Unit VII Forensics of Hand-Held Devices

Content

- Introduction to Cell-Phone Working Characteristics
- Hand-Held Devices and Digital Forensics
- Toolkits for Hand-Held Device Forensics.

INTRODUCTION

- "Computer forensics" is the application of forensic science techniques to the systematic discovery, collection and analysis of digital evidence.
- It is the preservation, identification, extraction, documentation and interpretation of computer media for evidentiary and/or root cause analysis using well-defined methodologies and procedures.
- The methodology used is acquiring the evidence without altering or damaging (safe custody of the evidence) the original digital evidence, authenticating that the recovered evidence is the same as the original seized and analyzing the data without modifying it (chain of custody concept).
- They are relevant here too because we will be introducing some more legal aspects of forensics.

Fig: Hand-held devices. (a) iPhone; (b) iPod; (c) palm pilot; (d) digital diary; (e) Smartphones; 2 GB MP2 player; (g) portable printer; (h) handycam and (i) PDA.

INTRODUCTION

- The terms “device forensics” and “hand-held forensics” are used interchangeably.
- According to the Internet and Mobile Association of India, Internet usage in the country has risen by 20% in the last year alone with people progressively spending more time online.
- Indians are increasingly accessing and transmitting sensitive information from their workstations/PCs, from home and while in transit through their laptops, netbooks or Smartphones.

Understanding Cell Phone Working Characteristics

- In modern times, cellular mobile phones have become an integral part of communication around the world.
- Forensics and digital analysis of mobile phones, therefore, is an area of interest, as crimes involving mobile devices are becoming increasingly common in the community.
- While mobile phones outsell personal computers (PCs) three to one, mobile phone forensics still lags behind computer forensics.

Understanding Cell Phone Working Characteristics

- Understanding the Types of Cellular Networks
- There are different types of digital cellular networks. these networks exist due to the distinct and incompatible sets of network protocol standards. the two most dominant types of digital cellular networks are:
- 1. Code Division Multiple Access (CDMA).
- 2. Global System for Mobile Communications (GSM) network.
- There are other common cellular networks; they include Time Division Multiple Access (TDMA) and Integrated Digital Enhanced Network (iDEN).
- iDEN networks use a proprietary protocol designed by Motorola, while the others follow standardized open protocols.
- NTT DoCoMo
- Digital Advanced Mobile Phone Service (D-AMPS) is the digital version of the original analog standard for cellular telephone phone service.
- Now “Do Communication over the Mobile Network” (DoCoMo) is also available. NTT DoCoMo is Japan’s largest wireless network carrier.

Box 8.1 CDMA, TDMA, GSM, AMPS and DoCoMo and other standards

- AMPS: Advanced mobile phone service is a standard for analog signal cellular telephone service in the United States and some other countries.
- It is based on the initial electromagnetic radiation spectrum allocation for cellular service by the Federal Communications Commission (FCC) in 1970.
- AMPS allocates frequency ranges within the 800 and 900 MHz spectrum to cellular telephone.
- D-AMPS is the 2G version of this technology. AMPS used cellular digital packet data (CDPD) to transfer data using unused bandwidth, at speeds up to 19.2 Kbps. Major carrier support for AMPS is likely to end in the US in 2008. Provider(s): Verizon, Alltel
- GSM: Global system for mobile is a digital mobile telephone system that is widely used in Europe and other parts of the world.
- GSM uses a variation of TDMA and is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA).
- GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot.
- It operates at either the 900 MHz or 1800 MHz frequency band. Provider(s): T-Mobile, Cingular

Box 8.1 CDMA, TDMA, GSM, AMPS and DoCoMo and other standards

- TDMA
- Time division multiple access is a technology used in digital cellular telephone communications and radio networks that divides each cellular channel into three time slots in order to increase the amount of data that can be carried.
- TDMA is used by D-AMPS, GSM, and PDC.
- The United States standard for TDMA for both the cellular (850 MHz) and PCS (1.9 GHz) spectrums. TDMA is also used for digital enhanced cordless telecommunications (DECT). Provider(s): US Cellular, Cingular.
- CDMA
- Code-division multiple access is a form of multiplexing, which allows numerous signals to occupy a single transmission channel, optimizing the use of available bandwidth.
- CDMA employs analog-to-digital conversion (ADC) in combination with spread spectrum technology.
- The technology is used in ultra-high-frequency (UHF) cellular telephone systems in the 800 MHz and 1.9 GHz bands. IS-95 uses CDMA. Provider(s): Verizon

Box 8.1 CDMA, TDMA, GSM, AMPS and DoCoMo and other standards

- NTT DoCoMo
- (NTT Mobile Communications Network, Inc., Japan) Founded in 1991, NTT DoCoMo is a spin-off of Japan's NTT (Nippon Telegraph and Telephone Corporation) which provides wireless services, including cellular, paging, satellite and maritime and in-flight telephone services.
- Established in 1992, DOCOMO launched its first digital cellular phone service the next year and the world's first mobile Internet-services platform in 1999. It helped to establish the W-CDMA standard for mobile communications and then kick off the first 3G service based on this standard in 2001. The company also introduced one of the earliest commercial LTE services in 2010.
- DoCoMo stands for “Do Communication Over the Mobile Network”. DoCoMo means "anywhere" in Japanese.
- Other standards
- Besides the major mobile standards, there are others as well used less frequently including NAMPS, iDEN/Nextel, NMT, TETRA/Dolphin, Iridium, and Globalstar.

Box 8.2 Mobile Handsets Challenges – Tracing Call Logs and Retrieving Information

- Mobile forensics is different from computer forensics and presents unique challenges to forensic examiners. One of the biggest forensic challenges is that data can be accessed, stored, and synchronized across multiple devices.
- As the data is volatile and can be quickly transformed or deleted remotely, more effort is required for the preservation of this data.
- Law enforcement and forensic examiners often struggle to obtain digital evidence from mobile devices. The following are some of the reasons:
- **Hardware differences**: The market is flooded with different models of mobile phones from different manufacturers. Forensic examiners may come across different types of mobile models, which differ in size, hardware, features, and operating system.
- Also, with a short product development cycle, new models emerge very frequently. As the mobile landscape is changing each passing day, it is critical for the examiner to adapt to all the challenges and remain updated on mobile device forensic techniques across various devices.
- **Mobile operating systems**: Unlike personal computers where Windows has dominated the market for years, mobile devices widely use more operating systems, including Apple's iOS, Google's Android, RIM's BlackBerry OS, Microsoft's Windows Mobile, HP's webOS, Nokia's Symbian OS, and many others.
- Even within these operating systems, there are several versions which make the task of forensic investigator even more difficult.

Box 8.2 Mobile Handsets Challenges – Tracing Call Logs and Retrieving Information

- **Mobile platform security features**: Modern mobile platforms contain built-in security features to protect user data and privacy. These features act as a hurdle during the forensic acquisition and examination.
- For example, modern mobile devices come with default encryption mechanisms from the hardware layer to the software layer. The examiner might need to break through these encryption mechanisms to extract data from the devices.
- **Lack of resources**: As mentioned earlier, with the growing number of mobile phones, the tools required by a forensic examiner would also increase. Forensic acquisition accessories, such as USB cables, batteries, and chargers for different mobile phones, have to be maintained in order to acquire those devices.
- **Anti-forensic techniques**: Anti-forensic techniques, such as data hiding, data obfuscation, data forgery, and secure wiping, make investigations on digital media more difficult.
- **Dynamic nature of evidence**: Digital evidence may be easily altered either intentionally or unintentionally. For example, browsing an application on the phone might alter the data stored by that application on the device.
- **Accidental reset**: Mobile phones provide features to reset everything. Resetting the device accidentally while examining may result in the loss of data.
- **Device alteration**: The possible ways to alter devices may range from moving application data, renaming files, and modifying the manufacturer's operating system. In this case, the expertise of the suspect should be taken into account.

Box 8.2 Mobile Handsets Challenges – Tracing Call Logs and Retrieving Information

- **Passcode recovery**: If the device is protected with a passcode, the forensic examiner needs to gain access to the device without damaging the data on the device. While there are techniques to bypass the screen lock, they may not work always on all the versions.
- **Communication shielding**: Mobile devices communicate over cellular networks, Wi-Fi networks, Bluetooth, and Infrared. As device communication might alter the device data, the possibility of further communication should be eliminated after seizing the device.
- **Lack of availability of tools**: There is a wide range of mobile devices. A single tool may not support all the devices or perform all the necessary functions, so a combination of tools needs to be used. Choosing the right tool for a particular phone might be difficult.
- **Malicious programs**: The device might contain malicious software or malware, such as a virus or a Trojan. Such malicious programs may attempt to spread over other devices over either a wired interface or a wireless one.
- **Legal issues**: Mobile devices might be involved in crimes, which can cross geographical boundaries. In order to tackle these multijurisdictional issues, the forensic examiner should be aware of the nature of the crime and the regional laws.
- **Preventing data modification**: One of the fundamental rules in forensics is to make sure that data on the device is not modified. In other words, any attempt to extract data from the device should not alter the data present on that device. But this is practically not possible with mobiles because just switching on a device can change the data on that device. Even if a device appears to be in an off state, background processes may still run. For example, in most mobiles, the alarm clock still works even when the phone is switched off. A sudden transition from one state to another may result in the loss or modification of data.

Understanding Cell Phone Working Characteristics

- Cell Phones: Hardware and Software Features
- Different devices have different technical and physical features/characteristics (e.g., size, weight, processor speed and memory capacity).
- Devices may also use different types of expansion capabilities to provide additional functionality.
- Cell phone capabilities sometimes include those of other devices such as personal digital assistants (PDAs), global positioning systems (GPS) and cameras.
- Irrespective of a cell phone type, all devices support voice and text messaging, a set of basic personal information management (PIM) applications including phonebook and date book facilities, and a means to synchronize PIM data with a desktop computer.
- More advanced devices also provide the ability to perform multimedia messaging, connect to the Internet and surf the Web, exchange E-Mail or chat using instant messaging.

Understanding Cell Phone Working Characteristics

Category	Feature Phone	Smart Phone
Processor	Speed is Limited	Speed is superior to the featured phone.
Memory	Memory is Limited	Memory is superior to that of a featured phone.
Display	Small size colour display (12 bit-18 bit)	Large size colour display (approx 24 bit)
Card Slots	None	MiniSDXC
Camera	Still	Still and Video (HD)
Text Input	Numeric Keypad	Touch Screen, Built-in QWERTY keypad
Voice Input	None	Voice Recognition (Dialing and Control)
Positioning	None	GPS receiver
Wireless	IrDA, Bluetooth	Bluetooth, WiFi and NFC

Table 8.1 Hardware characteristics:

Hand-held Devices

Understanding Cell Phone Working Characteristics

Table 8.1 Software characteristics:

Hand-held Devices

Category	Feature Phone	Smart Phone
Operating System	Closed	Andriod, BlackBerry, Windows, iOS
Personal Information Management	Phonebook, Calender and Reminder List	Enhanced Phonebook, Calender and Reminder List
Applications	Games, notepad etc	Games, office suite, social media, music etc
Call	Voice	Voice and Video
Messaging	Text messaging	Full multimedia messaging
Email	Via text messaging	Via POP or IMAP server
Web	Via WAP gateway	Direct HTTP

Hand-Held Devices and Digital Forensics

- There is no dearth of hand-held devices in the modern world of today. The use of these devices is rampant given the modern lifestyles in our digital economy.
- "Device forensics" has many aspects such as
  - mobile phone forensics,
  - PDA forensics,
  - digital music forensics,
  - iPod forensics and
  - Digital image forensics
  - printer and scanner forensics.

Box 8.3 Hand-held Devices and Digital Forensics

- Acquisition is the process of cloning the device or generating its mirror image in order to collect the information from mobile device.
- Acquisition has an added advantage that it saves the loss of information due to battery depletion, damage etc.
- This begins with identification of mobile device, the type of operating system, device characteristics, the interface the device is using and device label.
- Examination process reveals the hidden or the obscured data of the digital evidence. It takes the copy of the evidence which is acquired from the mobile device.
- It also reduces the data by separating the relevant information from the irrelevant.
- Mobile phone manufacturers provide a set of features to identify the type of data while gathering the information.
- The features are like Personal Information Management (PIM), applications, messaging, e-mail and browsing.

Box 8.3 Hand-held Devices and Digital Forensics

- With the help of these features set potential evidence could be obtained which further may help in the investigation process like:
  - Date/time, language, and other settings
  - Phonebook/Contact information (Both phonebook and SIM)
  - Calendar/Scheduler information
  - Text messages
  - To-do list
  - Outgoing, incoming, and missed call logs
  - Electronic mail
  - Photos Audio and video recordings
  - Multi-media messages
  - Instant messaging
  - Web browsing activities
  - Electronic documents
  - Social media related data
  - Application related data
  - Location information Geo location data
  - Subscriber and equipment identifiers
  - Registry (In Windows mobiles)

Hand-Held Devices and Digital Forensics

- Mobile Phone Forensics
- Mobile phone or cell phone is the most familiar hand-held device because it is the most ubiquitous one. Nathan B. Stubble field invented and patented the first mobile telephone 100 years ago.
- As mentioned before, modern cell phones are highly mobile communications devices designed to perform a range of functions from that of a simple digital organizer to that of a low-end PC.
- Designed for mobility, they are compact in size, battery powered and lightweight, often use proprietary interfaces or OS and may have unique hardware characteristics for product differentiation.
- "Mobile phone forensics" is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods.

Box 8.4 Cell Phone – Smart Tips

- Uninstall Apps You Don't Need.
- Use Digital Wellbeing Features.
- Keep an eye on configuration and privacy settings.
- Install Apps From the Official Application Store.
- Install Apps From Other Sources, make sure they are reliable.
- Try not to store sensitive information on your phone
- Install Antivirus/Antispyware
- Record Screen Activity
- Use Developer Options
- Turn on Find My Device
- Update Frequently
- Put a pass code on your phone
- Turn off Internet/Bluetooth connectivity when not in use
- What online accounts are you automatically logged into? Make sue they are safe.

Hand-Held Devices and Digital Forensics

Hand-Held Devices and Digital Forensics

Name	Link	Platform	Description
Oxygen Forensic Suite	http://www.oxygen-forensic.com/en/download/freeware	Windows	It forensically analyzes mobile phones. The software does not change any data on the phone. Oxygen runs on any version of the Windows Operating system.
Iphone analyzer	http://www.ipbackupanalyzer.com/downloads/windows-exe-build/copy-of-windows-exe-build-032013-3	Windows	It is a utility designed to easily browse through the backup folder of an iPhone. Read configuration files, browse archives, lurk into databases and so on.
Whatsapp xtract	http://www.code.google.com/p/hotoloti/downloads/list	Windows	This tool helps to recover the WhatsApp database from the phone. It also helps to read the configuration of the WhatsApp. It is possible to decrypt the encrypted data using this software.
Skype Xtractor	http://www.sourceforge.net/projects/skypextractor/	Windows	This tool takes the folder where the audio files are stored as input, copies the file in a temp folder and adds a header and converts them to another format and saves them to the specified folder, thus creating a backup.
Sim Manager	http://www.sourceforge.net/projects/agsm/	Windows	It recovers phone numbers and short message service (SMS) messages from a range of mobile phones.
OSAF-TK	http://www.sourceforge.net/projects/osaftoolkit/	Windows	This tool helps in android malware analysis and forensics.

Hand-Held Devices and Digital Forensics

- Mobile Phone Forensics
- The “IMEI number” (International Mobile Equipment Identity) of a cell phone is a very important starting point for the First Information Report (FIR) procedure as the FIR would most probably require the IMEI number as the basis when a compliant about a lost/stolen mobile phone is to be registered with the police.
- This is because a cell phone can be traced with its IMEI number. Mobile device representation comes in various forms:
- 1. Cellular phones
  - CDMA: typically, handset only;
  - GSM: handset and SIM;
  - iDEN: handset and SIM.

Hand-Held Devices and Digital Forensics

- Mobile Phone Forensics
- 2. PDAs
  - Palm Pilots (Palm OS);
  - Pocket PC's (Windows CE, Windows Mobile);
  - BlackBerry's (RIM OS) that contain no radio (cellular) capability;
  - others (Linux, Newton).
  - Smartphones: They are the hybrid between 1 and 2 have radio capability

Table 8.3 Cell Phone Forensic Tools

- **General free tools**
- **AFLogical OSE** – Open source Android Forensics app and framework is an application in APK format that has got to be installed beforehand within the Android terminal. Once the method is completed it allows varied information to be extracted to the SD card (call log, contact list and list of applications installed, text messages and multimedia), which must subsequently be recovered either by connecting the cardboard to an external device or through the ADB.
- **Open Source Android Forensics** is a framework that's distributed via a virtual machine image that brings together various tools which permit the analysis of applications for mobile devices, including both a static and a dynamic analysis or maybe a forensic analysis.
- **Andriller** is a software utility for Windows Operating System with a collection of forensic tools for smartphones. It performs read-only, forensically sound, non-destructive acquisition from Android devices. It has other features, such as powerful Lockscreen cracking for Pattern, PIN code, or Password; custom decoders for apps data from Android (and some Apple iOS) databases for decoding communications.

Table 8.3 Cell Phone Forensic Tools

- **General free tools**
- **FTK Imager Lite** allows us to figure with memory dumps of mobile devices to analyse them and acquire evidence.
- **Now Secure Forensics** Community Edition is distributed as a reflection that brings together various tools to hold out a forensic analysis, and may perform differing types of evidence extraction or maybe file carving in its commercial version.
- **LIME-** is a Loadable Kernel Module (LKM) Linux memory extractor which allows for volatile memory acquisition from Linux and Linux-based devices, such as Android. This makes LiME unique as it is the first tool that allows for full memory captures on Android devices.

Table 8.3 Cell Phone Forensic Tools

- **Specific free Tools**
- **Android Data Extractor Lite (ADEL)** may be a tool developed in Python that permits a forensic flowchart to be obtained from the databases of the mobile device. to hold out the method , it's necessary for the mobile device to be rooted or have personalised recovery installed.
- **WhatsApp Xtract** allows WhatsApp conversations to be viewed on the pc during a simple and user-friendly way. As such, the various databases that store information like messages should be obtained beforehand.
- **Skype Xtractor** is an application, supported both on Windows and Linux that permits us to look at information of the Skype main.db file, which stores information about contacts, chats, calls, transferred files, deleted messages etc.

Tool	Function
Cell Seizure	Acquisition, Examination, Reporting[2]
GSM .XRY	Acquisition, Examination, Reporting[3]
Mobiledit! Forensic	Acquisition, Examination, Reporting[4]
TULP 2G	Acquisition, Reporting[5]
Forensic Card Reader	Acquisition, Reporting[6]
ForensicSIM	Acquisition, Examination, Reporting[7]
SIMCon	Acquisition, Examination, Reporting[8]
SIMIS	Acquisition, Examination, Reporting[9]

Table 8.3 SIM card Forensic Tools

Table 8.3 Cell Phone Forensic Tools

- **Paid tools**
- **Cellebrite Touch** is one among the foremost well-known and complete evidence extraction devices. It allows us to figure with over 6,300 different terminals with the most mobile operating systems. it's also very simple and intuitive.
- **Encase Forensics**, additionally to Cellebrite, may be a worldwide reference in forensic analysis. Its wide selection of features includes that which identifies encrypted files which attempts to decipher them through Passware Kit Forensic, a tool that comes with specific algorithms for this purpose.
- **Oxygen Forensic Suite** is capable of obtaining information from quite 10,000 different mobile device models and even obtaining information from services on the cloud and import backups or images.
- **MOBILedit! Forensic** allows tons of data to be received and advanced operations to be administered like obtaining an entire memory dump, avoiding terminal-locking measures, and flexibly creating reports.
- **Elcomsoft iOS Forensic Toolkit** allows for physical acquisition on iOS devices like iPhone, iPad or iPod. It also includes other utility features like that of deciphering the keychain that stores user passwords within the terminal analysed or registering each action that's performed during the entire process to stay a record of them.

Hand-Held Devices and Digital Forensics

- PDA Forensics
- Personal digital assistant (PDA) is also referred to as “palm device” or “hand-held.”
- The most common operating system (OS) used are the Palm OS (Palm, Sony, Handspring), Windows for Palm (HP), MS Pocket PC (Compaq), Embedix (Sharp).
- PDAs differ in several important ways compared with PCs.
- PDAs vary in areas of OS, interface style and hardware components, and they work with different OS such as Linux, Palm OS and Microsoft Pocket PC.
- Investigating crimes involving PDAs are more challenging than those involving normal computers. This is mainly because these devices are more compact, battery operated and store data in volatile memory.

Hand-Held Devices and Digital Forensics

PDA devices are available in many configurations, with various features.

The list of available devices and models changes frequently as the technology improves:

- Psion
- Apple Newton
- Blackberry
- Hp iPAQ Pocket PC
- Hp Jornada Pocket PC
- Palm Pilot
- Tungsten
- LifeDrive
- Treo
- Zire
- Sharp Wizard
- Zaurus
- Sony CLIE
- Tapwave Zodiac
- AlphaSmart Dana
- Dell Axim
- GMate Yopy
- Fujitsu Siemens Loox
- PocketMail

Psion

Sharp Wizard

Apple Newton

Dell Axim

Hand-Held Devices and Digital Forensics

Common PDA features include:

- Note taking
- Calculator
- Clock
- Calendar
- Address book
- Spreadsheets
- E-mail and Internet access
- Video and audio recording
- Bluetooth, and WiFi
- Radio and music players
- Games
- GPS (Global Positioning System)

Information Stored in PDAs:

PDA devices store the following types of information:

- Business and personal notes
- Business and personal contacts
- Documents
- Passwords
- E-mails
- Bank records
- Company information
- Images and videos

Because PDAs are used to store sensitive and confidential information, care should be taken to protect them.

Hand-Held Devices and Digital Forensics

COMPONENTS OF PDA:

- Microprocessor
- Read only memory (ROM)
  - Holds Operating System for the device
  - Varieties include Flash ROM, which can be erased and reprogrammed with OS updates
- Random access memory (RAM)
  - Contains user data
  - Kept active by batteries
  - Data lost when powered off
- Hardware keys and other user interfaces
- Liquid crystal display, sometimes touch sensitive

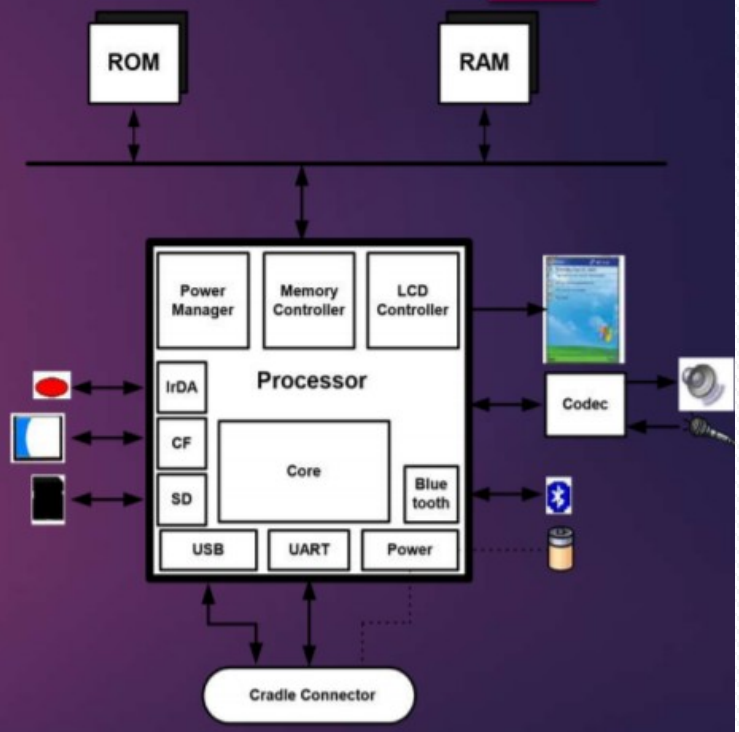


Figure 1: Generic Hardware Diagram

Hand-Held Devices and Digital Forensics

- PDA Forensics Tools

	Palm OS	Pocket PC	Linux
pdd	Acquisition	NA	NA
Pilot-Link	Acquisition	NA	NA
POSE	Examination, Reporting	NA	NA
PDA Seizure	Acquisition, Examination, Reporting	Acquisition, Examination, Reporting	NA
EnCase	Acquisition, Examination, Reporting	NA	Examination, Reporting
dd	NA	NA	Acquisition

Hand-Held Devices and Digital Forensics

- PDA Forensics Tools
- Though an investigator can browse the contents of the device using its user interface to obtain evidence, the approach is highly impractical and problematic, and should be used only as a last resort.
- A number of specialized tools are available for PDA forensic examinations, as follows:
- Device Seizure: A Paraben product that supports forensic acquisition, examination, and analysis of PDA devices for the PALM, Windows CE, and Blackberry operating systems.
- It provides the capture and reporting of data. It has two step acquisition of PDA device: All files in original structure and memory Card acquisition

Hand-Held Devices and Digital Forensics

- PDA Forensics Tools
- Palm dd (pdd): A Windows-based tool for memory imaging and forensic acquisition of data form the Palm OS family of PDAs.
- pdd will preserve the crime scene by obtaining a bit-for- bit image or snapshot of the Palm devices memory contents.
- Palm OS Emulator (POSE): is a software that emulates the hardware of various models of Palm powered handhelds making it a valuable tool for writing, testing, and debugging applications.
- It allows a user to create virtual handheld devices on your PC.

Hand-Held Devices and Digital Forensics

- PDA Forensics Tools
- Duplicate Disk (dd): A common UNIX program whose primary purpose is the low-level copying and conversion of files.
- Unlike the other tools described above, dd executes directly on the PDA device.
- Device Seizure: Complete a forensic acquisition, examination & analysis of PDA devices.
- *Used for*: The Palm Windows operating systems.
- *FEATURES:*
- Acquire Forensic Image
- Perform examiner-defined searches ◆ Generate hash values
- Generate a report of finding

Hand-Held Devices and Digital Forensics

- PDA Forensics Tools
- Depending on the Device and the Model, Device Seizure™ can access the following data: Phonebook (from the phone's memory and the SIM card) Call History including Received, Dialed and Missed Calls Datebook, Scheduler, and Calendar Current Text Messages Deleted Text Messages To-Do Lists Pictures and Videos Quick-notes RAM/ROM PDA Databases E-mail Deleted Data
- One amongst the features of the Paraben PDA Seizure is that it can create a forensic image of the handhelds and allow the investigator to conduct searches on the data acquired earlier, and later to execute a report generation of its findings.
- PDA Seizure can acquire images of the RAM and/or ROM, and also download the entire individual database off the Palms using Palm OS Emulators.
- Works on all types of Windows CE & PALM OS Devices. Perfect for law enforcement, corporate security, or anyone with an interest in computer forensics.

Hand-Held Devices and Digital Forensics

- PDA Forensics
- Relevant software in this segment is listed below:
- 1. PDD: It is based on the Unix dd. This is the most popular Palm forensics software.
- 2. CodeWarrior for Palm OS: It is used to put palm devices into “Debug Mode.” This allows communication via serial port, imaging and can be used to overcome lockout protection.
- 3. PDA defense: It is a third-party lockout software. It is difficult to bypass.
- Forensics tools acquire data from a device in one of the following two ways: “physical acquisition” and “logical acquisition.”

Hand-Held Devices and Digital Forensics

- Printer Forensics
- One may wonder how printers can pose security risks.
- Printers are not generally considered to be “hand- held” devices although “portable printers” are now available in the market.
- Modern day printers have computer-like characteristics with internal storage, FTP uploading, Simple Network Management Protocol (SNMP), etc. Some printers are loaded with vulnerable applications.
- No two printers of the same model will behave in the exact same pattern. This is because the mechanical parts that make the printer will not be 100% equivalent.

Hand-Held Devices and Digital Forensics

- Possible attacks through printer exploits are as follows:
- 1. Modifying IP address of the printer to an unused address on the same subnet.
- 2. Changing IP address of the target machine to the previous IP address of the printer.
- 3. Capturing all traffic sent over Port 9100 to the IP address to which end-users are configured to print. The attacker can keep collecting print jobs until it is found out.
- 4. Forwarding all print jobs onto the “new” IP address of the printer; when the end-user who submit- ted the job goes to the printer in question to collect the print job, he/she finds that it has been processed as normal.

Hand-Held Devices and Digital Forensics

- Scanner Forensics
- Today, a large portion of digital image data is available. Acquisition devices such as digital cameras and scanners are used to create that data.
- With cameras, it is possible to digitally reproduce scenes that may look almost as real as natural scenes.
- Scanners are used to create hard copy of the captured images.
- For sound forensic approach it is necessary to identify non-intrusive method for scanner model identification and authentication of the scanned images is also necessary.
- One approach to identify model of the scanner statistical features of scanning noise.
- One of the biggest challenges in scanner forensics is that, analytical procedures and protocols are not standardized nor do researchers and practitioners use standard terminology.

Hand-Held Devices and Digital Forensics

- iPhone Forensics
- One of the most used Smartphone, to date, is the Apple iPhone. The iPhone was introduced by Apple Inc. in January 2007.
- For the forensic analysis of an iOS device following concepts have to be clear:
  - Types of iOS devices: iPhone, iPOD, iPAD, Apple TV, Apple Watch and all these devices all the versions in use so far.
  - iOS device connectors: Lightning to 30-pin Adapter, Lightning to Micro USB Adapter, Lightning to SD Card Camera Reader, and all others.
  - iOS operating system
  - iDevice identification (Version, shape, etc.)
  - iOS file system (HSF, HSF+, APFS, and others)

Hand-Held Devices and Digital Forensics

- iPhone Forensics
- Using the ideviceinfo command in Unix, it is possible to extract some information from the device, with no need of unlocking it. The information that can be extracted is as follows:
  - Device name
  - Device class
  - Hardware model
  - iOS version
  - Telephony capability
  - Unique device ID
  - Bluetooth MAC address
  - Wi-Fi MAC address
- Forensic techniques utilized for iPhone are:
  - Acquire data directly from the iPhone
  - Acquire a backup or logical copy of the iPhone file system using Apple's protocol

Hand-Held Devices and Digital Forensics

- iPhone Forensics Tools
- 1. MacLockPick
- WOLF
- Cellebrite UFED Forensic System
- MDBackup Extract
- Zdziarski's method
- Challenges
- Few of the biggest challenges is iPhone forensic investigation is that not many iPhone forensic experts are available and that iPhone platform is proprietary.
- Also its one of the platform characterized by most frequent changes which makes the forensic experts difficult to keep themselves updated.

Hand-Held Devices and Digital Forensics

- Challenges in Forensics of Digital Images
- Forensic image processing is used so far for questioned document examination: footwear/tire impression, blood splatter evidence, bullet striation and primer mark examination, etc.
- An identity of the digital image is paramount in image forensics.
- As its frequently required to make corrections and adjustments to images, it is important to maintain the integrity of the images from capture through final use of the image.
- Due to migration from traditional to digital photography forensic institutions and lay enforcement agencies are worried about security, integrity and continuity of digital images.
- Two main interests in image forensics are: source identification and forgery detection.
- There is no clarity regarding what is original(unlike in physical images, negatives are there) copy of the image.
- Hence in some cases entire storage media has to be preserved to have first permanent copy of the image.

Hand-Held Devices and Digital Forensics

- Challenges in Forensics of Digital Images
- In modern times digital images can be easily created, morphed and manipulated without leaving any obvious traces.
- So it is important to determine the means by which a digital image has been created. Some of the approaches are:
- Verifying and evaluating the image statistics that are inherent to real life scenarios
- Detecting, classifying and measuring the qualities of spatial structures in an image
- Identifying signature traces to detect traces of certain types of operations used in image generation process by possible sources.

Hand-Held Devices and Digital Forensics

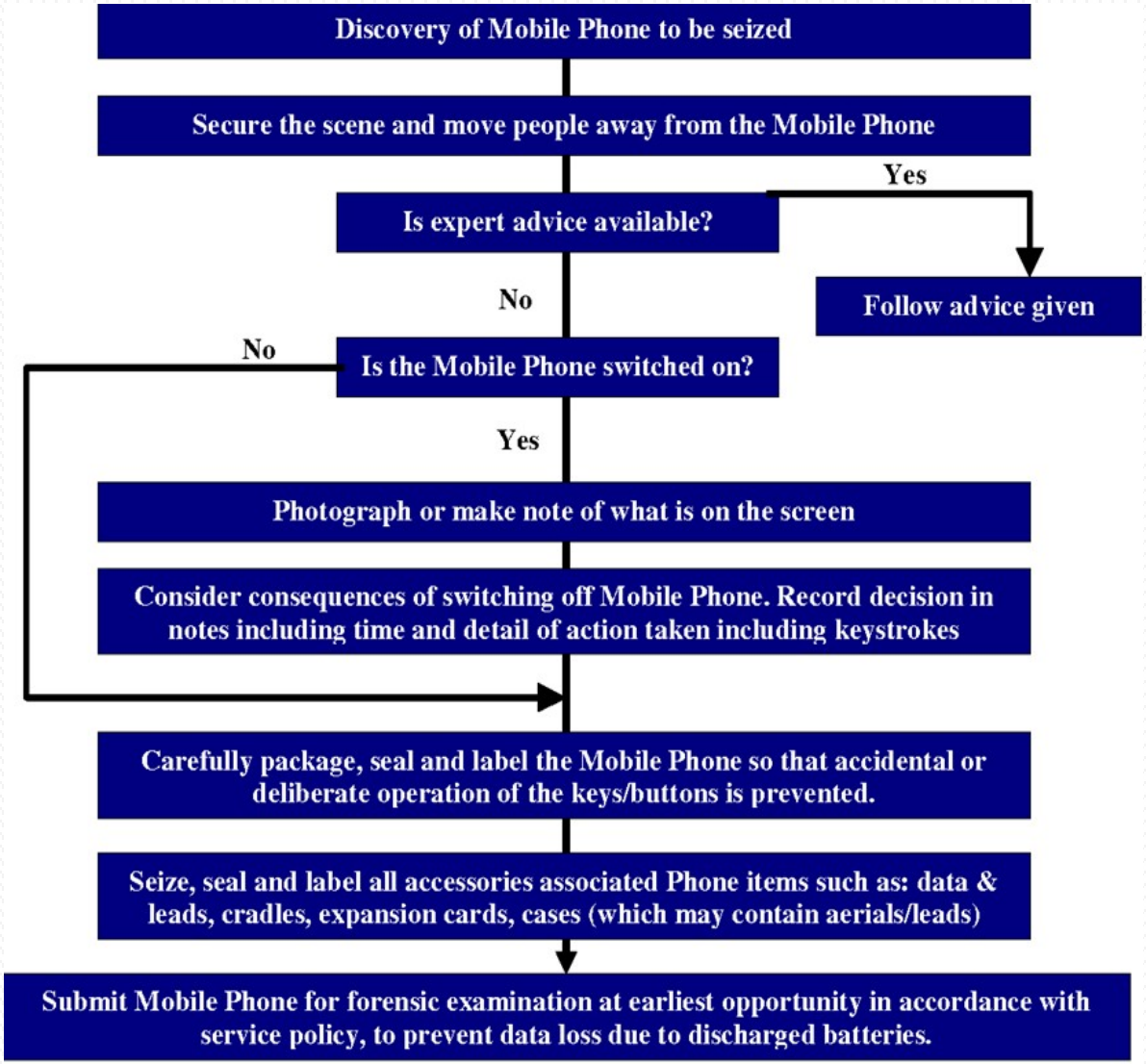
- Smartphone Forensics
- Workforce mobility is on the rise and Smartphones are gaining momentum as a device option for people working at the field (field workers include, e.g., sales personnel, technicians, insurance agents, medical officers, pathological laboratory technicians who offer door-to-door medical service, etc.).
- The main reason for rising popularity of Smartphones is their high functionality that comes in a relatively low-cost device.
- Smartphones are mobile phones based on high-level OS that are open to third-party application development.
- Smartphone features:
  - Works as a cell phone
  - Has full-fledged address book, a planner, an organizer, messagner, photo and video camera
  - Has GPS navigation facility
  - Works as a web client to access web-based applications
  - Provides a platform for third party applications as well.

Hand-Held Devices and Digital Forensics

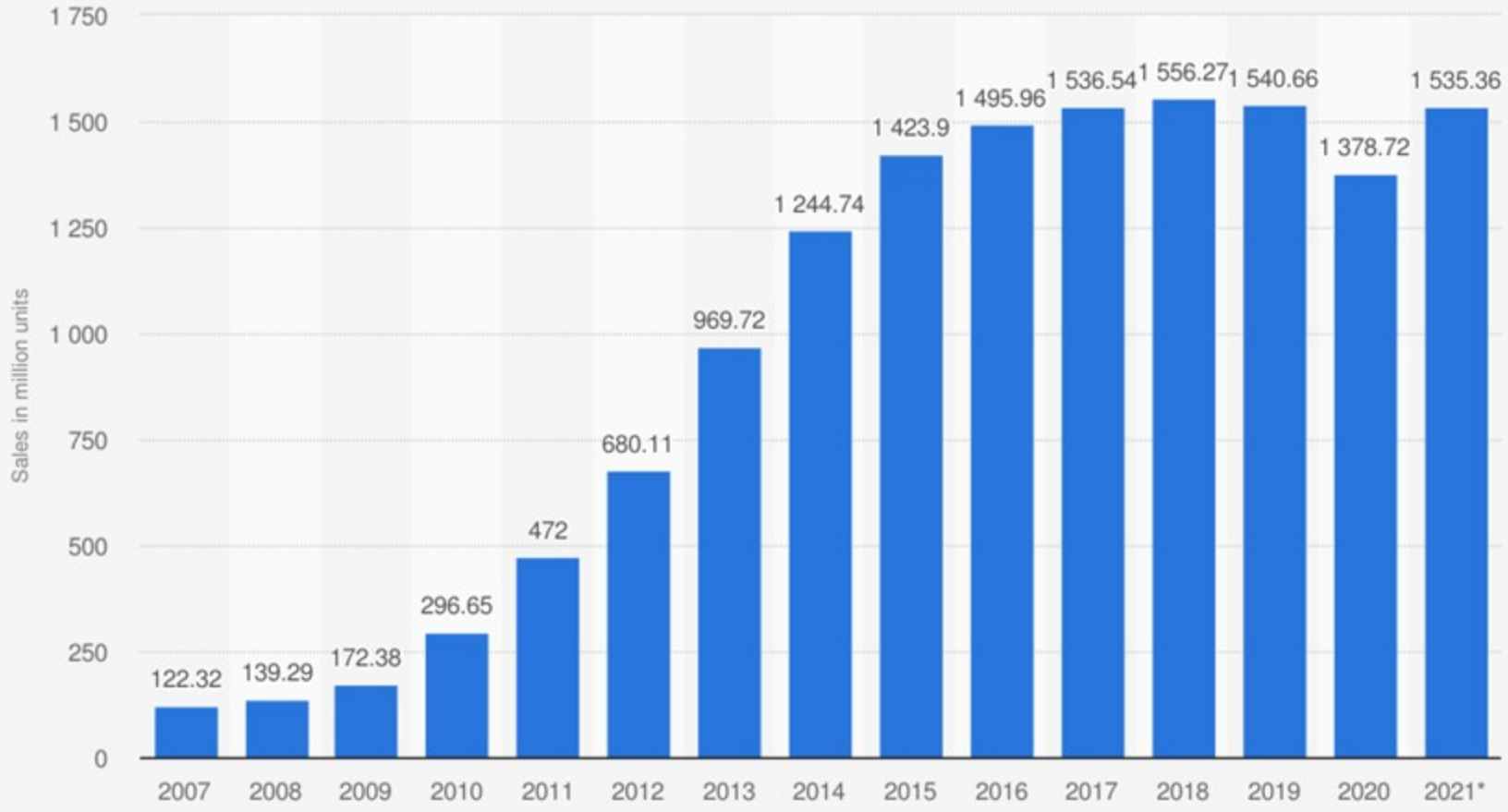
- Smartphone Forensics
- Enterprises evaluates Smartphone as the main device for certain types of field workers for below reasons:
  - They have always connected status
  - They have the ability to act as a user's primary communication terminal
  - They can be the platform for mobilizing enterprise applications.

Hand-Held Devices and Digital Forensics

- Smartphone Forensics

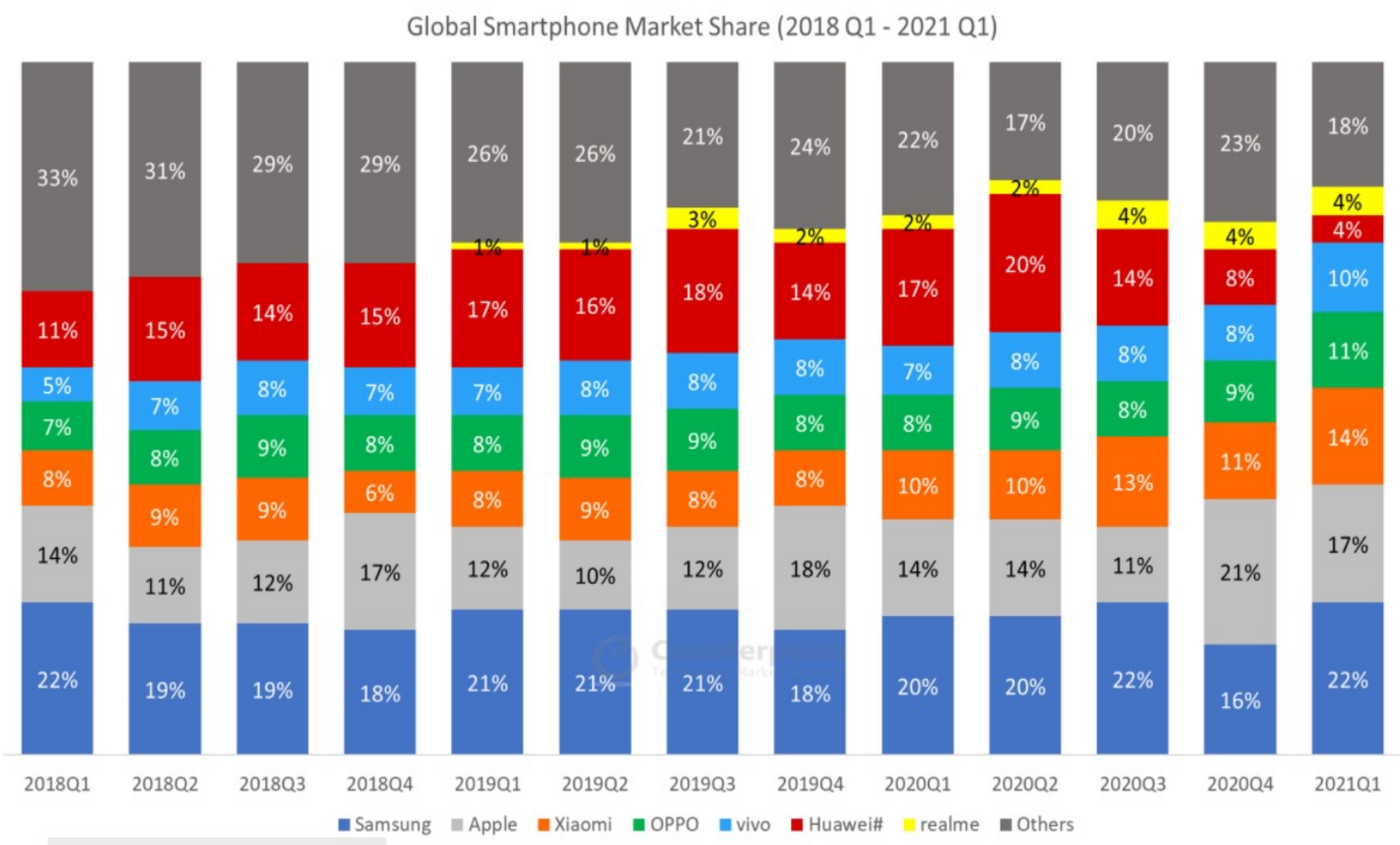


Number of smartphones sold to end users worldwide from 2007 to 2021 (in million units)



Source
Gartner
© Statista 2021

Additional Information:
Worldwide; Gartner; 2007 to 2021


Global Smartphone Market Share (2018 Q1 - 2021 Q1)
2018Q1
2018Q2
2018Q3
2018Q4
2019Q1
2019Q2
2019Q3
2019Q4
2020Q1
2020Q2
2020Q3
2020Q4
2021Q1
Samsung
Apple
Xiaomi
OPPO
vivo
Huawei#
realme
Others

Toolkits for Hand-Held Device Forensics

- So far, we have been through the forensics aspects of PDAs, Smartphones, cell phones, printers, scanners, iPhones BlackBerrys and digital images/digital cameras.
- Acquisition of data from a hand-held device is carried out in the following two ways:
- 1. Physical acquisition: In this particular type of acquisition, an exact copy bit-by-bit is collected of the entire physical storage which can be either a RAM chip or a disk drive.
- 2. Logical acquisition: This is an exact copy bit-by-bit of the logical storage such as file and directories, involved residing on a logical store which could be several disk drives.

Toolkits for Hand-Held Device Forensics

- EnCase
- EnCase is a popular software toolkit for hand-held device forensics. Its features support many features: analytical tools, suspect media acquisition, data capture, documentation and search features.
- Device Seizure and PDA Seizure
- These are two famous tools from Paraben. Paraben's device seizure is one of the many products used for viewing cell phone data.
- Palm DD (PDD)
- There was a mention of this tool (PDA Forensics). The PDD tool runs only on Windows based systems and is mainly used by forensics examiners for physical acquisition.

Toolkits for Hand-Held Device Forensics

- Forensics Card Reader
- The Forensics Card Reader (FCR) consists of FCR software. It allows forensics
- examiners to acquire data from SIM cards without modification and a smart card reader with USB connection.
- Cell Seizure
- Cell Seizure is a forensics software toolkit. It is used for acquiring, searching, examining and reporting data associated with cell phones operating over CDMA, TDMA and GSM networks.

Toolkits for Hand-Held Device Forensics

- Large type of data that can be obtained on most cell phones, using Cell Seizure includes:
- 1. SMS history: Inbox/outbox.
- 2. Phonebook: SIM card, own numbers, speed dialling, fixed dialling.
- 3. Call logs: Dialled numbers, received calls, missed calls.
- 4. Calendar: Reminder, meeting, memo.
- 5. Graphics: Wallpaper, picture camera images, EMS template images.
- 6. Wireless Application Protocol (WAP): WAP settings, WAP bookmarks.
- 7. SIM: GSM-specific data.

Toolkits for Hand-Held Device Forensics

- MOBILedit
- This is a forensics application that allows examiners to acquire logically, search, examine and report data from CDMA, Personal Communications Services (PCS) and GSM cell phones.
- Forensic SIM
- This toolkit comes from Radio Tactic. Its components include: acquisition terminal, analysis application, control card, data storage cards and the card reader.