

Prepared by Dr. Nermin Ewais

CYB 770
IT Forensics

Lecture 09



Social Media and Mobile Forensic

Lecture 09

CYB 770
IT Forensics

Prepared by
Dr. Nermin Ewais

- Social Media Forensic
- Mobile Forensics
 - Phones Devices
 - Service provider
 - Sim Card

Social Media Forensic

What is social media?

- Social media is the use of applications or programs that a user can use to create and share information, forms of expression, opinions, ideas, and so on through virtual communities through the global internet.
- Users can access social media through web-based technology such as a mobile device application.

- The majority of the social media that the artifacts will not be saved to the user system.
- The applications store the data in the service provider's cloud, which is a fancy way of saying the data will be on the service provider's servers.



The following is a short description of some popular social media applications you may come across during your investigations:

- **Facebook:** The most extensive social media application with nearly 2,000,000,000 users. It combines commercial advertisers and consumer users with their content. It is easy to use. Users can upload images, recorded videos, live videos, and chat via the messenger application.
- **Instagram:** A photo and video sharing social media application. Users can share photos and recorded videos and live videos. Users can also chat and comment with other users via the app.

- **Snapchat:** A video/photo-sharing social media application. Initially, when a user sent a "snap" after the recipient viewed the image, it would be deleted from the system. Now, users have the option of saving "snaps."
- **Twitter:** Social media application used for news, politics, sports, entertainment, and so on. Twitter allows 280-character tweets, with longer tweets being linked in the following messages.
- **WhatsApp:** A messaging application with the ability to send pictures/videos.

- **Telegram:** is a popular cross-platform messaging app that is widely used because it offers some enhanced privacy and encryption features as well as support for large group chat features.
- **Tumblr:** A blogging/social networking application. Users can post pictures/videos to a blog page.
- **Tinder:** A location-based social media application used as a dating service. Users "swipe right" or "swipe left" on profiles they like/dislike. If both parties "like" each other, then they can chat using the app.

- The application of computer investigation and analysis techniques to gather evidence from online sources suitable for presentation in a court law

Objectives

- **Identify digital evidence** related to a case.
- **Preserve evidence** in a forensically sound manner.
- **Analyze posts, messages, images, videos**, and metadata.
- **Reconstruct timelines** of user activities.

Sources of Evidence Investigators may extract and analyze:

- **Posts, comments, likes, shares**
- **Private messages** (if legally obtained)
- **Deleted content** (when recoverable)
- **Profile data** (bio, friends list, connections)
- **Photos and videos**
- **Hashtags and search history**
- **Network connections and interaction patterns**

Social media investigators have a variety of strategies for collecting and analyzing social media information, such as:

- Manually visiting social media account pages.
- Printing or taking screenshots.
- Downloading copies of photos or files.
- Accessing open source or other software programs to collect and preserve information.
- Subpoenaing or obtaining a court order for production of additional information and documents.

Challenges

- **Privacy restrictions**
- **Encrypted messages**
- **Fake profiles / identity spoofing**
- **Frequent platform updates and security features**

Here are tools designed to make your online investigations more successful and efficient:

- **WebPreserver:** Collect and preserve social media evidence in defensible format
- **Makeawebsitehub:** Identify the latest social media apps and platforms
- **Pipl Search:** Find public records, online data, and other information related to an individual
- **TinEye:** Use reverse image search to find the source of an online picture
- **TweetBeaver:** Use Twitter analytics to understand an account and identify connections

- **WebPreserver**

<https://youtu.be/gNLHue6TydM>

Mobile Forensics

- Mobile devices perform an array of functions ranging from a simple telephony device to those of a personal computer.
- Designed for mobility, they are compact in size, battery-powered, and lightweight.
- Most mobile devices have a basic set of comparable features and capabilities.

Depending on your phone's model, the following information might be stored on it:

- Incoming, outgoing, and missed calls
- Multimedia Message Service (MMS; text messages) and Short Message Service (SMS) messages
- E-mail accounts
- Instant messaging (IM) logs
- Photos, videos, and music files
- Calendars
- Social media account information
- GPS data
- Web pages
- address books
- Voice recordings and voicemail
- Access to your home
- Bank account logins

- Different mobile devices have different technical and physical characteristics (e.g., size, weight, processor speed, memory capacity)
- Mobile Devices have a microprocessor, read only memory (ROM), random access memory (RAM), a radio module, a digital signal processor, a microphone and speaker, a variety of hardware keys and interfaces and a liquid crystal display (LCD).
- The operating system (OS) of a mobile device may be stored in either NAND or NOR memory while code execution typically occurs in RAM.

Mobile Hardware

Phone category	Smart Phone features
Processor	Superior speed (~1GHz dual-core)
Memory	Superior capacity (~128GB)
Display	Large size color, 16.7 million (~24-bit)
Card Slots	MicroSD MicroSDXC
Camera	Still, Panoramic, and Video (HD)
Text	Input Numeric Keypad, QWERTY-style keyboard Touch Screen, Handwriting Recognition, QWERTY-style keyboard
Voice Input	None Voice Recognition (Dialing and Control)
Cell Interface	Voice and Limited Data Voice and High Speed Data (4G LTE)
Positioning	GPS receiver GPS receiver
Wireless	IrDA, Bluetooth, WiFi, and NFC
Battery	Fixed/Removable, Rechargeable Li-Ion Polymer

Mobile Software

OS	Android, BlackBerry OS, iOS, Symbian, WebOS and Windows Phone
PIM (Personal Information Management)	Phonebook, Calendar and Reminder List
Applications	Applications (e.g., games, office productivity and social media)
Call	Voice, Video
Messaging	Text, Enhanced Text, Full Multimedia Messaging
Chat	Enhanced Instant Messaging
Email	Via POP or IMAP Server
Web	Direct HTTP

Mobile Forensic Process

Identification

- Identify the purpose of investigation
- Identify the resources required

Preservation

- Data is isolate, secure and preserve

Analysis

- Identify tool and techniques to use
- Process data
- Interpret analysis results

Documentation

- Documentation of the crime scene along with photographing, sketching, and crime-scene mapping

Presentation

- Process of summarization and explanation of conclusions is done with the help to gather facts.

Objectives

- Recover **deleted or hidden data**
- Extract **call logs, contacts, messages, images, videos, and app data**
- Preserve evidence using forensically sound procedures
- Collect **location data, metadata, and timestamps**
- Analyze user activity and behavior
- Reconstruct timelines of events related to an investigation

**Internal Memory**

RAM, ROM or flash memory (NAND / NOR) is used to store mobile phone's OS, applications and data

**SIM Card**

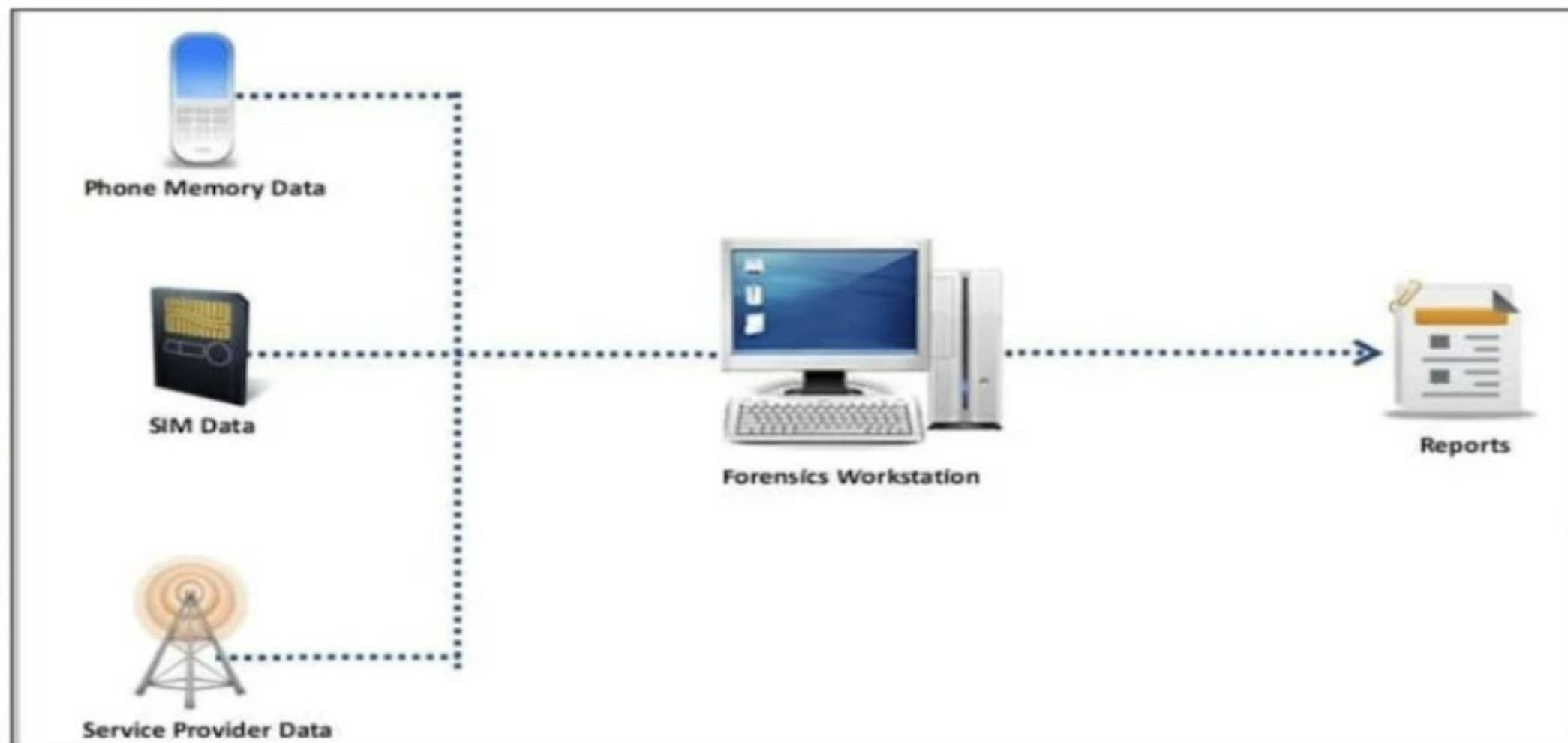
Stores personal information, address books, messages, and service-related information

**External Memory**

Stores personal information such as audio, video, images, etc.

Types of Mobile Evidence Common sources include:

- **Device data:** contacts, call logs, SMS, MMS
- **App data:** WhatsApp, Telegram, Facebook, Instagram, TikTok
- **Browser history & downloads**
- **Multimedia:** photos, videos, audio recordings
- **GPS and location data**
- **Deleted files** (when recoverable)
- **Network data:** Wi-Fi, Bluetooth, cell tower logs
- **SIM card data**
- **Cloud backups** (Google, iCloud)
- **System logs and configuration files**



Phone

Set Of Switching for On/Off

On State

- If The device is “On” , do Not turn it “OFF” , turning it “Off” could activate lockout feature.
- Write down all information on display (photography, if possible)

OFF State

- If the device is “OFF”, leave it “OFF”
- Turning it on could alter evidence on device (same as computer

- Mobile device should be protected from signal **Interruption**, data overwriting
- Use **signal Containment** devices and bags to achieve and maintain network isolation



- **Faraday Bag** : prevent any signal from being sent to or reaching the mobile phone.
- **Signal Disruption Bag/Wireless StrongHold Bag** : It Prevents any type of signal from reaching mobile device.



- **Arson Cans** : are mainly used in the mobile investigative process to prevent someone connected to the crime from hitting the with a text or email 'bomb' that floods the phone's memory with message that crowd out all other previous calls from the log.



- **Aluminum Foil** : the mobile devices is wrapped with three layers of aluminum foil to prevent an incoming signal and making data secure.
- **RF-shielded box**: it preserve the mobile device against radio frequency (RF) interferences resulting form noisy environmen



- A forensic investigator should not directly work on the original evidence. He/she should instead create a **forensic image** of the mobile device obtained at the crime scene
- **File carving** and **forensic analysis** is conducted on forensic image in order to leave the actual evidence intact

- **Forensic imaging** is an accepted standard of every company for the preservation of mobile-based evidences. The forensic investigator should not directly work on the actual evidence.
- The investigator needs to create an image of the mobile internal or external memory.
- Creating a forensic image is difficult since the data may change due to continuous mobile updates.
- An investigator may copy the content onto a separate hard device.
- The image tool such as : FTKImager, EnCase and Smart used to create a forensic image.

- **AccessData FTK Imager** is a forensics tool whose main purpose is to preview recoverable data from a disk of any kind. It can also create perfect copies, called forensic images, of that data.
- This powerful tool can create forensic images of local hard drives, floppy disks, Zip disks, CDs, and DVDs, entire folders, or even of individual files from various places within the media storage device.
- The fact that it can export files and folders from the created image means that this application can also recover data on its own (in some circumstances).

File carving

- File carving is a process used in computer forensics to extract data from a disk drive or other storage device without the assistance of the file system that originally created the file.
- It is a method that recovers files at unallocated space without any file information and is used to recover data and execute a digital forensic investigation.
- It also called “carving,” which is a general term for extracting structured data out of raw data, based on format specific characteristics present in the structured data.

- **The IMEI (International Mobile Equipment Identity)** is a unique number to identify GSM, WCDMA, and iDEN mobile phones, as well as some satellite phones.
- Mostly phone have one IMEI number, but in dual SIM phones are two.
- The **IMEI number** is a unique 15-digit code that precisely identifies the device.
- This number is an individual number assigned to each and every phone all over the world.

How to find this number:

- Dial *#06# on your keypad and press call or send button, your IMEI number will be retrieved and displayed on your screen.
- On the back or bottom of the device or under, IMEI number can be found printed.
- IMEI numbers can also be printed on the original packaging of your device.

- *#06#
- [IMEI CHECK - Free Online IMEI Number Checker | IMEI.info](#)



Dial *#06#



Under batter or package of device

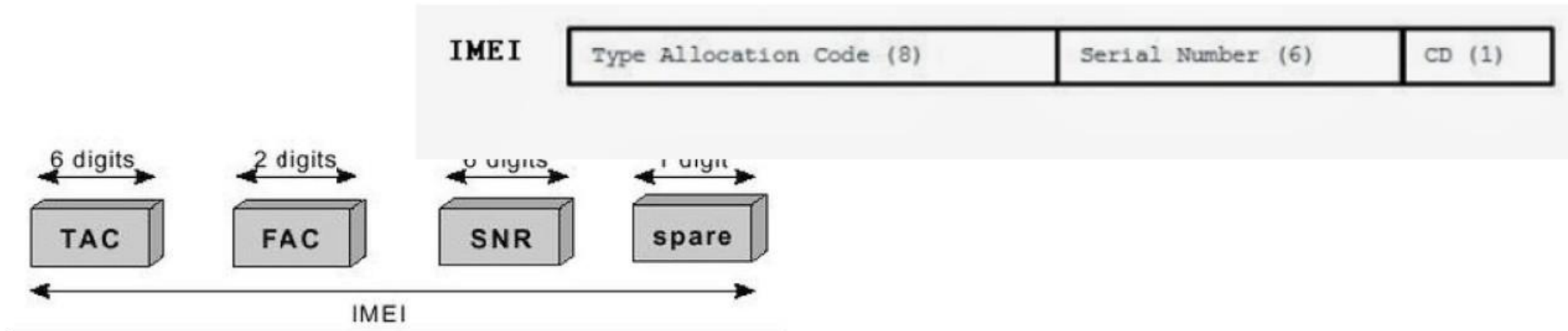
Sencomputing



Why would you need to check the IMEI Number?

- The number is useful when you would like to send the device for service to fill out warranty forms.
- Besides that, if you want to report a stolen or a lost phone at the police or network operator you should use the IMEI Number as well.
- After that, you can block your phone and it will make the device unusable, regardless of whether the SIM card is changed or removed.
- What is also really important is that IMEI contains a few secret information about the product but also sometimes allows you to locate the smartphone.



The Structure of an IMEI Number:

1) Type Allocation Code (TAC) : It is of 8 digits, tell the type of device, which governing body has approved it and Manufacture/Assembler of Device. Last 2 digit of TAC called as Final Assembly Code denotes the manufacturer or assembler.

2) Serial Number (SN) : This is used to uniquely identify the equipment within a TAC

3) Check Digits/Spare Digit (CD/SD): This digit is used to avoid Transmission error.

For example, a IMEI number: 354230061155201

Here TAC: 354230 | FAC: 06 | SNR: 115520 | CD: 1

Service Provider Data

- **Service Provider Data** contains information such as call history and text message, including the date and time.
- It can act as backup evidence when the user deletes the content from his mobile.
- The mobile forensic investigator should request the service provider to release data at the time of incident .

- This helps investigators pinpoint the exact location of the mobile device at the time of the incident in a situation where a user turns off the Geo location feature in the mobile.
- Investigators should investigate both the service provider data and the data found on the mobile phone, to find potential evidence.

Call Detail Record (CDR): contains information about user activities with the mobile phone.

The service providers records and store this information in their database.

The call data record contains several categories of information such as :

- Call telephone number or numbers
- Name and addresses of the subscribers or registered users
- Date and time of the start and end of the communication
- Telephone service used , e.g. voice, conference call , Short Message Service (SMS) Multimedia Service(MMS)
- Location label (Cell ID) at the start and end of the communication

SolarWinds Call Detail Record Tracker

Search

Settings

Call Origin

- All -

Call Destination

- All -

Call Status

Failed

Termination Causes

- All -

Call Quality

MOS - All -

Call Time

- All -

Reload Calls

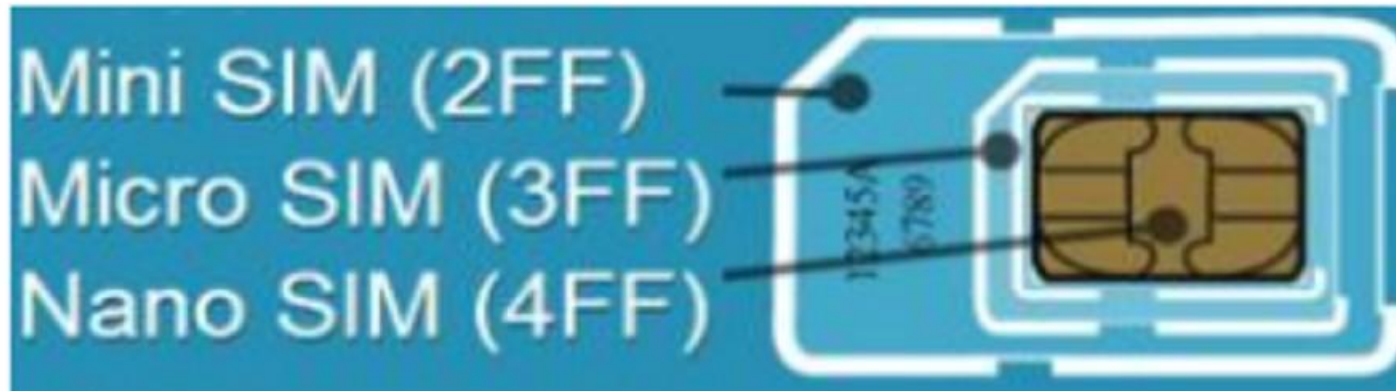
Search VoIP Calls

Origin IP	Origin Phone	Dest. IP	Dest. Phone	MOS	Start Date	End Date	Status	Origin Termin. Causes	Dest. Termin. Causes	Redirect reason
10.140.3.4	511120631	10.110.107.4	812134930606		8/16/2012 1:28:19 PM	8/16/2012 1:28:43 PM	Success	16	0	0
10.140.3.4	511120688	10.110.107.4	813128783081		8/16/2012 1:27:55 PM	8/16/2012 1:30:40 PM	Success	16	0	0
10.140.3.4	511120631	10.110.107.4	812134930606		8/16/2012 1:31:01 PM	8/16/2012 1:31:33 PM	Success	0	16	0
10.160.3.6	2906	10.110.44.223	9360		8/16/2012 1:22:05 PM	8/16/2012 1:40:54 PM	Success	16	0	0
10.160.3.6	2968	10.140.3.4	0617		8/16/2012 1:48:59 PM	8/16/2012 1:53:10 PM	Success	0	16	0
10.110.107.20	815129382004	10.110.107.30	7312		8/16/2012 1:53:08 PM	8/16/2012 1:53:15 PM	Success	16	0	0
10.140.3.4	511120688	10.110.107.4	812153831013		8/16/2012 1:31:34 PM	8/16/2012 1:58:12 PM	Success	16	0	0
10.140.3.4	511120638	10.110.107.4	819092590011		8/16/2012 1:32:23 PM	8/16/2012 2:04:10 PM	Success	16	0	0
10.140.3.4	511120688	10.110.107.4	818053090015		8/16/2012 2:00:47 PM	8/16/2012 2:25:16 PM	Success	16	0	0
10.140.3.4	511120652	10.110.107.4	812132890015		8/16/2012 2:02:45 PM	8/16/2012 2:32:49 PM	Success	16	0	0
10.140.3.4	511120688	10.110.107.4	813146271505		8/16/2012 2:32:33 PM	8/16/2012 2:46:14 PM	Success	16	0	0
10.140.3.4	511120637	10.110.107.4	813128783080		8/16/2012 2:36:49 PM	8/16/2012 2:53:07 PM	Success	16	0	0
10.200.3.4	5126829300	10.110.107.9	1990516		8/16/2012 3:10:36 PM	8/16/2012 3:10:52 PM	Success	16	0	2
10.160.3.6	2905	10.110.64.108	9356		8/16/2012 3:03:33 PM	8/16/2012 3:19:12 PM	Success	0	16	0
10.140.3.4	511120688	10.110.107.4	812134930605		8/16/2012 3:29:58 PM	8/16/2012 3:30:13 PM	Success	16	0	0
10.140.3.4	511120705	10.110.107.4	816093180020		8/16/2012 2:38:43 PM	8/16/2012 3:30:50 PM	Success	16	0	0
10.140.3.4	511120688	10.110.107.4	812134930605		8/16/2012 3:30:32 PM	8/16/2012 3:31:05 PM	Success	0	16	0
10.140.3.4	511120688	10.110.107.4	812134930605		8/16/2012 3:31:41 PM	8/16/2012 3:31:53 PM	Success	16	0	0

Displaying 6,852 calls

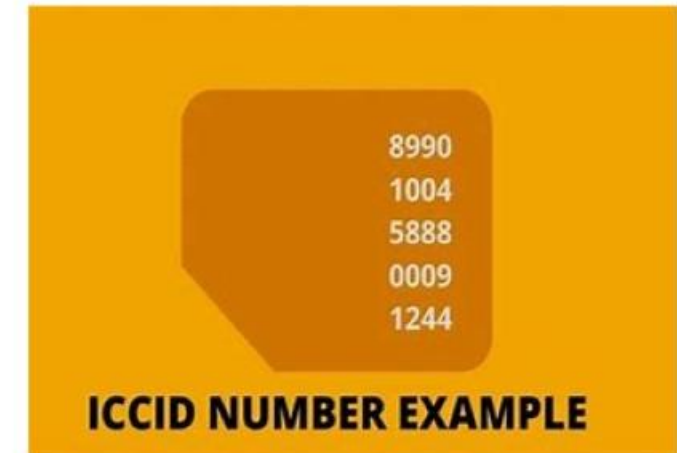
SIM Card

Mobile chips



ICCID : Integrated Circuit Card Identification

- Integrated Circuit Card ID (ICCID) is the unique identifier of a Subscriber Identity Module (SIM card) on a mobile device.
- ICCIDs are stored in the SIM cards and printed on the SIM card body.
- The ICCID is defined by the ITU-T recommendation E.118 as the Primary Account Number.
- A full ICCID is 19 or 20 characters containing **the Industry Identifier (ISO)**, **country code**, **issuer identity**, **account ID**, and other data which allows the network operator to identify the card.

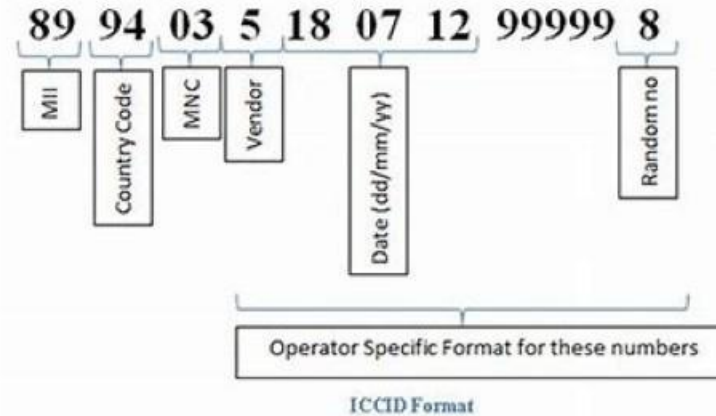


19 to 20 digit

Industry identifier : 89

Counter code : 94

Issuer identifier



Standard SIM



microSIM

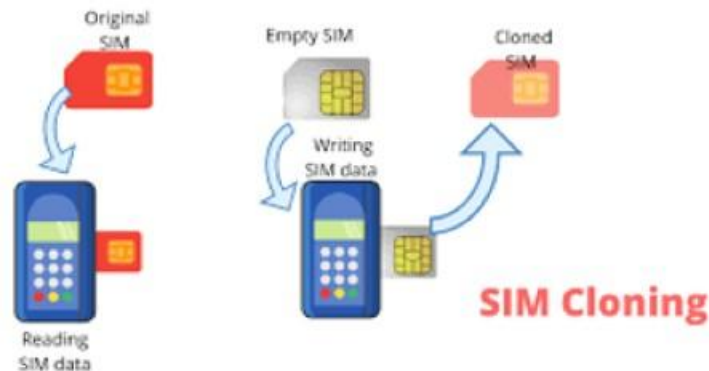


nanoSIM



What is a SIM cloning?

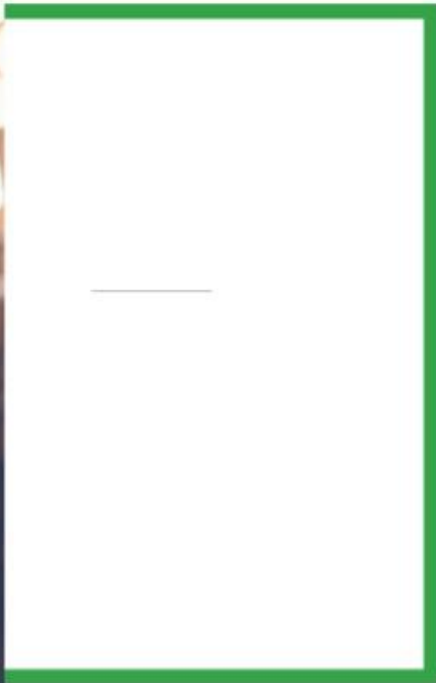
- SIM cloning is the process in which a legitimate SIM card is duplicated. When the cloning is completed, the cloned SIM card's identifying information is transferred onto a separate, secondary SIM card.
- The secondary card can then be used in a different phone while having all calls and associated charges attributed to the original SIM card.



- SIM Cloning as attack
- An attacker gaining physical access to your SIM card and then cloning it onto a new SIM card controlled by the hacker.
- Once the hacker has a clone of the SIM card, they can then use this in a device they control to access the victim's texts, phone calls and location data.



[How to Clone SIM Card -- Tenorshare](#)



Challenges

- Strong encryption (e.g., iPhone security)
- Locked devices and passcode protection
- Cloud-synced data
- Rapidly changing OS versions
- Legal and privacy constraints
- Damaged devices



Thank You