Mobile Device Forensics

MODULE 18

Contents

Mobile Device Forensics

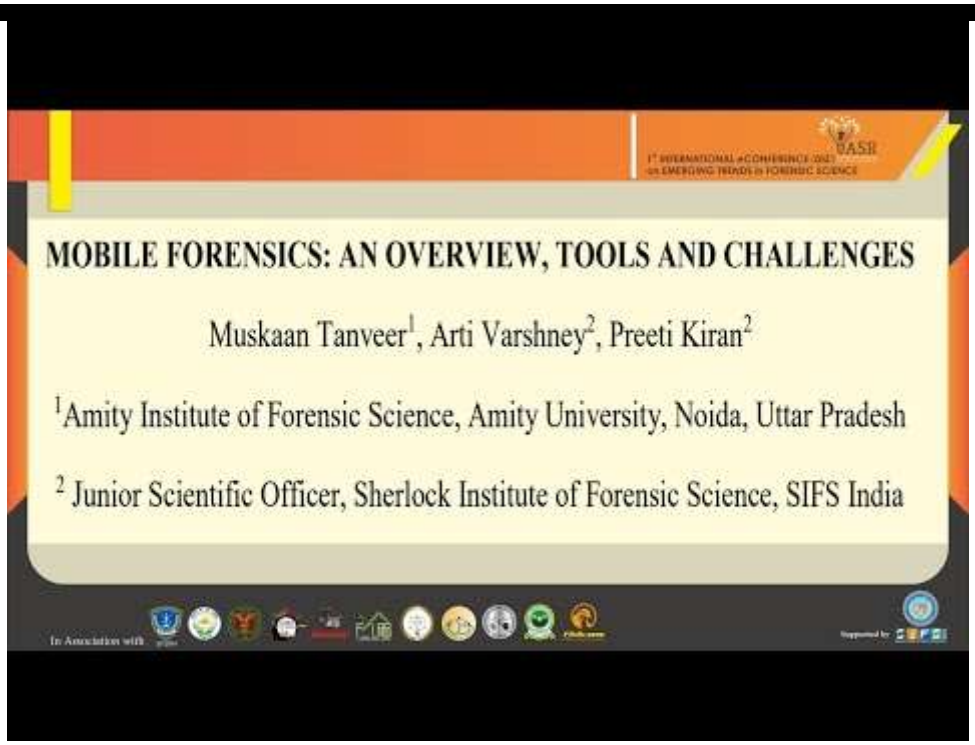
18.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Define Mobile communication and need for mobile forensics.
- Capture evidences from a mobile device.
- Explain various forms of logs in mobile.
- Perform mobile forensics.
- Use few mobile forensic acquisition tools.

18.2 INTRODUCTION

VIDEO LECTURE



This lecture is adopted from https://youtu.be/GfPrKc8rmIo available under Creative Commons Attribution license (reuse allowed)

Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions. The phrase mobile device usually refers to mobile phones; however, it can also relate to any digital device that has both internal memory and communication ability, including PDA devices, GPS devices and tablet computers.

The use of phones in crime was widely recognized for some years, but the forensic study of mobile devices is a relatively new field, dating from the early 2000s. A proliferation of phones (particularly smartphones) on the consumer market caused a demand for forensic examination of the devices, which could not be met by existing computer forensics techniques[1].

Mobile devices can be used to save several types of personal information such as contacts, photos, calendars and notes, SMS and MMS messages. Smartphones may additionally contain video, email, web browsing information, location information, and social networking messages and contacts.

There is growing need for mobile forensics due to several reasons and some of the prominent reasons are:

- Use of mobile phones to store and transmit personal and corporate information
- Use of mobile phones in online transactions
- Law enforcement, criminals and mobile phone devices.

18.3 CHALLENGES IN MOBILE FORENSICS

Evidential and technical challenges exist. For example, cell site analysis following from the use of mobile phone usage coverage, is not an exact science. Consequently, whilst it is possible to determine roughly the cell site zone from which a call was made or received, it is not yet possible to say with any degree of certainty, that a mobile phone call emanated from a specific location e.g. a residential address.

To remain competitive, original equipment manufacturers frequently change mobile phone form factors, operating system file structures, data storage, services, peripherals, and even pin connectors and cables. As a result, forensic examiners must use a different forensic process compared to computer forensics.

- Storage capacity continues to grow thanks to demand for more powerful "minicomputer" type devices.
- Not only the types of data but also the way mobile devices are used constantly evolve.
- Hibernation behavior in which processes are suspended when the device is powered off or idle but at the same time, remaining active.

As a result of these challenges, a wide variety of tools exist to extract evidence from mobile devices; no one tool or method can acquire all the evidence from all devices. It is therefore recommended that forensic examiners, especially those wishing to qualify as expert witnesses

in court, undergo extensive training in order to understand how each tool and method acquires evidence.

18.4 MOBILE COMMUNICATION

Mobile communication means can be categorized in basically three modes:

a) 802.11or WiFi
b) Bluetooth
c) Infrared(IrDA)

18.4.1 802.11 or WiFi

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method by which homes, communications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure. Wi-Fi (or WiFi) is a local area wireless computer networking technology that allows electronic devices to connect to the network. Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. A common misconception is that the term Wi-Fi is short for "wireless fidelity," however this is not the case. Wi-Fi is simply a trademarked phrase that means IEEE 802.11x. The Wi-Fi Alliance, the organization that owns the Wi-Fi registered trademark term specifically defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards." Initially, Wi-Fi was used in place of only the 2.4GHz 802.11b standard; however, the Wi-Fi Alliance has expanded the generic use of the Wi-Fi term to include any type of network or WLAN product based on any of the 802.11 standards, including 802.11b, 802.11a, dual-band, and so on, in an attempt to stop confusion about wireless LAN interoperability.

18.4.2 Bluetooth

Bluetooth is defined as being a short-range radio technology (or wireless technology) aimed at simplifying communications among Internet devices and between devices and the Internet. It also aims to simplify data synchronization between Internet devices and other computers.

Bluetooth products i.e. products using Bluetooth technology must be qualified and pass interoperability testing by the Bluetooth Special Interest Group prior to release. Bluetooth's founding members include Ericsson, IBM, Intel, Nokia and Toshiba. A new version of the Bluetooth wireless device-to-device technology that offers significantly lower power consumption than previous versions. Also referred to as Bluetooth Low Energy, Bluetooth 4.0 achieves its reduced power consumption by enabling devices to remain paired, or connected to each other, without requiring a continual stream of data to be transferred between the devices.

18.4.3 Infrared (IrDA)

Short for Infrared Data Association, a group of device manufacturers that developed a standard for transmitting data via infrared light waves. Increasingly, computers and other devices (such as printers) come with IrDA ports. This enables you to transfer data from one device to another without any cables. For example, if both your laptop computer and printer have IrDA ports, you can simply put your computer in front of the printer and output a document, without needing to connect the two with a cable. IrDA ports support roughly the same transmission rates as traditional parallel ports. The only restriction on their use is that the two devices must be within a few feet of each other and there must be a clear line of sight between them.

18.5 EVIDENCES IN A MOBILE DEVICE

As mobile device technology advances, the amount and types of data that can be found on a mobile device is constantly increasing. Evidence that can be potentially recovered from a mobile phone may come from several different sources, including handset memory, SIM card, and attached memory cards such as SD cards.

Traditionally mobile phone forensics has been associated with recovering SMS and MMS messaging, as well as call-logs, contact lists and phone IMEI/ESN information. However, newer generations of smartphones also include wider varieties of information; from web browsing, Wireless network settings, geo-location information (including geo-tags contained within image metadata), e-mail and other forms of rich internet media, including important data such as social networking service posts and contacts now retained on smartphone 'apps'.

18.5.1 Service provider logs

Although not technically part of mobile device forensics, the call detail records (and occasionally, text messages) from wireless carriers often serve as "back up" evidence obtained after the mobile phone has been seized. These are useful when the call history and/or text messages have been deleted from the phone, or when location-based services are not turned on. Call detail records and cell site (tower) dumps can show the phone owner's location, and whether they were stationary or moving (i.e., whether the phone's signal bounced off the same side of a single tower, or different sides of multiple towers along a particular path of travel). Carrier data and device data together can be used to corroborate information from other sources, for instance, video surveillance footage or eyewitness accounts; or to determine the general location where a non-geo-tagged image or video was taken.

The European Union requires its member countries to retain certain telecommunications data for use in investigations. This includes data on calls made and retrieved. The location of a mobile phone can be determined and this geographical data must also be retained. In the United States, however, no such requirement exists, and no standards govern how long carriers should retain data or even what they must retain. For example, text messages may be retained only for a week or two, while call logs may be retained anywhere from a few weeks to several months. To reduce the risk of evidence being lost, law enforcement agents must submit a preservation letter to the carrier, which they then must back up with a search warrant.

18.5.2 Subscriber identification module

A subscriber identity module (SIM) is a smart card inside of a GSM cellular phone that encrypts voice and data transmissions and stores data about the specific user so that the user can be identified and authenticated to the network supplying the phone service. The SIM also stores data such as personal phone settings specific to the user and phone numbers. If the phone not uses SIM cards then the identity information is stored in the phone hardware itself.This identification information can be used to trace a victim using service provider logs.

18.5.3 Mobile Logs

Mobile phones many a times are capable to maintain logs of calls that were made, missed and received. This information can be crucial forensically. Other logs that are also maintained mostly in the background are GPS information, connection information, etc. Using these we can track the locations of mobile phones quite easily.

18.5.4 Phone books/contact lists

Phonebook names and numbers often give investigative leads to potential witnesses and victims. Phone book can have typical information such as e-mail addresses, home addresses, phone numbers, profile photographs, and even alternative phone numbers.

18.5.5 Text messages

Text messages can have bits of evidence as well as date and time stamps, which can be very valuable to investigators. Often deleted messages can be recovered along with time stamps and can be used into establishing leads in an investigation.

18.5.6 Application files

Nowadays smart phones etc. have an operating system and the applications installed on these operating systems maintain lots of files and data logs which can be vita sometimes during forensic investigations.

Other forensically important data sources in a mobile devices can be Calendars and event's organizers, E-mail, Instant messages, Photos, Audio recordings etc.

18.6 MOBILE FORENSIC PROCESS

a) Seizure
b) Acquisition
c) Analysis

VIDEO LECTURE

18.6.1 Seizure

Seizing mobile devices is covered by the same legal considerations as other digital media. Mobiles will often be recovered switched on. As the aim of seizure is to preserve evidence, the device will often be transported in the same state to avoid a shutdown, which would change files. In addition, the investigator or first responder would risk user lock activation.

However, leaving the phone on carries another risk the device can still make a network/cellular connection. This may bring in new data, overwriting evidence. To prevent a connection, mobile devices will often be transported and examined from within a *Faraday cage* (or bag). Even so, there are two disadvantages to this method. First, it renders the device unusable, as its touch screen or keypad cannot be used. Second, a device's search for a network connection will drain its battery more quickly. While devices and their batteries can often be recharged, again, the investigator risks that the phone's user lock will have activated. Therefore, network isolation is advisable either through placing the device in Airplane Mode, or cloning its SIM card (a technique which can also be useful when the device is missing its SIM card entirely).At all costs, you must keep new data from contaminating the mobile device after it has been seized, for a couple of reasons.

Mobile devices can be isolated in many ways; following ways can be used to isolate a mobile on seizure:

a. **Isolating its wireless features:** By using a Faraday bag or a jamming device mobile phones can be isolated to network till the battery drains completely. Devices increase their strength to search a network; this drains the battery very fast
b. **Switch off the device:** This method is fine however, on switching on the phone lock or sim lock can be activated which can lead the phone unusable. Unlocking can be possible but is quite tricky.
c. **Airplane mode:** Airplane mode is a setting available on many mobile phones and other electronic devices that, when activated, suspends many of the device's signal transmitting functions, thereby disabling the device's capacity to place or receive calls or use text messaging – while still permitting use of other functions that do not require signal transmission (e.g., games, built-in camera, MP3 player). When the "airplane mode" is activated, it will disable all cellular services (GSM, UMTS, LTE) as well as other signal-transmitting technologies such as Wi-Fi and Bluetooth. Wi-Fi and Bluetooth can be enabled separately even while the device is in airplane mode.

18.6.2 Acquisition

The second step in the forensic process is acquisition, in this case usually referring to retrieval of material from a device (as compared to the bit-copy imaging used in computer forensics). Due to the proprietary nature of mobiles, it is often not possible to acquire data with it powered down; most mobile device acquisition is performed live. With more advanced smartphones using advanced memory management, connecting it to a recharger and putting it into a faraday cage may not be good practice. The mobile device would recognize the network disconnection and therefore it would change its status information that can trigger the memory manager to write data. Most acquisition tools for mobile devices are commercial in nature and consist of a hardware and software component, often automated.

Acquiring data from mobile phones can be very tricky and need slot of training and expertise. The acquisition can vary from mobile device to mobile device. Devices, such as cameras, are treated as storage devices in much the same way as USB drives. Mobile phones, require specific forensic software tools to extract data in a forensic way. Basic guidelines while handling digital forensic data is to be careful and see that the data on the original media is not altered in any way either by chance or intentionally. Secondly, we need to document every aspect of the investigation. Most importantly, we need to keep things centralized with proper responsibility attached to all investigators and companies involved.

Fundamentally we are looking into three components in a mobile device they are Read only Memory (ROM), Random Access Memory (RAM) and Data Storage. These components and their forensics can be very similar to that of windows or operating system forensics as discussed in Block II.

Acquiring data from mobile phones can be very tricky and need slot of training and expertise. The acquisition can vary from mobile device to mobile device. Devices, such as cameras, are

treated as storage devices in much the same way as USB drives. Mobile phones, require specific forensic software tools to extract data in a forensic way. Basic guidelines while handling digital forensic data is to be careful and see that the data on the original media is not altered in any way either by chance or intentionally. Secondly, we need to document every aspect of the investigation. Most importantly, we need to keep things centralized with proper responsibility attached to all investigators and companies involved.

Fundamentally we are looking into three components in a mobile device they are Read only Memory (ROM), Random Access Memory (RAM) and Data Storage. These components and their forensics can be very similar to that of windows or operating system forensics as discussed in Unit II.

Acquisition involves following things to be done:

a) Type of Cellular Network, Code Division Multiple Access (CDMA), Global System for Mobile Communication (GSM), Integrated Digital Enhanced Network (iDEN) (A proprietary system, developed by Motorola, that uses advanced SIM cards (USIMs) and is expected to replace both CDMA and GSM).
b) Manufacturer Information of the mobile phone can be identified by Logos, Serial numbers, manufacturing codes (like IMEI: International Mobile Equipment Identifier) etc. It is advisable to cross verify the facts through Internet from online databases of the manufacturer or contact the manufacturers.
c) Phone characteristics of the device can be found from the manufacturer advertisements blogs etc. The characteristics can also guide us find areas for initial search for evidence. Some of these characteristics can be Operating system, Wireless access methods (Bluetooth, WiFi, or infrared),Camera, manufacturer applications, internet access methods, messages etc.

18.6.3 Examination and Analysis

Mobile phone forensics analysis involves the technical examination of mobile phones and the retrieval of data from these devices. Data for analysis can be obtained from SIM cards, memory cards and from the phone handset itself. Forensic analysis of mobile phones can be carried out on various forms of data, including textual (SMS Messages),Graphic (Images), Audio Visual (Videos) and Audio (Sound recordings). Rapid advancements in mobile phone technology and the introduction of smart phones to the market by companies such as Apple and Blackberry providing large storage capacities has meant that increasingly, larger amounts of personal information is now being stored on these devices. Individuals are now becoming increasing reliant on their mobile phones as part of their daily lives. The variety of applications and facilities these devices provide including Internet, Wi-Fi, email, document viewing and editing software along with the more common mobile phone features of phonebook, call history, text messaging, voice mail, built in camera and audio facilities have seen it overlap with computer technology. The existing generation of mobile phones is sophisticated and increasingly difficult to examine however they can ultimately provide valuable evidence in prosecuting individuals. Quite often the information obtained from a phone, after intensive analysis techniques proves

to be adequate for a conviction of a criminal by detectives involved with the case. Internal memory and external memory as well as the call and text records can all be analyzed to gain an insight into the activities of the mobiles owner as well as who they have been speaking or exchanging messages with. The area is ever expanding and allows for cutting edge technology to be used to keep up with the evergrowing array of mobile phones on the market today and the ever-increasing feature list of these phones. Mobile forensic analysis will continue to be a specialised field while technology progresses rapidly with the sheer number of phones to be examined posing a challenge for the police.

18.7 FORENSIC ACQUISITION TOOLS

There are two categories of forensics acquisition tools. They are:

a) Hardware acquisition tools.
b) Software acquisition tools.

18.7.1 Hardware acquisition tools

We will require certain hardware to carry out acquisition. Some of the important ones are:

a. Faraday bag: A Faraday bag keeps a mobile device from communicating with an external wireless device, by intercepting radio waves and effectively acting as a large, external antenna that redirects the radio energy away from the device. Faraday bags work to keep data from reaching the mobile device and keep the mobile device from transmitting any data outward. A Faraday bag can be as small as the device you're isolating to as large as a tent when you need to do field work and need to isolate the device and your acquisition equipment at the same time. In the mobile forensic environment, isolating the device is of prime importance when you arrive on-scene. The last thing you need is the device synchronizing on its own by way of a wireless link and changing all kinds of data.

b. SIM card reader: Found in any computer supply store, a card reader is used to read SIM and USIM cards without having to use the handset. Some card readers are built into the computer platform, and other card readers use a USB interface.

c. Cable connections: With the multitude of mobile devices now on the market, having just one mobile device connector seriously hampers your ability to do an investigation. Different mobile device manufacturers have not only different data cable connections but also different power connection interfaces. At the top of your list should reside the standard USB cable followed by the USB cable with a mini-USB connection.

18.7.2 Software acquisition tools

Certain software tools which are quite helpful while acquisition are:

a. www.MobileForensicsCentral.com: This web site provides access to a comprehensive database of phones supported by various software suppliers. A user of the web site can enter a model of a phone and the site will return a detailed report of which software and cables support it, as well what information can be retrieved from the device with the

software. The goal of the site is to enable users to more efficiently find the right tool for the device they are confronted with.

b. BITPIM[1]: Allows you to view and manipulate data on LG vx4400/vx6000 and many SANYO sprint cell phones. This includes the phonebook, calendar, wallpapers, ringtones (functionality varies by phone) and the filesystem for most QUALCOMM CDMA chipset based phones.
c. CELLDEK[2]: The revolutionary celldek has been developed in cooperation with the UK's forensic science service. The portable celldek acquires data from over 200 of the most popular cell phones and PDA's. Built to perform in the field (not just in the lab), investigators can immediately gain access to vital information, saving days of waiting for a report from a crime lab.
d. Cell Seizure[3]: Cell seizure allows you to acquire, analyse, and report on cell phone data for certain models of GsmSim Cards, Nokia, Samsung, Motorola, Sony-Ericsson, Lg, And Siemens cell phones. It can also acquire data from CDMA/TDMA phones. Designed for computer forensic examiners, cell seizure offers complete forensic examinations that can be presented in court with md5 & sha1 hash verification, write protection, html reporting, and full data dumps on some models. Version 3.0 adds support for LG, updates model support for other manufacturers, and updates sim card support.
e. Mobilyze[4]: Mobilyze is a mobile data triage tool, designed to give users immediate access to data from iOS and Android devices. Specifically designed with ease of use in mind, Mobilyze was built to respond to the mounting backlogs of evidentiary mobile devices in law enforcement agencies, both domestically and overseas. The Mobilyze application runs on either Mac or Windows and can be effectively deployed in the field or within a forensics lab. Once Mobilyze has been installed, simply plug the smartphone or tablet into a USB port, and Mobilyze will begin collecting all relevant user data. This data is then available for viewing, searching, and filtering within minutes. Through its incredibly simple and intuitive user experience, Mobilyze allows users of all technical abilities to quickly ascertain whether a device contains relevant forensic evidence, whether immediate action needs to be taken, and/or whether the device needs to be sent to a forensics lab for a comprehensive analysis. Once relevant data is discovered, Mobilyze provides one-click reporting in a clean and easily readable format. If further analysis is required, users can seamlessly import Mobilyze data into BlackLight for a more comprehensive forensic analysis.
f. Oxygen Phone Manager II (Forensic Version)[5]: A special software for police departments, law enforcement units and all government services that wish to use the power of Oxygen Phone Manager IIfor investigation purposes. Forensic edition secures phone data to remain unchanged during extraction and exporting.

---

1 http://bitpim.sourceforge.net/

2 http://www.logicubeforensics.com/products/hd_duplication/celldek.asp

3 http://www.download.com/Paraben-s-Cell-Seizure/3000-2092_4-10373543.html

4 http://www.teeltech.com/

5 http://www.opm-2.com/forensic/

g. Oxygen Phone Manager II[6]: Oxygen phone manager ii offers management for phonebook, call register, calendar, todo lists, SMS and MMS messages, logos, tones, GPRS and WAP settings, profiles, phone dictionary, FM stations, Java games and applications.
h. Paraben's SIM Card Seizure[7]: Paraben's SIM card seizure takes the SIM card acquisition and analysis components from paraben's cell seizure and puts it into a specialized SIM card forensic acquisition and analysis tool. SIM card seizure includes the software as well as a forensic SIM card reader. If you already have cell seizure & the cell seizure toolbox, there's no need for you to get SIM card seizure as well because they contain the components to perform a forensic SIM card acquisition and analysis. This tool is for the investigator who only wants to acquire SIM cards and does not want to perform forensic exams of all cell phone data.
i. Paraben's PDASeizure[8]: Paraben's PDA seizure is a commercially available forensic software toolkit that allows forensic examiners to acquire and examine information on PDA s for both the pocket pc (PPC) and palm OS platforms 4. Paraben's product currently supports palm os up to version 5, pocket pc 2000-2003 (up to Windows CE 4.2), activesync 3.7, and hotsync. PDA seizure's features include the ability to acquire a forensic image of palm OS, pocket PC, and Blackberry devices, to perform examiner-defined searches on data contained within acquired files, generate hash values of individual files and to generate a report of the findings. PDA seizure also provides book-marking capabilities to organize information, along with a graphics library that automatically assembles found images under a single facility, based on the graphics file extension of the acquired files.
j. The forensicsim toolkit[9]: The forensicsim toolkit gives today's law enforcement agencies the capability to safely and confidently recover digital evidence from GSM SIM and 3G USIM devices. Acquisition, analysis and reporting form the three key stages of the forensically sound process that will save critical time and provide a cost effective solution to SIM card examinations. As an increasing number of mobile devices use high-level file systems, similar to the file systems of computers, methods and tools can be taken over from hard disk forensics or only need slight changes.

Different software tools can extract the data from the memory image. One could use specialized and automated forensic software products or generic file viewers such as any hex editor to search for characteristics of file headers. The advantage of the hex editor is the deeper insight into the memory management, but working with a hex editor means a lot of handwork and file system as well as file header knowledge. In contrast, specialized forensic software simplifies the search and extracts the data but may not find everything. Since there is no tool that extracts all possible information, it is advisable to use two or more tools for examination.

---

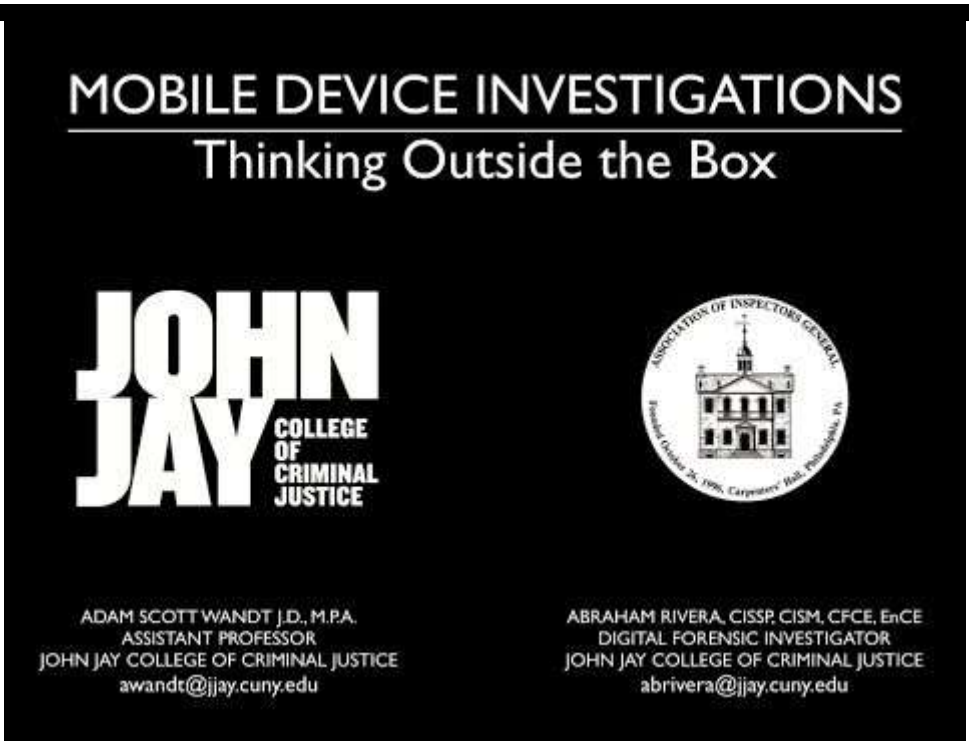
6 http://www.opm-2.com/OPM2/

7 http://www.paraben-forensics.com/catalog/product_info.php?cPath=25&products_id=289

8 http://www.paraben-forensics.com/handheld_forensics.htm

9 http://www.radio-tactics.com/forensic_sim.htm

VIDEO LECTURE



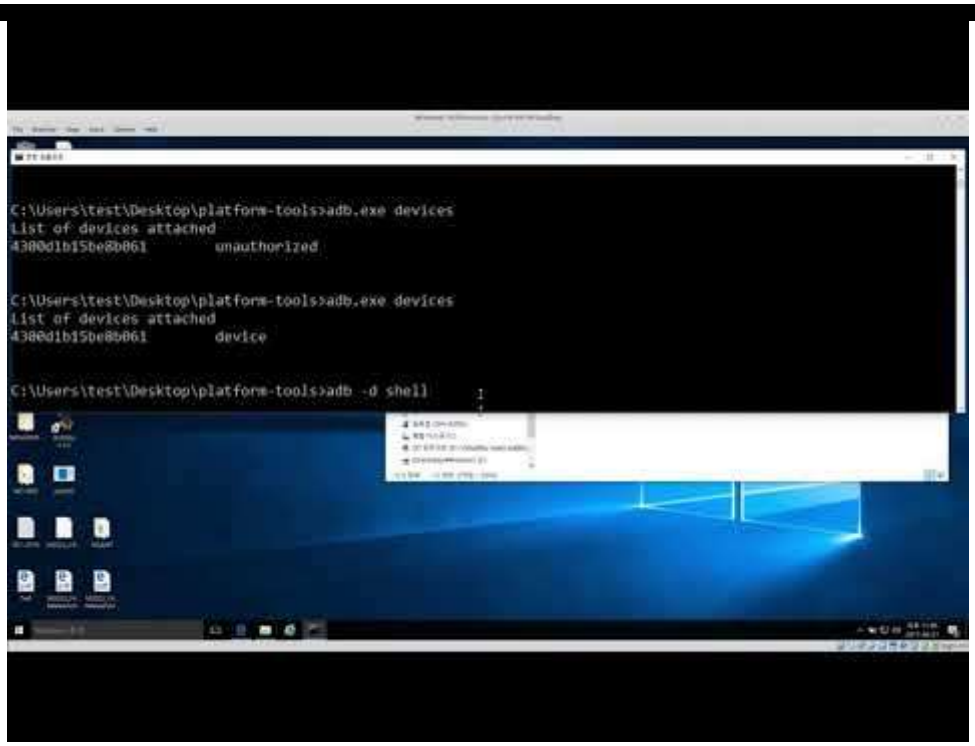
This lecture is adopted from https://youtu.be/1LdZWTiWSBI available under Creative Commons Attribution license (reuse allowed)

18.8 SUMMARY

1. Forensic study of mobile devices is a relatively new field.
2. There is growing need for mobile forensics due to several reasons like personal information in mobile devices; criminals as well as law agencies use mobile devices, online transactions with mobile devices.
3. Original equipment manufacturers frequently change mobile phone that's why forensic examiners must use a different forensic process compared to computer forensics.
4. Mobile communication means can be categorized in 802.11or WiFi, Bluetooth, Infrared(IrDA)
5. Mobile phone forensics involves recovering and analyzing SMS and MMS messaging, call-logs, contact lists and phone IMEI/ESN information, web browsing, Wireless network settings, geo-location information, e-mail and other forms of rich internet media such as social networking, Service provider logs, application files etc.
6. Mobile Forensic process involves seizure, acquisition, analysis. The seizure and acquisition are relatively different than that in windows system. Analysis is more like any other digital forensic analysis.

7. Forensic analysis of mobile phones can be carried out on various forms of data, including textual (SMS Messages),Graphic (Images), Audio Visual (Videos) and Audio (Sound recordings).
8. Forensic acquisition tools can be categorized in Hardware acquisition tools and Software acquisition tools. For example faraday's bag is a hardware acquisition tool whereas CellDek and CellSeizure are software tools for acquisition.

VIDEO LECTURE



This lecture is adopted from https://www.youtube.com/watch?v=K_RE3wEZwPc available under Creative Commons Attribution license (reuse allowed)

18.9 CHECK YOUR PROGRESS

1. Fill in the blanks.

a) _____ is a local area wireless computer networking technology that allows electronic devices to connect to the network.
b) Bluetooth 4.0 is also referred to as _____.
c) By using _____ mobile phones can be isolated to network till the battery drains completely.
d) _____ is usually referring to retrieval of material from a device for analysis and keeps its integrity intact so that they can be accepted as evidence in the court of law.

e) Various types of cellular network are: _____, _____, _____.

f) _____ work to keep data from reaching the mobile device and keep the mobile device from transmitting any data outward.

2. State True or False.

a) Bluetooth is defined as being a long-range radio technology (or wireless technology) aimed at simplifying communications among Internet devices and between devices and the Internet.
b) Network isolation is advisable either through placing the device in Airplane Mode, or cloning its SIM card.
c) Devices, such as cameras, are not treated as storage devices in much the same way as USB drives.
d) Celldek has been developed in cooperation with the UK's forensic science service.
e) Call detail records and cell site (tower) dumps cannot show the phone owner's location

18.10 ANSWERS TO CHECK YOUR PROGRESS

1. Fill in the blanks.

a) Wi-Fi (or WiFi).
b) Bluetooth Low Energy.
c) Faraday bag or a jamming device.
d) Acquisition.
e) Code Division Multiple Access (CDMA), Global System for Mobile Communication (GSM), Integrated Digital Enhanced Network (iDEN).
f) Faraday bags.

2. State True or False.

a) False.
b) True.
c) False.
d) True.
e) False.

18.11 FURTHER READINGS

1. Andrew Hoog, Android Forensics: Investigation, Analysis, and Mobile Security for Google Android, syngress, Elsevier, 2011
2. Linda Volonino, Reynaldo Anzaldua; Computer Forensics For Dummies, Wiley Publishing, Inc.
3. I.I. Androulidakis, Mobile Phone Security and Forensics: A Practical Approach, Springer Science & Business Media, 2012.
4. Li, Chang-Tsun, Crime Prevention Technologies and Applications for Advancing Criminal Investigation, IGI Global, 2012

5. Curran, K., Robinson, A., Peacocke, S., Cassidy, S. (2010) Mobile Phone Forensic Analysis, International Journal of Digital Crime and Forensics, Vol. 2, No. 2, pp:, April-May 2010, ISSN: 1941-6210, IGI Pub.
6. Linda Volonino, Reynaldo Anzaldua; Computer Forensics for Dummies, Wiley Publishing, Inc.
7. Mobilyze, http://www.teeltech.com
8. Oxygen Phone Manager II (Forensic Version), http://www.opm-2.com/forensic/
9. Oxygen Phone Manager II, http://www.opm-2.com/OPM2/
10. Paraben's PDA Seizure, http://www.paraben-forensics.com/handheld_forensics.html
11. Paraben's SIM Card Seizure, http://www.paraben-forensics.com/catalog/product_info.php?cPath=25&products_id=289
12. The forensicsim toolkit, http://www.radio-tactics.com/forensic_sim.htm.
13. BITPIM, http://bitpim.sourceforge.net/
14. Cell Seizure, http://www.download.com/Paraben-s-Cell-Seizure/3000-2092_4-10373543.html
15. CELLDEK, http://www.logicubeforensics.com/products/hd_duplication/celldek.asp

18.12 MODEL QUESTIONS

a) What are the major sources of evidences in a mobile device? Explain.
b) Describe the mobile forensic process.
c) What are the different mobile device logs important during mobile acquisition?
d) How text messages be analysed in forensics?
e) Explain various types of mobile communications and relate this to forensic investigation.
f) What are the various ways in which mobile devices can be isolated?
g) Write the steps involved in mobile acquisition.

References, Article Source & Contributors

[1] Mobile device forensics - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Mobile_device_forensics
[2] What is Bluetooth? Webopedia, www.webopedia.com, Reproduced with permission. Copyright 1999-2015 QuinStreet, Inc. All rights reserved.
[3] What is IrDA? A Webopedia Definition, www.webopedia.com, Reproduced with permission. Copyright 1999-2015 QuinStreet, Inc. All rights reserved.
[4] What is subscriber identity module? A Webopedia Definition, www.webopedia.com, Reproduced with permission. Copyright 1999-2015 QuinStreet, Inc. All rights reserved.
[5] MOBILE/PDA FORENSIC TOOLS – Securitytools, securitytools.wikidot.com/mobile-pda-forensic-tools

Recommended Youtube Video

Webinar: An Introduction to Mobile Forensics: https://youtu.be/5e5KdbY-xzE

EXPERT PANEL

Dr. Jeetendra Pande, Associate Professor- Computer Science, School of Computer Science & IT, Uttarakhand Open University, Haldwani

Dr. Ajay Prasad, Sr. Associate Professor, University of Petroleum and Energy Studies, Dehradun

Dr. Akashdeep Bharadwaj, Professor, University of Petroleum and Energy Studies, Dehradun

Mr. Sridhar Chandramohan Iyer, Assistant Professor- Universal College of Engineering, Kaman, Vasai, University of Mumbai

Mr. Rishikesh Ojha, Digital Forensics and eDiscovery Expert

Ms. Priyanka Tewari, IT Consultant

Mr. Ketan Joglekar, Assistant Professor, GJ College, Maharastra

Dr. Ashutosh Kumar Bhatt, Associate Professor, Uttarakhand Open University, Haldwani

Dr. Sangram Panigrahi, Assistant Professor, Siksha 'O' Anusandhan, Bhubaneswar

This MOOC has been prepared with the support of