UNIT V

ANALYSIS AND VALIDATION

Validating Forensics Data -Data Hiding Techniques - Performing Remote Acquisition – Network Forensics -Email Investigations - Cell Phone and Mobile Devices Forensics

Part-A

1. **Define bit-shifting**
   - ✓ The process of shifting one or more digits in a binary number to the left or right to produce a different value. key escrow A technology designed to recover encrypted data if users forget their passphrases or if the user key is corrupted after a system failure.
2. **Define Known File Filter (KFF).**
   - ✓ A database containing the hash values of known legitimate and suspicious files. It's used to identify files for evidence or eliminate them from the investigation if they are legitimate files. scope creep The result of an investigation expanding beyond its original description because the discovery of unexpected evidence increases the amount of work required.
3. **Define steganography.**
   - ✓ A cryptographic technique for embedding information in another file for the purpose of hiding that information from casual observers.
4. **Define network forensics.**
   - ✓ The process of collecting and analyzing raw network data and systematically tracking network traffic to determine how security incidents occur.
5. **Define client/server architecture.**
   - ✓ A network architecture in which each computer or process on the network is a client or server. Clients request services from a server, and a server processes requests from clients.
6. **Define Enhanced Simple Mail Transfer Protocol (ESMTP)** .
   - ✓ An enhancement of SMTP for sending and receiving e-mail messages. ESMTP generates a unique, non repeatable number that's added to a transmitted e-mail. No two messages transmitted from an e-mail server have the same ESMTP value.
7. **Define Multipurpose Internet Mail Extensions (MIME)**

- ✓ A specification for formatting non-ASCII messages, such as graphics, audio, and video, for transmission over the Internet. phishing A type of e-mail scam that's typically sent as spam soliciting personal identity information that fraudsters can use for identity theft.

8. Define spoofing

- ✓ Transmitting an e-mail message with its header information altered so that its point of origin appears to be from a different sender. Spoofed e-mails are also referred to as forged e-mail. Spoofing is typically used in phishing and spamming to hide the sender's identity.

9.How to Validating with Computer Forensics Programs

- Commercial computer forensics programs have built-in validation features
- ProDiscover's .eve files contain metadata that includes the hash value
  - Validation is done automatically
- Raw format image files (.dd extension) don't contain metadata
  - So you must validate raw format image files manually to ensure the integrity of data
- In AccessData FTK Imager
  - When you select the Expert Witness (.e01) or the SMART (.s01) format
    - Additional options for validating the acquisition are displayed
  - Validation report lists MD5 and SHA-1 hash values

10.List out the Addressing Data-hiding Techniques

- File manipulation
  - Filenames and extensions
  - Hidden property
- Disk manipulation
  - Hidden partitions
  - Bad clusters
- Encryption
  - Bit shifting
  - Steganography

11. DefineCode Division Multiple Access (CDMA)

- ✓ A widely used digital cell phone technology that makes use of spread-spectrum modulation to spread the signal across a wide range of frequencies.

12. Define Electronically erasable programmable read-only memory (EEPROM)

- ✓ A type of nonvolatile memory that can be reprogrammed electrically, without having to physically access or remove the chip.

13. Define fourth-generation (4G)

- ✓ The next generation of mobile phone standards and technologies promises higher speeds and improved accuracy. Sprint Nextel introduced 4G in 2009, and other major carriers intend to follow suit between now and 2012.

14. Define Global System for Mobile Communications (GSM)

- ✓ A second-generation cellular network standard; currently the most popular cellular network type in the world.

15. Define Orthogonal Frequency Division Multiplexing (OFDM)

- ✓ A 4G technology that uses radio waves broadcast over different frequencies; it's considered to use power more efficiently and be more immune to interference.

16. How to Exploring the Role of E-mail in Investigations

- With the increase in e-mail scams and fraud attempts with phishing or spoofing
  - Investigators need to know how to examine and interpret the unique content of e-mail messages
- Phishing e-mails are in HTML format
  - Which allows creating links to text on a Web page
- One of the most noteworthy e-mail scams was 419, or the Nigerian Scam
- Spoofing e-mail can be used to commit fraud

17. How to Exploring the Roles of the Client and Server in E-mail

- Send and receive e-mail in two environments
  - Internet
  - Controlled LAN, MAN, or WAN
- Client/server architecture
  - Server OS and e-mail software differs from those on the client side
- Protected accounts
  - Require usernames and passwords

18. List out E-Mail Headers.

- Learn how to find e-mail headers
  - GUI clients
  - Command-line clients

  - Web-based clients
- After you open e-mail headers, copy and paste them into a text document
- Headers contain useful information
- Outlook
- Outlook Express
- Pine and ELM
- AOL headers
- Hotmail
- Apple Mail

19. List out the E-mail Forensics Tools

- Tools include:
  - AccessData's Forensic Toolkit (FTK)
  - ProDiscover Basic
  - FINALeMAIL
  - Sawmill-GroupWise
  - DBXtract
  - Fookes Aid4Mail and MailBag Assistant
  - Paraben E-Mail Examiner
  - Ontrack Easy Recovery EmailRepair
  - R-Tools R-Mail
- Tools allow you to find:
  - E-mail database files
  - Personal e-mail files
  - Offline storage files
  - Log files

20.Define SIM Card Readers

- ✓ **SIM Card Readers** With GSM phones and many newer models of mobile devices, the next step is accessing the SIM card, which you can do by using a combination hardware/ software device called a SIM card reader.
- ✓ The general procedure is as follows:
  1. Remove the back panel of the device.
  2. Remove the battery.
  3. Under the battery, remove the SIM card from its holder.

4. Insert the SIM card into the card reader, which you insert into your forensic workstation's USB port.

Part-B

1. Determine what data to analyze in a computer forensics investigation.

Determining What Data to Collect and Analyze

- Examining and analyzing digital evidence depends on:
  - Nature of the case
  - Amount of data to process
  - Search warrants and court orders
  - Company policies
- Scope creep
  - Investigation expands beyond the original description
- Right of full discovery of digital evidence

Approaching Computer Forensics Cases

- Some basic principles apply to almost all computer forensics cases
  - The approach you take depends largely on the specific type of case you're investigating
- Basic steps for all computer forensics investigations
  - For target drives, use only recently wiped media that have been reformatted
    - And inspected for computer viruses
- Basic steps for all computer forensics investigations (continued)
  - Inventory the hardware on the suspect's computer and note the condition of the computer when seized
  - Remove the original drive from the computer
    - Check date and time values in the system's CMOS
  - Record how you acquired data from the suspect drive
  - Process the data methodically and logically
- Basic steps for all computer forensics investigations (continued)
  - List all folders and files on the image or drive
  - If possible, examine the contents of all data files in all folders
    - Starting at the root directory of the volume partition
  - For all password-protected files that might be related to the investigation
    - Make your best effort to recover file contents

- Basic steps for all computer forensics investigations (continued)
  - Identify the function of every executable (binary or .exe) file that doesn't match known hash values
  - Maintain control of all evidence and findings, and document everything as you progress through your examination

Refining and Modifying the Investigation Plan

- Considerations
  - Determine the scope of the investigation
  - Determine what the case requires
  - Whether you should collect all information
  - What to do in case of scope creep
- The key is to start with a plan but remain flexible in the face of new evidence

Using AccessData Forensic Toolkit to Analyze Data

- Supported file systems: FAT12/16/32, NTFS, Ext2fs, and Ext3fs
- FTK can analyze data from several sources, including image files from other vendors
- FTK produces a case log file
- Searching for keywords
  - Indexed search
  - Live search
  - Supports options and advanced searching techniques, such as stemming

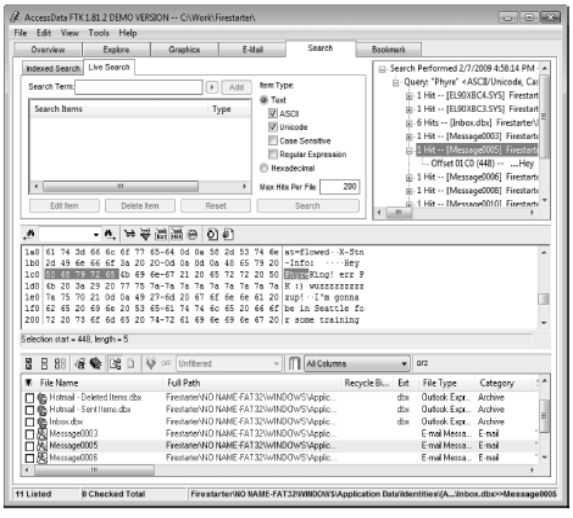


Figure 9-1 Viewing live search results in FTK

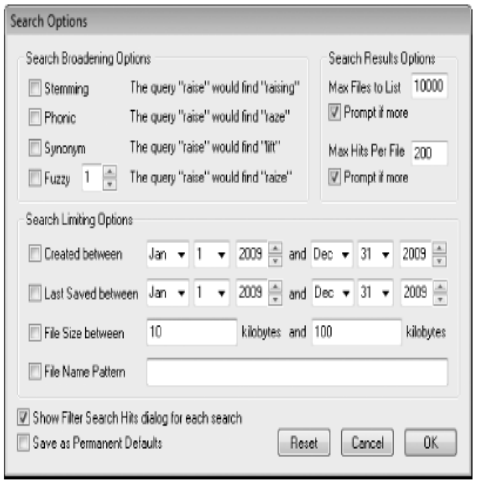


Figure 9-2 Selecting search options in FTK

- Analyzes compressed files

- You can generate reports
  - Using bookmarks

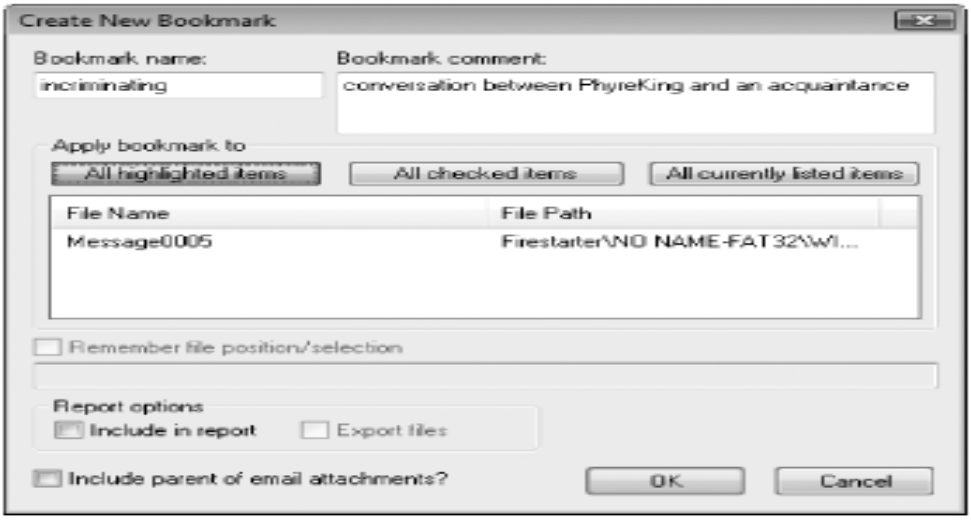


Figure 9-3 Creating a bookmark

2.Explain tools used to validate data.

Validating Forensic Data

- One of the most critical aspects of computer forensics
- Ensuring the integrity of data you collect is essential for presenting evidence in court
- Most computer forensic tools provide automated hashing of image files
- Computer forensics tools have some limitations in performing hashing
  - Learning how to use advanced hexadecimal editors is necessary to ensure data integrity

Validating with Hexadecimal Editors

- Advanced hexadecimal editors offer many features not available in computer forensics tools
  - Such as hashing specific files or sectors
- Hex Workshop provides several hashing algorithms
  - Such as MD5 and SHA-1
  - See Figures 9-4 through 9-6
- Hex Workshop also generates the hash value of selected data sets in a file or sector

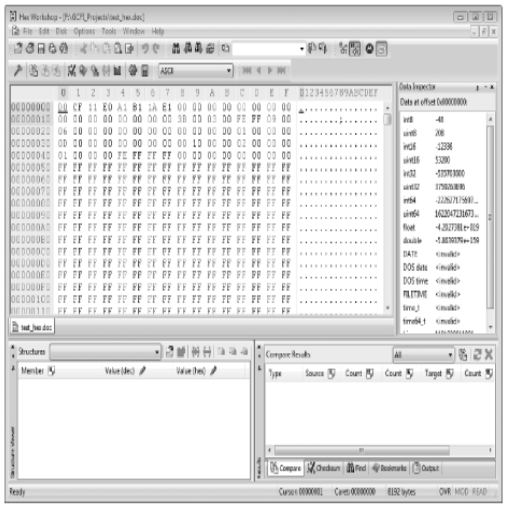


Figure 9-4 Viewing a file opened in Hex Workshop

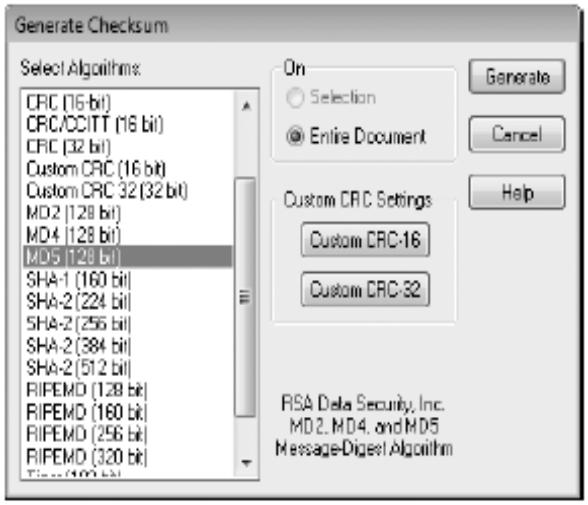


Figure 9-5 The Generate Checksum dialog box

- Using hash values to discriminate data
  - AccessData has a separate database, the **Known File Filter (KFF)**
    - Filters known program files from view, such as MSWord.exe, and identifies known illegal files, such as child pornography
  - KFF compares known file hash values to files on your evidence drive or image files
  - Periodically, AccessData updates these known file hash values and posts an updated KFF

Validating with Computer Forensics Programs

- Commercial computer forensics programs have built-in validation features
- ProDiscover's .eve files contain metadata that includes the hash value
  - Validation is done automatically
- Raw format image files (.dd extension) don't contain metadata
  - So you must validate raw format image files manually to ensure the integrity of data
- In AccessData FTK Imager
  - When you select the Expert Witness (.e01) or the SMART (.s01) format
    - Additional options for validating the acquisition are displayed
  - Validation report lists MD5 and SHA-1 hash values

3.Explain common data-hiding techniques.

Data hiding involves changing or manipulating a file to conceal information. Data-hiding techniques include hiding entire partitions, changing file extensions, setting file attributes to hidden, bit-shifting, using encryption, and setting up password protection.

Addressing Data-hiding Techniques

- File manipulation
  - Filenames and extensions
  - Hidden property
- Disk manipulation
  - Hidden partitions
  - Bad clusters
- Encryption
  - Bit shifting
  - Steganography

Hiding Partitions

- Delete references to a partition using a disk editor
  - Re-create links for accessing it
- Use disk-partitioning utilities
  - GDisk
  - PartitionMagic
  - System Commander
  - LILO
- Account for all disk space when analyzing a disk

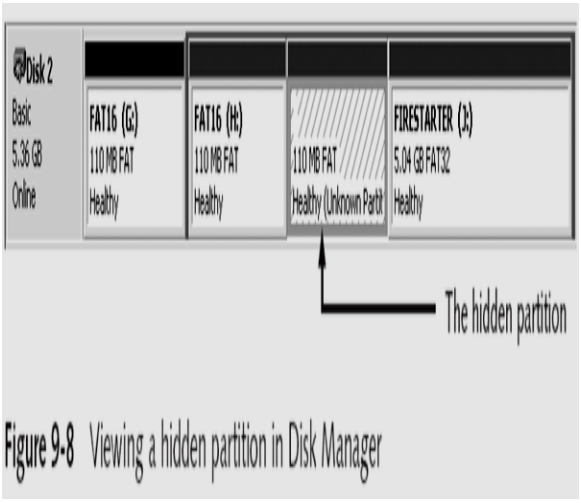


Figure 9-8 Viewing a hidden partition in Disk Manager

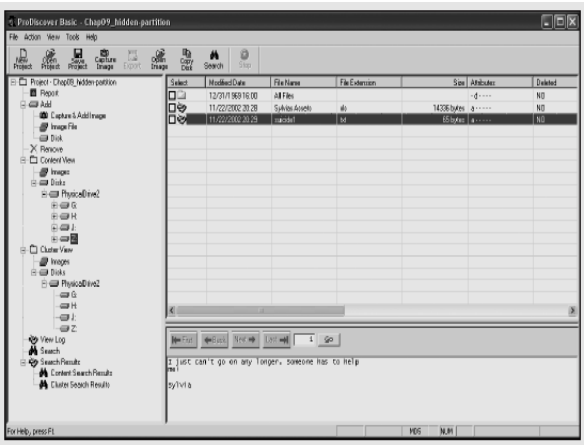


Figure 9-9 Viewing a hidden partition in ProDiscover

Marking Bad Clusters

- Common with FAT systems
- Place sensitive information on free space
- Use a disk editor to mark space as a bad cluster
- To mark a good cluster as bad using Norton Disk Edit
  - Type B in the FAT entry corresponding to that cluster

Bit-shifting

- Old technique
- Shift bit patterns to alter byte values of data
- Make files look like binary executable code
- Tool
  - Hex Workshop

Using Steganography to Hide Data

- Greek for "hidden writing"
- **Steganography** tools were created to protect copyrighted material
  - By inserting digital watermarks into a file
- Suspect can hide information on image or text document files
  - Most steganography programs can insert only small amounts of data into a file
- Very hard to spot without prior knowledge
- Tools: S-Tools, DPEnvelope, jpgx, and tte

Examining Encrypted Files

- Prevent unauthorized access
  - Employ a password or passphrase
- Recovering data is difficult without password
  - **Key escrow**
    - Designed to recover encrypted data if users forget their passphrases or if the user key is corrupted after a system failure
  - Cracking password
    - Expert and powerful computers
  - Persuade suspect to reveal password

Recovering Passwords

- Techniques
  - Dictionary attack

  - Brute-force attack
  - Password guessing based on suspect's profile
- Tools
  - AccessData PRTK
  - Advanced Password Recovery Software Toolkit
  - John the Ripper
- Using AccessData tools with passworded and encrypted files
  - AccessData offers a tool called Password Recovery Toolkit (PRTK)
    - Can create possible password lists from many sources
  - Can create your own custom dictionary based on facts in the case
  - Can create a suspect profile and use biographical information to generate likely passwords
- Using AccessData tools with passworded and encrypted files (continued)
  - FTK can identify known encrypted files and those that seem to be encrypted
    - And export them
  - You can then import these files into PRTK and attempt to crack them

4.Describe methods of performing a remote acquisition.

Performing Remote Acquisitions

- Remote acquisitions are handy when you need to image the drive of a computer far away from your location
  - Or when you don't want a suspect to be aware of an ongoing investigation

Remote Acquisitions with Runtime Software

- Runtime Software offers the following shareware programs for remote acquisitions:
  - DiskExplorer for FAT
  - DiskExplorer for NTFS
  - HDHOST
- Preparing DiskExplorer and HDHOST for remote acquisitions
  - Requires the Runtime Software, a portable media device (USB thumb drive or floppy disk), and two networked computers
- Making a remote connection with DiskExplorer

- Requires running HDHOST on a suspect's computer
- To establish a connection with HDHOST, the suspect's computer must be:
    - Connected to the network
    - Powered on
    - Logged on to any user account with permission to run noninstalled applications
    - HDHOST can't be run surreptitiously

Figure 9-18 Displaying the contents of the HDHOST folder in Windows Exp

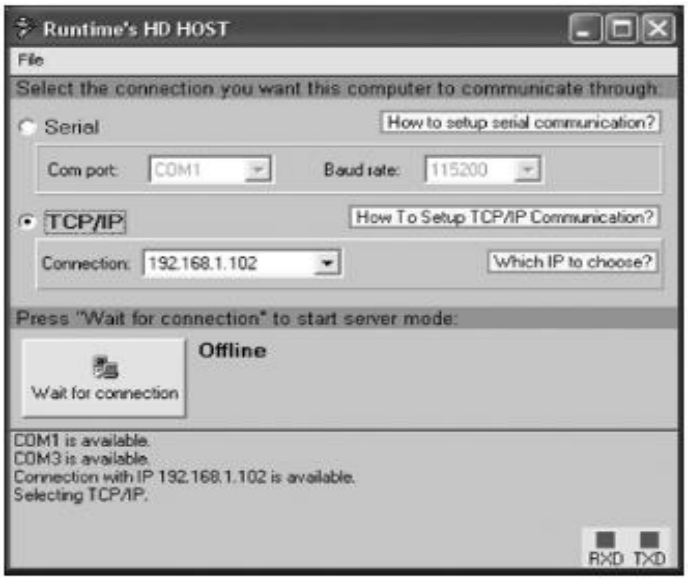


Figure 9-19 Selecting a connection type

- Making a remote acquisition with DiskExplorer
    - After you have established a connection with DiskExplorer from the acquisition workstation
        - You can navigate through the suspect computer's files and folders or copy data
    - The Runtime tools don't generate a hash for acquisitions

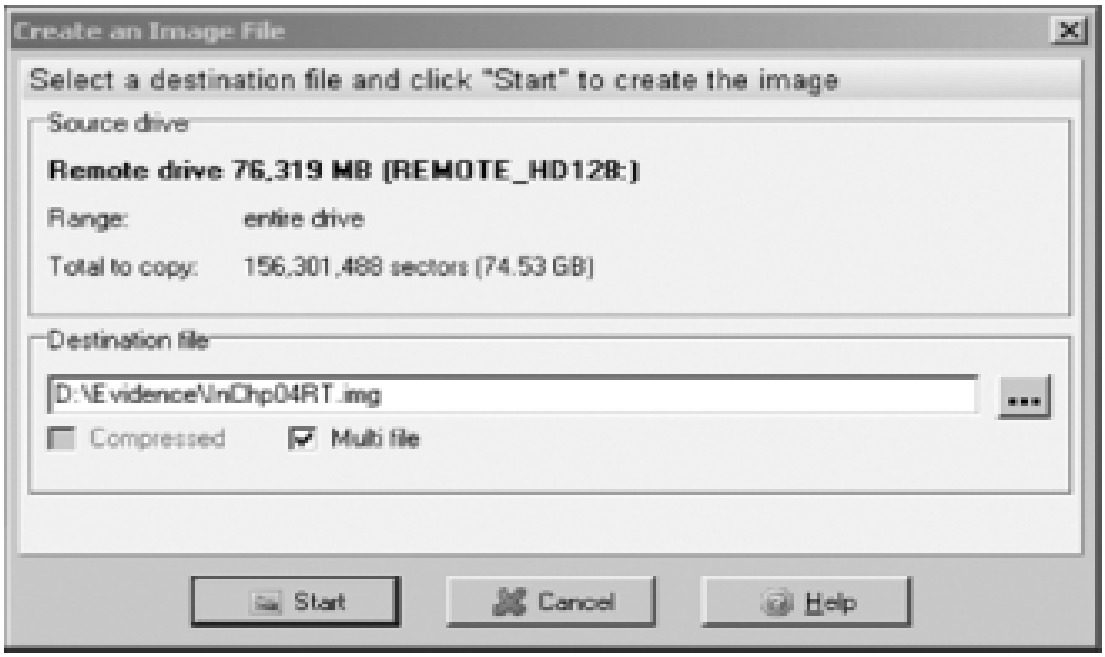


Figure 9-25 The Create an Image File dialog box

5. Explain in detail about the network forensics.

- Network forensics is the process of collecting and analyzing raw network data and tracking network traffic systematically to ascertain how an attack was carried out or how an event occurred on a network.
- Because network attacks are on the rise, there's more focus on this field and an increasing demand for skilled technicians.
- Labor forecasts predict a shortfall of 50,000 network forensics specialists in law enforcement, legal firms, corporations, and universities.
- When intruders break into a network, they leave a trail behind. Being able to spot variations in network traffic can help you track intrusions, so knowing your network's typical traffic patterns is important.
- *For example, the primary ISP in Windhoek, Namibia, has peak hours of use between 6 a.m. and 6 p.m. because most people in that city have Internet access only at work.*
- Network forensics can also help you determine whether a network is truly under attack or a user has inadvertently installed an untested patch or custom program, for example. A lot of time and resources can be wasted determining

that a bug in a custom program or an untested open-source program caused the "attack."

Securing a Network

- Network forensics is used to determine how a security breach occurred; however, steps must be taken to harden networks before a security breach happens, particularly with recent increases in network attacks, viruses, and other security incidents.
- Hardening includes a range of tasks, from applying the latest patches to using a layered network defense strategy, which sets up layers of protection to hide the most valuable data at the innermost part of the network.
- It also ensures that the deeper into the network an attacker gets, the more difficult access becomes and the more safeguards are in place.
- The National Security Agency (NSA) developed a similar approach, called the defense in depth (DiD) strategy. DiD has three modes of protection:

  • ***People***
  • ***Technology***
  • ***Operations***

If one mode of protection fails, the others can be used to thwart the attack. Listing people as a mode of protection means organizations must hire well-qualified people and treat them well so that they have no reason to seek revenge.

- In addition, organizations should make sure employees are trained adequately in security procedures and are familiar with the organization's security policy. Physical and personnel security measures are included in this mode of protection.

The technology mode includes choosing a strong network architecture and using tested tools, such as intrusion detection systems (IDSs) and firewalls. Regular penetration testing coupled with risk assessment can help improve network security, too. Having systems in place that allow quick and thorough analysis when a security breach occurs is also part of the technology mode of protection.

Finally, the operations mode addresses day-to-day operations. Updating security patches, antivirus software, and OSs falls into this category, as does assessment and monitoring procedures and disaster recovery plans.

6.Explain in detail about the E-mail investigation.

Explain the role of e-mail in investigations

Describe client and server roles in e-mail

Describe tasks in investigating e-mail crimes and violations

Explain the use of e-mail server logs

Describe some available e-mail computer forensics tools

Exploring the Role of E-mail in Investigations

- With the increase in e-mail scams and fraud attempts with phishing or spoofing
  - Investigators need to know how to examine and interpret the unique content of e-mail messages
- Phishing e-mails are in HTML format
  - Which allows creating links to text on a Web page
- One of the most noteworthy e-mail scams was 419, or the Nigerian Scam
- Spoofing e-mail can be used to commit fraud

Exploring the Roles of the Client and Server in E-mail

- Send and receive e-mail in two environments
  - Internet
  - Controlled LAN, MAN, or WAN
- Client/server architecture
  - Server OS and e-mail software differs from those on the client side
- Protected accounts
  - Require usernames and passwords

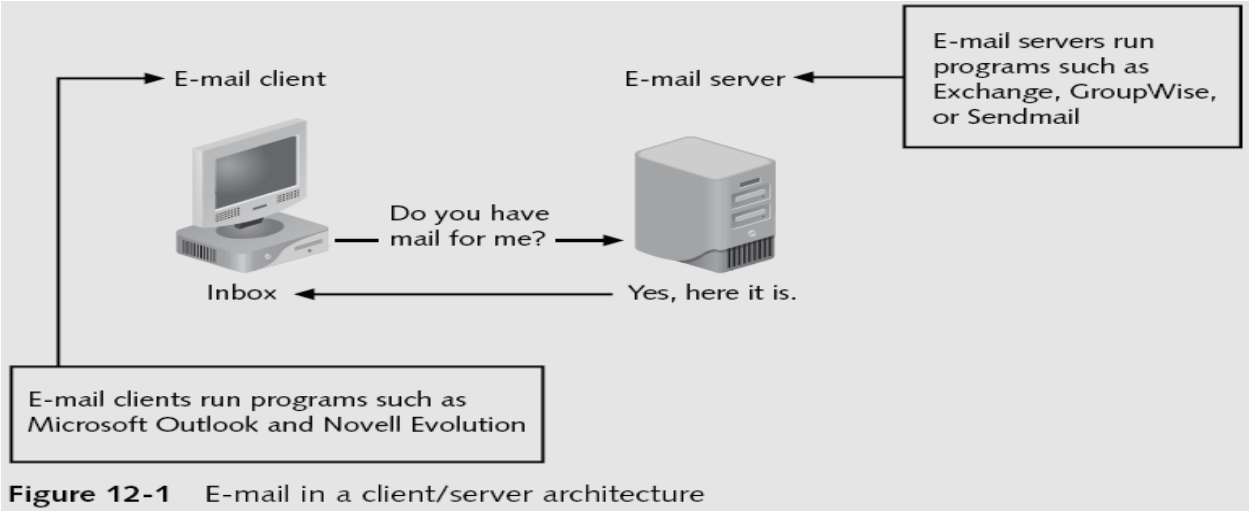


Figure 12-1 E-mail in a client/server architecture

- Name conventions
  - Corporate: john.smith@somecompany.com

  - Public: whatever@hotmail.com
  - Everything after @ belongs to the domain name
- Tracing corporate e-mails is easier
  - Because accounts use standard names the administrator establishes

Investigating E-mail Crimes and Violations

- Similar to other types of investigations
- Goals
  - Find who is behind the crime
  - Collect the evidence
  - Present your findings
  - Build a case
- Depend on the city, state, or country
  - Example: spam
  - Always consult with an attorney
- Becoming commonplace
- Examples of crimes involving e-mails
  - Narcotics trafficking
  - Extortion
  - Sexual harassment
  - Child abductions and pornography

Examining E-mail Messages

- Access victim's computer to recover the evidence
- Using the victim's e-mail client
  - Find and copy evidence in the e-mail
  - Access protected or encrypted material
  - Print e-mails
- Guide victim on the phone
  - Open and copy e-mail including headers
- Sometimes you will deal with deleted e-mails
- Copying an e-mail message
  - Before you start an e-mail investigation

- You need to copy and print the e-mail involved in the crime or policy violation

– You might also want to forward the message as an attachment to another e-mail address

- With many GUI e-mail programs, you can copy an e-mail by dragging it to a storage medium
  - Or by saving it in a different location

Viewing E-mail Headers

- Learn how to find e-mail headers
  - GUI clients
  - Command-line clients
  - Web-based clients
- After you open e-mail headers, copy and paste them into a text document
  - So that you can read them with a text editor
- Headers contain useful information
  - Unique identifying numbers, IP address of sending server, and sending time
- Outlook
  - Open the Message Options dialog box
  - Copy headers
  - Paste them to any text editor
- Outlook Express
  - Open the message Properties dialog box
  - Select Message Source
  - Copy and paste the headers to any text editor

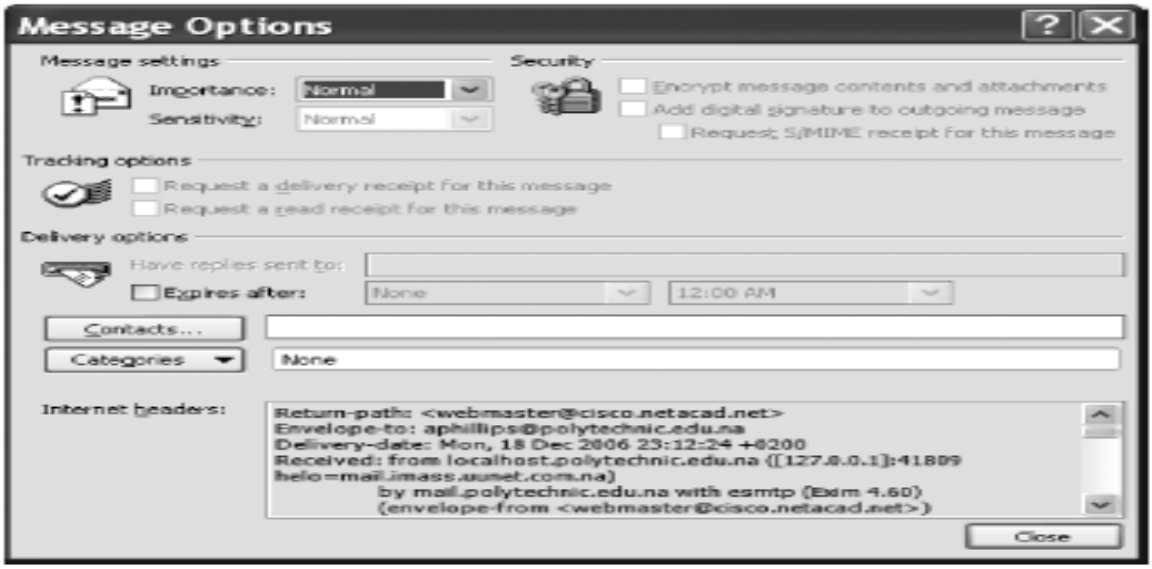


Figure 12-3 An Outlook e-mail header

- Novell Evolution

  - Click View, All Message Headers
  - Copy and paste the e-mail header
- Pine and ELM
  - Check enable-full-headers
- AOL headers
  - Click Action, View Message Source
  - Copy and paste headers
- Hotmail
  - Click Options, and then click the Mail Display Settings
  - Click the Advanced option button under Message Headers
  - Copy and paste headers
- Apple Mail
  - Click View from the menu, point to Message, and then click Long Header
  - Copy and paste headers

Figure 12-10 An Apple Mail e-mail header

- Yahoo
  - Click Mail Options
  - Click General Preferences and Show All headers on incoming messages
  - Copy and paste headers

Figure 12-11 Selecting the option to view headers in Yahoo!

Examining E-mail Headers

- Gather supporting evidence and track suspect
  - Return path
  - Recipient's e-mail address
  - Type of sending e-mail service
  - IP address of sending server
  - Name of the e-mail server
  - Unique message number
  - Date and time e-mail was sent
  - Attachment files information

Examining Additional E-mail Files

- E-mail messages are saved on the client side or left at the server
- Microsoft Outlook uses .pst and .ost files
- Most e-mail programs also include an electronic address book
- In Web-based e-mail
  - Messages are displayed and saved as Web pages in the browser's cache folders
  - Many Web-based e-mail providers also offer instant messaging (IM) services

Tracing an E-mail Message

- Contact the administrator responsible for the sending server

- Finding domain name's point of contact
  - www.arin.net
  - www.internic.com
  - www.freeality.com
  - www.google.com
- Find suspect's contact information
- Verify your findings by checking network e-mail logs against e-mail addresses

Using Network E-mail Logs

- Router logs
  - Record all incoming and outgoing traffic
  - Have rules to allow or disallow traffic
  - You can resolve the path a transmitted e-mail has taken
- Firewall logs
  - Filter e-mail traffic
  - Verify whether the e-mail passed through
- You can use any text editor or specialized tools

Understanding E-mail Servers

- Computer loaded with software that uses e-mail protocols for its services
  - And maintains logs you can examine and use in your investigation
- E-mail storage
  - Database
  - Flat file
- Logs
  - Default or manual
  - Continuous and circular
- Log information
  - E-mail content
  - Sending IP address
  - Receiving and reading date and time
  - System-specific information
- Contact suspect's network e-mail administrator as soon as possible
- Servers can recover deleted e-mails
  - Similar to deletion of files on a hard drive

Examining UNIX E-mail Server Logs

- /etc/sendmail.cf
  - Configuration information for Sendmail
- /etc/syslog.conf
  - Specifies how and which events Sendmail logs
- /var/log/maillog
  - SMTP and POP3 communications
    - IP address and time stamp
- Check UNIX man pages for more information

```
# The following line will send all mail logs to the /var/log/maillog
directory
mail.*                          /var/log/mail.log
# Log all emergency messages in the same place
*.emerg                         *
*.emerg                         @superiorbicycles.biz
# This line will put all news and e-mail encoded with uucp with
Critical errors in the #/var/log/spooler
uucp, news.crit
```

Figure 12-15 A typical syslog.conf file

Examining Microsoft E-mail Server Logs

- Microsoft Exchange Server (Exchange)
  - Uses a database
  - Based on Microsoft Extensible Storage Engine
- Information Store files
  - Database files *.edb
    - Responsible for MAPI information
  - Database files *.stm
    - Responsible for non-MAPI information
- Transaction logs
  - Keep track of e-mail databases
- Checkpoints
  - Keep track of transaction logs
- Temporary files
- E-mail communication logs
  - res#.log
- Tracking.log

  --Tracks messages

- Troubleshooting or diagnostic log
  - Logs events
  - Use Windows Event Viewer
  - Open the Event Properties dialog box for more details about an event

Examining Novell GroupWise E-mail Logs

- Up to 25 databases for e-mail users
  - Stored on the Ofuser directory object
  - Referenced by a username, an unique identifier, and .db extension
- Shares resources with e-mail server databases
- Mailboxes organizations
  - Permanent index files
  - QuickFinder
- Folder and file structure can be complex
  - It uses Novell directory structure
- Guardian
  - Directory of every database
  - Tracks changes in the GroupWise environment
  - Considered a single point of failure
- Log files
  - GroupWise generates log files (.log extension) maintained in a standard log format in GroupWise folders

Using Specialized E-mail Forensics Tools

- Tools include:
  - AccessData's Forensic Toolkit (FTK)
  - ProDiscover Basic
  - FINALeMAIL
  - Sawmill-GroupWise
  - DBXtract
  - Fookes Aid4Mail and MailBag Assistant
  - Paraben E-Mail Examiner
  - Ontrack Easy Recovery EmailRepair
  - R-Tools R-Mail
- Tools allow you to find:
  - E-mail database files

  - Personal e-mail files
  - Offline storage files
  - Log files
- Advantage
  - Do not need to know how e-mail servers and clients work
- FINALeMAIL
  - Scans e-mail database files
  - Recovers deleted e-mails
  - Searches computer for other files associated with e-mail

Using AccessData FTK to Recover E-mail

- FTK
  - Can index data on a disk image or an entire drive for faster data retrieval
  - Filters and finds files specific to e-mail clients and servers
- To recover e-mail from Outlook and Outlook Express
  - AccessData integrated dtSearch
    - dtSearch builds a b-tree index of all text data in a drive, an image file, or a group of files

Using a Hexadecimal Editor to Carve E-mail Messages

- Very few vendors have products for analyzing e-mail in systems other than Microsoft
- mbox format
  - Stores e-mails in flat plaintext files
- Multipurpose Internet Mail Extensions (MIME) format
  - Used by vendor-unique e-mail file systems, such as Microsoft .pst or .ost
- Example: carve e-mail messages from Evolution

7. Explain the basic concepts of mobile device forensics.

Understanding Mobile Device Forensics

- People store a wealth of information on cell phones, and the thought of losing your cell phone and, therefore, the information stored on it can be a frightening prospect.
- Despite this concern, not many people think about securing their cell phones, although they routinely lock and secure laptops or desktops. Depending on your phone's model, the following items might be stored on it:
  - Incoming, outgoing, and missed calls

- Text and Short Message Service (SMS) messages
- E-mail
- Instant messaging (IM) logs
- Web pages
- Pictures
- Personal calendars
- Address books
- Music files
- Voice recordings

Despite the usefulness of these devices in providing clues for investigations, investigating cell phones and mobile devices is one of the most challenging tasks in digital forensics. No single standard exists for how and where cell phones store messages, although many phones use similar storage schemes. In addition, new phones come out about every six months, and they're rarely compatible with previous models. Therefore, the cables and accessories you have might become obsolete in a short time.

Mobile Phone Basics

Since the 1970s, when Motorola introduced cell phones, mobile phone technology has advanced rapidly. Gone are the days of two-pound cell phones that only the wealthy could afford. In the past 40 years, mobile phone technology has developed far beyond what the inventors could have imagined.

Up to the end of 2008, there have been three generations of mobile phones: analog, digital personal communications service (PCS), and third-generation (3G). 3G offers increased bandwidth, compared with the other technologies:

- 384 Kbps for pedestrian use
- 128 Kbps in a moving vehicle
- 2 Mbps in fixed locations, such as office buildings

4G networks can use the following technologies:

• **Orthogonal Frequency Division Multiplexing (OFDM)—**The Orthogonal Frequency Division Multiplexing (OFDM) technology uses radio waves broadcast over different frequencies, uses power more efficiently, and is more immune to interference ("What You Need to Know About 4G," www.networkworld.com/news/2007/052107-specialfocus- 4g.html).

• **Mobile WiMAX**—This technology uses the IEEE 802.16e standard and Orthogonal Frequency Division Multiple Access (OFDMA) and is expected to support transmission speeds of 12Mbps. Sprint has chosen this technology for its 4G network, although some argue it's not true 4G.

• **Ultra Mobile Broadband (UTMS)—**Also known as CDMA2000 EV-DO, this technology is expected to be used by CDMA network providers to switch to 4G and support transmission speeds of 100 Mbps.

Table 13-1 Digital networks

Digital network	Description
Code Division Multiple Access (CDMA)	Developed during WWII, this technology was patented by Qualcomm after the war. One of the most common digital networks, it uses the full radio frequency spectrum to define channels. Sprint and Verizon, for example, use CDMA networks.
Global System for Mobile Communications (GSM)	Another common digital network, it's used by AT&T and T-Mobile and is the standard in Europe and Asia.
Time Division Multiple Access (TDMA)	This digital network uses the technique of dividing a radio frequency into time slots; GSM networks use this technique. It also refers to a specific cellular network standard covered by Interim Standard (IS) 136.
Integrated Digital Enhanced Network (iDEN)	This Motorola protocol combines several services, including data transmission, into one network.
Digital Advanced Mobile Phone Service (D-AMPS)	This network is a digital version of the original analog standard for cell phones.
Enhanced Data GSM Environment (EDGE)	This digital network, a faster version of GSM, is designed to deliver data.
Orthogonal Frequency Division Multiplexing (OFDM)	This technology for 4G networks uses energy more efficiently than 3G networks and is more immune to interference.

• **Multiple Input Multiple Output (MIMO)—**This technology, developed by Airgo and acquired by Qualcomm, is expected to support transmission speeds of 312 Mbps.

• **Long Term Evolution (LTE)—**This technology, designed for GSM and UMTS

Although digital networks use different technologies, they operate on the same basic principles. Basically, geographical areas are divided into cells resembling honeycombs.

As described in NIST SP 800-101 (mentioned earlier in this section), three main components are used for communication with these cells:

• **Base transceiver station (BTS)—**This component is made up of radio transceiver equipment that defines cells and communicates with mobile phones; it's sometimes referred to as a cell phone tower, although the tower is only one part of the BTS equipment.

• **Base station controller (BSC)—**This combination of hardware and software manages BTSs and assigns channels by connecting to the mobile switching center.

• **Mobile switching center (MSC**)—This component connects calls by routing digital packets for the network and relies on a database to support subscribers. This central database contains account data, location data, and other key information needed during an investigation. If you have to retrieve information from a carrier's central database, you usually need a warrant or subpoena.

Inside Mobile Devices

- Mobile devices can range from simple phones to small computers, also called smart phones.
- The hardware consists of a microprocessor, ROM, RAM, a digital signal processor, a radio module, a microphone and speaker, hardware interfaces (such as keypads, cameras, and GPS devices), and an LCD display. Many have removable memory cards, and Bluetooth and Wi-Fi are now included in some mobile devices, too.
- Most basic phones have a proprietary OS, although smart phones use the same OSs as PCs (or stripped-down versions of them). These OSs include Linux, Windows Mobile, RIM OS, Palm OS, Symbian OS, and, with the introduction of the Apple iPhone, a version of Mac OS X.
- Typically, phones store system data in electronically erasable programmable read only memory (EEPROM), which enables service providers to reprogram phones without having to access memory chips physically.

SIM Cards Subscriber identity module (SIM) cards are found most commonly in GSM devices and consist of a microprocessor and 16 KB to 4 MB EEPROM. There are also high-capacity, high-density, super, and mega SIM cards that boast as high as 1 GB EEPROM. SIM cards are similar to standard memory cards, except the connectors are aligned differently.

The SIM card is necessary for the ME to work and serves these additional purposes:

- Identifies the subscriber to the network
- Stores personal information
- Stores address books and messages
- Stores service-related information

SIM cards come in two sizes, but the most common is the size of a standard U.S. postage stamp and about 0.75 mm thick. Portability of information is what makes SIM cards so versatile.

By switching a SIM card between compatible phones, users can move their information to another phone automatically without having to notify the service provider.

Inside PDAs

Personal digital assistants (PDAs) can still be found as separate devices from mobile phones. Most users carry them instead of a laptop to keep track of appointments, deadlines, address books, and so forth. Palm Pilot and Microsoft Pocket PC were popular models when PDAs came on the market in the 1990s, and standalone PDAs are still made by companies such as Palm, Sharp, and HP.

A number of peripheral memory cards are used with PDAs:

• **Compact Flash (CF)—**CF cards are used for extra storage and work much the same way as PCMCIA cards.

• **MultiMedia Card (MMC)—**MMC cards are designed for mobile phones, but they can be used with PDAs to provide another storage area.

• **Secure Digital (SD)—**SD cards are similar to MMCs but have added security features to protect data.

8.Describe procedures for acquiring data from cell phones and mobile Devices.

Understanding Acquisition Procedures for Cell Phones and Mobile Devices

All mobile devices have volatile memory, so making sure they don't lose power before you can retrieve RAM data is critical. At the investigation scene, determine whether the device is on or off. If it's off, leave it off, but find the recharger and attach it as soon as possible. If the device is on, check the LCD display for the battery's current

charge level. Because mobile devices are often designed to synchronize with applications on a user's PC, any mobile device attached to a PC via a cable or cradle/docking station should be disconnected from the PC immediately.

The alternative is to isolate the device from incoming signals with one of the following options:

• Place the device in a paint can, preferably one that previously contained radio wave–blocking paint.

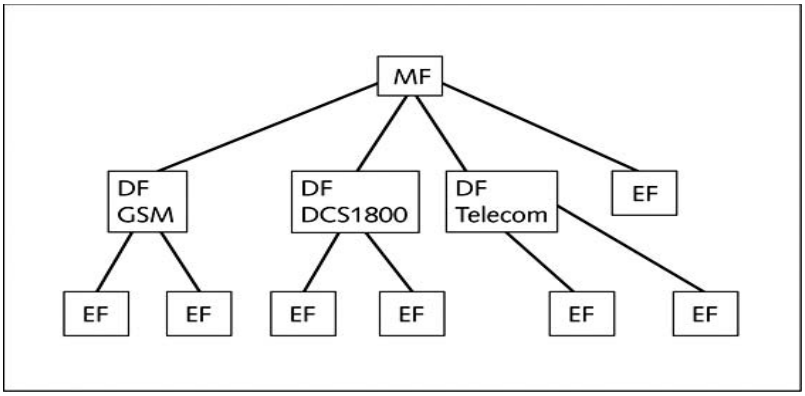
• Use the Paraben Wireless StrongHold Bag (www.paraben-forensics.com/catalog), which conforms to Faraday wire cage standards.

• Use eight layers of antistatic bags (for example, the bags that new hard drives are wrapped in) to block the signal.

When you're back in the forensics lab, you need to assess what can be retrieved. Knowing where information is stored is critical. You should check these four areas:

- The internal memory
- The SIM card
- Any removable or external memory cards
- The system server

- ✓ Memory storage on a mobile device is usually implemented as a combination of volatile and nonvolatile memory.
- ✓ Volatile memory requires power to maintain its contents, but nonvolatile memory does not.
- ✓ Although the specific locations of data vary from one phone model to the next, volatile memory usually contains data that changes frequently, such as missed calls, text messages, and sometimes even user files.
- ✓ Nonvolatile memory, on the other hand, contains OS files and stored user data, such as a personal information manager (PIM) and backed-up files.



You can retrieve quite a bit of data from a SIM card. The information that can be retrieved falls into four categories:

- Service-related data, such as identifiers for the SIM card and subscriber
- Call data, such as numbers dialed
- Message information
- Location information

Mobile Forensics Equipment

- ✓ Mobile forensics is such a new science that many of the items you're accustomed to retrieving from computers, such as deleted files, aren't available on mobile devices.
- ✓ The biggest challenge is dealing with constantly changing models of cell phones. This section gives you an overview of procedures for working with mobile forensics software, and specific tools are discussed in the following sections.
- ✓ The first step is identifying the mobile device. Most users don't alter their devices, but some file off serial numbers, change the display to show misleading data, and so on.
- ✓ When attempting to identify a phone, you can make use of several online sources, such as www. cellphoneshop.com, www.phonescoop.com, and www.mobileforensicscentral.com.
- ✓ The next step is to attach the phone to its power supply and connect the correct cables.
- ✓ Often you have to rig cables to connect to devices because cables for the model you're investigating are not available. U.S. companies usually don't supply cables for phones not commonly used in the United States, but the reverse is true for companies based in Europe.
- ✓ Some vendors have toolkits with an array of cables you can use (discussed later in "Mobile Forensics Tools").
- ✓ After you've connected the device, start the forensics program and begin downloading the available information.

SIM Card Readers

- ✓ **SIM Card Readers** With GSM phones and many newer models of mobile devices, the next step is accessing the SIM card, which you can do by using a combination hardware/ software device called a SIM card reader.

- ✓ The general procedure is as follows:
    1. Remove the back panel of the device.
    2. Remove the battery.
    3. Under the battery, remove the SIM card from its holder.
    4. Insert the SIM card into the card reader, which you insert into your forensic workstation's USB port.

iPhone Forensics

- ✓ **iPhone Forensics** Because the iPhone is so popular, its features are copied in many other mobile devices. The wealth of information that can be stored on this device makes iPhone forensics particularly challenging.
- ✓ At first, many researchers and hackers tried to find a way to "crack" the iPhone but were unsuccessful because the device is practically impenetrable.
- ✓ A more fruitful approach was hacking backup files. However, this method does have limitations: You can access only files included in a standard backup, so deleted files, for example, can't be accessed.

Mobile Forensics Tools

- ✓ **Mobile Forensics Tools** Paraben Software (www.paraben.com), a leader in mobile forensics software, offers several tools, including Device Seizure, used to acquire data from a variety of phone models. Paraben also has the Device Seizure Toolbox containing assorted cables, a SIM card reader, and other equipment for mobile device investigations. DataPilot (www.datapilot.com) has a similar collection of cables that can interface with Nokia, Motorola, Ericsson, Samsung, Audiovox, Sanyo, and others.

SIMCon's features include the following:

- Reads files on SIM cards
- Analyzes file content, including text messages and stored numbers
- Recovers deleted text messages
- Manages PIN codes
- Generates reports that can be used as evidence
- Archives files with MD5 and SHA-1 hash values
- Exports data to files that can be used in spreadsheet programs
- Supports international character sets

Important Questions

Part-A

1. Define bit-shifting
2. Define Known File Filter (KFF).
3. Define steganography.
4. Define network forensics.
5. Define client/server architecture.
6. Define Enhanced Simple Mail Transfer Protocol (ESMTP).
7. Define Multipurpose Internet Mail Extensions (MIME)
8. Define spoofing
9. How to Validating with Computer Forensics Programs
10. List out the Addressing Data-hiding Techniques
11. Define Code Division Multiple Access (CDMA)
12. Define Electronically erasable programmable read-only memory (EEPROM)
13. Define fourth-generation (4G).
14. Define Global System for Mobile Communications (GSM).
15. Define Orthogonal Frequency Division Multiplexing (OFDM).
16. How to Exploring the Role of E-mail in Investigations.
17. How to Exploring the Roles of the Client and Server in E-mail.
18. List out E-Mail Headers.
19. List out the E-mail Forensics Tools
20. Define SIM Card Readers

Part-B

1. Determine what data to analyze in a computer forensics investigation
2. Explain tools used to validate data
3. Explain common data-hiding techniques
4. Describe methods of performing a remote acquisition
5. Explain standard procedures for network forensics
6. Describe the use of network tools
7. Describe the importance of network forensics
8. Explain the basic concepts of mobile device forensics
9. Describe procedures for acquiring data from cell phones and mobile devices
10. Explain in detail about the E-Mail Investigations.