Mobile Forensics

Module 13

Designed by Cyber Crime Investigators. Presented by Professionals.

C|HFI™
Computer Hacking Forensic Investigator

Module Objectives

After successfully completing this module, you will be able to:

1 Discuss about mobile device forensics and understand why it is needed

2 Understand the role of mobile hardware and OS while conducting forensics on mobiles

3 Illustrate the architectural layers of mobile device environment

4 Illustrate Android architecture stack and demonstrate Android boot process

5 Illustrate iOS architecture stack and demonstrate iOS boot process

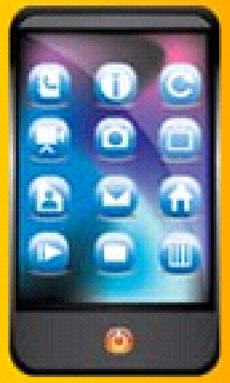
6 Determine the mobile storage and evidence locations

7 Understand what you should do before performing investigation

8 Perform mobile forensics

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Forensics



Mobile phone forensics is the **science of recovering digital evidence** from a mobile phone under forensically sound conditions

It includes recovery and analysis of data from **mobile devices' internal memory**, **SD cards** and **SIM cards**

Mobile forensics aims to trace the **perpetrators** of crimes that involve the use of **mobile phones**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Why Mobile Forensics?

Using Mobiles for Money Transactions

Mobile payment user

2015	2016
384 Million	425 Million
transactions	transactions
$450 Billion	$620 Billion

http://www.statista.com

2020

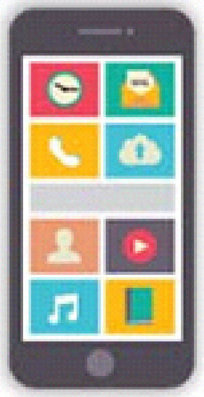
50%

of transactions will be made via mobile

http://www.three.co.uk

The Projected Growth of Mobile Use

Internet connections made via mobile devices



2015	2016	2019
52.7%	56.1%	63.4%

http://www.statista.com

Number of malwares targeting mobile devices tripled in 2015 in comparison with 2014

Among all the malwares, ransomware malwares capable of obtaining unlimited rights on an infected device, and data stealers proved to be the most dangerous threat in 2015

Approximately 94,344 unique users were attacked by mobile ransomware in 2015 in comparison with 18,478 users in 2014

2016 is likely to see an increase in the complexity of malwares and its modifications, with more geographies targeted

http://www.kaspersky.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Top Threats Targeting Mobile Devices

Web- & Network-based Attacks

- Launched by malicious websites or compromised legitimate sites
- Attacking site exploits device's browser
- Attempts to install malware or steal confidential data that flows through the browser

Malware

- Includes traditional computer viruses, computer worms and Trojan horse programs
- Example: IKee worm targeted iOS-based devices
- Example: Pjapps enroll infected Android devices on the botnet

Social Engineering Attacks

- Leverage social engineering to trick users
- Attempts to get users to disclose sensitive information or install malware
- Examples include phishing and targeted attacks

Resource Abuse

- Attempt to misuse network, device or identity resources
- Example: Sending spam from compromised devices
- Example: Denial of Service attacks using computer resources of compromised devices

Data Loss

- Employee or hacker exfiltrates sensitive information from device or network
- Can be unintentional or malicious
- Remains biggest threat to mobile devices

Data Integrity Threats

- Attempts to corrupt or modify data
- The purpose is to disrupt operations of an enterprise or geared toward financial gain
- Can also occur unintentionally

http://www.symantec.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Hardware and Forensics

Mobile device forensics is highly **dependent on the underlying hardware of mobile devices**

Investigators need to take different approaches for mobile forensics depending upon the **mobile hardware architecture**

Proprietary hardware of mobile devices makes forensics **acquisition difficult**

Knowledge of mobile hardware also becomes **essential in case of a broken or damaged device** when it is not possible to access device using data ports

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile OS and Forensics

A mobile operating system **determines the functions and features** available on mobile devices, and manages the communication between the mobile device and other compatible devices

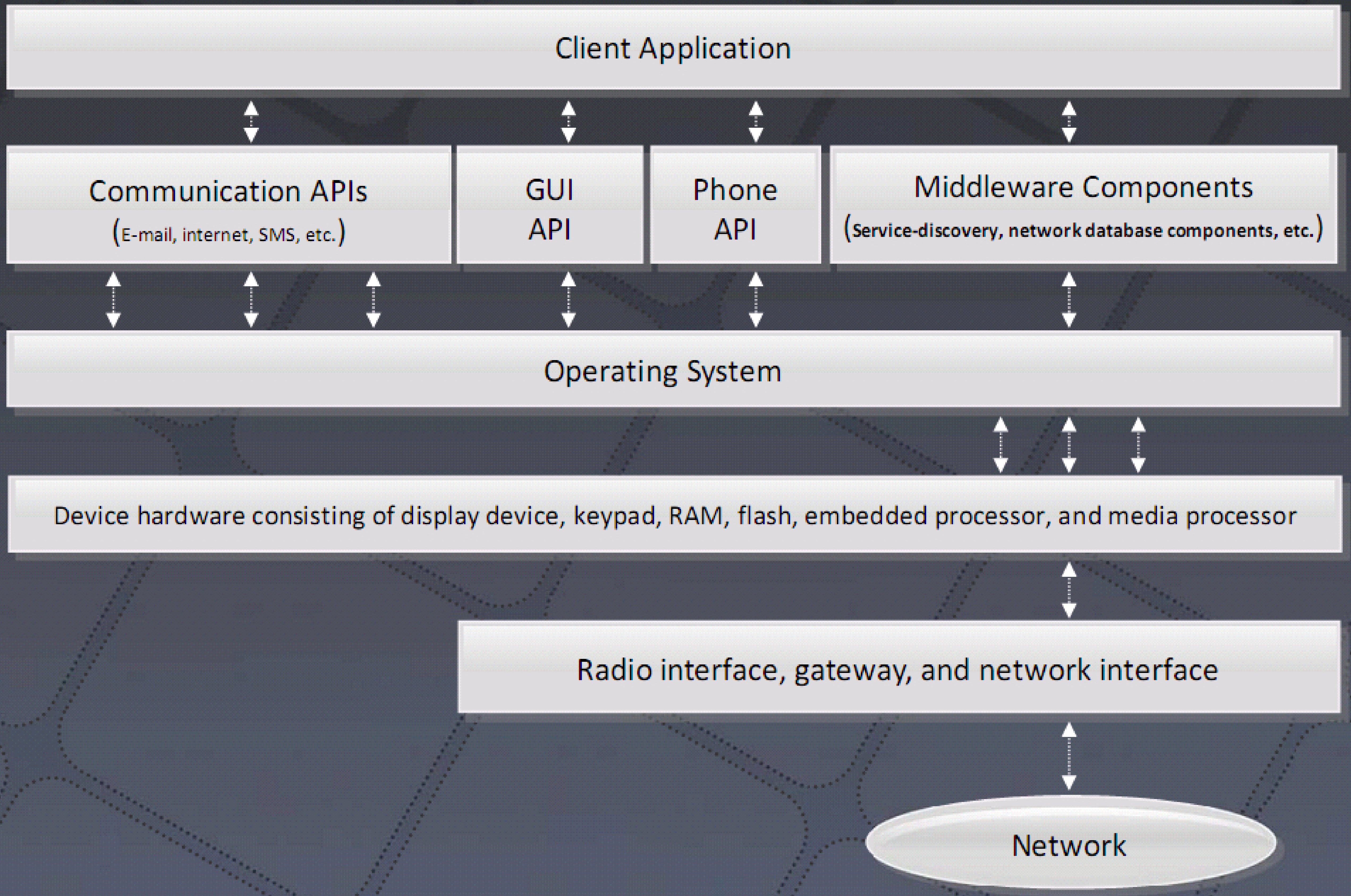
This diversity in the mobile OS architecture may impact **forensic analysis process**

Investigators require **knowledge of underlying OS**, architecture, and file systems of mobile device under investigation

Knowledge of **mobile OS booting process** helps investigator to gain lower level access

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Architectural Layers of Mobile Device Environment



Client Application

Communication APIs (E-mail, internet, SMS, etc.)

GUI API

Phone API

Middleware Components (Service-discovery, network database components, etc.)

Operating System

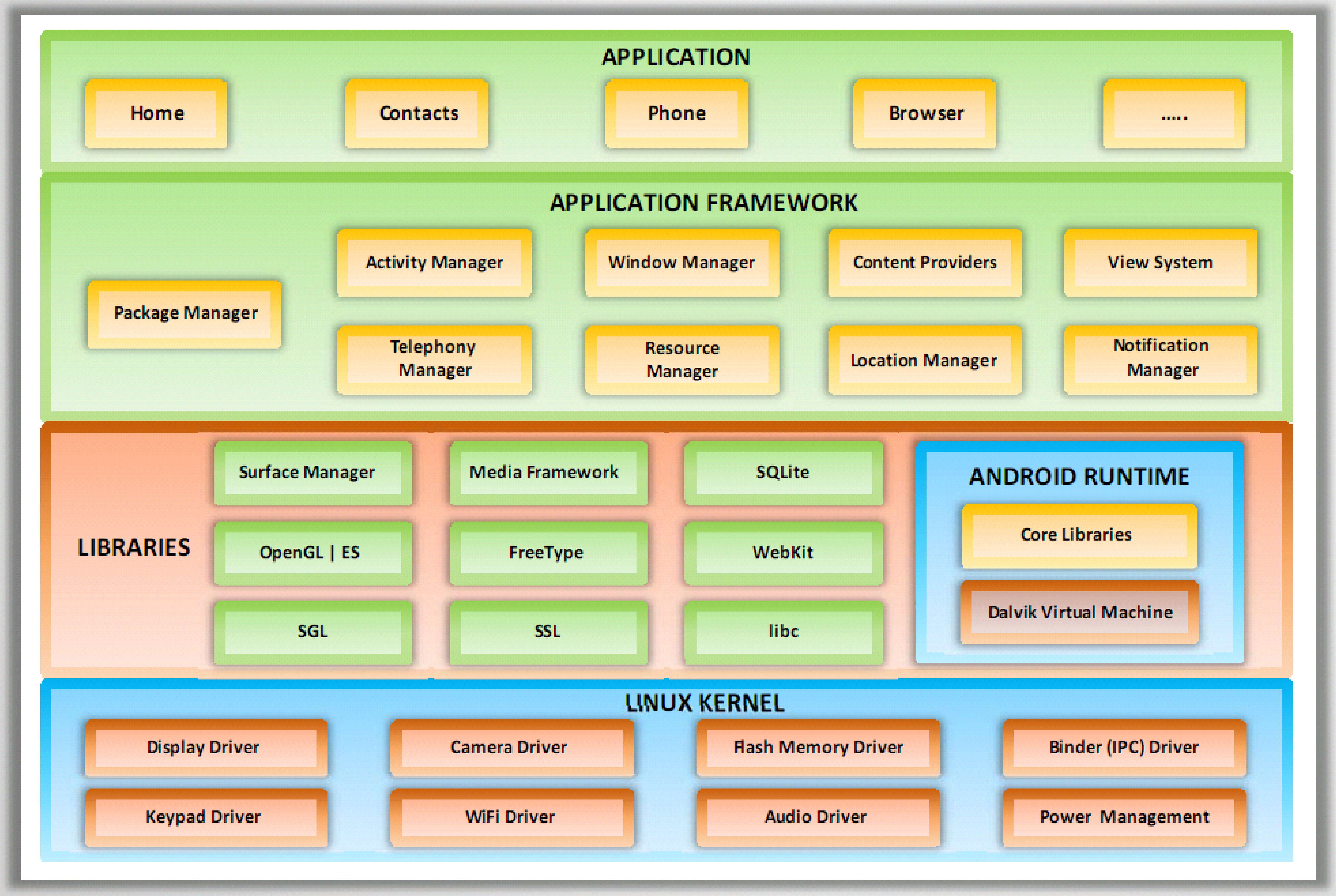
Device hardware consisting of display device, keypad, RAM, flash, embedded processor, and media processor

Radio interface, gateway, and network interface

Network

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android Architecture Stack



User-defined, standard applications

Supports application API interfaces

Native libraries written in C/C++, responsible for handling different types of data

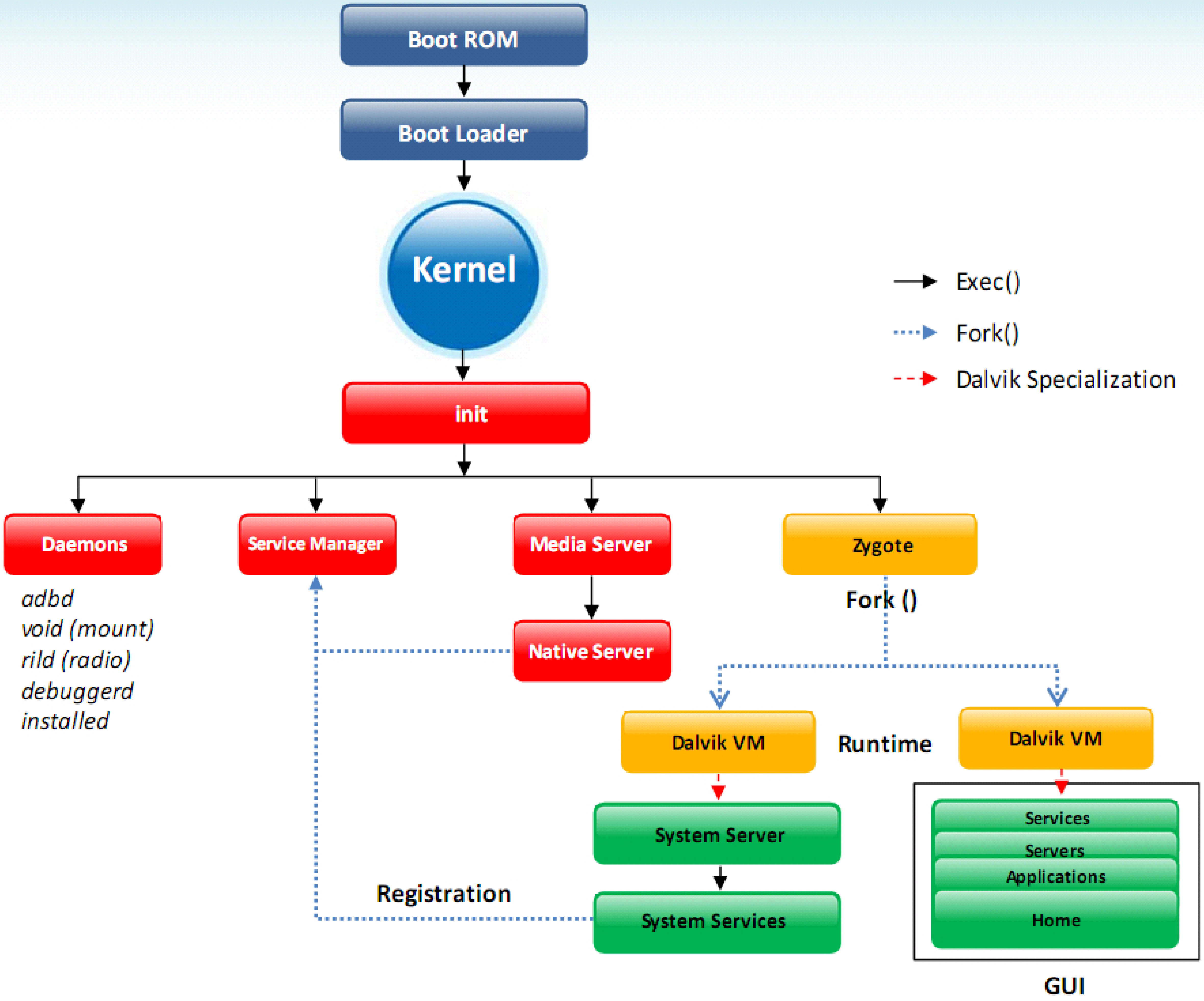
Custom-built virtual machine

Built on top of the Linux 2.6 Kernel, responsible for interacting with the hardware

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android Boot Process

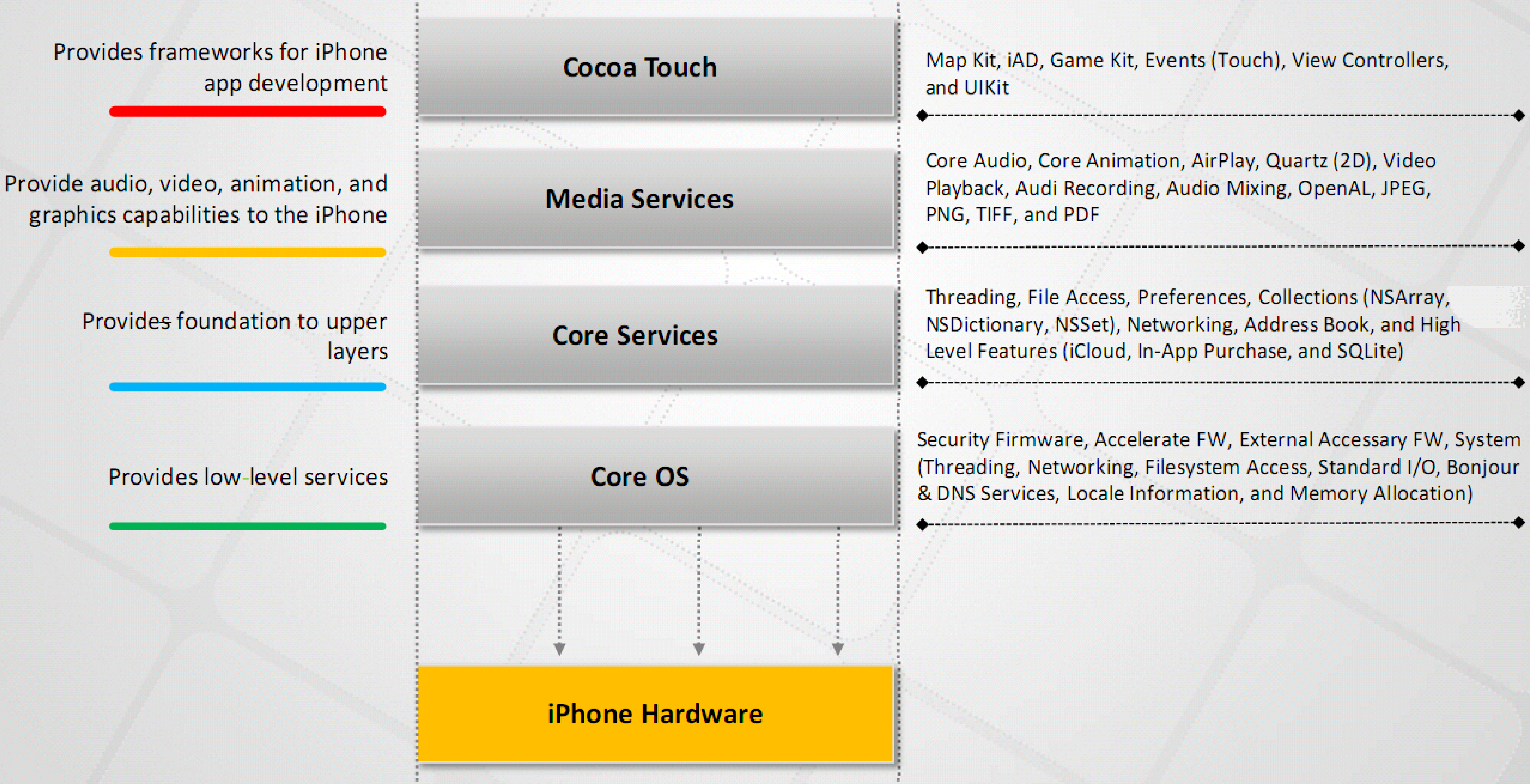
1. The Android Linux kernel component first calls the **init process**
2. The init process accesses the various processes and demons including init.rc mostly known as **zygote**, zygote is started
3. The zygote process **loads the core Java classes**, and **performs the initial processing steps**
4. After the initial load process, **zygote idles on a socket** and **waits for further requests**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

iOS Architecture

iPhone OS stack consists of four abstraction layers



Provides frameworks for iPhone app development

Cocoa Touch

Map Kit, iAD, Game Kit, Events (Touch), View Controllers, and UIKit

Provide audio, video, animation, and graphics capabilities to the iPhone

Media Services

Core Audio, Core Animation, AirPlay, Quartz (2D), Video Playback, Audi Recording, Audio Mixing, OpenAL, JPEG, PNG, TIFF, and PDF

Provides foundation to upper layers

Core Services

Threading, File Access, Preferences, Collections (NSArray, NSDictionary, NSSet), Networking, Address Book, and High Level Features (iCloud, In-App Purchase, and SQLite)

Provides low-level services

Core OS

Security Firmware, Accelerate FW, External Accessary FW, System (Threading, Networking, Filesystem Access, Standard I/O, Bonjour & DNS Services, Locale Information, and Memory Allocation)

iPhone Hardware

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

iOS Boot Process

The iPhone boot process consists of **multiple boot stages**. Each stage verifies the integrity and authenticity of the next stage

The normal booting process uses a **built-in chain-of-trust mechanism** that prevents lower level access to iOS implementation layers

Device Firmware Upgrade (DFU) mode is used during a forensics investigation to gain lower level access to the device

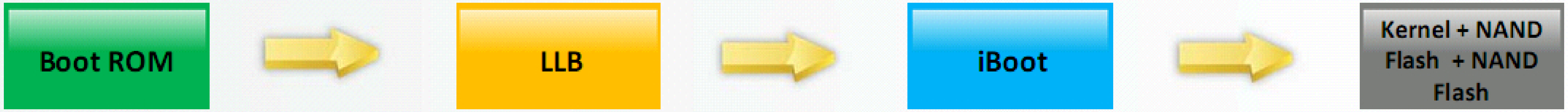
Using this mode, the investigator can **alter the boot sequence**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Normal and DFU Mode Booting

Normal Boot Process:

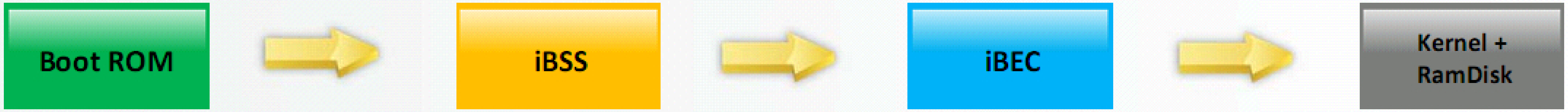
- BootRom starts the booting process
- LLB, the first level boot loader, is loaded after verification of integrity and authenticity
- The stage 2 bootloader iBoot starts after verification of integrity and authenticity
- Kernel and NAND flash is also loaded after verification of integrity and authenticity



Boot ROM → LLB → iBoot → Kernel + NAND Flash + NAND Flash

DFU Mode:

- iBoot is not booted during the DFU mode boot sequence



Boot ROM → iBSS → iBEC → Kernel + RamDisk

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

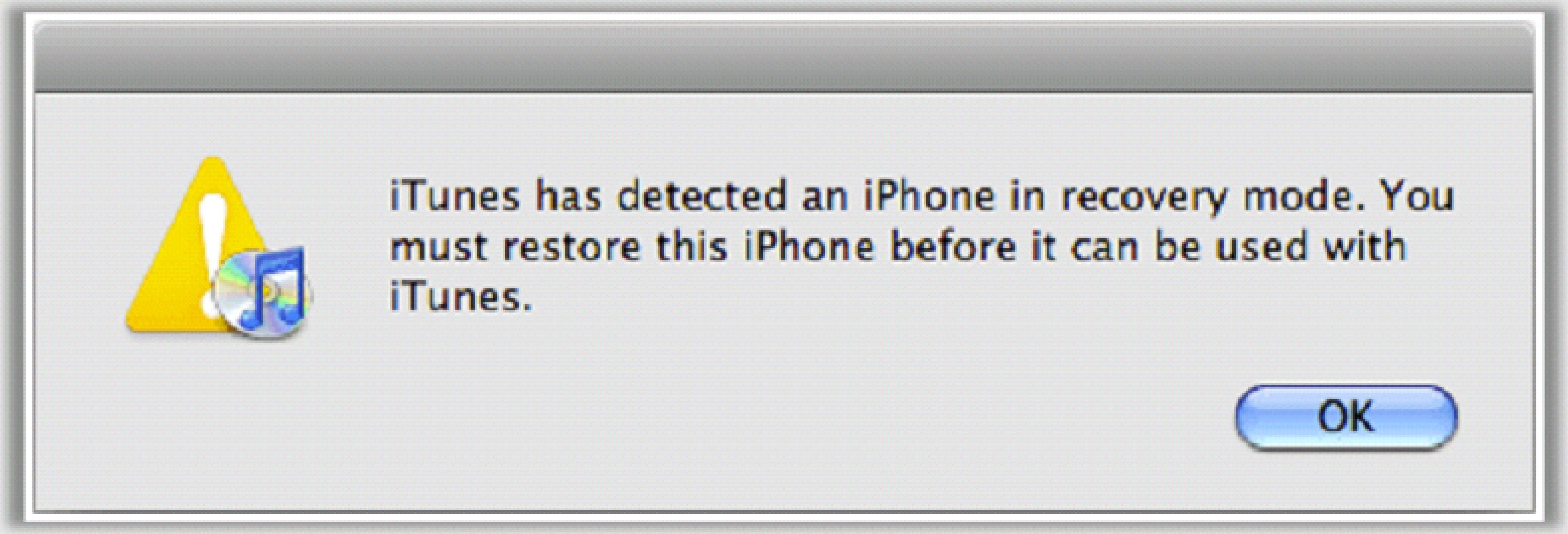
Booting iPhone in DFU Mode

I Connect the iPhone to a computer and launch **iTunes**

II Turn the **iPhone off**

III Hold down the **sleep/power button** and **home button** together for exactly **10 seconds**, then release the power button

IV Continue to hold down the **Home button** until a message appears in iTunes saying that "**iTunes has detected an iPhone in recovery mode**"



iTunes has detected an iPhone in recovery mode. You must restore this iPhone before it can be used with iTunes.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Storage and Evidence Locations

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.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

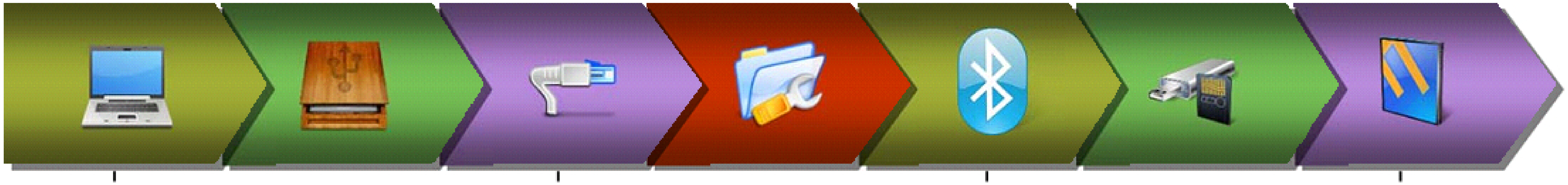
What Should You Do Before the Investigation?

1. Build a Forensics Workstation
2. Build the Investigation Team
3. Review Policies and Laws
4. Notify Decision Makers and Acquire Authorization
5. Risk Assessment
6. Build a Mobile Forensics Toolkit

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Build a Forensics Workstation

Build a mobile forensic workstation with the following equipment:



A laptop or a desktop computer

A USB (universal serial bus) connector

Mobile hardware toolkit (Eg: Pro Tech Toolkit)

Mobile forensics toolkit

Cables (including FireWire, Bluetooth and IR)

Micro SD Memory card Reader

SIM card Reader

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Build the Investigation Team

- The investigation team should consist of persons who possess **expertise** in, responding to seizing, collecting and reporting **evidence** from mobile devices. The investigation team includes Expert Witness, Evidence Manager, Evidence Documenter, Evidence Examiner/Investigator, Attorney, Photographer, Incident Responder, Decision Maker, and Incident Analyzer

- Each team member should have in-depth knowledge of a wide variety of mobile devices, their **hardware architecture**, **operating systems**, and **mobile apps**

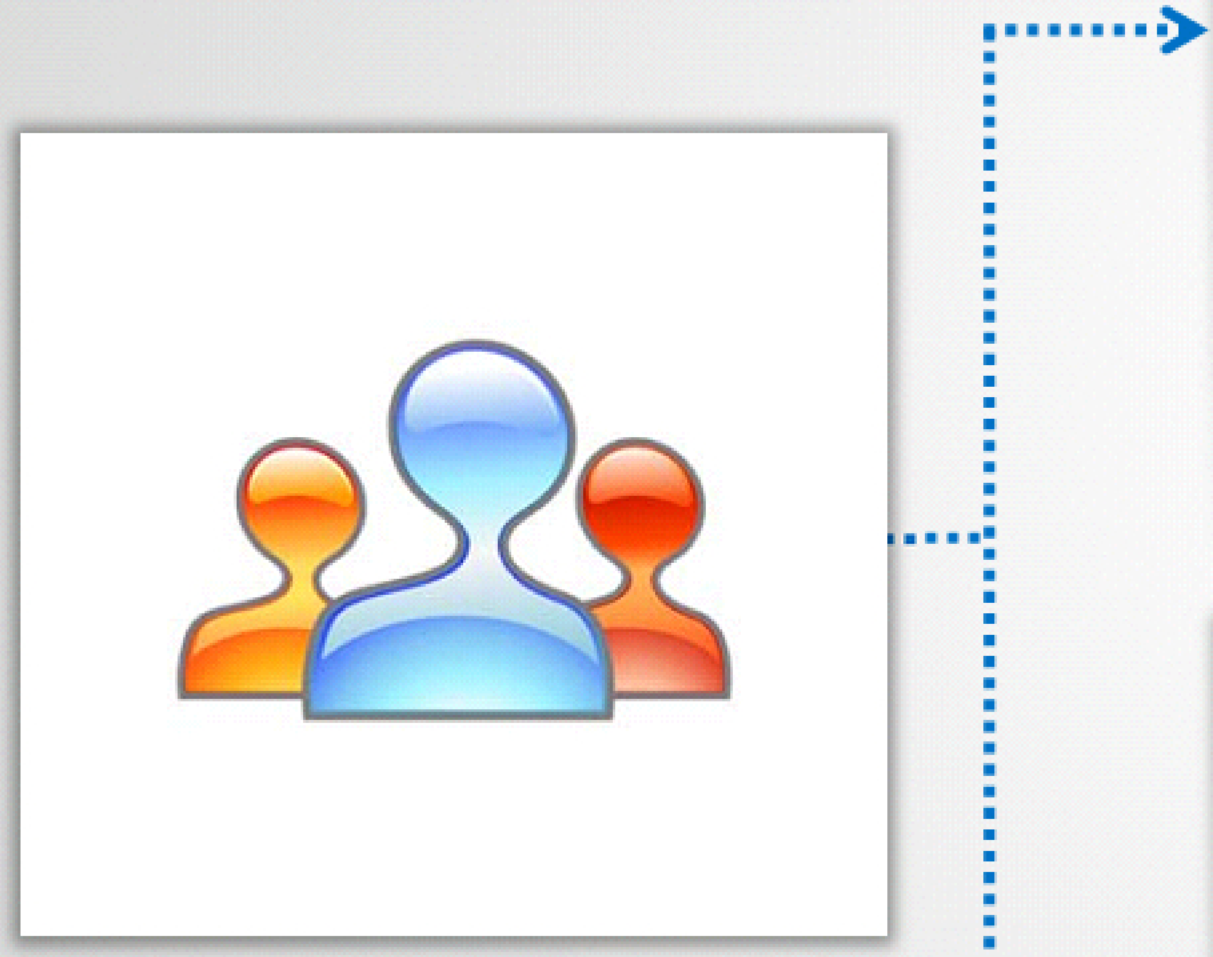
- Each team member should be aware of local **laws and legal issues** associated with mobile-related crime

- Every team member should have the necessary clearance and authorization to conduct assigned tasks
- Keep the investigation team as small as possible to **ensure confidentiality**

- Identify team members and assign a **responsibility** to each team member
- Assign one team member as the **technical lead** for the investigation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Review Policies and Laws



Review local laws that may influence the forensics investigation; investigators must follow a **legally accepted** forensics investigation process, and create documentation accordingly

Review internal **Bring Your Own Device (BYOD)** and **information security policies** of the organization carefully in cases of forensics investigation involving mobile phones issued by the organization

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Notify Decision Makers and Acquire Authorization

1

Notify the decision makers of the need to perform forensics investigation, and obtain the written authorization

2

Generally, incident response policies and procedures define the decision-making authority and the process to obtain authorization

3

After obtaining the authorization, assess the situation and define the course of action

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Risk Assessment

- To prevent new data from **contaminating** the evidence, seal the device in an isolation container properly

- Do not use **plastic bags** to carry out seized mobile device. Use recommended isolation containers

- Consider the power state of mobile device seized. Expiration of the battery would be disastrous as important data may reside in **battery-dependent** volatile memory

- Handle and transport mobile devices carefully as they are **fragile** and can be easily **damaged**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Build a Mobile Forensics Toolkit

- Forensic investigators should be equipped with a right **set of tools**
- The mobile forensics toolkit includes both **hardware** and **software** tools required to **recover** and **analyze** data from mobile devices

Hardware Tools

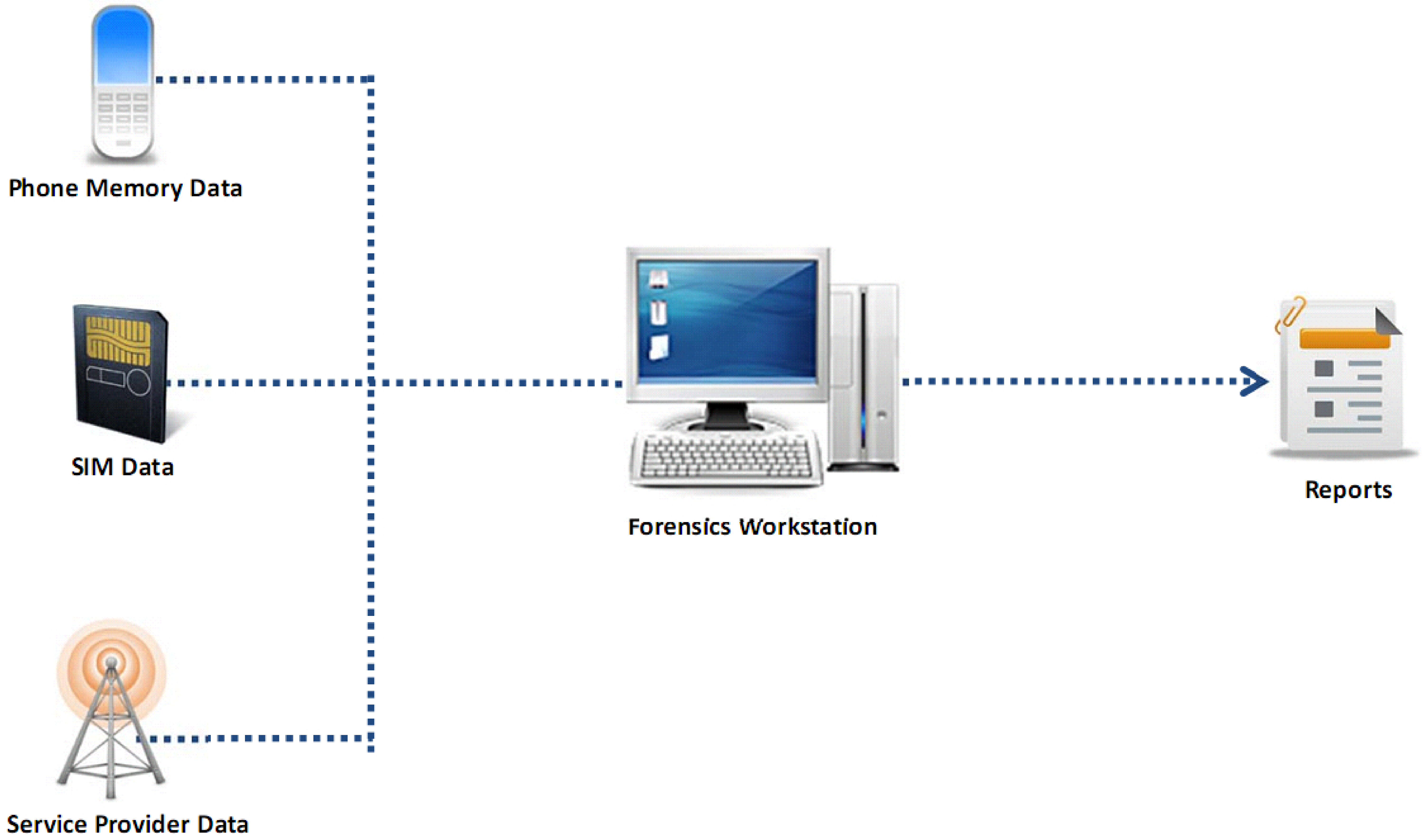
- Cellebrite UFED System
- Secure ViewKit for Forensics
- DS-Device Seizure & Toolbox
- USB reader for SIM cards
- iGo
- DC Lab Power Supply 0-15V/3A
- Digital Display with Backlight
- Paraben's Phone Recovery Stick

Software Tools

- SEARCH Investigative Toolbar
- BitPim
- Oxygen Forensics Analayst
- Paraben's Sim Card Seizure
- MOBILedit! Forensic
- TULP2G
- iDEN Phonebook Manager
- SUMURI's PALADIN
- floAt's Mobile Agent
- XRY Logical & XRY Physical

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Phone Evidence Analysis



Phone Memory Data

SIM Data

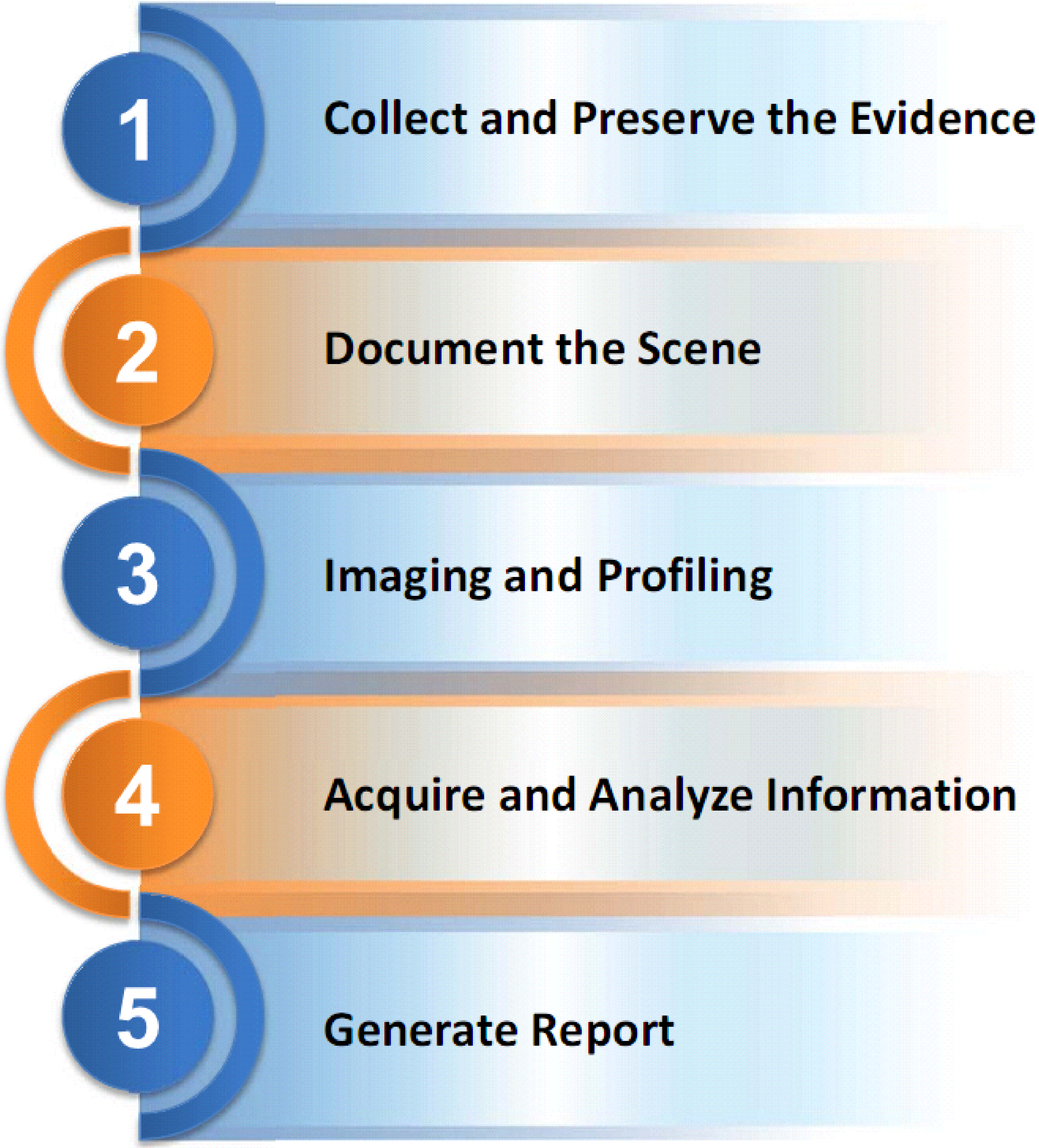
Service Provider Data

Forensics Workstation

Reports

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Forensics Process



1. Collect and Preserve the Evidence
2. Document the Scene
3. Imaging and Profiling
4. Acquire and Analyze Information
5. Generate Report

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting the Evidence

1. Protect the **integrity** of traditional and electronic evidence
2. Prevent **unauthorized users** from entering at the scene and touching the evidence
3. Collect all the **electronic devices** found at the crime scene
4. Check whether the **mobile device** is **connected to a computer**
5. Confirm the **power state** of the devices by checking flashing light
6. Collect **non-electronic evidence** such as written passwords, handwritten notes, and computer printouts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Document the Scene

1. Document all the **electronic devices** found at the crime scene
2. Take photographs of all evidence at the scene, and **write notes on what you have seen** on the screen
3. Document the **state of the device** during seizure
4. Document any **activity on the electronic devices** found at the crime scene

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Document the **Evidence**

Phone Identification

- Identify the brand, model, operating system, and the network **service provider**
- It helps to choose **an appropriate forensics tool** for the data acquisition

Connection Identification

- Identify the type of **connection** used to connect to the forensics workstation
- It may be a cable, Infrared, or Bluetooth
- This depends upon the phone, forensics tool and acquisition conditions

Tool Selection

Based on the mobile device model and the connection, select a forensics tool that have the following capabilities:

- Usable
- Comprehensive
- Accurate
- Deterministic
- Verifiable

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Evidence Preservation

- The aim of the preservation step is to **seize the suspect mobile phone** and its associated peripherals without altering the data in it
- It is the first step carried out **prior to the actual investigation**
- It involves **discovering**, **recognizing**, **documenting**, and **collecting** the digital evidence obtained at the crime scene

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Set of Rules for Switching ON/OFF Mobile Phone

01

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** (photograph, if possible)
- **Power down** prior to transport (take any power supply cord present)

02

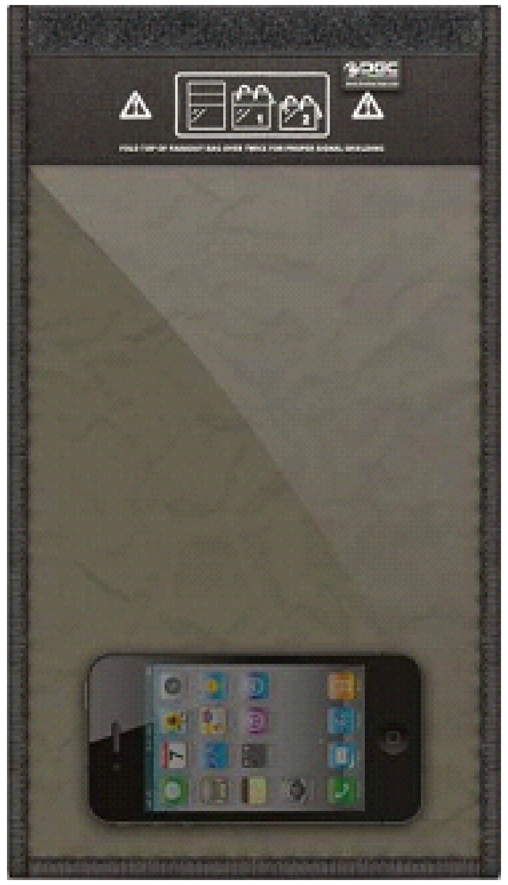
OFF State

- If the device is "**OFF**", leave it "**OFF**"
- Turning it on could alter evidence on device (same as computers)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

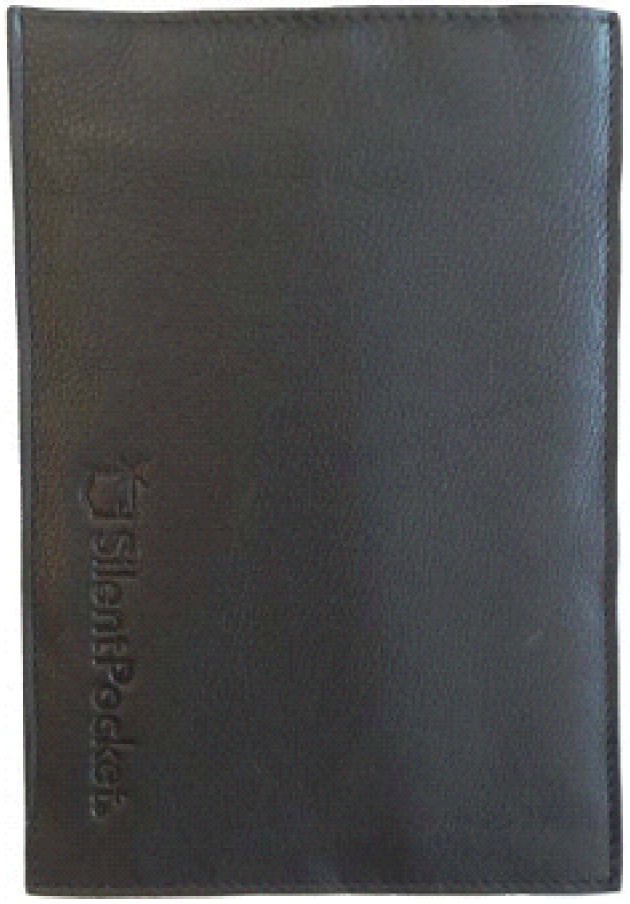
Mobile Phone Signal Containment

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

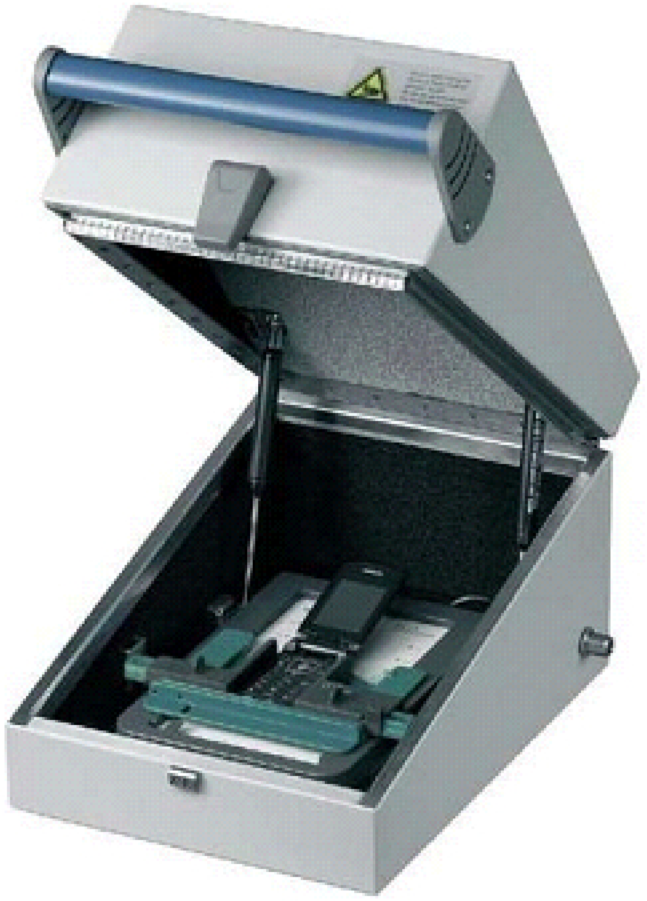


Faraday Bag

Wireless StrongHold Bag



RFID Shielding Cell Phone Case



RF Shield Box

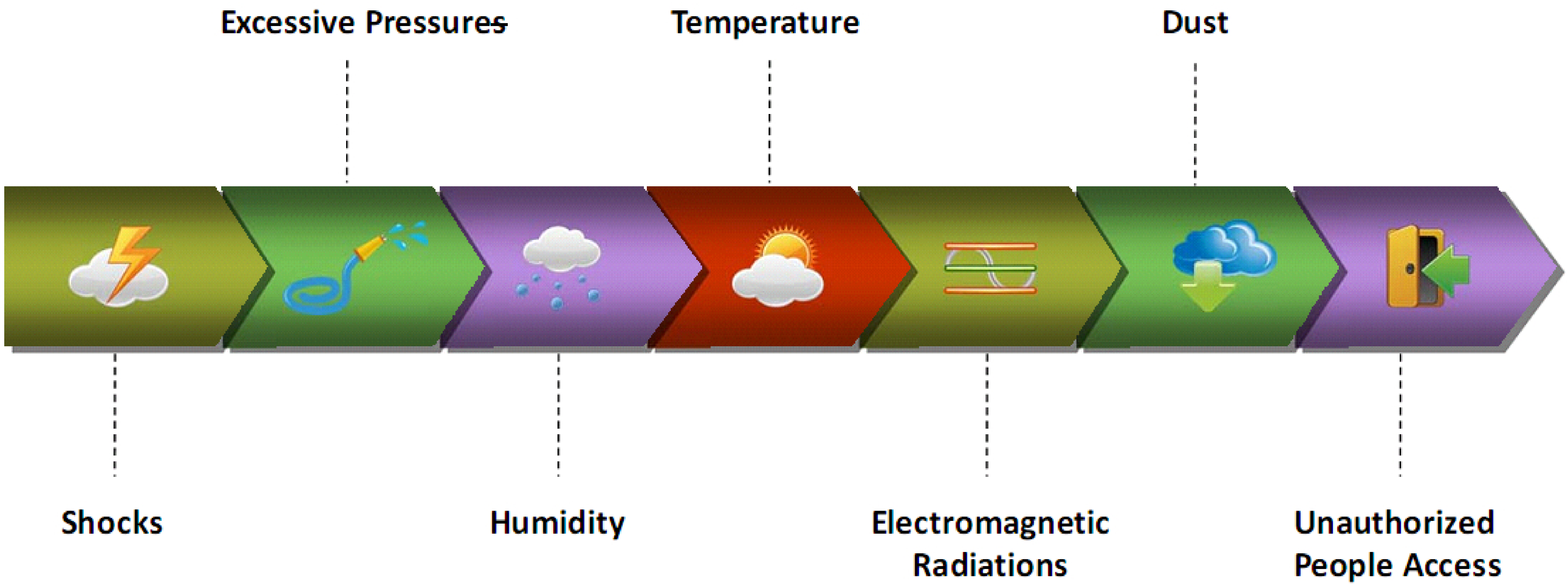
Arson Cans

http://www.amazon.com, http://www.meratronik.com, http://www.sirchie.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Packing, Transporting, and Storing the Evidence

- Pack the collected evidence in a static proof bag duly signed and dated by the investigator
- Evidence collected from the crime scene must be transported carefully to the forensics workshop


Factors that might affect mobile devices during transportation:
Excessive Pressures
Temperature
Dust
Shocks
Humidity
Electromagnetic Radiations
Unauthorized People Access

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Forensic Imaging

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

Possible **mobile phone storage** for imaging:

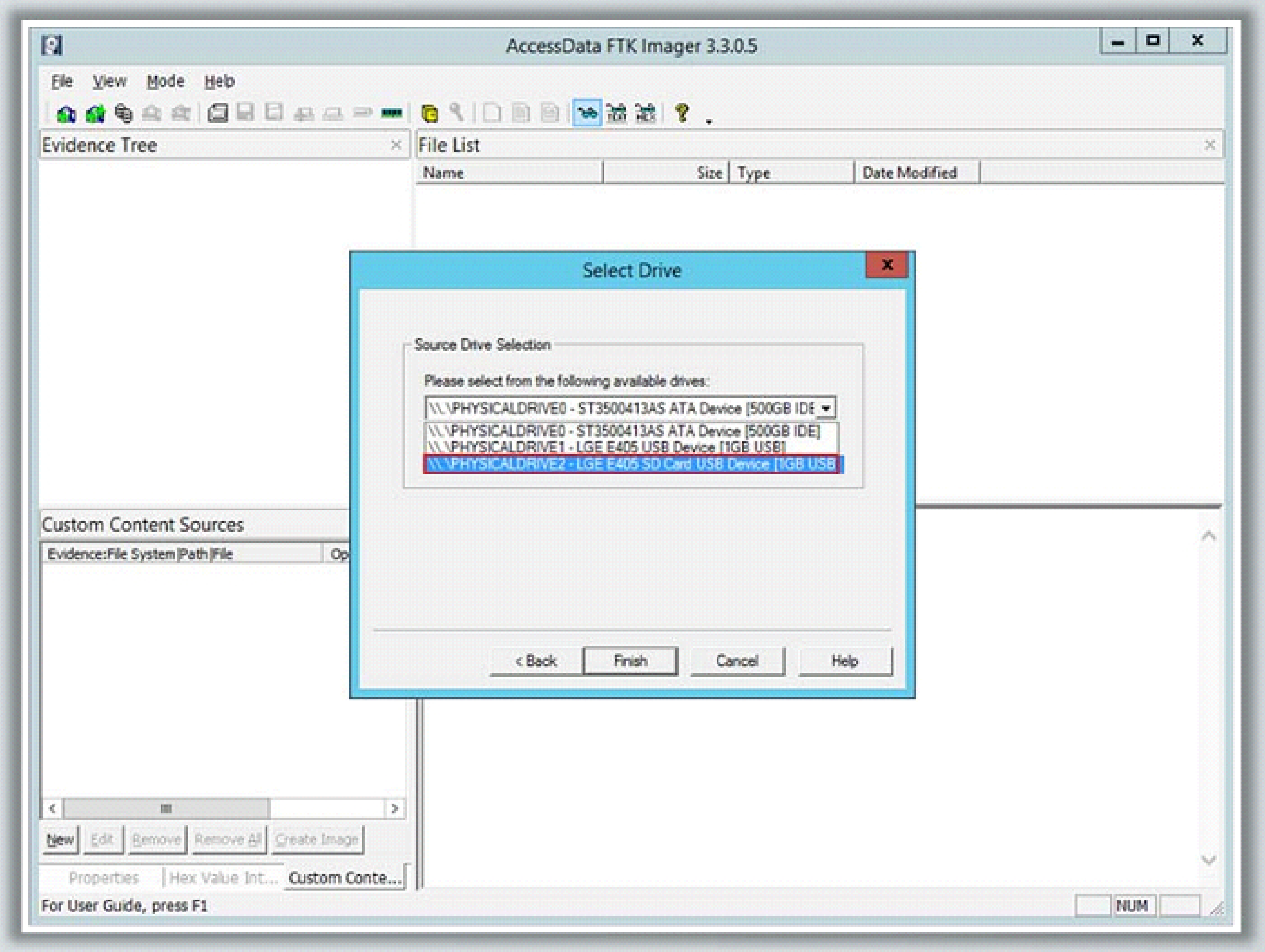
- Mobile phone memory
- SD card memory
- SIM card memory

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Forensic Imaging of **Android Device** Using **FTK Imager**

Forensic Imaging of Phone Memory:

- Connect mobile phone to **forensics workstation**
- Launch FTK Imager
- Select the **drive** that represents the attached mobile phone
- Create a **forensic image** of the selected drive



Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE0 - ST3500413AS ATA Device [500GB IDE

\\.\PHYSICALDRIVE0 - ST3500413AS ATA Device [500GB IDE]
\\.\PHYSICALDRIVE1 - LGE E405 USB Device [1GB USB]
\\.\PHYSICALDRIVE2 - LGE E405 SD Card USB Device [1GB USB

http://accessdata.com

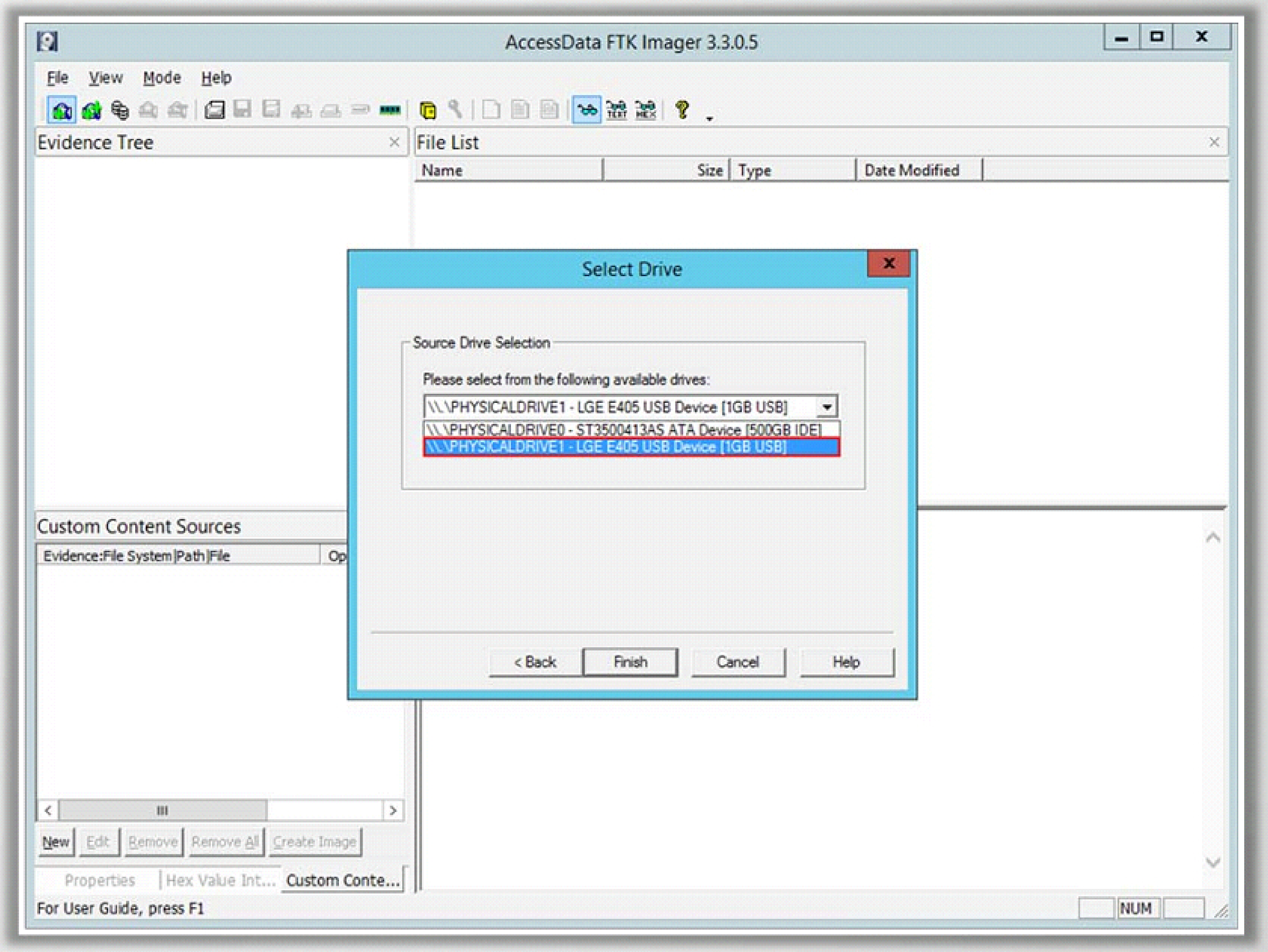
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Forensic Imaging of Android Device Using FTK Imager (Cont'd)

C|HFI Computer Hacking Forensic Investigator™

Forensic Imaging of SD Card:

- Safely **remove** the SD card from the mobile phone
- Connect to the SD card to the workstation using **an SD card reader**
- Launch **FTK Imager** tool
- Select the **drive** that represents the SD card memory
- Create **a forensic image** of the SD card


AccessData FTK Imager 3.3.0.5
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Custom Content Sources
Evidence:File System|Path|File Op
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
For User Guide, press F1
NUM
Select Drive
&lt; Back Finish Cancel Help

Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE1 - LGE E405 USB Device [1GB USB]

\\.\PHYSICALDRIVE0 - ST3500413AS ATA Device [500GB IDE]

\\.\PHYSICALDRIVE1 - LGE E405 USB Device [1GB USB]

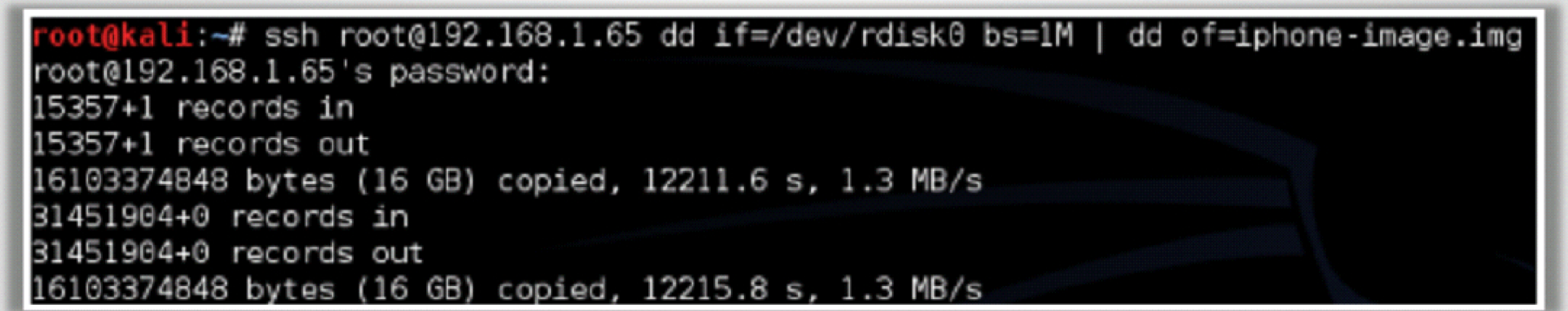
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Creating Disk Image of an iPhone Using SSH

Run following **command on Linux**:

Syntax:

```
ssh -l <username> <your Linux box host address>  dd if=/dev/disk0 | dd
of=~/myiphoneback.img
```



```
root@kali:~# ssh root@192.168.1.65 dd if=/dev/rdisk0 bs=1M | dd of=iphone-image.img
root@192.168.1.65's password:
15357+1 records in
15357+1 records out
16103374848 bytes (16 GB) copied, 12211.6 s, 1.3 MB/s
31451904+0 records in
31451904+0 records out
16103374848 bytes (16 GB) copied, 12215.8 s, 1.3 MB/s
```

What you need before **creating the image**:

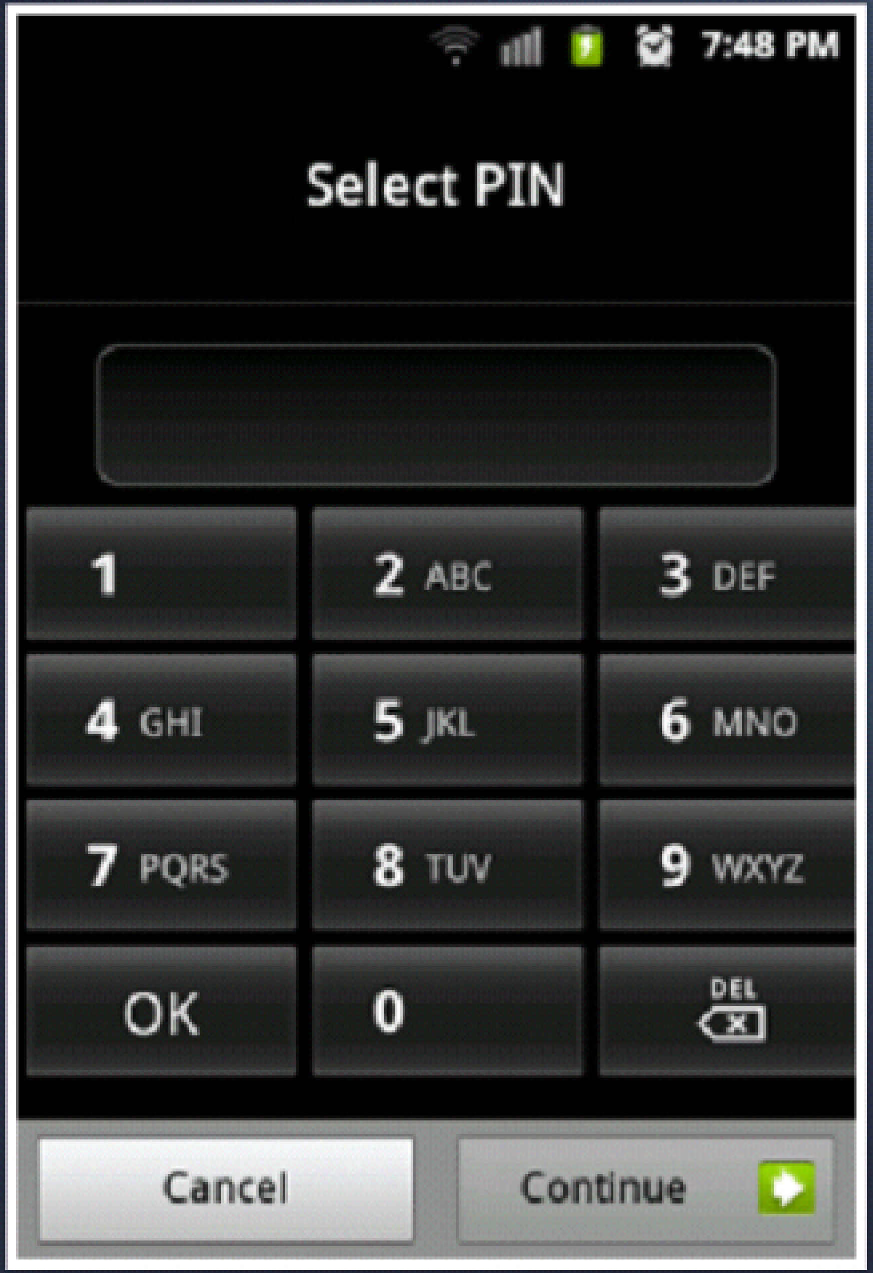
- iPhone should be jailbroken
- SSH should be installed on both iPhone and workstation running Linux OS
- iPhone's IP address
- Computer's IP address

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

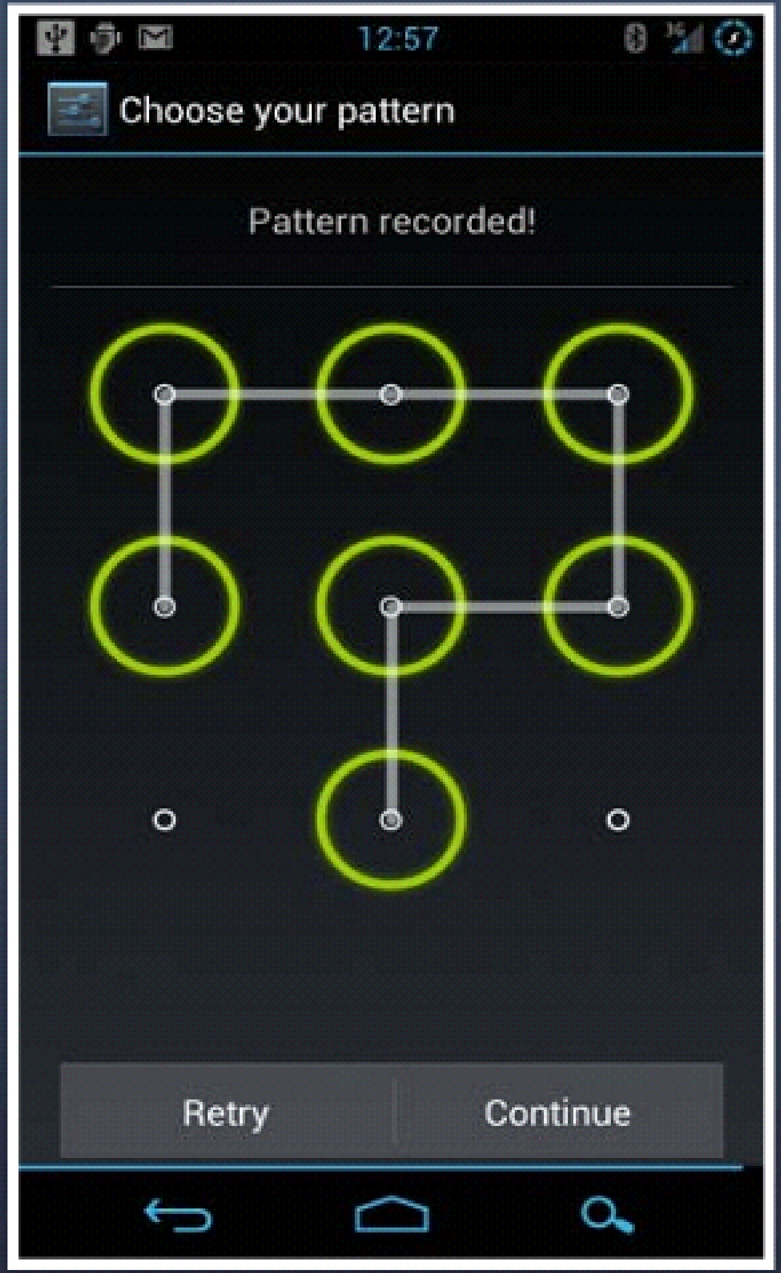
Phone Locking

- Mobile phones use three types of **phone lock schemes** to prevent unauthorized user access
- If phone device obtained at a crime scene is in a **locked state**, the challenge of unlocking it arises
- Forensics investigator needs to **bypass the phone lock** to forensically investigate the mobile phone

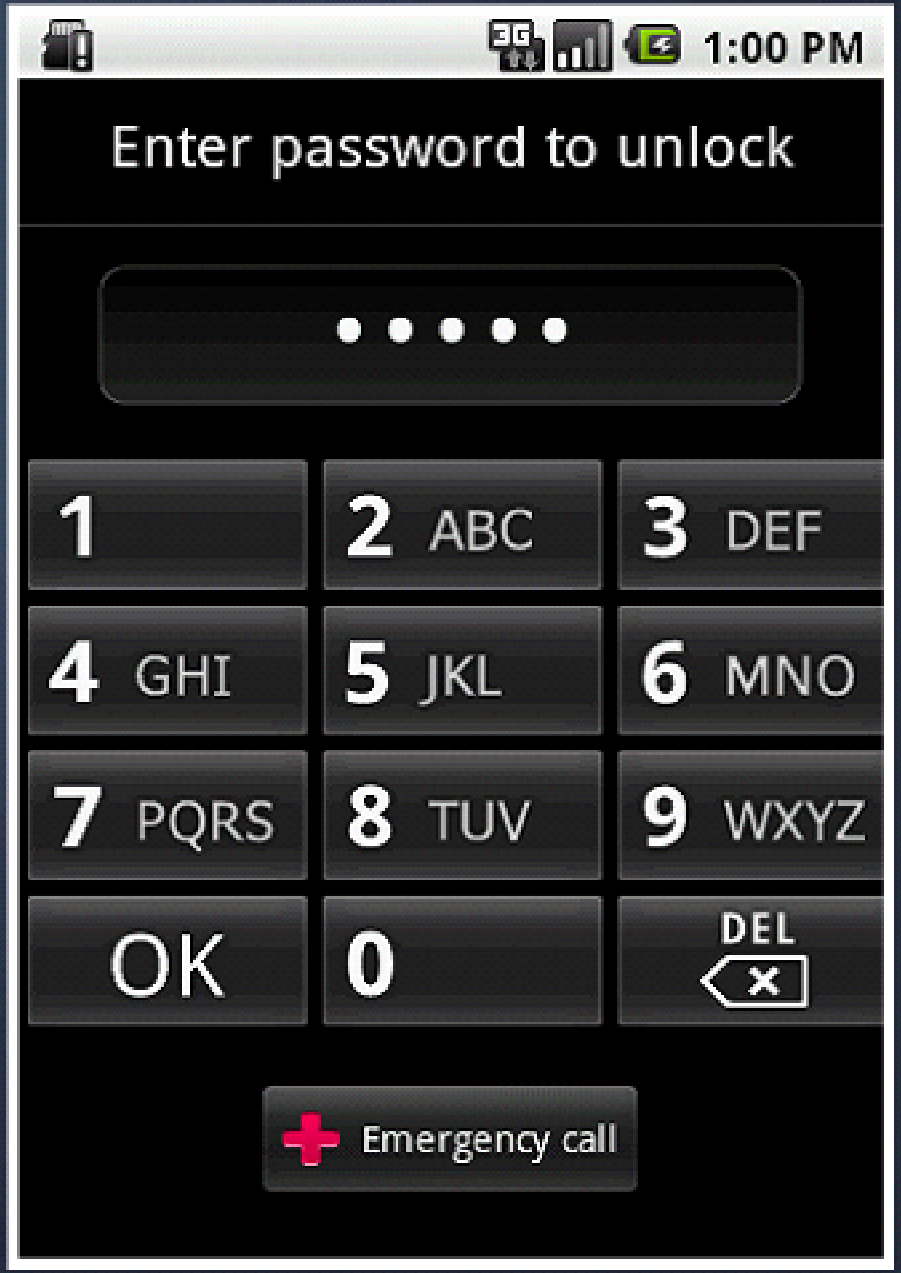
PIN Lock



Pattern Lock



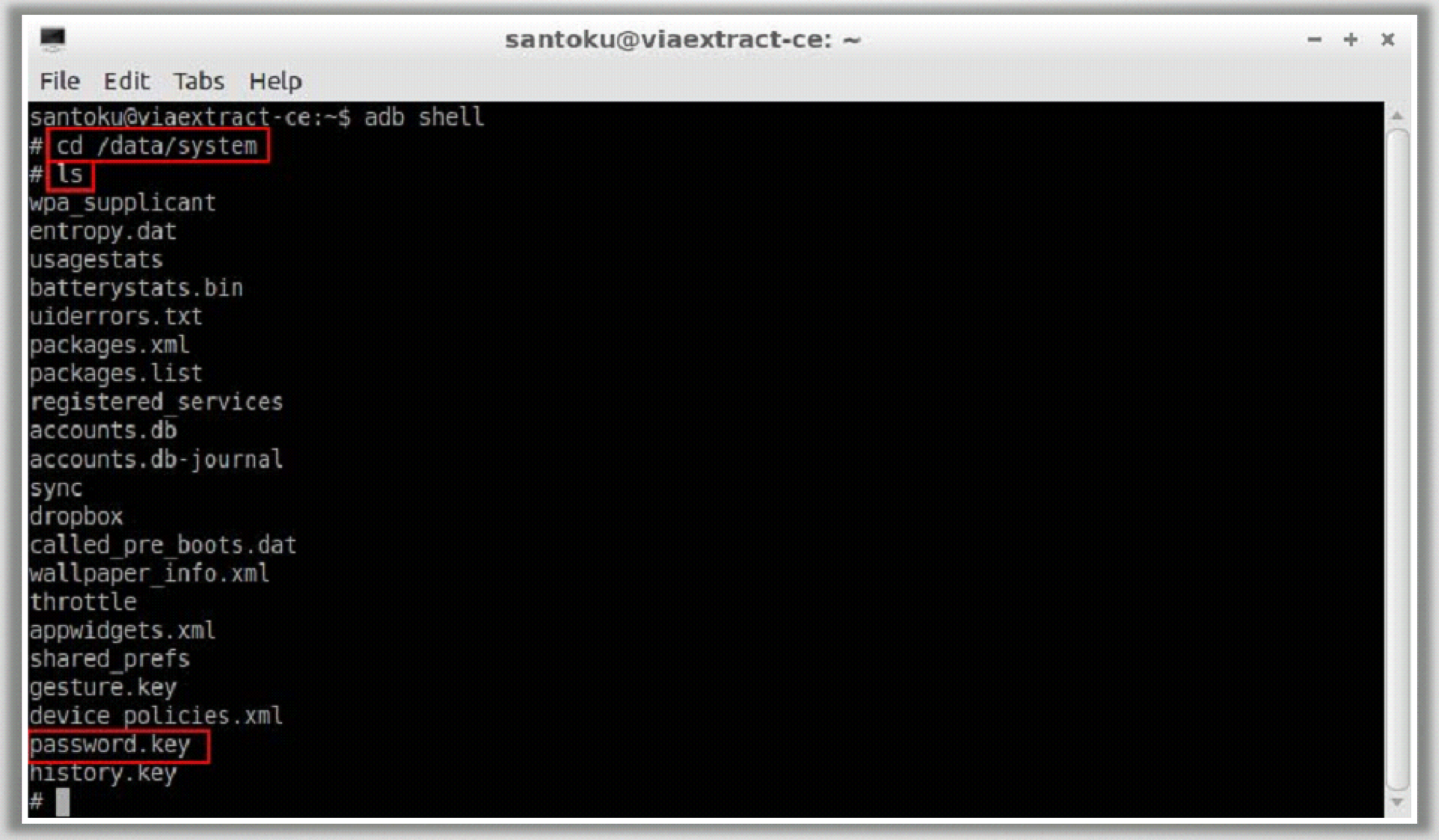
Password Lock



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bypassing Android Phone Lock Password Using ADB

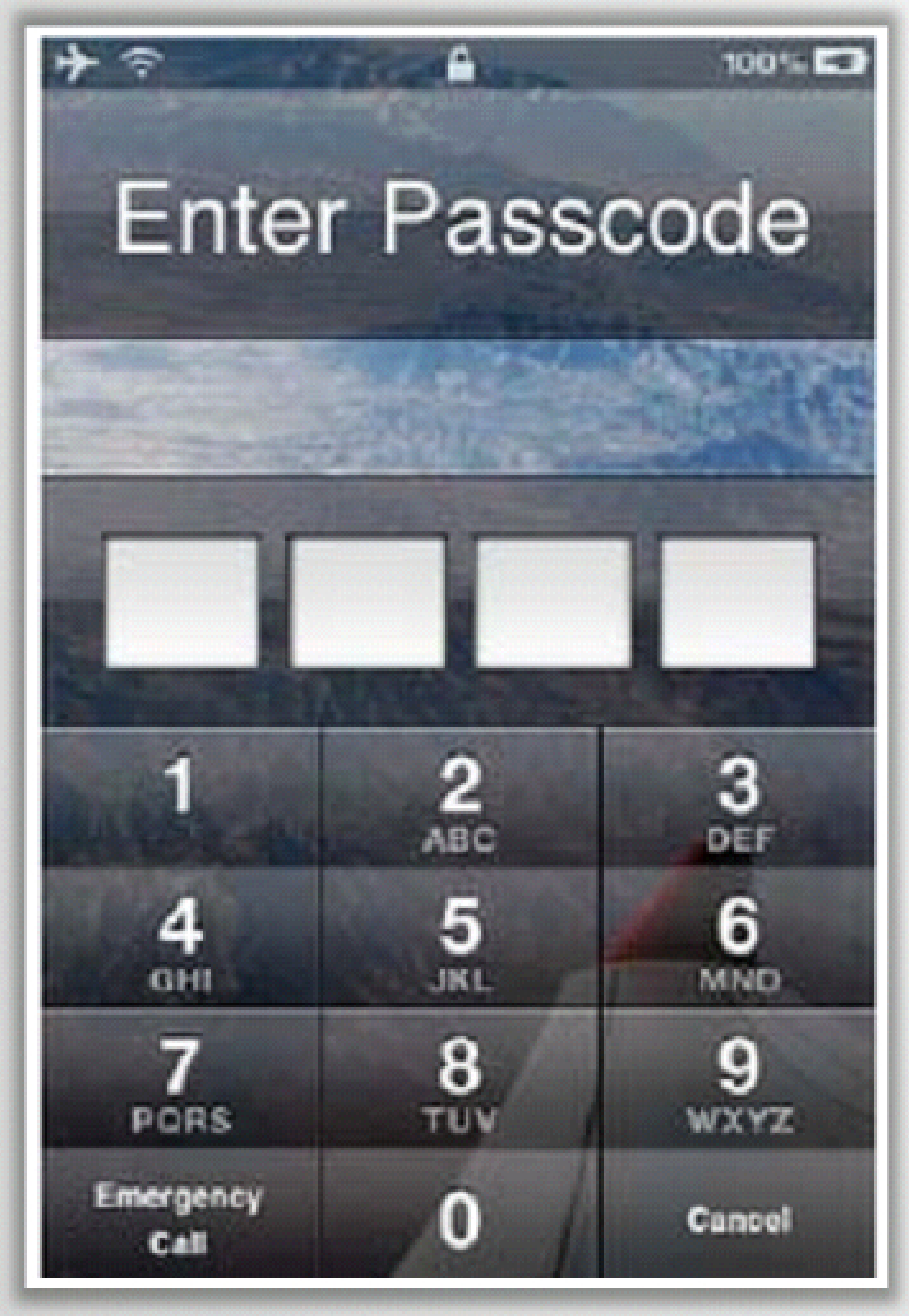
- Connect the device to the **forensics workstation** through USB
- Launch **adb shell** using ViaExtract
- Remove **password.key** file from **android directory**



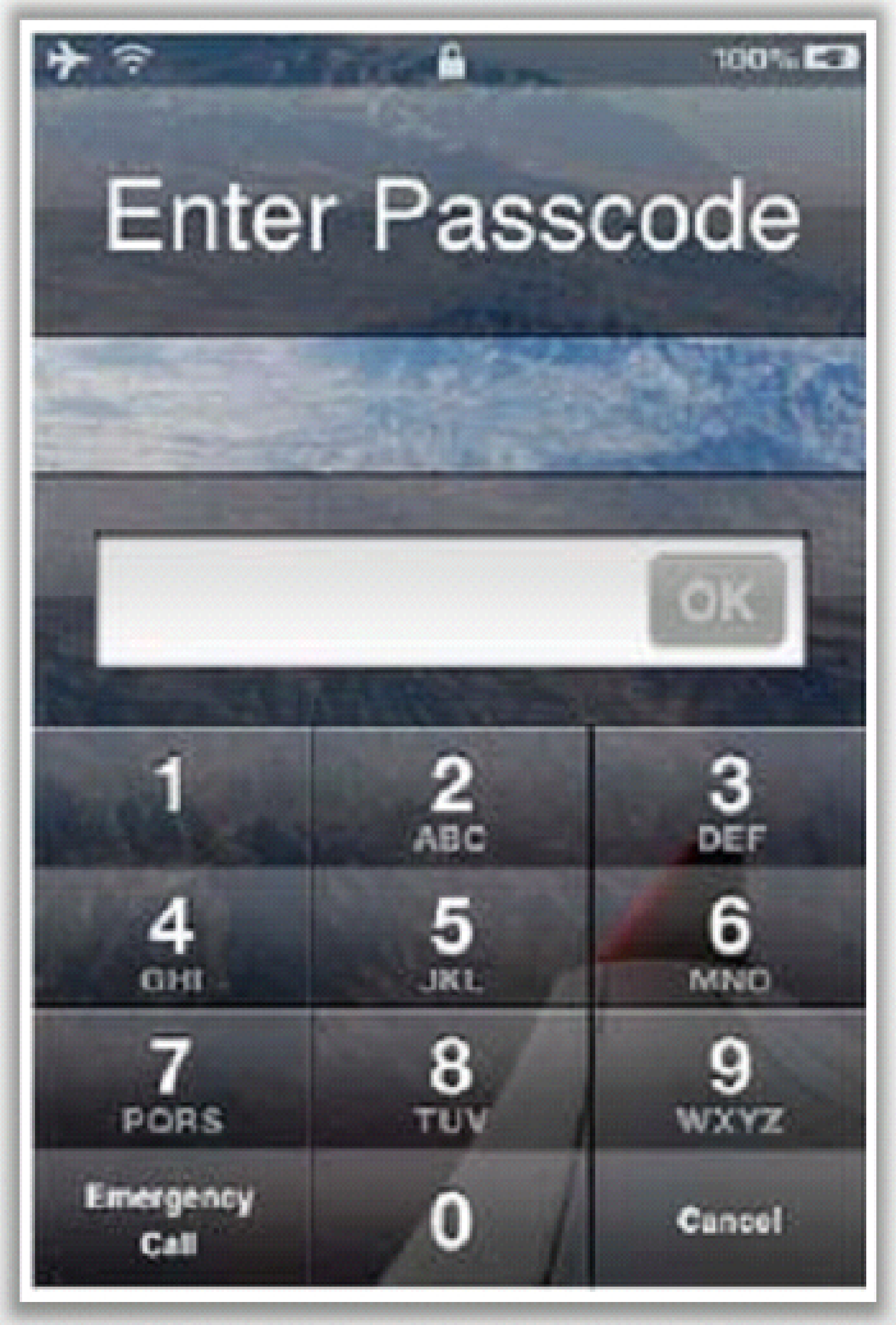
```
santoku@viaextract-ce:~$ adb shell
# cd /data/system
# ls
wpa_supplicant
entropy.dat
usagestats
batterystats.bin
uiderrors.txt
packages.xml
packages.list
registered_services
accounts.db
accounts.db-journal
sync
dropbox
called_pre_boots.dat
wallpaper_info.xml
throttle
appwidgets.xml
shared_prefs
gesture.key
device_policies.xml
password.key
history.key
# 
```

iPhone Passcodes

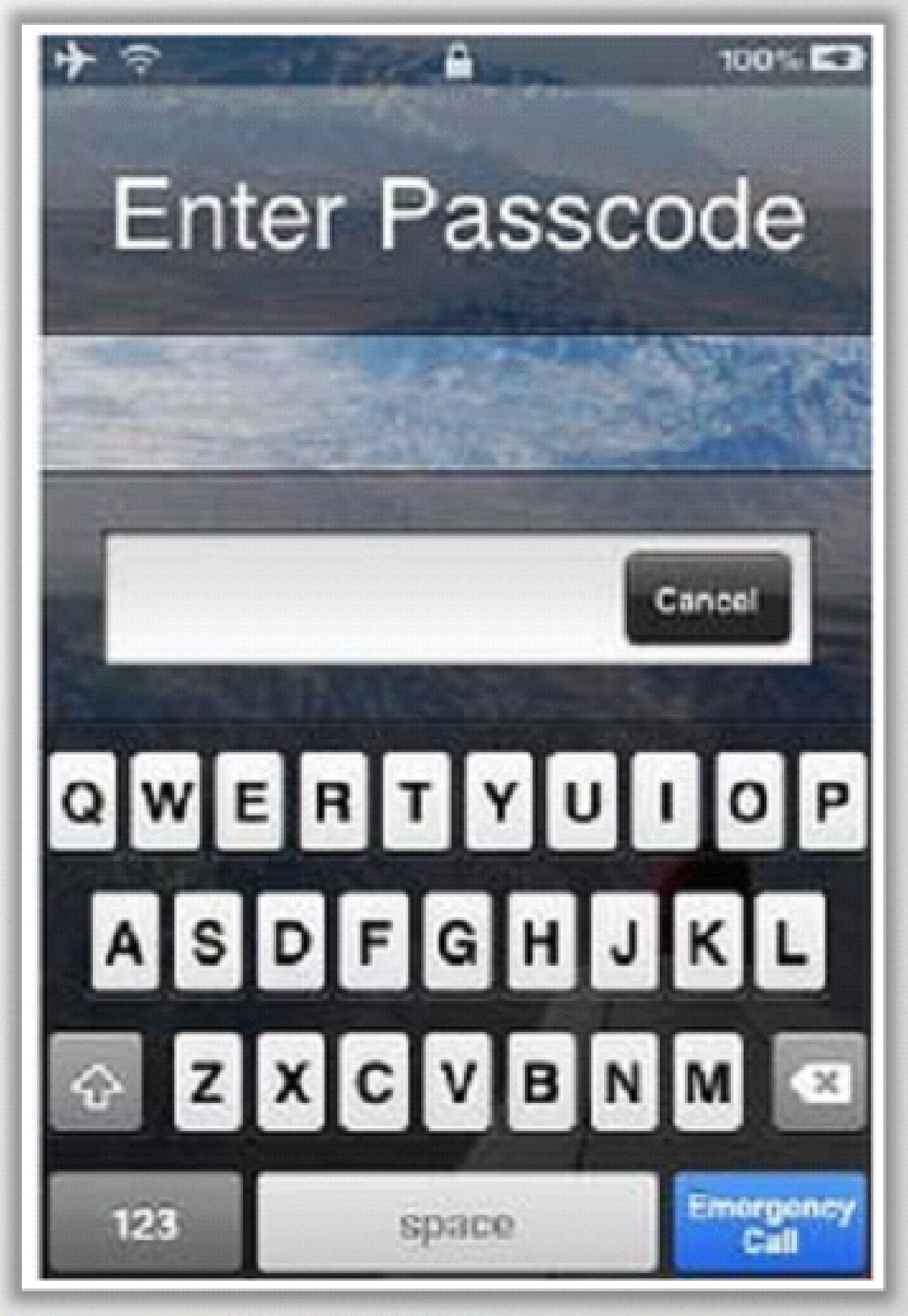
Password Type: Numeric Only
Length:4



Password Type: Numeric Only
Length: not equal to 4



Password Type: Alpha Numeric
Length: Any length

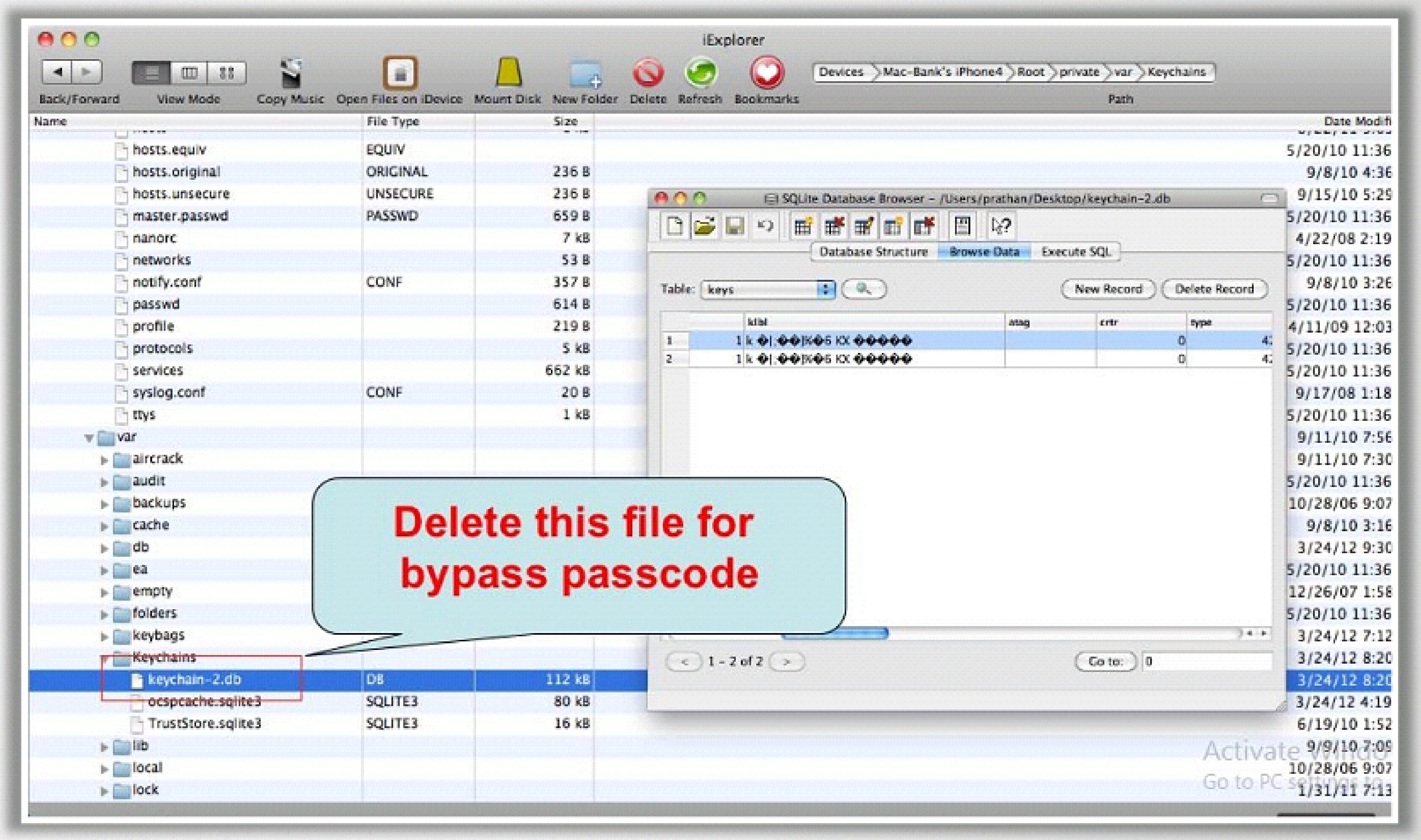


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bypassing the iPhone Passcode Using IExplorer

- Connect the device to the **workstation**
- Browse the iPhone **file system** with IExplorer
- Navigate to the **directory** /var/mobile/Library/Preferences/ and **delete com.apple.springboard.plist**
- Navigate to the directory **/var/Keychains/** and **delete keychain-2.db**
- **Reboot** the iPhone

Note: This technique works for **jailbroken** devices only



Name	File Type	Size	Date Modifi
hosts.equiv	EQUIV		5/20/10 11:36
hosts.original	ORIGINAL	236 B	9/8/10 4:36
hosts.unsecure	UNSECURE	236 B	9/15/10 5:29
master.passwd	PASSWD	659 B	5/20/10 11:36
nanorc		7 kB	4/22/08 2:19
networks		53 B	5/20/10 11:36
notify.conf	CONF	357 B	9/8/10 3:26
passwd		614 B	5/20/10 11:36
profile		219 B	4/11/09 12:03
protocols		5 kB	5/20/10 11:36
services		662 kB	5/20/10 11:36
syslog.conf	CONF	20 B	9/17/08 1:18
ttys		1 kB	5/20/10 11:36
var			9/11/10 7:56
aircrack			9/11/10 7:30
audit			5/20/10 11:36
backups			10/28/06 9:07
cache			9/8/10 3:16
db			3/24/12 9:30
ea			5/20/10 11:36
empty			12/26/07 1:58
folders			5/20/10 11:36
keybags			3/24/12 7:12
Keychains			3/24/12 8:20
keychain-2.db	DB	112 kB	3/24/12 8:20
ocspcache.sqlite3	SQLITE3	80 kB	3/24/12 4:19
TrustStore.sqlite3	SQLITE3	16 kB	6/19/10 1:52
lib			9/9/10 7:09
local			10/28/06 9:07
lock			1/31/11 7:13

SQLite Database Browser – /Users/prathan/Desktop/keychain-2.db

Table: keys

		klbl	atag	crtr	type
1	1	k �|;��|K�6 KX �����		0	4
2	1	k �|;��|K�6 KX �����		0	4

1 - 2 of 2

Delete this file for bypass passcode

Activate Windo
Go to PC settings to

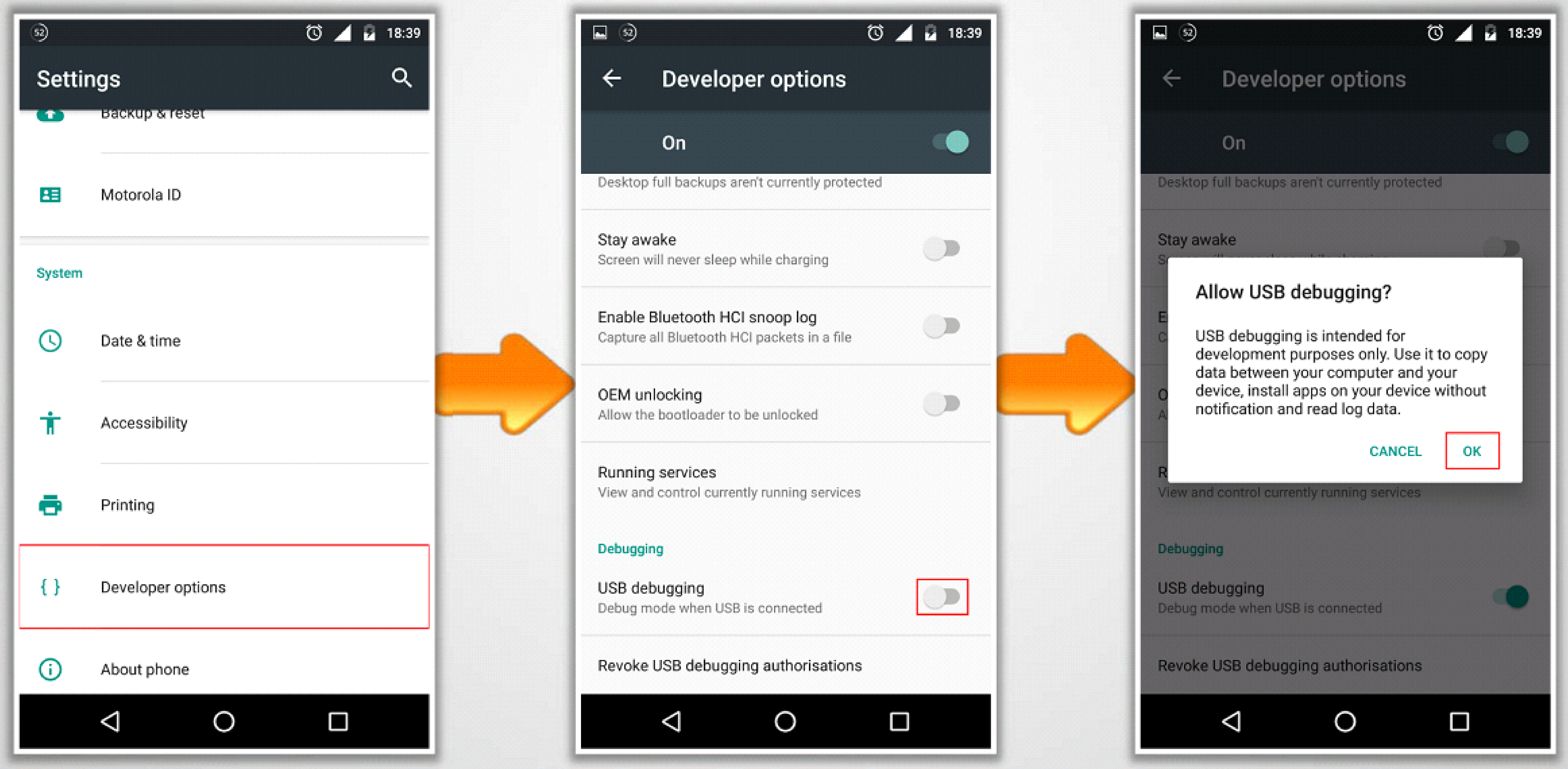
http://www.macroplant.com

- In addition to this, tools like **iPhoneBrowser**, **iFunBox**, **OpenSSHSSH** and **iMazing** also help in bypassing the passcode

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enabling USB Debugging

- Go to **Settings** → **Developer options**, and select **USB Debugging**



Desktop full backups aren't currently protected

Stay awake
Screen will never sleep while charging

Enable Bluetooth HCI snoop log
Capture all Bluetooth HCI packets in a file

OEM unlocking
Allow the bootloader to be unlocked

Running services
View and control currently running services

USB debugging
Debug mode when USB is connected

Revoke USB debugging authorisations

Allow USB debugging?

USB debugging is intended for development purposes only. Use it to copy data between your computer and your device, install apps on your device without notification and read log data.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Platform Security Removal Techniques: Jailbreaking/Rooting

- Forensic investigators use rooting/jailbreaking to **attain privileged control** (known as "root access") within device’s subsystem, so as to perform data acquisition

Android Rooting Tools

One Click Root	*https://www.oneclickroot.com*
Kingo Android ROOT	*https://www.kingoapp.com*
Towelroot	*http://towelroot.info*
RescueRoot	http://rescueroot.com

iOS Jailbreaking Tools

PANGU JAIL BREAK	*http://en.pangu.io/*
Redsn0w	*http://www.redsn0w.us*
Sn0wbreeze	*http://ih8sn0w.sexy*
GeekSn0w	*http://geeksn0w.it*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

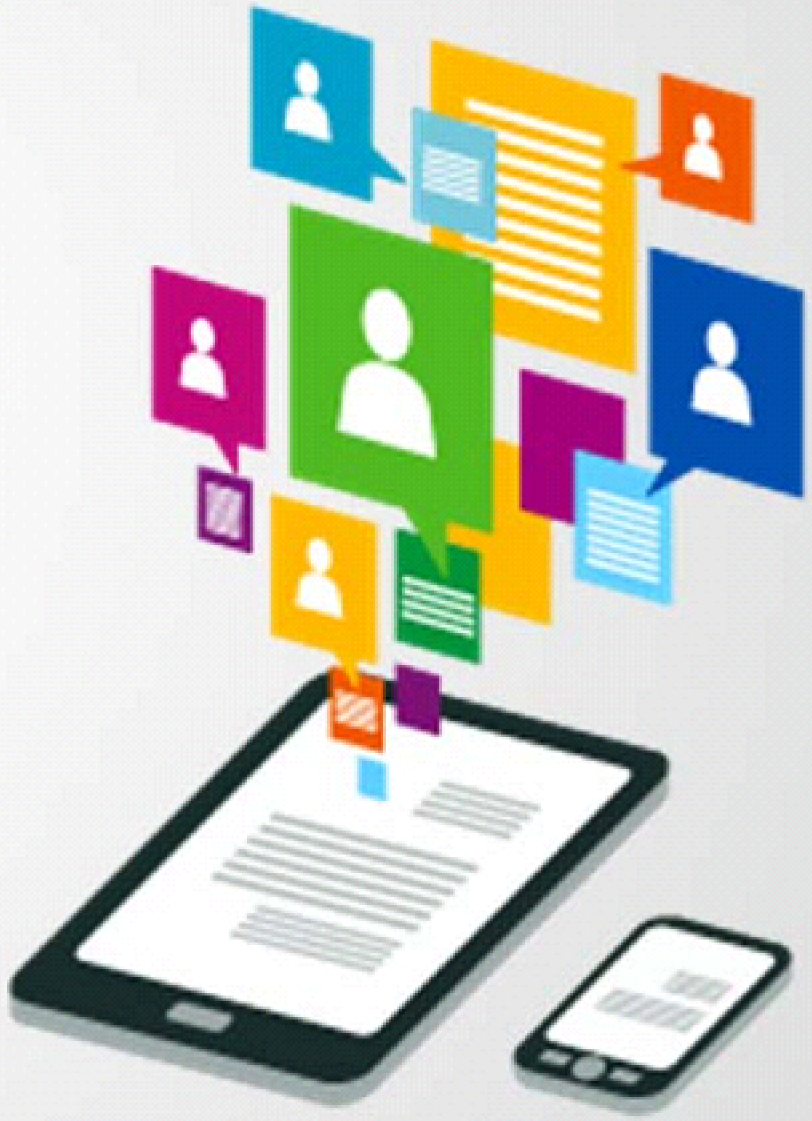
Mobile Evidence Acquisition

- The seized mobile phone undergoes **data acquisition** and **forensic imaging** process at the forensics workstation
- During the acquisition process, all possible data from **internal** and **external** memory of the mobile phone is extracted for forensic analysis

- Data acquisition and forensic analysis requires:
  - **Unlocking** the device
  - **Rooting** or **Jailbreaking** of the device
  - Enabling **USB debugging** mode in the device

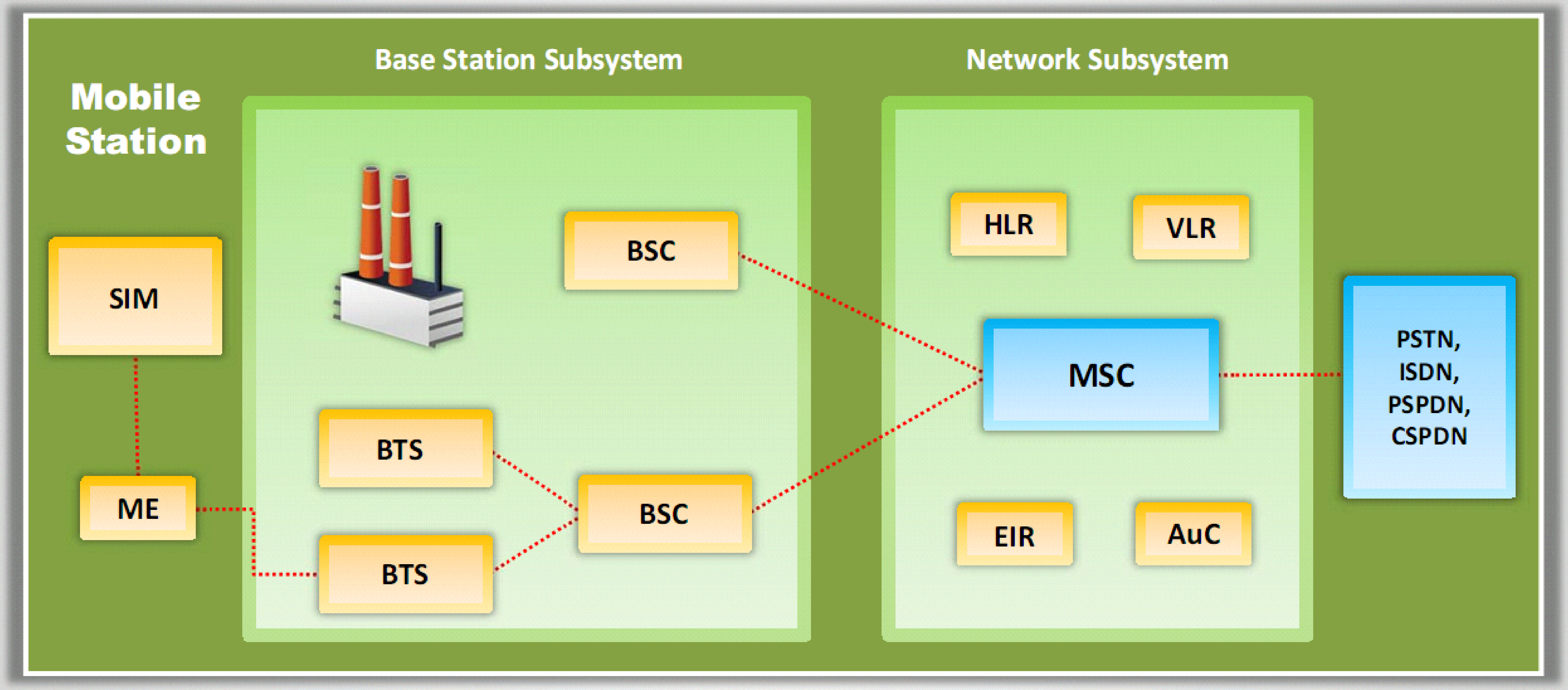
Data Acquisition Methods

- Cellular Data Acquisition
- SIM File System Acquisition
- Logical Acquisition
- Physical Acquisition
- File System Acquisition



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cellular Network



SIM: Subscriber Identity Module

MSC: Mobile Services Switching Center

HLR: Home Location Register

BTS: Base Transceiver Station

AuC: Authentication Center

VLR: Visitor Location Register

BSC: Base Station Controller

ME: Mobile Equipment

EIR: Equipment Identity Register

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Components of Cellular Network

1. Mobile Switching Center (MSC): It is the **switching system** for the cellular network

2. Base Transceiver Station (BTS): It is the radio transceiver equipment that **communicates with mobile phones**

3. Base Station Controller (BSC): It manages the transceiver's equipment and performs **channel assignment**

4. Base Station Subsystem (BSS): is responsible for managing the radio network and is controlled by the **Mobile Service Switching Center** (MSC). It consists of the elements Base Station controller (BSC), Base Transceiver Station (BTS), and Transcoder (TC)

5. Home Location Register (HLR): It is the database at the MSC. It is the **central repository system** for subscriber data and service information

6. Visitor Location Register (VLR): It is the **database** used in conjunction with the HLR for mobile phones roaming outside their service area

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Different Cellular Networks

1 Code Division Multiple Access (CDMA)

2 Enhanced Data Rates for GSM Evolution (EDGE)

3 Integrated Digital Enhanced Network (iDEN)

4 General Packet Radio Service (GPRS)

5 Global System for Mobile Communications (GSM)

6 High Speed Downlink Packet Access (HSDPA)

7 Time Division Multiple Access (TDMA)

8 Universal Mobile Telecommunications System (UMTS)

9 Unlicensed Mobile Access (UMA)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cell Site Analysis: Analyzing Service Provider Data

Service provider data can act as **back up evidence** for the mobile forensics investigator

It is useful when the **attacker** or owner of the mobile phone has deleted call history and/or text messages from the device in order to **wipe out** evidence

It can also be required in the following cases:

- When recovering of **deleted data** is not possible
- When **location-based** services are not turned ON in the phone

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cell Site Analysis: Analyzing Service Provider Data (Cont'd)

- Potential evidence that could be obtained from **Service Provider Data**:
  - Phone owner's location
  - Call Detail Records (**CDR**)
  - Billing information
  - Whether mobile phone was in stationary or moving state at a specific interval of time

- CDR can provide a detail information about particular call made
- CDR has **probative value** for investigative or legal purposes
- Investigator should investigate both device data (**internal, external,** and **SIM**) and service provider data to find out potential evidence

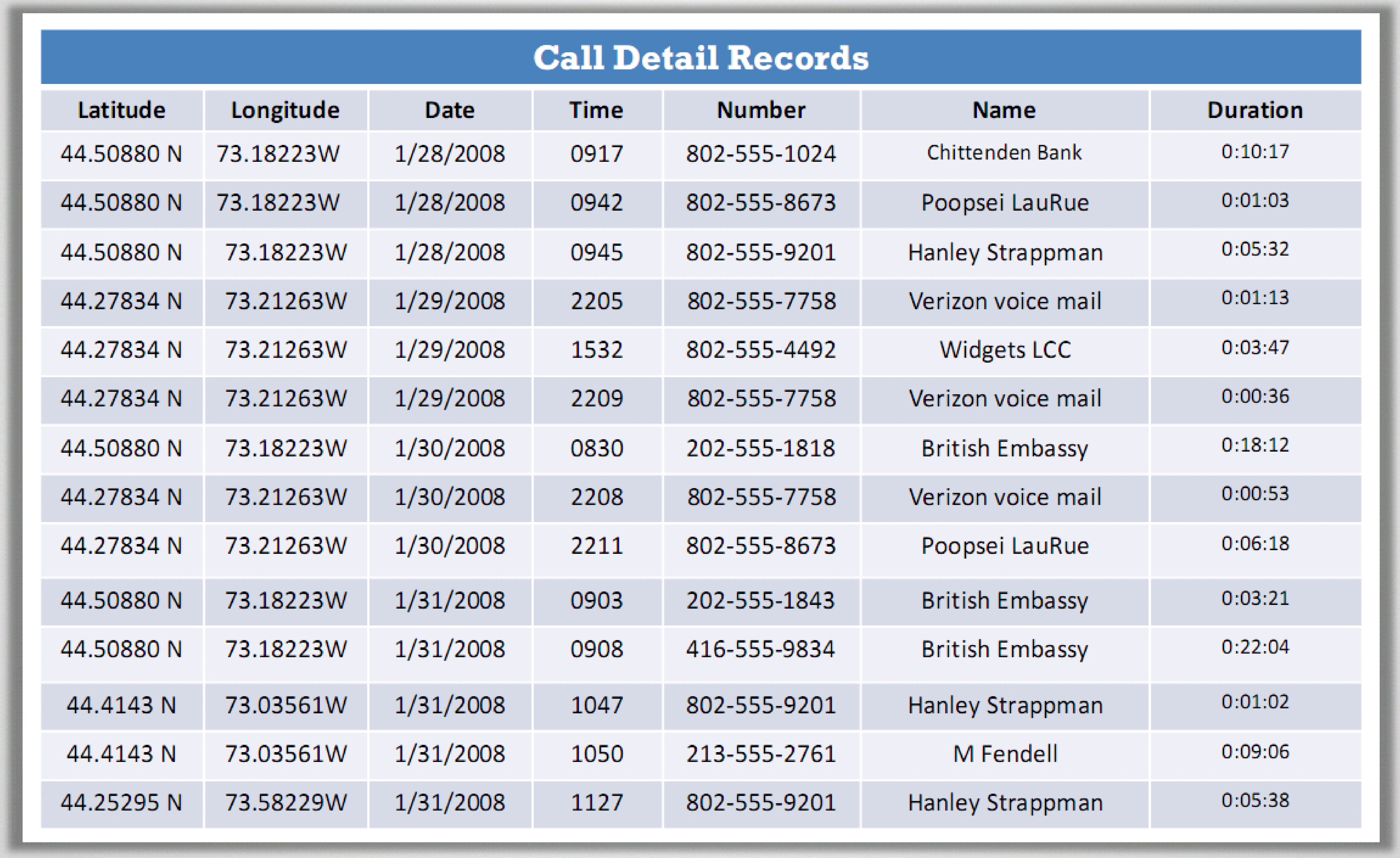
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

CDR Contents

1	The phone number of the subscriber from where call originated (calling party, A-party)
2	The phone number receiving the call (called party, B-party)
3	The starting time of the call (date and time)
4	The call duration
5	The billing phone number that is charged for the call
6	The identification of the telephone exchange or equipment writing the record
7	A unique sequence number identifying the record
8	Additional digits on the called number used to route or charge the call
9	The disposition or the results of the call, indicating, for example, whether the call was connected
10	The route by which the call entered the exchange
11	The route by which the call left the exchange
12	Call type (voice, SMS, etc.)
13	Any fault condition encountered

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sample CDR Log File



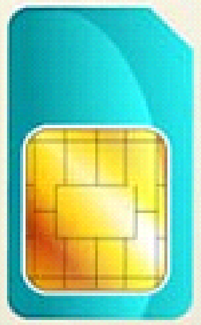
Call Detail Records

Latitude	Longitude	Date	Time	Number	Name	Duration
44.50880 N	73.18223W	1/28/2008	0917	802-555-1024	Chittenden Bank	0:10:17
44.50880 N	73.18223W	1/28/2008	0942	802-555-8673	Poopsei LauRue	0:01:03
44.50880 N	73.18223W	1/28/2008	0945	802-555-9201	Hanley Strappman	0:05:32
44.27834 N	73.21263W	1/29/2008	2205	802-555-7758	Verizon voice mail	0:01:13
44.27834 N	73.21263W	1/29/2008	1532	802-555-4492	Widgets LCC	0:03:47
44.27834 N	73.21263W	1/29/2008	2209	802-555-7758	Verizon voice mail	0:00:36
44.50880 N	73.18223W	1/30/2008	0830	202-555-1818	British Embassy	0:18:12
44.27834 N	73.21263W	1/30/2008	2208	802-555-7758	Verizon voice mail	0:00:53
44.27834 N	73.21263W	1/30/2008	2211	802-555-8673	Poopsei LauRue	0:06:18
44.50880 N	73.18223W	1/31/2008	0903	202-555-1843	British Embassy	0:03:21
44.50880 N	73.18223W	1/31/2008	0908	416-555-9834	British Embassy	0:22:04
44.4143 N	73.03561W	1/31/2008	1047	802-555-9201	Hanley Strappman	0:01:02
44.4143 N	73.03561W	1/31/2008	1050	213-555-2761	M Fendell	0:09:06
44.25295 N	73.58229W	1/31/2008	1127	802-555-9201	Hanley Strappman	0:05:38

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Subscriber Identity Module (SIM)

SIM is a removable component that contains essential **information about the subscriber**



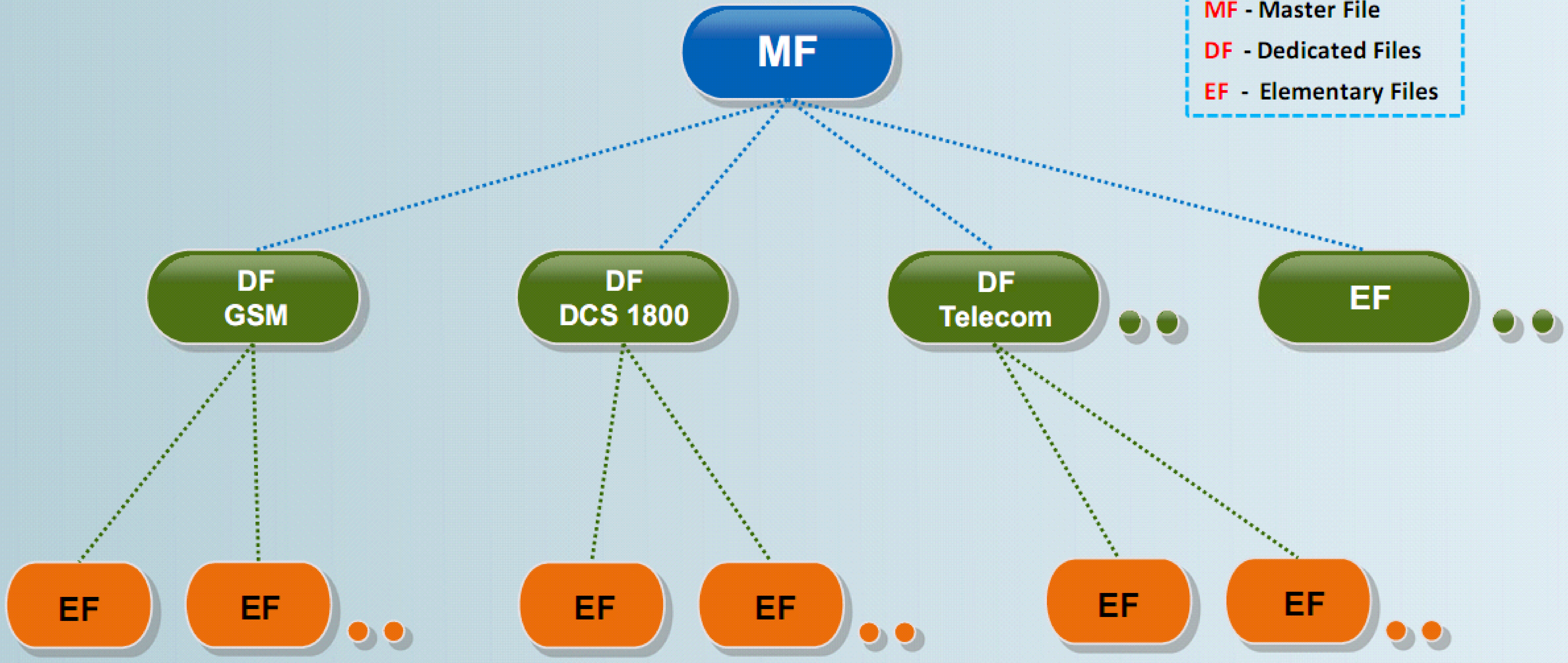
It has both **volatile** and **nonvolatile memory**

The **file system** of a SIM resides in nonvolatile memory

The SIM's main function entails **authenticating the user of the cell phone** to the network to gain access to subscribed services

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SIM File System



MF - Master File

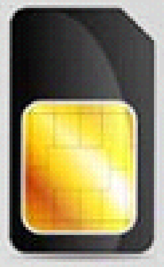
DF - Dedicated Files

EF - Elementary Files

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Stored in a Subscriber Identity Module

SIM is a microcontroller-based smart card that stores important data including:



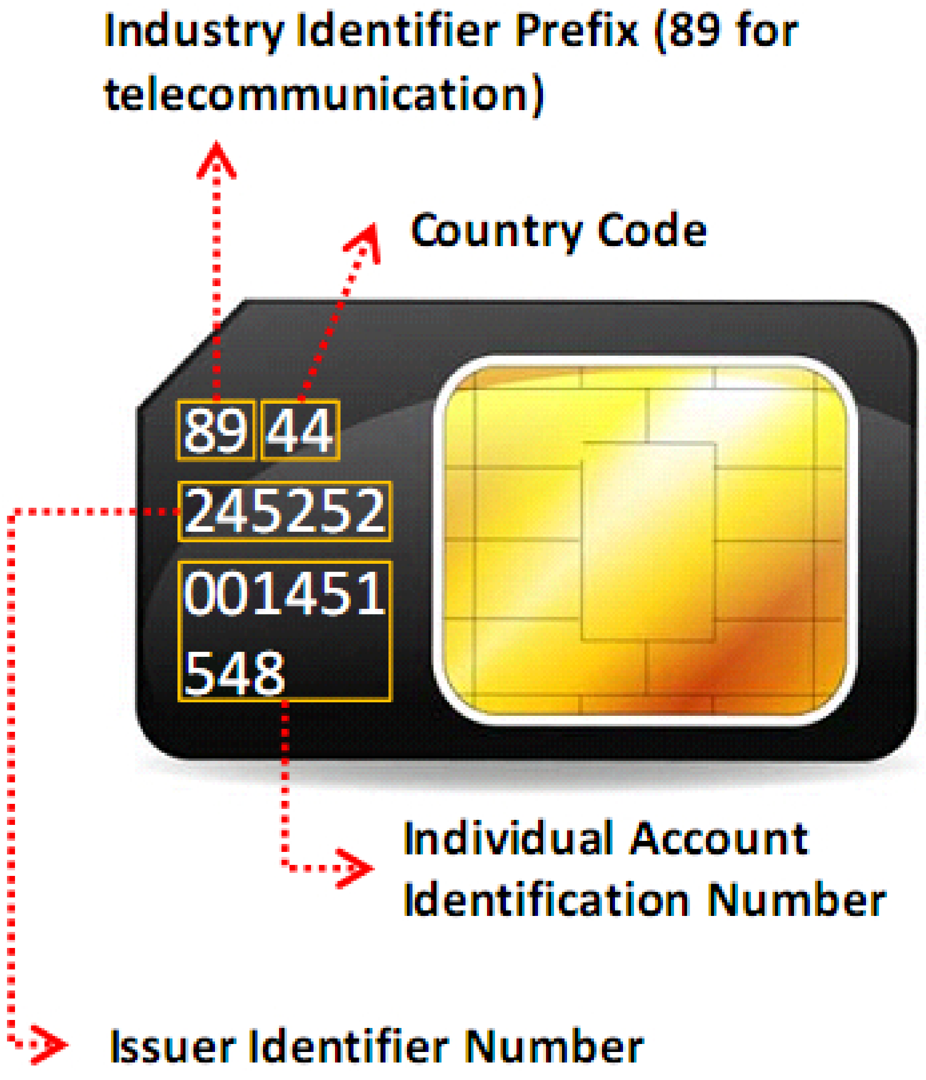
- Integrated circuit card identifier (ICCID)
- International mobile subscriber identity (IMSI)
- Service provider name (SPN)
- Mobile country code (MCC)
- Mobile network code (MNC)
- Mobile subscriber identification number (MSIN)
- Mobile international subscriber directory number (MSISDN)
- Abbreviated dialing numbers (ADN)
- Last dialed numbers (LDN)
- Short message service (SMS)
- Text Message parameters (SMSP)
- Text message status (SMSS)
- Phase ID (Phase)
- SIM Service table (SST)
- HPLMN search period (HPLMNSP)
- PLMN selector (PLMNsel)
- Forbidden PLMNs (FPLMN)
- Capability configuration parameter (CCP)
- Access control class (ACC)
- Broadcast control channels (BCCH)
- Language preference (LP)
- Card holder verification (CHV1 and CHV2)
- Ciphering key (Kc)
- Ciphering key sequence number
- Emergency call code
- Fixed dialing numbers (FDN)
- Dialing Extension (EXT1 & EXT2)
- Groups (GID1 & GID2)
- Preferred network messages (CBMI)
- Calls per unit (PUCT)
- Accumulated Call Meter (ACM)
- Call Limit (ACMmax)
- Location Information (LOCI)
- Local area identity (LAI)
- Own dialing number
- Temporary mobile subscriber identity (TMSI)
- Routing area identifier (RIA) network code
- Service dialing numbers (SDNs)
- Depersonalization Keys

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Integrated Circuit Card Identification (ICCID)

ICCID

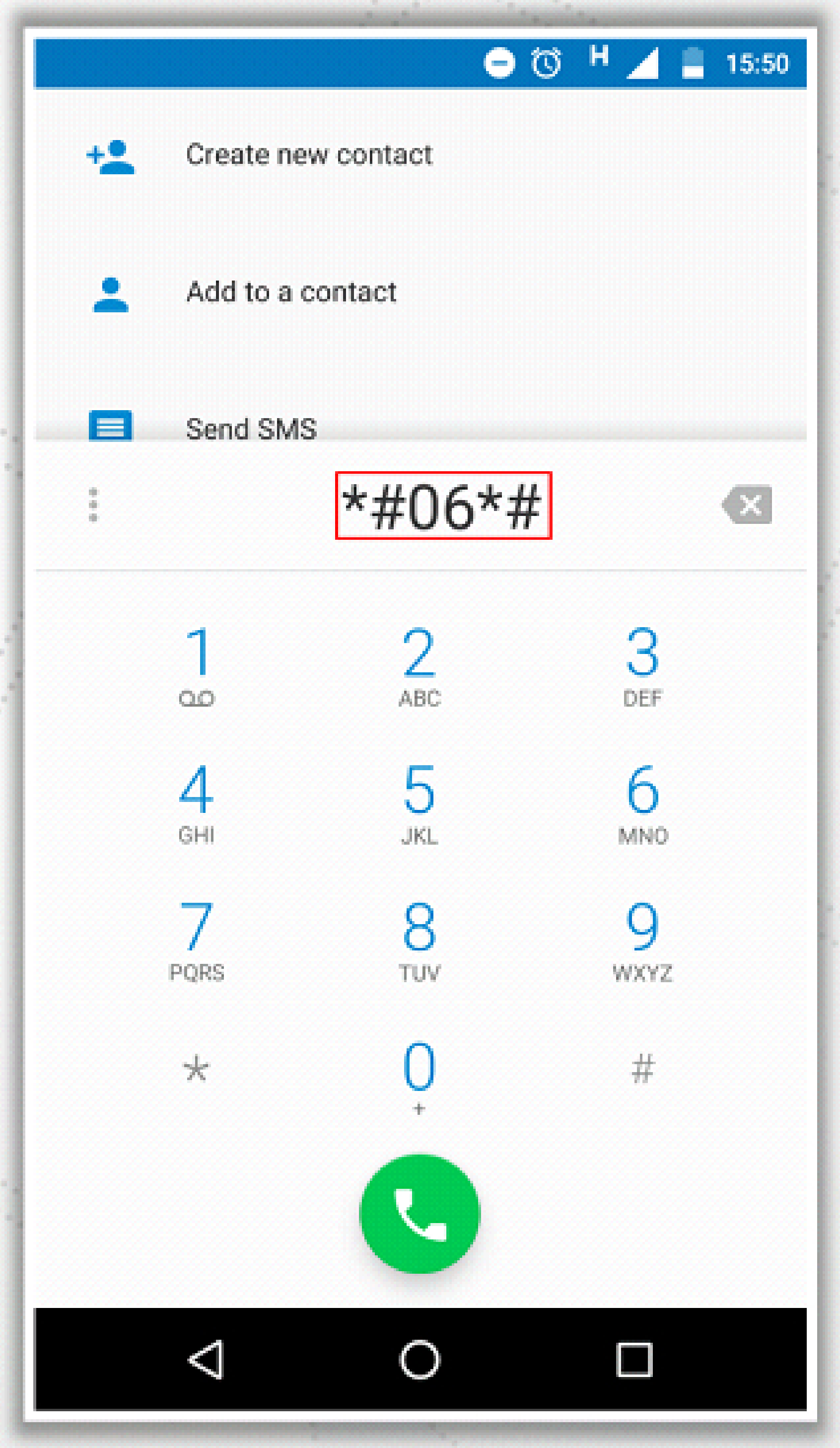
- The ICCID of the (U)SIM can be up to **20 digits long**
- It consists of an **industry identifier prefix** (89 for telecommunications), followed by a country code, an issuer identifier number, and an individual **account identification** number
- This code helps to identify the **country** and **network operator's name**
- If ICCID does not exist on the SIM, get it by using a (U)SIM acquisition tool such as **ForensicSIM** Toolkit


Industry Identifier Prefix (89 for telecommunication)
Country Code
89 44
245252
001451
548
Individual Account Identification Number
Issuer Identifier Number

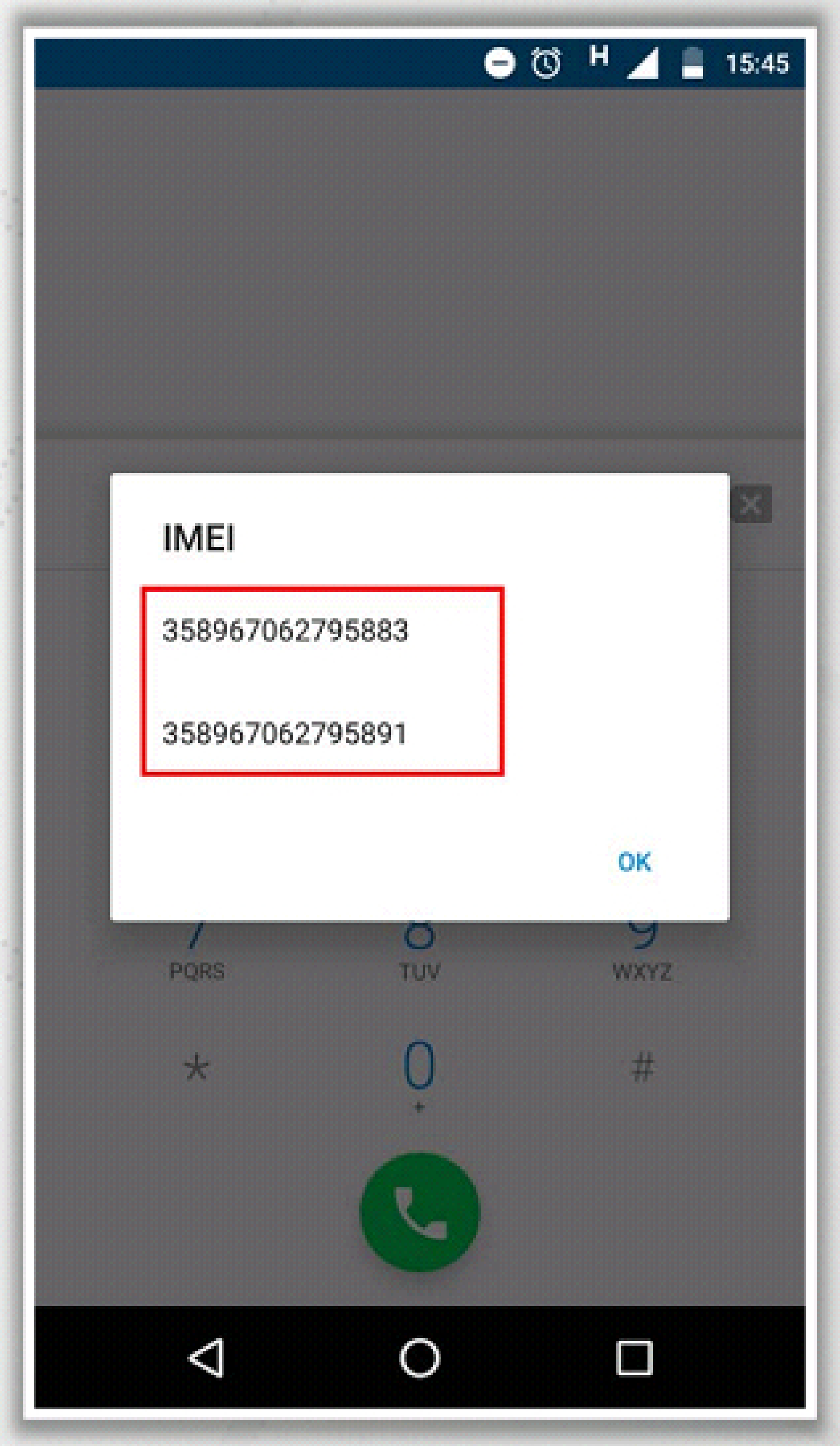
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

International Mobile Equipment Identifier (IMEI)

- IMEI is a **15-digit number** that indicates the manufacturer, model type, and country of approval for GSM devices
- First eight digits, known as the **Type Allocation Code** (TAC), give the model and origin
- For powered on GSM and UMTS phones, the IMEI can be obtained by keying in ***#06#**



#06#



IMEI

358967062795883

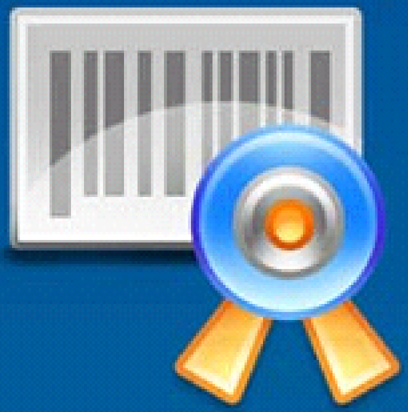
358967062795891

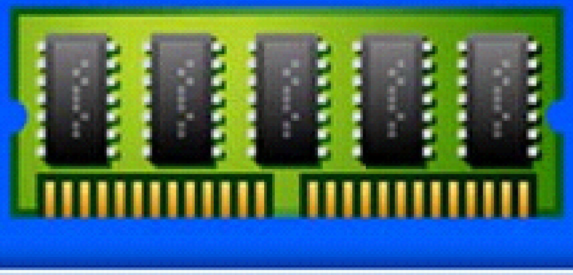
OK

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Electronic Serial Number (ESN)

- ESN is a unique **32-bit identifier recorded on a secure chip** in a mobile phone by the manufacturer
- The first 8-14 bits identify the **manufacturer**, and the remaining bits identify the assigned **serial number**





Mobile Station Information

ESN (Hex):	0x801599A1	
ESN (Dec):	28-01415585	
MCC:	0	
MCC:		
MSD1:	0000009233	
Slot Class:	Slotted	
Slot Cycle Index:	1	
Protocol Revision:	7 (IS-2000-A)	
Band Class:	US Cell	US PC9
MS Operating Mode:	COMA	COMA
Max EIRP (dBII):	-7	-7
Registration Type:	Timer Based	
QPCH Supported:	Yes	
Enhanced RC Support:	Yes	
Min Power Control Step:	0.25 d8	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SIM Cloning

- **Duplicating a SIM card** for further investigation in order to avoid **accidental tampering** of original SIM data

SIM Cloning Tool - MOBILedit

http://www.mobiledit.com

Prerequisites:

- SIM card Reader
- Blank SIM card or Super SIM card
- SIM cloning software

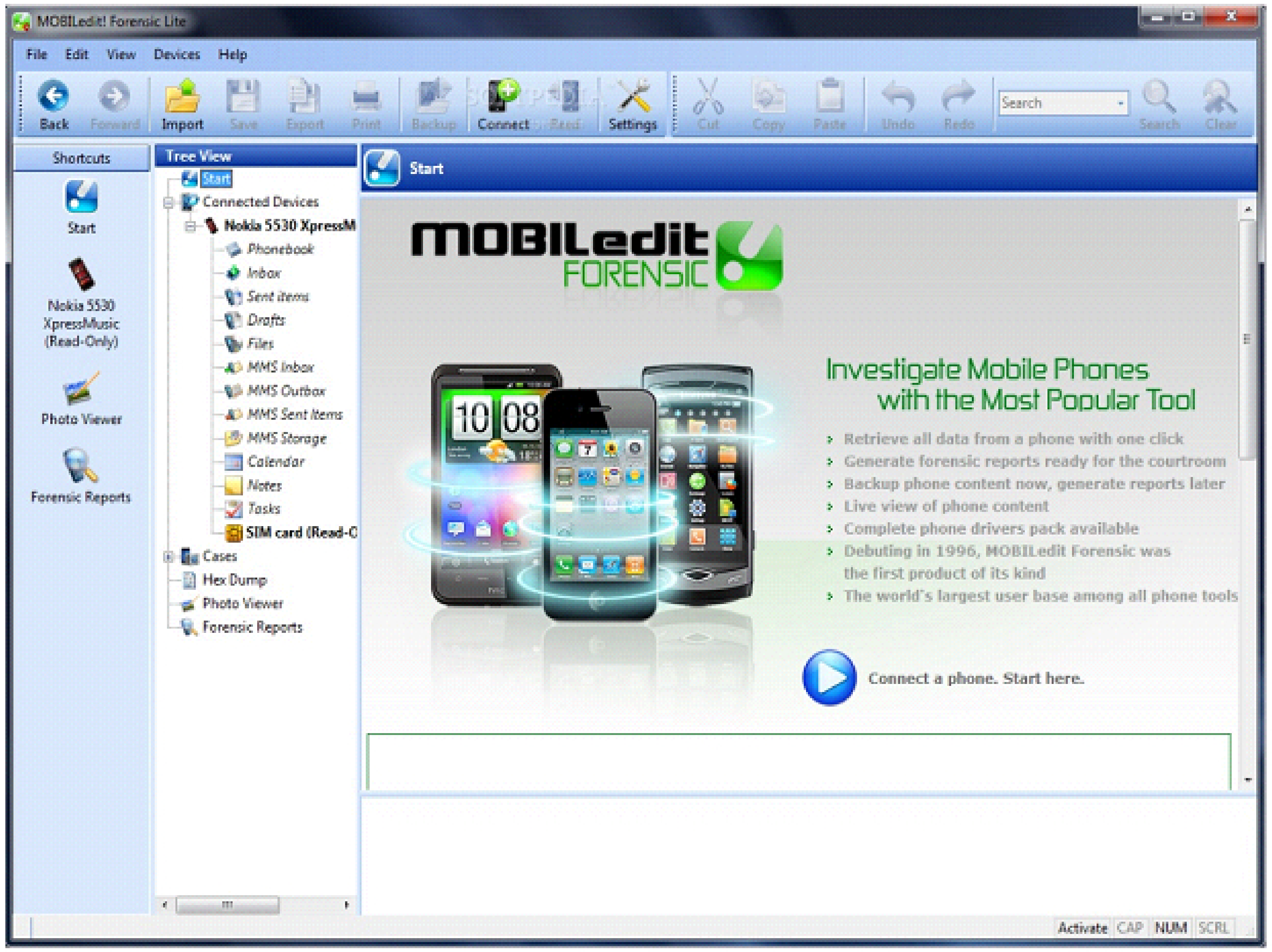
SIM Cloning Tools

- SIMiFOR ASC - SIM Cloner (http://www.forensicts.co.uk)
- 001Micron Data Recovery (http://www.simrecovery.com/)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SIM Data Acquisition Tools

MOBILedit



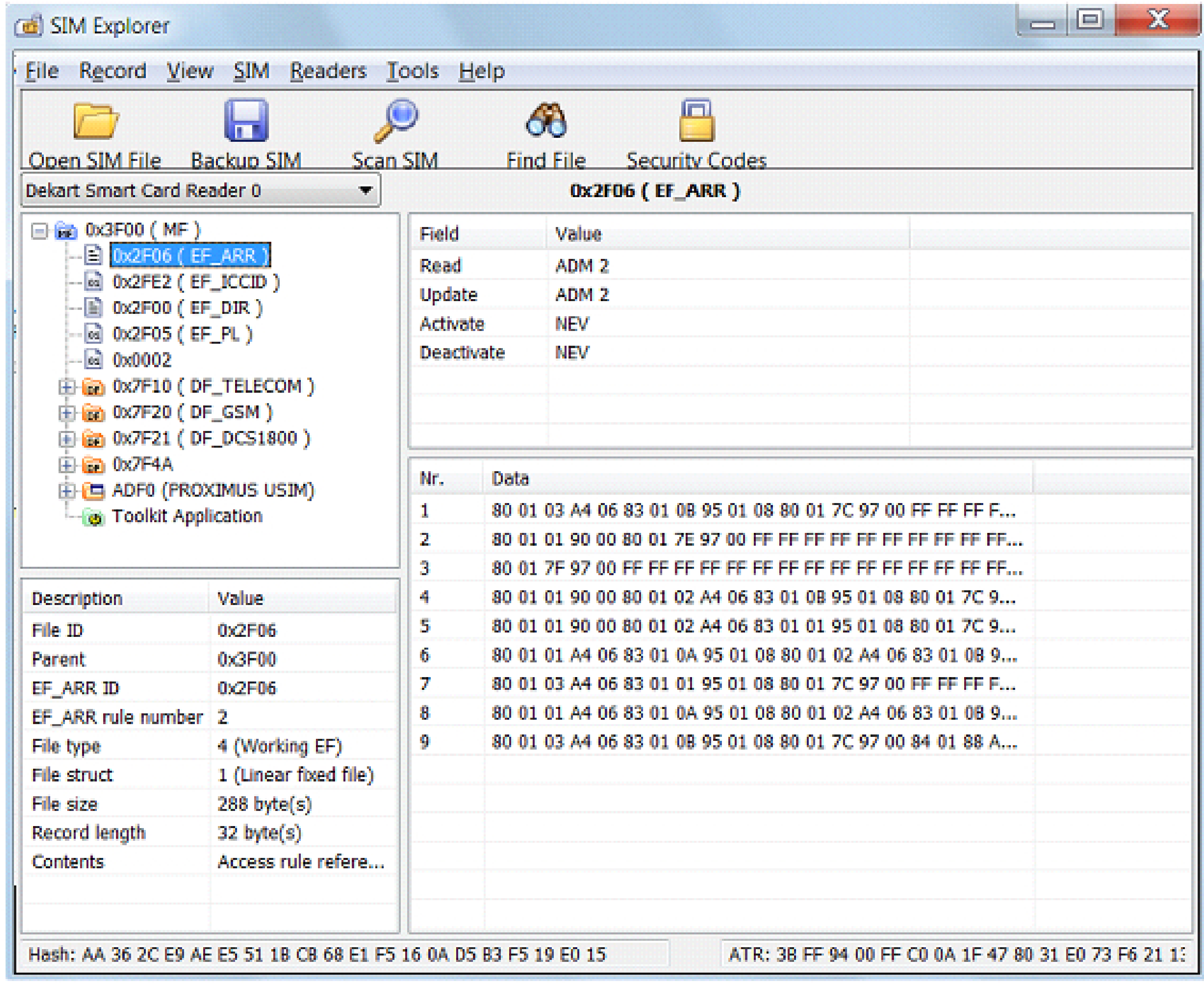
Investigate Mobile Phones with the Most Popular Tool

- Retrieve all data from a phone with one click
- Generate forensic reports ready for the courtroom
- Backup phone content now, generate reports later
- Live view of phone content
- Complete phone drivers pack available
- Debuting in 1996, MOBILedit Forensic was the first product of its kind
- The world's largest user base among all phone tools

Connect a phone. Start here.

http://www.mobiledit.com

SIM Explorer



0x2F06 (EF_ARR)

Field	Value
Read	ADM 2
Update	ADM 2
Activate	NEV
Deactivate	NEV

Nr.	Data
1	80 01 03 A4 06 83 01 0B 95 01 08 80 01 7C 97 00 FF FF FF F...
2	80 01 01 90 00 80 01 7E 97 00 FF FF FF FF FF FF FF FF FF FF...
3	80 01 7F 97 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF...
4	80 01 01 90 00 80 01 02 A4 06 83 01 0B 95 01 08 80 01 7C 9...
5	80 01 01 90 00 80 01 02 A4 06 83 01 01 95 01 08 80 01 7C 9...
6	80 01 01 A4 06 83 01 0A 95 01 08 80 01 02 A4 06 83 01 08 9...
7	80 01 03 A4 06 83 01 01 95 01 08 80 01 7C 97 00 FF FF FF F...
8	80 01 01 A4 06 83 01 0A 95 01 08 80 01 02 A4 06 83 01 08 9...
9	80 01 03 A4 06 83 01 0B 95 01 08 80 01 7C 97 00 84 01 88 A...

Description	Value
File ID	0x2F06
Parent	0x3F00
EF_ARR ID	0x2F06
EF_ARR rule number	2
File type	4 (Working EF)
File struct	1 (Linear fixed file)
File size	288 byte(s)
Record length	32 byte(s)
Contents	Access rule refere...

Hash: AA 36 2C E9 AE E5 51 1B CB 68 E1 F5 16 0A D5 B3 F5 19 E0 15

ATR: 3B FF 94 00 FF C0 0A 1F 47 80 31 E0 73 F6 21 1:

http://www.dekart.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SIM Data Acquisition Tools (Cont'd)

Cellebrite UFED Logical Analyzer
http://www.cellebrite.com

AccessData Mobile Phone Examiner (MPE) Plus
http://accessdata.com

MOBILedit! Forensic
http://www.mobiledit.com

EnCase Forensic
https://www.guidancesoftware.com

Paraben's SIM-Card Seizure
https://www.paraben.com

Data Pilot Secure View Kit
http://www.datapilot.com

SIMiFOR
http://www.forensicts.co.uk

USIM Detective
http://www.quantaq.com

SIM Explorer
http://www.dekart.com

SIM Card Data Recovery
http://www.datadoctor.in

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SIM Forensic Analysis Tools

SIMIS 2.0
http://www.crownhillmobile.com

SIMIS 3G
http://www.crownhillmobile.com

SIMulate
http://www.crownhillmobile.com

SIMXtractor
http://www.cyberforensics.in

Last SIM Details
http://lastsimdetails.blogspot.in

SIM Brush
https://code.google.com

USIM detective
http://www.quantaq.com

SIMQuery
http://vidstrom.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Logical Acquisition

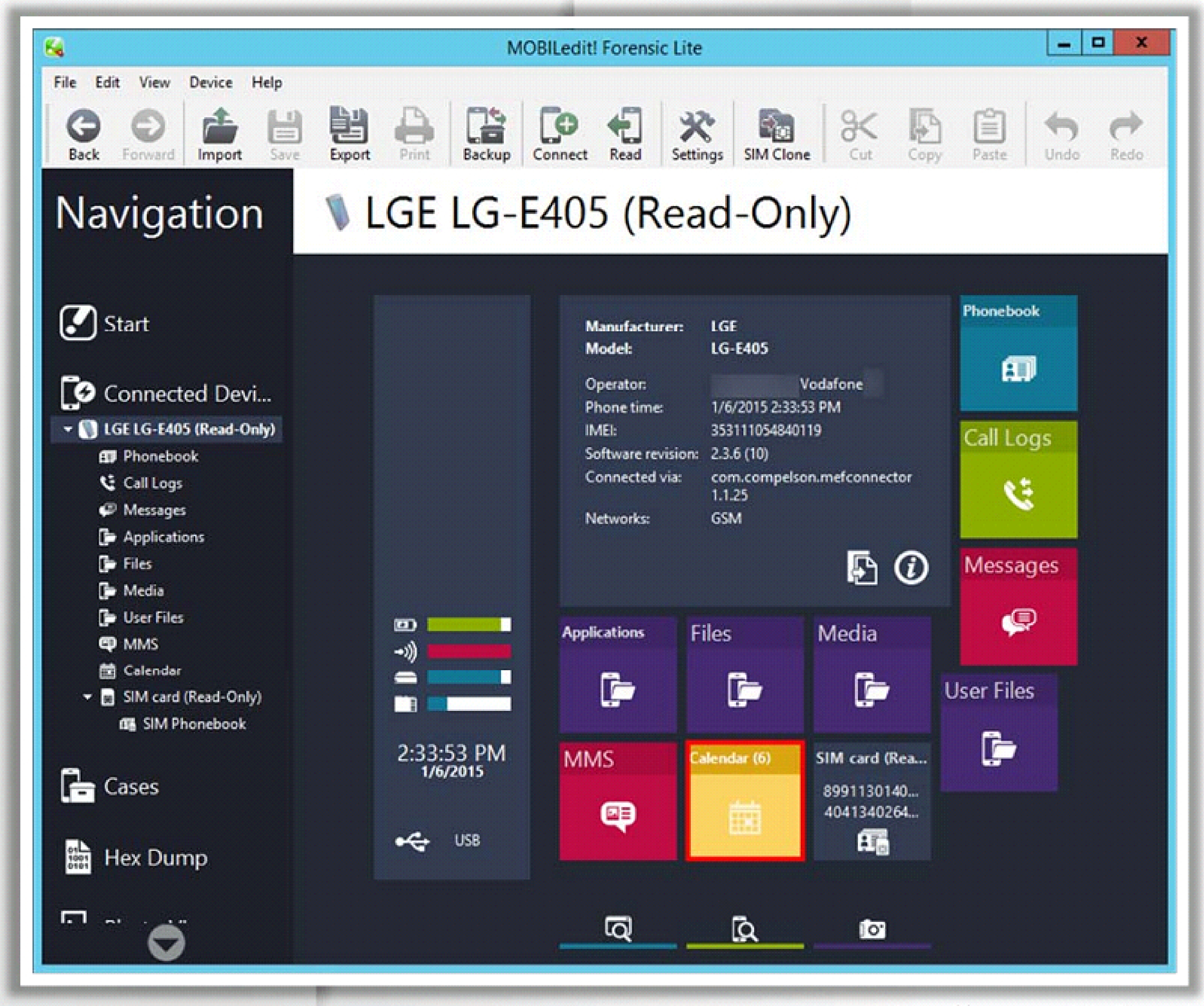
Logical acquisition involves creating a bit-by-bit copy of **logical storage** of mobile phone

Logical storage includes data stored within mobile **files** and **directories**

Mobile data is extracted through **mobile device's OS**, using a known set of commands

Android Logical Acquisition Using MOBILedit

- Connect mobile device to the forensics workstation through USB
- Launch **MOBILedit**
- Logical extraction of data will be performed automatically



LGE LG-E405 (Read-Only)

Manufacturer: LGE
Model: LG-E405
Operator: [redacted] Vodafone
Phone time: 1/6/2015 2:33:53 PM
IMEI: 353111054840119
Software revision: 2.3.6 (10)
Connected via: com.compelson.mefconnector 1.1.25
Networks: GSM

8991130140...
4041340264...

http://www.mobiledit.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Additional Logical Acquisition Tools

UFED Logical Analyzer

Source: www.cellebrite.com

XRY LOGICAL

Source: www.msab.com

Paraben Device Seizure

Source: www.paraben.com

Oxygen Forensic® Extractor

Source: www.oxygen-forensic.com

DATA PILOT

DataPilot

Source: www.datapilot.com

MPE+
Mobile Phone Examiner *Plus*

Mobile Phone Examiner *Plus*

Source: www.accessdata.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Physical Acquisition

- Physical acquisition involves creating a bit-by-bit copy of data stored in the **internal flash memory** of mobile phone
- It extracts **maximum amount of data** directly from the mobile device's flash memory(s)
- It can also **extract hidden or deleted data** from flash memories
- It is the most difficult extraction as **manufacturers** of mobile devices often do not allows arbitrary reading of the device's memory

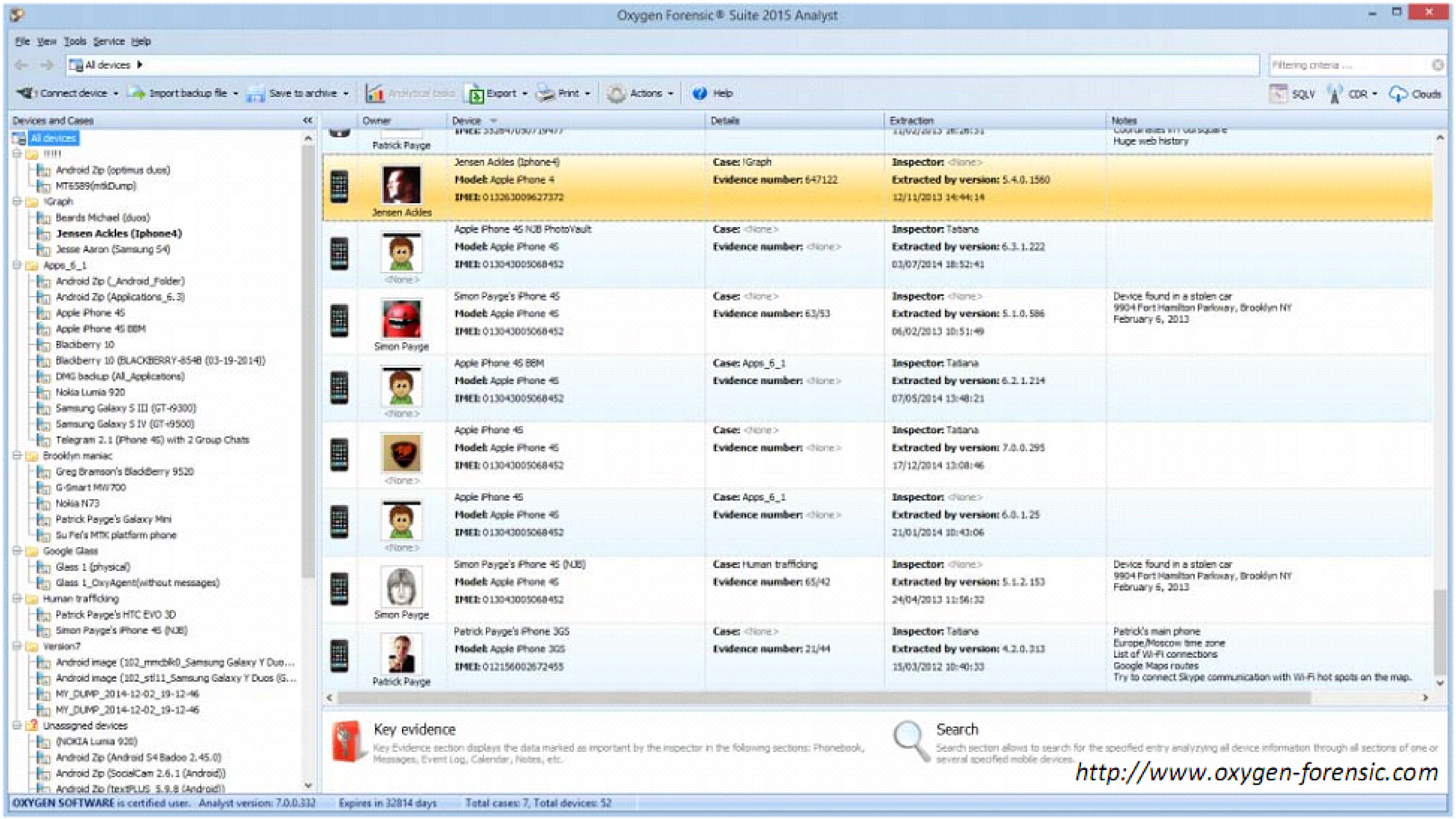
Physical Extraction Techniques:

- Physical extraction using forensics tools such as:
  - **ViaExtract**
  - **XRY Physical**
  - **UFED Physical Analyzer**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Physical Acquisition Using Oxygen Forensic Detective

- Launch **Oxygen Forensic Detective**
- Connect mobile device to the forensics workstation through USB
- Perform **physical acquisition** using **Oxygen Forensic Suite**



Devices and Cases

- All devices
  - !!!!!
    - Android Zip (optimus duos)
    - MT6589(mtkDump)
  - !Graph
    - Beards Michael (duos)
    - **Jensen Ackles (Iphone4)**
    - Jesse Aaron (Samsung S4)
  - Apps_6_1
    - Android Zip (_Android_Folder)
    - Android Zip (Applications_6.3)
    - Apple iPhone 4S
    - Apple iPhone 4S BBM
    - Blackberry 10
    - Blackberry 10 (BLACKBERRY-8548 (03-19-2014))
    - DMG backup (All_Applications)
    - Nokia Lumia 920
    - Samsung Galaxy S III (GT-i9300)
    - Samsung Galaxy S IV (GT-i9500)
    - Telegram 2.1 (iPhone 4S) with 2 Group Chats
  - Brooklyn maniac
    - Greg Branson's BlackBerry 9520
    - G-Smart MW700
    - Nokia N73
    - Patrick Payge's Galaxy Mini
    - Su Fei's MTK platform phone
  - Google Glass
    - Glass 1 (physical)
    - Glass 1_OxyAgent(without messages)
  - Human trafficking
    - Patrick Payge's HTC EVO 3D
    - Simon Payge's iPhone 4S (NJB)
  - Version7
    - Android image (102_mmcblk0_Samsung Galaxy Y Duo...
    - Android image (102_stl11_Samsung Galaxy Y Duos (G...
    - MY_DUMP_2014-12-02_19-12-46
    - MY_DUMP_2014-12-02_19-12-46
  - Unassigned devices
    - (NOKIA Lumia 920)
    - Android Zip (Android S4 Badoo 2.45.0)
    - Android Zip (SocialCam 2.6.1 (Android))
    - Android Zip (textPLUS 5.9.8 (Android))

Owner	Device	Details	Extraction	Notes
Patrick Payge				Huge web history
Jensen Ackles	Jensen Ackles (Iphone4) **Model:** Apple iPhone 4 **IMEI:** 013263009627372	**Case:** !Graph **Evidence number:** 647122	**Inspector:** <None> **Extracted by version:** 5.4.0.1560 12/11/2013 14:44:14	
<None>	Apple iPhone 4S NJB PhotoVault **Model:** Apple iPhone 4S **IMEI:** 013043005068452	**Case:** <None> **Evidence number:** <None>	**Inspector:** Tatiana **Extracted by version:** 6.3.1.222 03/07/2014 18:52:41	
Simon Payge	Simon Payge's iPhone 4S **Model:** Apple iPhone 4S **IMEI:** 013043005068452	**Case:** <None> **Evidence number:** 63/53	**Inspector:** <None> **Extracted by version:** 5.1.0.586 06/02/2013 10:51:49	Device found in a stolen car 9904 Fort Hamilton Parkway, Brooklyn NY February 6, 2013
<None>	Apple iPhone 4S BBM **Model:** Apple iPhone 4S **IMEI:** 013043005068452	**Case:** Apps_6_1 **Evidence number:** <None>	**Inspector:** Tatiana **Extracted by version:** 6.2.1.214 07/05/2014 13:48:21	
<None>	Apple iPhone 4S **Model:** Apple iPhone 4S **IMEI:** 013043005068452	**Case:** <None> **Evidence number:** <None>	**Inspector:** Tatiana **Extracted by version:** 7.0.0.295 17/12/2014 13:08:46	
<None>	Apple iPhone 4S **Model:** Apple iPhone 4S **IMEI:** 013043005068452	**Case:** Apps_6_1 **Evidence number:** <None>	**Inspector:** <None> **Extracted by version:** 6.0.1.25 21/01/2014 10:43:06	
Simon Payge	Simon Payge's iPhone 4S (NJB) **Model:** Apple iPhone 4S **IMEI:** 013043005068452	**Case:** Human trafficking **Evidence number:** 65/42	**Inspector:** <None> **Extracted by version:** 5.1.2.153 24/04/2013 11:56:32	Device found in a stolen car 9904 Fort Hamilton Parkway, Brooklyn NY February 6, 2013
Patrick Payge	Patrick Payge's iPhone 3GS **Model:** Apple iPhone 3GS **IMEI:** 012156002672455	**Case:** <None> **Evidence number:** 21/44	**Inspector:** Tatiana **Extracted by version:** 4.2.0.313 15/03/2012 10:40:33	Patrick's main phone Europe/Moscow time zone List of Wi-Fi connections Google Maps routes Try to connect Skype communication with Wi-Fi hot spots on the map.

Key Evidence section displays the data marked as important by the inspector in the following sections: Phonebook, Messages, Event Log, Calendar, Notes, etc.

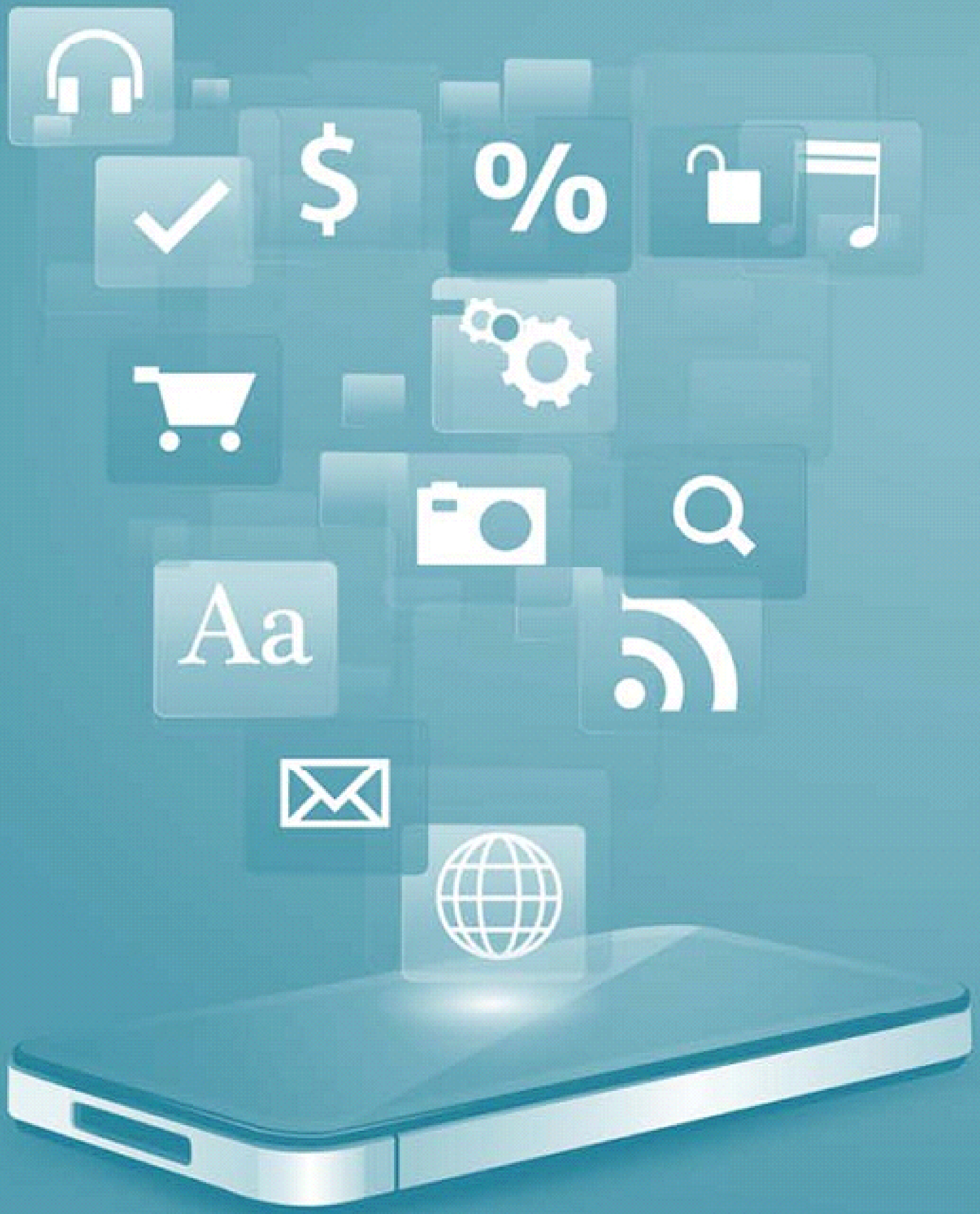
Search section allows to search for the specified entry analyzing all device information through all sections of one or several specified mobile devices.

OXYGEN SOFTWARE is certified user. Analyst version: 7.0.0.332 Expires in 32814 days Total cases: 7, Total devices: 52

http://www.oxygen-forensic.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

File System Acquisition



- Logical acquisition cannot help in extracting **deleted** data from the file and directory of mobile phone

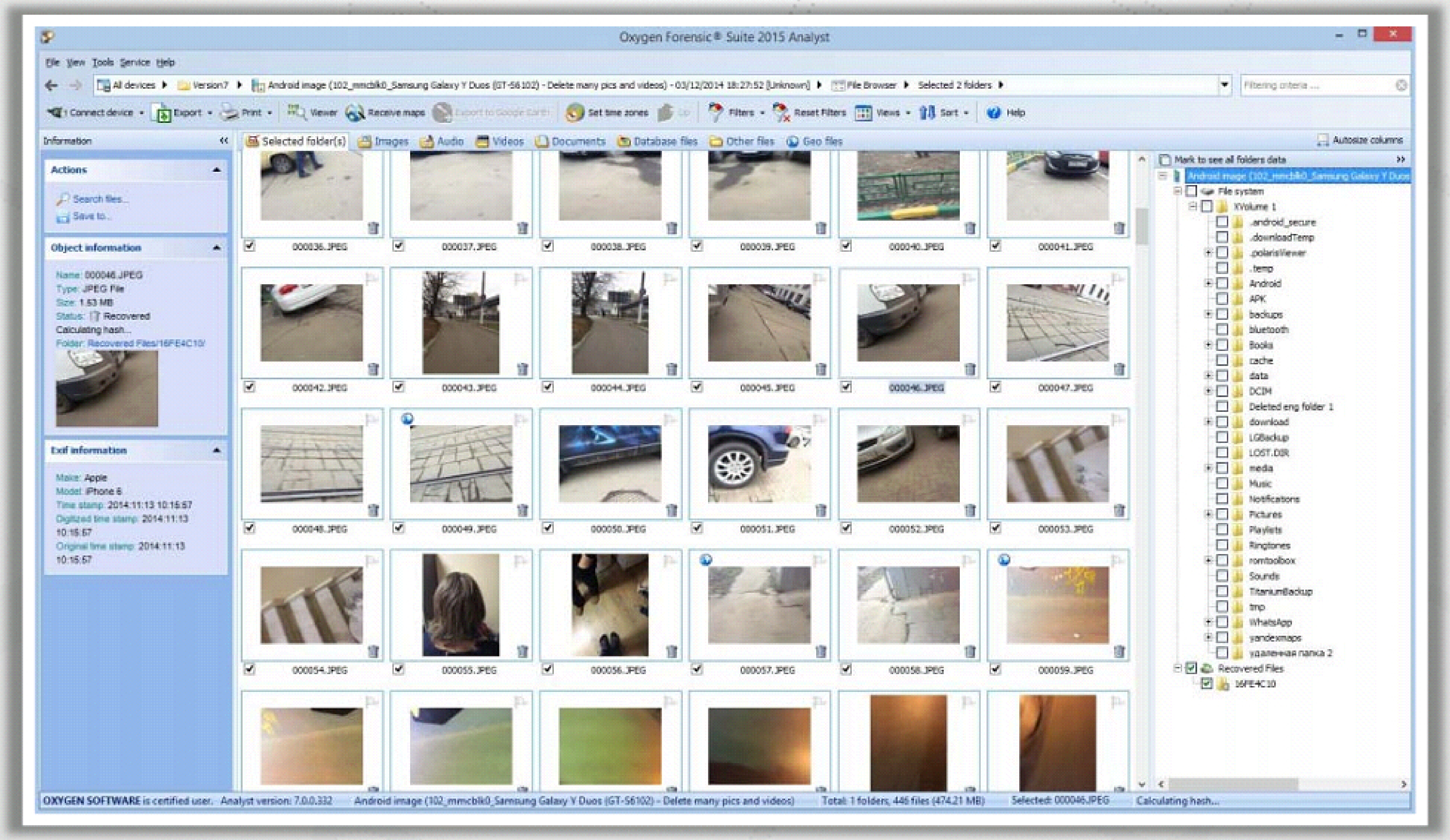
- File system acquisition helps in **recovering** and **extracting deleted data**

- Moreover, the file system acquisition shows **file structure**, **application data**, and **web artifacts** available in the mobile

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

File System Acquisition Using Oxygen Forensic Detective

- Launch **Oxygen Forensic Detective**
- Connect mobile device to the forensics workstation through USB
- Perform **file system acquisition** using **Oxygen Forensic Suite**



Oxygen Forensic® Suite 2015 Analyst

All devices ▸ Version7 ▸ Android image (102_mmcblk0_Samsung Galaxy Y Duos (GT-S6102) - Delete many pics and videos) - 03/12/2014 18:27:52 [Unknown] ▸ File Browser ▸ Selected 2 folders ▸

Object information

Name: 000046.JPEG
Type: JPEG File
Size: 1.53 MB
Status: Recovered
Calculating hash...
Folder: Recovered Files/16FE4C10/

Exif information

Make: Apple
Model: iPhone 6
Time stamp: 2014:11:13 10:15:57
Digitized time stamp: 2014:11:13 10:15:57
Original time stamp: 2014:11:13 10:15:57

OXYGEN SOFTWARE is certified user. Analyst version: 7.0.0.332 Android image (102_mmcblk0_Samsung Galaxy Y Duos (GT-S6102) - Delete many pics and videos) Total: 1 folders, 446 files (474.21 MB) Selected: 000046.JPEG Calculating hash...

https://www.oxygen-forensic.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

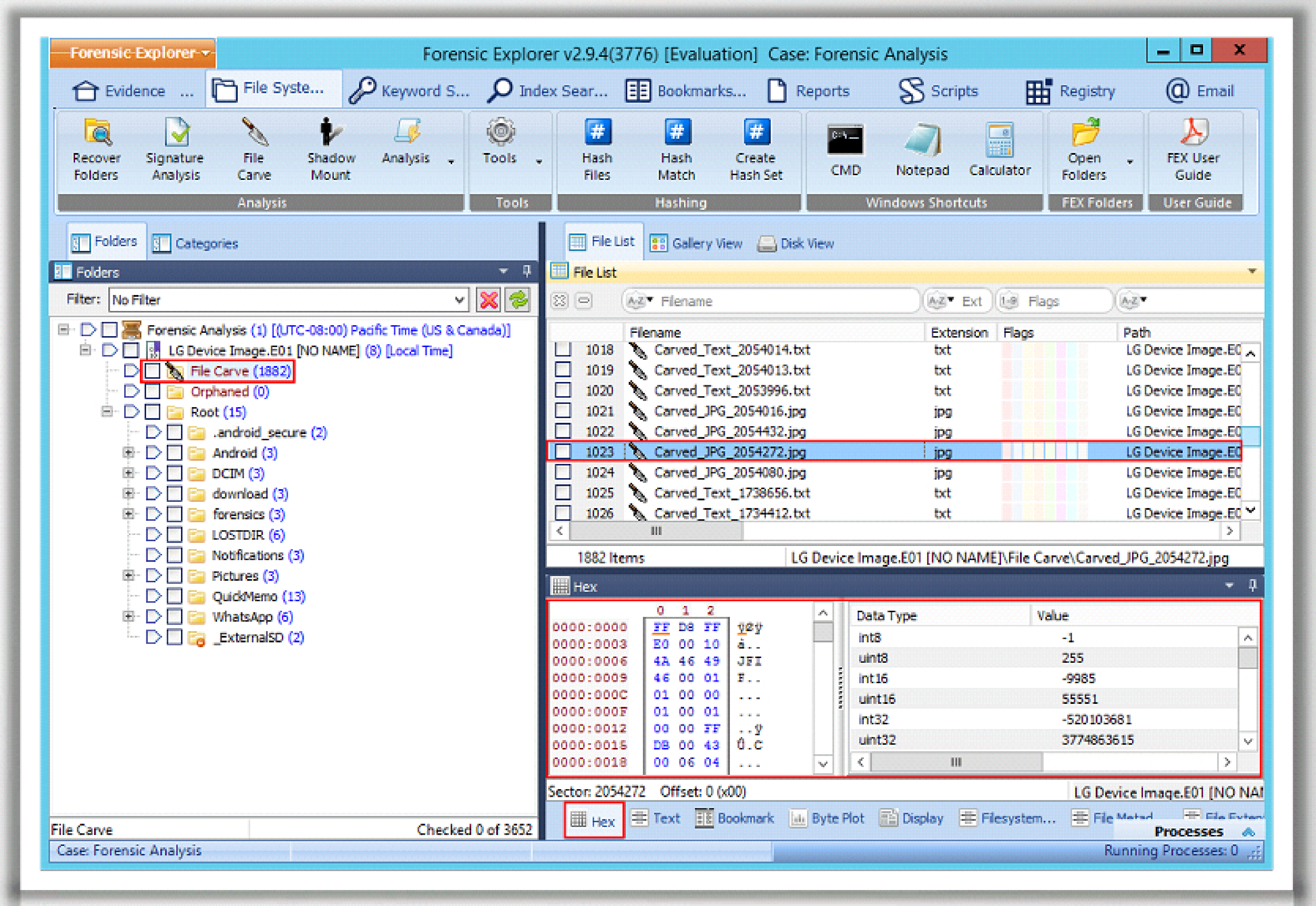
File Carving

- File carving involves recovering **deleted** or **hidden** data from mobile phones
- Persons involved in the incident may delete certain data, and wipe out **potential evidence** from the mobile phone
- You should try to recover such deleted data for **forensic analysis**
- Use **file carving tools** to recover:
  - Keyboard caches
  - Deleted photos
  - Browser cache items and other personal data
  - Call history data
  - Map tiles from maps application
  - Cached, and deleted email messages
  - SMS messages with timestamp data
  - Deleted voicemails

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

File Carving Using Forensic Explorer

- Forensic Explorer **recovers** and **analyzes** hidden system files, deleted files, slack space, and unallocated clusters
- **Data carving** types supported:
  - Cluster based file carving
  - Sector based file carving
  - Byte based file carving



Forensic Explorer v2.9.4(3776) [Evaluation] Case: Forensic Analysis

Folders

Filter: No Filter

```
Forensic Analysis (1) [(UTC-08:00) Pacific Time (US & Canada)]
  LG Device Image.E01 [NO NAME] (8) [Local Time]
    File Carve (1882)
    Orphaned (0)
    Root (15)
      .android_secure (2)
      Android (3)
      DCIM (3)
      download (3)
      forensics (3)
      LOSTDIR (6)
      Notifications (3)
      Pictures (3)
      QuickMemo (13)
      WhatsApp (6)
      _ExternalSD (2)
```

File Carve — Checked 0 of 3652

File List

	Filename	Extension	Flags	Path
1018	Carved_Text_2054014.txt	txt		LG Device Image.E0
1019	Carved_Text_2054013.txt	txt		LG Device Image.E0
1020	Carved_Text_2053996.txt	txt		LG Device Image.E0
1021	Carved_JPG_2054016.jpg	jpg		LG Device Image.E0
1022	Carved_JPG_2054432.jpg	jpg		LG Device Image.E0
1023	Carved_JPG_2054272.jpg	jpg		LG Device Image.E0
1024	Carved_JPG_2054080.jpg	jpg		LG Device Image.E0
1025	Carved_Text_1738656.txt	txt		LG Device Image.E0
1026	Carved_Text_1734412.txt	txt		LG Device Image.E0

1882 Items — LG Device Image.E01 [NO NAME]\File Carve\Carved_JPG_2054272.jpg

Hex

```
             0  1  2
0000:0000   FF D8 FF   ÿØÿ
0000:0003   E0 00 10   à..
0000:0006   4A 46 49   JFI
0000:0009   46 00 01   F..
0000:000C   01 00 00   ...
0000:000F   01 00 01   ...
0000:0012   00 00 FF   ..ÿ
0000:0015   DB 00 43   Û.C
0000:0018   00 06 04   ...
```

Data Type	Value
int8	-1
uint8	255
int16	-9985
uint16	55551
int32	-520103681
uint32	3774863615

Sector: 2054272 Offset: 0 (x00) LG Device Image.E01 [NO NAI

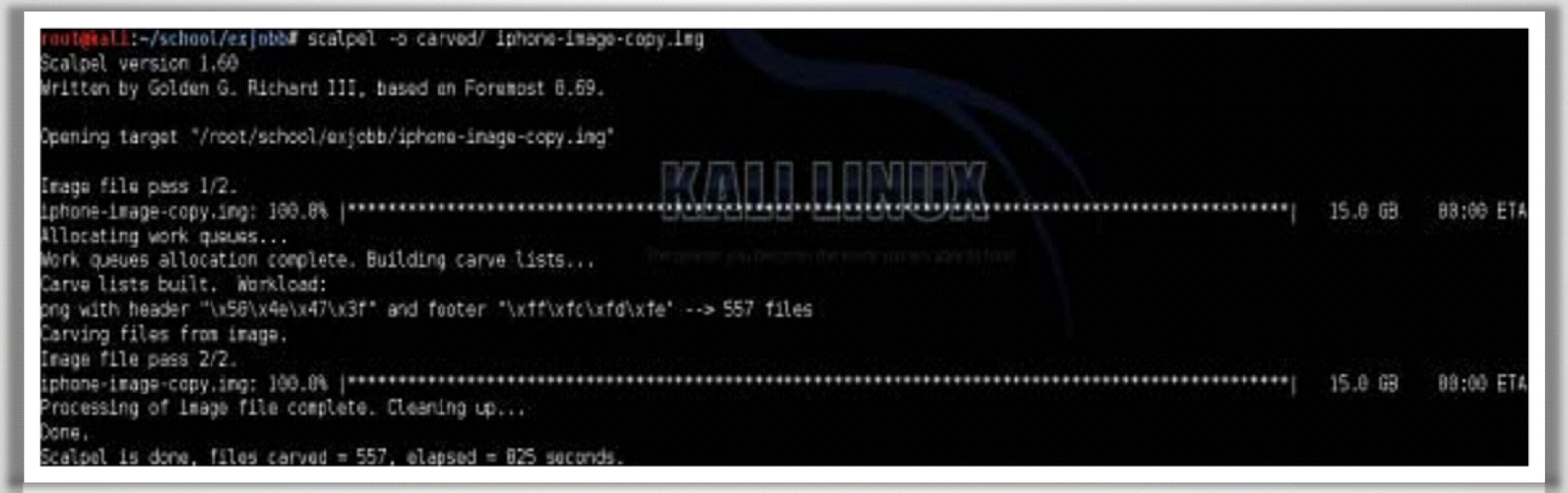
Case: Forensic Analysis Running Processes: 0

http://www.forensicexplorer.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

iPhone File Carving Using Scalpel Tool

Scalpel is a **file carving**, and **indexing application** that runs on Linux and Windows



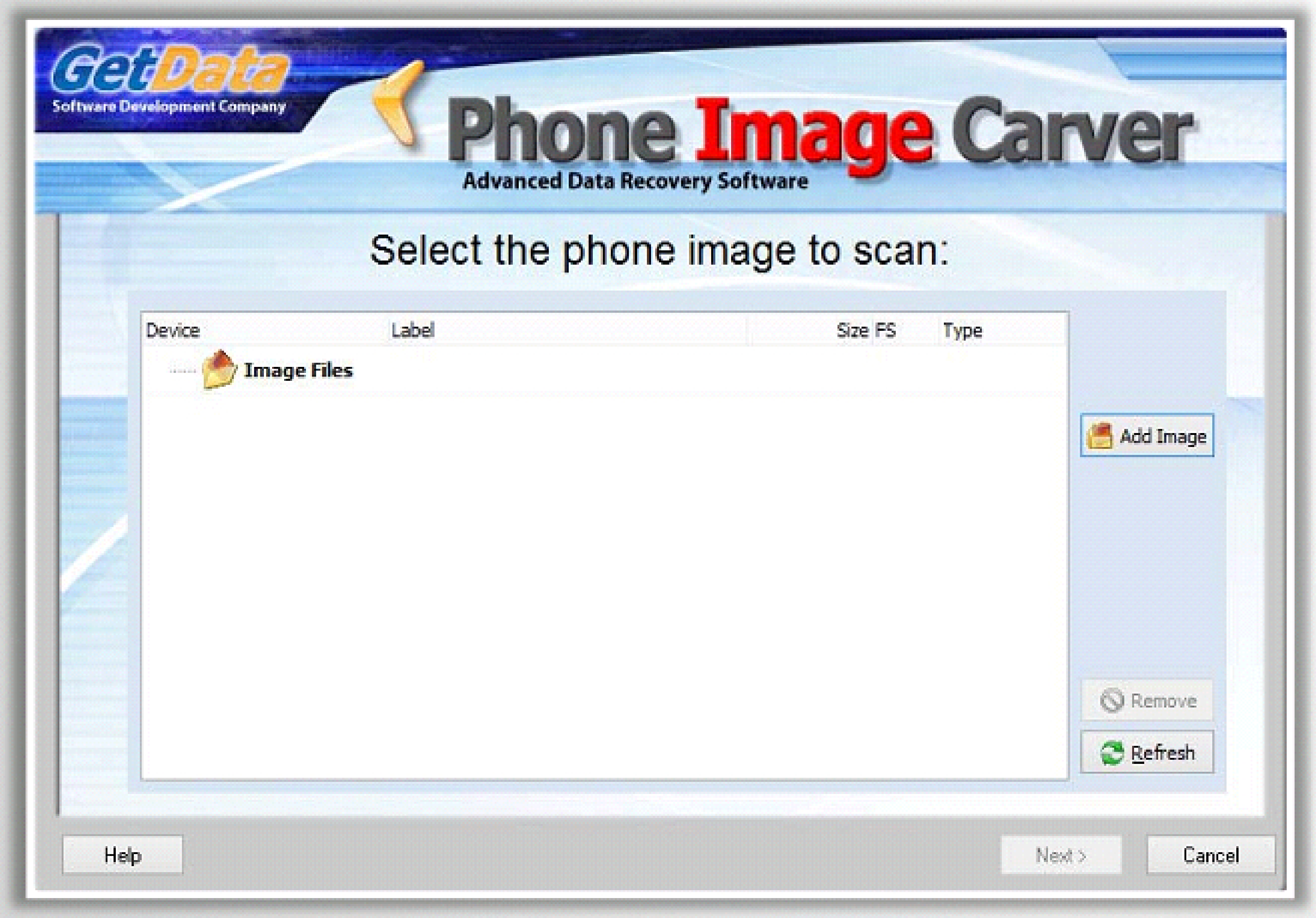
```
root@kali:~/school/exjobb# scalpel -o carved/ iphone-image-copy.img
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/root/school/exjobb/iphone-image-copy.img"

Image file pass 1/2.
iphone-image-copy.img: 100.0% |********************************************************************************|  15.0 GB   00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built.  Workload:
png with header "\x50\x4e\x47\x3f" and footer "\xff\xfc\xfd\xfe" --> 557 files
Carving files from image.
Image file pass 2/2.
iphone-image-copy.img: 100.0% |********************************************************************************|  15.0 GB   00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 557, elapsed = 825 seconds.
```

https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

File Carving Tools

Phone Image Carver



GetData Software Development Company

Phone Image Carver

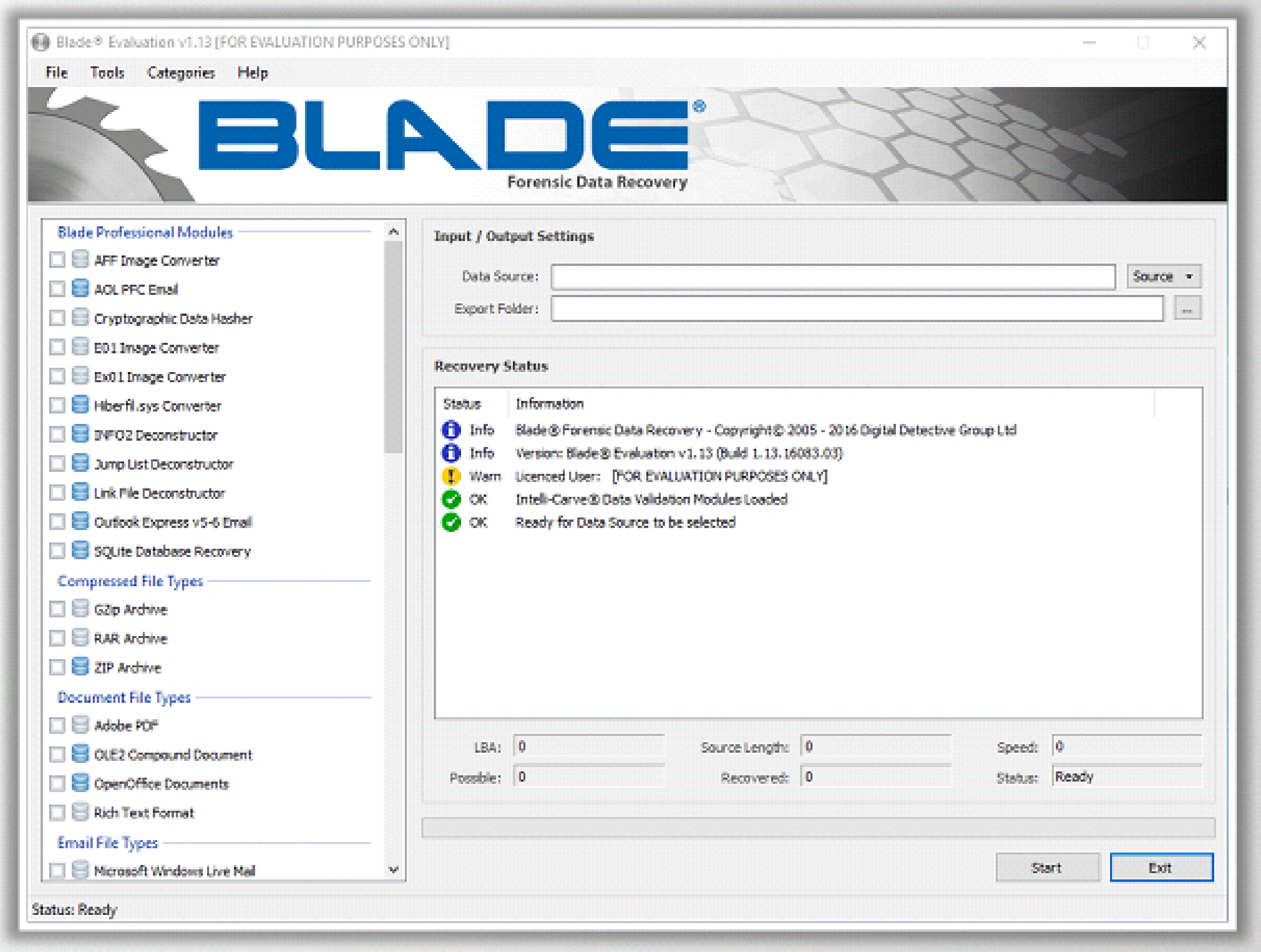
Advanced Data Recovery Software

Select the phone image to scan:

Device	Label	Size	FS	Type
Image Files				

http://www.phoneimagecarver.com

Blade® Professional v1



Blade® Evaluation v1.13 [FOR EVALUATION PURPOSES ONLY]

Blade Professional Modules

- ☐ AFF Image Converter
- ☐ AOL PFC Email
- ☐ Cryptographic Data Hasher
- ☐ E01 Image Converter
- ☐ Ex01 Image Converter
- ☐ Hiberfil.sys Converter
- ☐ INFO2 Deconstructor
- ☐ Jump List Deconstructor
- ☐ Link File Deconstructor
- ☐ Outlook Express v5-6 Email
- ☐ SQLite Database Recovery

Compressed File Types

- ☐ GZip Archive
- ☐ RAR Archive
- ☐ ZIP Archive

Document File Types

- ☐ Adobe PDF
- ☐ OLE2 Compound Document
- ☐ OpenOffice Documents
- ☐ Rich Text Format

Email File Types

- ☐ Microsoft Windows Live Mail

Input / Output Settings

Data Source:

Export Folder:

Recovery Status

```
Status  Information
Info    Blade® Forensic Data Recovery - Copyright© 2005 - 2016 Digital Detective Group Ltd
Info    Version: Blade® Evaluation v1.13 (Build 1.13.16083.03)
Warn    Licenced User:   [FOR EVALUATION PURPOSES ONLY]
OK      Intelli-Carve® Data Validation Modules Loaded
OK      Ready for Data Source to be selected
```

LBA: 0 Source Length: 0 Speed: 0

Possible: 0 Recovered: 0 Status: Ready

Status: Ready

http://www.digital-detective.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SQLite Database Extraction

- Mobile phones use SQLite database files to store information such as address book contacts, SMS messages, email messages, and other sensitive information

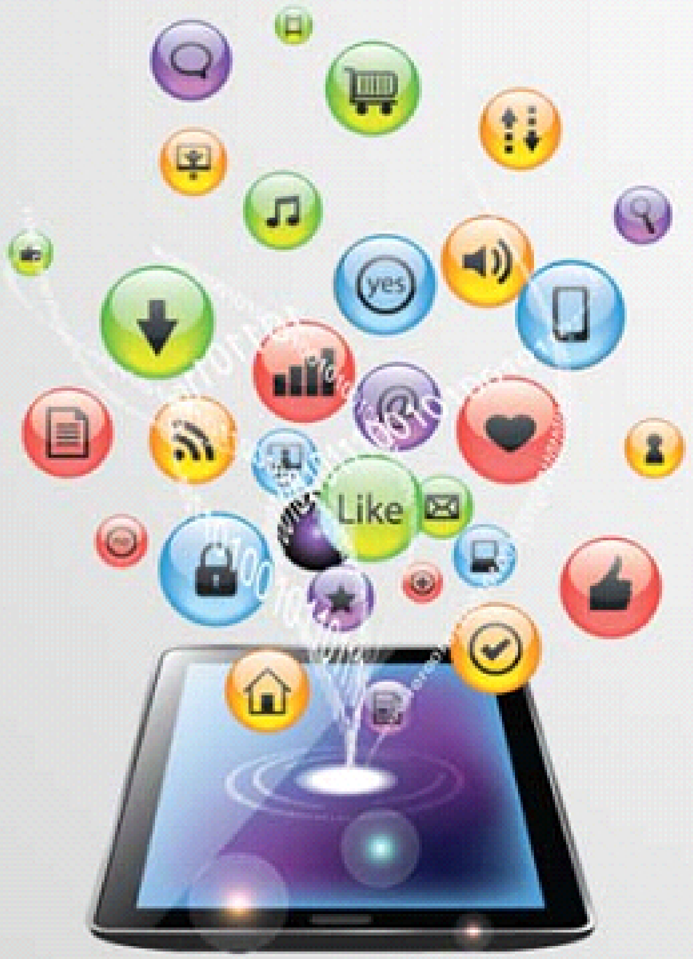
- These SQLite database files need to be extracted and analyzed forensically in order to find potential evidence

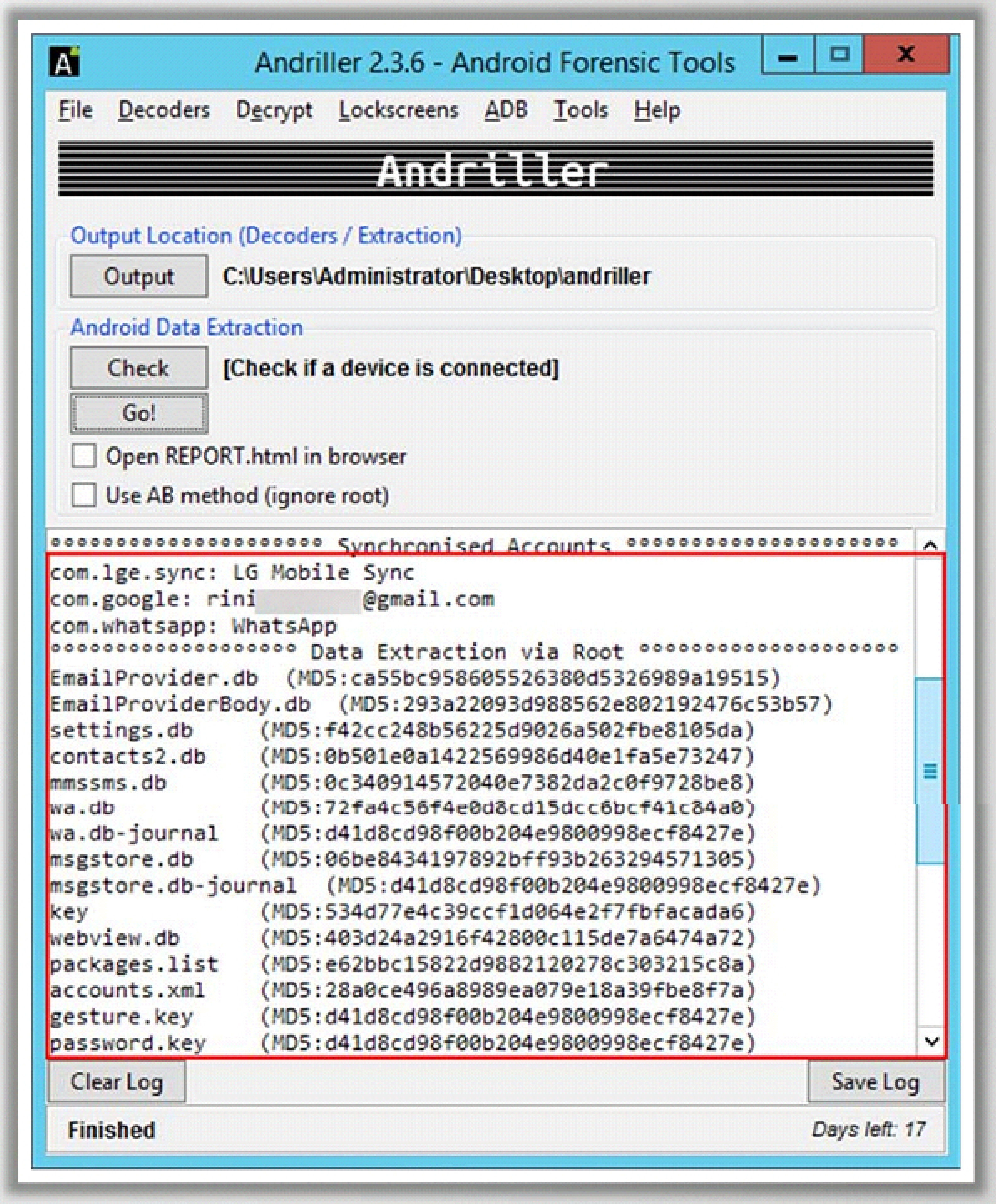
- Extract SQLite database files with SQLite browsing tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Forensic Analysis of SQLite Database Using Andriller

- Connect the device to **forensics workstation**
- Explore and analyze the **SQLite files** from mobile phone with Andriller





Output Location (Decoders / Extraction)

Output: C:\Users\Administrator\Desktop\andriller

Android Data Extraction

[Check if a device is connected]

□ Open REPORT.html in browser

□ Use AB method (ignore root)

```
oooooooooooooooooooooo Synchronised Accounts oooooooooooooooooooooo
com.lge.sync: LG Mobile Sync
com.google: rini[redacted]@gmail.com
com.whatsapp: WhatsApp
ooooooooooooooooooo Data Extraction via Root ooooooooooooooooooooo
EmailProvider.db  (MD5:ca55bc958605526380d5326989a19515)
EmailProviderBody.db  (MD5:293a22093d988562e802192476c53b57)
settings.db     (MD5:f42cc248b56225d9026a502fbe8105da)
contacts2.db    (MD5:0b501e0a1422569986d40e1fa5e73247)
mmssms.db       (MD5:0c340914572040e7382da2c0f9728be8)
wa.db           (MD5:72fa4c56f4e0d8cd15dcc6bcf41c84a0)
wa.db-journal   (MD5:d41d8cd98f00b204e9800998ecf8427e)
msgstore.db     (MD5:06be8434197892bff93b263294571305)
msgstore.db-journal  (MD5:d41d8cd98f00b204e9800998ecf8427e)
key             (MD5:534d77e4c39ccf1d064e2f7fbfacada6)
webview.db      (MD5:403d24a2916f42800c115de7a6474a72)
packages.list   (MD5:e62bbc15822d9882120278c303215c8a)
accounts.xml    (MD5:28a0ce496a8989ea079e18a39fbe8f7a)
gesture.key     (MD5:d41d8cd98f00b204e9800998ecf8427e)
password.key    (MD5:d41d8cd98f00b204e9800998ecf8427e)
```

Finished

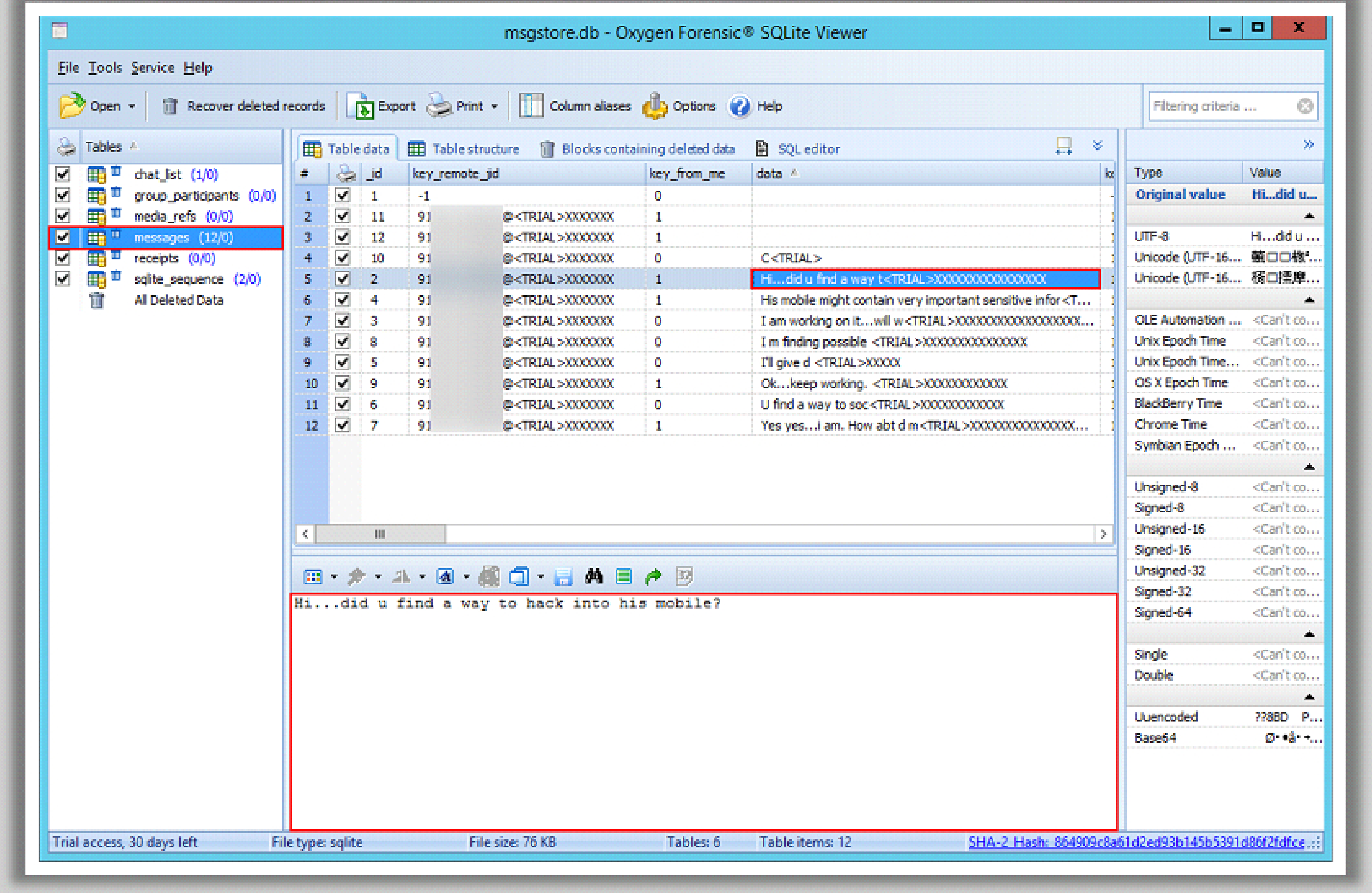
Days left: 17

https://andriller.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SQLite Database Browsing Tools: Oxygen Forensics SQLite Viewer

SQLite Viewer allows forensic investigators to **explore the database files** with the following extensions: **.sqlite**, **.sqlite3**, **.sqlitedb**, **.db**, and **.db3**



☑ chat_list (1/0)
☑ group_participants (0/0)
☑ media_refs (0/0)
☑ messages (12/0)
☑ receipts (0/0)
☑ sqlite_sequence (2/0)
All Deleted Data

#		_id	key_remote_jid	key_from_me	data
1	☑	1	-1	0	
2	☑	11	91[redacted]@<TRIAL >XXXXXXX	1	
3	☑	12	91[redacted]@<TRIAL >XXXXXXX	1	
4	☑	10	91[redacted]@<TRIAL >XXXXXXX	0	C<TRIAL >
5	☑	2	91[redacted]@<TRIAL >XXXXXXX	1	Hi...did u find a way t<TRIAL >XXXXXXXXXXXXXXXX
6	☑	4	91[redacted]@<TRIAL >XXXXXXX	1	His mobile might contain very important sensitive infor<T...
7	☑	3	91[redacted]@<TRIAL >XXXXXXX	0	I am working on it...will w<TRIAL >XXXXXXXXXXXXXXXXX...
8	☑	8	91[redacted]@<TRIAL >XXXXXXX	0	I m finding possible <TRIAL >XXXXXXXXXXXXXXX
9	☑	5	91[redacted]@<TRIAL >XXXXXXX	0	I'll give d <TRIAL >XXXXX
10	☑	9	91[redacted]@<TRIAL >XXXXXXX	1	Ok...keep working. <TRIAL >XXXXXXXXXXXX
11	☑	6	91[redacted]@<TRIAL >XXXXXXX	0	U find a way to soc<TRIAL >XXXXXXXXXXXX
12	☑	7	91[redacted]@<TRIAL >XXXXXXX	1	Yes yes...i am. How abt d m<TRIAL >XXXXXXXXXXXXXXX...

```
Hi...did u find a way to hack into his mobile?
```

Type	Value
Original value	**Hi...did u...**
UTF-8	Hi...did u ...
Unicode (UTF-16...	螄口口檄...
Unicode (UTF-16...	稲口揺崋...
OLE Automation ...	<Can't co...
Unix Epoch Time	<Can't co...
Unix Epoch Time...	<Can't co...
OS X Epoch Time	<Can't co...
BlackBerry Time	<Can't co...
Chrome Time	<Can't co...
Symbian Epoch ...	<Can't co...
Unsigned-8	<Can't co...
Signed-8	<Can't co...
Unsigned-16	<Can't co...
Signed-16	<Can't co...
Unsigned-32	<Can't co...
Signed-32	<Can't co...
Signed-64	<Can't co...
Single	<Can't co...
Double	<Can't co...
Uuencoded	??8BD P...
Base64	Ø••å•+...

Trial access, 30 days left | File type: sqlite | File size: 76 KB | Tables: 6 | Table items: 12 | SHA-2 Hash: 864909c8a61d2ed93b145b5391d86f2fdfce...

http://www.oxygen-forensic.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SQLite Database Browsing Tools

DB Browser for SQLite

(http://sqlitebrowser.org)

X-plore

(http://www.lonelycatgames.com/?app=xplore)

SQLitePlus Explorer

(http://www.eztools-software.com/Tools/sqliteplus/default.asp)

SQLite Viewer

(http://www.totalcmd.net/plugring/sqliteviewer.html)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android Forensic Analysis

- After logical, physical, and file system acquisition, forensic **examination** and **analysis** is carried out on the extracted data
- It involves finding out source of **evidence** from information obtained by extraction

The forensics examiner should investigate:

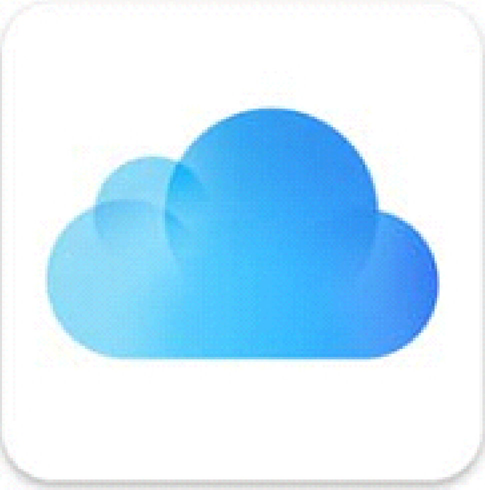
- Mobile phone data artifacts such as **contacts**, call history, browser, **SMS/MMS**, and geolocation
- Raw data artifacts
- **Timeline** of activities

https://www.oxygen-forensic.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

iPhone Data Extraction

- Investigators can adopt three ways to extract iPhone data in order to analyze it forensically
  - Create a **physical memory image** of the iPhone data using forensics tools such as **Cellebrite**, XRY, Lantern, Elcomsoft, MPE, Zdziarski, etc.
  - Create **file System dump** using forensics tools such as Cellebrite, Blacklight, Oxygen or XRY
  - Creates **iPhone backup** using iCloud or iTunes



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

iPhone Data Acquisition Tools

UFED Touch2
http://www.cellebrite.com

Mobilyze
http://www.blackbagtech.com

SecureView
http://mobileforensics.susteen.com

NowSecure Forensics
https://www.nowsecure.com/forensics

MOBILedit
http://www.mobiledit.com

Lantern
http://katanaforensics.com

Aceso
http://www.radio-tactics.com

Athena
http://www.radio-tactics.com

Elcomsoft iOS Forensic Toolkit
https://www.elcomsoft.com/eift.html

iXAM
http://www.ixam-forensics.com

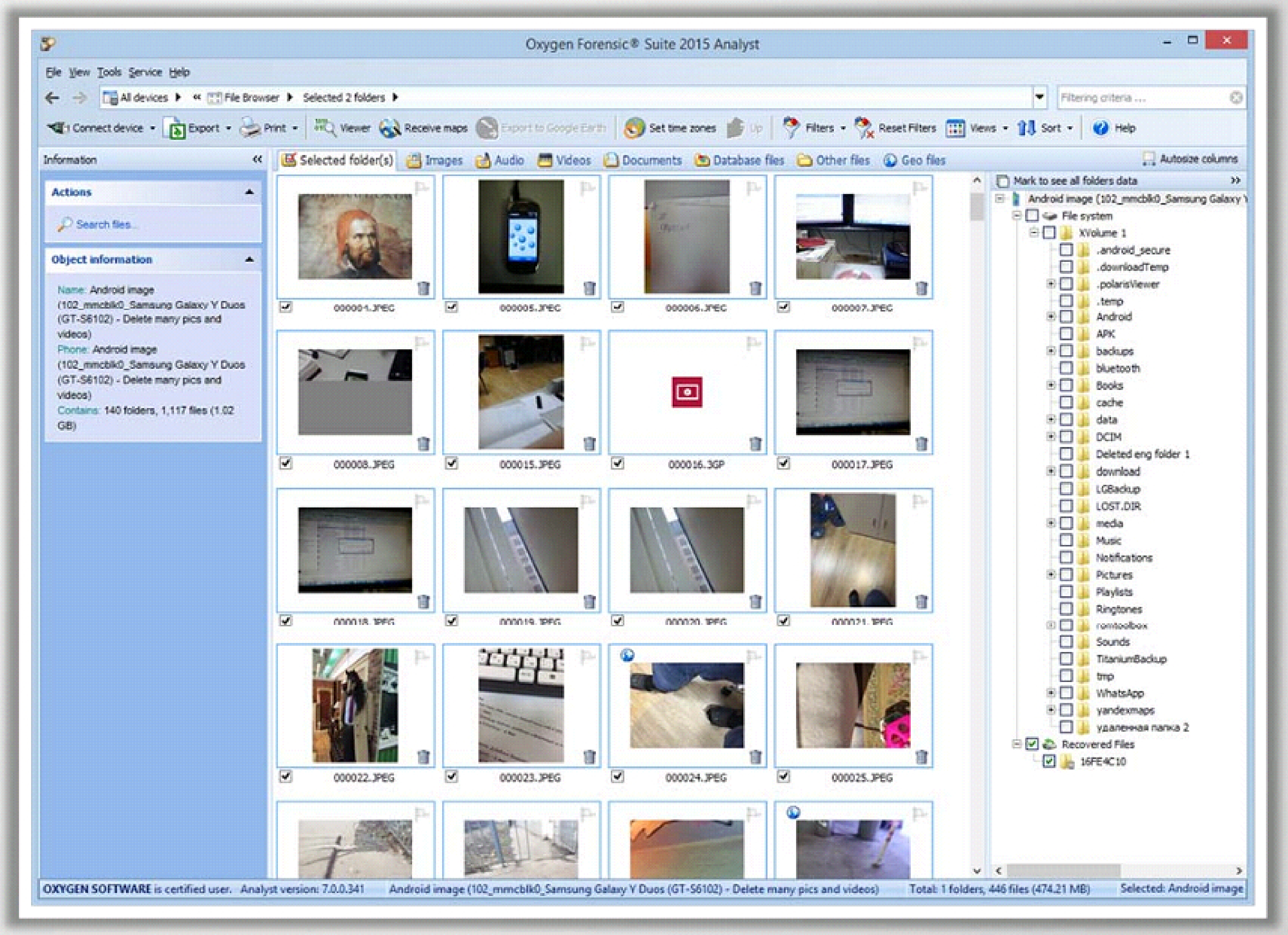
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

iPhone Forensic Analysis Using the Oxygen Forensics Detective

- Perform iPhone forensic analysis using the Oxygen Forensics site
- It can extract device information, contacts, calendar events, **SMS messages**, event logs, and files

OXYGEN FORENSICS

Helping good people to make this world safer



Oxygen Forensic® Suite 2015 Analyst

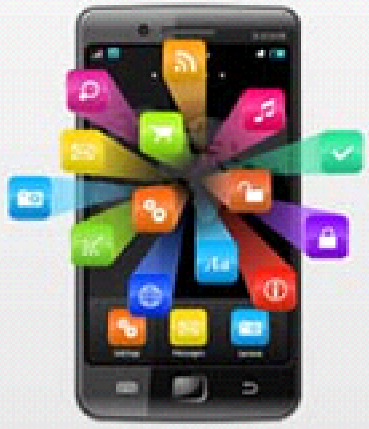
Name: Android image (102_mmcblk0_Samsung Galaxy Y Duos (GT-S6102) - Delete many pics and videos)
Phone: Android image (102_mmcblk0_Samsung Galaxy Y Duos (GT-S6102) - Delete many pics and videos)
Contains: 140 folders, 1,117 files (1.02 GB)

OXYGEN SOFTWARE is certified user. Analyst version: 7.0.0.341 Android image (102_mmcblk0_Samsung Galaxy Y Duos (GT-S6102) - Delete many pics and videos) Total: 1 folders, 446 files (474.21 MB) Selected: Android image

http://www.oxygen-forensic.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Examination and Analysis



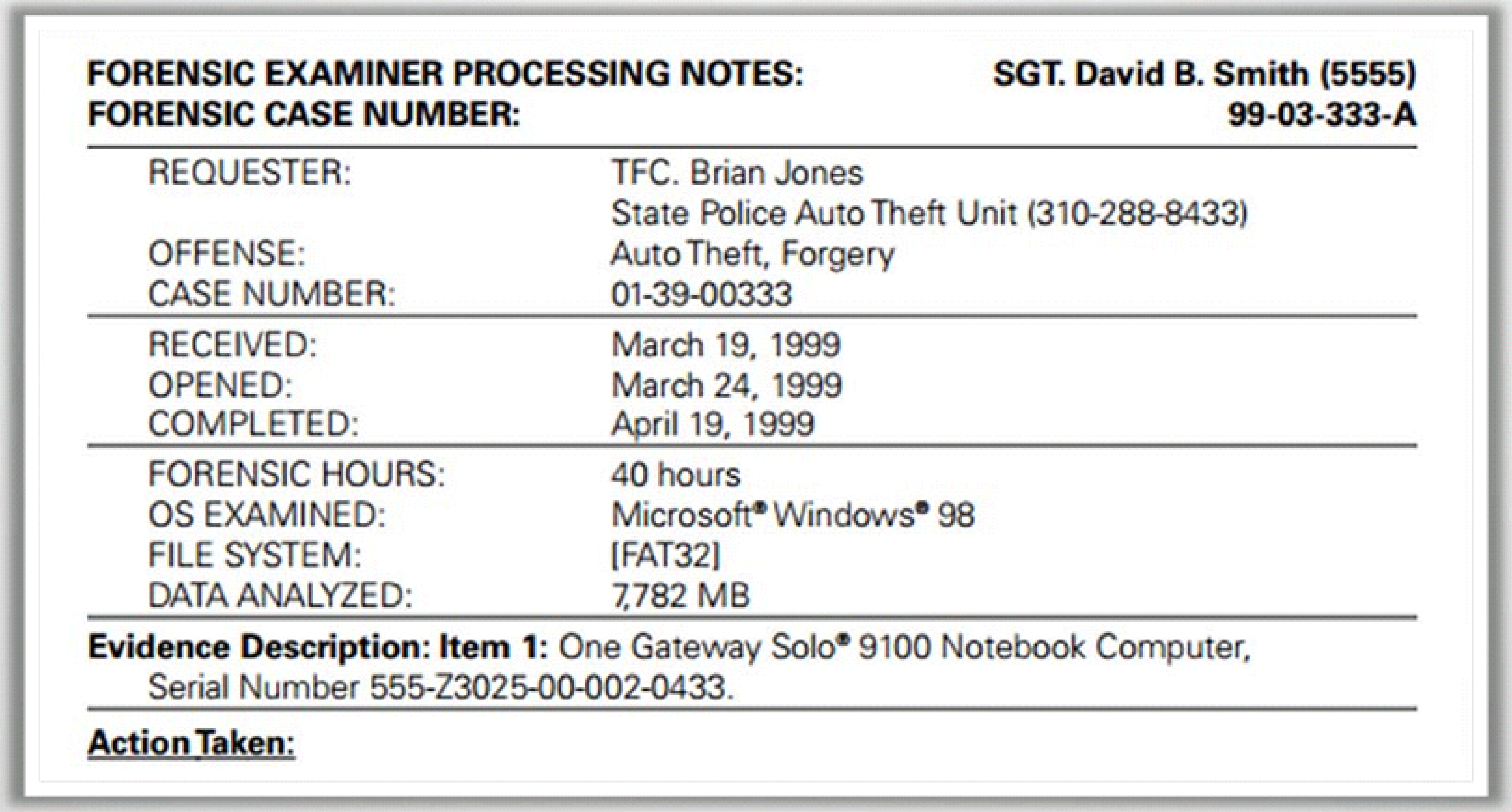
During forensic analysis, the investigator should try to find **all the information** that may help in solving the case

Forensic examination and analysis helps in **revealing potential evidence** and uncovering useful information related to the crime

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Generating Investigation Report

- The results obtained in all the steps of forensics process needs to be presented in a **prescribed standard format**
- A forensics report should include the complete forensics investigation process followed along with supporting documents such as **photographs**, notes, and **signatures** of specialists
- A forensics tool is used to prepare reports to present the forensics result in a prescribed format



FORENSIC EXAMINER PROCESSING NOTES: **SGT. David B. Smith (5555)**
FORENSIC CASE NUMBER: **99-03-333-A**

REQUESTER:	TFC. Brian Jones State Police Auto Theft Unit (310-288-8433)
OFFENSE:	Auto Theft, Forgery
CASE NUMBER:	01-39-00333
RECEIVED:	March 19, 1999
OPENED:	March 24, 1999
COMPLETED:	April 19, 1999
FORENSIC HOURS:	40 hours
OS EXAMINED:	Microsoft® Windows® 98
FILE SYSTEM:	[FAT32]
DATA ANALYZED:	7,782 MB

Evidence Description: Item 1: One Gateway Solo® 9100 Notebook Computer, Serial Number 555-Z3025-00-002-0433.

Action Taken:

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Forensics Report Template

The mobile forensics report should contain:

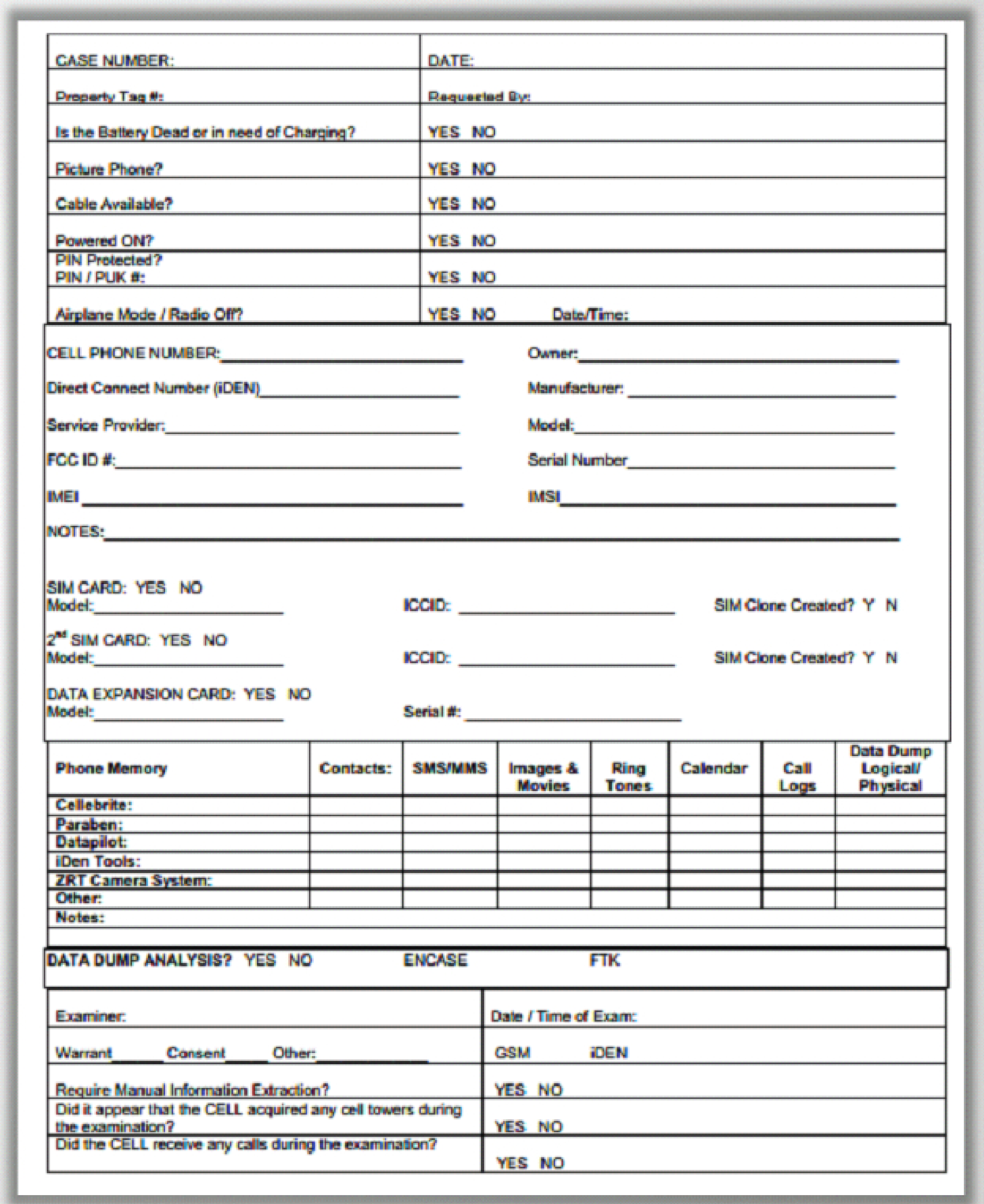
- Summary
- Objectives
- Date and time the incident allegedly occurred
- Date and time the incident was reported to agency personnel
- Name of the person or persons reporting the incident
- Examination start date and time
- The physical condition of the phone
- Photos of the phone and individual components
- Phone status when received turned on or off
- Make and Model

- Mobile Subscriber International ISDN Number (MSISDN)
- Integrated Circuit Card ID (ICCID)
- Service Provider Name (SPN)
- Abbreviated dialing numbers
- Last Numbers received
- Last Numbers dialed
- Missed calls
- Short Message Services (SMS)
- Calendar entries
- Photographs stored in the handset
- Video stored in the handset
- Smart Media/ Compact Flash

- MMS
- International Mobile Subscriber Identity (IMSI)
- Mobile Country Code (MCC)
- Mobile Network Code (MNC)
- Mobile Subscriber Identification Number (MSIN)
- Preservation of the evidence
- Investigative techniques
- Tools used for the acquisition
- Tools used for the examination
- Data found during the examination
- Notes from peer review
- Supporting expert opinion

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sample Mobile Forensic Analysis Worksheet



CASE NUMBER:	DATE:
Property Tag #:	Requested By:
Is the Battery Dead or in need of Charging?	YES NO
Picture Phone?	YES NO
Cable Available?	YES NO
Powered ON?	YES NO
PIN Protected? PIN / PUK #:	YES NO
Airplane Mode / Radio Off?	YES NO Date/Time:

CELL PHONE NUMBER:______________________ Owner:______________________

Direct Connect Number (iDEN)______________________ Manufacturer: ______________________

Service Provider:______________________ Model:______________________

FCC ID #:______________________ Serial Number______________________

IMEI ______________________ IMSI______________________

NOTES:____

SIM CARD: YES NO
Model:__________________ ICCID: __________________ SIM Clone Created? Y N

2nd SIM CARD: YES NO
Model:__________________ ICCID: __________________ SIM Clone Created? Y N

DATA EXPANSION CARD: YES NO
Model:__________________ Serial #: __________________

Phone Memory	Contacts:	SMS/MMS	Images & Movies	Ring Tones	Calendar	Call Logs	Data Dump Logical/ Physical
Cellebrite:							
Paraben:							
Datapilot:							
iDen Tools:							
ZRT Camera System:							
Other:							
Notes:							

DATA DUMP ANALYSIS? YES NO ENCASE FTK

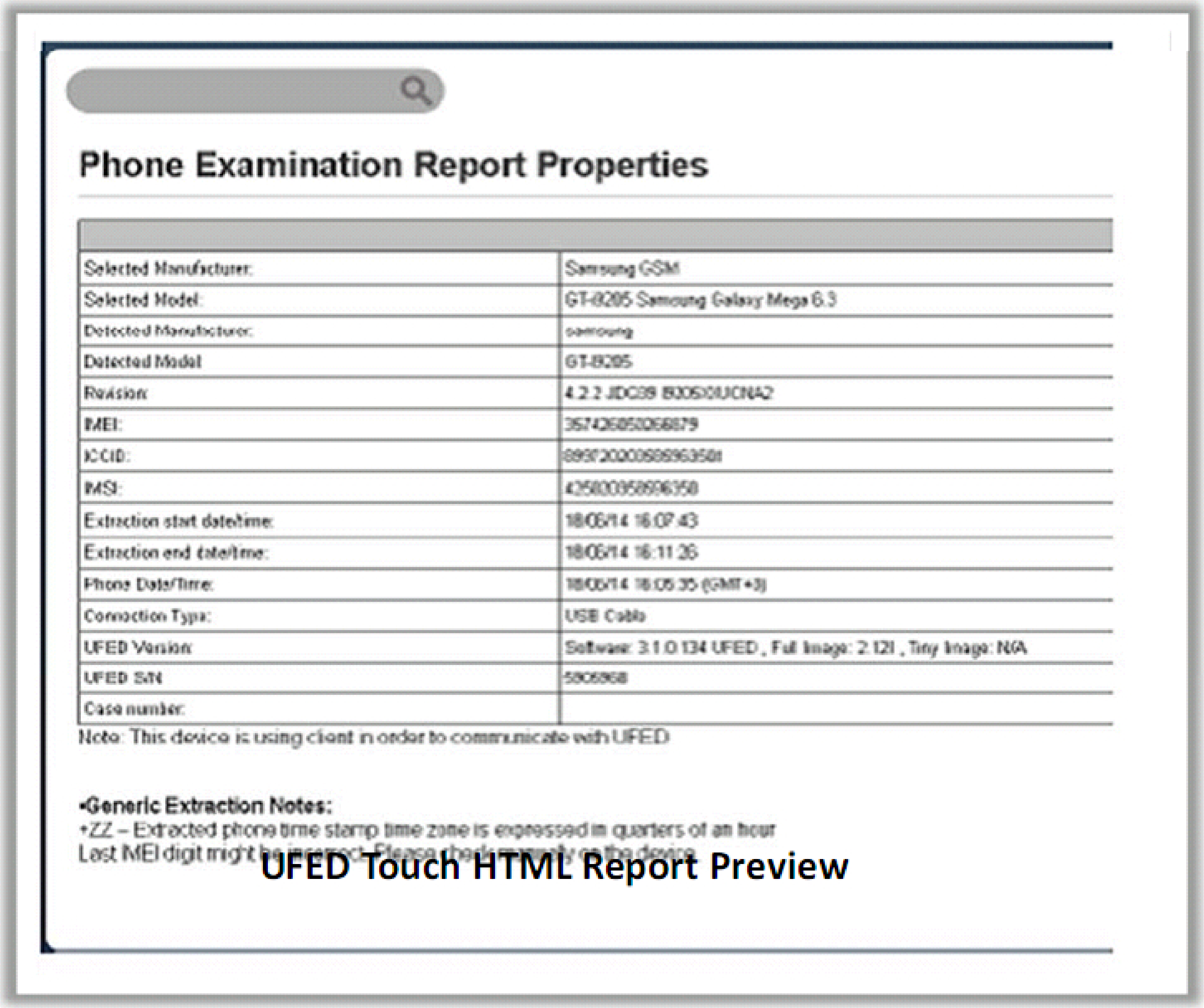
Examiner:	Date / Time of Exam:
Warrant_____ Consent_____ Other:__________	GSM iDEN
Require Manual Information Extraction?	YES NO
Did it appear that the CELL acquired any cell towers during the examination?	YES NO
Did the CELL receive any calls during the examination?	YES NO

http://ccf.cs.uml.edu

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cellebrite UFED Touch Sample Mobile Forensics Report Snapshot

- UFED Touch is a mobile forensics solution enabling investigators to **extract, decode, and analyze evidentiary data** in a forensically sound manner from a wide range of mobile devices



Phone Examination Report Properties

Selected Manufacturer:	Samsung GSM
Selected Model:	GT-I9205 Samsung Galaxy Mega 6.3
Detected Manufacturer:	samsung
Detected Model:	GT-I9205
Revision:	4.2.2 JDQ39 I9205XXUCNA2
IMEI:	357426050266879
ICCID:	8997202003689963501
IMSI:	425020358896358
Extraction start date/time:	18/05/14 16:07:43
Extraction end date/time:	18/05/14 16:11:26
Phone Date/Time:	18/05/14 16:05:35 (GMT+3)
Connection Type:	USB Cable
UFED Version:	Software: 3.1.0.134 UFED , Full Image: 2.121 , Tiny Image: N/A
UFED S/N:	5806868
Case number:	

Note: This device is using client in order to communicate with UFED

•Generic Extraction Notes:

+ZZ – Extracted phone time stamp time zone is expressed in quarters of an hour
Last IMEI digit might be incorrect. Please check manually on the device.

UFED Touch HTML Report Preview

http://www.cellebrite.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions
- Diversity in the mobile OS architecture may impact forensic analysis process
- Knowledge of mobile OS booting process helps investigators to gain lower level access
- Mobile storage and evidence locations include: internal memory, SIM card, and external memory
- Identifying cell phone brand, model, OS, and network service provider assists in choosing an appropriate forensics tool for data acquisition
- Rooting/Jailbreaking provides privileged control (known as "root access") within device's subsystem, enabling data acquisition
- Standard tools such as Cellebrite UFED Touch can be used to prepare mobile forensics report

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.