Parul® University

Cyber Security and Forensics - I
05201296

Prof. Dipak L. Agrawal, Assistant Professor
Faculty of IT & Computer Science

Parul®
University

DIGITAL LEARNING CONTENT

CHAPTER-7

Forensics of Hand-Held Devices

Topics

- Introduction, Hand-held devices and digital forensics -mobile phone, Personal Digital Assistant (PDA), printer, scanner, smart phone, iPhone, Challenges in forensics of the Digital images/still camera, Forensics of the BlackBerry wireless device,
- Toolkits for hand-held device forensics - EnCase, device seizure and PDA seizure, Palm DD, Cell seizure, MOBILedit, Forensic SIM, Organizational guidelines on cell phone forensics – hand-held forensics as the specialty domain in crime context.

Parul®
University

DIGITAL LEARNING CONTENT

Introduction, Hand-held devices and digital forensics -mobile

- Computer forensics is about investigating digital evidence related to criminal or suspicious behavior where computers or computer-related equipment may or may not be the targets. This process of "identifying, preserving, analyzing, and presenting" digital evidence which is legally acceptable is not much different from traditional forensic science.
- Digital evidence includes computer-generated records such as outputs of computer programs and computer-stored records such as email messages. It is important to criminal investigations because it can be used as proof of crime.

Parul®
University

DIGITAL LEARNING CONTENT

Introduction, Hand-held devices and digital forensics -mobile

- Computer forensics is about investigating digital evidence related to criminal or suspicious behavior where computers or computer-related equipment may or may not be the targets. This process of "identifying, preserving, analyzing, and presenting" digital evidence which is legally acceptable is not much different from traditional forensic science.
- Digital evidence includes computer-generated records such as outputs of computer programs and computer-stored records such as email messages. It is important to criminal investigations because it can be used as proof of crime.

Importance of Mobile Phones and PDAs

- Falling prices of handheld devices and their resultant mass adoption make it more likely for forensic investigators to deal with mobile phones and PDAs today than 10 years ago.
- As more people use handheld devices for applications such as e-mail, SMS (Short Message Service), MMS (Multimedia Messaging Service) and online transactions, such devices provide a good source of evidence for forensic investigators to prove or disprove the commitment of crimes or location of suspects/victims. Evidence stored on a handheld device, such as its unique IMEI (International Mobile Equipment Identification) number, recent incoming and outgoing numbers, text messages, stored calendar events, as well as evidence stored beyond the device itself, such as the subscriber database and call data records maintained by network providers, can be useful to investigators.

FORENSIC TOOLKITS

- Forensic examiners have to conduct well-defined procedures when dealing with digital handheld devices and various removable media's physical or logical acquisition is used by forensic tools to obtain information.
- Physical acquisition easily imports images of physical devices into another tool for reporting and allows examining of unused file system space; whereas logical acquisition gives a natural and understandable structure of acquired information.

FORENSIC TOOLKITS FOR PDAs

- The range of tools available for PDA's is limited and only a couple of tools assist the forensic examiner's with a full range of examination, organization, acquisition, reporting and documenting functions whereas the remaining tools focus on a single function (Valli, 2005).
- The tools available for the forensic examiner to investigate a crime when a PDA is involved are PDA Seizure, EnCase, Palm dd (pdd), Pilot-lint, and other miscellaneous tools. All these tools are not applicable for each and every operating system for PDAs; they are narrowed to Pocket PC and Palm OS.

ENCASE

- This is the most popular forensic software toolkit. Some of the various features supported by this toolkit are analytical tools, suspect media acquisition, data capture, documentation and search features.
- EnCase doesn’t support Pocket PC devices, although it is a very familiar tool for PCs and Palm OS devices.
- A complete physical bit-stream image of Palm OS devices is created and this bit-stream image is checked with the already obtained existing CRC (Cyclical Redundancy Checksum) values.
- Each case is bookmarked and is saved in case files. Any data can be bookmarked for future reference. The forensic examiners can utilize the reporting feature of EnCase and can then search for information of one file, two files, multiple files, all the files in the case etc. The examiner can also obtain a report of the entire case file that is created.

PDA SEIZURE

- PDA seizure is another forensic software toolkit to obtain and examine the data on PDAs. This tool can only produce a forensic image of Palm OS and Pocket PC devices.
- PDA seizure searches acquired files for data and generates a report of the findings. Similar to EnCase, PDA Seizure also includes the capability to bookmark and organize information.
- The graphics library provides the functionality of automatic collection of images according to their file extensions.
- Data can only be acquired from the Palm OS device when in console mode. The logical data can be obtained once the image or screen shot of the memory of the Palm device is obtained.

PALM DD (PDD)

- The Palm dd (pdd) tool runs only on Windows based systems and is mainly used by forensic examiners for physical acquisition. Palm dd has no GUI support and everything has to be done from the command prompt of Windows. The tool also lacks support for bookmarking, search capability, and report generation.
- A complete copy of the device's memory is acquired during the acquisition stage, and the data retrieved by pdd includes all user applications and databases.
- Two files are generated from the information obtained. One file is a text file which has all the information pertaining to the Palm device in investigation (Grant, 2002). The other file is created from the output sent by the user. Both these files contain an image copy of the Palm device. The forensic examiner can then inspect these two files to find any evidence.

FORENSIC TOOLKITS FOR CELL PHONES

- Cell phones are not limited to just phone calls but they provide lots of functions such as accessing the Internet, sending and receiving emails, sharing photos on the web, access to a calendar similar to that available on windows for organizing information, and also as a small storage device for storing important data and files. Many tools are available for cell phones for performing forensic analysis, but these tools are not always compatible with all the manufacturers and different models of cell phones. These tools can obtain data from these phones in a variety of ways such as IrDA (Infrared Data Association), through a USB connection, by Bluetooth, or by a serial cable connected to a computer. Tools can acquire a wide range of information that includes PIM (Personal Information Management) data, SMS/EMS/MMS messages, logs of phone calls; email, IM content; URLs and content of visited Web sites; audio, video, and image content; SIM content; and uninterrupted image data.

CELL SEIZURE

- Cell Seizure is a forensic software toolkit for acquiring, searching, examining, and reporting (Ayers, 2004) data associated with cell phones operating over CDMA (Code Division Multiple Access), TDMA (Time Division Multiple Access), and GSM (Global System for Mobile communication) networks.
- The following data can be obtained on most cell phones with the tool: SMS History: Inbox/Outbox

Phonebook: SIM-Card, Own Numbers, Speed Dialing, Fixed Dialing

Call Logs: Dialed Numbers, Received Calls, Missed Calls

Calendar: Reminder, Meeting, Memo

Graphics: Wallpaper, Picture Camera Images, EMS Template Images

WAP: WAP Settings, WAP Bookmarks

SIM: GSM Specific data

CELL SEIZURE

- Cell Seizure is a forensic software toolkit for acquiring, searching, examining, and reporting (Ayers, 2004) data associated with cell phones operating over CDMA (Code Division Multiple Access), TDMA (Time Division Multiple Access), and GSM (Global System for Mobile communication) networks.
- The following data can be obtained on most cell phones with the tool: SMS History: Inbox/Outbox

Phonebook: SIM-Card, Own Numbers, Speed Dialing, Fixed Dialing

Call Logs: Dialed Numbers, Received Calls, Missed Calls

Calendar: Reminder, Meeting, Memo

Graphics: Wallpaper, Picture Camera Images, EMS Template Images

WAP: WAP Settings, WAP Bookmarks

SIM: GSM Specific data

CELL SEIZURE

- Cell Seizure is a forensic software toolkit for acquiring, searching, examining, and reporting (Ayers, 2004) data associated with cell phones operating over CDMA (Code Division Multiple Access), TDMA (Time Division Multiple Access), and GSM (Global System for Mobile communication) networks.
- The following data can be obtained on most cell phones with the tool: SMS History: Inbox/Outbox

Phonebook: SIM-Card, Own Numbers, Speed Dialing, Fixed Dialing

Call Logs: Dialed Numbers, Received Calls, Missed Calls

Calendar: Reminder, Meeting, Memo

Graphics: Wallpaper, Picture Camera Images, EMS Template Images

WAP: WAP Settings, WAP Bookmarks

SIM: GSM Specific data

MOBILEDIT!

- MOBILedit! is a forensic application that allows examiners to acquire logically, search, examine and report data from CDMA (Code Division Multiple Access), PCS (Personal Communications Services), and GSM (Global System for Mobile communication) cell phones.
- The tool connects to cell phone devices through an Infrared (IR) port, a Bluetooth link, or a cable interface. Once the connection is established, the phone model is identified by its manufacturer, model number, serial number and a corresponding picture of the phone.

DIGITAL LEARNING CONTENT

Parul® University

www.paruluniversity.ac.in