Mobile And Digital Forensics

Satvik Gupta

May 10, 2023

Contents

satvikgupta.com

Risks Created By Wireless Technology

1. Wireless is shared and uncontrolled.
2. Mobile devices are transient. They are always moving around. Detecting suspicious activity becomes difficult.
3. Ease of use - As wireless is easy to use, people become familiar with it and become comfortable and careless with security.
4. It's easier to attack.

Wireless Technologies in Use

PAN (Personal Area Network)

- WPANs are used in short distances, <10 m.
- Connect computers and peripherals
- High speed

Satvikgupta.com

Bluetooth

Infrared

- Line of sight
- Short range (0-2m)
- LoS makes it easy to think it's secure, but attackers can detect reflected light and filter out ambient noise, and gain access to the data.

Ultrawideband (UWB)

- Superfast, wireless.
- Doesn't use any carrier wave.
- Superfast pulses in timed sequences over a large continuous spectrum

ZigBee

- Home Area Network
- Designed to replace remote controls
- Cost effective, low power

Wireless USB

- 10m range
- 480 Mbps, upto 1 Gbps in future.

LAN

Wireless Local Area Networks

802.11

- AKA Wifi
- 1-2 Mbps, 2.4 GHz

900 MHz Packet Radio

- Cordless, pagers, medical equipment.
- Interference sometimes happens
- Transports IP based data.

MAN

A Metropolitan Area Network is designed to provide broadband connectivity to a densely populated area. Could be cities, counties, campuses. AKA *Last Mile Solutions.*

Microwave

- P2P,LoS
- AM Radio
- Less cost, Easy to Deploy
- High frequency

Free Space Optics

- Uses lasers instead of radio frequency
- High data rates
- Incorporates security of Fiber optic cables
- Transmits a LoS laser btw two points.

saurikgupta.com

Ricochet

- Wireless ISP network solution for a particular geographic location
- Allows portable clients to move through an area and access Internet

WiMax

Worldwide Interoperability for Microwave Access, 802.16

- 2-11 GHz
- Long range
- High throughput ~70 Mbps

WANs

WANs are intended for communications between mobile and fixed devices worldwide.

Satellite

Use radio waves just like other wireless technologies. TElevision, GPS< ISPs, etc.

Cellular

- Cellular Digital Packet Data (CDPD)

  Uses unused cellular channels to transmit data packets.
- Global System for Mobile Comm. (GSM)

  Uses narrow band TDMA method to allow 8 simultaneous calls on the same radio frequency.
- 3GSM

  Will support multimedia, video, and Internet
- TDMA

  Each cellular channel is divided into 3 time slots to increase amount of data.

Blackberry

Email, File sharing, Voice and SMS, Calendar, Internet, Attachments, etc. btw Blackberry users.

Paging

SMS

Wireless Network Security Threats

Eavesdropping

Someone else can read the transmitted information, even from outside the building.

Traffic Analysis

Patterns of communication and data flow can be monitored and may yield information.

Data Tampering

Information can be deleted, or modified via MITM attack.

satvikgupta.com

Masquerading

Attacker can impersonate an authorized user and gain access to information.

Denial of Service (DoS)

Attacker can jam frequency channels, using hardware blockers or by sending large amount of requests.

Wireless Client Attacks

Attacker can trick clients into connecting to an unsecured network and gain access to the data present on the client machine. The compromised client can now also be used to access the internal network and the data stored on it.

Other Issues with Wireless

Spread Spectrum isn't Secure

Spread Spectrum is a modulation technique used to prevent radio jamming.

In general, spread spectrum has **spreading codes**, that can be changed. Without knowing the correct code, it is impossible to decipher data sent through the spread spectrum.

However, the 802.11 standard publicly describes the spreading codes so that interoperable 802.11 components can be created. An attacker with a radio compliant with 802.11 would be able to connect.

SSIDs are not designed as passwords

SSID - Service Set Identifier.

- Were initially used to prevent people from connecting to the access point (AP) without knowing the SSID.
- However, they should not be relied upon as passwords.

WEP is weak

Wired Equivalent Privacy.

WEP occasionally produces cryptographically weak ciphers.

Steps to attack WEP.

1. Hacker runs Kismet to discover WLANs in the area. He gets its SSID, channel number and its BSSID (Basic SSID - the Ethernet Address).
2. APs can hide their SSIDs, using an option called SSID Cloaking/SSID Broadcast Disable.

   If this is the case, the attacker has to wait for a client to connect to the AP (the client and the AP will both disclose the SSID). The attacker can also force an already connected client to reconnect. This is done by sending a packet to the client, pretending to be from the AP. The packet tells the client that they have lost their connection with the AP (***You are no longer connected***). The client attempts to reconnect, and exposes the SSID.
3. The attacker puts his wireless card into Monitor mode. The card will eavesdrop on the WLAN (even without connecting to it.) He makes the card monitor the channel on which the target AP is. All the traffic monitored is saved in a *capture file.*
4. WEP uses Initialization Vectors (IVs), which are values used to start a cryptographic process. When a certain number of weak IVs have been captured, we can determine the WEP key. 125k packets are needed to crack 40-bit WEP keys. 200-250k packets for 128-bit WEP keys.
5. If the WLAN is slow, the hacker will need to accelerate the attack to capture the right amount of weak IVs. The attacker will inject already captured WEP frame back into the network. WEP has no replay protection mechanism.

satvikgupta.com

512 packets injected per second - 10 mins for 40-bit keys, 30 mins for 128-bit keys.

6. After sufficient amount of IVs are captured, the attacker runs AirCrack, which will attempt to crack and return the WEP key. Once the key is known, the attacker can connect to the AP in the same way a legitimate client would.

War Driving

People driving around in a car equipped with wireless gear, looking for unsecured wireless network. Generally they try to look for APs that are running a certain kind of server behind them, such as important security servers or financial servers, etc.

Sometimes people just do it harmlessly, for e.g, just checking the radio environment.

War Chalking

War driving + marking the places with chalk. Different symbols are used for open, closed, and WEP APs.

War Flying

War driving, but using airplanes,helicopters, etc. instead of cars. Due to increased range of wireless networks, hundreds of APs can be found in a short trip.

Security Recommendations vs Reality

Recommendation	Reality
Turn SSID Broadcasting off	SSIDs can be easily discovered as described above.
Use static IP Addresses	Static IP addresses can be found easily using traffic analysis
Turn 128-bit WEP on	WEP can be easily cracked
Change WEP keys	New keys can be cracked easily
Enable MAC Address Filtering	Traffic analysis will yield the authorized MAC Addresses. WLAN cards can specify their own MAC Address, so hackers can just claim to be using an authorized one
Utilize shared key auth	WEP keys can be cracked
Use personal firewalls	Hackers may be able to fool you that they are a trusted system
Use SSH/HTTPs	May be vulnerable to MITM sometimes

satvikgupta.com

PDA (Personal Digital Assistants)

Common attacks:

1. Copying/Stealing information from the device
2. Loading malicious code onto the device
3. Destroying key files or applications on the device

Trojans

A program disguised as another program.

Worms

Programs that duplicate themselves over and over, and steal system resources in doing so.

Logic Bombs

Programs within programs that perform certain actions based on a trigger event. PDAs can also be carriers of such programs instead of the target.

Theft of the Device

Data Theft

Data can be easily copied from a PDA/Blackberry to a flash card within minutes.

Mobile Code

S/w transmitted from server to a local device, and then executed. This code may give the attacker access to the data on the PDA.

Auth Theft

Stealing a PDA may lead to auth information being stolen.

DoS Attacks

Any attack in which an organization is denied access to a resource can be termed DoS. For PDAs, anything from mobile code to device theft can be considered DoS.

Session Hijacking

A TCP session can be taken over by an attacker. TCP auth only occurs during the start, so an attacker can find ways to do this.

Providing Security to PDAs

- Use AntiVirus - Norton, Symantec, F-Secure, Kaspersky
- DB Security and Auth
- Faraday Bag - Block all wireless signals to the device
- Encryption - Ccrypt, PDA Secure
- Firewalls - Mobile Firewall Plus
- Password Enforcement - HotSync Security, PDA Defense.
- VPN - VPN 3000, Movian VPN

sotvikgupta.com

Best Security Practices

1. Define handheld security policy
2. Centrally enforce and monitor handheld security
3. Enforce use of power-on passwords
4. Block unauthorized handheld network activity
5. Detect handheld intrusions
6. Protect handheld integrity
7. Encrypt sensitive data stored on handhelds
8. Protect traffic sent/received by handhelds
9. Maintain up-to-date anti-virus protection
10. Back up frequently

SMS Security Issues

SMS is a store and forward service. The SMS is stored in a server first, before being forwarded to the receiver. This is necessary in case the receiver's mobile phone is out of coverage or switched off when the SMS is sent.

- **SMC** - Short Message Center. This is where the SMSes are sent to be stored, before they are forwarded.
- **SME** - Short Message Entity. This is an application or program that generates an SMS message. It can be a mobile phone, a computer, or a service network.
- **GMSC** - Gateway Short Message Service (Actual full form is Gateway Mobile Switching Center)- acts as an interface between different networks. It uses the HLR (Home location register) to determine the recipient's network, and forwards the message there.

Availability Issues

- Many attacks try to create a DoS scenario.
- They may send thousands of messages to a particular user, using software or the Internet. If it is an older device, it's memory will fill up and it will be unable to accept more messages.
- With modern devices, the recipient will have difficulty identifying which SMSes are real and meant for him, and which are fake.
- The attacker may trick the OS/device into blocking actions until the SMSes are deleted. These messages usually contain special characters or symbols, long names, or do not follow standard structure for an SMS message.
- Silent DoS is also possible, where the phone works normally but doesn't receive any SMS.
- Continuous messaging can also drain the battery.
- DoS can be done by installing a fake base station, or a jamming device that makes the user unable to send or receive SMSes.
- Sometimes DoS can happen without any attack on the system, for e.g, on holidays when millions of SMSes are sent together which causes delay and overload in the system.

Confidentiality Issues

- Encryption for SMS/Voice calls are usually done between the phone and the provider network (if done at all). Once in the network, the data is unencrypted. Employees of the provider may have access to it.
- An attacker can hack an employee's mobile phone to gain access to the network and view other people's SMSes.
- Fake base stations can also be used by attackers to intercept and read SMSes. The attacker can also forward the SMS to the actual recipient to avoid any suspicion, using various techniques to hide his identity (SMS Masquerading)
- Even without knowing the content of SMS we can learn about the user's habits, such as when they switch their phone off and when they switch it on. A switched off phone will not receive an SMS, and the SMS will be marked as *delivered* only after the phone is switched on.

  Attackers usually send *invisible* messages for this purpose, which do not show anything on the screen and don't show any notification either.

satvikgupta.com

- Mobile operators are sometimes required to share details of SMSes viewed and sent by a person for law enforcement. Even without operator's help, there are ways to view deleted messages from a device.

Integrity Issues

Integrity issues are those relating to an SMS's content being changed, or the sender is pretending to be someone else.

- **SMS Spoofing** is when a sender masquerades as another sender. Using the internet we can send messages in bulk using a number of our choice. Since this can be abused, operators now ask for some alphabets to be added in the ID along with digits. To combat this, fraudsters are using O instead of 0 and I instead of 1. The catalog's functionality can also be exploited, as the catalog only matches the last 4 digits. So, an attacker sending a message using AA5483 will be matched by a catalog containing an entry for 88885483
- Attackers can also connect directly to a messaging center and use spoofing techniques to hide their identity, and pretend to be someone else. We can check if the number of the SMS, and the country of the message center match. For e.g, if the number is from Greece, but the message center is from Japan, we can figure out something is wrong. Timestamps can also be used, since message centers timestamp using their local time. If a message arrives from an Indian number , to an Indian receiver, with a timestamp of 2 hours before, we can guess that something is wrong (since it should have the same timestamp as the current time)
- Cipher can be used to change phone settings, such as turning ciphering indicator on or off.
- Special binary messages can also be sent using SMS. They don't appear to the user, but go directly to the phone or SIM card. OTA updates of software were done using this method, but this can also be exploited by hackers.

Other Security Issues

- SMSes that can be modified/deleted later, but stay in the same memory location. Their initial use was for stuff like news, stocks, weather, where the SMS's content would change daily and the user wouldn't have to wait for a new SMS to arrive. They can obviously be misused.
- SMSes that show on the screen directly without any warning (flash SMS), without the user going into messages. These make the user think these are from the provider and hackers can trick users into calling certain numbers or paying money, etc.
- SMSes can be used to influence outcome of contests or voting procedures that allow SMS. Bulk messages can be sent for a particular participant.

SMS Spamming

- Spam is unsolicited commercial messages from unknown senders.
- Spam is profitable and can be completely anonymous.
- Internet sites allowing users to download free ringtones ask for their phone number, then sell that phone number to spammers.
- SMS spam filtering is more difficult than email spam filtering because SMSes are short so we have less information. ML algorithms such as Bayesian networks have proven effective.
- Techniques of protecting SMSC from spam sometimes use blacklisted words, which ends up blocking legitimate messages containing those words. Challenge/response protocols have been suggested.
- Many providers allow users to report spam, or stop SMS service altogether. Some also allow SMS aliases. Only messages sent to the alias are delivered, those sent to the number aren't.

A promising scheme is shown below.

Satvikgupta.com

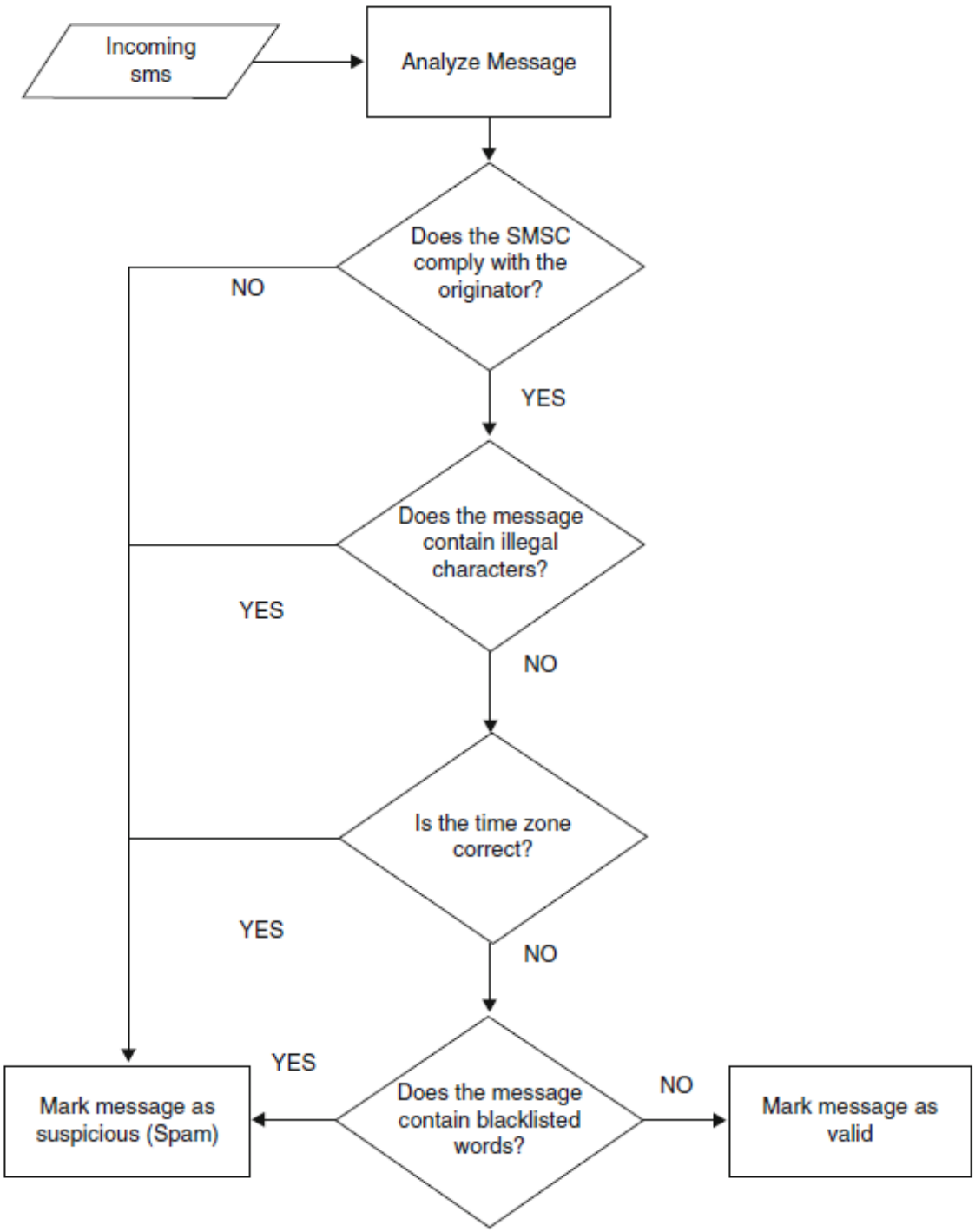

Figure 1: image-20230509195001350

1. Originator's phone number and the SMSC used are compared. If the originator sent a message earlier using a different SMSC, the message is marked as suspicious.
2. SMSC and originator country is checked and compared.
3. SenderId is checked. Non-numerical IDs have a greater chance of being spam.
4. Timezone is checked. If the sender and receiver country are same, but the timestamp from SMSC is more than 1 minute ahead, the message is suspicoius.
5. Keyword blacklist.

6. HTTP links are checked.
7. SMS Protocol is checked (TP-PID). Some SMSes, such as silent SMSes, which get deleted upon reception. The application notifies the user of such SMSes, even though it has been deleted.

Mobile Phone Forensics

Crime in Mobile Phones

- Communication method for criminal activity
- Device theft
- Harassment calls
- Mobile phones can be used as a detonation mechanism
- Telecommunication fraud
- Identity theft
- Industrial espionage (using data stored on the device, or using the device as a bug)

Sources of Evidence

We can find evidence on a mobile device in the following places

- Phone catalog/contacts
- Call history
- SMS/MMS
- Photographs and videos
- Emails
- Calendar
- Reminders
- Browser history
- Documents
- GPS information
- Memos/Reminders/To-do-lists

Data can remain in places even after it has been deleted.

Forensic Procedures

When dealing with digital evidence,

- All general forensic principles must be applied.
- Actions taken on digital evidence should not change it
- Only trained people should be able to access the evidence in its original form
- All activity done on a device, such as seizure,storage, transfer must be documented.
- All processes performed on the device must also be recorded. A third party must be able to examine these processes.

General Principles

- Maintain data integrity
- Document and photograph everything on the scene
- All actions done on the device or to the device must be documented and must be available for audit.
- The mobile phone's screen should be photographed as it was found.
- Evidence should not be altered.
- Analysts should be trained.
- Each evidence holder is responsible for anything that happens to it.
- Procedures should be completed as quickly as possible.

Training and Competence

- All involved people should be trained to perform and document actions.

satvikgupta.com

- Different people will need different training. E.g, police officer needs to know how to properly secure and seize the phone. Analyst needs to know how to get the data from the phone without changing it.
- Involved people should keep themselves updated with latest technology and research.
- Practice with the same kind of device and software first.
- Head office must maintain constant communication with analysts and provide guidance.

Analysis Procedure

- We want to know the *who, when, where,why.* Data is examined, including application files, timeline is established for events, and hidden data is also looked for.
- We try to avoid any data loss.
- First thing to do is to ensure the phone is isolated from the network.
- If the phone is on, memory and SIM card is examined first.
- If the phone is off and the owner doesn't reveal the pincode, we need to ask for help from the provider.
- Each step should be photographed or videoed, even in the case of automatic data analysis.
- If the phone was deactivated, SIM analysis takes place first. Activating the phone may cause change in data, such as in Location Area Information file. If we place a different SIM, we may lose data such as call history.

Preserving data and isolating from network

- Only qualified software should be used.
- If the phone is not compatible with specialized software, test the methods on a test phone first before executing it on the real device.
- New data from the network, such as phone calls, emails, SMSes, etc. must be avoided. They an also be used to delete or modify the data on the device. Therefore, we need to isolate the device from the network.
- Best solution is to use a Faraday cage.
- Phone should be charged constantly to avoid it turning off. We need to avoid any signal entering the phone using the charging cable. This is done by placing a power source inside the Faraday cage
- Jammers can also be used instead of Faraday cages.
- In modern phones we can also use flight mode.
- We can collaborate with the network to disable network access to the phone. We can also use a special SIM that activates the device but doesn't allow network access. This may lead to loss of data such as call logs.

Identify the phone

- Try to identify it visually
- Look up different mobile phones' photographs online
- Take out the battery and see the IMEI and MAC address, and identify using those.
  - Typing *#06# also reveals the IMEI
- User manuals and characteristics of the phone must be studied, so we know what kind of data loss is possible. Test device is still recommended,
- Use manufacturer's cables instead of local ones. Connecting via WiFi and Bluetooth should be avoided as it will write data to the phone's memory.

Examine SIM Card and Memory

- Get PIN for phone and sim from user. If user doesn't cooperate, contact provider.
- User should not be allowed to touch the phone
- SIM provides access to its data through its own microcontroller, therefore it cannot be cloned. The analysis has to take place on the original SIM card.
- Hashes are used to check if two sets of files are identical or not.
- The process must be filmed.
- Extracting the sim generally involved removing the battery, which may lead to loss in data. In these cases, the data in the mobile must be analyzed before the SIM card.
- After extraction of data with automated tools, manual extraction must also be done to find data that the software missed.
- Extracted evidence must be verified, such as with the network operator.

satvikgupta.com

SIM Card

- Cannot be cloned
- Contains EEPROM memory
- SIM is protected by 4 or 6-digit PIN that the user can set. After 3 wrong entries of PIN, the SIM will lock itself. To unlock it, we need a PUK (Pin Unblocking Key), which is an 8-digit key. After 10 unsuccessful entries of PUK, the SIM card will become unusable.
- PUK and PIN are both initially set by the SIM manufacturer, but the user can change them.
- ADM code is known only to the manufacturer, and it provides complete access to all data as well as their modification.

Files Present in SIM Card

- Files are present in directories and subdirectories, similar to in computers.
- MF stands for Master File and represents the root directory. DF (Dedicated File) are subdirectories. EF (Elementary File) are the actual files.
- Some files can be read without any authentication. Some need the SIM PIN. The most important files need the ADM code which only the provider has.

SIM contains many files such as:

- Card's serial number
- List of providers and their names
- Default network
- Default language
- Contacts
- Messages
- Settings for messages
- List of last outgoing calls
- Temporary identity (IMSI-TMSI) (International Mobile Subscriber Identity - Temporary Mobile Subscriber Identity)
- Coarse location (Location Area Identifier)
- Control Channels (BCCH)
- Current Encryption Key (K_c)

Around 100 files are present, but each provider can also add their own files. Users generally can't access or delete these files, which makes them important.

IMSI

International Mobile Subscriber Identity (15-digit number) is used to uniquely identify the SIM internationally.

It consists of MCC + MNC + MSIN.

MCC - Mobile Country Code (3-digit). MNC - Mobile Network Code (2-digit , 3-digit for USA and Canada). MSIN is 10 digit (9 in USA/Canada)

ICCID

Integrated Circuit Card Identifier. It is a unique serial number that is printed on the plastic wrapping of the card. It identifies the actual printed circuit.

It consists of :

89 + MCC + MNC + Serial Number

89 is fixed and represents that this circuit (the SIM) is used for telecommunication.

Location Information File and BCCH File

- LIF (Location Information File) stores the last TMSI and last LAI. TMSI is a temporary identity that is used for security purposes, so we don't transmit the permanent identity of the user again and again.

saurikgupta.com

- LAI = MCC + MNC + LAC (Location Area Code)
- LAC gives a wide area which can have many phones.
- BCCH list stores the current BCCH and its six neighboring channels. By combining BCCH and LAC information we can get a better idea of where the phone was.

SMS Storage File

Modern SIMs can store SMS, usually upto 35. The first byte of each SMS storage slot tells the message's status.

00000000 - Empty Slot

00000001 - Read incoming message

00000011 - Unread incoming message

00000101 - Outgoing message that has been sent

00000111 - Outgoing message which hasn't been sent.

If a message is deleted by the user, usually the first byte's last bit is changed to 0, which marks the slot as empty. But the actual content of the slots aren't changed. So, by reading data directly, we can sometimes get old messages that the user thinks have been deleted.

Another file stores SMS Settings, such as the default alphabet, message center number, etc.

Contact List

SIM Cards can store contacts. Old SIMs stored upto 100, newer ones offer 250. When a contact is deleted, the slot is filled with binary "1", so deleted contacts cannot be recovered. But slots are assigned in order, so if we find an empty slot between slot 34 and 36, we can assume there was a contact in slot 35 that has been deleted.

Outgoing Calls

SIMs can store the last 10 dialled numbers. Most manufacturers prefer to use the phone's memory of this. SIM doesn't store incoming calls, only outgoing.

Device Data

- Contains messages, emails, IMEI, call logs, contacts, pictures, application files, etc.
- Deleted information can be recovered from the depths of memory.
- Data should be recovered without altering
- Memory can be cloned, unlike with SIM
- Official and unofficial tools exist for memory cloning.

Issues :

- Hard to detect whether there have been changes in memory during our procedures
- During memory dumps, positions of files may change
- Searching for information in large memory dumps is difficult and time consuming
- Phones may have encrypted memory

External memory dumps, that use hardware, can be used. In this, the memory circuits are desoldered from the phone. This ensures no changes occur while doing memory dump. This is less used because we may damage the whole memory while performing desoldering.

External memory cards may be present in the device. Extracting data from these is fairly easy.

Evidence in Operator's Network

The SIM card operator may also have evidence in their database.

- Call logs
- SMS exchanged
- HLR keeps data about IMSI, SIM serial number, PIN and PUK code, etc.

satvikgupta.com

- Call Detail Records (CDR) have all information about the numbers called - date, duration,etc.

satvikgupta.com