Mobile Forensics

Module 20

Designed by Cyber Crime Investigators. Presented by Professionals.

C|HFI™
Computer Hacking Forensic Investigator

Smartphones: Scammers New Playgrounds

FOX BUSINESS
THE POWER TO PROSPER

May 17, 2011

From **malware** to fake Web sites, the increasing popularity of smartphones is making them more vulnerable to scammers. While the threat is not as prevalent as scams targeted at PCs, there are a **rising number of attacks hitting iPhone and Android-based phones**.

"The main threat is getting malware on your phone," says Andrew Hoog, chief investigative officer at ViaForesnics, a mobile and computer forensics company. "There's more **malware popping** up in this particular space."

Other attacks surfacing on mobile phones include text messages designed to charge users for premium services, fake websites created to capture sensitive data and **hacking phones** that are using unsecure websites, according to Hoog.

Despite people using their smart phones as mini computers, there is little concern over scams, creating the perfect breeding ground for attacks.

http://www.foxbusiness.com

April 25, 2011

South Korea, Europe Start iPhone Location Tracking Investigations

South Korea's Korea Communications Commission is now asking Apple questions about the location data being stored on **iPhones** and **iPads** and backed up to users' computers. South Korea joins the governments of France, Germany, and Italy, which late last week notified Apple that they *also* had questions about location data collection. These investigations follow stern letters from US Sentaor Al Franken (D-MN) and US Representative Ed Markey (D-MA), both of whom asked Apple to answer why the data is retained on users' devices, how it is collected, and what Apple does to protect users' privacy.

iOS security experts noted that the location log wasn't new—previous versions of iOS stored the same information in a different database. Nor was **consolidated.db** necessarily a secret—forensic teams often **accessed and analyzed this file in addition to SMS logs, e-mails, contact databases, photos, and more during investigations.** Further analysis by developers and security experts suggests that the data points recorded are more likely cell tower and WiFi base station locations, and not necessarily actual device locations.

http://arstechnica.com

ElcomSoft to Sell iPhone Decryption Toolkit

May 25, 2011 8:02 AM PDT

A Russian computer forensics company, ElcomSoft, says it has developed a toolkit that can help law enforcement agencies quickly access encrypted file systems on Apple's iPhone.

ElcomSoft's toolkit is an important development as smartphone security and privacy have become a hot-button issue.

Last month, researchers discovered that the iPhone was tracking users' locations as they moved from place to place. The information was stored in an unencrypted file on the iPhone, as well as in iTunes backups. After privacy advocates complained that the iPhone was tracking user movements, Apple responded saying that it had no desire to track users, and the issue was simply a bug.

"Apple is not tracking the location of your iPhone," the company wrote on an FAQ page last month. "Apple has never done so and has no plans to ever do so." Earlier this month, Apple released iOS 4.3.3 to remove the location-tracking feature.

Other smartphones, including those running the Windows Phone 7 and Android operating systems, also track a certain amount of location data. Apple's fix could be a setback to law enforcement agencies, which for months have been using iPhone and iPad geolocation data in criminal investigations.

http://news.cnet.com

Module Objectives

- Mobile Phone
- Different Mobile Devices
- Hardware and Software Characteristics of Mobile Devices
- Cellular Network
- Mobile Operating Systems
- Types of Mobile Operating Systems
- What a Criminal Can Do with Mobiles Phones

- Mobile Forensics
- Mobile Forensics Challenges
- Memory Considerations in Mobiles
- Precautions to Be Taken Before Investigation
- Mobile Forensics Process
- Mobile Forensics Software Tools
- Mobile Forensics Hardware Tools



Module Flow

Mobile Phones

Mobile Operating Systems

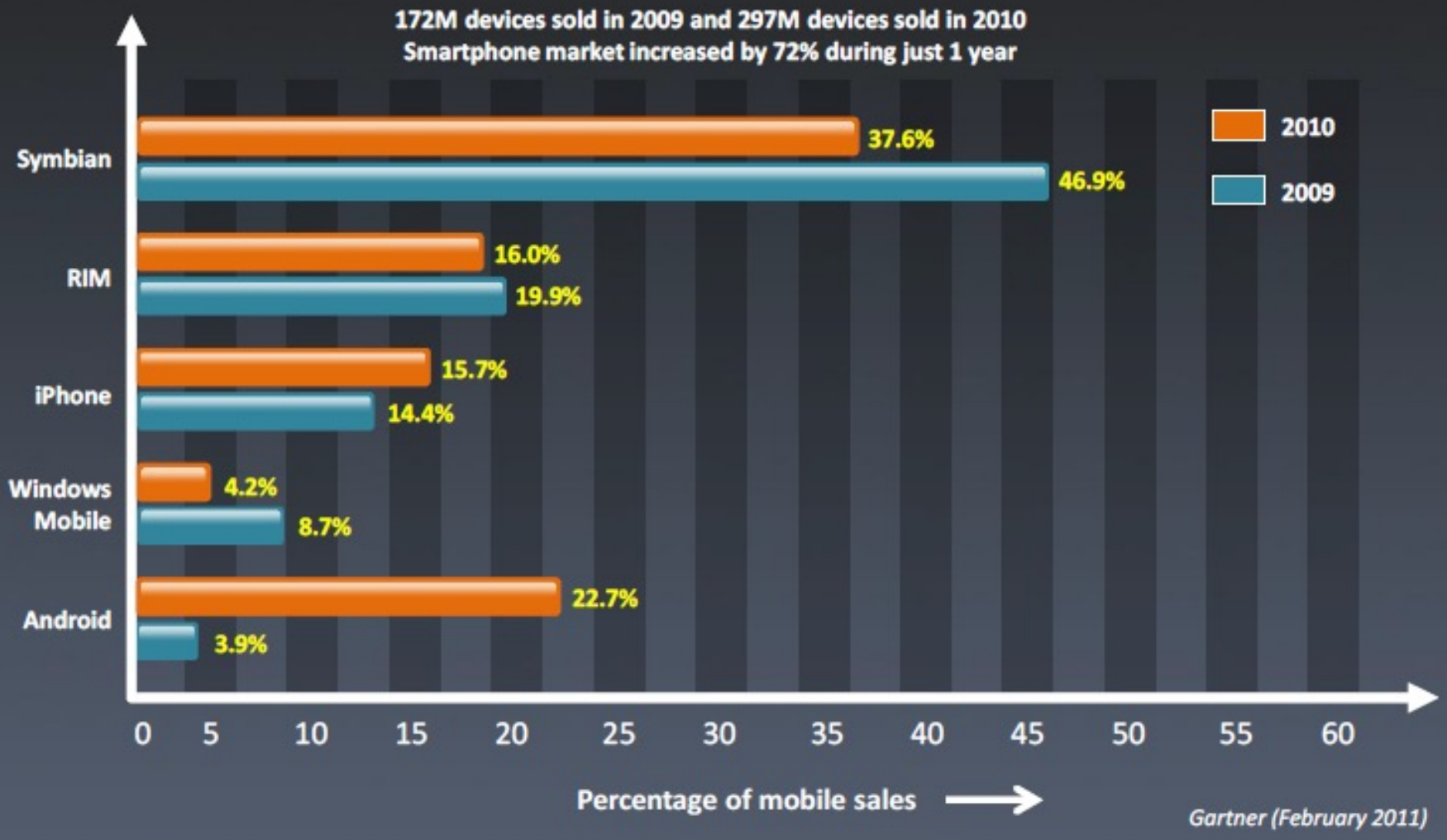
Mobile Forensics

Mobile Forensics Process

Mobile Forensics Software Tools

Mobile Forensics Hardware Tools

Smartphone Sales Statistics 2010/2011



Gartner (February 2011)

Mobile Phone

The mobile phone or cellular phone is a **complex electronic device** that contains many features

- Voice and text messaging
- Personal Information Management (PIM)
- SMS and MMS messaging
- Internet and email
- Chat

Features

- Store the images and videos
- Games
- Camera with video recorder
- Bluetooth and infrared
- GPS navigator

Different Mobile Devices

BlackBerry

- BlackBerry is a **personal wireless handheld device** that supports email, mobile phone capabilities, text messaging, web browsing and other wireless information services
- A BlackBerry can be used as a **phone, address book, or calendar, and to create to-do lists and access wireless Internet**

iPod

- iPod is a **portable digital audio and video player** offering a huge storage capacity

iPhone

- The iPhone is an **Internet-connected multimedia Smartphone** designed and marketed by Apple Inc. with a **multi-touch screen and a minimal hardware interface**

Hardware Characteristics of Mobile Devices

Characteristics	Basic Phone	Advanced Phone	Smartphone
Processor	Limited Speed	Improved speed	Superior Speed
Memory	Limited Capacity	Improved Capacity	Superior Capacity, Built-in Hard Drive Possibility
Display	Grayscale	Color	Large size, 16-bit Color (65,536 colors) or Higher
Card Slots	None	MiniSD or MMCmobile	MiniSD or MMCmobile
Camera	None	Still	Still, Video
Text Input	Numeric Keypad	Numeric keypad, soft keyboard	Touch Screen Handwriting Recognition, Built-in QWERTY style keyboard
Cell Interface	Voice and Limited Data	Voice and High Speed Data	Voice and Very High Speed Data
Wireless	IrDA	IrDA, Bluetooth	IrDA, Bluetooth, WiFi
Battery	Fixed, Rechargeable Lithium Ion Polymer	Removable, Rechargeable Lithium Ion Polymer	Removable, Rechargeable Lithium Ion

Software Characteristics of Mobile Devices

Characteristics	Basic Phone	Advanced Phone	Smartphone
OS	Proprietary	Proprietary	Linux, Windows Mobile, RIM OS, Palm OS , Symbian
PIM	Simple Phonebook	Phonebook and Calendar	Reminder List, Enhanced Phonebook and Calendar
Applications	None	MP3 Player	MP3 Player, Office Document Viewing
Messaging	Text Messaging	Text with Simple Embedded Images and Sounds	Text, Enhanced Text, Full Multimedia Messaging
Chat	None	SMS chat	Instant Messaging
Email	None	Via Network Operator's Service Gateway	Via POP or IMAP Server
Web	None	Via WAP Gallery	Direct HTTP
Wireless	IrDA	IrDA, Bluetooth	IrDA, Bluetooth, WiFi

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 radio transceiver equipment that communicates with mobile phones

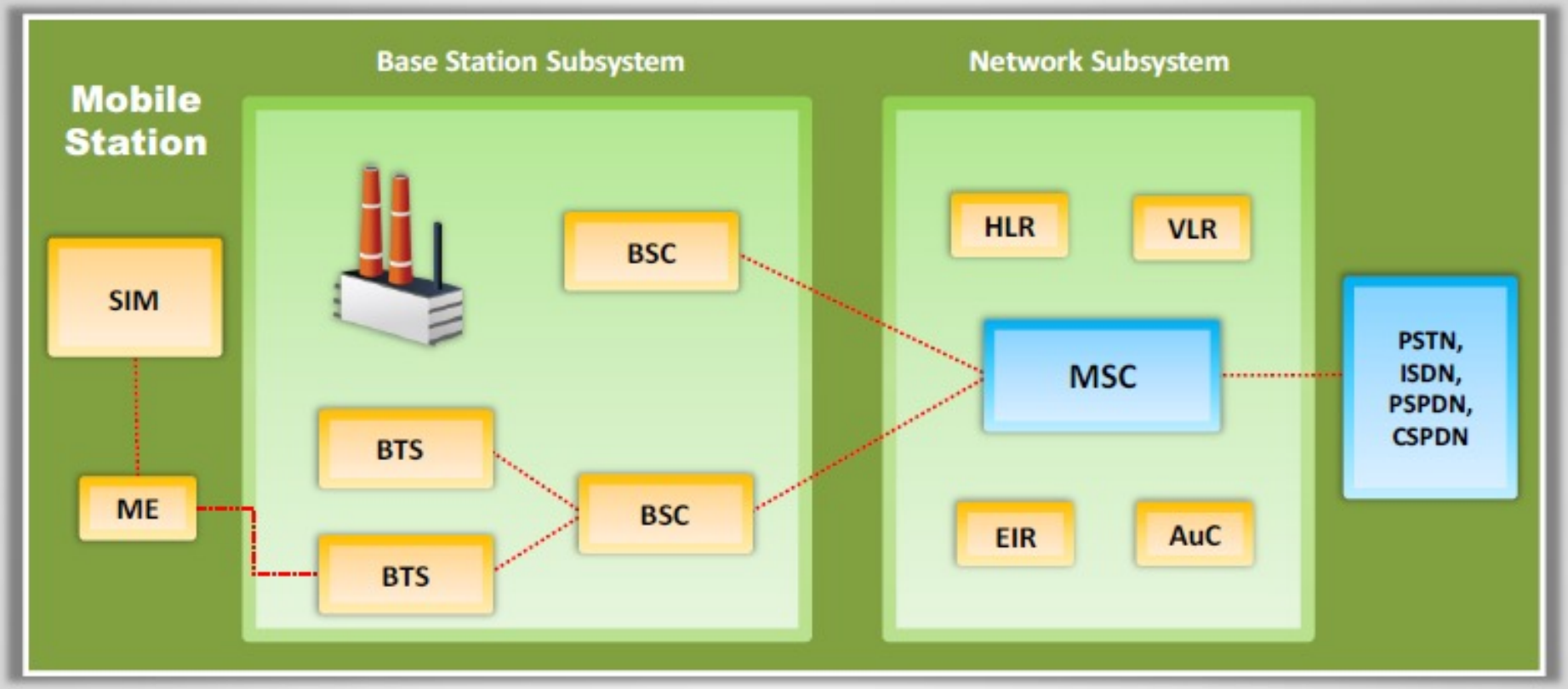
3. Base Station Controller (BSC): It manages the transceiver's equipment and performs channel assignment

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

5. Home Location Register (HLR): It is the database at 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

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

Different Cellular Networks

- Code Division Multiple Access (CDMA)
- Enhanced Data Rates for GSM Evolution (EDGE)
- Integrated Digital Enhanced Network (iDEN)
- General Packet Radio Service (GPRS)
- Global System for Mobile Communications (GSM)
- High Speed Downlink Packet Access (HSDPA)
- Time Division Multiple Access (TDMA)
- Universal Mobile Telecommunications System (UMTS)
- Unlicensed Mobile Access (UMA)

Module Flow

Mobile Phones

Mobile Operating Systems

Mobile Forensics

Mobile Forensics Process

Mobile Forensics Software Tools

Mobile Forensics Hardware Tools

Mobile Operating Systems

1

A mobile operating system is the **operating system** that operates a mobile device like a mobile phone, smartphone, PDA, etc.

2

It determines the **functions and features** available on mobile devices such as keyboards, applications, email, text messaging, etc.

3

It **manages the communication** between the mobile device and other compatible devices like computers, televisions, or printers

It controls which **third-party applications** can run on the device

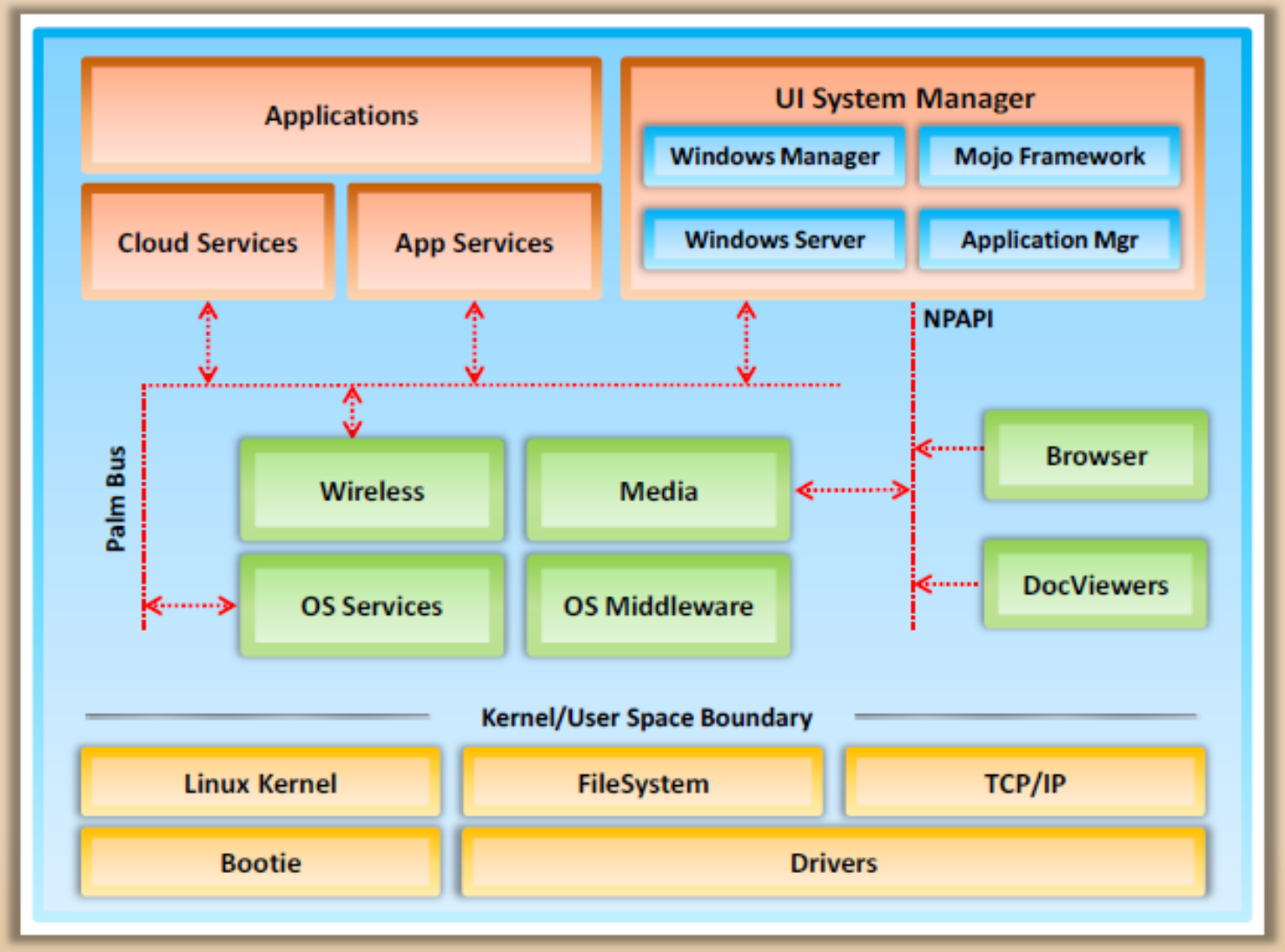
4

Types of Mobile Operating Systems

webOS

- webOS is a **mobile operating system** running on the **Linux kernel**
- It uses **multi-touch gestures** to navigate on the **touchscreen**
- It allows users to access Gmail, Yahoo!, Facebook, LinkedIn, etc., using its **Synergy** feature, and integrates all these sources into a single list
- It uses the **WebKit layout engine** to access web browsers

webOS System Architecture



Symbian OS

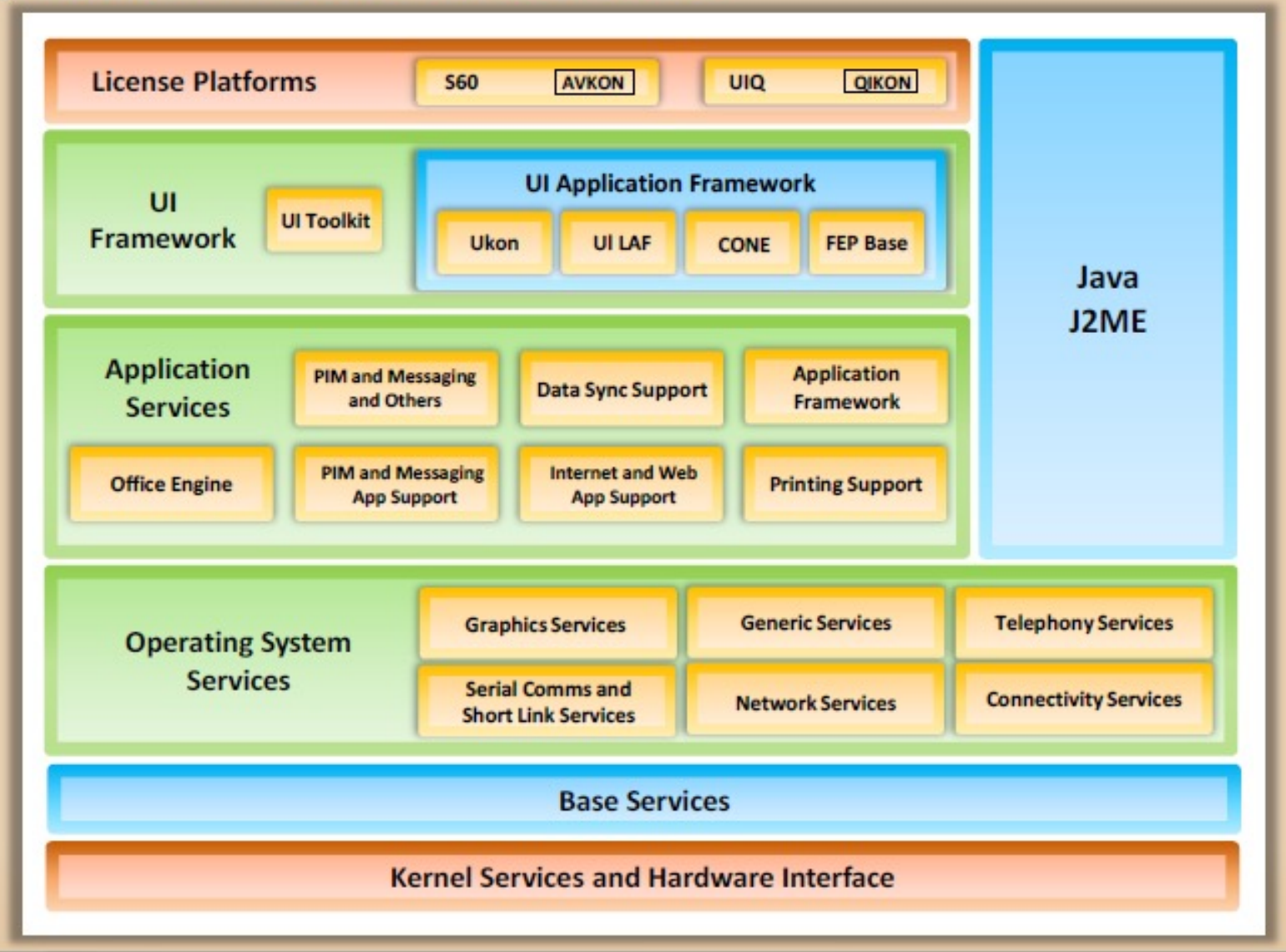
- Symbian OS is a mobile operating system designed for smartphones and currently maintained by Nokia
- It is designed to make minimal demands on batteries and to have low memory

symbian OS

Features

- Associated libraries
- User interface frameworks
- Memory management optimized for embedded software environment
- WebKit-based browser
- Object-oriented software architecture

Symbian OS Architecture



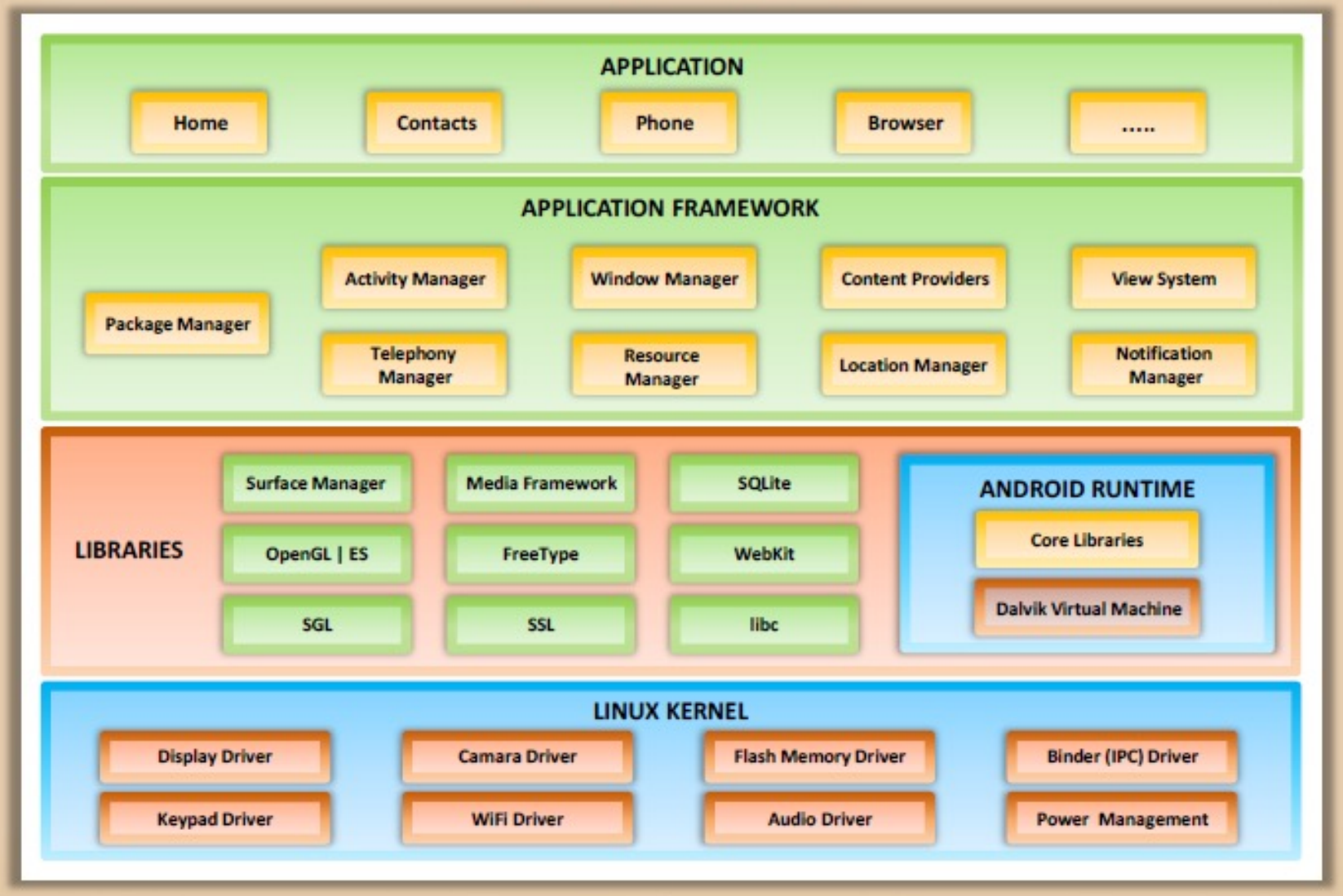
Android OS

Android is a software stack developed by Google for mobile devices that includes an operating system, middleware, and key applications

- Application framework enabling reuse and replacement of components
- Dalvik virtual machine optimized for mobile devices
- Integrated browser based on the open source WebKit engine
- SQLite for structured data storage
- Media support for common audio, video, and still image formats (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, GIF)
- Rich development environment including a device emulator, tools for debugging, memory and performance profiling, and a plugin for the Eclipse IDE

http://developer.android.com

Android OS Architecture



RIM BlackBerry OS

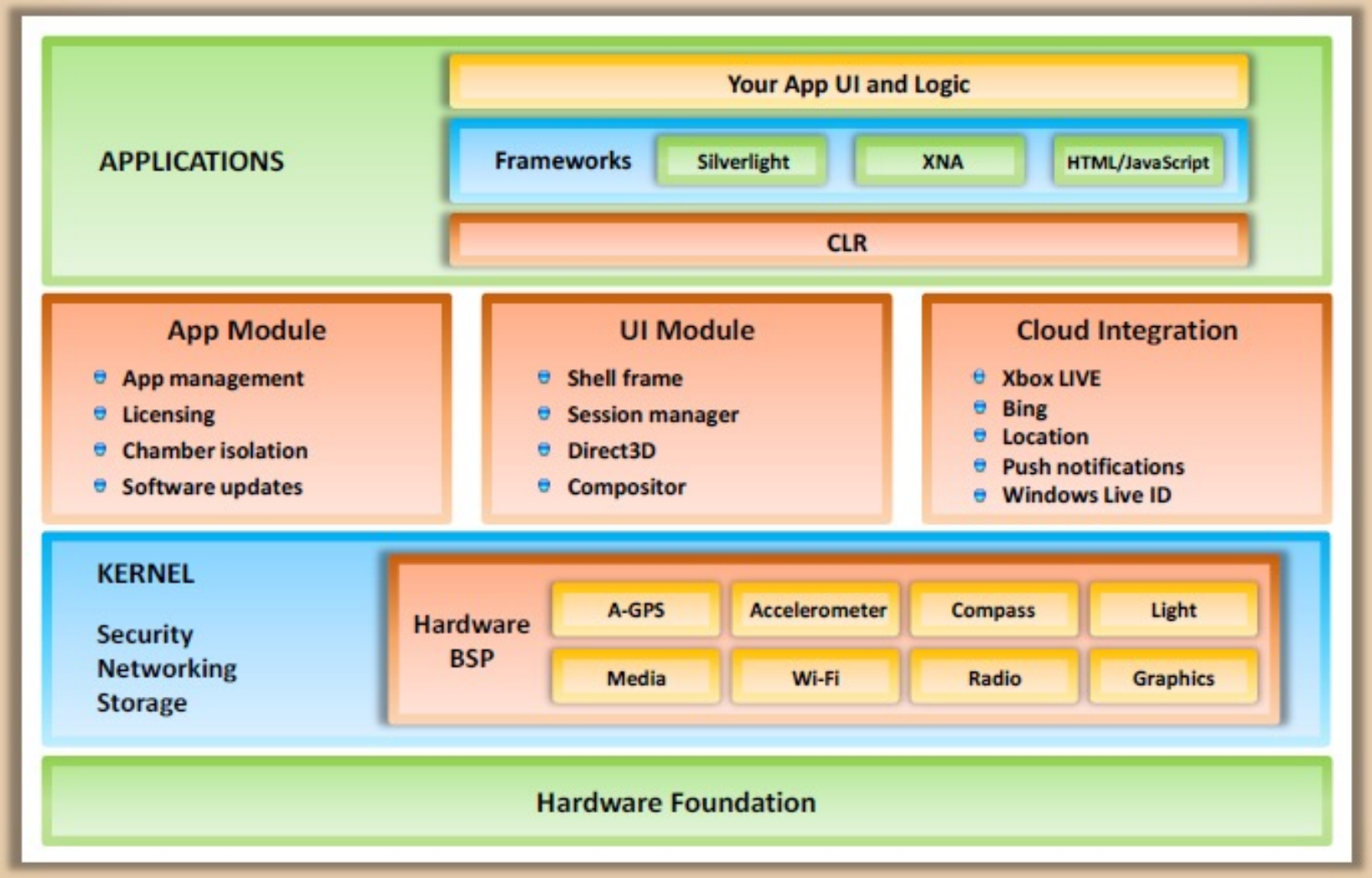
- BlackBerry OS is a mobile operating system developed by Research In Motion (RIM) for its BlackBerry line of smartphone handheld devices
- It provides multitasking and supports particular input devices used in BlackBerry such as trackwheel, trackball, trackpad, and touchscreen

Windows Phone 7

- Windows Phone 7 is a mobile operating system developed by Microsoft, and is the successor to its Windows Mobile platform
- Windows Phone 7 features:

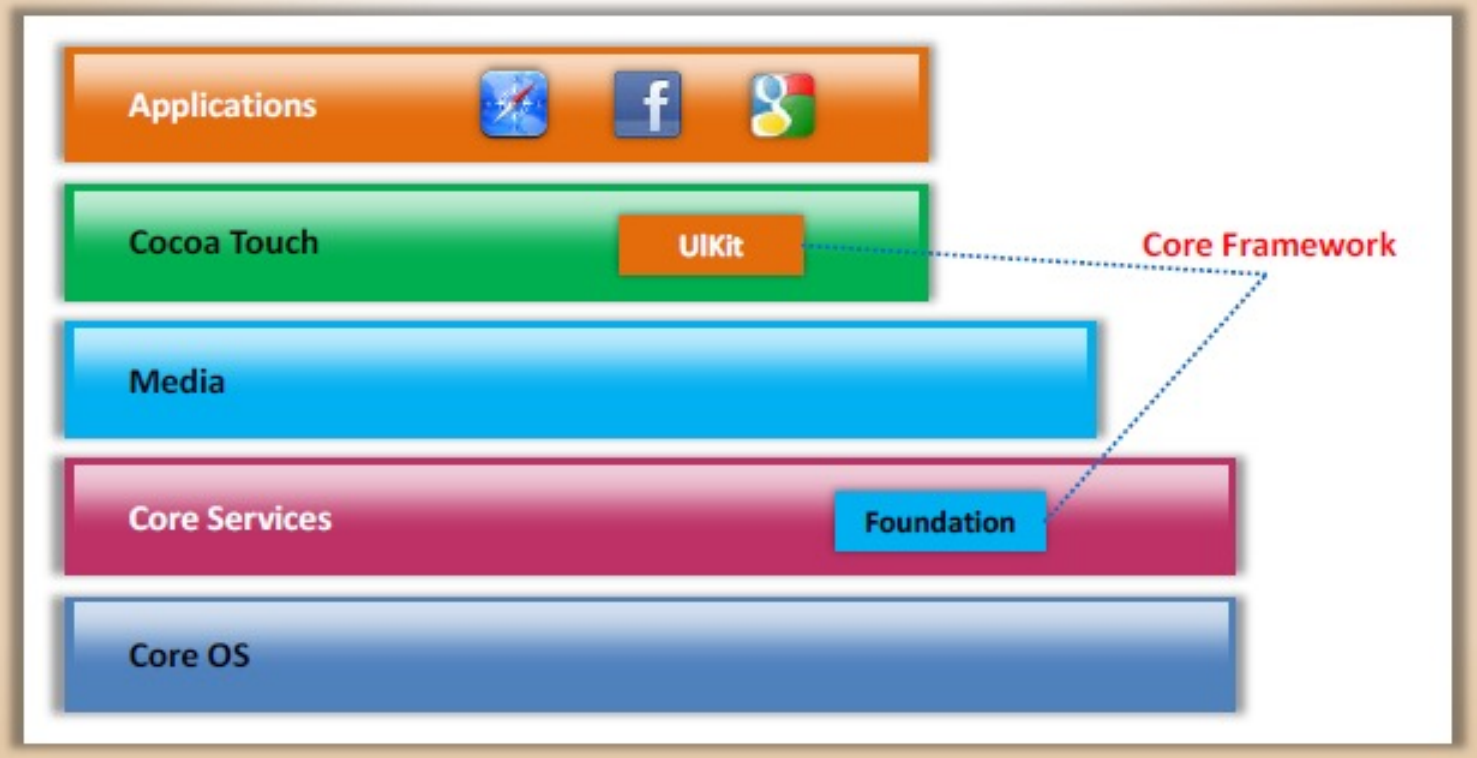
- Smooth transitional user interface
- Good Office integration and support
- Easy setup for Google, Windows Live, Yahoo! Mail, and others
- Informative lock screen and auto-hidden top status bar

Windows Phone 7 Architecture



Apple iOS

- iOS is Apple's mobile operating system, which supports Apple devices such as iPhone, iPod touch, iPad, and Apple TV
- The user interface is based on the concept of direct manipulation, using multi-touch gestures



Module Flow

Mobile Phones

Mobile Operating Systems

Mobile Forensics

Mobile Forensics Process

Mobile Forensics Software Tools

Mobile Forensics Hardware Tools

What a Criminal Can Do with Mobiles Phones

1. Harassing or threatening
2. Sending viruses and Trojans to other users
3. Distributing pornographic images and videos
4. Data theft and spamming
5. Storing and transmitting personal and corporate information
6. Sending dangerous or offensive SMS and MMS
7. Cloning the SIM data and manipulating SIM properties for illicit use
8. Remove the Service Provider Lock (SP-Lock)

Mobile 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 and SIM cards

- Mobile forensics aim to catch the perpetrators of crimes that involve the use of mobile phones

Mobile Forensics Challenges

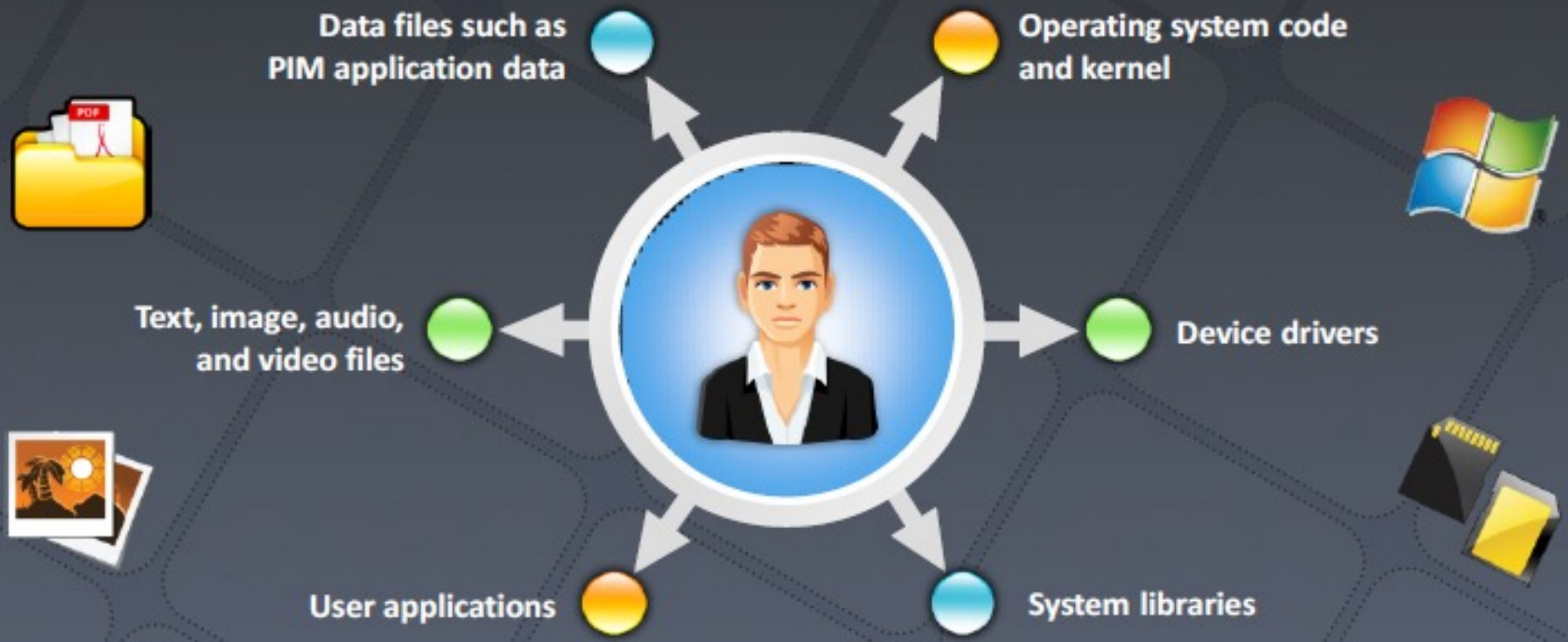
- Often a disposable solution for criminals
- Devices are not widely supported by forensic solutions
- No contract and no identity tied to the device or service contract
- No single standardized approach to investigate mobile devices
- Various forensic tools are only able to operate on a particular handset, specific platforms for a specific product, a distinct operating system, or specific hardware architecture
- Ever-changing advancement of mobile devices increases the complexity of mobile device examinations

Forensics Information in Mobile Phones

	Call history	SIM card information	Phonebook information
Subscriber and equipment identifiers	SMS and MMS	GPRS, WAP, and Internet settings	IMEI
Photos and sound files	Audio and video recording	Network Information, GPS location	Phone info (CDMA Serial Number)
Web browsing activities	Electronic documents	Emails, memos, calendars, etc.	

Memory Considerations in Mobiles

- A mobile phone contains various types of volatile and nonvolatile memory
- It stores several kinds of data, including:



Subscriber Identity Module (SIM)

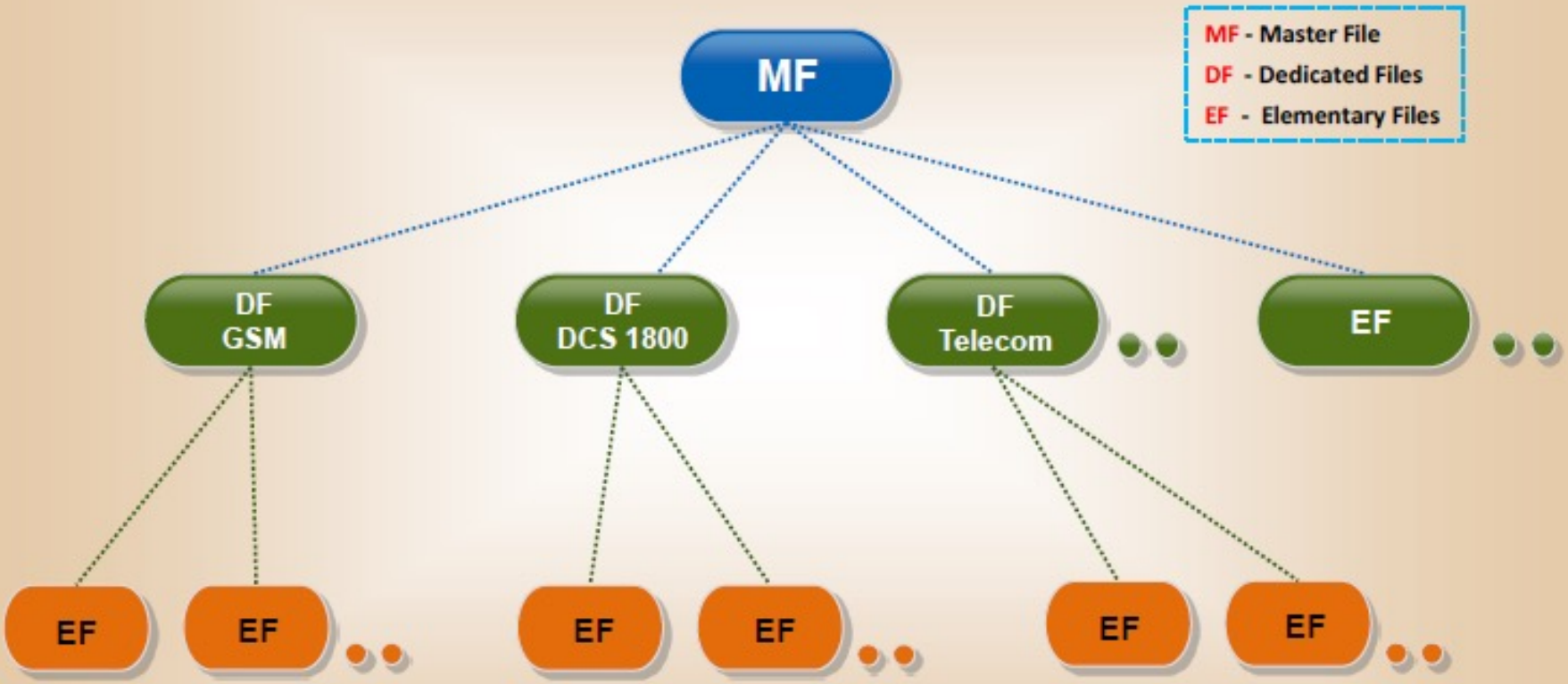
SIM is a removable component that contains essential information about the subscriber

It has both volatile and nonvolatile memory

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

The file system of a SIM resides in nonvolatile memory

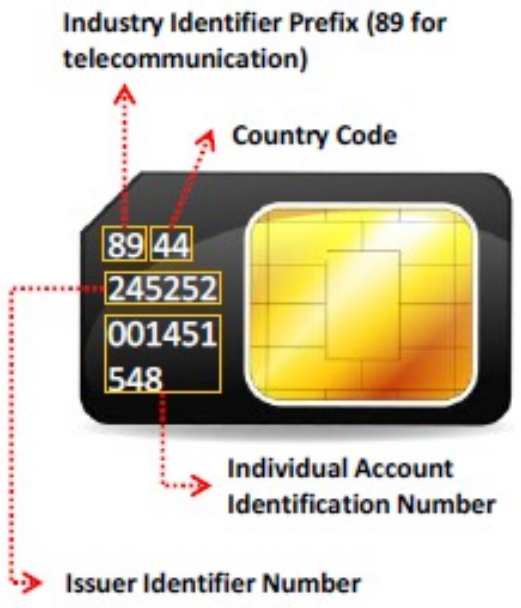
SIM File System



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



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 International Mobile Equipment Identifier (IMEI) can be obtained by keying in ***#06#**

Electronic Serial Number (ESN)

- ESN is a unique **32-bit identifier recorded on a secure chip** in a mobile phone by the manufacturer
- 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	

Precautions to Be Taken Before Investigation (Cont'd)

1. Handle cell phone evidence properly to maintain physical evidence such as fingerprints

2. To avoid unwanted interaction with devices found on the scene, turn off wireless interfaces such as Bluetooth and Wi-Fi radios on equipment brought into the search area

3. Photograph the crime scene including mobile phones, cables, cradles, power connectors, removable media, and connections

4. If the device's display is ON, the screen's contents should be photographed and, if necessary, recorded manually, capturing the time, service status, battery level, and other displayed icons

5. Collect other sources of evidence such as (U)SIM, media, and other hardware in the phone, but do not remove them from the device

Precautions to Be Taken Before Investigation

If the phone is in a cradle or connected to a PC with a cable, then seize the phone with the cable and cradles, because unplugging the device from the computer may eliminate the data transfer or overwrite the synchronization

If the phones are found in a compromised state such as immersed in a liquid, remove the battery to prevent electrical shorting and seal the remainder of the mobile phone in a proper container filled with the same liquid, which should not be caustic

Isolate the phone from the radio network, which helps to keep new traffic from overwriting the existing data

Isolate the phone from other synchronized devices, which keeps the new data from affecting the existing data

Some mobile communication devices use alkaline batteries as a power source; replace such batteries in transit to minimize the risk of data loss due to complete battery discharge

Module Flow

Mobile Phones

Mobile Operating Systems

Mobile Forensics

Mobile Forensics Process

Mobile Forensics Software Tools

Mobile Forensics Hardware Tools

Mobile Forensic Process

Collecting the Evidence

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

Points to Remember while Collecting the Evidence

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)
- Keep it charged and protect it from tampering
- Do not press any key, it may lose the data in the device

If the device is off, leave it off

- Turning it on could alter evidence on device
- Do not remove the battery; this may cause the contents of some devices to be lost

Collecting an iPod/iPhone Connected to a Computer

If an iPod/iPhone is connected to a Mac computer

- Check whether the **device is mounted** by looking at the screen
- If it is mounted, **eject the device by dragging the icon** of the iPod/iPhone to the trashcan on the Macintosh desktop

If an iPod/iPhone is connected to a Windows computer

- Note the name of the iPod/iPhone and check whether **the device is mounted or not**
- If it is mounted, eject the device by clicking the "**Unplug or eject hardware**" icon on the task bar

Document the Scene and Preserve the Evidence (Cont'd)

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
5. Handle electronic evidence in a manner that preserves its integrity
6. Protect the electronic evidence from magnetic fields, dust, vibration, and other factor that may damage the integrity of the electronic evidence
7. Secure the devices from mechanical or electrical shock

Document the Scene and Preserve the Evidence

- Preserve all the evidence and documents in a secure location
- Focus on hidden or trace evidence and take necessary actions to preserve it
- Pack the electronic devices in antistatic packaging
- Make sure that all the containers that hold the evidence are labeled in an appropriate way
- Keep electronic evidence away from magnetic sources while transporting
- Store the evidence in a secure area and weather controlled environment that is away from high temperature and humidity
- Maintain the chain of custody documents

Imaging and Profiling

- Imaging is the process of creating an exact copy of the contents of a digital device to prevent the accidental modification of the original evidence
- Use data imaging tools, which make exact bit-to-bit copies of the originals and prevent any alteration

Acquire the Information

- Acquisition of data at the scene avoids loss of information due to battery depletion, damage during transportation and storage
- Data acquisition process at the crime scene is hampered due to lack of controlled settings, appropriate equipment, and other prerequisites
- Try to acquire the data from images of the evidence such as SIM cards, memory cards, or directly from the mobile device itself
- Use data acquiring tools such as SIM Card Data Recovery and SIMCon to recover the data from evidence, SIM cards, or memory cards

Device Identification

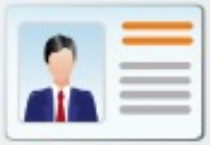
- Mobile **device needs to be identified** by the model, operating system, and service provider
- This information allows examiners to **choose the proper data acquisition tool** to collect the evidence

Check the following for device identification:

- Check the **battery cavity** to find manufacturer's name
- If the mobile device is powered on, **check the screen to find the type of phone**, service provider name, and operating system used
- If the mobile device is powered off, remove the battery and check the manufacturer logo to **find the model number, IMEI, and FCC ID**

Acquire Data from SIM Cards (Cont'd)

SIM contains important information related to the forensics investigation:



Service related information such as unique identifiers for the (U)SIM, the Integrated Circuit Card Identification (ICCID), and the subscriber, the International Mobile Subscriber Identity (IMSI)

Phonebook and call information such as Abbreviated Dialing Numbers (ADN) and Last Numbers Dialed (LND)

Messaging information including SMS, EMS, and multimedia messages

Location information, including Location Area Information (LAI) for voice communications and Routing Area Information (RAI) for data communications

Acquire Data from SIM Cards

To access the SIM, PIN code (Personal Identification Number) is required

Failure to enter a valid PIN in three attempts blocks the card and then an eight-digit PUK (Personal Unlock Number) must be entered

PUK is provided by the network operator and cannot be changed by the user

Failure to get correct PUK in 10 attempts disables the SIM permanently

Investigator should ask the network operator for PUK to gain access to the SIM

Use SIM card data recovery tool such as SIM Analyzer, SIMCon, etc., to recover data

Acquire Data from Unobstructed Mobile Devices

- An unobstructed device does not require a password or other authentication technique to access the device and perform an acquisition
- Unobstructed devices include mainly CDMA phones, freestanding (U)SIMs, and GSM phones containing a (U)SIM
- Record the time and date in the phones
- Check with the contacts, SMS, and other entries
- Use different data recovery tools such as Cell Phone Analyzer to recover the deleted information from the device

Acquire the Data from Obstructed Mobile Devices

- Obstructed devices typically refer to devices that are shut off and require successful authentication to gain access

- Recover the information from such devices using the following techniques:
  - Ask the victim or suspect for PIN
  - Review the seized non-electronics materials such as notes or print outs
  - Contact the service provider
  - Contact the device manufacturer and service provider for information on known backdoors and vulnerabilities that might be exploited
  - Contact the device maintenance and repair companies, as well as commercial organizations that provide architecture information on handheld device products
  - Use different forensics tools such as Cell Phone Analyzer
  - Use a data recovery tool such as SIM Analyzer and SIMCon

Acquire Data from Memory Cards (Cont'd)

Removable media extends the storage capacity of mobile phones, allowing individuals to store additional files beyond the device's built-in capacity and to share data between compatible devices

1

Mobile phone supports Secure Digital (SD), MultiMedia Cards (MMC), and other types of removable media containing significant amounts of data

2

Recover the data from removable media and memory cards with the use of a media reader and a Memory Card Data Recovery tool

3

Acquire Data from Memory Cards (Cont'd)

Name	Characteristics
Compact Flash Card (CF)	Matchbook size (length-36.4mm, width-42.8mm, thickness-3.3mm for Type I cards and 5mm for type II cards) 50-pin connector, 16-bit data bus
MMCplus (compatible with original MultiMedia Card or MMC)	Postage stamp size (length-32mm, width-24, and thickness-1.4mm) 13-pin connector, 1, 4, or 8 bit data bus (7-pin connector, 1-bit data bus, MCC compatibility)
MMCmobile (compatible with original Reduced Size MMC or RS-MMC)	Thumbnail size (length-18mm, width-24mm, and thickness-1.4 mm) 13-pin connector, 1, 4, or 8 bit data bus (7-pin connector, 1-bit data bus, RS-MMC compatibility) Reqiures a mechanical adapter to be used in a full size MMCplus slot
MMCmicro	Contact lens size (length-14 mm, width-12 mm, and thickness-1.1 mm) 10-pin connector and a 1 or 4-bit data bus Requires a mechanical adapter to be used in a full size MMCplus slot
Secure Digital (SD) Card	Postage stamp size (length-32 mm, width-24 mm, and thickness-2.1 mm) 9-pin connector, 1 or 4-bit data bus Features a mechanical erasure-prevention switch

Acquire Data from Memory Cards

Name	Characteristics
MiniSD Card	Thumbnail size (length-21.5 mm, width-20mm, and thickness-1.4 mm) 9-pin connector, 1 or 4 bit data bus Requires a mechanical adapter to be used in full size SD slot
MicroSD (formerly Transflash)	Contact lens size (length-15 mm, width-11 mm, and thickness-1 mm) 6-pin connector, 1 or 4-bit data bus Requires a mechanical adapter to be used in a full size SD slot
Memory stick	Chewing gum stick size (length-50 mm, width-21.45 mm, thickness-2.8 mm) 10-pin connector, 1-bit data bus Features a mechanical erasure prevention switch
Memory Stick Duo	Partial chewing gum stick size (length-31mm, width-20 mm, thickness-1.6 mm) 10-pin connector, 4-bit data bus Features a mechanical adapter to be used in a full size Memory Stick slot
Memory Stick Duo	Contact lens size (length-12.5 mm, width-15 mm, and thickness-1.2 mm) 11-pin connector, 4-bit data bus Requires a mechanical adapter to be used in a full size Memory Stick slot

Acquire Data from Synched Devices

Mobile phones are generally synched with the computer to save the data as another backup copy

A significant amount of evidence on a mobile phone may also be present on the suspect's laptop or personal computer

Search for types of evidence including contacts, SMS, email details, images, and videos

Gather Data from Network Operator

- Gather the detailed information from the network operator including calls made/received, message traffic, data transferred, and connection location/timing

Home Location Register (HLR) provides:

- Customer's name and address
- Billing name and address (if other than customer)
- User's name and address (if other than customer)
- Billing account details
- Telephone number (MSISDN)
- IMSI
- SIM serial number (as printed on the SIM-card)
- PIN/PUK for the SIM
- Subscriber services allowed

Check Call Data Records (CDRs)

CDR files created in the MSC and records information about:

- Originating MSISDN
- Terminating MSISDN
- Originating and terminating IMEI
- Initial serving Base Station (BTS)
- Connection time
- Time the call was disconnected and reason

Time[26]	Qualifier[11]	Calling Number[21]	Called Number[21]	PRI ID Number[5]	B-Channel[3]	Time[26]	Text[35]
Orig time	Call Rqst	calling	called	PRI id	B-channel		
Disc time	Call Disc	calling	called	PRI id	B-channel	connect time	Cause
Orig time	Setup Fail	calling	called	PRI id	B-channel		
Disc time	Disc Fail	calling	called	PRI id	B-channel	connect time	Cause

Gather Data from SQLite Record (Cont'd)

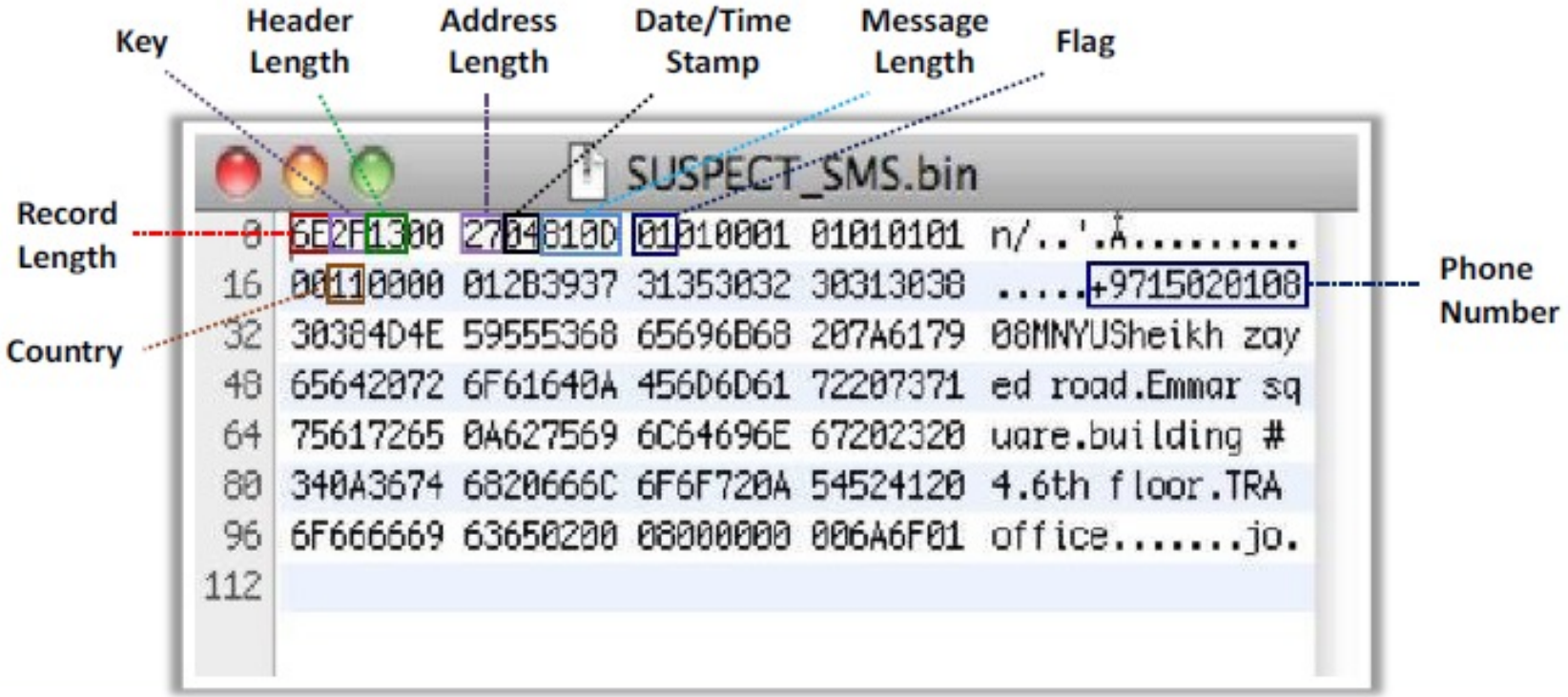
- Mobile operating systems iOS and Android use SQLite databases to store vital information such as **contacts, SMS,** and **call records**
- Use **Base Mac SQLite editor** to see the **schema of the message table**

Schema | Data | SQL | Log

Name	Type	Constraints
ROWID	INTEGER	PK
address	TEXT	
date	INTEGER	
text	TEXT	
flags	INTEGER	
replace	INTEGER	
svc_center	TEXT	
group_id	INTEGER	
association_id	INTEGER	
height	INTEGER	
UIFlags	INTEGER	
version	INTEGER	
subject	TEXT	
country	TEXT	
headers	BLOB	
recipients	BLOB	
read	INTEGER	

Gather Data from SQLite Record

- Look for the records in Hex viewer to get the information about record length, key, record header length, address length, telephone number, date and time stamp, message length, flag, and country



Analyze the Information (Cont'd)

- Subscriber and equipment identifiers
- Date/time, language, and other settings
- Phonebook information
- Appointment calendar information
- Text messages
- Dialed, incoming, and missed call logs

- Electronic mail
- Photos
- Audio and video recordings
- Multi-media messages
- Instant messaging and web browsing activities
- Electronic documents
- Location information

Analyze the Information

1. Identify the individuals who created, modified, or accessed a file
2. Determine when events occurred by analyzing call logs, the date/time, and content of messages and email
3. Create the timeline of the events
4. Recover the hidden information
5. If the entries such as SMS, contacts, emails, etc., are encrypted, then use cryptanalysis tools such as crank
6. Use password cracking tools such as Hydra to read the password protected information
7. Try to find out the geographical location of the attacker

Generate Report

- Report generation is the process of preparing a comprehensive summary of all the steps performed and conclusions reached in the forensics investigation
- A good report relies on proper documentation, notes, photographs, sketches, and software-generated content
- Report generated by the forensics tool include items from the case file, such as case number, date, title, evidence category, outcome, etc.
- Investigator needs to include only related findings in the final report to minimize its size and lessen confusion for the reader

- Mobile forensics report contains the following information:
  - Reporting agency name
  - Case number
  - Case investigator name
  - Case submitter name
  - Date of receipt and report
  - List of items submitted for examination
  - Examiner name and signature
  - Equipment and setup used in the examination
  - Brief description of steps taken during examination
  - Details of findings
  - Report conclusions

Module Flow

Mobile Phones

Mobile Operating Systems

Mobile Forensics

Mobile Forensics Process

Mobile Forensics Software Tools

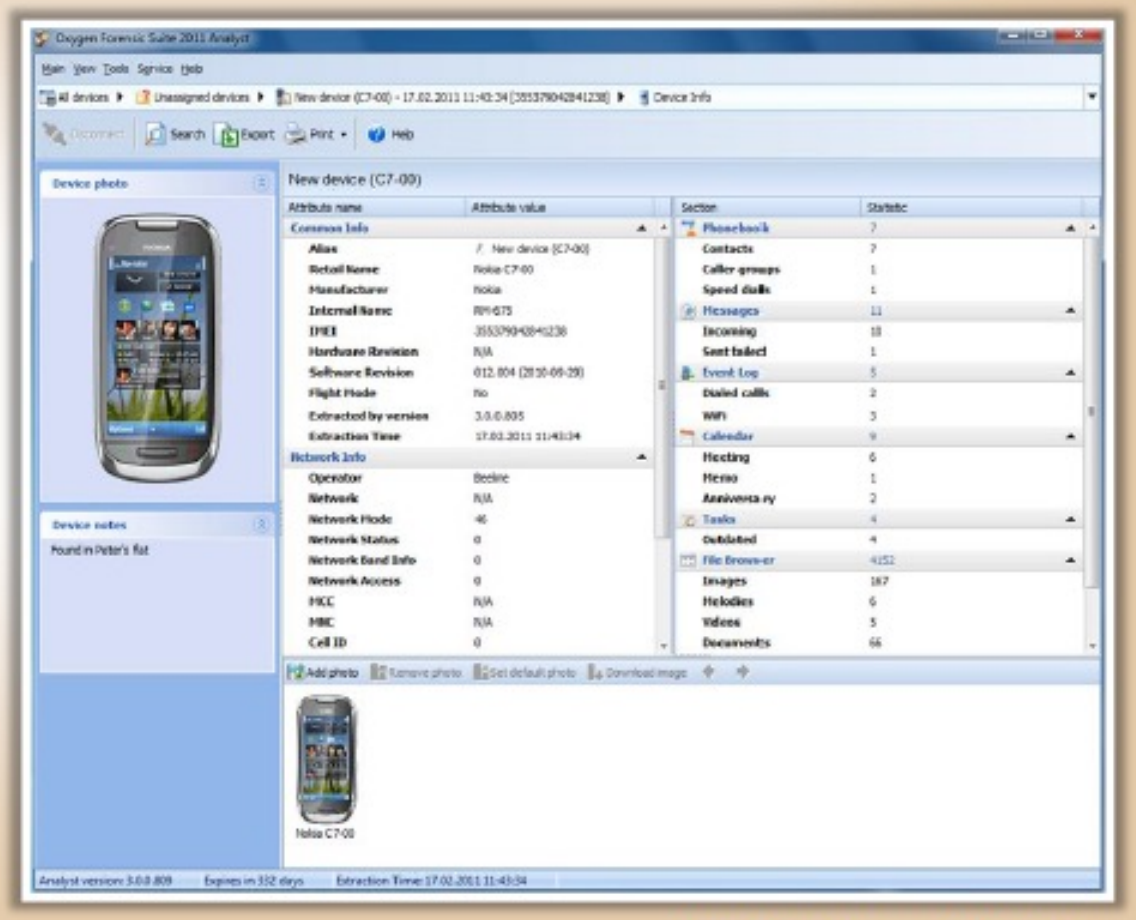
Mobile Forensics Hardware Tools

Oxygen Forensic Suite 2011

Oxygen Forensic Suite 2011 is mobile forensics software that recovers data from cell phones, smartphones, and PDAs

Features

- Supports Symbian OS, Apple iPhone, Android, Windows Mobile, and RIM BlackBerry devices
- Stores messages in custom folders and subfolders
- Extracts all files from phone memory as well as from flash card, including installed applications and their data



http://www.oxygen-forensic.com

MOBILedit! Forensic

MOBILedit! Forensic collects all possible data from the mobile phone and generates an extensive forensics report

Features

1. Retrieves all data from a phone with one click

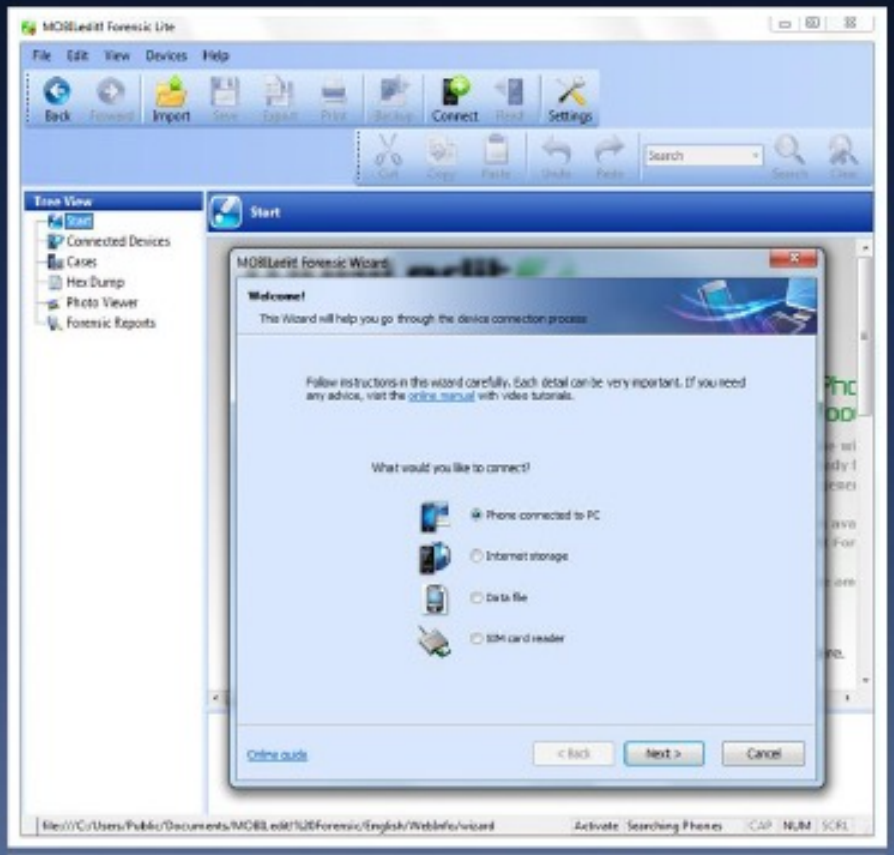
2. Reads deleted messages from the SIM card

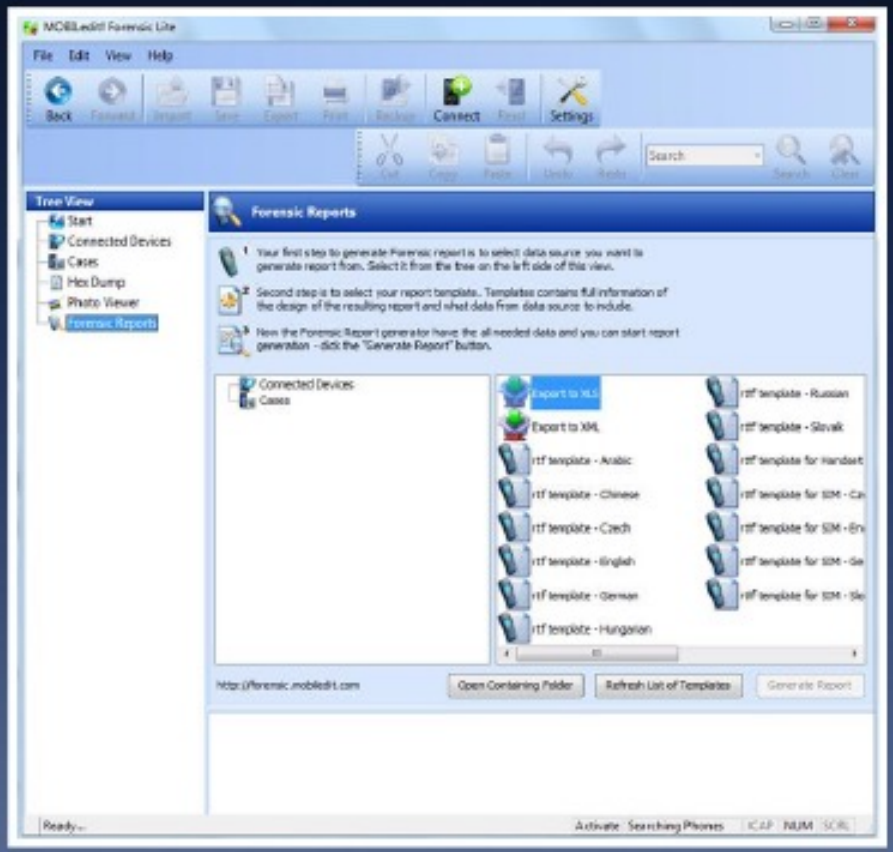
3. Generates forensic reports ready for the courtroom in a variety of formats

4. Allows investigator to manually look through the contents of the phone and back up data to the PC

5. Direct SIM analyzer through SIM readers

MOBILedit! Forensic: Screenshot

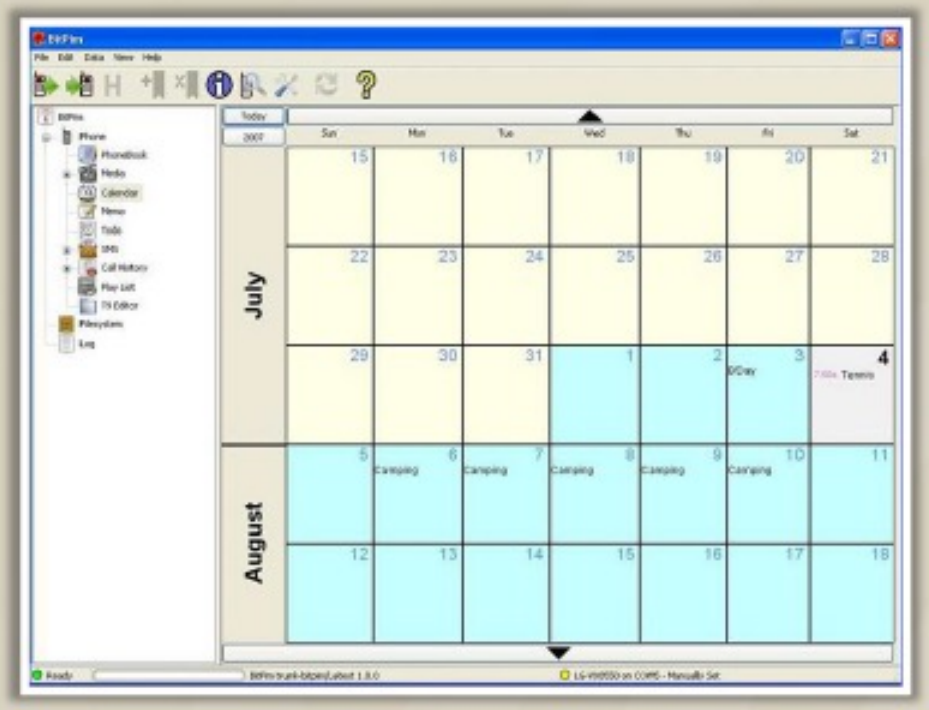


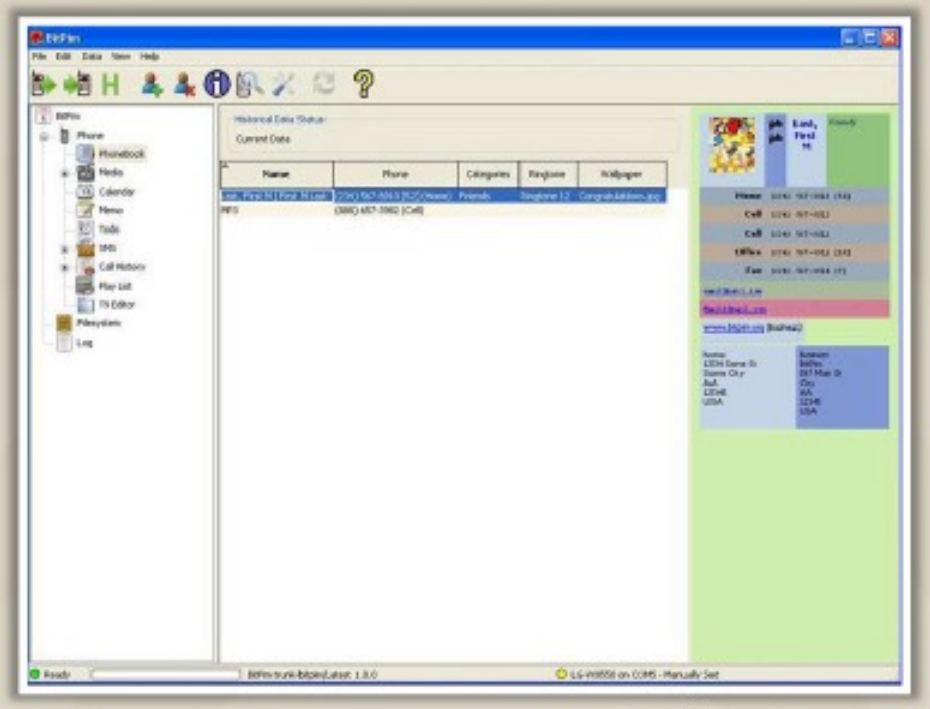


http://www.mobiledit.com

BitPim

- BitPim is a program that allows you to view and manipulate data on many CDMA phones from LG, Samsung, Sanyo etc.
- This data includes the Phonebook, Calendar, Wallpapers, Ringtones, and the File system for most Qualcomm CDMA chipset-based phones





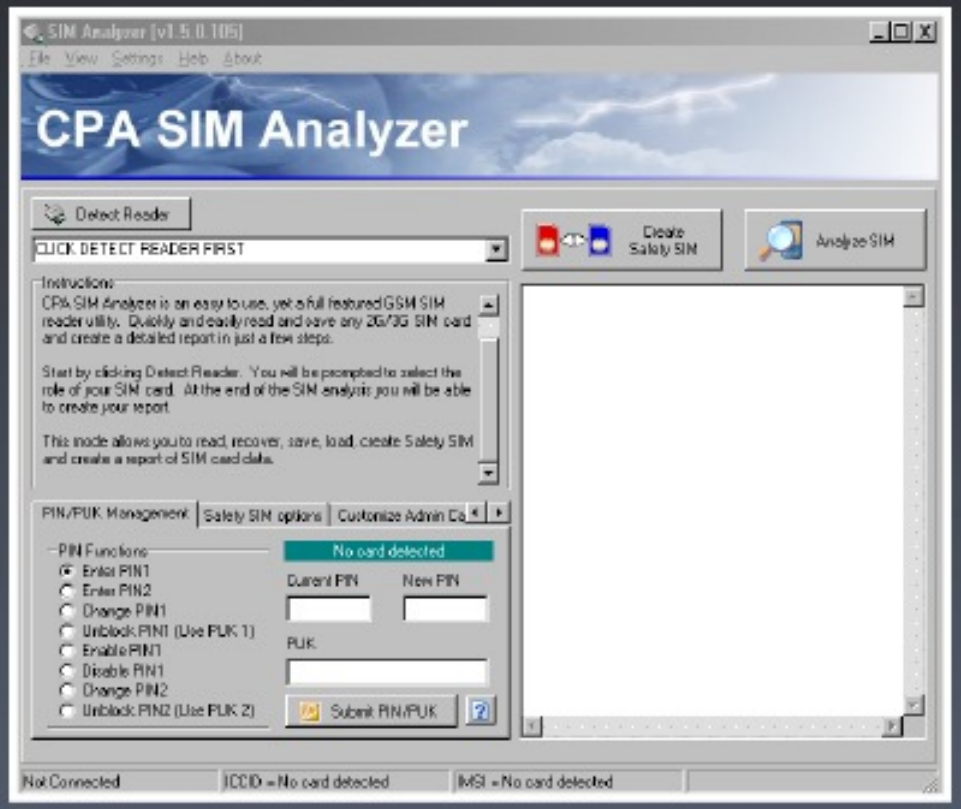
http://www.bitpim.org

SIM Analyzer

SIM Analyzer is a cell phone forensics tool that **recovers the contents from SIM cards** of different mobile devices

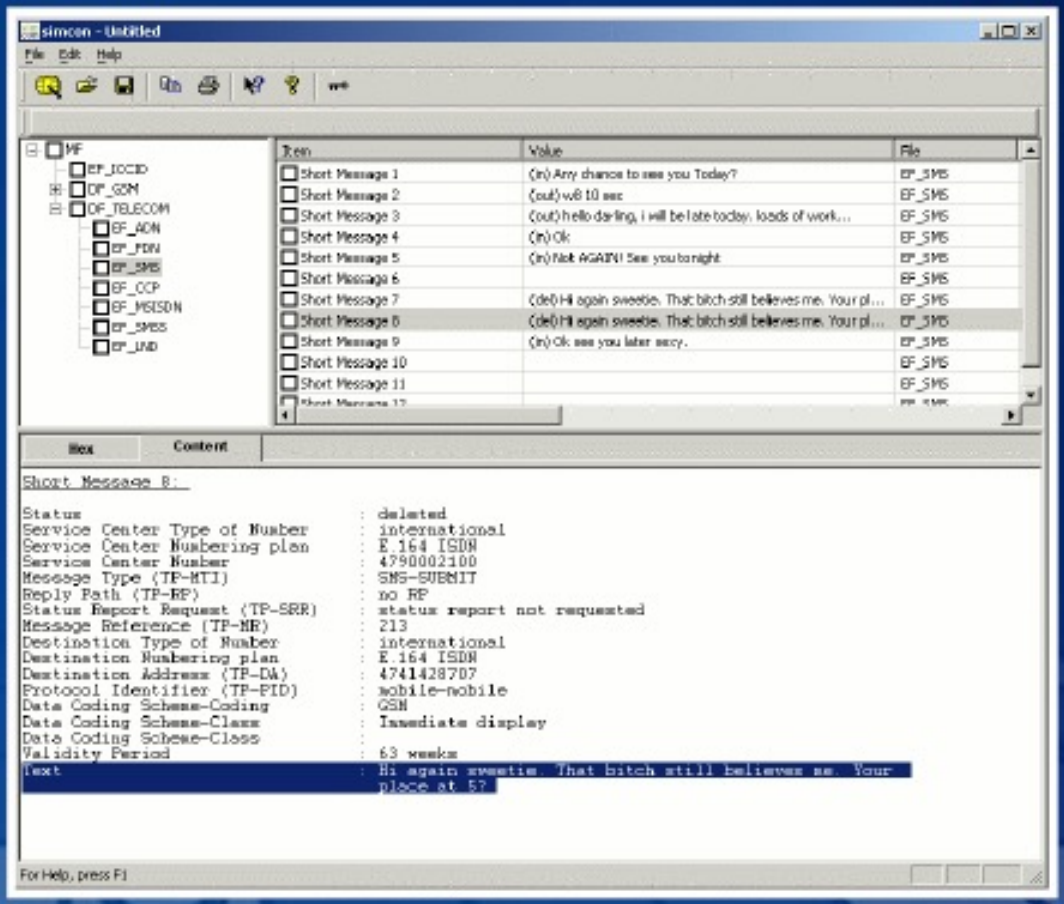
It recovers:

- **Last** Number Dialed, **Abbreviated** Dialing Numbers
- Active and Deleted **text (SMS) messages**
- All the general files found in the Telecom group as **defined in the GSM 11.11v6 standards**



SIMCon

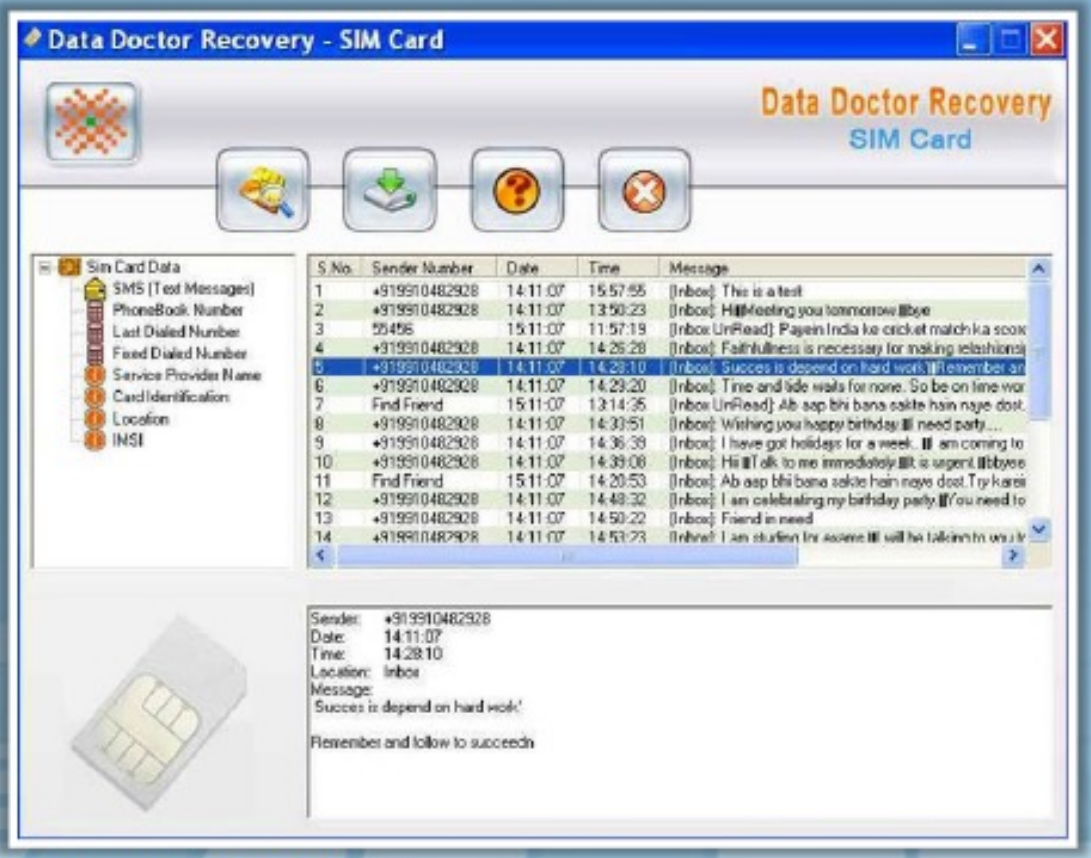
- SIMCon is a program that allows the user to **securely image all files** on a GSM/3G SIM card to a computer file with the SIMCon forensic SIM card reader
- It recovers deleted text **messages stored on the card** but not readable on phones



http://www.simcon.no

SIM Card Data Recovery

- SIM Card Data Recovery software recovers accidentally deleted data from mobile phone SIM cards



Features

- Recovers all SIM card details missing due to accidental data deletion, human fault, and software or hardware malfunction
- Displays SIM card IMSI number, ICC Mobile Identification number, and Service provider name
- Supports all PC/SC standards or Phoenix standard SIM card reader used to connect the SIM card with the computer

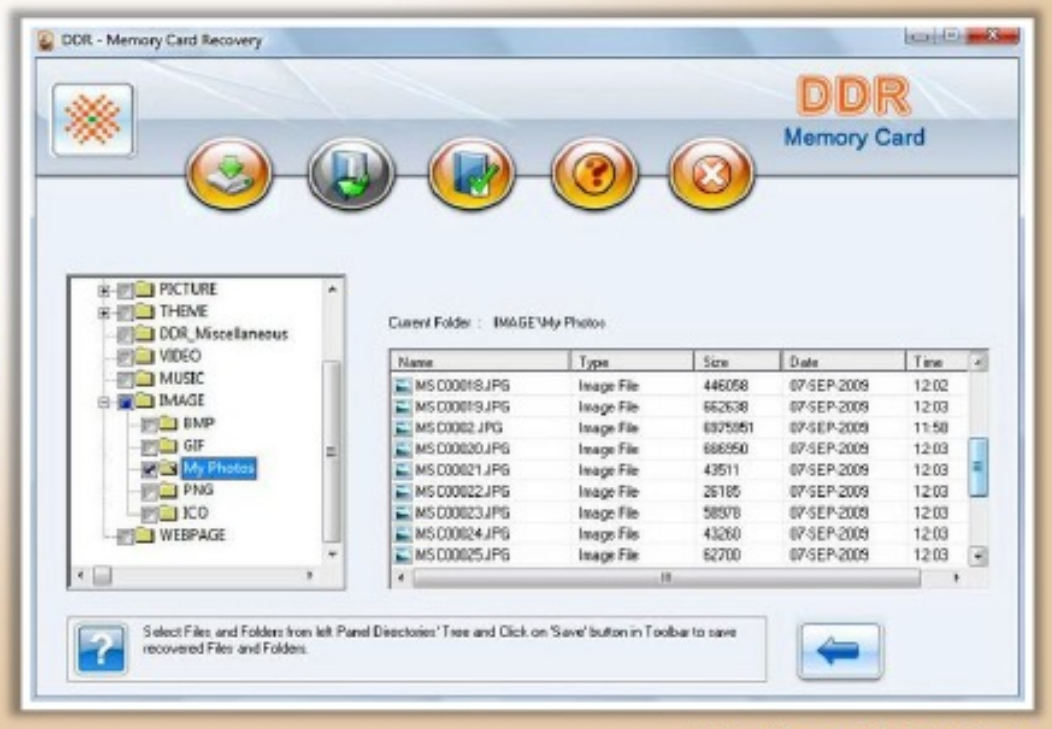
http://www.datadoctor.in

Memory Card Data Recovery

Memory Card Data Recovery recovers deleted pictures, lost images/photos, formatted audio/video files and folders, and encrypted data from the corrupted memory card storage devices

Features

- Retrieves deleted, erased or missing files and information from corrupted or damaged memory cards
- Supports easy recovery of all media files including image files, video files, audio files, text files, etc.
- Supports all USB memory card storage media devices including Compact Flash Memory card, Secure Digital SD, Multimedia Card, xD Picture card, Memory Stick, and other commonly used memory card storage media



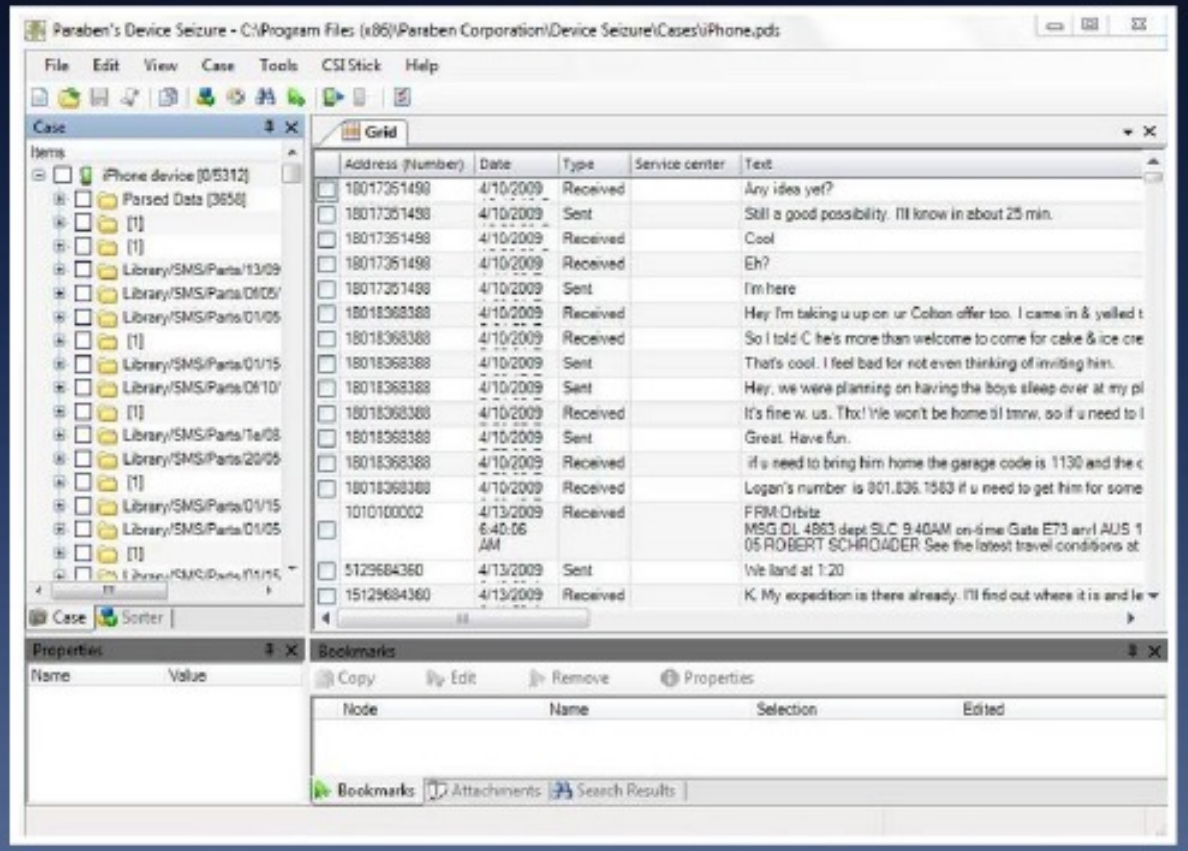
http://www.datadoctor.in

Device Seizure

Device Seizure is a **forensic acquisition and analysis tool** for examining cell phones, PDAs, and GPS devices

Features:

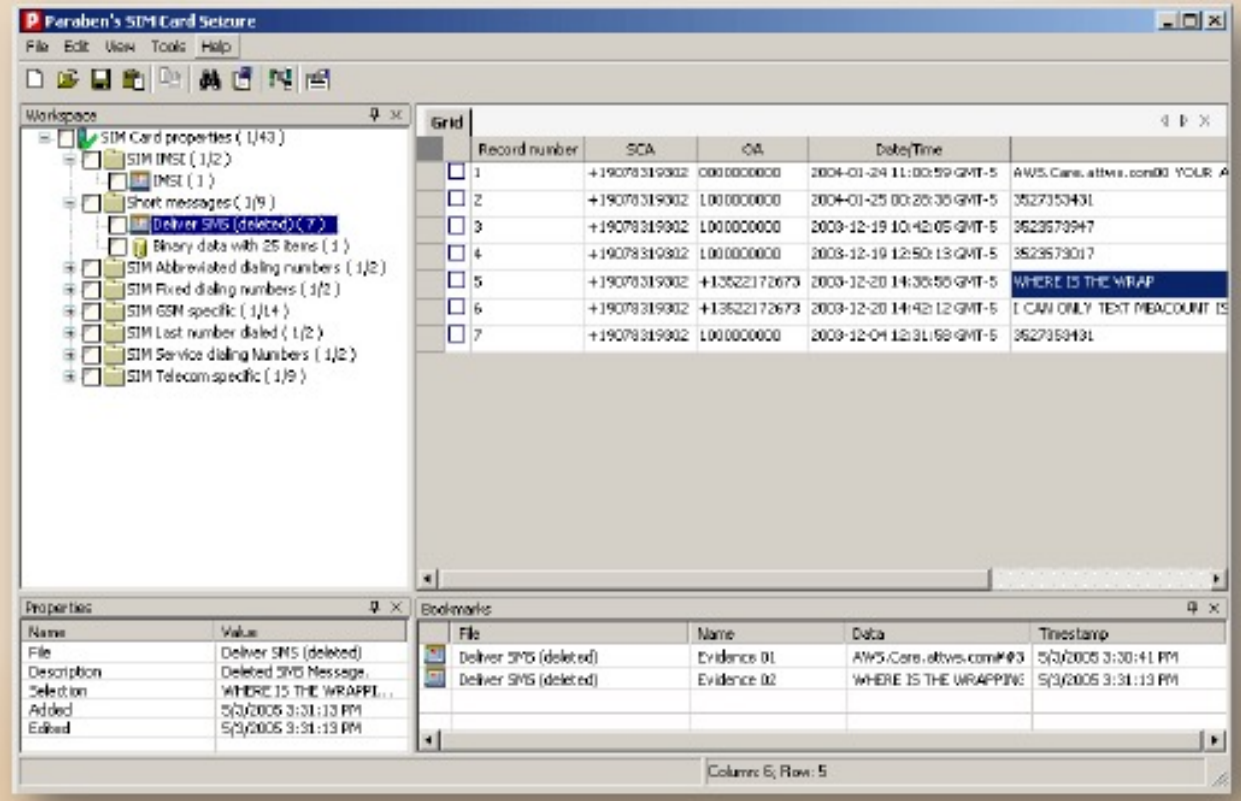
- **Support of more than 1,900 devices**
- **Verification of file integrity using MD5 and SHA1 hash values**
- **Image viewing for graphic information, including data carving for multi-media files for most devices**



http://www.paraben.com

SIM Card Seizure

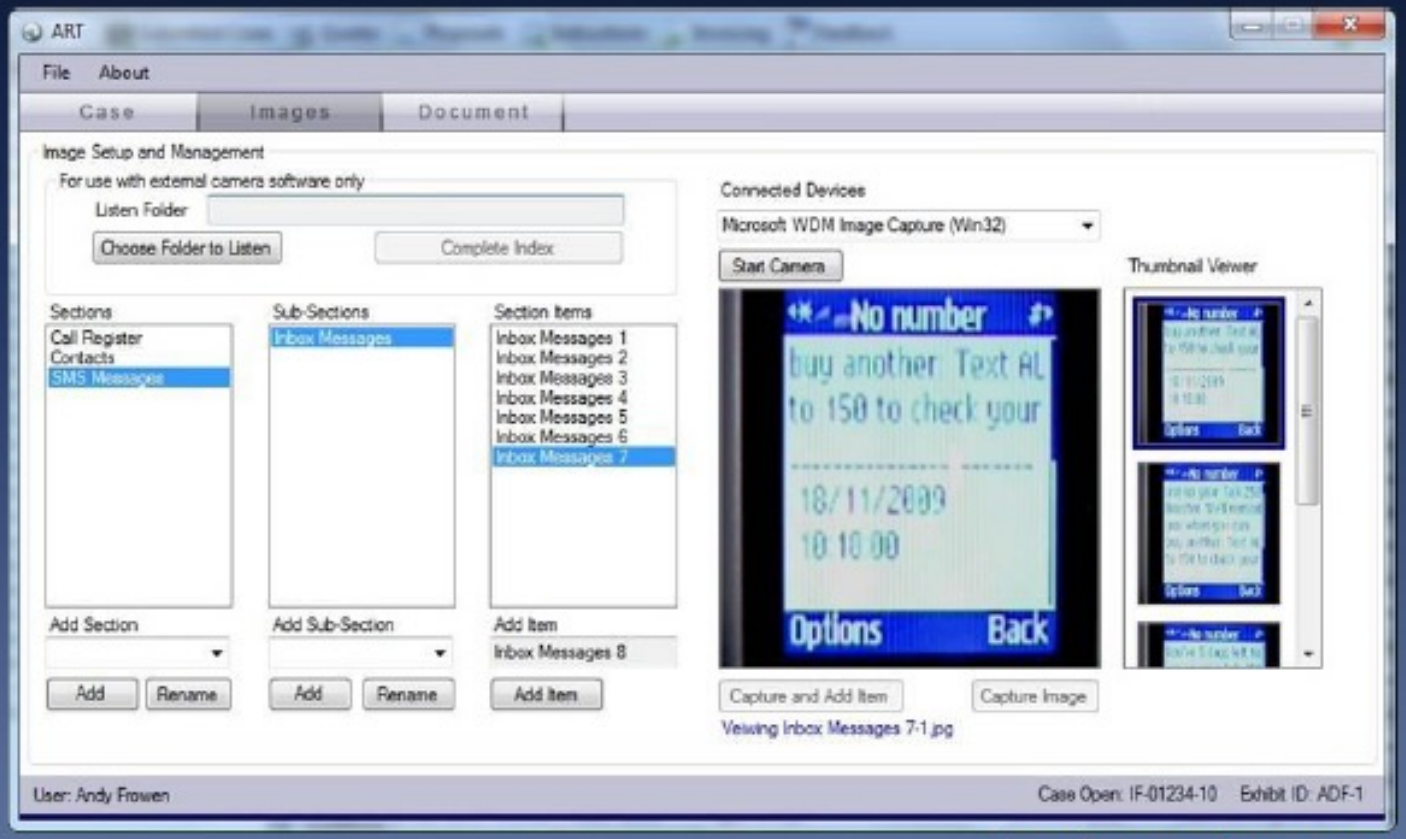
SIM Card Seizure recovers deleted SMS/text messages and performs comprehensive analysis of SIM card data



http://www.paraben.com

ART (Automatic Reporting Tool)

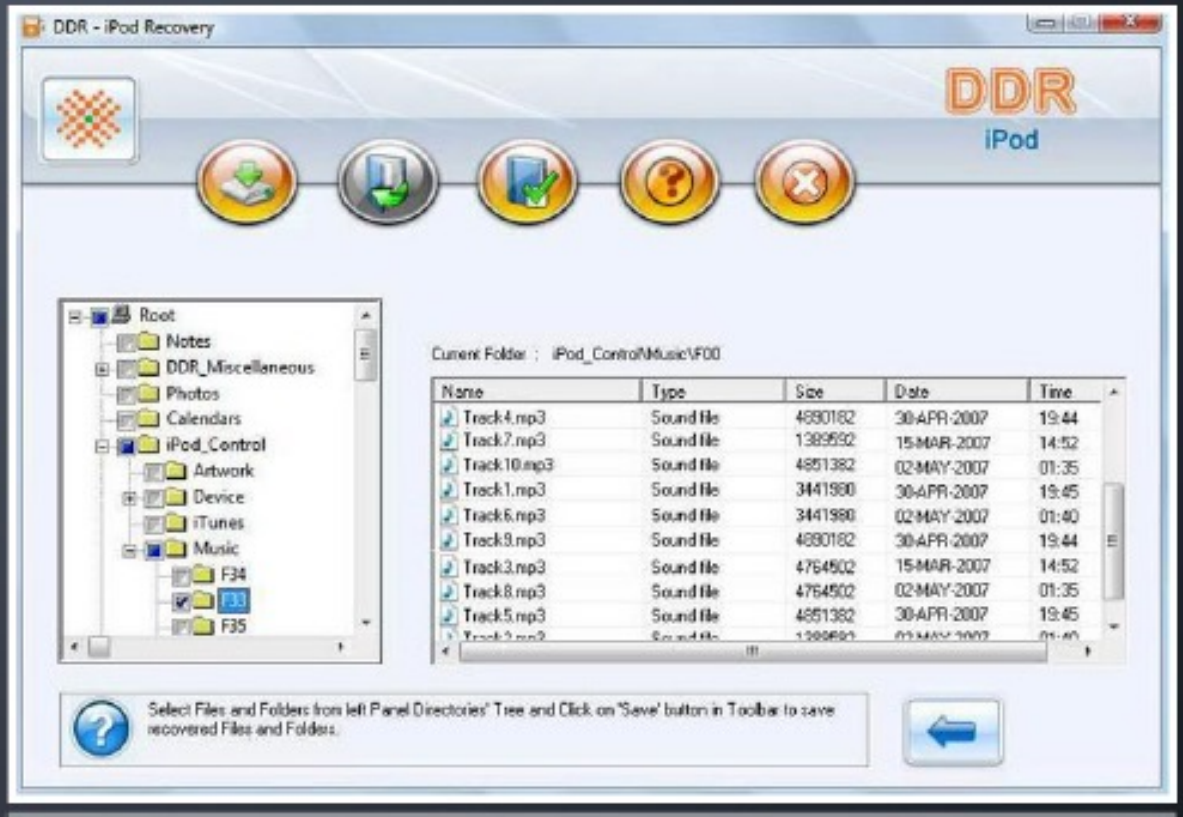
ART (Automatic Reporting Tool) is a software application developed to help Mobile Phone Forensic examiners to **capture images (via a USB camera) of mobile devices** and subsequently **produce a Microsoft Word document**



http://www.intaforensics.com

iPod Data Recovery Software

- iPod data recovery software easily **retrieves all lost deleted music files** from iPod digital media player
- It supports all **iPod models,** including iPod Classic, iPod Touch, iPod Mini, iPod Shuffle and other popular iPod audio-video models



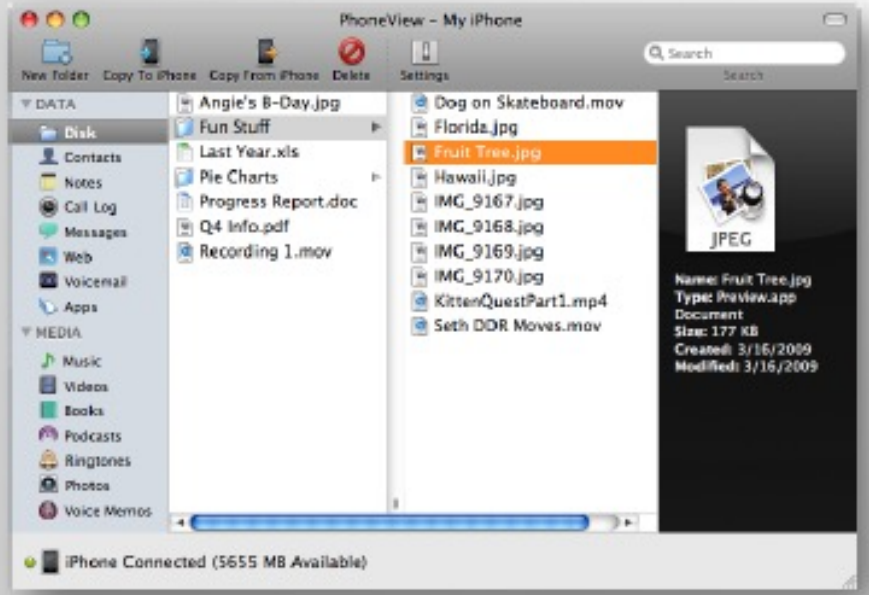
Recover My iPod

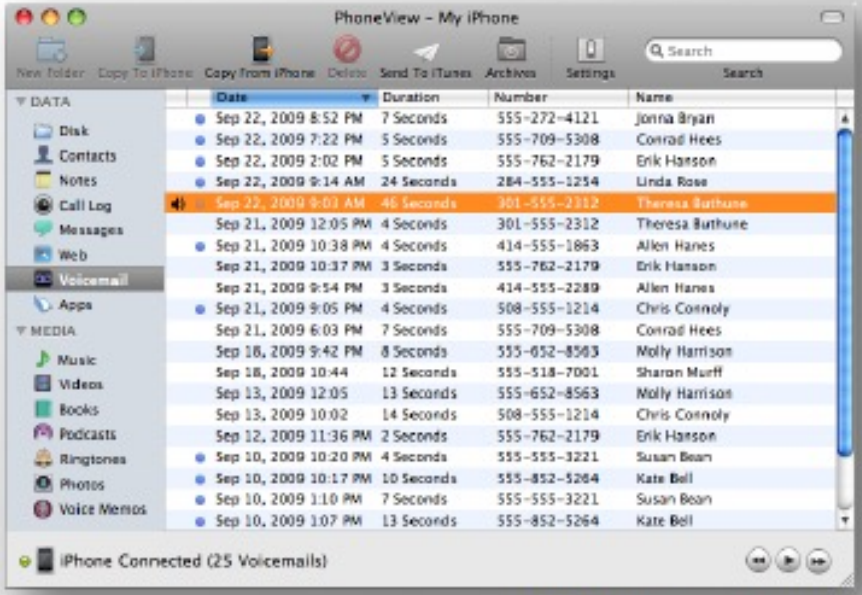
- Recover My iPod is iPod music recovery software to recover deleted or lost iPod files
- It recovers data after an iPod Reset or Restore
- It recovers data when an iPod gives a "Drive Not Formatted" message, or when an iPod is not recognized by a computer

http://www.recovermyipod.com

PhoneView

- PhoneView provides access to an iPhone's media, photos, notes, SMS messages, call history and contacts
- It automatically backs up messages from an iPhone and exports them as PDF, text, or XML files

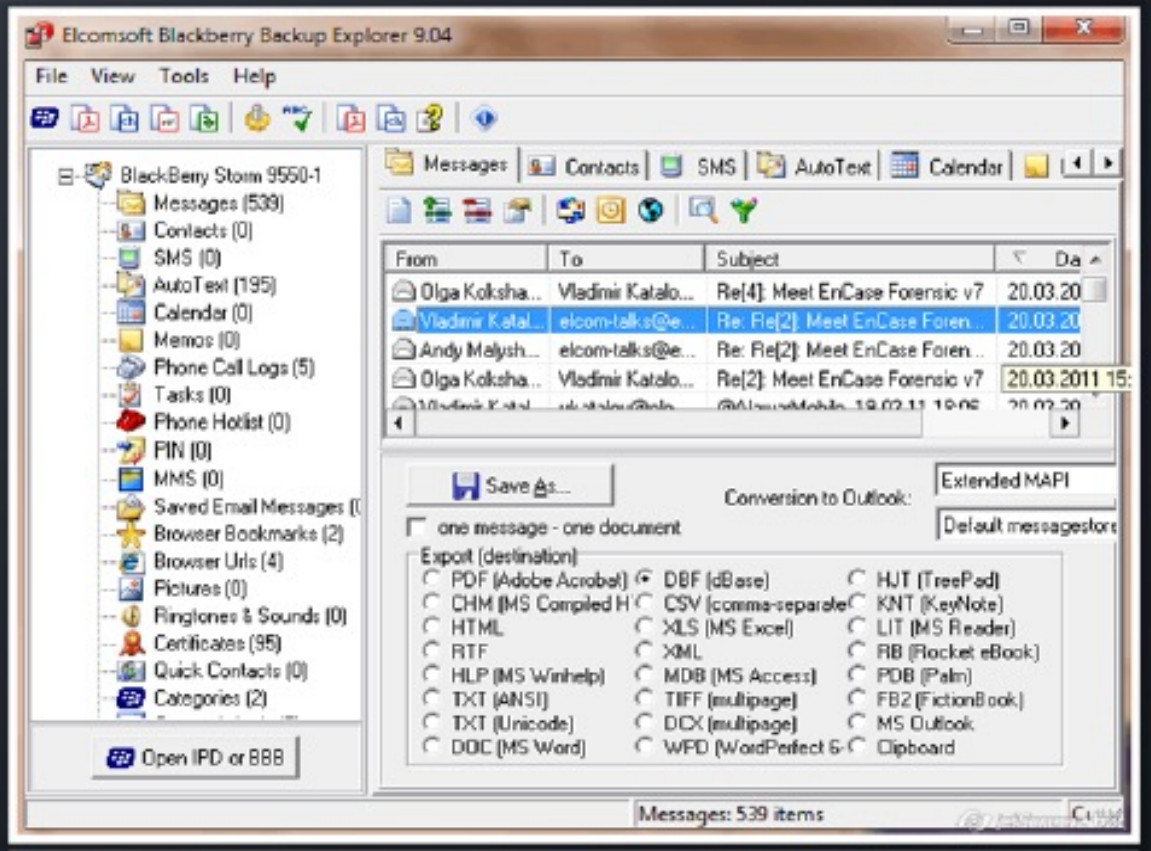




http://www.ecamm.com

Elcomsoft Blackberry Backup Explorer

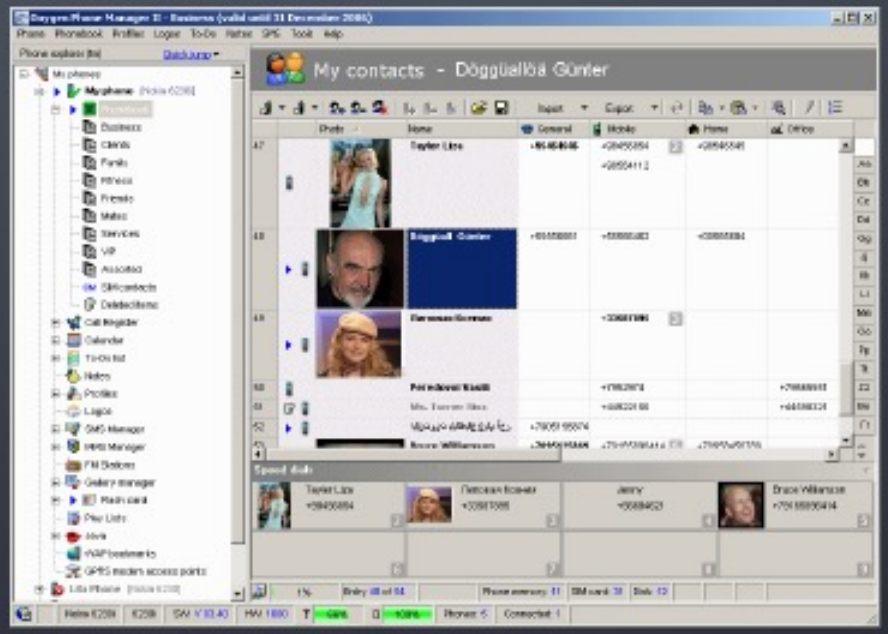
- Elcomsoft Blackberry Backup Explorer assists **forensic specialists investigating the content of BlackBerry** devices by extracting, analyzing, printing or exporting the content of a BlackBerry backup produced with BlackBerry Desktop Software
- It supports a variety of **exporting options and formats** including PDF and HTML

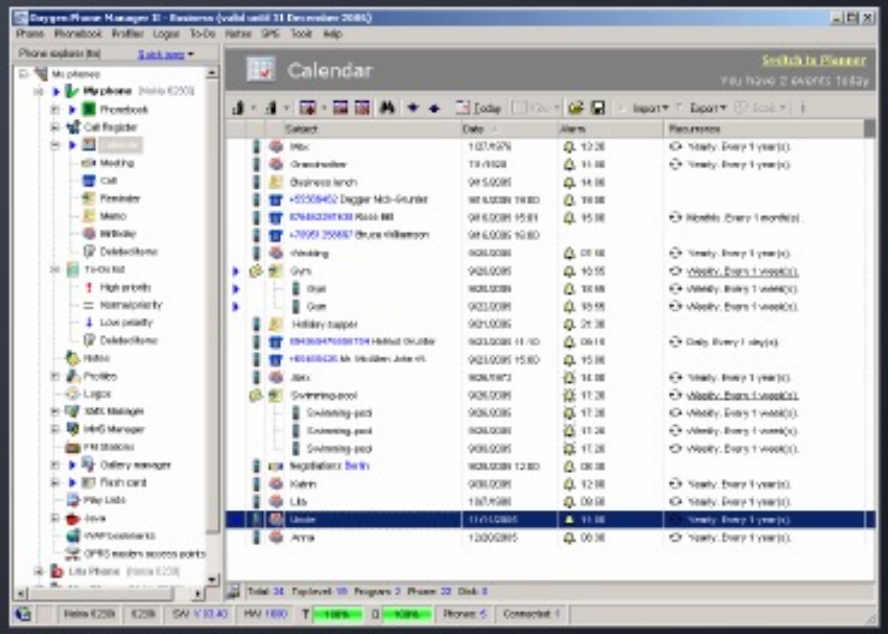


http://www.elcomsoft.com

Oxygen Phone Manager II

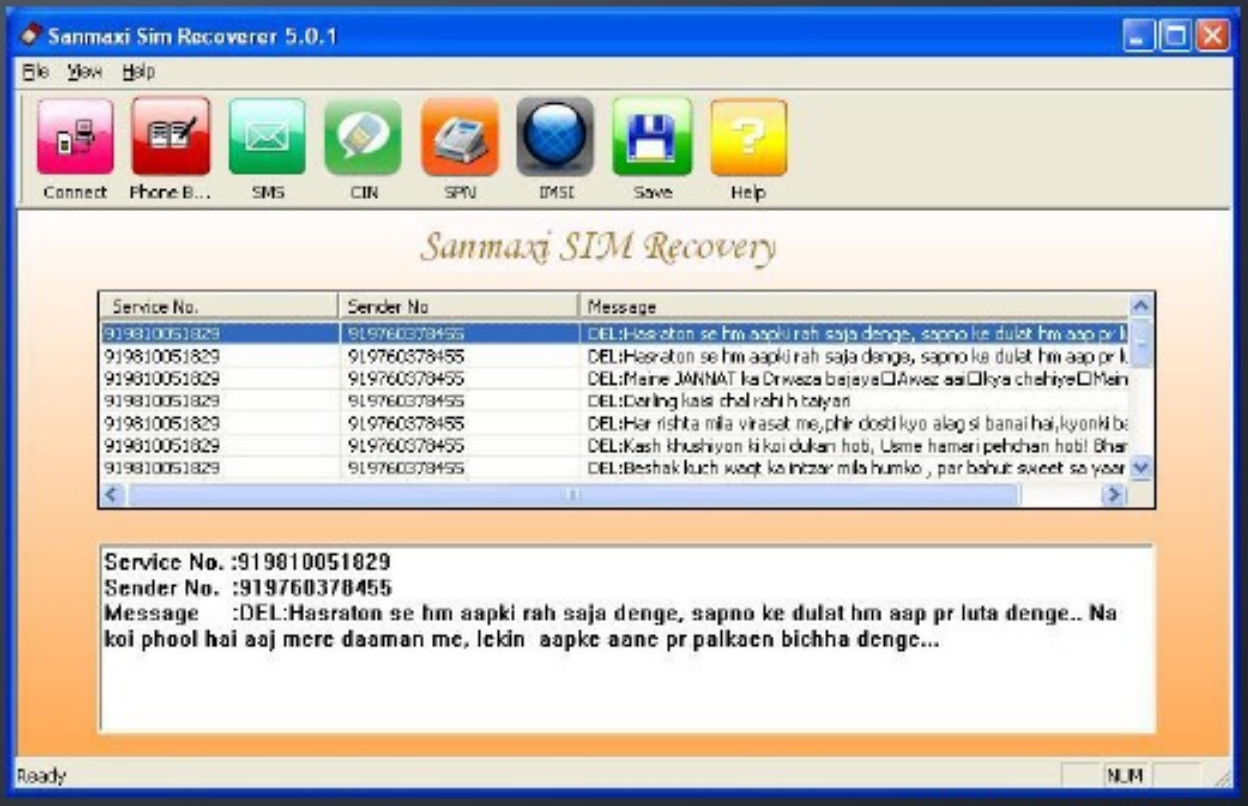
- Oxygen Phone Manager II for Nokia phones provides a simple and convenient way to control mobile phones from a PC
- It imports and exports data from Windows Address Book and CSV files and saves data in various formats: MS Excel, MS Word, HTML, XML, etc.





Sanmaxi SIM Recoverer

- Sanmaxi SIM Recoverer recovers and restores deleted inbox, outbox or SMS messages from your mobile cell phone
- It can recover recently deleted text SMS messages and contacts



http://www.sanmaxi.com

Mobile Forensics Tools

USIMdetective
http://quantaq.opiah.com

CardRecovery
http://www.cardrecovery.com

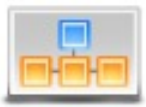
Stellar Phoenix iPod Recovery Software
http://www.stellarinfo.com

iCare Data Recovery Software
http://www.icare-recovery.com

Cell Phone Analyzer
http://www.bkforensics.com

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

BlackBerry Database Viewer Plus
http://www.cellica.com



BlackBerry Signing Authority Tool
http://us.blackberry.com

Module Flow

Mobile Phones

Mobile Operating Systems

Mobile Forensics

Mobile Forensics Process

Mobile Forensics Software Tools

Mobile Forensics Hardware Tools

Secure View Kit

- Secure View for Forensics is a software and hardware solution that provides logical data extraction of the content stored in a mobile phone
- It acquires cell phone data via USB, Bluetooth, IrDA, and SIM card reader

It acquires:

- Serial numbers: IMEI (for GSM phones), and ESN (for CDMA) phones
- Recent calls: Received calls, dialed calls & missed calls
- Contacts (internal phone memory, as well as SIM card on supported GSM phones)
- Calendar and to do lists
- Pictures and wallpapers
- Ring tones and music
- Video and movies

http://www.datapilot.com

Deployable Device Seizure (DDS)

- Deployable Device Seizure (DDS) is a version of Device Seizure designed for use in the field
- It is integrated into a tablet PC and is designed for one-click acquisitions of basic cell phone data such as call logs, address books, SMS messages, etc.

http://www.paraben.com

Paraben's Mobile Field Kit

http://www.paraben.com

- Paraben's Mobile Field Kit is a **portable handheld forensic solution** that includes everything investigators need to perform a **comprehensive digital forensic analysis** of over 4,000 cell phones
- Features:
  - Performs **comprehensive analysis** to acquire data
  - Examines various types of media such as **USB drives and SD Cards**
  - **Recovers deleted data** with physical acquisitions
  - Searches for **illicit images and chat logs** on computers

PhoneBase

- PhoneBase extracts data from any standard SIM card using a SIM Card Reader
- It recovers the contents of SIM cards and phone memories, including lists of phone numbers and associated names, recently made calls, and text messages

http://www.phonebase.info

XACT System

http://www.forensicpeople.com

- XACT enables you to perform "physical" **data investigations** of confiscated phones and allows **recovery of deleted information**
- It allows you to **acquire data** from locked phones and **deleted information**
- It **recovers deleted SMS** recovered from the SIM card and other information

Logicube CellDEK

- CellDEK is a **portable handset data extraction kit** designed for use at the scene of a crime and all working environments associated with ongoing investigations
- It can **access, read, and copy stored data** from GSM, CDMA, TDMA, iDen handsets, SIM cards, PDAs, and 15 types of flash cards

Features

- **Extracts handset time and date**, serial numbers (IMEI, IMSI), dialed calls, missed calls, received calls, phonebook (both handset and SIM), SMS (both handset and SIM), deleted SMS from SIM, calendar, memos, and to do lists
- **Built-in SIM card reader** and SIM card-reading software
- **Connection and control** of external jammer to prevent loss of data
- Time-stamped forensic audit trail records data sent and received from target device

http://www.logicubeforensics.com

Logicube CellDEK TEK

The CellDEK® TEK is designed for the technically experienced forensic investigator who requires a comprehensive, compact and portable data extraction hardware solution for mobile devices

It is compatible with 2000 of the most popular cell phones and PDAs, including Blackberry devices

It extracts data from Apple iPhone, iPhone 3G, and iPod touch devices as well as Garmin, TomTom, and iPAQ satellite navigation devices

http://www.logicubeforensics.com

RadioTactics ACESO

- RadioTactics ACESO recovers digital evidence from mobile phones, SIM cards and media cards
- It allows investigators to examine and interrogate phones and other mobile devices, quickly and accurately

http://www.radio-tactics.com

Features:

- Provides critical details, including time and date, geotagging and make and model of device used
- Safely block network access using the patent pending Handset Access Card
- Capture data from devices such as sat navs and flash media

UME-36Pro - Universal Memory Exchanger

Cellebrite's UME-36Pro is a phone memory transfer and backup solution

Supports transfer of content across all mobile handset technologies

Transfer of phones' internal memory and SIM card content with integrated SIM/Smart Card reader

Transfer, backup, and restoration of mobile phone content

http://www.cellebrite.com

Cellebrite UFED System - Universal Forensic Extraction Device

Using OpenSSH you can tunnel all of the traffic from your local box to a remote box that you have an account on

http://www.cellebrite.com

- It extracts data from all cell phones: phonebooks, pictures, videos, text messages, call logs, ESN and IMEI information
- It is a standalone kit, with no computer required for extraction
- It generates complete, MD5 verified evidence reports
- It supports over 1,400 handset models

ZRT 2

- ZRT 2 is a **cell phone forensic investigation solution that supports all phones** and can be used on its own or in conjunction with existing tools

Features:

- It completely streamlines the process of taking **high-resolution photographs** of screen displays
- It **merges photos** into custom designed report templates

http://www.fernico.com

ICD 5200

- Paraben's Project-A-PhoneTM ICD-5200 is a cell phone screen capture device that **allows you to take pictures or videos** of the screen of almost any cell phone and display them right on your computer
- It **captures the display screen** at up to 5.2 megapixel resolution

Features:

- It captures **evidence** in cell phone forensics
- It assists at **live meetings** where you want to present from a computer
- It provides **web-based** demonstrations
- It can take **screen shots** for print marketing materials or documentation

http://www.projectaphone.com

ICD 1300

http://www.projectaphone.com

- ICD 1300 is a Project-a-Phone product designed for forensic investigations of cell phones
- It captures the display screen at up to 1.3 megapixel resolution

Features:

- It records forensic evidence
- If offers screenshots for digital marketing materials or documentation

Module Summary

- A mobile phone or cellular phone is an electronic device used for mobile voice or data communication over a network
- A mobile operating system is an operating system that operates a mobile device like a mobile phone, smart phone, PDA, etc.
- Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions
- Collect and preserve all the electronic devices found at the crime scene
- The data acquisition process at the crime scene is hampered due to the lack of controlled settings, appropriate equipment, and other prerequisites
- Mobile Forensic software collects all possible data from a mobile phone and generates an extensive forensics report

"This phone has a special voice filter. It makes you sound honest when you discuss business, sincere when you apologize, and terminal when you call in sick."