyi belgelendirme işleminden kimin sorumlu olacağı, ikinci ise incelemenin derinliğinin ne olması gerektiğidir. İnceleme için laboratuvara verilen telefonların incelemelerinde olayın gerçeklerine ve şartlarına bağlı olarak farklılıklar çıkacaktır.

Bazı olaylarda cep telefonlarından elde edilen deliller elle ya da fotoğrafik olarak belgelendirilebilir. Örneğin delil değeri olan bilgi hala belgelendirilme aşamasındayken, bir kurbanın temel iletişim kurma hakkının iade edilmesi ya da ciddi olmayan bir suç veya kusurda delilin belgelendirilmesi durumunda cihazın yakalanması için belgelendirme yapmak mantıklı bir alternatiftir. Diğer

---

the Internet, Academic Pres, 2011 http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf Et:10.07.2014

127 Murphy, Cynthia. "Cellular Phone Evidence Data Extraction and Documentation". Retrieved 4 August 2013. https://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf

durumlarda, cep telefonlarının incelenmesi konusunda temel eğitim almış bir yetkili veya analiz uzmanının olması yeterlidir.

Cep telefonlarının daha küçük bir alt kümesi, delil değeri olan veriden hedeflenen verinin çıkartılması amacıyla inceleme için verilebilir. Diğer depolanmış veriler inceleme için alakasız olabilirken, resimler, videolar, arama geçmişi, metin mesajları ya da diğer spesifik veriler gibi hedeflenmiş veriler, inceleme için önem arz edebilir. Ayrıca yasal kısıtlamalardan ötürü verilerin sadece belirli bir alt kümesinin incelenebiliyor olması bir başka husus olabilir. Hangi durumda olursa olsun incelemenin kapsamını daraltmak büyük olasılıkla verinin çıkartılması ve belgelendirilmesi için harcanan zamanı azaltacaktır.

İncelemenin amacı telefonun hafızasından silinen verinin geri getirilmesi olabilir. Bu, yalnızca belirli bir telefon için fiziksel ya da dosya sistemi seviyesinden veri çıkartabilen özel bir aracın olması durumunda mümkündür. Eğer böyle bir araç mevcutsa, incelemeye ham veriden orijinal veri elde etme yöntemi (data carving, hexdecoding ve SQLite veri tabanları) gibi geleneksel adli bilişim metotları dahil edilecektir. Dolayısıyla inceleme süreci zaman alıcı ve teknik gerektiren bir uğraş olabilir. Çünkü incelemenin ilerleyen safhaları teknik olarak daha karmaşık ve zaman alıcı bir süreç gerektirmektedir.

İnceleme amacı, telefonun incelenmesi için hangi araçların ve tekniklerin kullanıldığı konusunda önemli bir fark yaratabilir. İncelemenin hedefini belirlemek için harcanan zaman ve emek, inceleme sürecinde hızlı ve verimli çalışmayı gerektirebilir[128]. Bu tür gerçekliklere eğitim esnasında değinilmelidir. Cep telefonlarının inceleme için ilk kez ibraz edilmeleri ile ilgili olarak incelemenin özelliklerine göre sınıflandırılması süreci, bireysel şartlara ve olayın ciddiyeti temeline dayandırılmalıdır.

3. Cihazın Tanımlanması

Herhangi bir cep telefonu incelemesinin bir parçası olarak, telefonun tanımlama bilgisinin belgelenmesi gerekir. Bu belgelendirme incelemeyi yapan kişinin sonraki bir zamanda belli bir telefonu tanımlamasına ve telefonla birlikte hangi araçların işe yarayabileceği konusunda karar vermesine yardımcı olur. Çünkü çoğu cep telefonu adli bilişim araçları, telefonun yapım ve modeline dayanarak desteklenen telefonların listelerini temin eder. Tüm telefonlar için cep telefonuyla özdeşleşen imalatçı, model numarası, taşıyıcı ve mevcut telefon

128 https://www.packtpub.com/books/content/introduction-mobile-forensics/ Et:02.01.2015.

numarası belirlenmeli ve belgelendirilmelidir[129]. Ayrıca ilgili cep telefonu teknolojisine bağlı olarak, ek tanımlama bilgisi belgelendirilmedir.

4. CDMA Cep Telefonları

Elektronik Seri Numarası (ESN) cep telefonu bataryasının altında yer alan ve Federal Communications Commission (FCC) tarafından mobil cihazların tanımını sağlayan özel ve eşsiz bir numaradır[130]. ESN ağdaki her bir mobil telefona tahsis edilen 32 haneli özgün bir numaradır. 11 basamaklı onluk ve/veya 8 basamaklı olarak onaltılık düzende listelenebilir. İnceleme uzmanının ESN'nin hex versiyonunun onluk değerin doğrudan bir nümerik dönüşümü olduğunu bilmesi gerekir. Örnek çevirim işlemi http://www.elfqrin.com/esndhconv.html sitesinden yapılabilmektedir.[131]

Mobil Ekipman Kimliği (MEID) bataryanın altında yer alan, 32 rakamlı ESN numaralarının sınırlı sayısından dolayı ESN yerine geçen 56 rakamlı bir numaradır. MEID onaltılık düzende listelenir. İlk bayt bölgesel kod, sonraki üç bayt imalatçı kodu ve kalan üç bayt imalatçıya tahsis edilmiş seri numarasıdır. CDMA telefonları genellikle SIM kartı içermez ama bazı yeni karma telefonlar ikili CDMA ve GSM teknolojisi içerir ve bu telefonlar ya CDMA ya da GSM ağlarında kullanılabilir. Bu ikili teknoloji telefonlarının içinde SIM kart için bir yuva bulunur. Bu telefonların bataryalarının altındaki tanımlama bilgisi, ESN/MEID numarasına ek olarak bir IMEI numarası listeleyebilir.

CDMA telefonlarının ayrıca iki diğer tanımlama numarası vardır. Bunlar Mobil Kimlik Numarası (MIN) ve Mobil Rehber Numarası (MDN)'dir[132]. MIN taşıyıcıya tahsis edilmiş, taşıyıcıya özgü 24 rakamlı (10'luk tabanda) telefon numarasıdır. Bir arama geldiğinde, telefon ESN ve MIN numarasını yerel kuleye iletir. MDN telefonun dünyada eşsiz olan telefon numarasıdır. Kablosuz Numara Taşınabilirliğinden önce, MIN ve MDN aynıydı, fakat günümüz şartlarında müşteriler taşıyıcıları değiştirseler bile, telefon numaralarını (MDN) ellerinde bulundurabilirler.

5. GSM Cep Telefonları

Uluslararası Mobil Ekipman Kimlik numarası (IMEI) 15 basamaklı, özgün bir sayıdır. Bu numara genellikle cep telefonunun bataryasının altında bulunur. İlk

---

129https://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf Et:02.01.2015

130 http://en.wikipedia.org/wiki/Electronic_serial_number Et:02.01.2015

131 Murphy, Cynthia. "Cellular Phone Evidence Data Extraction and Documentation". Retrieved 4 August 2013. https://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf

132 http://en.wikipedia.org/wiki/Mobile_identification_number Et:05.01.2015

8 basamak Tip Ayırma Kodu (TAC), sonraki 6 basamak Cihaz Seri Numarası (DSN)'dir. Son basamak kontrol basamağıdır ve genellikle 0 olarak belirlenir[133]

GSM telefonunda en azından bir adet SIM kart yuvası bulunur ve bu numara da bataryanın altında yer alır. SIM kart, kartın kayıtlı olduğu şebeke ismiyle markalanabilir. Ayrıca SIM kart üzerinde Entegre Devreli Kart Tanılama (ICCID) numarası yer alır. Bu, 18 ila 20 basamaklı (10 Bayt), her bir SIM kartı tanılama özelliğine sahip özgün bir numaradır. ICCID numarası, Uluslararası Mobil Abone Kimlik (IMSI) numarasına bağlı, genellikle 15 basamaklı (56 rakam) bir numaradır. Elektronik olarak SIM içerisinde depolanan üç bölümden oluşur: Mobil Ülke Kodu (MCC; 3 basamaklı), Mobil Şebeke Kodu (MNC; Amerika ve Kanada'da 3 basamaklı, diğer yerlerde 2 basamaklı) ve Mobil İstasyonu Kimlik Numarası (MSIN; Amerika ve Kanada'da 9 basamaklı, diğer yerlerde 10 basamaklı). IMSI, SIM kartın analiz edilmesiyle ya da taşıyıcı aracılığıyla elde edilebilir.

6. Çıkarılabilir Hafıza

D. Hazırlık (Preparation) Safhası

Sürecin Tanılama Safhasında inceleme uzmanı, telefonun incelenmesi öncesi yapılan önemli hazırlıklara dâhil olmuş olur.[134] Bununla birlikte hazırlık safhası incelenecek belirli mobil cihaz, inceleme esnasında kullanılacak uygun araçlar ve inceleme için gereken tüm donanım, kablolar, yazılım ve sürücülerin yerli yerinde olduklarından emin olmak için inceleme makinesinin hazırlığı konularında daha çok özel araştırmaları kapsar.

İnceleme uzmanının telefondan istenilen veriyi çıkartmak için hangi araçların uygun olduğuna karar vermesi maksadıyla çok özel bir cihazı araştırması, ancak mobil cihazın yapım ve modeli tanımlandıktan sonra mümkün olabilir.Phonescoop.com ve mobileforensicscentral.com gibi kaynaklar, cep telefonları ve belirli telefonlardan verilerin çıkartılması ve belgelendirilmesi için hangi araçların işe yarayacağı konusuna açıklık getirmede oldukça değerli olabilir.SEARCH arama çubuğu (www.search.org adresinden ücretsiz

133 http://tr.wikipedia.org/wiki/IMEI Et:05.01.2015
134 Ramabhadran, Anup. forensıc ınvestıgatıon process model for wındows mobıle devıces.s 8-16 http://www.forensicfocus.com/downloads/windows-mobile-forensic-process-model.pdf

indirilebilir) cep telefonu incelemelerinde ekstra ve düzenli olarak güncellenen kaynaklar içermektedir.135

1. Uygun Araçların Seçimi ve kapasiteleri

Mobil bir cihazın incelenmesi için uygun araçlar incelemenin amacı, incelemeden sorumlu organizasyonun ulaşabileceği kaynaklar, incelenecek cep telefonunun tipi ve harici depolama kapasitesinin varlığı gibi faktörlere göre belirlenir.

Piyasada inceleme uzmanının karşılaşacağı ve işleme alacağı cep telefonu ve diğer mobil cihaz modellerinden elde edilecek tüm veriler için yeterli olacak tek bir cihaz yoktur.[136]Tam aksine piyasada bugün hala içindeki bilgilerin sadece manuel olarak çıkartılmasının ve belgelendirilmesinin yapıldığı çok sayıda telefon vardır. Mevcut cihazların çeşitliliğinin hızlı ve yoğun bir şekilde değişmesine bağlı olarak piyasadaki çeşitli telefon verisi çıkartma cihazlarının farklı tipteki telefonları işlemden geçirme konusunda kapasiteleri birbirinden farklıdır.

2. Obje Çıkarımı

Bu terimler genellikle bir cep telefonundan çıkartılan metin mesajı, arama geçmişi, resim, video, zil sesi tonu, takvim gibi belirli tip ve tiplerdeki verilerle ilgilidir. Bir araç herhangi bir modeldeki telefondan bir veya daha fazla sayıda veri konteynır çıkarımında destek sağlayabilir. Nesne çıkarımı yazılımın telefondaki dosya sisteminin belirli bir bölgesinde depolanan veriye ulaştığı mantıksal yâda fiziksel bir çıkarım fonksiyonudur.

3. Mantıksal Çıkarım

Bu terimler bir cep telefonundan tüm dosya sisteminin çıkarılmasıyla ilgilidir. Bununla birlikte bazı bayiiler mantıksal edinimi bir telefondan özel bir veri tipini elde etme yeteneği olarak tanımlarlar. Bu terim genellikle bir cep telefonundan tüm dosya sisteminin çıkartılması ile ilgilidir. Ayrıca cihazın

---

135 Murphy, Cynthia. "Cellular Phone Evidence Data Extraction and Documentation". Retrieved 4 August 2013. https://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf

136 Murphy, Cynthia. "Cellular Phone Evidence Data Extraction and Documentation". Retrieved 4 August 2013. https://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf

içindeki çıkabilen medya kartlarından dosya sisteminin çıkartılması ile de ilgili olabilir.

4. Fiziksel Çıkarım

Bu terimler cep telefonundaki bir veya daha fazla hafıza kartının ya da cep telefonu dâhili hafızasının çıkartılması ile ilgilidir. Fiziksel çıkarım, fiziksel edinim ya da bellek dökümünden gelene veri ham veri formunda onaltılık döküm şeklinde gelir. Bu terim özel bir cep telefonu adli bilişim işlemi ya da veri çıkarımının hangi özel yapılı ve modeldeki cep telefonu ya da mobil cihazdan alınabileceğini tanımlamak için yakın geçmişte ortaya çıkmıştır.

5. Cihaz Analiz Seviyeleri

Cep telefonlarının analizi için uygun araçlar belirlemede yararlı olacak bir örneklem Cep Telefonu araç düzeyleme sistemidir.[137]Bu sistem mobil telefon ve GPS adli bilişim analizi araçlarının verilen bir cihazda ulaşabildikleri veri derinliğine göre kategorize edilmeleri için tasarlanmıştır. Genel anlamda piramidin üst basamaklarına doğru çıktığınızda;

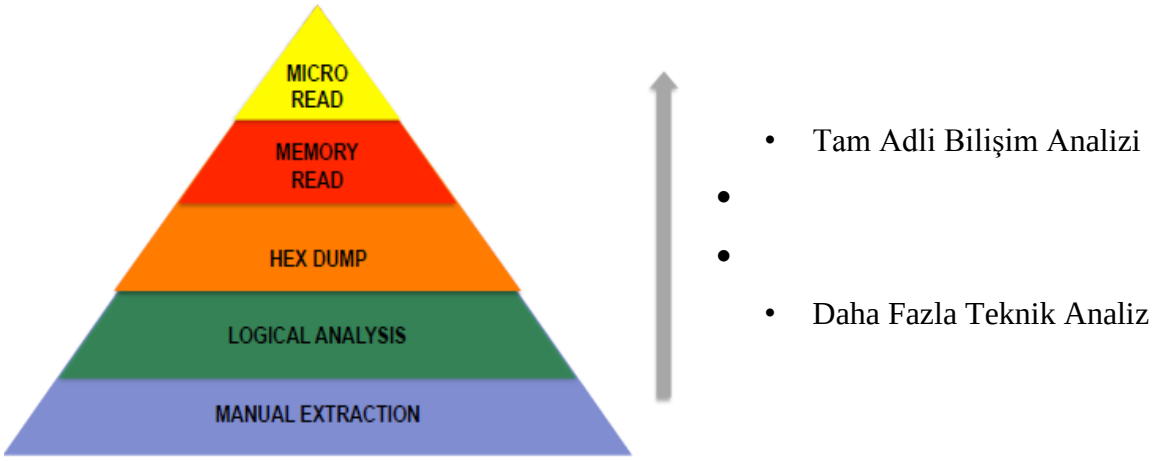
- Daha detaylı adli yöntemler kullanılır
- Araçlar daha pahalı hale gelir
- Yöntemler daha teknik bir hal alır
- Analiz süreleri daha da uzar
- Daha fazla eğitim gerektirir

Piramidin en alt basamağı: Manuel çıkarım, İkinci basamağı: Mantıksal Analiz,Üçüncü Basamağı: Hex Dökümü, Dördüncü Basamağı: Çip Çıkarımı ve en üst son basamak olan Beşinci (En üst) basamağı: Mikro okumadır.[138]

---

137 MURPHY, Cindy. Cellular Phone Evidence Data Extraction and Documentation. 2011. http://digitalforensicsmagazine.com/blogs/wp-content/uploads/2010/07/Cell-Phone-Evidence-Extraction-Process-Development-7.8.pdf Et:03.012015

138 AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. Guidelines on mobile device forensics. *NIST Special Publication*, 2013, 800: 101.page.17-18 http://www.nist.gov/forensics/research/upload/draft-guidelines-on-mobile-device-forensics.pdf



Şekil 20-Akıllı Telefon Analiz seviyeleri[139]

E. İzolasyon (Isolation) safhası

Cep telefonları ve diğer mobil cihazlar, cep telefonu ağları ve diğer ağlar aracılığıyla iletişim kurmak amacıyla tasarlanmışlardır. Ayrıca diğer ağlara Bluetooth, kızılötesi ve kablosuz (Wi-Fi) ağlar aracılığıyla bağlanırlar. Bu sebeple inceleme öncesinde cihazın bu iletişim kaynaklarından ayrıştırılması önemlidir.Telefonun söz konusu kaynaklardan ayrıştırılması, gelen aramalar ve metin mesajları yoluyla telefona yeni bilgi eklenmesini engeller.[140]Ayrıca "ölü sinyal" aracılığıyla uzaktan erişim veya uzaktan silme yoluyla verinin yok edilme ihtimalinin de önüne geçer. Bir başka önemli nokta da yeni aramalar ve metin mesajları geldiğinde var olan verinin üzerine yanlışlıkla yeni veri yazılma ihtimalinin önüne geçilmesidir. Eğer telefon ağdan izole edilirse, inceleme uzmanı yanlışlıkla sesli mesaja, e-maile, internet tarama geçmişine ya da cihazın kendisinden ziyade servis sağlayıcısının ağında depolanmış olan diğer verilere ulaşamaz.

Bir cep telefonunun izole edilmesi Faraday çantası ya da bu amaçla tasarlanmış radyo frekansı koruma kalkanları ile yapılabilir. Çeşitli katmandaki folyolar gibi diğer mevcut maddeler de bazı cep telefonlarının ayrıştırılmasında

---

139 BROTHERS, S. How Cell Phone" Forensic" Tools Actually Work-Proposed Leveling System. *Mobile Forensics World, Chicago, US*, 2009. http://www.lb7.uscourts.gov/documents/10-380316.pdf

140 AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. Guidelines on mobile device forensics. *NIST Special Publication*, 2013, 800: 101.page 28 http://www.nist.gov/forensics/research/upload/draft-guidelines-on-mobile-device-forensics.pdf

kullanılabilir. Bununla birlikte hem resmi hem de gayri resmi faraday metotları ve cihazları başarısız sonuçlar vermeye eğilimlidirler [141]. Bu ayrıştırma metotları ile ilgili bir başka problem de bu metotların kullanımı esnasında telefonla çalışmanın zor ya da imkânsız olmasıdır.Çoğu kurumda bu tarz cihazların kullanımı yasa dışıdır ve ancak belirli bir kurum için bu tür cihazların kullanımının yasal olduğu doğrulandıktan sonra kullanılabilirler.

Bir diğer uygulanabilir seçenek cep telefonunun radyo frekansı koruma kumaşına sarmak ve sonra telefonu uçak moduna almaktır. Cep telefonunun uçak moduna nasıl alınacağı üreticinin verdiği telefon kullanma rehberinde bulunabilir.

GSM cep telefonları için izolasyon SIM ID klonu kullanımıyla yapılabilir. SIM ID klonu cep telefonunun SIM kartının tam olarak klonlanmış kopyası değildir. Daha çok inceleme uzmanının oluşturduğu, orijinal SIM'den sadece ICCID ve IMSI içeren bir karttır[142]. Bu, telefonun etraftaki diğer ağlara bağlanmasına ya da bu ağların telefonu tanımasına izin vermeksizin cep telefonu içeriğinin incelenmesine izin verir. SIM ID klonları oluşturmak için Cellebrite UFED, XRY/XACT ve Adli Bilişim SIM çoklayıcı gibi çeşitli ticari aletler vardır.

Ne yazık ki, tüm telefonlarda uçak modu ya da buna benzer mod özellikleri yoktur ve bazen görünüşte en kusursuz ayrıştırma metotları bile başarısız olabilir. Ayrıca bazı cihazlar tarih ve zaman bilgisini cep telefonu ağından alır ve ayrıştırma hatalı tarih ve zaman bilgisi ile sonuçlanabilir. Bir cep telefonu tüm ağlardan başarılı bir şekilde ayrıştırılsa bile, alarmlar ya da randevu bildirisi gibi otomatik fonksiyonlar ayarlanmışsa, kullanıcı verileri etkilenebilir. Böyle durumların ortaya çıkması durumunda inceleme uzmanının telefonu ayrıştırmak için yaptığı teşebbüsleri ve inceleme süresince gelen herhangi bir aramayı, metin mesajlarını ya da diğer veri aktarımlarını belgelemesi gerekir.

F. İşlem (Processing) Safhası

Telefonun cep telefonundan ve diğer iletişim ağlarından ayrıştırılmasından sonra, telefonun asıl işlem süreci başlayabilir. İncelemenin amacına ulaşması için gereken uygun aletler daha önce bahsedilen adımlarla tanımlanmıştı. Şimdi artık

---

141 KATZ, Eric. A field test of mobile phone shielding devices. 2010.page 1-3 http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1033&context=techmasters

142 AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. Guidelines on mobile device forensics. *NIST Special Publication*, 2013, 800: 101.page 46-48 http://www.nist.gov/forensics/research/upload/draft-guidelines-on-mobile-device-forensics.pdf

bu adımlar telefondan istenilen verilerin çıkartılması için ideal olarak kullanılabilirler.

Çıkartılabilir veri depolama kartları mümkün olduğunda telefondan ayrı olarak işlenebilirler, cep telefonunun inceleme süreci esnasında bu kartlarda depolanan verilere ulaşım, veri depolama kartı üzerindeki verileri değiştirebilir. Yüklenmiş herhangi bir veri depolama/hafıza kartları telefonun incelenmesinden önce cep telefonundan çıkartılmalı ve veri depolama/hafıza kartlarında depolanan dosyaların tarih ve zaman bilgisini oluşturmak için kullanılan geleneksel bilgisayar adli bilişim metotları inceleme esnasında değiştirilmelidir.[143]İnceleme uzmanının işlem için gereken aletlerinin olmaması ya da veri kartının telefona kilitli ya da şifrelenmiş olması durumunda, telefon olmaksızın veriye erişimin sağlanamaması gibi çıkartılabilir veri depolama kartının telefondan ayrı olarak işleme tabi tutulmasının mümkün olmadığı durumlar vardır. Bu gibi durumlarda telefonun ve kartın işlendiği zamanın belgelenmesi oldukça önemli olup bu işlem telefon üzerinde de imaj alınarak yapılabilir.

Cep telefonunun incelenmesi esnasında kullanılan yazılım ve donanım araçlarının sırasına önem verilmelidir. Bir cep telefonunun incelenmesi esnasında kullanılan araçların düzeni avantaj getirir. Bu düzen inceleme yapan uzmanın sonraki bir zamanda yapılacak incelemede araçların sırasını hatırlamasına yardımcı olur. Ayrıca, şartlara bağlı olarak inceleme esnasında incelemenin amaçlarına dayanarak öncesinde ya da sonrasında daha intrüsif araçların kullanılması mantıklı olabilir. Örneğin incelemenin amacı silinmiş bilgileri telefonun fiziksel hafızasından çıkartmaksa, incelemeye hafızanın çıkartılmasıyla başlamak (eğer bu fonksiyon için uygun aletler mevcutsa) telefondan dosya sistemini ya da bireysel dosyaları çıkartmaktan daha mantıklı olacaktır. Aynı cihazdan çok sayıda farklı veri çıkarımı yapmak da telefondan elde edilen verinin çözümlenmesinde yardımcı olabilir.

G. Doğrulama (Verification) Safhası

Telefon işleme tabi tutulduktan sonra, inceleme uzmanının telefondan çıkartılan veriyi bir şekilde doğrulaması gerekir. Cep telefonu araçları için hatalı ya da eksik bir biçimde veri raporlamak ya da aletten alete çelişkili bilgi rapor etmek ne yazık ki olağandışı bir durum değildir. Çıkartılan verinin doğrulanması çeşitli şekillerde yapılabilir.

---

143 Murphy, Cynthia. "Cellular Phone Evidence Data Extraction and Documentation". Retrieved 4 August 2013 page 6-7 https://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf

1. Çıkartılan Verinin Telefondaki veri ile Karşılaştırılması

Çıkartılan verinin kıyaslanması basit anlamda mobil cihazdan çıkartılan verinin, cihazın kendisi tarafından gösterilen veriyle uygun olduğundan emin olmak için kontrol etmek gerekir. Bu karşılaştırma, cihazların telefon bilgisini doğru olarak rapor ettiklerinden emin olmak için tek güvenilir yoldur. Bu karşılaştırma işlemi HASH dediğimiz; Değişken uzunluklu veri kümelerini, sabit uzunluklu veri kümelerine haritalayan matematiksel algoritma programdır[144.] Çeşitli Hash algoritma türleri olup bunlar 128 bitlik (hexadecimal özet değer oluşturabilen MD2, MD4,MD5 ile Secure Hash Algorithm (SHA) algoritması olup bu algoritmanın "SHA-1, SHA-2, SHA-256, SHA-384 ve SHA-512" olarak birçok çeşidi bulunmaktadır.

Eğer fiziksel çıkarım ya da dosya sistemi çıkarımı destekleniyorsa çıkartılan verinin doğrulanması amacıyla geleneksel adli bilişim araçları kullanılabilir. Bu, sonuçların araç tarafından rapor edilen sonuçlarla tutarlı olmalarını sağlamak amacıyla hexin manuel olarak incelenmesi ve verinin şifresinin çözülmesi yoluyla gerçekleşir. Bu metot, verinin kontrol edilmesi için geleneksel dijital adli bilişim yöntemlerini kullanır, ancak daha yüksek seviyede uzmanlık ve deneyim gerektirir. Farklı mobil cihazlarda kullanılan çok sayıda dosya formatı ve şifreleme yöntemi bulunmaktadır.

2. Birden Fazla Araç Kullanılarak Sonuçların Karşılaştırılması

Çıkartılan verinin doğruluğunu sağlamak ve aletten alete rapor edilen veri sonuçlarını kıyaslayarak çapraz doğrulama yapmak için bir başka yol da cep telefonundan veri çıkartmak için birden fazla araç kullanılmasıdır.[145] Çelişkilerin olması durumunda, inceleme uzmanı telefondan çıkartılan verinin doğruluğunu onaylamak için başka yollar denemelidir. Her iki alet de tutarlı bir biçimde bilgi rapor etmiş olsa bile, ahizenin manüel olarak incelenerek doğrulama yapılması gerekir çünkü her iki aletin de hatalı bir şekilde rapor etme olasılığı olabilir.

Bazı durumlarda, telefondan çıkartılan bilginin doğruluğunu onaylamak için doğrulama tekniklerinin bir kombinasyonu da kullanılabilir.

---

144 http://fdset.org/cms/images/Computer%20Forensics.pdf et:01.03.2015

145 CASEY, Eoghan; TURNBULL, Benjamin. Digital evidence on mobile devices. *Eoghan Casey, Digital Evidence and Computer Crime. Third Edition. Forensic Science, Computers, and the Internet, Academic Pres,* 2011.s:40 http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf

H. Belgelendirme/Raporlama (Documentation/Reporting) Safhası

İncelemenin belgelendirilmesi, inceleme sırasında ne yapıldığı göz önünde bulundurularak işlem yapılan süre boyunca eş zamanlı biçimde yapılmalıdır.[146]İnceleme kâğıtları, temel bilginin kaydedildiğinden emin olmak için inceleme sürecinde yararlı olabilir.

İnceleme uzmanının notları ve hazırladığı belgeler şu bilgileri içerebilir:[147]

- İncelemenin başlatıldığı tarih ve saat
- Telefonun fiziksel durumu
- Telefonun resimleri, bireysel içerikler (ör., SIM kart ve bellek genişletme kartı) ve tanımlayıcı bilgi etiketi
- Alındığında telefonun durumu (açık ya da kapalı)
- Yapım, model ve tanımlayıcı bilgi
- İnceleme esnasında kullanılan aletler
- İnceleme esnasında hangi verilerin belgelendiği bilgisi

Çoğu cep telefonu adli bilişim analiz yazılımı raporlama fonksiyonları içerir, fakat bu fonksiyonlar belgelendirme için yeterli olmayabilir. Bazen cep telefonu aletleri yanlış ESN, MIN/MDN numaraları, model ya da hatalı tarih ve zaman bilgisi gibi yanlış bilgi rapor edebilirler. Dolayısıyla veri doğrulama safhasından sonra doğru bilgiyi belgelendirmek için özen gösterilmelidir.

Telefondan veri çıkartmak için kullanılan işlem, çıkartılan ve belgelenen veri türleri ve konuyla ilgili herhangi bir bulgu, raporlarda doğru bir şekilde belgelenmelidir. İnceleme uzmanı mevcut aletleri kullanarak istenilen veriyi çıkartmada başarılı olsa bile, bilginin fotoğraflarla belgelendirilmesi özellikle de mahkemeye sunulmak amacıyla yapılan işlemlerde yararlı olabilir.

1. Saat Dilimi Ayarları

Mobil adli bilişim yazılım araçlarının standartlaştırdığı diğer formatlarla rapor edilen tarih ve zaman bilgilerine özel ilgi gösterilmesi gerekir. Çoğu alet,

---

146 https://www.ncjrs.gov/pdffiles1/nij/199408.pdf Et:05.03.2015 s:28
147 Murphy, Cynthia. "Cellular Phone Evidence Data Extraction and Documentation". Retrieved 4 August 2013 page 6-7 https://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf

inceleme uzmanının tarih ve zaman bilgisini yerel saat dilimine göre ayarlamasına olanak sağlar, fakat olay her zaman bu değildir. Raporu okuyan diğer insanların yanlış anlama ya da verilen detayları kaçırma ihtimalleri göz önünde bulundurularak saat dilimi ve gün ışığından daha fazla yararlanma ayarlarının ya da standart saat bilgisinin izahının yapılması gerekir. Yanlış anlaşılmalar, araştırmacıların ilgili konuyu kaçırmalarıyla sonuçlanabilir. Raporunuzda saat dilimi ayarlarının yapıldığını ya da yapılmadığını belirtmeniz, daha sonra karşılaştığınız bir olayda zaman kazanmanıza, ilgili saat farklarının karışıklık yaratmasını önlemeye ve izahının yapılmasına yardımcı olur.

İ. Sunum/Arşiv (Presentation/Archiving) Safhası

Mobil cihazdan bilginin nasıl çıkartıldığı ve belgelendirildiğinin net ve doğru bir şekilde başka bir uzmana, savcıya ya da mahkemeye sunulmasına önem verilmelidir. Çoğu durumda alıcı, arama geçmişinin ya da diğer verilerin ilerleyen analizlerde sınıflandırılabilmesi ya da diğer yazılımlara aktarılabilmesi için çıkartılan verinin hem kâğıt üzerinde hem de elektronik formatta sunulmasını isteyebilir.

İnceleme uzmanı ayrıca tarih ve zaman bilgisinin kaynağı, görsellerden ya da diğer veri formatlarından alınan EXIF verisi ile ilgili referans bilgisi almak isteyebilir. Böylelikle veriyi alanlar bilgiyi daha iyi anlarlar.

Exif verisi; (Exchangeable image file format), Türkçesiyle değiş-tokuş yapılabilir görüntü dosyası biçimi, sayısal fotoğraf makineleri (cep telefonu / akıllı telefonlardakiler dahil), tarayıcı, kamera vb. cihazlar tarafından kaydedilen görüntü ve ses dosyalarının içerisine çekilen medya ile ilgili metadatanın (enstantane, diyafram,pozlama, fotoğraf makinesi markası, modeli, çekim tarihi vb.) gömülmesini sağlayan, bir veri tanımlama standardıdır.[148]

Verilerin cep telefonundaki halleriyle resimlerinin ya da videolarının olması adli amaçlar için yarar sağlayabilir. Çıkartılan metin mesajları büyük bir kanıt oluşturabilir, ama aynı metin mesajlarının resimlerinin olması mahkeme önüne sunmak adına daha yaygın ve görsel olarak daha zorlayıcı bir unsur olabilir.

İzleyici ister bir yargı üyesi, ister bir uzman, isterse bir topluluk olsun, iletişim ilerleyişinin daha net gösterilmesi için PowerPoint sunum ya da zaman çizelgesi yazılımı aracılığıyla metin mesajlarının ve arama geçmişi günlüklerinin kronolojik

148 http://tr.wikipedia.org/wiki/Exchangeable_image_file_format Et:21.04.2015

sırayla sunulması her zaman daha çok yarar getirir. Bu tutum, bir olaya karışan birden fazla cep telefonu olması durumunda etkilidir.

Cep telefonundan çıkarılan ve belgelendirilen verinin korunması tüm sürecin önemli bir parçasıdır. İlerideki mahkeme işlemleri, bilirkişi raporu ve kayıt saklama gereklilikleri sebebiyle verinin kullanılabilir bir formatta muhafaza edilmesi gereklidir. Bazı vakaların nihai bir çözüme kavuşturulması çok seneler alabilir ve birçok yargı yetkisi bu verinin değişik zamanlarda başvurulması amacıyla muhafaza edilmesini ister.

Cep telefonu verilerinin çıkartılması ve belgelendirilmesi amacıyla piyasada var olan çeşitli adli bilişim araçlarının telifle korunuyor olmasına bağlı olarak kaydedilen veriye sonraki bir tarihte ulaşılabilme yeteneği üzerine düşünmek gerekir. Eğer mümkünse veriyi hem telifle korunan hem de korunmayan formatta standart ortamda kaydedin. Böylece orijinal yazılım aracının olmadığı durumda, olaydan sonra dahi veriye ulaşım sağlanabilecektir. Yazılımın kendisinin de bir kopyasının muhafaza edilmesi sonraki bir tarihte verinin yerinde incelenmesini kolaylaştıracaktır.

7.MOBİL CİHAZLARIN ADLİ BİLİŞİM YAZILIMLARI İLE ANALİZ EDİLMESİ (ÖRNEK CİHAZ İNCELEMELERİ)

A. Araştırma Metodolojisi

Piyasada mobil cihazlar üzerinde adli bilişim incelemesi gerçekleştirmek için kullanılan ve bu işleri gerçekten de çok iyi yapan yazılım ve donanım çözümleri bulunmaktadır.

Bu bölümde farklı platformalar ve farklı işletim sistemleri ait "Smart Phones –Non Smart" cihazların farklı adli bilişim yazılımları ile analizleri yapılarak etkinliği ve avantaj/dezavantajları araştırılıp incelemeler açısından da bir farkındalık ortaya konulacaktır. Öncelikle cihazların imajı alınarak işleme başlanacak olup iki tür imajdan bahsedilmektedir.

1. Mantıksal İmaj

Mantıksal imaj, aktif dosya sisteminde yer alan dosyaları başka bir sisteme kopyalayıp, inceleme işlemine verilen addır.[149]

2. Fiziksel İmaj

Mobil cihaz üzerindeki NAND Flash diskin imajının bit-by-bit alınması işlemidir. Silinmiş verilerin kurtarılması noktasında çok daha başarılı sonuçlara ulaşılmasına imkân tanır.[150]

Her iki yöntemde ortak olan ve analiz işleminden önce yapılması gereken bazı önemli işlemler mevcut olup bu durum telefonun zarar görmemiş hali düşünülerek yapılması gerekmekte olup bu işlemler Akıllı telefonlarda Rooting ve jailbreak işlemleridir.

3. Test Ortamı ve Gereksinimler

Bir adli bilişim delil incelemesi ve analizi yapılacak bir bilgisayarda birçok adli bilişim yazılımı ve donanımı bulunması gerekmektedir. Mümkünse hem ücretli hem de açık kaynak yazılımlar kullanılması fayda sağlayacaktır.

Bu araştırmada kullanılan donanım ve yazılımlar:

---

149 http://www.bilgiguvenlik.net/2012/05/ios-forensic.html/ Et:11.03.2015
150 http://www.bilgiguvenlik.net/2012/05/ios-forensic.html/ Et:11.03.201

- Windows 7 Professional 64-bit işletim sistemi 4 Gb Ram
- Samsung GT-N7100 Note II 10 Gb Dâhili “Android 4.4.1Kit Kat” Akıllı Telefon
- Samsung Monte S5620 256 Mb Dahili / 256 MB SD kart hafıza Samsung OS
- Nokia 5800 126 Mb dahili/ 8 Gb Harici Bellek Symbian v9.4
- Nokia 6300 “Non-smart” 8 Mb dahili hafıza/8 Gb harici Bellek
- Apple Iphone 4S (A1457 çip, 8 GB kapasiteli ve iOS
- XRY 6.11.1
- MobilEdit 7,5
- Oxygen 2014 Suite
- 2 adet Vadofone SIM kart
- Micro Usb kablo
- Iphone Usb Kablo

Bu araştırma da Windows 7 Professional işletim sistemi üzerine yüklenmiş adli bilişim yazılımları “XRY 6.11.1,MobilEdit 7.5 ve Oxygen Suite 2014” kullanılarak mantıksal ve fiziksel imajlar alınmış olup bu işlemler direk yazılımların Grafik (GUI) arabirimleri, Hexa Decimal Editörleri ve SQL lite editör vasıtasıyla yapılmıştır. Alınan fiziksel ve mantıksal imajlar XRY imajları için XRY Reader, MobilEdit kendi bünyesinde bulunan Hex Dump editör ile Oxygen Suite’in kendi üzerinde bulunan SQL lite editör yazılımı ile inceleme işlemi yapılmıştır.

Bu araştırmada daha önce kullanılmış cihazlar ile bu cihazlar üzerinde bulunan veriler analiz için bilinçli bir şekilde silinmiştir. İnceleme yapılan cihazlar üzerinde rooting ve jailbreaking işlemi yapılmıştır. Ayrıca Samsun GT-N7100 üzerinde usb debuggin işlemi gerçekleştirilmiştir.

Aşağıdaki tabloda hangi yazılım ile hangi cihazların kullanıldığı belirtilmiştir.

	Samsung GT-N7100	Samsun S5620	Nokia 5800	Nokia 6300	Iphone 4S
XRY 6.11.6	İncelenmiştir	-	İncelenmiştir.	İncelenmiştir.	-
MOBİL EDİT 7,5	İncelenmiştir	İncelenmiştir	İncelenmiştir	İncelenmiştir.	İncelenmiştir
OXYGEN SUITE 2014	İncelenmiştir	İncelenmiştir	İncelenmiştir	İncelenmiştir.	İncelenmiştir

Tablo 3-İncelenecek Cihaz ve Yazılım tablosu gösterilmiştir

Araştırmada kullanılacak yazılımların genel özellikleri, analiz seviyeli gösteren tablo aşağıda sunulmuştur.

	Analiz seviyesi	Network Tipi			Adli Bilişim Araçları (Forensics Tools)	İnceleme (Examination)	Analiz (Analysis)	Rapor (Report)
		GSM	CDMA	TDMA				
XRY 6.11.6	1-2-3-4-5	+	+	+	+	+	+	+
MOBİL EDİT	1-2-3-4-5	+	+	+	+	+	+	+
OXYGEN	1-2-3-4-5	+	+	+	+	+	+	+

Tablo 4-Yazılımların özellikleri gösterilmiştir

Yapılan analiz sonuçlarında kullanılan cihazlarda bulunan hangi verilerin bulunduğunu gösteren tablolar aşağıda sunulmuştur.

	Cihaz Marka Model	**Analiz Seviyesi**	**Rehber kaydı**	**Arama Kaydı**	**Mesaj (SMS)**	**Dosya Bilgisi**						**Web Kaydı**		**Uygulama**	**Tanımlanayan Dosya**
						Resim	**Video**	**Dosya**	**Ses**	**Veritabanı**	**Arşiv**	**History**	**Bookmarks**		
XRY 6.11.6	Samsung N7100	Mantıksal	584	500	383	1701	71	641	175	34	480	76	35	310	26
	Nokia 6300	Mantıksal	66	132	243	73	16	132	23	2	16	-	-	-	446
	Nokia 5800	Fiziksel	31/9	-	-	803/706	-	71/22	5/2	28/15	-	-	-	-	4990/2326

Tablo 5-XRY Analiz Sonuçları

	Cihaz Marka Model	Analiz Seviyesi	Rehber Kaydı Dahili/Sim	Arama Kaydı			Mesaj SMS Kaydı		Dosya Bilgisi Kaydı						Web Kaydı		Uygulama
				Cevapsız	Giden	Gelen	Gelen	Giden	Resim	Video	Dosya	Ses	Veri Tabanı	Arşiv	History	Bookmarks	-
MOBİL EDİT 7,5	Samsung N7100	Mantıksal	357/226	92	310	75	428	207	-	-	-	-	-	-	200	-	-
	Samsung N7100	Fiziksel	230/157	105	302	69	401	185	-	-	-	-	-	-	-	-	573
	Samsung S5620	Mantıksal	205/40	22	20	21	224	6	-	-	-	-	-	-	-	-	-
	Nokia 5800	Mantıksal	63	19	-	-	20	2	63					-	-	-	-
	İphone 4	Mantıksal	351	-	-	-	100	30	-					-	-	-	-

Tablo 6-Mobiledit Analiz Sonuçları.

	Cihaz Marka Model	Analiz Seviyesi	Rehber kaydı Dâhili/Sim	Arama Kaydı			Mesaj SMS		Dosya Bilgisi kaydı						Web Kaydı Bilgisi		Uygulama
				Cevapsız	Giden	Gelen	Gelen	Giden	Resim	Video	Dosya	Ses	Veri Tabanı	Arşiv	History	Bookmarks	-
OXYGEN SUİTE	Samsung N7100	Mantıksal	593	111	300	83	160	168	49	2	52	1	230	-	2191	58	213
	Samsung N7100	Fiziksel	426	114	306	107	626	264	1231	20	20198	179	834	20933	2054	100	312
	İphone 4S	Mantıksal	-	-	-	-	-	-	147	-	-	-	-	-	-	-	-

Tablo 7-Oxygen Suite Analiz Sonuçları

4. Analizler Esnasında Yaşanan Sıkıntılar

Analiz esnasında kullanılan cihazların işletim sistemleri "IOS, ANDROID ve SYMBIAN" farklı mobil adli bilişim platformlarına ve farklı donanım, yazılımsal ayarlara gereksinim duyabilmekte hatta cihazlara göre bile birçok değişik ayar ve yöntemlere ihtiyaç duyulmuştur. Diğer bir sorun ise cihazların donanım yapısı yüklenen uygulamaların farklılıklar göstermesidir. Ayrıca kullanılan yazılımların ücretli ve çok yüksek maliyetli olmasıdır. Analizi yapılacak cihazların bağlantı şekilleri değiştirmek için yapılan teknik ayar ve yazılım yüklemelerinde işletim sistemi çökmeleri yaşanmış bu cihazların yeniden yüklenmesi yapılmıştır. Bu tanımların açıklaması aşağıda sunulmuştur.

5. Rooting and Jailbreaking

Tüm akıllı cihazlar üzerinde kullanıcı cihaz üzerinde yetkili kullanıcı olmayıp birçok sistem dosyasına erişme yetkisi olmaz.

a) Rooting

Sahip olduğunuz cihaz üzerinde bulunan dosya sistemi dosyalarına erişim yetkisi sağlamakta olup yetkili kullanıcı olunması işlemi olup bu işleme rooting denilmektektedir.[151]

b) Jailbreak

Genelde, Apple'ın iOS İşletim Sistemi yüklü cihazlarına dayattığı kısıtlamalardan kurtulmak için uygulanan yöntem anlamında kullanılır (iPhone, iPad, iPod Touch, Apple TV gibi.[152]

6. Senaryo

Jailbreak ve rooting işleminden sonra telefon tekrar bilgisayara bağlanır. Bu işlem kullanacağımız telefon sürücüleri otomatik olarak yüklenmekte olup eğer gerekli sürücüler analiz için kullanacağımız yazılım bünyesinde olmaz ise internet bağlantı var ise otomatik olarak yüklemeye çalışacak teknik bir sıkıntı yok ise cihaz sürücüleri yüklenecektir.

Bu araştırmada aynı marka ve model cihazlar farklı yazılımlar ile analiz edilecek, Mobil Cihaz "dâhili hafıza, SIM kart ve Harici bellek" üzerinde veri kurtarma işlemi ve analizi yapılacaktır.

---

151 http://www.andropedi.com/root-nedir-android-telefonda-root-ne-ise-yarar/ Et:02.02.2015

152 http://tr.wikipedia.org/wiki/Jailbreak_%28iOS%297 Et:03.02.2015

B. Araştırmalar (Örnek SIM, Dâhili/Harici Hafıza ve Uygulama Analizleri)

1. XRY Analizleri

a) Samsung GT-N7100-Mantıksal İmaj Analizi

Samsung Gt-N7100 akıllı telefonu bilgisayara bağlandığımızda cihaz ile yazılım iletişime geçip bağlanılamamıştır. Kullanılan Usb kablo değiştirilerek Micro Usb kablo kullanılarak bağlantı sağlanabilmiştir.

Analizi yapılacak cihaz 10 Gb dâhili hafıza ve Android 4.4.1 işletim sistemine olan SAMSUNG GT-N7100 marka/model cihaz üzerinde gerçekleştireceğiz. Android cihazlar üzerinde bulunan Dâhili hafıza, SIM kart ve harici bellek üzerinde olabilecek kanıtları bulup ve analiz edeceğiz.

Usb Debugging işlemi yukarıda belirtildiği marka ve model cihazlara göre değişmekte olup bizim incelemeye tabi tutacağımız samsung GT-N7100 marka akıllı telefon için şu şekilde yapılmaktadır. Cep telefonu "Settings,Applications,Development kısmında bulunan girilip "USB debuggin" etkin hale getirilir. Ya da bu işlem için "Thirt Party" bir yazılım kullanılıp yapılabilir. Ayrıca cihazın bağlantı tipi *#7284# sembol ve rakamlar tuşlanarak bağlantı şekli "Usb PDA" cihaz olarak seçilip analiz işlemi yapılmıştır.

Analizini yapacağımız Android cihaz üzerinde Fiziksel veya mantıksal işlem yapmadan önce gerekli ayarlar yapılmış olup birinci aşama sağlanmıştır.

Cihazımı direk bağlandığımızda sürücüler mevcut ise yazılım ile telefon senkronizasyonu sağlanmış olup XRY ile ne tür bir analiz yapacağımızı belirlediğimiz ekran gelmektedir. Gelen ekran üzerinde Mantıksal **"Logical"** analiz türünü seçip analiz işlemine başlanmıştır.

Şekil 21-Samsung GT-N7100 XRY bağlantısı

Yukarı şekilde göründüğü gibi cihazın mantıksal imajı alınmış inceleme bu imaj üzerinde XRY Reader 6.11 ile yapılmıştır.

XRY ile inceleme yaparken yazma koruma modu otomatik olarak etkinleşmekte ve analiz işlemi esnasında cihaza herhangi bir veri girdisi yapılması engellemektedir. Ayrıca cihaz Uçak moduna alınarak izolasyon işlemi yapılmış, arama ve mesaj gelmesinde engellenmiştir. Aşağıdaki şekilde XRY tarafından görülen cihaza ait bilgiler sunulmuştur. Şekil 20 de XRY tarafından tespit edilen cihaza ait tanımlayıcı temel bilgileri "cihaz türü, yazılım düzeyi, mobil bilgileri veri toplama başlama/bitiş zamanı gibi bilgileri gösterilmiştir.

General information about the device

Model Picture: Actual Picture:

Subscriber Id (IMSI)	286020320123263
SIM Identification (ICCID)	8990029300291286537
Network Code (from IMSI)	28602
Mobile Id (IMEI)	356000056562606
Manufacturer	samsung
Model	GT-N7100
Revision	4.4.2/KOT49H/N7100XXUFND4
Device Clock	21.01.2015 17:21:56 UTC+02:00, Doğu Avrupa Standart Saati (Device)
PC Clock	21.01.2015 17:21:54 UTC+02:00, GTB Standard Time
WiFi Address	88:32:9B:DA:A1:71
Model	GT-N7100
Manufacturer	samsung
Device Name	t03gxx
Device Name	t03gxx

Şekil 22-XRY ile tespit edilen Samsun GT-N7100 cihaz bilgisi

Cihaz Üzerinde tespit edilen kayıt bilgiler aşağıda olduğu gibidir:

- Telefon rehberi "Phonebook" kaydı :(584) ad,
- Arama "calls" kaydı 500 ad.
- Takvim "calendar" 47 ad.
- Mesaj "Message" kaydı 383
- Web "Log" 500 ad.

  Web History 76 ad.

  Web bookmarks 35 ad.

  Web Searches 3 ad.
- Dosya "files" kaydı

  Resim "Pictures" 1701,

  Video "Videos" 71,

  Ses "Audio" 175

  Doküman "Document" 641

  Arşiv "Archives" 480

  Veritabanı "Database" 34

  Tanımlanamayan "Unrecognized" 26

- Uygulama “Application” 310

(1) SIM Analizi

XRY ile analizi yapılacak cihazın üzerinde root işlemi yapılmadığı takdirde SIM üzerindeki arama “Call Sim” kayıtlarına erişim sağlanamamaktadır.Bu bilgi Samsung GT-N7100 analizi Device Overview bölümünde “XRY can retrieve additional data like e-mail and application data such as chat messages,call logs,locations and web history on Android When devices is “Rooted”. Şeklinde bir teknik uyarı mevcuttur.

Samsung GT-N7100 üzerinde de analiz öncesinde her hangi bir Root işlemi yapılmadığı için yalnızca SIM kart üzerindeki “Calls Sim” kayıtlarına erişim sağlanamamıştır. Bu noktada yasal süreç işletilerek abonenin bağlı olduğu operatör aracılığı ile CDR “Call detail record” Erişim sağlanabilir.

(a) SMS Kayıtları

XRY Analizi ile yapılan analiz sonucunda cihaz üzerinde 383 adet silinmiş SMS kaydına ulaşılmış olup Mesaj “Messages” Menüsü altında bulunan SMS sekmesine girdiğimizde aşağıda silinen SMS kaydına ulaşılmıştır.

Şekil 23 XRY ile Tespit Edilen Samsung GT-N7100 SMS kaydı

(b) Arama Kayıtları

Toplamda 500 adet arama kaydına ulaşılmış, “ 15 adet Giden arama, 25 gelen arama 15’i” ise cevapsız çağrı olarak görülmektedir. Bu kayıtlara CALLS menüsü altıdan ulaşılmıştır. XRY ile yapılan analiz de geçmiş tarihe ait arama kayıt örneği Şekil-24’de gösterilmiştir.

Şekil 24-XRY ile Tespit Edilen Samsung GT-N7100 Tespit Edilen Arama Kaydı

(2) Dâhili/Harici Hafıza Analizi

(a) Dosya Kayıtları

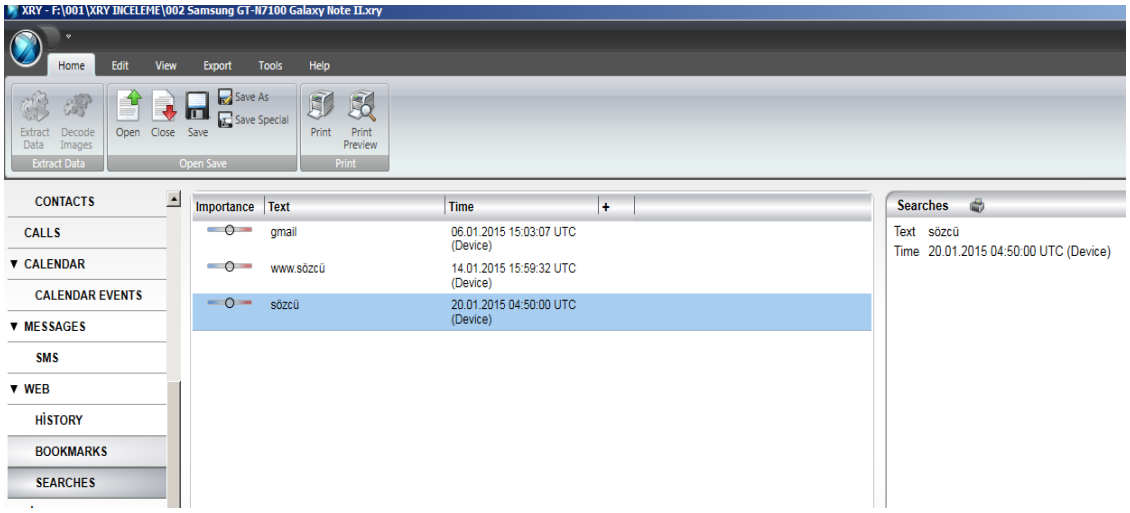
XRY ile yapılan çalışmada telefon kamerasından çekilen dâhili/ harici hafızadan “1701 adet resim, 71 video ve 175 ses dosyası ile 641 doküman, 480 arşiv,34 adet database ve 2622 unrecognized” kayıt bulunmuştur. Telefonun dâhili ve harici belleğinde bulunan silinmiş verilerin çıkarımı aşağıda sunulmuştur. Video dosyaları **/mnt/Shell/emulated/0/DCIM/Camera** altında Ses dosyaları dosyaları

/mnt/Shell/emulated/0/Music/ altında resim dosyaları dosyaları **/mnt/Shell/emulated/0/DCIM/.Thumbnails** altında ve diğer dosyalar ise dosyaları **/mnt/Shell/emulated/0/Downlaod** altında bulunmuştur.

(3) Uygulama Analizi

(a) Web Geçmişi

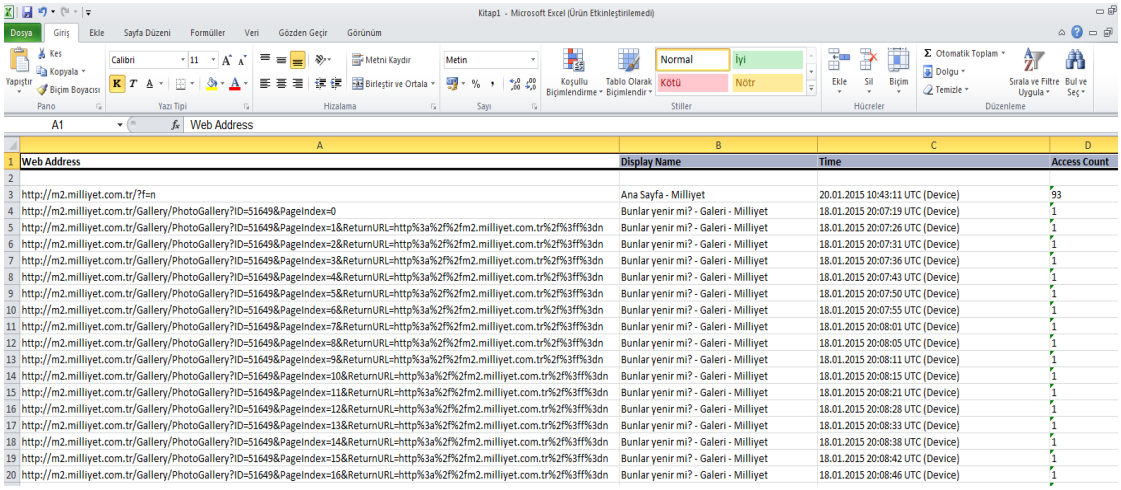
Bu analiz de incelenen cihaz akıllı olması sebebiyle XRY.6.11.1'de Web"History, Bookmarks ve Searches" analiz seçenekleri aşağıdaki şekil 25'te gösterilmiştir. Samsung GT-N7100 cihazı ile "76 web history", "35 web bookmarks" ve 3 adet "web search" bilgisi tespit edilmiştir.



Şekil 25-XRY ile Tespit Edilen Samsung GT-N7100 Web History Kaydı

Özellikle bu kısımda web analizi ve SIM kart üzerinde bulunan veriler analiz edilmiştir. Cihaz üzerinde bulunan web sayfaları üzerinde bulunabilecek kanıtlar elde edilmeye çalışılmıştır.

Web sayfası geçmiş " history" kayıt bilgileri XRY web history butonu seçilerek export menüsünden çıkarım yapılarak dosya tipi seçilerek Office Excel formatında çıkarımı yapılarak aşağıda şekil-26'da sunulmuştur.

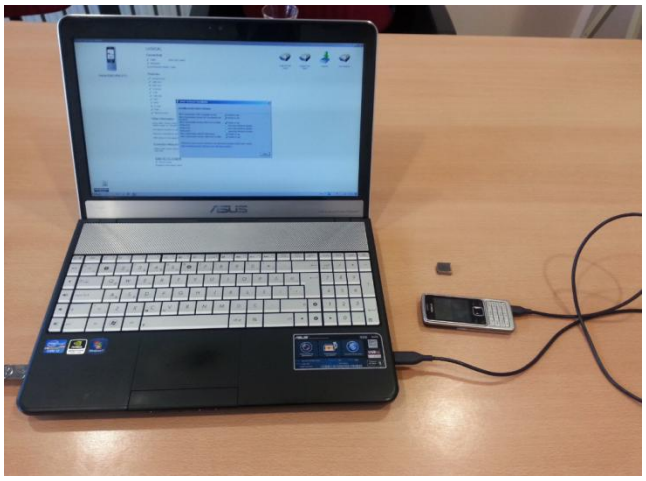


	A	B	C	D
1	Web Address	Display Name	Time	Access Count
2				
3	http://m2.milliyet.com.tr/?f=n	Ana Sayfa - Milliyet	20.01.2015 10:43:11 UTC (Device)	93
4	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=0	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:07:19 UTC (Device)	1
5	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=1&ReturnURL=http%3a%2f%2fm2.milliyet.com.tr%2f%3ff%3dn	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:07:26 UTC (Device)	1
6	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=2&ReturnURL=http%3a%2f%2fm2.milliyet.com.tr%2f%3ff%3dn	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:07:31 UTC (Device)	1
7	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=3&ReturnURL=http%3a%2f%2fm2.milliyet.com.tr%2f%3ff%3dn	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:07:36 UTC (Device)	1
8	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=4&ReturnURL=http%3a%2f%2fm2.milliyet.com.tr%2f%3ff%3dn	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:07:43 UTC (Device)	1
9	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=5&ReturnURL=http%3a%2f%2fm2.milliyet.com.tr%2f%3ff%3dn	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:07:50 UTC (Device)	1
10	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=6&ReturnURL=http%3a%2f%2fm2.milliyet.com.tr%2f%3ff%3dn	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:07:55 UTC (Device)	1
11	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=7&ReturnURL=http%3a%2f%2fm2.milliyet.com.tr%2f%3ff%3dn	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:08:01 UTC (Device)	1
12	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=8&ReturnURL=http%3a%2f%2fm2.milliyet.com.tr%2f%3ff%3dn	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:08:05 UTC (Device)	1
13	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=9&ReturnURL=http%3a%2f%2fm2.milliyet.com.tr%2f%3ff%3dn	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:08:11 UTC (Device)	1
14	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=10&ReturnURL=http%3a%2f%2fm2.milliyet.com.tr%2f%3ff%3dn	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:08:15 UTC (Device)	1
15	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=11&ReturnURL=http%3a%2f%2fm2.milliyet.com.tr%2f%3ff%3dn	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:08:21 UTC (Device)	1
16	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=12&ReturnURL=http%3a%2f%2fm2.milliyet.com.tr%2f%3ff%3dn	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:08:28 UTC (Device)	1
17	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=13&ReturnURL=http%3a%2f%2fm2.milliyet.com.tr%2f%3ff%3dn	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:08:33 UTC (Device)	1
18	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=14&ReturnURL=http%3a%2f%2fm2.milliyet.com.tr%2f%3ff%3dn	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:08:38 UTC (Device)	1
19	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=15&ReturnURL=http%3a%2f%2fm2.milliyet.com.tr%2f%3ff%3dn	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:08:42 UTC (Device)	1
20	http://m2.milliyet.com.tr/Gallery/PhotoGallery?ID=51649&PageIndex=16&ReturnURL=http%3a%2f%2fm2.milliyet.com.tr%2f%3ff%3dn	Bunlar yenir mi? - Galeri - Milliyet	18.01.2015 20:08:46 UTC (Device)	1

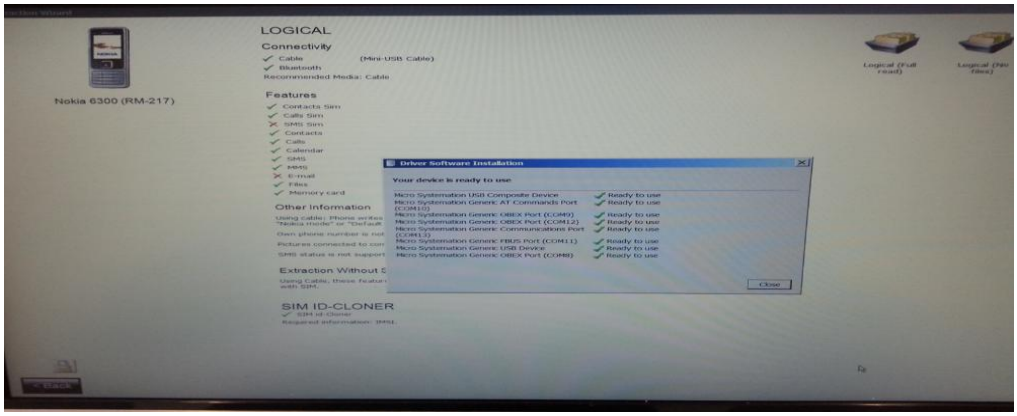
Şekil 26-XRY ile Tespit Edilen Samsung GT-N7100 Web Kaydı

b) Nokia 6300-Mantıksal İmaj Analizi

XRY ile Nokia 6300 marka model cihazımızın fiziksel imaj desteği olmadığı için sadece mantıksal imajı desteklediği için mantıksal imaj işlemi gerçekleştirilmiştir. Bilgisayara bağlanan cihazın yazılım tarafından tanınmasını gerekmekte olup şekil-27'de görülmektedir.



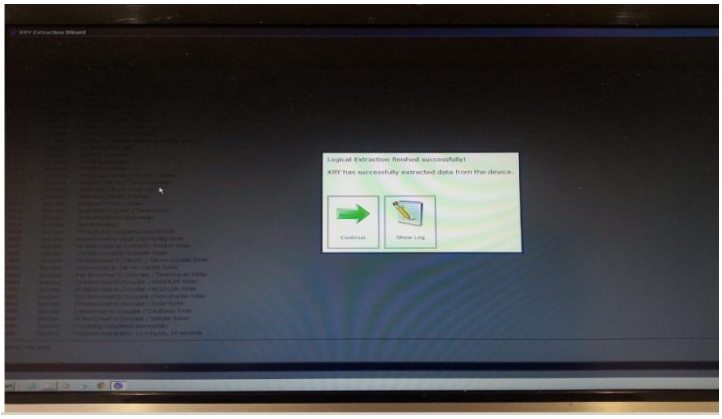
Şekil 27-Nokia 6300 XRY ile Bağlantısı



Şekil 28-XRY ile Tespit Edilen Nokia 6300 Cihaz Bilgisi

Bağlantı işlemi sağlıklı bir şekilde gerçekleştirildikten sonra yazılım donanınım hakkında bilgi toplamı işlemi gerçekleştirmektedir. Tespit edilen bilgiler ilk **Şekil 28'de** gösterilmiştir. Bulunan cihaza ait bilgiler içerisinde bağlantı şeklinin usb kablo ile yapıldığını, SMS ve SIM özelliği ile E-Mail bilgilerinin analiz işleminin gerçekleştiremeyeceğini bildirmektedir. Cihaz akıllı telefon olamadığı için belirtilen analizler pasif durumda gözükmektedir.

Bu aşmadan sonra XRY yazılımı üzerindeki Logical (Full Read) butonuna basılarak veri elde işlemini başlatıyoruz ve bir sonraki adımda karşımıza **"Backup" veya "Agent"** olarak mı işlem yapacağımız sorulmaktadır. Bu iki işlem arasındaki fark, bazı marka model cihazlar üretim şekli sebebiyle mevcut hali ile veri analizi için imkân vermemektedir. Bu kısıtlama işleminin önüne geçmek için cihaza analizi yapılan yazılım tarafında ajan yüklenmesi gerekmektedir. Bu ajan işlem sonunda kullanılan adli bilişim yazılımı tarafından otomatik olarak "Uninstall" edilip kaldırılmaktadır. Analizin bu aşamasında backups seçeneğini seçiyoruz. Bir sonraki analiz adımında alınacak imaj dosyasının nereye kayıt edileceğini sorulmaktadır. Bilgisayarınızın disk durumuna göre tercih yapılması gerekmektedir. Bu analiz için yerel sürücü altında "e:\XRY adında bir klasör oluşturup ileri tuşuna basarak işlemi başlatıyoruz. Aşağıdaki şekilde veri elde işleminin başladığını ve başarılı bir mantıksal imaj aldığımızı yazılım göstermekte olup "Continue" tuşuna basarak yazılım tarafından doğrulama yapılarak işlemi sonlandırıyoruz.



Şekil 29-XRY ile tespit edilen Nokia 6300 analizin son ekran görüntüsü.

Bu işlemin sonunda artık elde ettiğimiz cihaza ait mantıksal imaj "Nokia 6300 (rm-217).xry dosyasını Reader 6.11 ile açıp analiz işlemini gerçekleştirebiliriz. Nokia 6300 cihazı üzerinde işletim sistemi olmayıp 8Mb'lık bir dahili hafıza ve 256 Mb'lık bir SD kart mevcut idi analiz sonucunda "66 adet rehber, 132 arama kaydı, 21 adet takvim, 243/3 SMS/MMS verisi ile "73 adet resim,16 video, 23 Ses, 2 adet veritabanı ve 446 adet dosya kaydı tespit edilmiştir.

Nokia 6300 Üzerinde buluna veri bilgiler aşağıda sunulmuştur.

- Telefon rehberi “Phonebook” (66) adet
- Arama “Calls” kayıtları 132 ad.
- Takvim “Calendar” kayıtları 21
- Mesaj SMS/MMS “Message” bilgisi (243/3)
- Dosya “files” kayıtları

  Resim “Pictures” 73

  Görüntü “Video” 16

  Ses “Audio” 23

  Doküman “Document” 132

  Arşiv “Archives” 16

  Veritabanı “Database” 2

  Tanımlanamayan “Unrecognized” 446

XRY üzerinde “Device” menüsü altında General Information kısmını açtığımızda cihaz **“ marka/model, üretici ve IMEI numarası”** tanımlama bilgilerine ulaşılabilmekteyiz. Analiz sonucunda bulunan kayıtlara ait örneklemeler aşağıda başlıklar altında sunulmuştur.

(1) SIM Analizi

Cihaz üzerinde herhangi bir SIM kart olmadığı için SIM analizi gerçekleştirilememiştir.

(2) Dâhili/Harici Hafıza Analizi

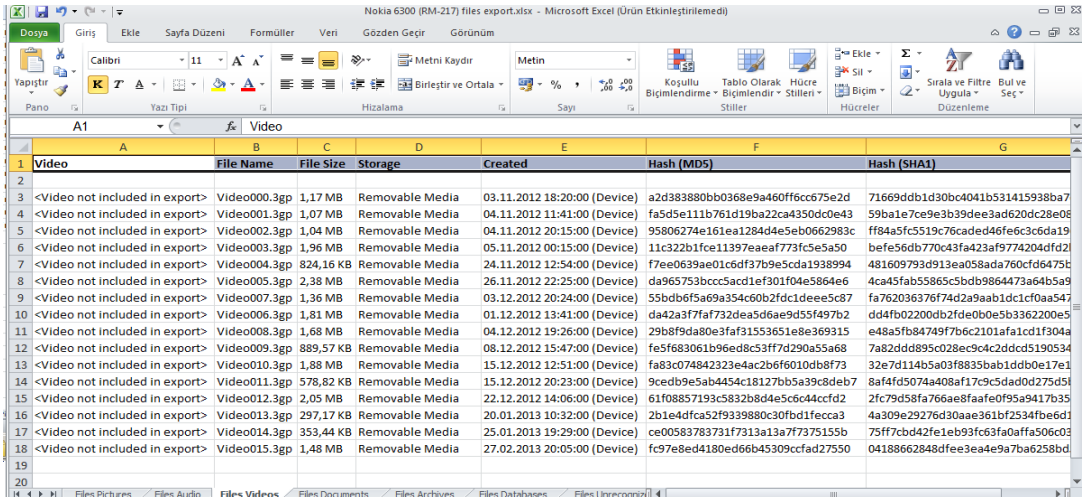
Cihaz üzerinde 256 MB’lık SD kart mevcut olup normal analiz şartlarında cihaz üzerinde herhangi bir Harici hafıza mevcut ise analiz yapılmadan önce çıkarılması gerekmektedir. Çünkü analiz esnasında harici hafızanın üzerindeki dosya sistemi bozulabilir ve üzerindeki bulunabilecek veriler kayıp olabilir. Normal şartlarda harici hafızanın ayrı olarak imajının alınıp analiz edilmesinin faydalı olacağı değerlendirilmektedir.

(a) Dosya Kayıtları

XRY “Files” Menüsü altında bulunan çeşitli Dâhili hafıza ve Harici bellekte rehber bilgileri tespit edilmiş ve “Export” menüsünden excell formatı seçilerek çıkarım yapılmış şekil-31’de gösterilmiştir.

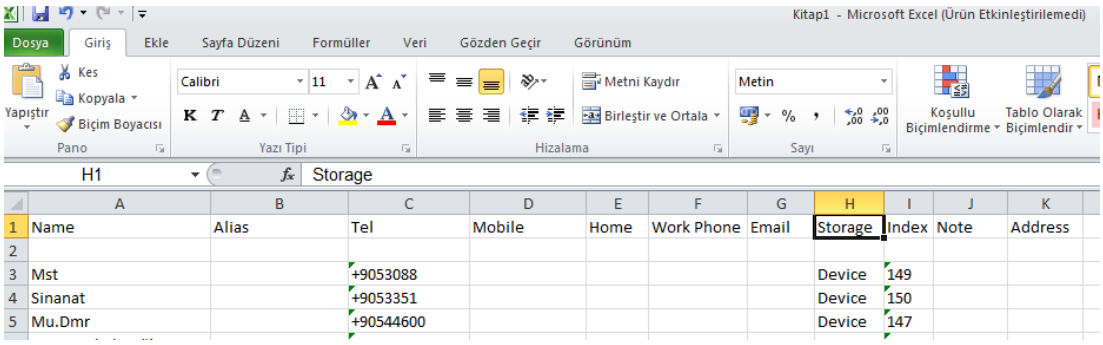
Ayrıca aşağıda şekilde cihaz üzerinde harici belleğinde bulunan “video, resim, müzik, veritabanı ve diğer” dosyalar tespit edilmiş olup Şekil-30’da görüldüğü gibi çıkartılan

verilerin delil zinciri kapsamında doğrulundan emin olunması sağlayan MD5 ve **SHA1** Hash değerlerinin de mevcut olduğu görülmektedir.



Video	File Name	File Size	Storage	Created	Hash (MD5)	Hash (SHA1)
<Video not included in export>	Video000.3gp	1,17 MB	Removable Media	03.11.2012 18:20:00 (Device)	a2d383880bb0368e9a460ff6cc675e2d	71669ddb1d30bc4041b531415938ba7
<Video not included in export>	Video001.3gp	1,07 MB	Removable Media	04.11.2012 11:41:00 (Device)	fa5d5e111b761d19ba22ca4350dc0e43	59ba1e7ce9e3b39dee3ad620dc28e08
<Video not included in export>	Video002.3gp	1,04 MB	Removable Media	04.11.2012 20:15:00 (Device)	95806274e161ea1284d4e5eb0662983c	ff84a5fc5519c76caded46fe6c3c6da19
<Video not included in export>	Video003.3gp	1,96 MB	Removable Media	05.11.2012 00:15:00 (Device)	11c322b1fce11397eaeaf773fc5e5a50	befe56db770c43fa423af9774204dfd2
<Video not included in export>	Video004.3gp	824,16 KB	Removable Media	24.11.2012 12:54:00 (Device)	f7ee0639ae01c6df37b9e5cda1938994	481609793d913ea058ada760cfd6475b
<Video not included in export>	Video005.3gp	2,38 MB	Removable Media	26.11.2012 22:25:00 (Device)	da965753bccc5acd1ef301f04e5864e6	4ca45fab55865c5bdb9864473a64b5a9
<Video not included in export>	Video007.3gp	1,36 MB	Removable Media	03.12.2012 20:24:00 (Device)	55bdb6f5a69a354c60b2fdc1deee5c87	fa762036376f74d2a9aab1dc1cf0aa547
<Video not included in export>	Video006.3gp	1,81 MB	Removable Media	01.12.2012 13:41:00 (Device)	da42a3f7faf732dea5d6ae9d55f497b2	dd4fb02200db2fde0b0e5b3362200e5
<Video not included in export>	Video008.3gp	1,68 MB	Removable Media	04.12.2012 19:26:00 (Device)	29b8f9da80e3faf31553651e8e369315	e48a5fb84749f7b6c2101afa1cd1f304a
<Video not included in export>	Video009.3gp	889,57 KB	Removable Media	08.12.2012 15:47:00 (Device)	fe5f683061b96ed8c53ff7d290a55a68	7a82ddd895c028ec9c4c2ddcd519053
<Video not included in export>	Video010.3gp	1,88 MB	Removable Media	15.12.2012 12:51:00 (Device)	fa83c074842323e4ac2b6f6010db8f73	32e7d114b5a03f8835bab1ddb0e17e1
<Video not included in export>	Video011.3gp	578,82 KB	Removable Media	15.12.2012 20:23:00 (Device)	9cedb9e5ab4454c18127bb5a39c8deb7	8af4fd5074a408af17c9c5dad0d275d5
<Video not included in export>	Video012.3gp	2,05 MB	Removable Media	22.12.2012 14:06:00 (Device)	61f08857193c5832b8d4e5c6c44ccfd2	2fc79d58fa766ae8faafe0f95a9417b35
<Video not included in export>	Video013.3gp	297,17 KB	Removable Media	20.01.2013 10:32:00 (Device)	2b1e4dfca52f9339880c30fbd1fecca3	4a309e29276d30aae361bf2534fbe6d1
<Video not included in export>	Video014.3gp	353,44 KB	Removable Media	25.01.2013 19:29:00 (Device)	ce00583783731f7313a13a7f7375155b	75ff7cbd42fe1eb93fc63fa0affa506c03
<Video not included in export>	Video015.3gp	1,48 MB	Removable Media	27.02.2013 20:05:00 (Device)	fc97e8ed4180ed66b45309ccfad27550	04188662848dfee3ea4e9a7ba6258bd

Şekil 30- XRY ile tespit edilen Nokia 6300 Harici bellek verileri



Name	Alias	Tel	Mobile	Home	Work Phone	Email	Storage	Index	Note	Address
Mst		+9053088					Device	149		
Sinanat		+9053351					Device	150		
Mu.Dmr		+90544600					Device	147		

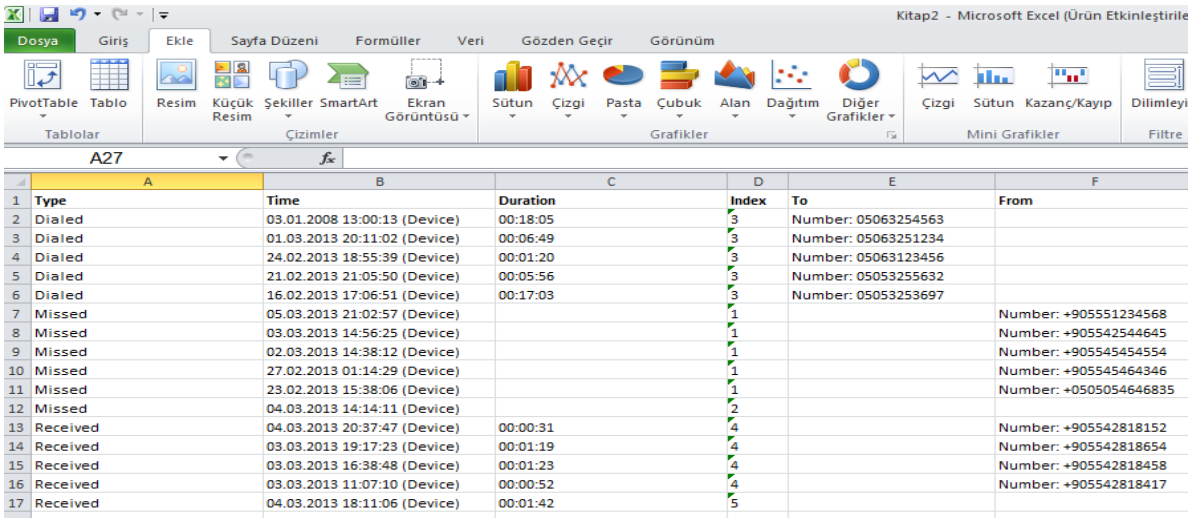
Şekil 31-XRY ile tespit edilen Nokia 6300 Dâhili hafıza verileri

(b) Arama Kayıtları

XRY "Calls" menüsü altında arama kayıtlarına erişim sağlanabilmektedir. "Calls" kaydı butonunu tıklandığında cihaz üzerinde gerçekleştirilen aramalar listelenmektedir. Aralık 2014 yılına ait bir gelen arama kaydı aşağıda şekil-32 ve şekil-33'te gösterilmiştir.

Received	+905322237179	Yucelaslan	28.12.2014 14:55:33 UTC (Device)	00:03:06	Device	Yucelaslan +905322237179

Şekil 32- XRY ile tespit edile n Nokia 6300 Arama kaydı

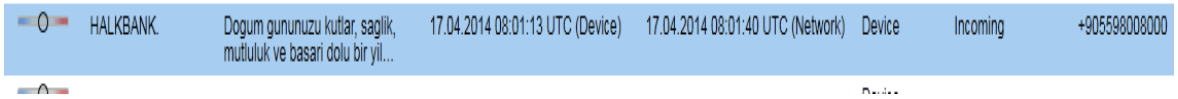


	Type	Time	Duration	Index	To	From
2	Dialed	03.01.2008 13:00:13 (Device)	00:18:05	3	Number: 05063254563	
3	Dialed	01.03.2013 20:11:02 (Device)	00:06:49	3	Number: 05063251234	
4	Dialed	24.02.2013 18:55:39 (Device)	00:01:20	3	Number: 05063123456	
5	Dialed	21.02.2013 21:05:50 (Device)	00:05:56	3	Number: 05053255632	
6	Dialed	16.02.2013 17:06:51 (Device)	00:17:03	3	Number: 05053253697	
7	Missed	05.03.2013 21:02:57 (Device)		1		Number: +905551234568
8	Missed	03.03.2013 14:56:25 (Device)		1		Number: +905542544645
9	Missed	02.03.2013 14:38:12 (Device)		1		Number: +905545454554
10	Missed	27.02.2013 01:14:29 (Device)		1		Number: +905545464346
11	Missed	23.02.2013 15:38:06 (Device)		1		Number: +0505054646835
12	Missed	04.03.2013 14:14:11 (Device)		2		
13	Received	04.03.2013 20:37:47 (Device)	00:00:31	4		Number: +905542818152
14	Received	03.03.2013 19:17:23 (Device)	00:01:19	4		Number: +905542818654
15	Received	03.03.2013 16:38:48 (Device)	00:01:23	4		Number: +905542818458
16	Received	03.03.2013 11:07:10 (Device)	00:00:52	4		Number: +905542818417
17	Received	04.03.2013 18:11:06 (Device)	00:01:42	5		

Şekil 33-XRY ile tespit edilen Nokia 6300 Sim hafıza Arama Kaydı

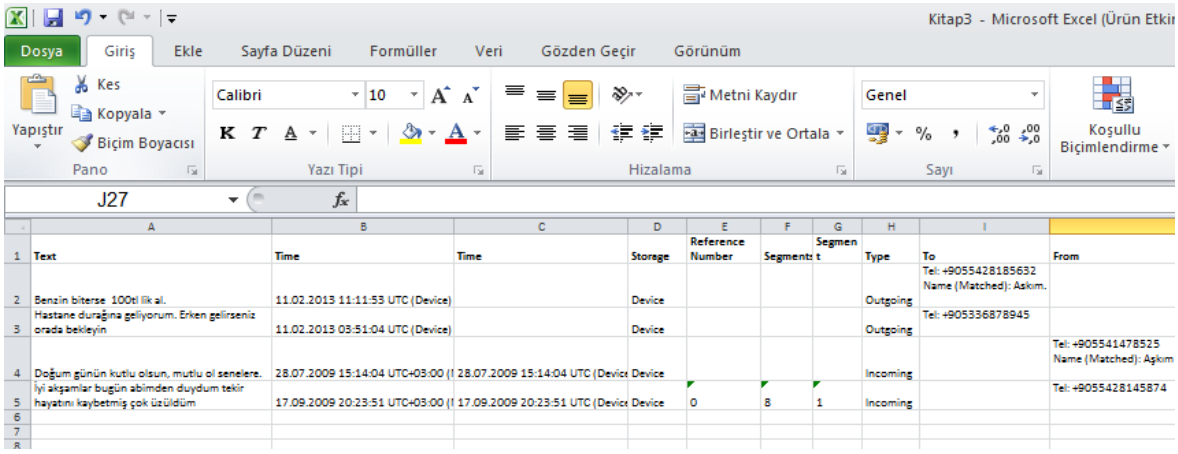
Burada bulunan arama kayıtları cihazda kullanılan SIM kartın kayıtlı olduğu GSM şirketi aracılığı ile de elde edilebilir.

(c) SMS/MMS Mesaj Kayıtları



HALKBANK.	Dogum gununuzu kutlar, saglik, mutluluk ve basari dolu bir yil...	17.04.2014 08:01:13 UTC (Device)	17.04.2014 08:01:40 UTC (Network)	Device	Incoming	+905598008000

Şekil 34-XRY ile tespit edilen Nokia 6300 Mesaj Kaydı



	Text	Time	Time	Storage	Reference Number	Segments	Segment	Type	To	From
2	Benzin biterse 100tl lik al.	11.02.2013 11:11:53 UTC (Device)		Device				Outgoing	Tel: +9055428185632 Name (Matched): Askım.	
3	Hastane durağına geliyorum. Erken gelirseniz orada bekleyin	11.02.2013 03:51:04 UTC (Device)		Device				Outgoing	Tel: +905336878945	
4	Doğum günün kutlu olsun, mutlu ol senelere.	28.07.2009 15:14:04 UTC+03:00 (	28.07.2009 15:14:04 UTC (Device	Device				Incoming		Tel: +905541478525 Name (Matched): Aşkım
5	İyi akşamlar bugün abimden duydum tekir hayatını kaybetmiş çok üzüldüm	17.09.2009 20:23:51 UTC+03:00 (	17.09.2009 20:23:51 UTC (Device	Device	0	8	1	Incoming		Tel: +9055428145874

Şekil 35-XRY ile tespit edilen Nokia 6300 SMS kaydı.

(3) Uygulama Analizi

Nokia 6300 akıllı bir telefon olmaması nedeni analiz esnasında cihaz üzerinde herhangi uygulama verisine erişim sağlanmamıştır. XRY reader ile “Device Overview” kısmına girildiğinde özellikler “Features” altında cihazın hangi analizleri desteklediği

görülmektedir. Burada E-mail ve Call Sim desteklenmediği ve Sim kartsız analiz işleminin gerçekleştirildiği aşağıdaki şekilde görülmektedir.

Features

Contacts Sim	✓ Full Support
Calls Sim	✓ Full Support
SMS Sim	✗ Not Supported
Contacts	✓ Full Support
Calls	✓ Full Support
Calendar	✓ Full Support
SMS	✓ Full Support
MMS	✓ Full Support
E-mail	✗ Not Supported
Files	✓ Full Support
Memory card	✓ Full Support

Şekil 36-XRY tarafından Nokia 6300 desteklenen Analiz Özellikleri

c) Nokia 5800-Fiziksel İmaj Analizi

Nokia 5800 Xpress Music (RM-356) marka/model cihazımız Symbian S60 işletim sistemi,256 Mb dâhili hafıza ve 8 Gb Sd kart mevcuttur. XRY ile fiziksel bit byte bit imajı alınmıştır. İmaj alma işlemi yaklaşık 25 dk sürmüştür. Cihaza takılı SIM kart mevcut değildir.

Fiziksel imaj bitiminde yapılan analiz sonucunda 31 adet SMS,bunların 9 adeti silinmiş, 803 adet resim dosyası bunun da 706 adeti silinmiş,5 adet ses dosyası 2 adeti silinmiş ,71 adet dosya 22 adeti silinmiş , 28 adet veritabanı 15 adeti silinmiş ve 4990 adet tanımlanamayan veri bunlarında 2326 adeti silinmiş olarak yazılım tarafından tespit edilmiştir.

Üzerinde tespit edilen aşağıda sunulmuştur:

- Mesaj “Message” kaydı (31/9 ad. Deleted)
- SIM kaydı bulunamadı.
- Dosya Files kaydı

  Resim “Pictures” 803/ 706 deleted items

  Ses “Audio” 5/2 ad deleted items

  Doküman “Documents” 71 / 22 deleted items

  Veritabanı “Database” 28 / 15 deleted items

  Tanımlanamayan “Unrecognized” 4990/ 2326 deleted items

(1) SIM Analizi

Cihaz üzerinde herhangi bir SIM kart olmadığı için SIM analizi gerçekleştirilememiştir. XRY her bir farklı marka model cihaz için desteklediği özellikler farklı olmakla birlikte Nokia 5800 için desteklemediği özellikler aşağıda şekil-37’de gösterilmiştir.

Physical Decode

Features

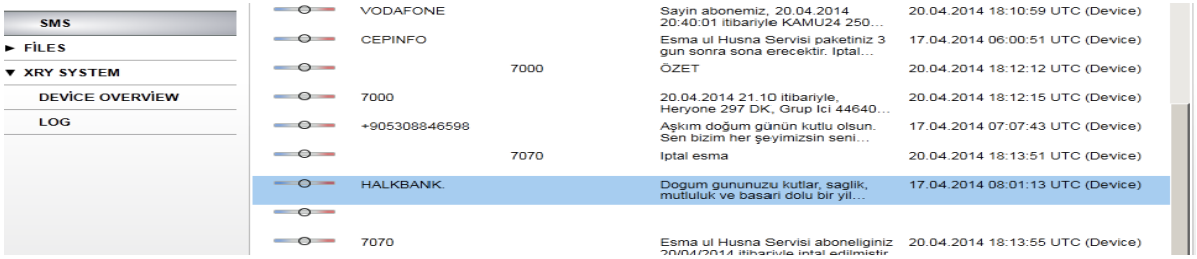
Contacts	✗ Not Supported
Calls	✗ Not Supported
Calendar	✗ Not Supported
SMS	✓ Partial Support
MMS	✓ Partial Support
E-mail	✓ Partial Support
Files	✓ Supported

Şekil 37- XRY tarafından desteklenen Nokia 5800 Analiz özellikleri

(2) Dâhili/Harici Hafıza Analizi

(a) SMS Kayıtları

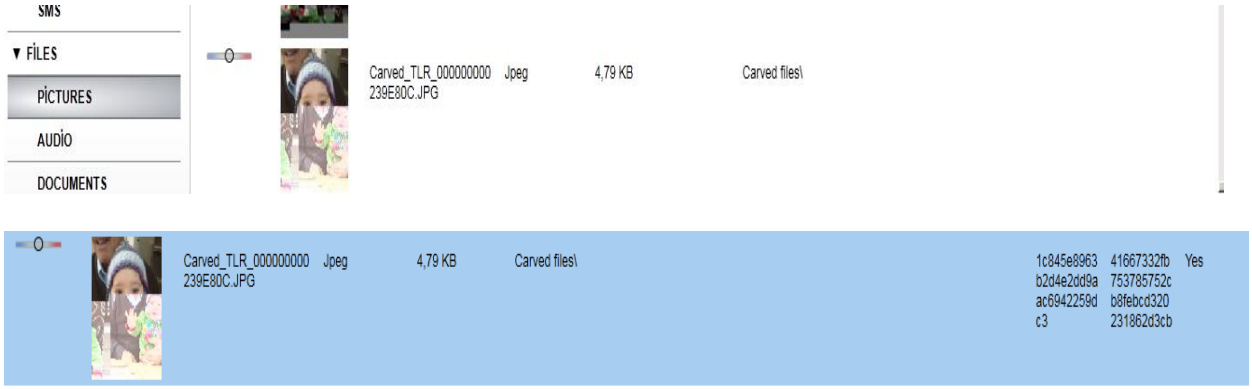
XRY üzerinde "SMS" butonu çalıştırdığımızda cihaz üzerinde tespit edilen SMS/MMS kayıtlarına erişilmektedir. Tespit edilen SMS kayıtları içerisinden 2014 yılına ait bir banka tarafından müşterisine gönderilmiş SMS kaydı aşağıda şekil-38'de gösterilmiştir. Mesaj içerikleri tıkladığında detaylı zaman bilgisine erişilmektedir.



Şekil 38-XRY ile tespit edilen Nokia 5800 SMS kaydı

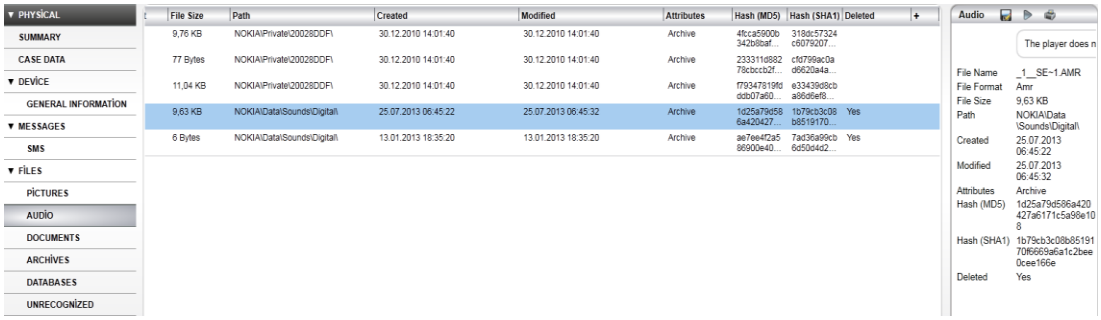
(b) Dosya Kayıtları

XRY analiz ettiği cihaz üzerindeki bulduğu dosyaları kategorilerine göre ayırabilmektedir. "Files" bölümü açıldığında bu kategoriler görülebilmektedir. Aşağıdaki resimde "Pictures" bölümünde 2011 yılına ait silinmiş bir resim dosyası tespit edilerek gösterilmiştir.



Şekil 39- XRY ile tespit edilen Nokia 5800 Tespit Edilen Resim Kaydı

“Audio” bölümüne girdiğimizde cihaz üzerindeki ses kaydı bilgilerine erişilmektedir. Aşağıdaki şekil-40’da 2013 yılına ait silinmiş ses kaydı tespit edilip gösterilmiştir.



Şekil 40-XRY ile tespit edilen Nokia 5800 Ses kaydı.

d) Yazılımın Değerlendirmesi

(1) Avantajları

- Grafik ara yüz ile herhangi bir komut işlemi yapılmadan “arama kayıtları, resim, video, müzik, web ve uygulama “ verileri bulunmuştur.
- Hem fiziksel hem de mantıksal imajı desteklemesi büyük bir kolaylık olup ne tür bir bağlantı şekli yaptığınız “DEVİCE OVERVİEW” sekmesinde görülebilmektedir. Cihazın hangi network ve işletim sistemine ait olduğu Device Overview sekmesinde görebilmektedir.
- Yaklaşık Samsung GT-N7100 cihazının mantıksal imajı alma işlemi 1,5 saat gibi bir zamana diliminde gerçekleştirilmiştir.
- Bulunan her bir dosyanın hash ve sha1 değerlilerini tek tek göstermesi ayrı bir avantaj olup küçük bir veri çıkartıldığı zaman doğrulama verisi ile birlikte elde edilmektedir.
- Aynı anda birden fazla imaj analiz edilebiliyor.

(2) Dezavantajları

- Cihazın alınan imajının export edilirken hash değerini verememesi.
- Direk olarak sosyal medya ve diğer web uygulamalarını analiz edememektedir.
- Yazılım üzerinde direk bir direk inceleme yapmamızı sağlayacak bir SQL Lite browser bulunmamaktadır.
- Yüklü olan uygulama isimleri görülebilmekte fakat yükleme ve uygulamayı kaldırma tarihi bir bilgiye rastlanmamıştır.
- Cihaz üzerinde sim kart ve faal olmasına rağmen SIM CALL not support gibi bir mesaj görünmekte olup Ayrıca bir modül olarak SIM modül kısmının olmaması ciddi bir

olumsuz özellik olup bulunan rehber bilgilerinin SIM demi yoksa cihaz dahili hafızasında mı olduğu görülememekte olup telefon üzerinden bakılarak görülmektedir.

- Ayrıca telefona hafızasında olup silinmeyen bazı rehber bilgileri de "Contact" sekmesinde görülememiştir.
- Device Overview kısmında Görevler "task ve notlar "notes" verileri desteklemediği görülmektedir
- Ayrıca e-mail ve uygulama ait mesaj, lokasyon bilgileri ve web geçmişinin Android cihazlar ile görülebilmesi için Cihaz üzerinde rooting işleminin kesinlikle yapılması gerekmektedir.
- Cihazın IMEI numarası bilgisine rastlanamamıştır.
- Genel olarak bir raporlama aracı olmayıp sadece bulunan veriler belli tip dosya biçiminde export edilmektedir.
- Veritabanı bilgileri içerisinde gezerek veriler kolay bir şekilde elde edilebilmekte

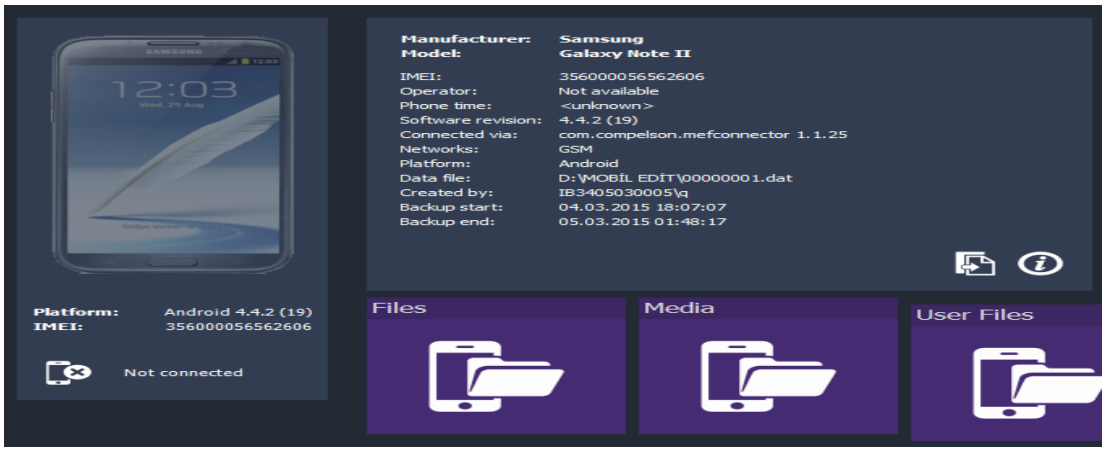
2. MobilEdit Analizleri

a) Samsung GT-N7100-Mantıksal İmaj Analizi

Kablo ile cihaza bağlanma "Connecting the device via a data cable" olup Cihazlara ait sürücüler http://www.mobiledit.com/downloads.htm?show=14 adresinden tedarik edilmiştir.[153]

Samsung GT-N7100 Note II Android "4.4.1" cihazın mantıksal imajı alınarak analiz edilmiştir. Samsung GT-N7100 Android işletim sistemi sahip akıllı cihaz olup donanım özelliklerinin iyi olması nedeni ile analiz işlemi zaman bakımından kayda değer bir zaman almış "36 saatte" analiz işlemi bitmiştir. Aşağıda şekilde cihaza ait tanımlama bilgisi ile analizin başlangıç ve bitiş zamanı gösterilmiştir.

153 http://www.mobiledit.com/downloads.htm?show=14 Et:05.04.2015



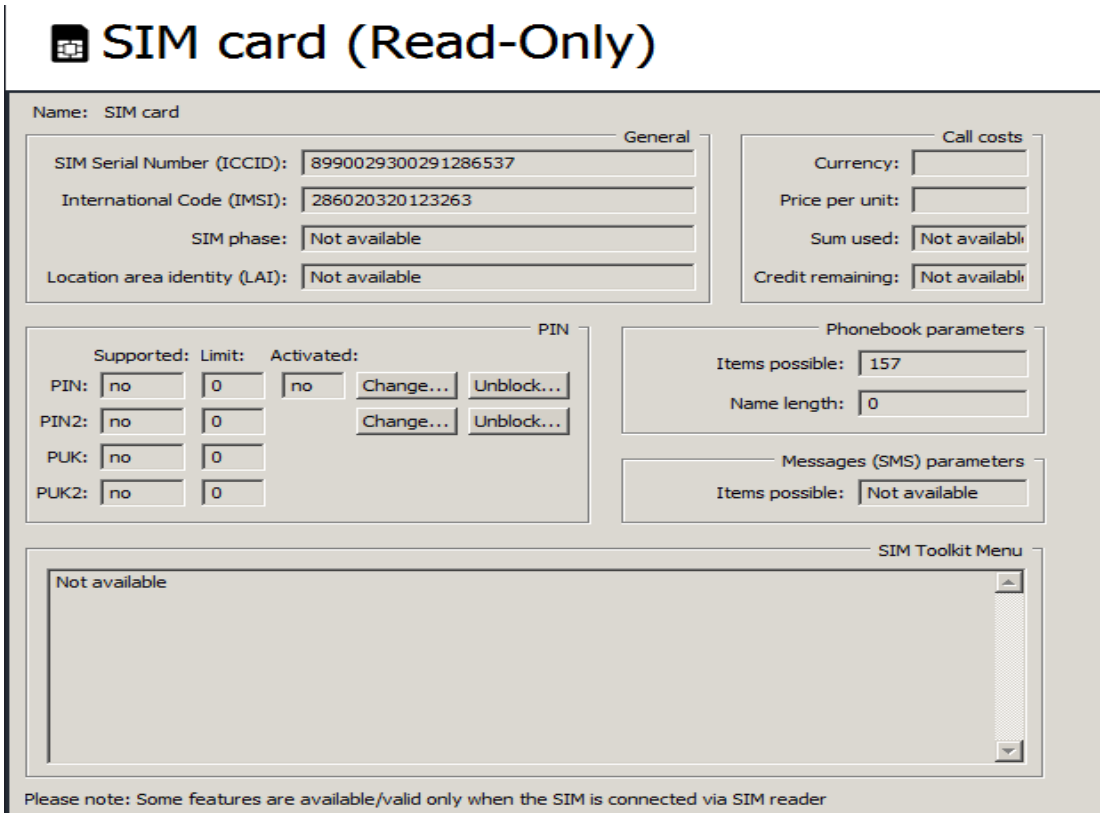
Şekil 41-Mobiledit ile tespit Samsung GT-N7100 cihaz bilgisi.

Samsung Gt-N7100 mantıksal imaj üzerinde tespit edilen kayıt bilgileri aşağıda sunulmuştur.

- Telefon rehberi “Phonebook” :(583) adet
  Telefon Hafıza “Phone memory” (226)
  Google Hesabı (200)
  Sim Hafızası “SIM memory” (157)
- Arama “Calls Logs” Kaydı (477)
  Cevapsız “Missed calls” (92)
  Giden “Outgoing” Arama kaydı (310)
  Gelen “Incoming” Arama kaydı (75)
- SMS/MMS Mesaj “Message” Log (635)
  Gelen “Received” Mesaj kaydı (428)
  Giden “Send” Mesaj Kaydı (207)

(1) SIM Analizi

MobilEdit Cihaz ile birlikte Sim analizi yapabilme özelliğine sahip olup ayrıca bir araç ve yazılıma ihtiyaç duyulmamaktadır. Samsun GT-N7100 üzerine takılı Sim kart bilgileri Şekil-42’de gösterilmiştir.

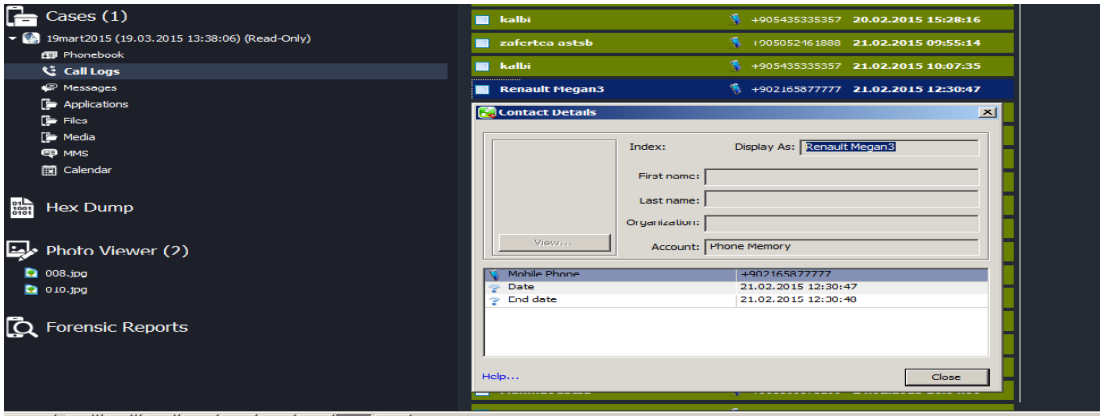


Şekil 42-Mobiledit Samsung GT-N7100 Sim Kart bilgisi

(2) Dâhili/Harici Hafıza Analizi

(a) Arama Kayıtları

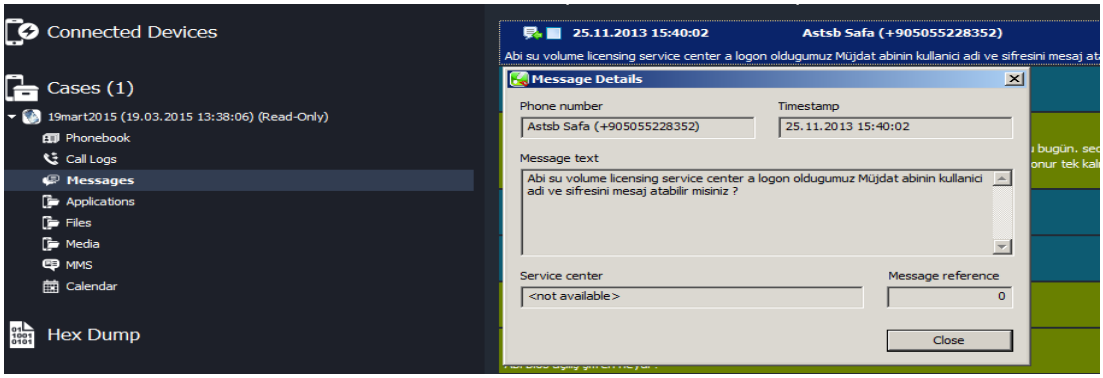
Analiz sonucunda “Call Logs” kısmında girildiğinde cihaz üzerinde tespit edilen arama kayıtlarına ulaşılmaktadır. Analizde sonucunda silinen arama kayıtları tespit edilmiş aşağıda şekil-43’te gösterilmiştir.



Şekil 43-MobileDit ile tespit edilen Samsung GT_N7100 Arama Kaydı

(b) SMS Kayıtları

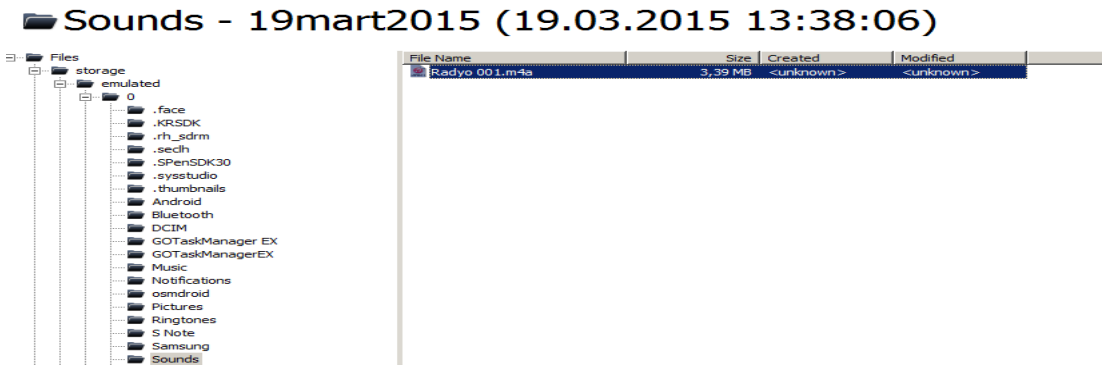
Mobiledit “Messages” bölümüne girildiğinde cihaz üzerindeki bütün gelen/giden mesaj kayıtlarına erişilmektedir. Aşağıdaki şekil-44’de 2013 yılına ait SMS mesaj kaydı gösterilmiştir.



Şekil 44-Mobiledit ile tespit edilen Samsung GT-N7100 SMS kaydı

(c) Dosya Kayıtları

Mobiledit ile “Files” menüsü girildiğinde dosyalar kategoriler halinde bulunmaktadır. “Sounds” kısmına girdiğimizde cihaz üzerinde bulunan ses kaydı bilgisi tespit edilmiş Şekil-45’te gösterilmiştir.



Şekil 45-Mobiledit ile tesit edilen Samsung GT-N7100 Ses Kaydı

b) Samsung GT-N7100-Fiziksel İmaj Analizi

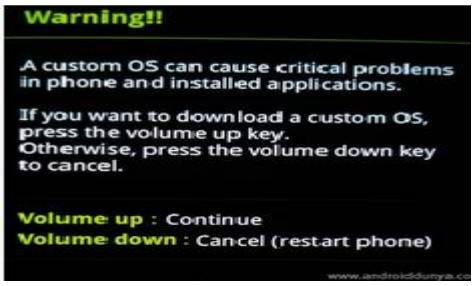
Bu işlem öncesinde telefonda “rooting” işlemi yapılmış olup bu işlemin nasıl yapıldığı aşağıda anlatılmıştır.

Samsung telefonunuzu USB kablosu ile bilgisayara bağladıktan sonran cihazın bilgisayar tarafından görülmesi gerekmektedir. Samsung cep telefonu sürücüleri yüklü olduğu için otomatik cihaz tanınmıştır.

Birinci adımda gerekli olan **ODIN 3.07** ve **CF-Auto-Root** yazılım ve dosyalarını bilgisayarımıza indiriyoruz.

İkinci adım olarak; Cihaz üzerinde daha önce anlattığımız "Usb Debugging" usb hata ayıklama modunun açılması gerekmekte olup bizim cihazımız da açılmıştır. Kapalı olan cihazlar için " Ayarlar -> Geliştirici seçenekleri bölümünden Usb hata ayıklama "Usb Debugging" açık hale getirilerek açılabilir.

Üçünçü Adım, Telefonunuzu kapatınız. Kapalı iken **Alt ses düğmesi + Home tuşu + Güç düğmesine** aynı anda 5 saniye kadar aşağıdaki resimde görünen Samsung yazılım yükleme ekran uyarısı gelinceye kadar basıyoruz.[154]

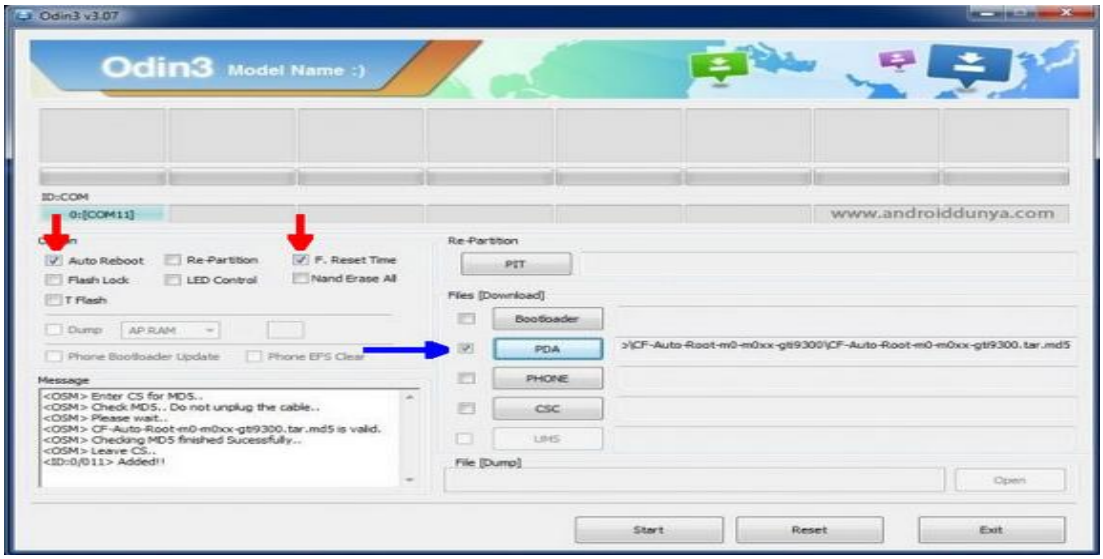


Şekil 46-Samsung GT-N7100 Root Yazılımı Yükleme Ekranı

Bu logo ekrana çıkınca **Üst Ses düğmesine** basılır ve Android logolu yazılım yükleme ekranı gelir bu esnada alt ses düğmesine basılarak telefon yeniden başlatılır. Android simgesi görülünce telefon takılır.

Dördüncü adım da **ODIN3 v3.07** uygulamasını çalıştırılır ve aşağıdaki gibi bir ekran gelmektedir.

154http://www.androiddunya.com/samsung-galaxy-note-ii-n7100-nasil-root-yapilir/ Et:02.04.2015



Şekil 47-ODIN Uygulama Ekranı

Yukarıdaki ekranda PDA butona basıp aynı klasör içindeki CF-Auto-Root-t03g-t03gxx-gtn7100.tar.md5 dosyasını seçilir ve seçeneklerden Re-Partition işaretli olmadığına emin olun. Ayarlar yukarıdaki gibi olmalıdır. Son olarak start butonuna basılarak telefon root yapılmış olur.[155]

Root işleminden sonra MobilEdite açılır ve cep telefonu yazılım tarafından sağlıklı bir şekil tanınması gerekmektedir. Cihaz yazılım tarafından erişebilir olduktan sonra yeni "case" açılıp analiz işlemi başlatılır. Cihazın yazılım tarafından Genel bağlantı görüntüsü Şekil-48'de gösterilmiştir.

Şekil 48-Mobiledit ile tespit edilen Samsung GT-N7100 Cihaz bilgisi

155http://www.androiddunya.com/samsung-galaxy-note-ii-n7100-nasil-root-yapilir/ Et:02.05.2015

Analiz işlemi yaklaşık 30 saat gibi bir zaman almış, analiz sonucunda aşağıdaki dosyalar çıkarılmıştır. Cihazın toplam boyutu 10 Gb olmasına rağmen 26 gb bir veri çıkartılmış ve aşağıda gösterilmiştir.

- Samsung_Galaxy_Note_II_356000056562606_cache.dump
- Samsung_Galaxy_Note_II_356000056562606_data.dump
- Samsung_Galaxy_Note_II_356000056562606_efs.dump
- Samsung_Galaxy_Note_II_356000056562606_preload.dump
- Samsung_Galaxy_Note_II_356000056562606_system

Yukarıda belirtilen dosyaların analizi sonucunda bulunan veriler başlıklar halinde aşağıda sunulmuştur.

Samsung GT-N7100 fiziksel imaj üzerinde bulunan kayıt bilgileri aşağıda olduğu gibidir:

- Telefon rehberi “Phonebook” :(587) adet

Telefon hafıza “Phone memory” 230

SIM “ memory” hafıza 157

- Arama “Calls Logs” kaydı 476

Cevapsız “Missed calls” Arama Kaydı 105

Giden “Outgoing” Arama Kaydı 302

Gelen “Incomıng” Arama Kaydı 69

- Uygulama “Applications” 573
- Takvim “Calendar” 49
- SMS/MMS Mesaj “Message” Log kaydı 587

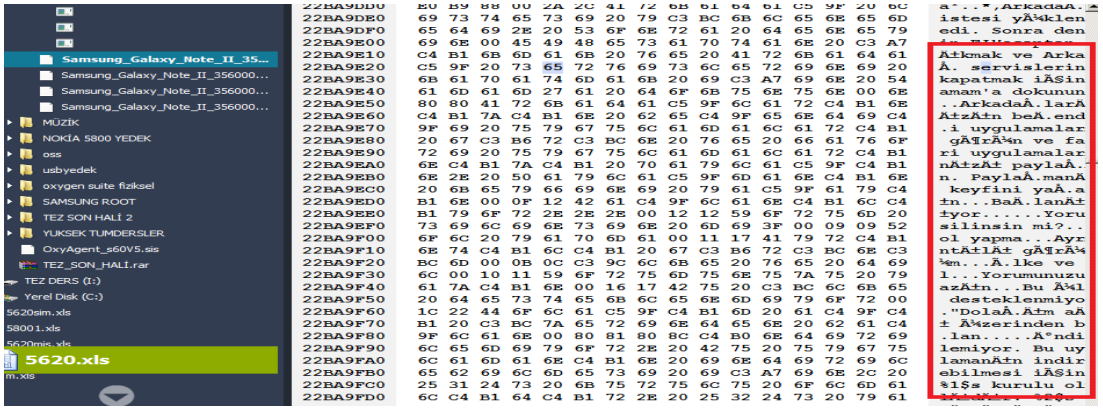
Gelen “Received” Mesaj 401

Giden “Send” Mesaj 185

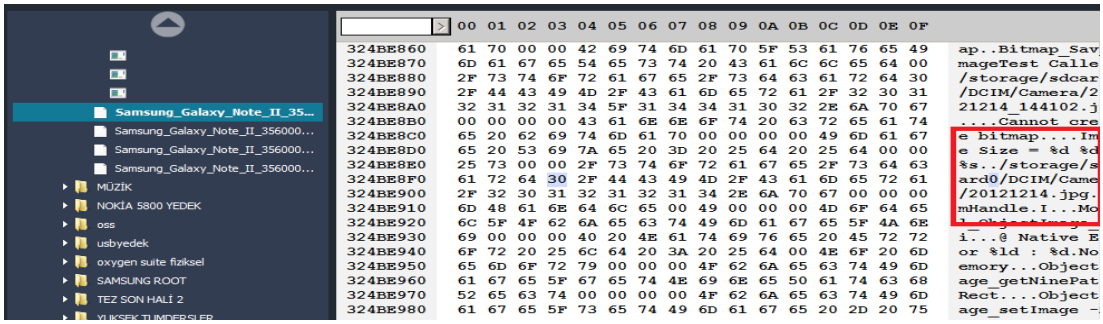
Şablon “Drafts” 1

Samsung GT-N7100 fiziksel analiz dosyaları *.Dump uzantılı dosyalar olarak çıkarımı yapılmış olup mantıksal analizde olduğu gibi detaylı bir şekilde kategorize edilememek aşağıda belirtilen beş farklı uzantılı dosya şeklinde çıkarım yapılıp analiz edilebilmektedir.

Samsung_Galaxy_Note_II_356000056562606_cache.dump analizi sonucu ulaşılan web erişim kayıt bilgisi aşağıda sunulmuştur.



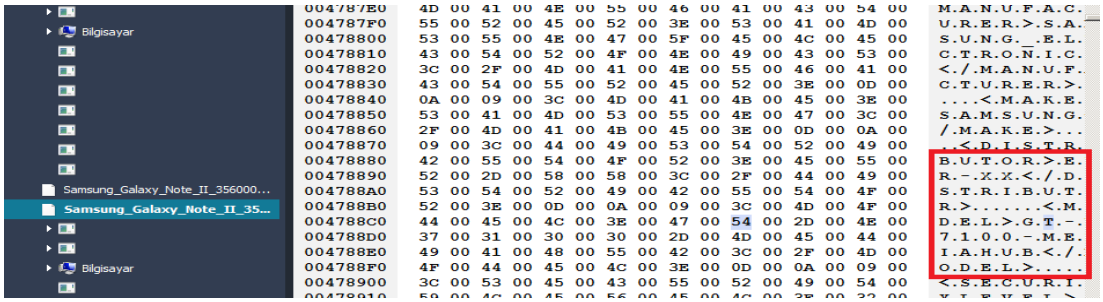
Şekil 49-Mobiledit ile tespit edilen Samsung GT-N7100 Web kaydı



Şekil 50-Mobiledit ile tespit edilen Samsung GT-N7100 resim dosyası bilgisi.

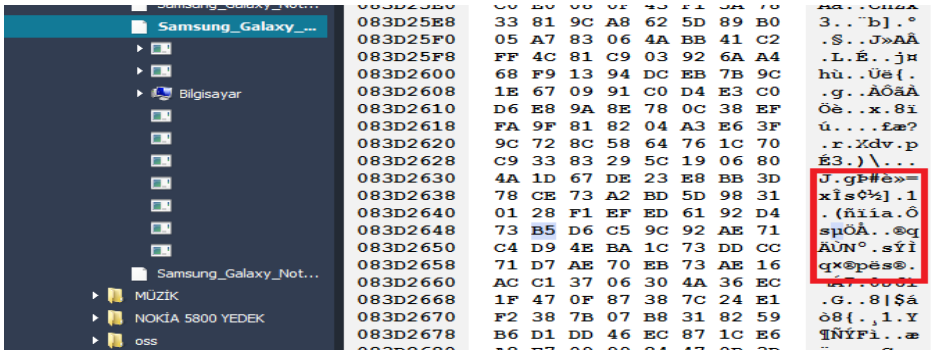
Samsung_Galaxy_Note_II_356000056562606_data.dump dosyasının analizinde her hangi bir anlamlı kayıt bilgisi tespit edilmemiştir.

Samsung_Galaxy_Note_II_356000056562606_efs.dump analizi ile analizi yapılan cihaza ait bilgiler tespit edilmiştir.



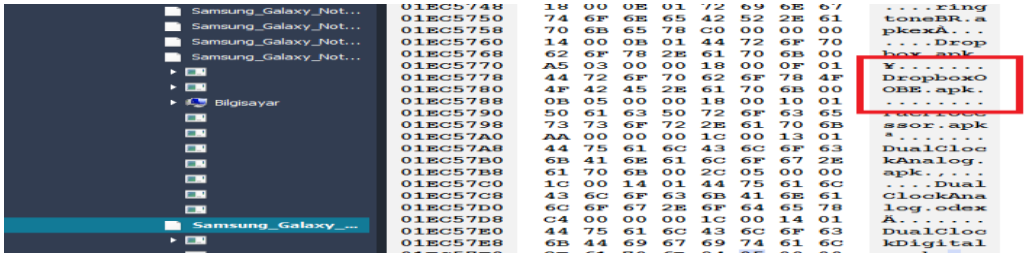
Şekil 51-Mobiledit ile tespit edilen Samsung GT-N7100 Cihaz Bilgileri

Samsung_Galaxy_Note_II_356000056562606_preload.dump analizi ile kullanıcıya ait mail bilgisi tespit edilmiştir.

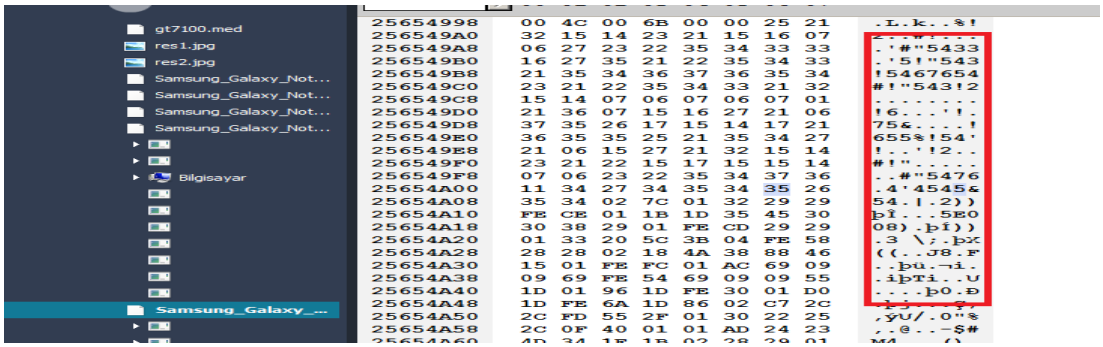


Şekil 52-Mobiledit ile tespit edilen Samsung GT-N7100 mail Adresi kaydı

Samsung_Galaxy_Note_II_356000056562606_system.dump analizinde cihaza yüklenmiş Dropbox uygulama bilgisi tespit edilmiştir.



Şekil 53-Mobiledit ile tespit edilen Samsung GT-N7100 Uygulama Kaydı



Şekil 54-Mobiledit ile tespit edilen Samsung GT-N7100 Arama Kaydı**.**

c) Samsung GT-S5620-Mantıksal İmaj Analizi

Bu analizde Samsung GT-S5620 cihazımız ve takılı olan SIM kart a imajı alınarak analiz edilmiştir. Aşağıda analiz sonucunda Samsung Gt-S5620'nin Mobiledit ile bulunan kayıt bilgileri sunulmuştur. Bu dosyalar Mobiledit HEX DUMP menüsü ile analiz edilmiştir.

Üzerinde buluna veri bilgiler aşağıda olduğu gibidir:

- Telefon rehberi "Phonebook" :(205) adet

SIM memory (40)

- Arama "Calls Logs" Kaydı (63)

Cevapsız "Missed Calls logs" Kaydı (22)

Giden "Last Dialed Logs" kaydı (20)

Gelen "Received Logs" kaydı (21)

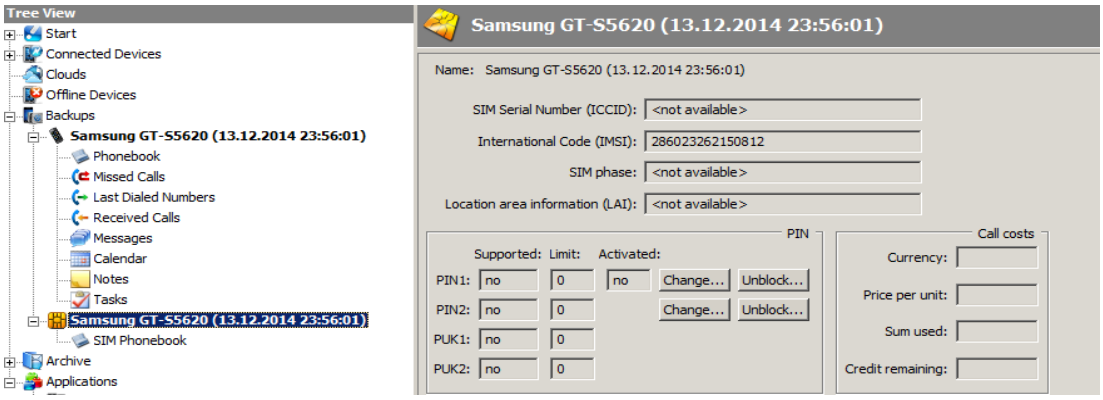
- SMS/MMS Mesaj "Message" Log (236)

Gelen "Received Messages" Mesaj (224)

Giden "Send Message" Mesaj (6)

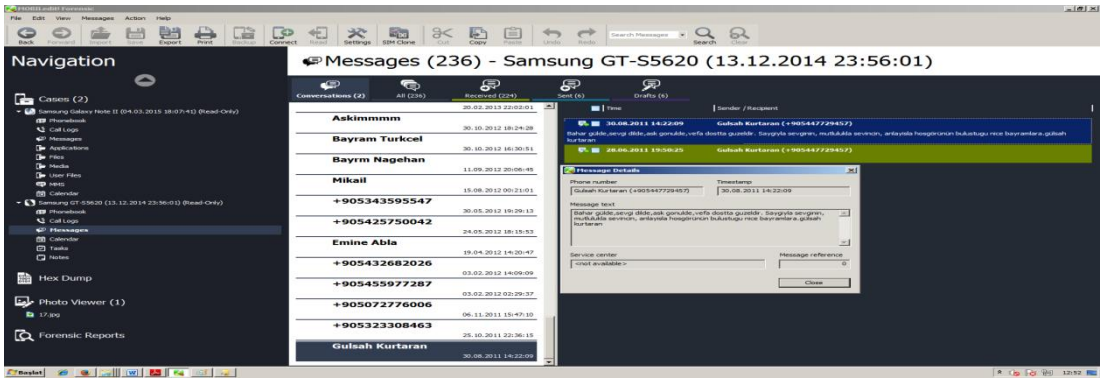
Şablon "Draft Messages" Mesaj (6)

(1) SIM Analizi



Şekil 55-Mobiledit ile tespit edilen Samsung SIM GT-S5620 SIM kart bilgisi.

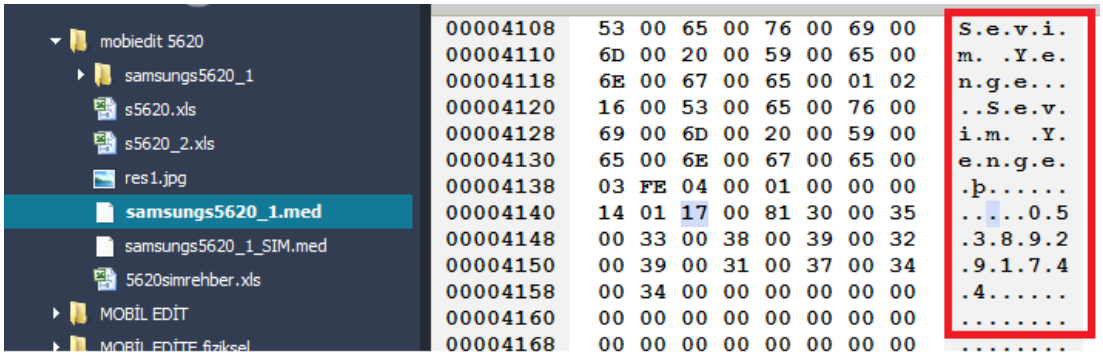
Analiz ile tespit edilen Mesajlar "Messages" bölümüne girilerek görülebilmektedir. Aşağıda şekil-56'da 2011 yılına ait tespit edilen SMS mesajı gösterilmiştir.



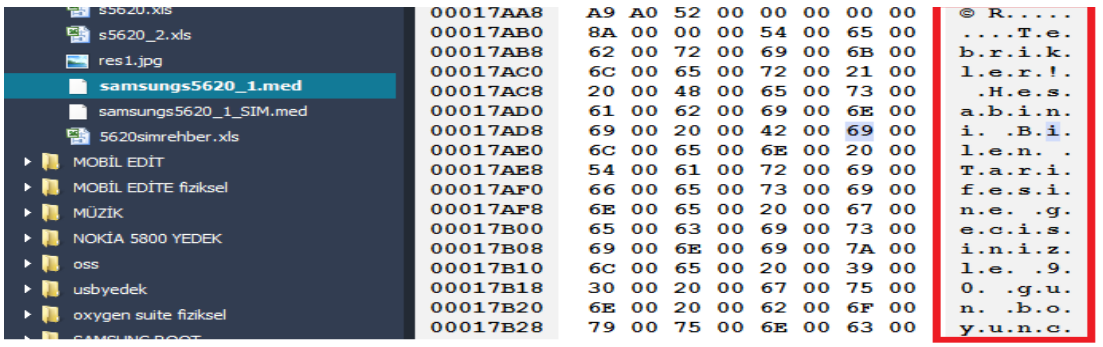
Şekil 56-Mobiledit ile tespit Samsung S5620 SMS kaydı

(2) Dâhili/Harici Hafıza Analizi

HexDump Editör ile cihaza ait "Samsung GT-S5620" .MED" uzantılı imaj dosyası açılıp analiz edilmiştir. Analiz sonucunda tespit edilen Rehber ve Mesaj verileri aşağıda sunulmuştur.



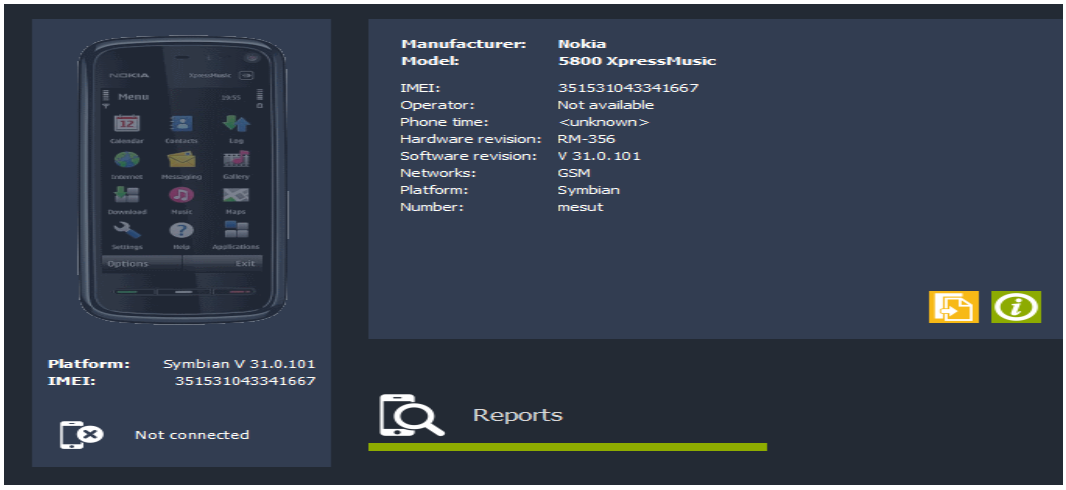
Şekil 57-Mobiledit ile tespit edilen Samsung GT-S5620 Rehber Kaydı



Şekil 58-Mobiledit ile tespit edilen Samsung GT-S5620 mesaj kaydı

d) Nokia 5800-Mantıksal İmaj Analizi

Bu analiz kısmında Nokia-5800 Music Expres telefonu mantıksal imajı alınıp analiz işlemi gerçekleştirilmiştir. Cihazın yazılım tarafından erişimi sağlanmıştır. Şekil-56'da cihazın yazılım erişimi gösterilmiştir.



Şekil 59-Mobiledit ile tespit edilen Nokia 5800 Cihaz Bilgisi.

Üzerinde buluna veri bilgiler aşağıda olduğu gibidir:

- Telefon rehberi "Phonebook" :(63) adet
- Arama "Calls Logs" Kaydı (19)
- Dosya "Files" Kaydı (63)
- Takvim "Calendar" (1)
- SMS/MMS Mesaj "Message" Log kaydı (23)

  Alınan "Received" Mesaj (20)

  Gönderilen "Send" Mesaj (2)

  Tanımlanamayan "Drafts" Kayıt (1)

(1) SIM Analizi

Mobiledit ile analizi geçekleştirilen Nokia 5800 cihaz üzerinde Sim kart takılı olmaması nedeniyle Sim kart analizi gerçekleştirilmemiştir.

(2) Dâhili/Harici Hafıza Analizi

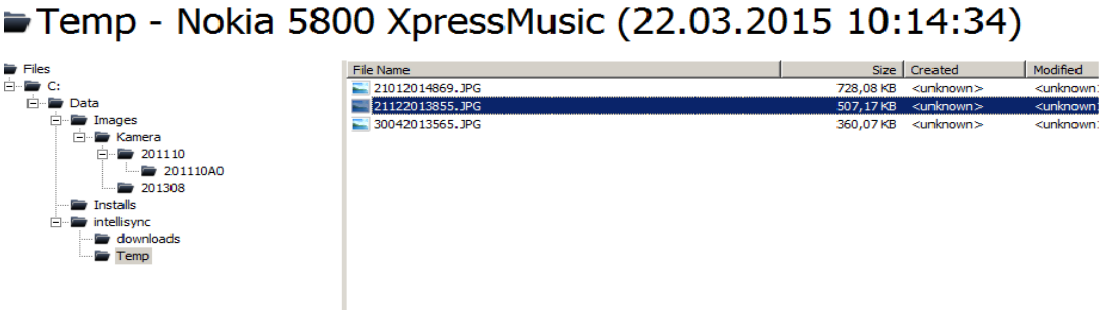
(a) SMS Kayıtları

MobilEdit ile Nokia 5800 cihaz üzerinde tespit edilen mesajlar kısmında 2013 yılına ait mesaj bilgisi Şekil-60'da gösterilmiştir.

Şekil 60-Mobiledit ile tespit edilen Nokia 5800 Mesaj Kaydı

(b) Dosya Kayıtları

Mobiledit üzerinde dosya "Files" kısmına girildiğinde 2013 yılına ait silinmiş bir resim dosyası tespit edilmiş, şekil-61'de gösterilmiştir.



Şekil 61-Mobiledit ile tespit edilen Nokia 5800 Resim Kaydı

e) Iphone 4S-Mantıksal İmaj Analizi

Iphone 4S ile imaj işlemine başlamadan önce her hangi bir rooting ve jailbreaking işlemi yapılmamıştır. Cihazı bilgisayara bağladıktan sonra Internal Storage olarak bilgisayarım simgesi içinde gözükmektedir. Cihazın sadece içindeki resimlerin olduğu "DCIM" klasörü gözükmekte olup bunun dışında başka bir sistem veya kişisel veri tespit edilmemiştir. Analiz ile tespit edilen kayıtlar aşağıda sunulmuştur.

Iphone 4s üzerinde bulunan veriler:

- Telefon rehberi "Phonebook" :(351) adet,
- Mesaj "Message" bilgisi (130)

  Gelen "incomin" mesaj kaydı,

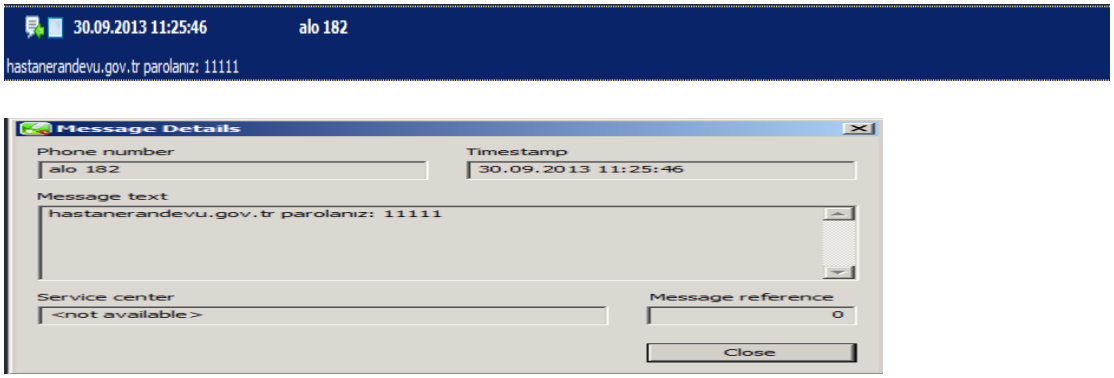
  Gönderilen "Send" mesaj kaydı,
- Notlar "Notes" (18)
- Takvim "Calendar" 49

Cihaz Genel bilgileri: Iphone 4S'in MobilEdite ile bağlantısı ile yapılmış yazılım tarafından tespit edilen bilgiler şekil-62'de gösterilmiştir.

Şekil 62-Mobiledit ile tespit edilen Iphone 4S Cihaz Bilgisi

(1) SMS Kayıtları

Analiz sonucunda sadece 2013 yılına ait gelen bir randevu SMS mesaj bilgisi tespit edilmiş şekil-63'te gösterilmiştir.



Şekil 63-Mobiledit ile tespit edilen Iphone 4S Mesaj Kaydı

f) Yazılımın Değerlendirmesi

(1) Avantajları

- Dosya analiz kısmında üzerine tıkladığımız da HexDump eklentisi ile fiziksel imaj verilerini kendi üzerinde analiz edilebilmektedir.
- Alınan İmajlar daha sonradan import edilmek istediğinde alınan imajın MD5 ile alınmış hash dosyasını istemesi doğrulama açısından önemli bir avantaj sağlamaktadır.
- Kendi üzerinde extra SIM analizi için bir modül bulunmaktadır.
- SIM modülü dahil 10 adet modül ile analiz sonuçlarını gösterebilmekte.
- Ayrıca resimleri görebilmek için photoviewer özelliği bulunmakta.
- Bulunan verileri çeşitli formatlarla çıkartıp rapor halinde sunabilmektedir

(2) Dezavantajları

- Alınan mantıksal ve fiziksel imajların süresi ortalama 24 saat gibi bir zaman almış olup örneğin Samsung GT-N7100 Android analizi yaklaşık 20 ile 30 saat arasında gibi bir zaman dilimi almıştır.
- Analizi yapılan cihazın zaman dilimi bilgisine ulaşılamamıştır.

3. OXYGEN Suite Analizleri

a) Samsung GT-N7100-Mantıksal İmaj Analizi

Oxygen Suite 2014 yazılımını çalıştırdığımızda karşımızsa gelen ekran da çeşitli imaj seçenekleri sunmaktadır. İmaj alma işlemi için yazılımı çalıştırdığımızda sunulan seçeneklerden "live device Acquaistion" seçip bir sonraki adımda mantıksal imaj seçeneğini seçiyoruz burada "default veya advanced" modu sunmakta analiz için default modu seçtiğimizde Oxygen ajanı cihaza yüklenememekte ve imaj işlemine başlamakta. İşlemin sonunda yazılım tarafından tespit edilen cihaza ait bilgiler şekil-61'de gösterilmiştir. Cihazın fiziksel olarak imajının alınması için "Need to Root" özelliği istemektedir. Cihaz üzerinde tespit edilen veri miktarları ve veri alanları aşağıda sunulmuştur.

- Telefon rehberi "Phonebook" kaydı :(593) adet ,
- Mesaj "Message" bilgisi kaydı (919)
- Olay "Event Log" kaydı (999)

  Aranan "Dialed Calls" Arama kaydı

  Cevaplanan "Answered call" kaydı

  Cevapsız "Missed Calls)
- Dosya "File Browser" kaydı 5678
- Takvim "Calendar" kaydı 48
- Zaman "Timeline" kaydı 1111,
- Uygulama "Applications" kaydı

  Applicaitons

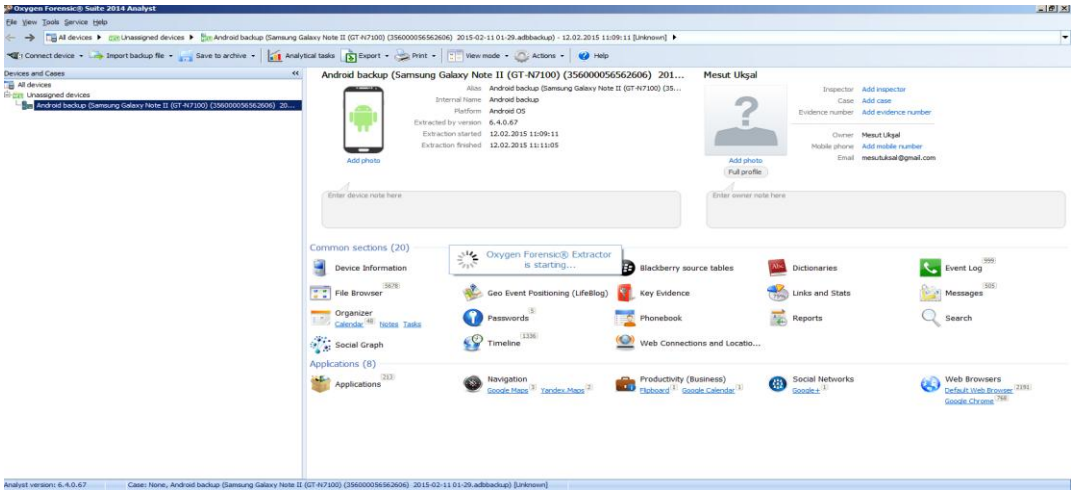
  Navigation Google Maps 3,Yandex Maps 2

  Flipboard 1 ,Google Calendar 1

  Google + 1

  Default Web Browser 2191, Google Chrome 768

Samsung GT-N7100 Oxygen ile analizi sonucuna elde edilen genel bağlantı görüntüsü aşağıda gösterilmiştir



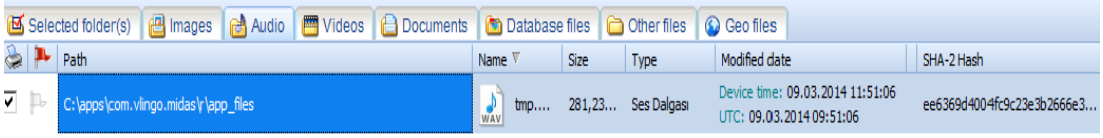
Şekil 64-Oxygen Suite ile tespit edilen Samsun GT-N7100 Cihaz Genel Bilgisi

(1) SIM Analizi

(2) Dâhili/Harici Hafıza Analizi

(a) Dosya Kayıtları

Analiz de **\apps\com.vlingo.midas.\r\app-files** altında dosya bilgileri tespit edilmiştir. 2014 yılına ait ses verisi tespit edilmiş ve şekil-65'te gösterilmiştir.



Şekil 65-Oxygen Suite ile tespit edilen Samsung GT-N7100 Ses Kaydı

(b) SMS Kayıtları

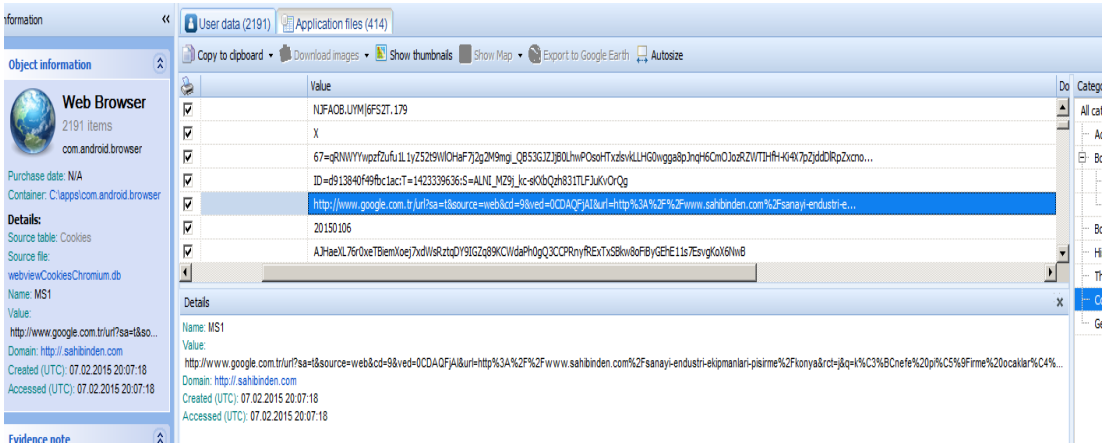
Mesaj "Messages" bölümüne girdiğimizde cihaza ait tüm mesaj kayıtlılarına erişim sağlanmaktadır. Şekil-66'da 2013 yılına ait gelen bir SSM kaydı gösterilmiş olup SHA-2 değeri ile elde edilebilmektedir. Bulunan her bir kayıt bilgileri SHA-2 hash değeri ile gösterilmektedir.

Şekil 66-Oxygen Suite ile tespit edilen Samsung GT-N7100 SMS Kaydı

(3) Uygulama Analizi

(a) Web Geçmişi

Oxygen Suite de "default Web browser" bölümüne girdiğimizde 2191 web kaydı, 768 adet Google Chrome kaydı tespit edilmiştir. Oxgyen Suite ile tespit edilen web sayfası erişim bilgisi Şekil-67'de gösterilmiştir.



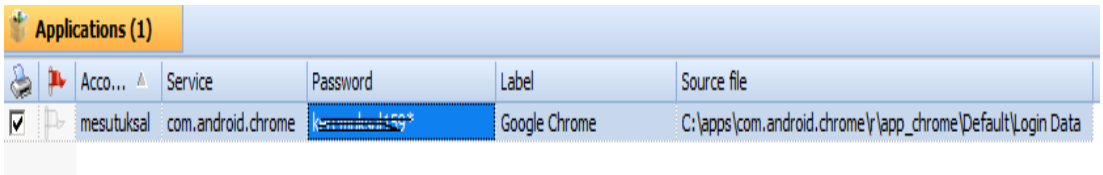
Şekil 67-Oxygen Suite Samsung GT-N7100 Web Sayfası Erişim Kaydı

Web Bookmarks kaydı cihaz üzerinde tespit edilen Bookmarks bilgisi şekil-68'de sunulmuştur

Şekil 68-Oxygen Suite ile tespit edilen Samsung GT-N7100 Bookmarks Kaydı

(b) Google Hesabı Şifresi

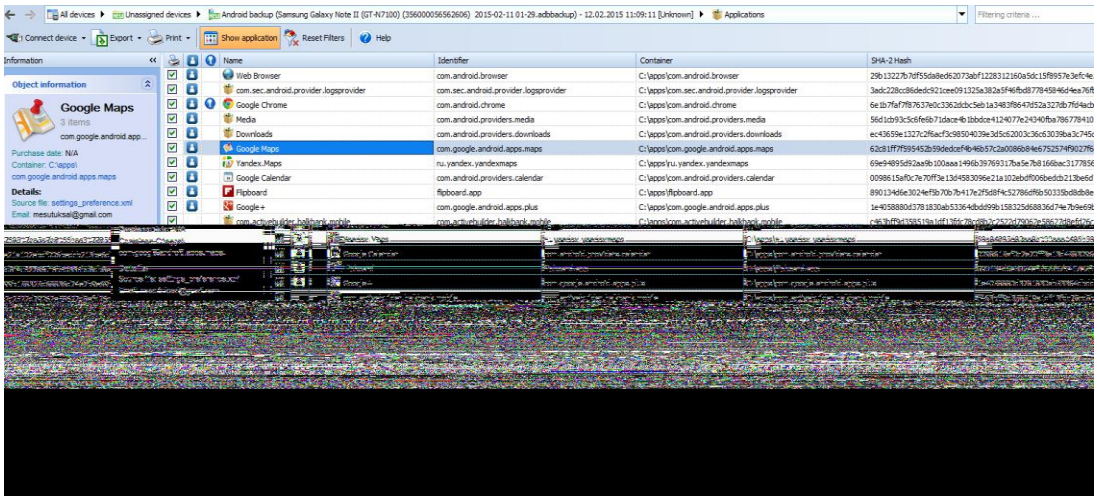
Yapılan analiz sonucunda google hesab şifresi elde edilmiş olup cihaz üzerindeki bilginin bulunduğu alan **"\apps\com.android.chrome\r\app_chrome\Default\Login Data"** alanı olarak verilmiştir.



Şekil 69-Oxygen Suite ile tespit Samsung GT-N7100 Google Hesap Şifresi kaydı

(c) Google Harita

Google maps bilgisi cihaz üzerinde **apps\com.google.android.apps.maps** kısmında tespit edilmiş şekil-70 ve şekil-71'de gösterilmiştir.

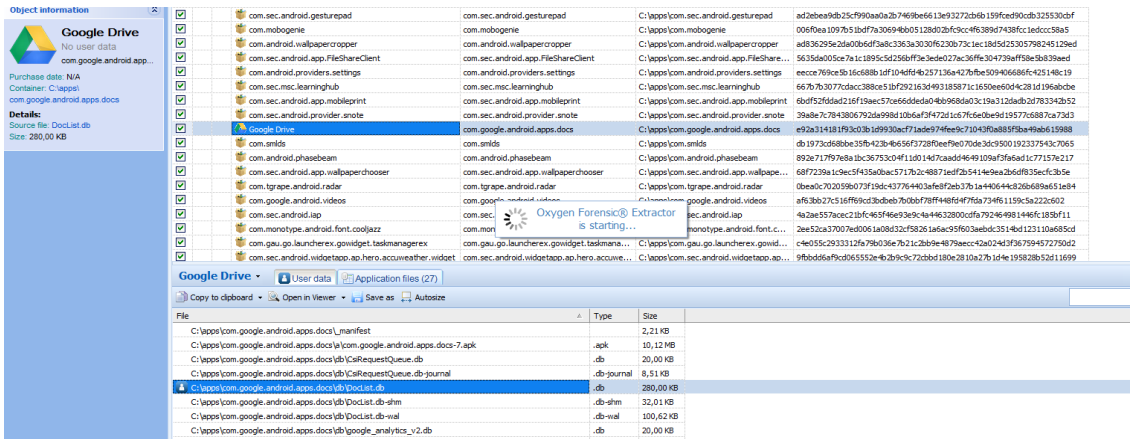


Şekil 70-Oxygen Suite ile tespit edilen Samsung GT-N7100 Google Maps Kaydı

Şekil 71-Oxygen suite Samsung GT-N7100 Google lokasyon kaydı

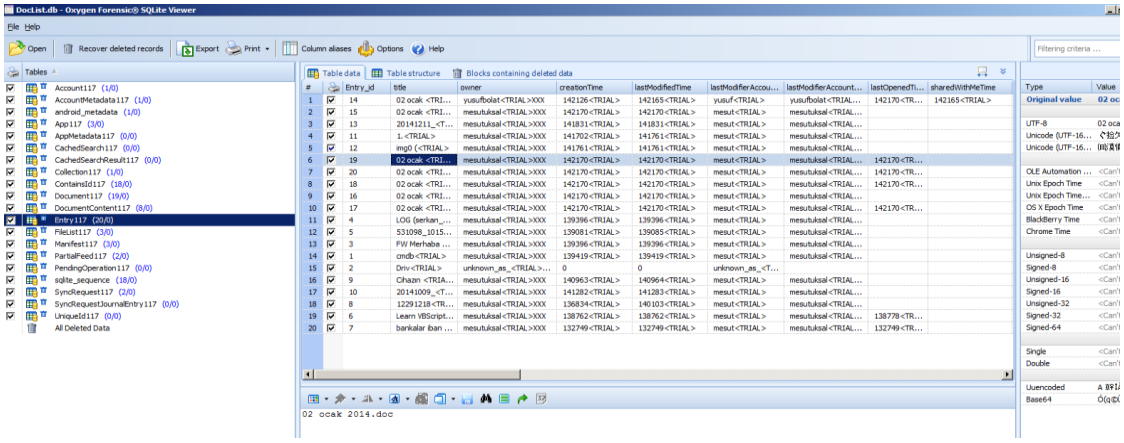
(d) Google Drive

Google drive yüklenmiş verileri belirtiğimiz path **\apps\com.google.android.apps.docs.\db\\DocList.db** kısmında tespit edilmiş şekil-72'de gösterilmiştir.



Şekil 72-Oxygen Suite Samsung GT-N7100 Google Drive Kaydı

Yukarıdaki resimdeki Google drive butonuna tıkladığımızda Oxygen Suite ile bütünleşik çalışan SQL lite browser açılmakta olup inceleme yaptığımızda Google drive yüklenen veriler kimin tarafından ve ne zaman konulduğu görülebilmektedir. Aşağıda şekil-73'te SQL lite ile tespit edilen Google Drive bilgisi gösterilmiştir.



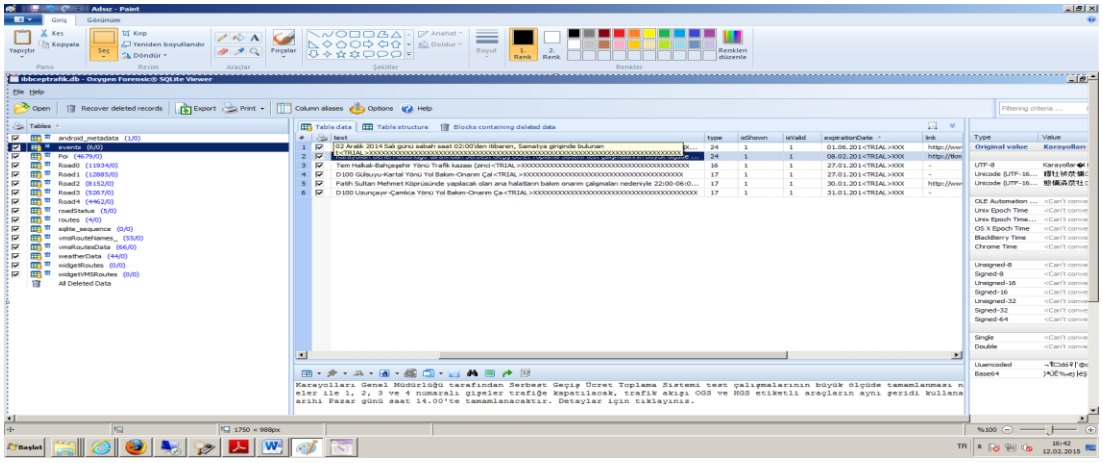
Şekil 73-Oxygen Suite SQL lite Samsung GT-N7100 Google Drive Kaydı

Yukarıda SQL lite browser üzerinde yapılan inceleme de Google Drive üzerinde tespit "02 ocak 2014.doc" isimli dosya gösterilmiştir.

(e) İBB Cep Trafik

Cihaz üzerine yüklenmiş olan uygulamalara "\apps\ klasörü altında tespit edilmiştir. Cihaza yüklemiş olan "ibbceptrafik" uygulaması "**\apps\tr.gov.ibb.ibbceptrafik**" altında tespit edilmiş Şekil-74'te gösterilmiştir.

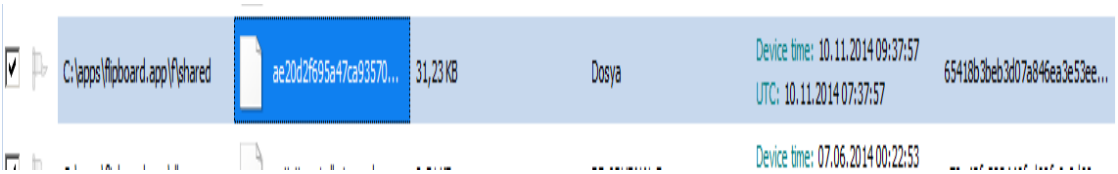
Bulunan veriye tıkladığımızda SQL lite browser ile daha detaylı bir inceleme edilmiş şekil-74'te gösterilmiştir.



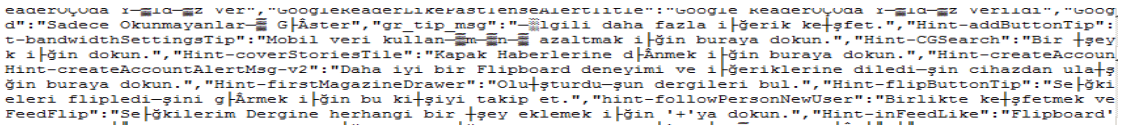
Şekil 74-Oxygen Suite SQL lite GT-N7100 Ibbceptrafik kaydı

(f) Flipboard

Cihaz üzerinde Flipboard uygulamasının yüklendiği **\Apps\Flipboard.app\f\Share** kısmında tespit edilmiştir. Bulunan veriye tıkladığımızda ise verinin içeriği şekil-75 ve Şekil-76'da ise metadata hali gösterilmiştir.



Şekil 75-Oxygen Suite Samsung GT-N7100 Flipboard Uygulama Kaydı



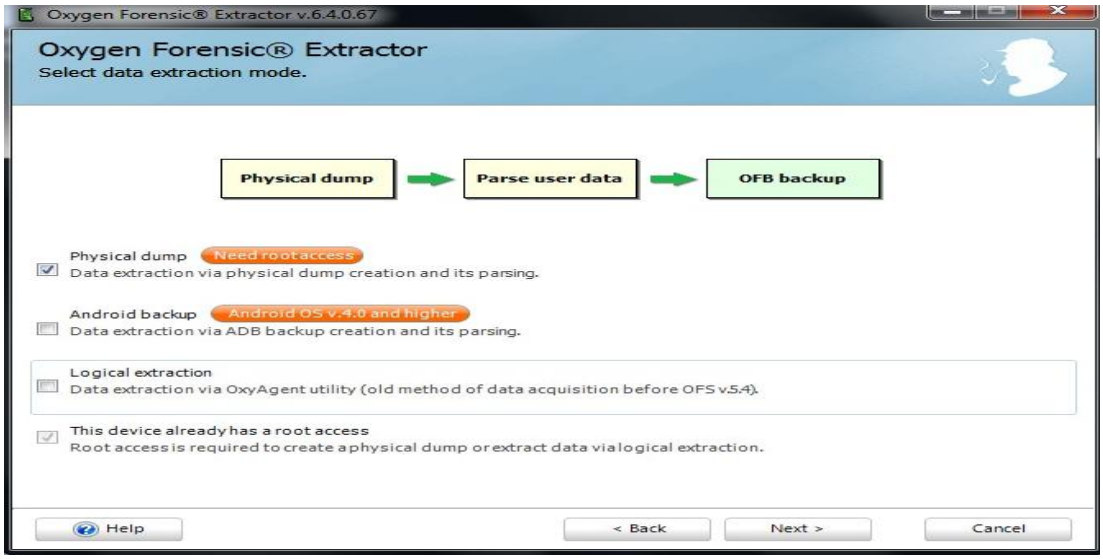
Şekil 76-Oxygen Suite Samsung GT-N7100 Flipboard Metadata Kaydı

b) Samsung GT-N7100-Fiziksel İmaj Analizi

Akıllı cihazın Samsung GT-N7100'nin Oxygen Suite ile bağlantısının sağlandığı şekil-77'de gösterilmiştir.

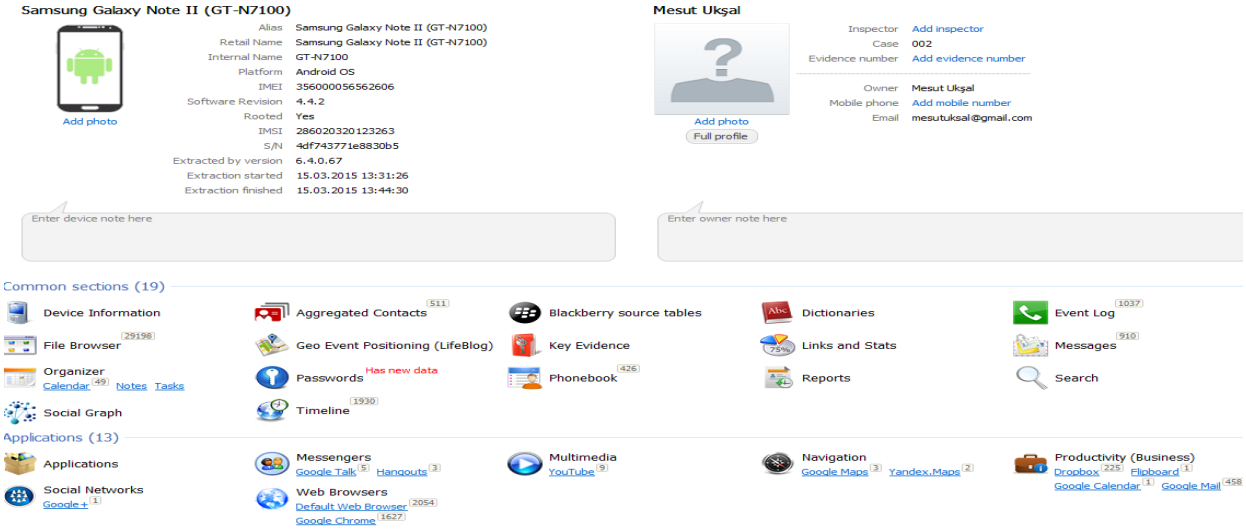
Şekil 77-Oxygen Suite Samsung GT-N7100 Cihaz Bağlantı bilgisi

Sonra ki adımda ise ne tür bir imaj alacağımız sorulmaktadır. Bu aşamada fiziksel imaj alacağımız için fiziksel imaj seçeneğini seçip imaj işlemi başlatılmış şekil-78'de gösterilmiştir.



Şekil 78-Oxygen Suite Samsung GT-N7100 Fiziksel İmaj başlatma Ekranı

Fiziksel imaj sonun da bulunan veriler ve sayıları aşağıda şekil-79'da gösterilmiştir.



Şekil 79-Oxygen Suite ile tespit edilen Samsung GT-N7100 Genel Analiz verileri

Analiz ile bulunan kayıt bilgisi ve sayıları aşağıda sunulmuştur.

- Telefon rehberi "Phonebook" kaydı :(511),
- Mesaj "Message" bilgisi kaydı (910)
- Olay "Event Log" kaydı (1037)

  Aranan "Dialed Calls" Arama kaydı

  Cevaplanan "Answered call" kaydı

  Cevapsız "Missed Calls) kaydı
- Dosya "File Browser" kaydı 29198
- Takvim "Calendar" kaydı 49

- Zaman “Timeline” kaydı 1930
- Uygulama “Applications” kaydı

  Uygulama “Applicaitons” 13 kaydı

  “Google Talks” 5

  “Hangouts” 3

  “Youtube” 9

  Navigation Google Maps 3,Yandex Maps 2

  Flipboard 1 ,Google Calendar 1

  Google + 1

  Google Mail 458

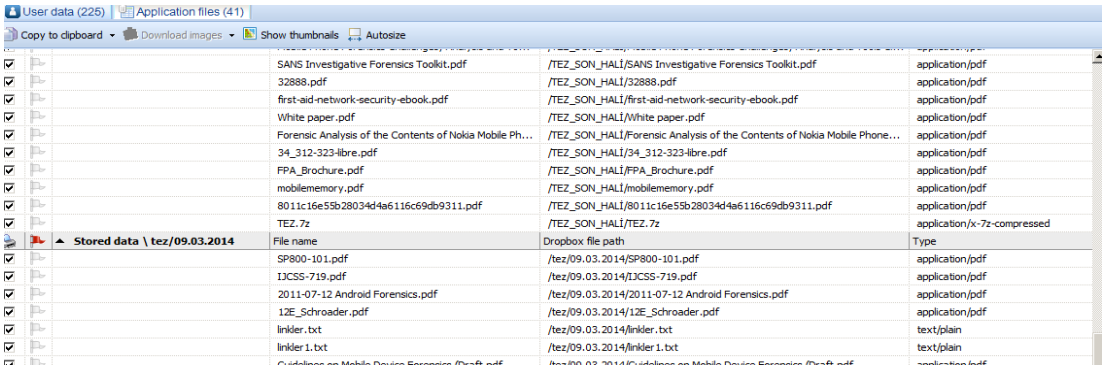
  Default Web Browser 2054, Google Chrome 1627

Mantıksal analiz ile ulaşılan bilgiler dışında tespit edilen bilgiler aşağıda gösterilmiştir.

(1) Uygulama Analizi

(a) Dropbox

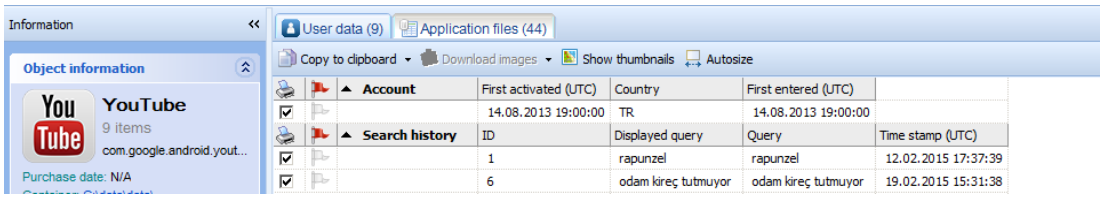
Oxygen üzerinde Productivity (Business) menüsünde Dropbox ikonuna tıkladığımızda Dropbox’a konulan ve \stored data\tez/09.03.2014 bulunan veriler tespit edilmiştir. Aşağıdaki şekil-80’de 2014 yılında Dropbox’a kopyalanan veriler gösterilmiştir.



Şekil 80-Oxygen Suite ile tespit edilen Samsung GT-N7100 Dropbox Kaydı

(b) Youtube

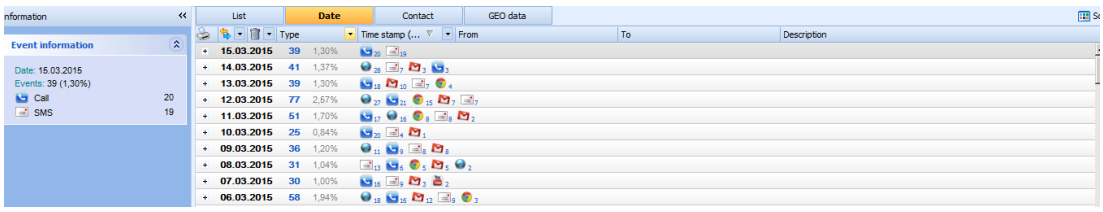
Fiziksel imaj analizi sonucu Application files bölümünde Youtube verilerine erişilmiş ve akıllı cihazın history bilgisinin silinmesine rağmen Youtube üzerinde izlenen videolar tespit edilmiş 2015 yılında izlenen “Rapunzel” isimli çizgi film bilgisi şekil-81’de gösterilmiştir.



Şekil 81-Oxygen Suite ile tespit edilen Samsung GT-N7100 Youtube Kaydı

(c) Zaman "Timeline" Bilgisi

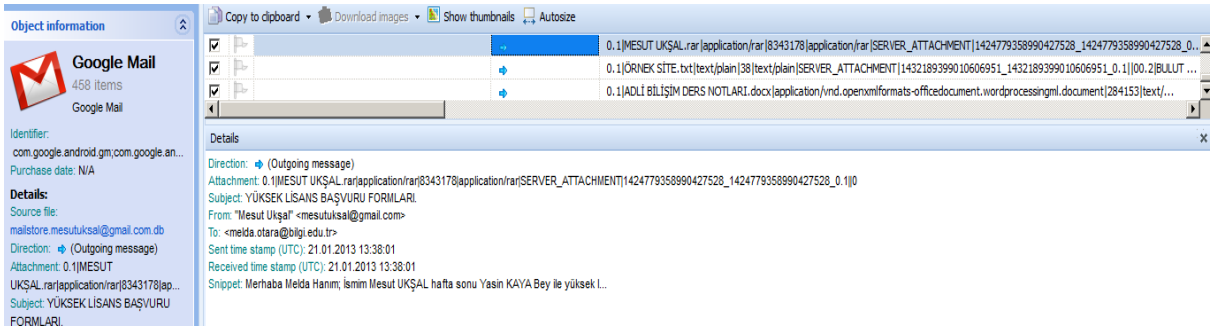
Fiziksel imaj analizinde çeşitli uygulamalara ait tespit edilen **zaman bilgileri** şekil-82'de gösterilmiştir.



Şekil 82-Oxygen Suite Samsung GT-N7100 Uygulama Zaman bilgisi

(d) G-Mail

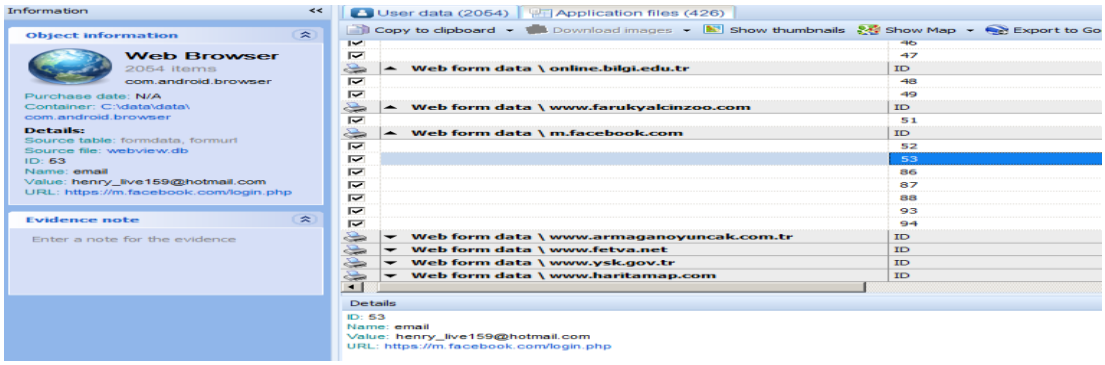
Analiz sonucunda silinmiş Google Mail erişimine ait kayıt bilgileri tespit edilmiştir. Aşağıdaki şekil-83'te 2013 yılında gönderilmiş bir mail bilgisi gösterilmiştir.



Şekil 83-Oxygen Suite ile tespit edilen Samsung GT-N7100 Google Mail Kaydı

(e) Facebook

Akıllı cihaz üzerinde "Web Browser" bölümünde Facebook hesabı ile giriş yapıldığı bilgisi tespit edilmiş şekil-84'de gösterilmiştir.



Şekil 84-Oxygen Suite ile tespit edilen Samsung GT-N7100 Facebook Kaydı

c) Iphone 4S-Mantıksal İmaj Analizi

Cihazımızı bilgisayara bağladıktan sonra Oxygen Suite tarafından otomatik olarak tanınmıştır Şekil-86'da cihazın yazılım tarafından tespit edildiği gösterilmiştir.

Şekil 85-Oxgyen Suite İphone4S Cihaz Bağlantı Bilgisi

Iphone 4s Üzerinde buluna veri bilgileri aşağıda sunulmuştur:

- Telefon rehberi "Phonebook" kaydı :(-) adet ,
- Mesaj "Message" bilgisi kaydı (-)

  Gelen "incomin" mesaj kaydı ,

  Gönderilen "out mesaj kaydı
- Olay "Event Log" kaydı (-)

  Aranan "Dialed Calls" Arama kaydı

  Cevaplanan "Answered call" kaydı

  Cevapsız "Missed Calls) arama kaydı
- Dosya "File" bilgisi kaydı (147)

  Resim "Picture" dosyası kaydı 147

Iphone analiz sonucunda yalnızca 147 adet resim bilgisine erişim sağlanmıştır.

d) Yazılımın Değerlendirilmesi

(1) Avantajları

- Çeşitli formatlarda IOS ve Android imajı alınabilmesini sağlaması ve güzel ve kolay bir arayüz olması büyük bir avantaj.
- 19 ana modül ile bunlara bağlı alt modüller sunması çok farklı çeşitli analizler yapabilmesi büyük bir avantaj.
- Ayrı bir zaman (Tümeline) sekmesi olup bulunan verilerin zaman bilgisi alınabilmektedir.
- Ayrıca bulduğu her verinin SHA-2 değerini göstermekte ve doğrulamasını yapabilmektedir.
- Sekmelere ait bulduğu verileri grafik şeklinde gösterebilmektedir.
- Hem mantıksal hem fiziksel imaj ile bulunan verilerin sayılarının birbirine yakın olarak göstermiştir.
- Üzerinde bulunan SQL lite browser ile çok rahatlıkla veritabanı verileri analiz edilebilmekte.
- Uygulama analizi modülü ile Messengers, Social networks, Web Browsers; Mutimedia, Navigaiton, Dropbox, Flipboard, Google, Google Mail, Google Calendar gibi araçların şifre ve verilerine başarılı bir şekilde hem mantıksal hem de fiziksel imajda ulaşan tek yazılım olması ile büyük bir fark olarak görülmüştür.
- Tüm bulunan veriler içinde arama yapabilmemizi sağlayan bir arama motoru mevcut olması büyük bir kolaylık sunmaktadır.
- Aynı anda birden fazla cihaz imajı incelenebilmektedir.

(2) Dezavantajları

- Yazılım üzerinde doğrudan bir sim kart analizi yapabilen ve bilgilerini gösteren modül bulunmamaktadır.

C. Araştırma Bulguları

Bu araştırmada mobil cihazlar üzerinde bulunabilecek ve delil olarak sunulabilecek verilerin tepsit edilmesi ve mobil cihazlar üzerindeki verilerin nerede bulunabileceği ve nasıl elde edilebileceğine dair bilgilerin sunulması amaçlanmıştır.

Bu araştırmada üç farklı ücretli yazılım ve faklı işletim sistemine sahip 6 farklı marka model akıllı ve normal telefonlar kullanılmış, analiz işlemi yapılmıştır. Cihazların SIM kartı dahili hafıza ile harici hafızalarında olabilecek "Arama kayıtları, Rehber kayıtları,Resim, Video, Ses ile yüklenmi ş uygulamalara ait veriler,sosyal medya araçlarına ait veriler" örnek olarak gösterilebilir.

Bu verilerin çoğu mobil cihazların bünyesinde bulundurduğu kullanıcıya ait olan kişisel verilerdir.Bu veriler şifreli veya şifresiz bulunabilmekte olup adli bilişim analiz işlemine bu verilere zarar vermeden cihazlar üzerinde bu veriler yazılımlar tarafından tespit edilerek bu verileri elde etmektir. Bütün bu çalışmaların tek bir amacı olması gerekmekte olup bir olayın açığa kavuşturulması veya yeniden gözden geçirilmesini sağlayacak seviyede bir sonuç ortaya koymak ve bu sonucu yasal makamlara d elil ve kanıt olarak sunulacak seviyede ve yapıda raporlama işelmi yaparak sunmaktır.

Mobil cihazların kendilerine özgü dosya sistemi ve koruma yöntemleri olması nedeniyle cep telefonları üzerinde kullanıcıları tarafından görülebilen veriler olabildiği gibi kullanıcı tarafından görülemeyen veriler veya bu verilere ai izler mevcut olabilmektedir. Bu veriler şifreli dahi olsa mobil cihaz adli bilişim yazılımları tarafından bulunamaz ise dahi ileri seviye forensics data recover işlemleri ile elde edilebilir. Bu sistemler üzerine yüklenmiş olan aynı uygulamalara ait izler ve bulma yöntemleri cihaz marka modellerine göre çeşitli farklı özellikler gösterebilir ve farklı alanlarda bulunabilmektedir.Ya da farklı dijital izler bırakabilmektedir. Ayrıca tek bir yazılım ile istenilen verilere erişim sağlanamayabilir olup bu sebeple farklı farklı yazılımlar kullanılarak yapılan analiz sonuçları karşılaştırılmalı ve her zaman bir doğrulama işlemi yapılması analiz işlemine kesinlik katacaktır.

Şifreli sistemler de daha fazla derine inmek gerekebilir ve bu nokta da ileri seviye dediğimiz adli bilişim teknikleri kullanılarak fiziksel imajlar alınarak imaj üzerinde analiz işlemleri HexaDecimal veri üzerinde yapılarak delil gerekebilir. Çünkü işleme tabi tutulan bu cihazlar bilinçli bir şekilde güvenli sil işlemi yapılarak silinmiş de olabilir.

Bu analiz ve inceleme sürecinde 3 adet " XRY, MobilEdite ve Oxygen Suite 2014" yazılımları ile Android,Symbian,iOS işletim sistemleri ile işletim sistemi olmayan cihazlar birçok metot kullanılarak analiz edilmiş ve analiz neticesinde kullanıcıya ait silinmiş kişisel verileri araştırılıp ve bulunmuştur.

Bu araştırma göstermektedir ki inceleme yapan bir adli bilişim uzmanı tarafından özel mesajlar mailler zaman bilgileri, paylaşılmış verileri, yer ve zaman bilgileri ve diğer kişisel verilerin elde edilebileceği görülmüştür.

Yapılan analizler de çıkartılan sonuçlara göre bulunan veri içerikleri farklı zaman bilgileri ve log kayıtları içerebilmektedir.

Bütün platformlarda rehber bilgileri, arama kayıtları dosyalar "Resim, müzik, video" verileri farklılıklar gösterilmiş olup tespit edilen değerler sayfa 81 ve 85 'deki tablolarda sunulmuştur. Bazı platformlar da 2008 yılına ait veriler bulunabilmiş ve bazı cihaz analizinde ise çok kısa bir zaman dilimindeki verilere erişilebilmiştir.

Android ve iOS arasındaki en temel fark şifreleme mekanizması olup her iOS cihazı kendine has bir 250 bit AES kriptolama yapısına sahiptir. Tüm dosya sistemi donanım bazında şifrelenmiş bir yapıya sahiptir. Analiz aşamasında imaj alınabilmiş fakat direk içeriği görüntülenememiştir.

Andorid, siatemler ise iOS göre daha esnek bir yapıya sahip olup Android cihazların mantıksal imajında analiz neticesinde verilere erişilebilirken iOS üzerindeki mantıksal imaj analizlerinde hemen hemen hiç denilecek verilere erişilebilmiştir. İki sistemin "Andorid ve iOS" cihazların mantıksal imajında bulunan veriler ile Fiziksel imajı analizi sonucunda bulunan veri sayıları arasında büyük farklar mevcut olup fiziksel imaj üzerinde bulunan verilerin daha fazla olduğu görülmüştür.

Özellikle hem Android hem de iOS cihazlar üzerinde yapılan rooting ve jailbreak ileminin ardından yapılan analiz sonucunda bile bulunan verilerin özellikleri ve sayıları açısından ciddi farklılıklar tespit edilmiştir. iOS analizinde yazılım ile analiz işlemi başlatmak için bilgisayara bağladığımız cihazın kapalı bir sistemi olması nedeni ile sadece cihaz üzerinde bulunan resim klasörleri görülebilmiştir. Bu da iOS sisteminin diğer sistemlerden daha güvenli olduğunu gösteren bir somut özellik. Farklı platformlarda yapılan analiz işlemleri öncesi yapılan jailbreak ve rooting işlemleri birbirine benzer gibi de gözükse cihaz ve yazılımlar üzerinde farklı sonuçlar çıkmasına neden olmuştur.

Diğer bir hususta kullanılan yazılımlara cihazların bağlantı şekli ve kullanılan donanımlar olmuştur Nokia 5800 ve Samsung GT-N7100 kendi orijinal kablosu ile bilgisayar ve yazılımlar ile bağlantı işlemini greçekleştirememiştir.Farklı marka model cihaza ait bir mikro usb kablo ile bağlantı sağlanarak analiz edilebilmiştir.

Kullanılan yazılımların avantaj ve dezavantajları yukarıda her bir yazılım için ayrı ayrı her bölümde değerlendirilmiştir. Günün sonunda bir adli bilişim uzmanı olarak veya kolluk birimi hem mantıksal hem fiziksel imaj alınıp delil aranması işlemi yapacak ise ve bulunan değerlerin doğruluğu ve bütünlüğü hakkında düşük bir risk almak isterse bu nokta analiz için kullanılan "XRY, Mobiledit ve Oxygen suite" arasında çok büyük olumlu farkların olduğu tespit edilmiştir.Özellikle Oxygen Suite yazılımı ile bulunan veri sayısı gözönüne alındığında yazılımlar arasında bulunan veri sayılarında büyük bir fark olduğu tespit edilmiştir. Oxygen suite yazılımının mobil adli bilişim yazılımı özellikleri noktasında daha geniş teknik imkân ve kabiliyete sahip olduğu tespit edilmiştir. Bu yazılım ve üzerindeki diğer adli bilişim araçları ile ilk aşamada ayrı bir analiz yazılımına ihtiyaç olmadığı değerlendirilmektedir.Fakat sonuç ne kadar kesin ve doğru gibi gözükse de yapılan analizler

farklı farklı yazılımlar ile hem klasik computer forensics hem de mobile forensics araçları kullanılarak yapılmalı, sonuçlar karşılaştırılmalı ve ilgili yasal merciye verilecek sonuç raporunun bu şekilde ortaya konulmasında fayda olacağı değerlendirilmektedir.Bu şekilde olması yapılan analizin daha tutarlı olmasını ve yasal sürecin sağlıklı ve adil bir şekilde devam veya sonlamasını sağlayacaktır.Her bir yazılımda veri kurtarma işlemi Android için kolay olmasına rağmen iOS için bu kolaylığı söylemek mümkün değildir.

8.SONUÇ, YORUM VE ÖNERİLER

Akıllı Cep telefonları gün geçtikçe daha karmaşık ve yetenekli hale gelerek yaygınlaşmaktadır. Bütün kurum ve kuruluşlar gelişen mobil teknoloji ile birçok kolaylığı ve rahatlığı kullanıcılara sunabilmekte. Fakat gelebilecek saldırı ve tehditlere karşı çeşitli önlemler alınmasına rağmen hem kişisel hem de kurumsal anlamda tam güvenlik sağlanamamakta "Gizlilik, Erişebilirlik ve Bütünlük "kavramları zarar görebilmektedir.

Mobil teknoloji kapsamında işlenen suçlar açıklığa kavuşturulabilmesi maksadıyla adli bilişim metotları ile yapılan incelemeler geniş zaman ve büyük bütçe maliyetleri gerektirmektedir. Mobil cihazların kullanım oranlarının artması adli bilişim metotlarına ilişkin ilke ve yöntemlerin belirlenmesi ihtiyacını ortaya koymuştur. Akıllı telefonların donanımsal ve yazılımsal olarak çok çeşitli standartlara sahip olması her cihazın inceleme metotlarının birbirinden farklı olmasına sebep olmaktadır. Yapılan incelemede her ne kadar metotlar birbirinden farklı olsa da standart olması gerekli hususlar incelemenin belgelendirilmesi, sonuçların tekrarlanabilmesi ve mahkemede sunulabilir olması gerektiğinden akıllı cep telefonları kullanımı ile ortaya çıkan sonuçlar "Adli Bilişim, Hukuk ve Sosyal" açılardan değerlendirilmesi gereken kavramlardır.

Öyle ki kendinden önceki tüm iletişim ve bilgisayar teknoloji sistemlerini geride bırakarak basit bir iletişim aracı olmaktan çıkmış, kişisel bilgisayarlarla akıllı mobil cihazlar arasındaki fark neredeyse kapanmıştır. Mobil cihazların donanım ve işletim sistemleri neredeyse bilgisayarlarla ile aynı kapasite ve özelliklilere ulaşmış, bu cihazların kullanımın özellikleri ve kapasitelerinin artması bilgisayar ortamında yapılan birçok işlemin "Bankacılık, Fotoğraf, Video Kamera, Yön bulma, Oyun, İnternet ve Sosyal Medya ve iletişim" gibi daha birçok işlem yapılabilmektedir. Özellikle 4G teknolojisinin de yakın bir zaman da kullanılması ile birlikte evimiz ve işyerimizde bulunan birçok elektronik cihazı yönetebilecek seviyede olacaktır. Bu teknolojik kolaylık ile birlikte bu dünyadaki suç ortamları da artacak olup özellikle bu teknoloji dünyasındaki teknik suç analizleri önem kazanacaktır. Bu açıdan bakıldığında bu araştırmada üç farklı yazılım ile çeşitli farklı marka ve model cihazlar analiz işlemine tabir tutulmuştur. Bu analizler neticesinde aslında mobil cihazlar üzerinde bulunan delil alanlarının belli olmasına rağmen her bir yazılım ile bulunan sonuçlar da benzerlikler olmasına rağmen ciddi farklılıklar da mevcuttur.

Sonuç olarak akıllı mobil cihazlar ile akıllı olmayan cihazlar dahi kullanılmaya başlandığı andan itibaren hem cihaz sistemine dair hem de kullanıcı dair izler oluşturmaya başlamakta, "Veritabanı dosyaları, olay kayıtları, xml dosyaları (database files, log files, xml files and plist files)" olup veriler gizli ve açık şekilde bulunabilmektedir. Bu veriler ücretli/ücretsiz ve açık kaynak mobil adli bilişim yazılımları ile analiz edilip kolay bir şekilde elde edilebilir. Kullanıcı isimleri, telefon numaraları, arkadaş listeleri, E-mail içerikleri, SMS/MMS mesajları, resimler, videolar, uygulamalara ait veriler, dosya zaman bilgileri, lokasyon bilgileri ve internete uygulamalarında dair bilgiler silinmelerine rağmen elde edilip potansiyel delil olarak sunabilir. Ayrıca bu veriler CMK'nın bu sürece izin veren maddeleri

işletilerek yetki merciler vasıtasıyla da mobil cihaz kullanıcısına ait delil olabilecek veriler abonesi olduğu ilgili operatör aracılığı ile elde edilebilmektedir. Bu araştırma da akıllı cihazların üzerinde tutabildiği kullanıcılara ait kişisel verilerin silinmelerine rağmen tamamen ortadan kalkmadıklarını ve bir şekilde bir iz ve olaydan yola çıkılarak geri döndürülebildiği gösterilmeye çalışılmıştır. Bu sürecin bu şekilde yeni işletim sistemleri ve uygulamalar çıktıkça devam edeceği aşikâr olup bura da yapılması gereken hususlar Adli bilişim yöntem ve yazılımlarının bilirkişi ve yasal merciler tarafından sürekli takip edilmesi her çıkan yazılım ve donanımları yetenekleri çok iyi bir şekilde incelenip öğrenilmesi gerekir. Bir mobil cihaz adli bilişim analizi bir yazılım veya bir uzaman ile sınırlandırıldığı takdirde o analizin sağlıklı olduğu her daim tartışmaya açık olup yasal merciler önünce verilecek kararların doğrudan verilmesi şartında bireyleri masumiyet karinesi ve adil yargılanmasına sorun teşkil edecektir. Yapılması gereken bir cihazın birkaç yazılım ve yapılabilirse farklı uzman kişilerce analiz edilip sonuçların karşılaştırılması ve doğruluğunu kontrol edilmesi gerekir. Özellikle iOS platformalar güçlü ve gizli bir dananım ve yazılım yapısına sahip olması nedeniyle bu cihazlarda mobil adli bilişim yazılımlarının yanı sıra klasik "computer forensics" analizlerinin yapılmasında fayda olacağı değerlendirilmektedir.

Mobil cihazların güvenliği desteklenmesi ve bu cihazlar kullanılırken daha dikkatli olunması gerekmektedir. Cihazların çeşitliliği bu durumun hem kontrol ihtiyaçlarını hem de mevcut güvenlik çözümleri ciddi manada dezavantaj olarak etkilemekte olup mobilitenin güvenlik sorununu çözecek doğrudan, bir yöntemin olmadığı unutulmamalıdır. Mobil cihaz kullanıcıları bireysel ve kurumsal anlamda bu konuda eğitilmeli ve bilinçlendirilmesi gerektiğini alınabilecek temel güvenlik önlemlerini "Gazi Üniversitesi tarafından Bilimsel Araştırma Kapsamında Yapılan Proje " Şeref SAĞIROĞLU ve Hülya BULUT tarafından aşağıda belirtilen mobil cihazlarda temel güvenlik önlemlerinin aşağıda belirtilen maddeler kapsamında alınması gerektiğine dair dikkat çekmişlerdir.[156]

- Mobil cihazlarda mutlaka (anti-virüs, anti-casus, anti-spam) yazılımlar kullanılmalı ve işletim sistemi dâhil olmak üzere sürekli güncel tutulmalıdır.
- Wireless ağ İnternet bağlantısı kullanan mobil cihazlarda güvenlik duvarı kurulmalı ve sürekli açık tutulmalıdır.
- Cihazların ağ uygulamaları kapalı konuma getirilmeli ya da 'görünme durumu' seçeneği 'gizli' yapılıp açık hedef olması engellenmelidir.
- Mobil telefon PIN kodları ve diğer şifreleri kesinlikle konulup kullanılmalı ve kesinlikle şifre politikası basit bir yapıdan oluşmamalı

156 SAĞIROĞLU, Şeref; BULUT, Hülya. Mobil ortamlarda bilgi ve haberleşme güvenliği üzerine bir inceleme. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, 2009, 24.3. http://www.mmfdergi.gazi.edu.tr/article/viewFile/1061000183/1061000154 Et:28.04.2015

- Tüm mobil cihazları GSM ağında kendini tanıtan 15 haneli bir uluslararası mobil cihaz kimlik numarasına (IMEI – International Mobile Equipment Identification) sahip olup kullanıcıların çalınma ya da kaybolma riskine karşı cihazlarının IMEI numarasını kaydettirmeleri gerekir.

- Mobil cihaz içerisindeki veriler kesinlikle şifrelenmiş olarak saklanmalıdır. Mümkün olduğunca da bu şekilde tutulmamaya çalışılmalıdır.

- Mobil cihaza kopyalanan ve indirilen tüm dosyalar virüs taraması yapıldıktan sonra kullanılmalıdır.

- Mobil telefonların, pil seviyesi, pil tüketim oranı, veri aktarımı ve işlemci aktiviteleri gibi en kritik istatistiklerinin günlüklerini kontrol edilmelidir.

- Kurumlarda kullanılacak mobil cihazlar, erişim için kimlik kanıtlama isteyecek şekilde ayarlanmalıdır. Cihazın yapılandırmasında güvenlik ayarları da göz önünde bulundurulmalıdır. Mobil cihazda saklanan verilerin düzenli olarak yedeğini alınmalı

- Tüm kullanıcılar, mobil ortamlardaki güvensizliğin farkında olmaları ve güvenlik önlemlerini almaları gerektiği bilincinde olmalı ve önceki maddelerde belirtilen hususları uygulamaya çalışmalı ve mobil ortam güvenliğinden kendilerinin de sorumlu olduklarını unutmamalıdırlar. Bu noktada kendilerini eğitip bilinçli bir kullanıcı olmalılar.

- Mobil cihazlarına indirip kuracakları uygulamaların kaynağı çok iyi araştırıp lisanlı uygulama kullanmaya dikkat etmeleri gerekir.

Hukuki olup en önemli bölümünü olan bu yönüne bakmaktadır. Çünkü adli bilişim alanına giren tüm incelemeler neticesinde bulunan deliller mahkeme ve diğer resmi kuruluşlar tarafından bir olayın aydınlatılması açısından kullanılmaktadır. Bu nokta inceleme yapan birim ve kişiler yaptırdıkları incelemeleri sonucunu yoruma açık bırakmayacak kadar bir yüzde oranında sağlanmalıdır. Çünkü bu nokta da atlanabilecek çok küçük nokta insanların masumiyet karinesi zedeleyici bir işlem olacaktır.

Türk Hukuk sistemimizde Adli Bilişime ilişkin kanun maddeleri CMK 134'ncü maddesinin 1'nci bendinde bilişim sistemlerinde arama yapılabilmesi için mahkeme kararı olması gerektiği belirtilmektedir. Mahkeme kararı olmadan arama ve inceleme yapılması mümkün kılmamaktadır. 2'nci bendinde ise; adli bir olay esnasında delillerin şifrelenmiş olması veya içerisinde gizlenmiş bilgiler olabilmesi ihtimali nedeni ile verilere ulaşılamaması durumunda veya şifrelerin çözülmesi ve inceleme yapılabilmesi maksadıyla İMAJ "Görüntü Kopyası" oluşturmak için delillere ve cihazlara el konulabileceği belirtilmiştir. Ayrıca şifrelerin çözülmesi ve gerekli kopyaların alınması durumunda, el konulan cihazların geciktirilmeden iade edilmesi hükmü bulunmaktadır.

Bu nokta da ise mağduriyetlerin ve su istimallerin yaşanmaması için özellikle Adli bir olay da olaya mahallinde ve sonrasında çok dikkatli olunmalı deliller kayıp ve zarar

görmeyecek şekilde toplanmalı inceleme yapılacak mahalde güvenli bir şekilde ve bütünlüğü bozulmayacak şekilde ulaştırılmalı ve en önemli kısmı analiz dikkatli ve bilinçli bir şekilde yapılması gerekmektedir.

CMK da birkaç madde ile sıkıştırılmış olan bu alan daha kapsamlı bir şekilde tanımlanmalı ve bu işi yapacak uzmanların görevleri ve sorumlulukları da yasal çerçeveye konulup belirtilmelidir.

Unutulmamalıdır ki adli makamlara sunulan deliller herkes tarafından kabul görmüş standartlara sahip güvenirliliği testler kabul görmüş adli bilişim yazılımları, cihaz, teknik ve yöntem ile elde edilip adli birimlerle sunulmalıdır.

Tüm eylemlerin ve gözlemlerin dikkatli bir şekilde kayıt altına alınmasına, testlerin ve inceleme sonuçlarının ifade edilmesine ve kanıtlarla yapılan çıkarımların açıklanmasına bağlıdır. İyi bir rapor güvenilir belgelere, notlara, fotoğraflara ve cihazlarla ortaya çıkartılan içeriğe dayanır.

Akıllı cihaz kullanan bireyler kötü niyetli kişileri birçok yöntem "Sosyal medya, e-posta ve SMS ve Sahte aramalar tuzaklarına çekilebilmekte ve bu nokta Özel hayatın gizliği ve mahremiyeti ile maddi mağduriyetlerin yaşanmasına neden olabilmektedirler.

Bu nokta bireyler olarak hukuksal haklarımızın neler olduğunu ve nelerin olması gerektiğini böyle bir mağduriyette hangi kanun yoluna nasıl başvuru yapılacağını bilmek gerekmektedir. Ayrıca sivil ve resmi kurumlar noktasında bilgi Güvenliği standartlarının sağlanması gerekmektedir. Kurumsal manada bilgi güvenliği standartlarının sağlanması gerekmektedir.

Mobil ortamlarda işlenen suçların kapsamı her geçen gün artmakta olup bizler bu dünyanın bir parçası olarak hayatımızı bu kadar kolaylaştıran bu teknolojiden maksimum seviyede faydalanırken bize getireceği zararlarında bilincinde olmalıyız. Bu şekilde hem kendimizi hem de kurumumuzu ciddi mağduriyetlerden korumuş oluruz. Diğer ve son bir husus ise sunulan adli bilişim raporlarının içeriğinin net ve anlaşılır bir şekilde oluşturulması olup, Adli bilişim incelemelerinin sonuç raporları davayı ve davanın kaynağını tanımlamak, test sonuçlarının ve bulgularının taslağını çıkarmak için gereken tüm bilgileri içermeli ve incelemenin içeriğinden sorumlu olan kişinin imzasını taşımalıdır.

Bu teknolojinin bilgi, adli bilişim konusunda inceleme yapan uzmanları ve akıllı cep telefonu kullanan insanları teknik, hukuki ve kişisel güvenlikleri açısından bilgilendirme amaçlanmıştır.

İstanbul Bilgi Üniversitesi
LAUREATE INTERNATIONAL UNIVERSITIES

SOSYAL BİLİMLER ENSTİTÜSÜ

TEZ TESLİM FORMU

01.06.2015

Sosyal Bilimler Enstitüsü'ne

Tez danışmanlığını yürüttüğüm, Bilişim ve Teknoloji Hukuku Programı öğrencilerinden 112692044 numaralı Mesut UKŞAL tez çalışmasını bitirmiş olup, savunma aşamasına gelmiş bulunmaktadır. Tezin ciltlenmemiş kopyası tarafıma teslim edilmiştir.

Durumu bilgilerinize sunar, gereğini arz ederim.

Saygılarımla,