Unit-5

Mobile Phone and Android Forensics

contents

- Crime and mobile phones
- Evidences
- Forensic procedures
- Files present in SIM Card
- Device data
- External memory dump
- Evidences in memory card
- Android forensic fundamental
- Data extraction techniques
- Screen lock bypassing techniques

Mobile Hacking –SMS and call Forging

- Cell phone are getting hacked
- The hackers who hack cell phone have apparently found how chips are manufactured
- Another requirement for hacking the phone is that hacker must have cell phone in hand, which is physical access to cell phone for minimum 3 minutes
- 70% hacked phones fall in first generation category, problem has been solved in second and third generation category.

What can a hacker do?

- Steal your number:
  - Hackers use your cell phone and make calls and bill is paid by you as it is charged by network provider.
- Take your information:
  - Hackers access your phone for download all addresses and another information stored in cell phone.
  - Hackers delete your contact numbers, so backup of all information must be placed some place, like your e-mail account or drive. This technique is known as Bluesnarfing.

What can an attacker do?

- Rob your money
  - Hacker sitting one place and access multiple phones at a same time and collect huge amount in no time at all.
  - It takes hardly few seconds or minutes for a hacker to do so.
- Give the system a virus:
  - Using hack code to another cell phone, hacker could steal your phone and return after installing virus-this cause cell phone to crash or system to stop working.
- Spy on you:
  - A hacker can gain unauthorized access to cell phone and take away cell phone for spying and hacking mobile phone remotely
- Access your voice mails:
  - Recorded voice mails received from other clients can be retrieved by hackers by simply hacking cell phone
  - Done easily if you phone is not secured with passwords or patterns or pin numbers.

What can you do?

- Use your passwords
  - Keep security lock to avoid giving unauthorized access to other people for various purpose.
- Leave the phone off:
- Upgrade your phone:
  - Upgrades should be installed so security features are upgraded

Call Spoofing/Forging

- Call forging is to spoof caller Id number displayed on cell phone/landline.
  - It relies on VoIP(voice over Internet Protocol)
  - VoIP is an emerging and exciting innovation is far as information and communication technology is concerned
  - It can be considered as GEN Next Cyber Crime.

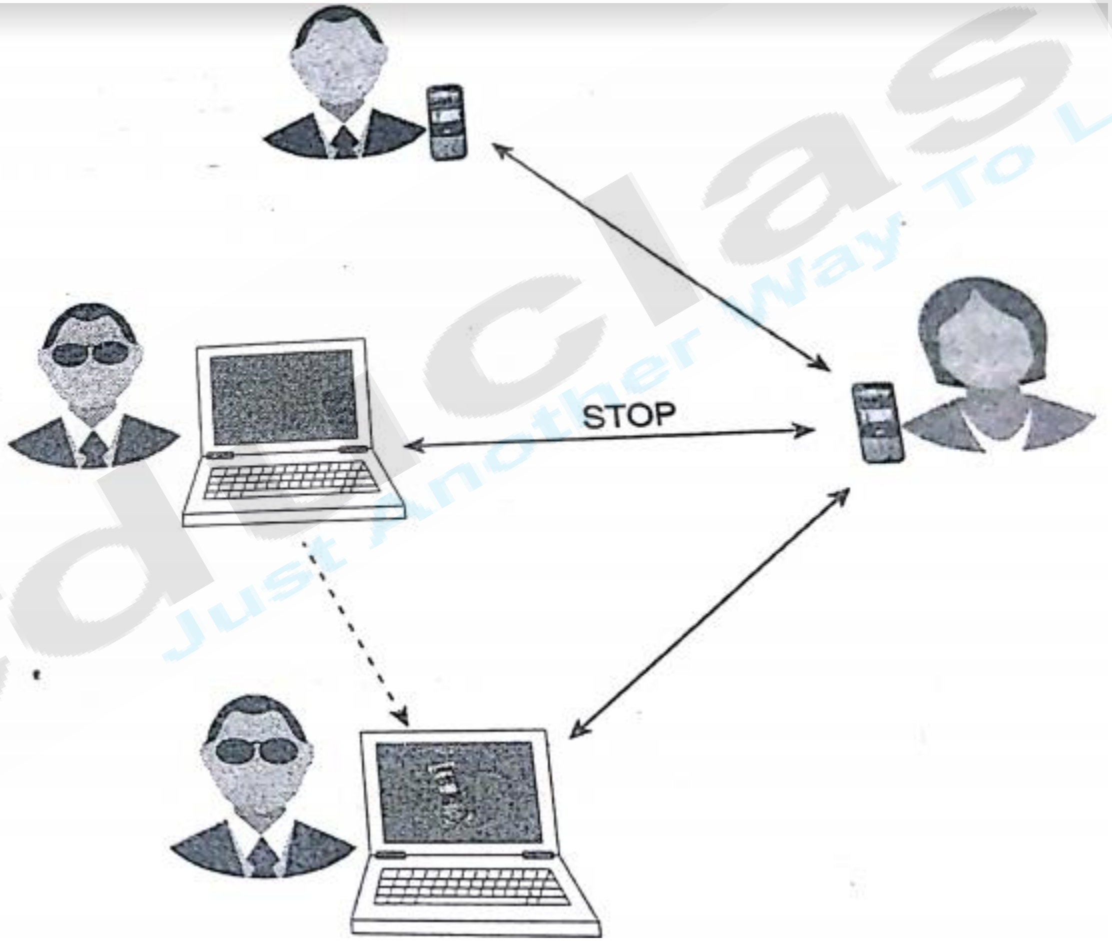


Fig. Call Forging

1)about caller ID forging/Spoofing:

- Method of making or forcing the telephone network to display incoming call number on the cell phone display, which is actually not coming from genuine source or originating station.
- Caller ID spoofing is nothing but making victim feel that it is coming from genuine source.
- People are prone to attend calls only when they know the identity of the caller.

2)Basics of call forging:

- First VoIP is used to call via internet Pc to a telephone
- VoIP there are many loopholes which actually allows hacker or intruder to spoof the call.
- There are many websites on internet allow these services to help people when balance goes nil.

(1) Enter your cell phone number from which call needs to be made

(2) Provider will bridge the calls to required network provider, no authentication required on website and server is located in USA, so tracing hacker or intruder is next to impossible.

- When hacker logs on server and enter wrong cell number then makes a call through internet and shows wrong identity as it is spoofed call.
- They are traced and trapped they get out of it very easily as there are no laws passed for it.
- Individual to be alert and do not entertain such calls .

SMS Forging

- SMS is one of the most popular, easy and cost-efficient means of communications
- SMS forging is the method to spoof sender ID from where message is sent
- One can send sms to international no from any number of sender’s choice
- Facility to choose sender ID is up to 11 characters/names

SMS Routing in GSM

- First sender sends SMS through SMS Gateway. The identity of the sender who sends the message is appended to the SCCP packet of SMS
- Once SMS reaches the respective gateway, it is routed or directed to the recipient’s or destination gateway
- SMS is sent to recipient’s cell phone

- There are many possible ways through which an individual can send SMS to respective SMS gateway.
- One of the medium or gateway can be Internet.
- SMS forging lies in changing the SCCP(Signaling Connection Control Part) package which contains sender’s information before delivering the SMS to the SMS gateway.
- The hacker can change contets of the SCCP packet and send same packet to many recipients as a spoofed SMS.

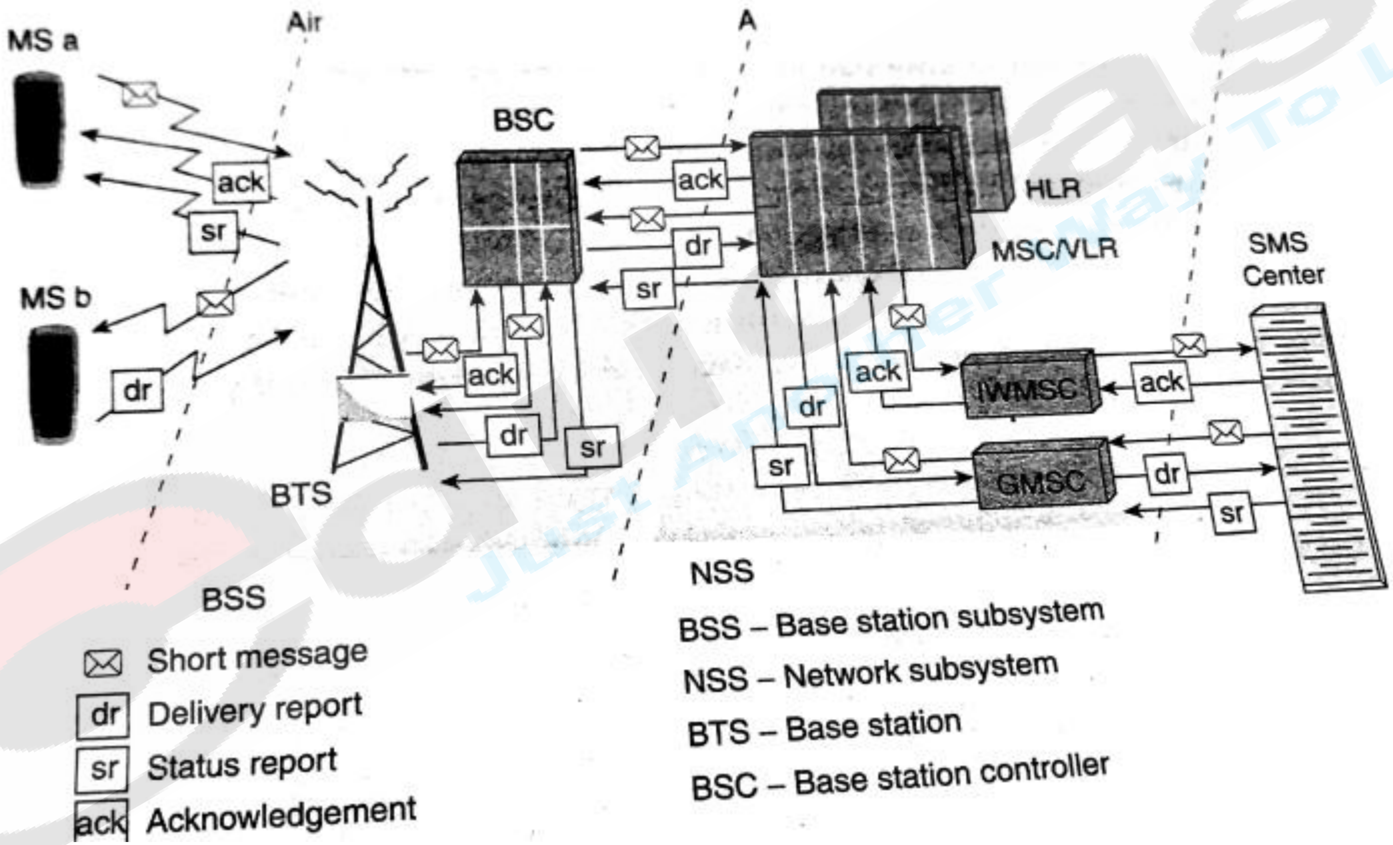
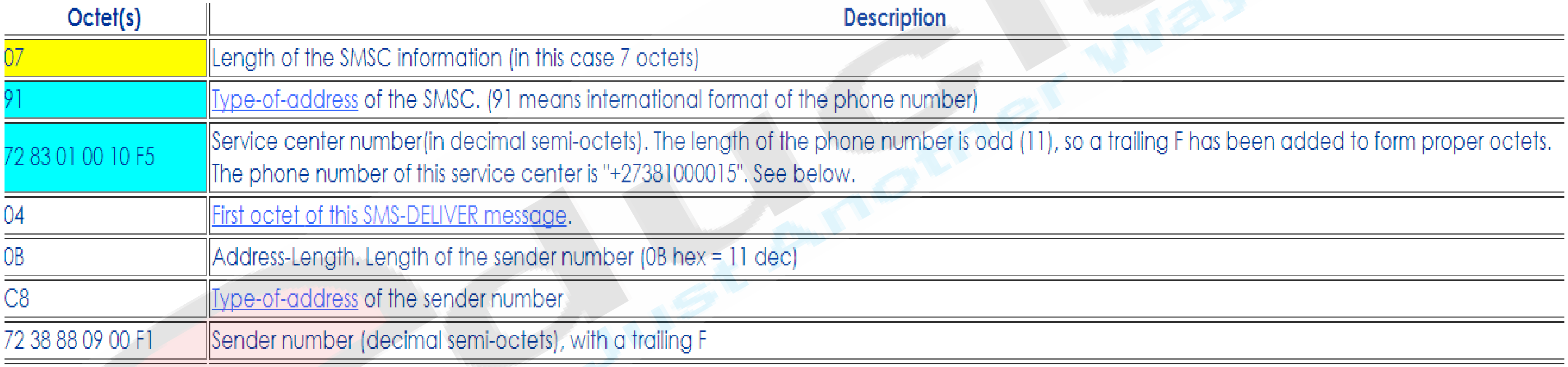


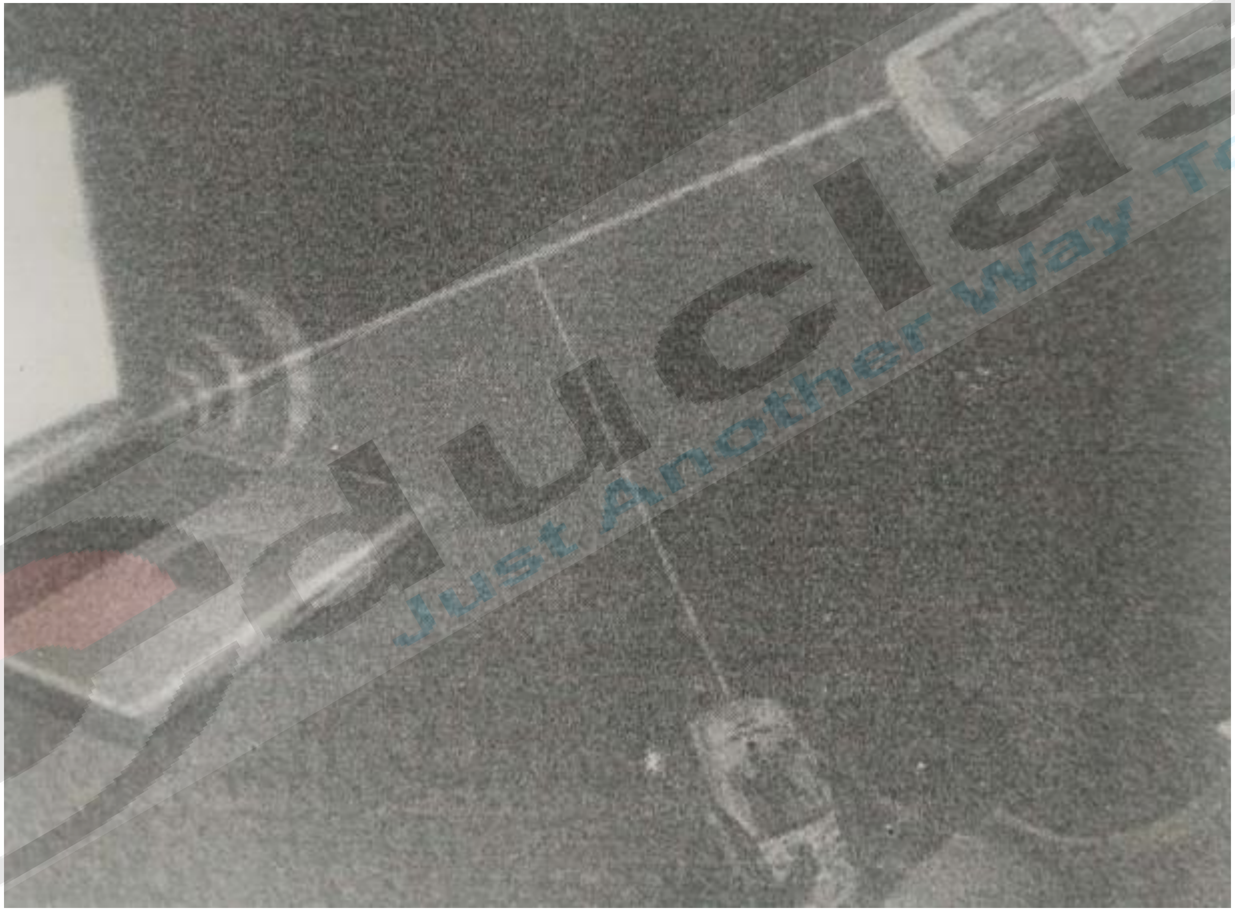
Fig. SMS routing in GSM



Octet(s)	Description
07	Length of the SMSC information (in this case 7 octets)
91	Type-of-address of the SMSC. (91 means international format of the phone number)
72 83 01 00 10 F5	Service center number(in decimal semi-octets). The length of the phone number is odd (11), so a trailing F has been added to form proper octets. The phone number of this service center is "+27381000015". See below.
04	First octet of this SMS-DELIVER message.
0B	Address-Length. Length of the sender number (0B hex = 11 dec)
C8	Type-of-address of the sender number
72 38 88 09 00 F1	Sender number (decimal semi-octets), with a trailing F

Bluesnarfing

- Refers to stealing information or data from any wireless device using a Bluetooth connection between two devices or cell phones, laptops, PDAs.
- Bluesnarfing allows hacker to gain access to calendar, contacts, e-mails, messages.
- Any cell phone device with its Bluetooth connection enabled or turned on and set to “discoverable” can be attacked or hacked.
- By turning off the Bluetooth, one can protected from the possibility of being bluesnarfed or hacked.
- As Bluetooth will be replaced by Wi-Fi,there will be less risk for Bluetooth attacks

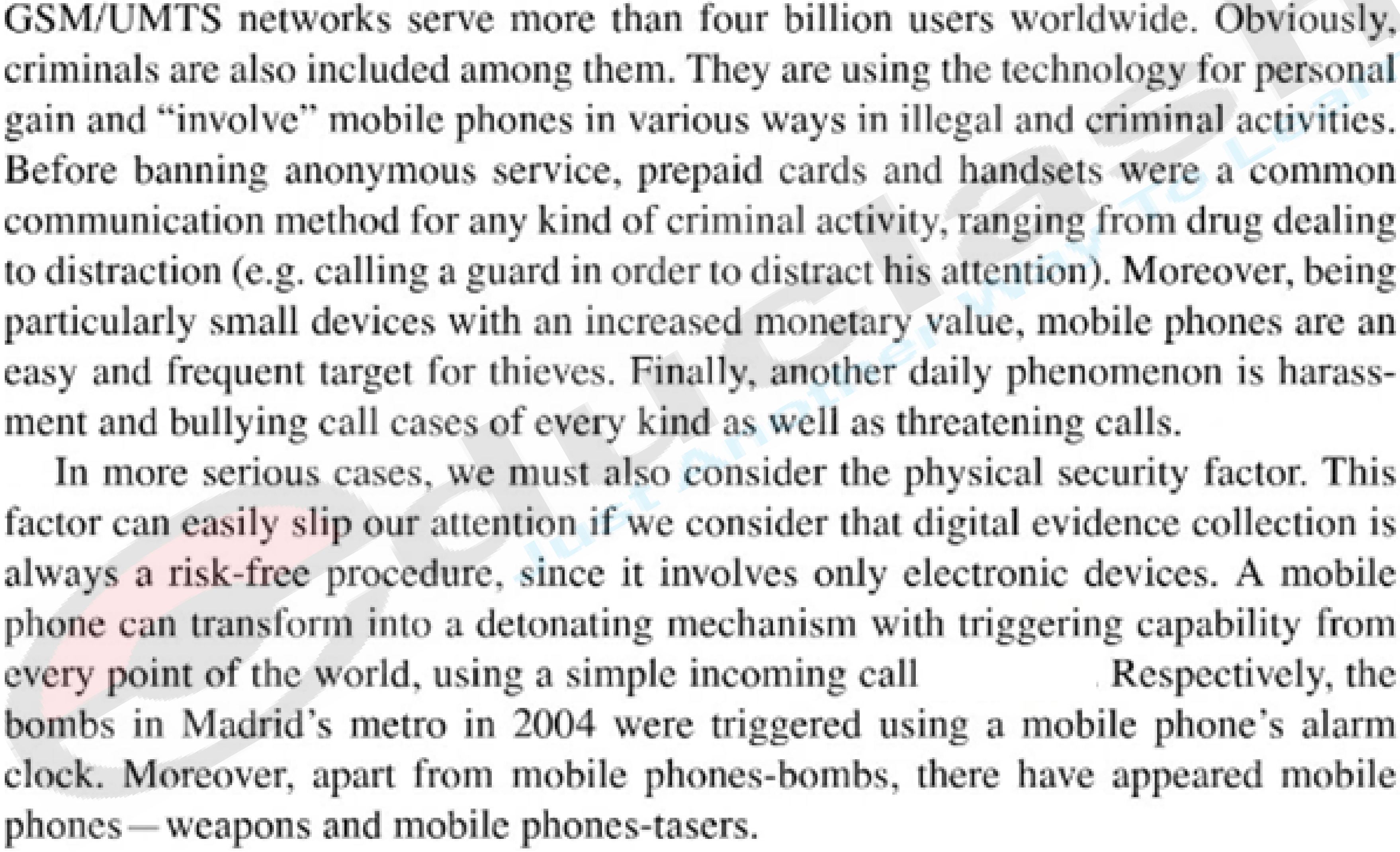


Example of Bluesnarfing

Mobile Phone Forensics

- Use of evidence plays vital role in court case hearings
- Digital forensics analysts accumulate all evidences from crime scene and then evaluate evidences and analyze result before presenting it in case hearing
- Digital evidence analysis can be done with use of data that is extracted from any type of digital electronic device.
- Most important and very common digital device is cell phones.
- The need and importance of cell phones are increasing day by day.
- Android phones are latest trend in cell phone with advanced technology and functionality.
- These phone used for communication as well as storing data, organizing data as well as processing data for using or browsing internet.
- Using biometric characters to unlock the device to achieve individually of each device and user or owner of it.

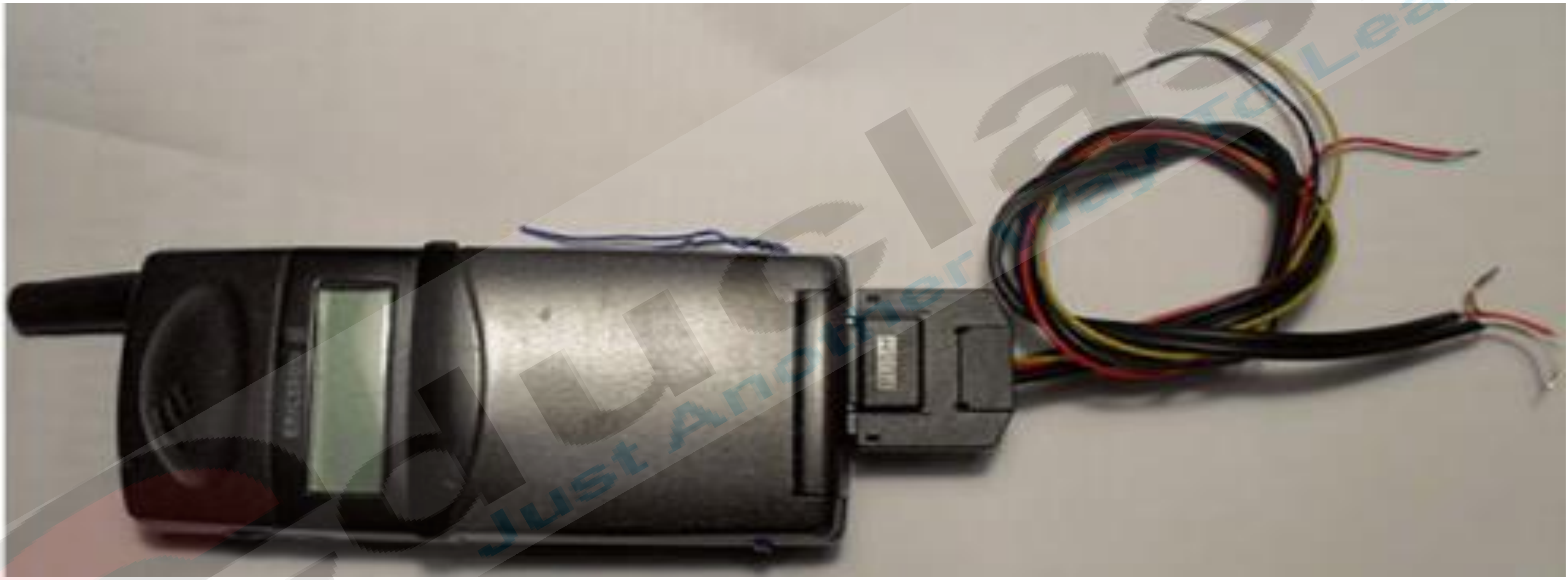
Crime and Mobile phones



GSM/UMTS networks serve more than four billion users worldwide. Obviously, criminals are also included among them. They are using the technology for personal gain and “involve” mobile phones in various ways in illegal and criminal activities. Before banning anonymous service, prepaid cards and handsets were a common communication method for any kind of criminal activity, ranging from drug dealing to distraction (e.g. calling a guard in order to distract his attention). Moreover, being particularly small devices with an increased monetary value, mobile phones are an easy and frequent target for thieves. Finally, another daily phenomenon is harassment and bullying call cases of every kind as well as threatening calls.

In more serious cases, we must also consider the physical security factor. This factor can easily slip our attention if we consider that digital evidence collection is always a risk-free procedure, since it involves only electronic devices. A mobile phone can transform into a detonating mechanism with triggering capability from every point of the world, using a simple incoming call . Respectively, the bombs in Madrid’s metro in 2004 were triggered using a mobile phone’s alarm clock. Moreover, apart from mobile phones-bombs, there have appeared mobile phones—weapons and mobile phones-tasers.

At the same time, focusing in "white collar" crime level and with the mobile phones in presence, we observe all kinds of telecommunications fraud, personal data theft, identity infringement-theft, industrial espionage (using the memory of the mobile phone or the phone itself as a bugging device to intercept and to transfer data and commercial secrets), and so on. The future mobile commerce options, using mobile phones to buy goods and services, will obviously make the problem more immense, providing more space for criminal activities.



Mobile Phone Detonator. We have a clear view of the connection with the mobile phone input/output port

The evidence

- Cell phone provide a sequential flow of information and data that represents user and their respective behavior.
- This data are not stored in cell phones, but in computers and laptops and even the providers of networks.
- The data stored in cell phones usually reside in internal memory, SIM card, external SD cards if attached.
- Evidence of cell phone usage can be found in his/her desktop or laptops.

Data that could be used as evidence are listed below:

1. Phone catalog
2. Phone contacts
3. Incoming calls
4. Outgoing calls
5. Missed Calls
6. Incoming text messages
7. Outgoing text messages
8. Incoming MMS
9. Outgoing MMS
10. Voice notes or voice messages
11. Calling sounds or music
12. Sound recording
13. Photographs
14. Videos

15.Graphics

16. Workspace

17. Calendar

18.Alaram clocks and/or reminders

19. To-do lists

20. Written texts

21.Memos

22. E-mail stored in phone or e-mail accounts

23. Websites visited using cell phone

24. Documents and file of any type

25. User identifiers(pin,password)

26.Device identifiers(IMEI number)

27.GPS receivers

28. GPRS

29. WAP

30. Internet settings

Forensic Procedure

- IOCE(International Organization on Computer Evidence) states following :-

1. When dealing with digital evidence all the general forensic and procedural principle must be applied.
2. Upon seizing digital evidence action taken should not change that evidence.
3. When it is necessary for a person to access storage or transfer of digital evidence must be fully documented , preserved and available for review.
4. All activity relating to the seizure ,access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
5. An individual is responsible for all action taken with respect to digital evidence while the digital evidence in their possession.
6. Any agency which is responsible for seizing , accessing , storing or transferring digital evidence is responsible for compliance with their principles.

- The Guidelines form ACPO(Association of chief Police officer)

1. No action taken by law enforcement agencies or their agent should change data held on a computer or storage media, which may subsequently be relied upon its court.
2. In exceptional circumstance where a person finds its necessary to access original data held on a computer or on storage media , she or he must competent enough to do so and to give evidence explaining the relevance and their implication of their action.
3. An audit trail or other record of all process applied to computer based electronic evidence should be created and preserved .
4. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principle are adhered to

File Present in SIM card Device Data

- The GSM 11.11 standard defines the existence of the directory structure which includes specific and important file in the SIM.
- User can consider it as the resemblance of files and folder in the hard disks.
- It is important for a user to know that inside these directories there are some files stored in memory slots where essential information is stored.
- This hierarchy is described in FIG where master file (MF) is considered to be the root directory, dedicated file (DE) is the subdirectories and elementary file (EF) is the actual file in which the data is stored. There are different read, write , modification and deletion authorization existing for these files.
- Some file can be viewed without any authentication pin or password . While other require them.
- The most important files can be accessed only by the provider by using appropriate ADM code.
- SIM contains files which contains cell phone capability, card's serial and unique number, network, default language list of providers with their names, incoming or outgoing message or MMS , contacts , setting , list of dialed or missed or received calls and many more.
- There are some files which include the host network subscriber temporary or permanent identity

  control channel , subscriber's coarse location and the encryption key.
- 100 files will are present. These standardized files, each provider is allowed to use their own files.
- Issuing the right commands to perform the brute force reading of all the memory areas through SIM's microprocessor or provider ' s response more exciting data could be found in such no documented files.

tion existing

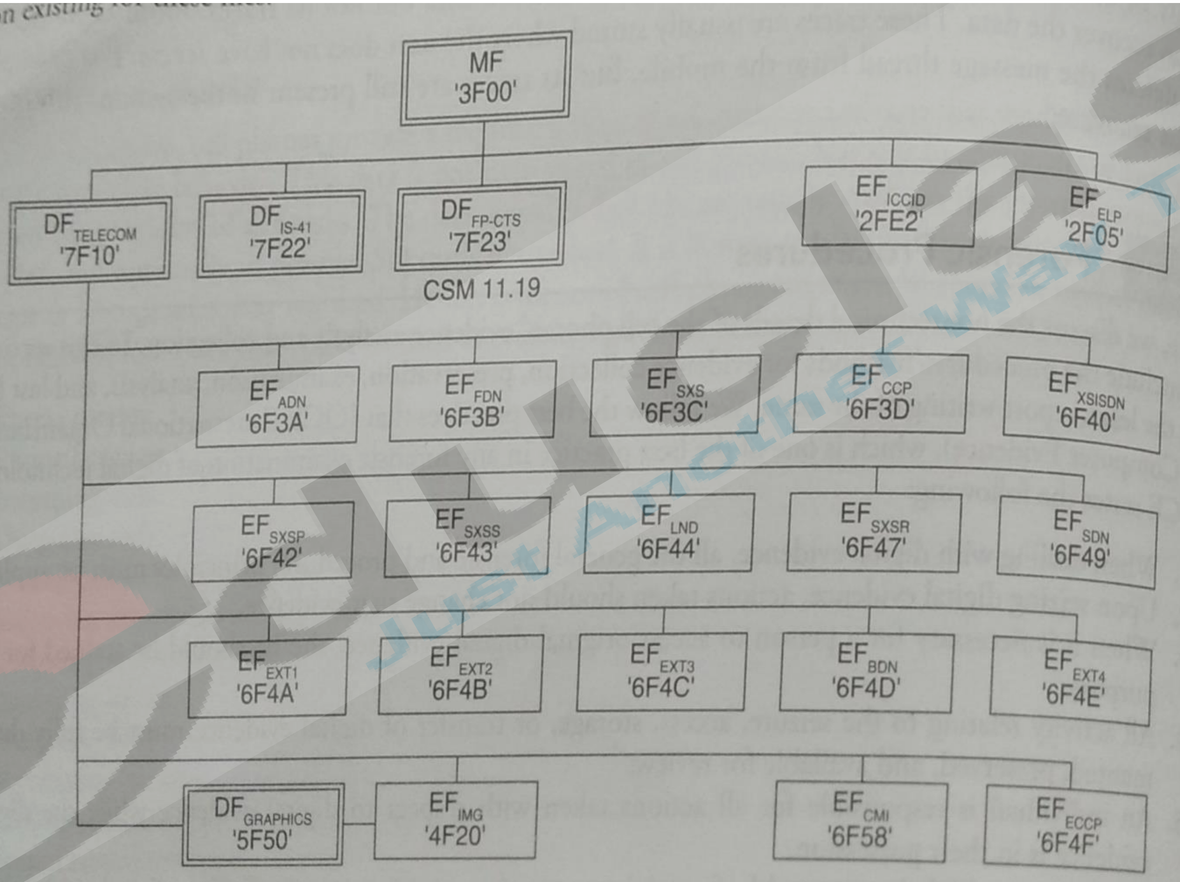


Figure 13.5 SIM file structure.

- Most of the contents found in all these files have increased value as evidence.
- The fact that the user usually cannot directly access them, and as such it is more difficult for him or her to delete them is of great importance.
- A criminal not knowing these details will not be able to erase incriminating data , leaving behind valuable evidence.
- It is possible to verify these data in comparison to the ones the provider retains and spot a possible forgery.

The Device data

- SIM card stores certain type of data.
- The remaining data needs to be stored in the phone memory.
- There are two types used NAND Flash and NOR Flash.
- Internal memory flash memory usually has date, time, volume, SMS , calendar data, IMEI number, sound setting , call logs etc.
- Application, games, executable files are stored in external storage.
- Along with current data even older or deleted data can be recovered from the depth of the cell phone memory as data chunks are present which helps in recovering the data.
- Some type of data is either partially or fully recoverable after the delete operation.
- SIM data is individually stored in memory. It includes previous Sim card IMSI which was used in the same cell phone.
- An examiner can resort to the memory dump byte by byte for NOR memory by using special software and hardware tools which clone or replicate the content of the memory .
- In comparison to SIM card the examiner can recover the complete data image in the physical layer.

- It’s a complicated process as the data is in unstructured format and they have to be interpreted in some specific file system.
- The main functionality of tools used for dumping the memory contents is to upload new firmware varieties, upgrade , debug and repair the cell phone. Should be provided by the manufacturer.
- But many third party sells relevant tools for the same.
- The usage of such unofficial tools is at times related to certain illegal activities like changing the serial numbers , unlocking the device unethically.

- These tools can contribute in DE extraction lies in the fact that they can function even the cell phone is switched off, turned off, blocked or partially broken.
- The tools are harmful enough to alter the data if the user of the cell phone is not cautious and knowledgeable enough.
- These tools can help to destroy the evidence.
- JTAG (Joint Test Action Group) is a special bug interface originally used to examine the printed circuit board of electronic devices. It allows to check , debug, and the monitor the embedded system. For forensic practice and usage it can assume the memory dump but it is very difficult to search a specific test point and documentation is proprietary evidence and not readily available.

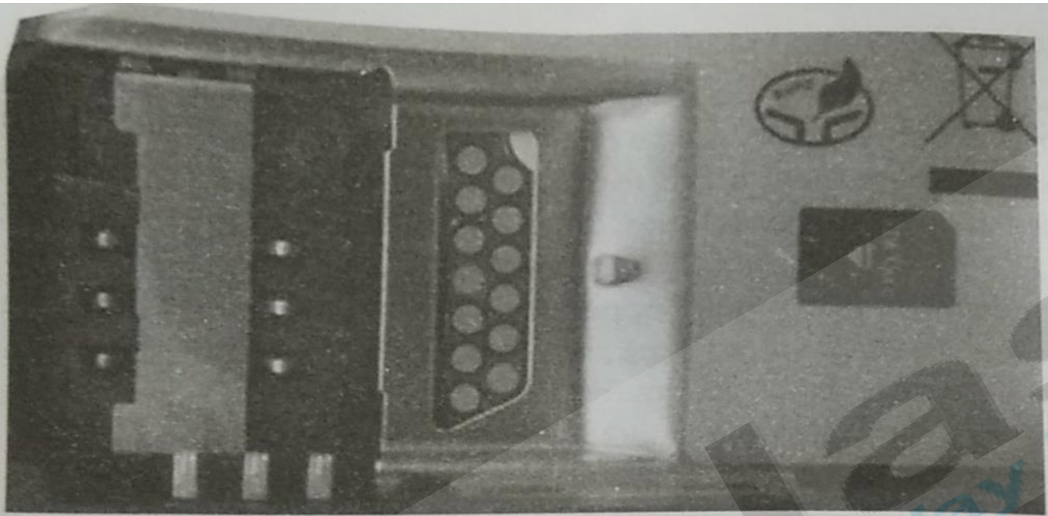


Figure 13.6 JTAG pinouts.

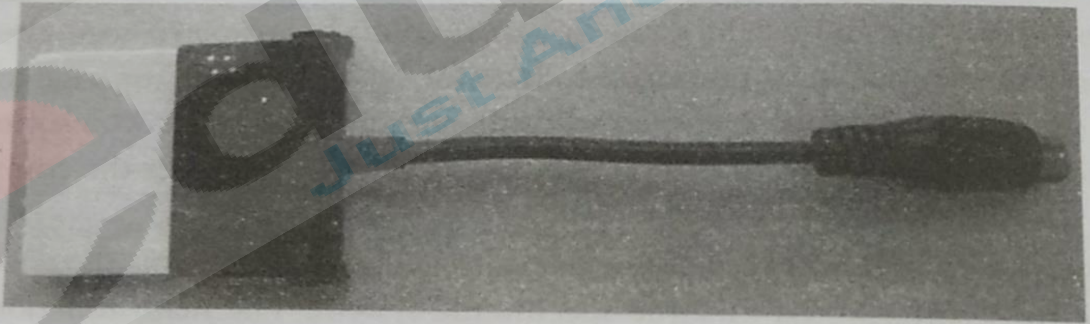


Figure 13.7 JTAG cable.

- JTAG had many limitations main problem is that there is no defined way to sense the external changes which have taken place in the flash memory, meaning that the data would have been modified.
- Cell phone use memory managers who dynamically allocate and reform the memory data. This is done in command to attain optimal memory use and minimal wear leveling. Basically this means that the exact location where the certain piece of data or information evidence reside in the memory dump will change each time the dump operation is performed.
- The search for valuable information or data in the dump of some GB ‘s in size is a tough and time consuming job; too some cell phones have encrypted memory contents.
- It is important to note that some cell phones delete some parts of data which is stored in memory when switched from one sim card to another.

External Memory dump

- If the cell phone fully or partially destroyed then it is possible to separate and remove the integrated memory circuits by using special precision surface mount device (SMD) soldering/de soldering station.
- In this external memory dump occur using the right hardware tools.
- This procedure assures that no data or information is infected as the cell phones remain to be switched off or turned off. This procedure has a serious risk of destructing the complete circuit during this subtle process of detaching and dis soldering
- Cell phones should be disassembled in order to extract the integrated memory circuit.
- As this method has many difficulties associated with it .this method is the least preferred one.

Evidence in Memory card

- With the increased multimedia capabilities of smart phone, external memory cards have become a trend now.
- They provide data storage for image , video, sounds, applications, documents, data.
- It can also be used as computer and other devices like MP3 player, PDA, camera, video camera and so on.
- Data can also be transferred from it.
- A set of interfaces and standard are available for interconnection.
- It make easier to read memory types as there is wide range of products available starting from the beginners to the advanced user.
- The principle of extracting data from the memory apply as analyzed before.
- It is important to note that these cards can be transferred to desktop or devices or even computers can be connected to the cell phones.

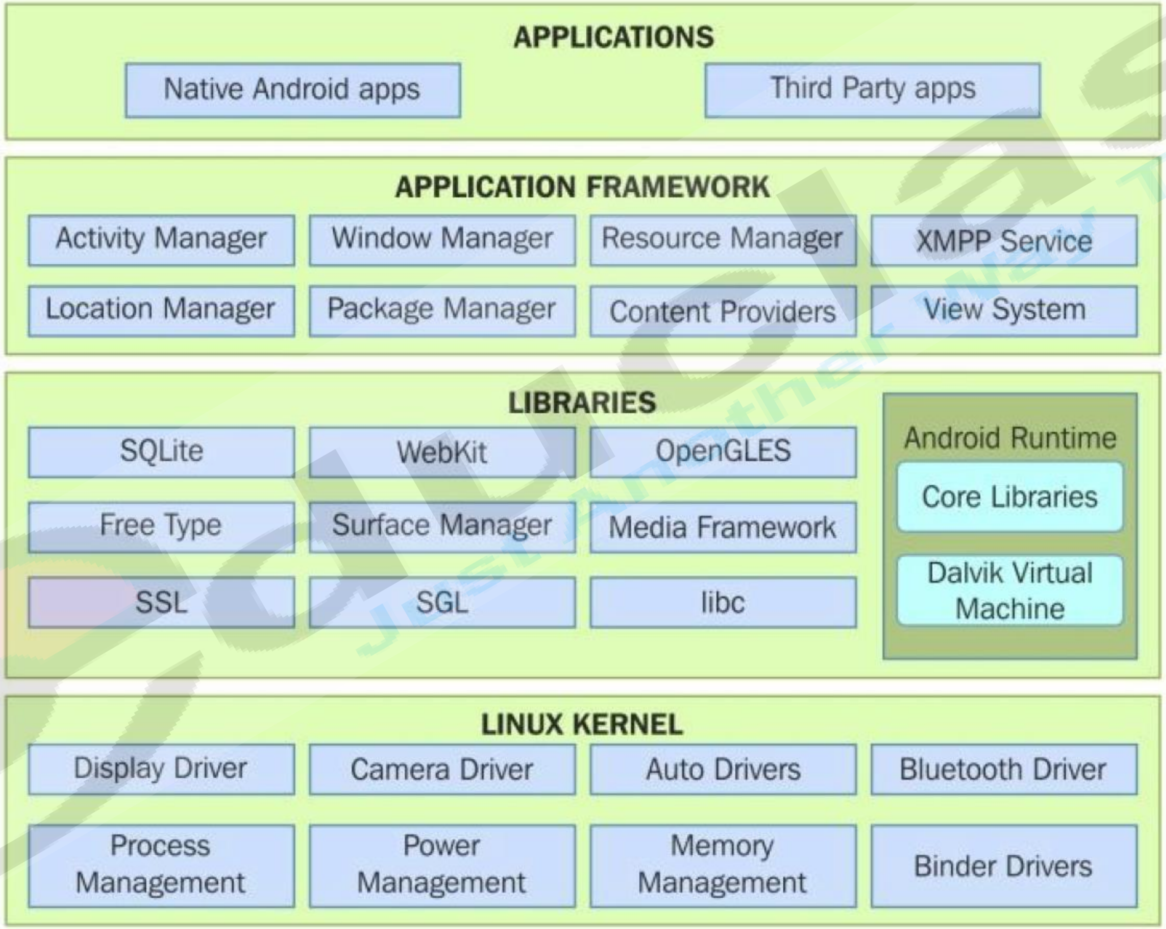
Evidence in the operator ‘s Network

- Along with the data that the examiner / expert extract from the cell phones, the operator maintains logs of calls, SMS , data usage, geographical data like GPS location and may more.
- The home location register is one of the most important element of cell phone network.
- It keeps all the details about the user, identification number IMEI, IMSI, SIM serial number, PUK/PIN code, services subscribed by the user and more.
- The most important is the call details record(CDRs).
- They have an analytical data or information about the calling number and the called number , date, time , duration of the call, cell which served the call and so on.
- This data can be correlated to call log evidence which is extracted from the cell phone.

Android forensics

- Android consist of a stack layers running one above the other.
- Each of these layers performs several operations that support specific operating system functions.
- Each layers provides services to the layer lying above it.

Android Architecture



APPLICATIONS

Native Android apps

Third Party apps

APPLICATION FRAMEWORK

Activity Manager

Window Manager

Resource Manager

XMPP Service

Location Manager

Package Manager

Content Providers

View System

LIBRARIES

SQLite

WebKit

OpenGLES

Free Type

Surface Manager

Media Framework

SSL

SGL

libc

Android Runtime

Core Libraries

Dalvik Virtual Machine

LINUX KERNEL

Display Driver

Camera Driver

Auto Drivers

Bluetooth Driver

Process Management

Power Management

Memory Management

Binder Drivers

The linux Kernal Layer

- Android OS is built on top of the linux kernal with some architectural changes made by GOOGLE.
- Linux is a portable platform that can be compiled easily on different hardware.
- The Kernel acts as abstraction layer between the software and hardware present on the device.
- If user does an action for eg camera click this hardware instruction is converted in to software instruction. The kernel contains driver to facilitate the process.
- Linux kernel is responsible for managing the core functionality of android , such as process management , memory management, security and networking.

Libraries

- The next layer in the android architecture consist of Android’s native libraries.
- The libraries are written in the C or C++ language and help the device to handle different kinds of the data.
- SQLite libraries are useful for storing and retrieving the data from a database.
- Other libraries include Media Framework, Webkit, Surface Manager, SSL and so on.
- The WebKit library provides web pages in the web browser and the surface manager maintains the graphics.

- Android Runtime , which consists of Dalvik virtual machine(DVM) and core libraries.
- The Android runtime is responsible for running application on android devices.

Dalvik Virtual Machine

- All application written on Java Programming language uses JVM as a OS to run a Window OS on a MAC or vice versa.
- In android it uses DVM
- DVM runs Dalvik bytecode which is Java bytecode converted by the DEX compiler.
- Compare with JVM , DVM is more suitable for android and uses low memory and low processing environment.
- Android application runs its won instance of Dalvik Virtual Machine.

The application Framework layer

- The application framework is the layer responsible for handling the basic functioning of a phone, such a resource management, handling calls and so on.
- This is the block with which the application installed on the device directly talk to it
- The following are some of the important blocks in the application framework layer

- Telephony Manager: This block manages all the voice calls.
- Content Provider: This block manages the sharing of data between different application.
- Resource manager: This block help manage various resource used in application.

The application Layer

- This is the topmost layer where the user interact directly with the device.
- There are two application
  - Preinstalled application eg Dialer, Web browser, contacts
  - User installed application eg Play store, Facebook etc.

Data Extraction Technique

- Android Virtual Device
- AVD is also called Emulator has a forensic perspective view.
- AVD helps us to understand how application behave and execute on a device.
- While working a device which is running in a older platform you can design a emulator can be used to find out how the forensic tool works and changes contents of android devices.

- Emulator can help to configure email accounts, install application, surf the internet, send text messages.
- The data created when working on a emulator is stored in your home directory, in a folder named .android.
- Forensic are interest in cache.img, sdcard.img and userdata-qemu.img

Data extraction techniques

- The data extraction techniques on an Android device can be classified into three types:
  - Manual data extraction
  - Logical data extraction
  - Physical data extraction

Manual data extraction

- This method of extraction involves the examiner utilizing the normal user interface of the mobile device to access content present in the memory. The examiner will browse through the device normally by accessing different menus to view the details such as call logs, text messages, and IM chats.
- The content of each screen is captured by taking pictures and can be presented as evidence. The main drawback with this type of examination is that only those files that are accessible by the operating system (in the UI mode) can be investigated.

- Care must be taken when manually examining the device as it's easy to press the wrong button and erase or add data. Manual extraction should be used as a last resort to verify findings extracted using one of the other methods. Certain circumstances may warrant the examiner to conduct manual examination as the first step. This may include life or death situations or missing persons where a quick scan of the device may lead the police to the individual.

Logical data extraction

- Logical data extraction techniques extract the data present on the device by accessing the file system. These techniques are significant because they provide valuable data, work on most devices, and are easy to use.
- the concept of rooting comes into picture while extracting the data. Logical techniques do not actually require root access for data extraction.

- some data may be extracted on a non-rooted device while root access will open the device and provide access to all the files present on the device. Hence, having root access on a device would greatly influence the amount and kind of data that can be extracted through logical techniques.

- Logical extraction can be performed on a device in two ways
  - Using adb pull commands
  - Using content providers

- **Using the adb pull command**
  - adb is a command-line tool that helps you communicate with the device to retrieve information
  - Using adb, you can extract data from all the files on the device or only the relevant files in which you are interested.
  - To access an Android device through adb, it's necessary that the USB debugging option is enabled.
  - If the device is locked and USB debugging is not enabled, try to bypass the screen lock using the techniques.
- The application data can be stored in one of the following locations:
  - **Shared preferences:** Data is stored in key-value pairs in a lightweight XML format. Shared preference files are stored in the shared_pref folder of the application /data directory.
  - **Internal storage:** Data stored here is private and is present in the device's internal memory. Files saved to the internal storage are private and cannot be accessed by other applications.
  - **External storage:** This stores data that is public in the device's external memory, which does not usually enforce security mechanisms. This data is available under the /sdcard directory.
  - **SQLite database:** This data is available in the /data/data/PackageName/database. They are usually stored with a .db file extension

- **Using content providers**
- In Android, the data of one application cannot be accessed by another application under normal circumstances.
- Android provides a mechanism through which data can be shared with other applications. This is precisely achieved through the use of content providers.
- Content providers present data to external applications in the form of one or more tables.
- These tables are no different from the tables found in a relational database.
- They can be used by the applications to share data usually through the **URI addressing** scheme.
- They are used by other applications that access the provider using a provider client object.
- During the installation of an app, the user determines whether or not the app can gain access to the requested data (content providers).
- For instance, contacts, SMS/MMS, calendar, and so on, are examples of content providers.

- **Physical data extraction**
- Android data extraction through physical techniques (hardware-based) mainly involves two methods: JTAG and chip-off. These techniques are usually hard to implement and require great precision and experience to try them on real devices during the course of an investigation.

JTAG

- **JTAG (Joint Test Action Group) involves using advanced data acquisition methods,** which involve connecting to specific ports on the device and instructing the processor to transfer the data stored on the device.
- By using this method, a full physical image of a device can be acquired.
- Examiners must have proper training and experience prior to attempting JTAG as the device may be damaged if handled improperly

Chip-off

- Chip-off, as the name suggests, is a technique where the NAND flash chip(s) are removed from the device and examined to extract the information.
- Hence, this technique will work even when the device is passcode-protected and USB debugging is not enabled.
- JTAG technique where the device functions normally after examination, the chip-off technique usually results in destruction of the device, that is, it is more difficult to reattach the NAND flash to the device after examination.
- The process of reattaching the NAND flash to the device is called re-balling and requires training and practice.

Chip-off techniques usually involve the following forensic steps:

1. All of the chips on the device must be researched to determine which chip contains user data.

2. The chip is then cleaned and repaired to make sure that the connectors are present and functioning.

3. Using specialized hardware device adapters, the chip can now be read. This is done by inserting the chip into the hardware device, which supports the specific NAND flash chip. In this process, raw data is acquired from the chip resulting in a .bin file.

4.The data acquired can now be analyzed using forensic techniques and the tools.

Screen lock bypassing techniques

- Due to the increase in user awareness and the ease of functionality, there has been an exponential increase in the usage of passcode options to lock Android devices. Hence, bypassing the device's screen lock during a forensic investigation is becoming increasingly important. The screen lock bypass techniques discussed have their applicability based on the situation.

- The examiner must have authorization to make the required changes to the device, document all steps taken, and be able to describe the steps taken if a courtroom testimony is required

- there are three types of screen lock mechanisms offered by Android. Although there are some devices which have voice lock and face lock options, we will limit our discussion to the following three options since these are most widely used on all Android devices

- **Pattern Lock: The user sets a pattern or design on the phone and the same must be drawn to unlock the device. Android was the first smartphone to introduce a pattern lock.**
- **• PIN code: This is the most common lock option and is found on many mobile phones. The PIN code is a 4-digit number that needs to be entered to unlock the device.**
- **• Passcode (alphanumeric): This is an alphanumeric passcode. Unlike the PIN, which takes four digits, the alphanumeric passcode takes more than just digits**

Using adb to bypass the screen lock

- If USB debugging appears to be enabled on the Android device, it is wise to take advantage of it by connecting with adb using USB, as discussed in the earlier sections. The examiner should connect the device to the forensic workstation and issue the adb devices command. If the device shows up, it implies that USB debugging is enabled. If the Android device is locked, the examiner must attempt to bypass the screen lock.

- The following are the two methods that may allow the examiner to bypass the screen lock when USB debugging is enabled.
- **Deleting the gesture.key file**
- This is how the process is done:
- Connect the device to the forensic workstation (a Windows machine in our example) using a USB cable.
- Open the command prompt and execute the following instructions:

- **adb.exe shell**
- **cd /data/system**
- **rm gesture.key**
- Reboot the device. If the pattern lock still appears, just draw any random design and observe that the device should unlock without any trouble.

- This method works when the device is rooted. This method may not be successful on unrooted devices. Rooting an Android device should not be performed without proper authorization as the device is altered

- **Updating the settings.db file**
- To update the settings.db file, perform the following steps:
- Connect the device to the forensic workstation using a USB cable.
- Open the command prompt and execute the following instructions:

- **adb.exe shell cd /data/data/com.android.providers.settings/databases**
- **sqlite settings.db**
- **sqlite>update system set value=0 where name='lock_pattern_autolock';**
- **sqlite>update system set value=0 where name= 'lockscreen.lockedoutpermenantly';**
- Exit and reboot the device.
- The Android device should be unlocked. If not, attempt to remove gesture. key as explained earlier