MODULE 4

UNDERSTANDING MOBILE DEVICE FORENSICS

- People store a wealth of information on cell phones and smartphones, and the thought of losing your phone and, therefore, the information stored on it can be a frightening prospect.

- Despite this concern, not many people think about securing their phones, although they routinely lock and secure laptops or desktops.

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

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

- Many people store more information on smartphones and tablets than on computers.

- When you consider that smartphones have the same computing power as desktops of a few years ago, the amount of information stored on them is often enough to piece together a case’s facts.

MOBILE PHONE BASICS

- Mobile phone technology has advanced rapidly in the past few decades and developed far beyond what its inventors could have imagined.
- Gone are the days of two-pound cell phones that only the wealthy could afford.
- By the end of 2008, mobile phones had gone through three generations:
  - Analog
  - digital personal communications service (PCS)
  - third-generation (3G) .

- 3G introduced unheard-of capabilities, such as being able to download while you were walking or in a moving vehicle.

- Sprint Nextel introduced the fourth-generation (4G) network in 2009.

- Fifth-generation (5G) cellular networks, expected to be finalized in 2020, will incorporate emerging technologies, including the ever-expanding cloud and device-to-device networks.

Digital network	Description
Code Division Multiple Access (CDMA)	Developed during World War II, this technology was patented by Qualcomm . **Code Division Multiple Access (CDMA)** is a **digital communication technology** used in mobile networks that allows **multiple users to share the same frequency** band at the same time. Each user's data is assigned a **unique code**, which helps differentiate it from other signals.
Global System for Mobile Communications (GSM)	Another common digital network, it's used by AT&T and T-Mobile in the United States and is the standard in Europe and Asia. **TDMA-based (Time Division Multiple Access)**: GSM divides each frequency into time slots. Each user is assigned a specific time slot for their communication.
Time Division Multiple Access (TDMA)	a single frequency channel is divided into multiple time slots. Each user on the network is assigned a specific time slot in which they can send or receive their data (like voice or internet packets); 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. Ie, that integrates two-way radio (also known as push-to-talk or PTT), digital cellular voice, and data services into a single network. iDEN uses **TDMA (Time Division Multiple Access)** technology, dividing the frequency channel into time slots.

Digital network	Description
Digital Advanced Mobile Phone Service (D-AMPS)	D-AMPS, or Digital Advanced Mobile Phone System, is a digital mobile phone standard developed for second-generation (2G) mobile networks and was designed to provide better voice quality, improved capacity, and enhanced security.
Enhanced Data GSM Environment (EDGE)	This digital network, a faster version of GSM, is designed to deliver data. It is often considered a bridge between 2G and 3G networks and is sometimes referred to as 2.5G due to its intermediate data capabilities.
Orthogonal Frequency Division Multiplexing (OFDM)	This technology for 4G networks uses energy more efficiently than 3G networks and is more immune to interference.

CDMA (Code Division Multiple Access) Networks:

- **IS-95 (Interim Standard 95)**: A standard used in CDMA networks, developed by the **Telecommunications Industry Association (TIA)**. CDMA systems based on IS-95 are also called **CDMAOne**.
- **CDMA2000**: When CDMA networks upgraded to 3G (third-generation), they became **CDMA2000**, which offers faster data and better services.

GSM (Global System for Mobile Communications):

- **TDMA (Time Division Multiple Access)**: GSM uses TDMA technology, which lets multiple phones share the same channel by taking turns (like a round-robin system).
- **EDGE (Enhanced Data GSM Environment)**: A standard created to improve GSM networks and provide 3G services, offering faster data speeds.

- **3G Standard:**
- Developed by the **International Telecommunication Union (ITU)** and works with **CDMA, GSM,** and **TDMA** technologies.
- **4G Networks:**
- In 2008, the **International Telecommunication Union Radio (ITU-R)** defined what is needed for a network to be called **4G**. Some of the main technologies used in 4G networks are:

1. **OFDM (Orthogonal Frequency Division Multiplexing)**:
    1. Uses multiple smaller signals instead of one large signal. This helps avoid interference and provides better performance.
2. **Mobile WiMAX**:
    1. Based on the **IEEE 802.16e** standard and uses **OFDMA** (a variant of OFDM). WiMAX can reach speeds of 12 Mbps.
3. **UMB (Ultra Mobile Broadband)**:
    1. Also known as **CDMA2000 EV-DO**, used by CDMA networks to switch to 4G. It supports high transmission speeds (up to 275 Mbps for downloads).
4. **MIMO (Multiple Input Multiple Output)**:
    1. Uses multiple antennas to send and receive more data, making networks faster. It supports speeds up to 312 Mbps and is used in 4G, WiMAX, and other technologies.
5. **LTE (Long Term Evolution)**:
    1. Designed for GSM and **UMTS** (Universal Mobile Telecommunications Systems) networks. It supports speeds from 45 Mbps to 144 Mbps and is commonly called **4G LTE**.

How Mobile Networks Work:

Even though different networks (like CDMA and GSM) use different technologies, they work similarly by dividing areas into cells. These cells allow **phones to communicate with the network** using three main components:

1. **Base Transceiver Station (BTS)**:
    1. Commonly called a "cell tower," this equipment handles communication between phones and the network.

2. **Base Station Controller (BSC)**:
    1. Manages several BTS units and assigns channels for phone calls. It connects to the main control center.

3. **Mobile Switching Center (MSC)**:
    1. Routes calls between different network areas. It uses a database that stores information about users and their locations to manage services efficiently.

INSIDE MOBILE DEVICES

- Mobile devices can range from simple phones to smartphones , tablets, and smartwatches.

- 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 up to 64 GB of internal memory, and Bluetooth and Wi-Fi are included in most mobile devices

- <u>Proprietary OS vs. Smartphone OS</u>

1. Proprietary OS: Basic phones often use a proprietary operating system, which means the software is designed specifically for that manufacturer's hardware. This OS is usually less flexible and feature-rich compared to those on smartphones.
2. Smartphone OS: Smartphones, on the other hand, typically use operating systems that are more similar to those used on personal computers (PCs).

Common smartphone OSs include:

1. Windows Mobile: A now-discontinued OS from Microsoft designed for mobile devices.
2. RIM OS: The operating system used by BlackBerry devices, also less common now.
3. Android: Based on the Linux kernel, it's an open-source OS developed by Google and widely used in many smartphones.
4. Google OS: This might refer to Google’s version of Android or related services.
5. iOS: The operating system designed for Apple devices like the iPhone and iPad.

- The operating system (OS) is stored in Read-Only Memory (ROM), which is a type of nonvolatile memory. This means that the OS and other stored data remain accessible even when the phone loses power.

- For personal use, personal digital assistants (PDAs) have been replaced by iPods, iPads, and other mobile devices.

- The use of PDAs has shifted to more specific markets, such as medical or industrial PDAs; they’re now called “handhelds” and are still sold on sites such as Amazon and eBay.

- Palm Pilot and Microsoft Pocket PC were popular models when PDAs came on the market in the 1990s.
- HP purchased Palm and used the OS in its first tablet devices called touchpads.
- Similar to smartphones, PDAs housed a microprocessor, flash ROM, RAM, and other hardware components.
- As with smartphones, the amount of information on a PDA varied depending on the model.
- Usually, you could retrieve a user's calendar, address book, Web access, and other items

A number of peripheral memory cards were used with PDAs:

- Compact Flash (CF)—CF cards were used for extra storage and work much the same way as PCMCIA cards.
- MultiMediaCard (MMC)—MMC cards were 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; they're now used on smartphones.

- Most PDAs were designed to synchronize with a computer, so they had built-in slots for that purpose (whether hard-wired or wireless synchronization).
- Although you’re not likely to encounter PDAs during an investigation, having some background information on PDAs is still useful.

SIM CARDS

- Subscriber identity module (SIM) cards are usually found in GSM devices, and consist of a microprocessor and internal memory.
- SIM cards are similar to standard memory cards, except the connectors are aligned differently.
- iPhones and many Android phones have micro SIM and nano SIM slots. However, some can be accessed only if the phone has been unlocked.

- GSM (Global System for Mobile Communications) refers to mobile phones as "mobile stations," which are made up of two main parts:

1. **SIM Card**: This is the part that stores the user's information, such as the phone number and network details.
2. **Mobile Equipment (ME)**: This refers to the rest of the phone, including the hardware and software that enable the phone to make calls, send texts, and access data.

- In essence, a mobile station in GSM consists of the SIM card and the mobile equipment that work together for mobile communication.
- The SIM card is necessary for the ME to work and serves these additional purposes:
  - Identifies the subscriber to the network
  - Stores service-related information
  - Can be used to back up the device (Contacts, SMS Messages, Network Settings, Service Provider Information)

- SIM cards come in three sizes: standard, micro, and nano.
- Portability of information is what makes SIM cards so versatile.
- By switching a SIM card between compatible phones, users can move their provider usage and other information to another phone automatically without having to notify the service provider.

- For example, if you travel between neighboring countries often, you could have a GSM phone and two SIM cards. When you travel to another country, you simply switch to the other SIM card. With phones on which this switching is allowed, information such as your contact list is stored on the phone, so when you switch to another carrier, all you have to do is change the SIM card. Another common practice is switching to another SIM card when you have used most of your monthly minutes on your main SIM card.

- many phones now include SD cards for external storage.
- Standard SD cards range from 16 GB to 64 GB and can be part of a mobile device or game console.
- Other sizes include miniSD and microSD cards.

UNDERSTANDING ACQUISITION PROCEDURES FOR MOBILE DEVICES

- Search and seizure procedures for mobile devices are as important as procedures for computers.
- The main concerns are loss of power, synchronization with cloud services, and remote wiping (the process of erasing data on a mobile device or computer from a distance, typically using software or services designed for device management and security)
- 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 charger and attach it as soon as possible. If the device is on, check the display for the battery's current charge level.

- Because mobile devices are often designed to synchronize with applications on a user's laptop or tablet, any mobile device attached to a PC or tablet via a USB cable or micro USB cable should be disconnected immediately.
- Many people use their smartphones to get Internet access for tablets or laptops, so you might find these devices already connected to the Internet.

- Disconnecting them immediately helps prevent synchronization that might occur automatically on a preset schedule and overwrite data on the device.
- In addition, collect the laptop and any peripheral devices to determine whether the hard drive contains any information that’s been transferred and then deleted from the mobile device, including pictures, videos, and other files that have been transferred and then deleted.

- Depending on the warrant the **time of seizure might be relevant**.
- In addition, **messages** might be received on the mobile device **after seizure** that may or may not be admissible in court.
- **If** you determine that the device **should be turned off** to preserve battery power or prevent a possible attack, **note the time and date** when you take this step.

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

- Place the device in airplane mode, if this feature is available.
- Place the device in a paint can, preferably one that previously contained radio wave blocking paint.
- Use a Faraday bag that conforms to Faraday wire cage standards.
- Turn the device off.

- **Drawbacks of Isolating Mobile Devices from Signals:**

1. **Increased Battery Drain**:When a mobile device is isolated from signals (for example, by putting it in airplane mode or a Faraday bag), it may switch to **roaming mode** to keep searching for a signal, which causes the battery to drain faster.
2. **Device Shutoff or Sleep Mode**: Once the battery gets too low, the device may automatically shut off or enter a **sleep state**.
3. **Important Step in Investigations**: Despite these drawbacks, it's still necessary to **isolate the device from signals** to prevent it from sending or receiving data during an investigation.

- This isolation ensures that no new data can affect the evidence on the phone, even though it may drain the battery faster.

- To determine whether you should do a logical acquisition or physical acquisition, you need to know where information is stored.
- As with laptops and desktops, a logical acquisition involves accessing files and folders as you would see them when looking at them in File Explorer.
- A physical acquisition is a bit-by-bit acquisition done to find deleted files or folders.

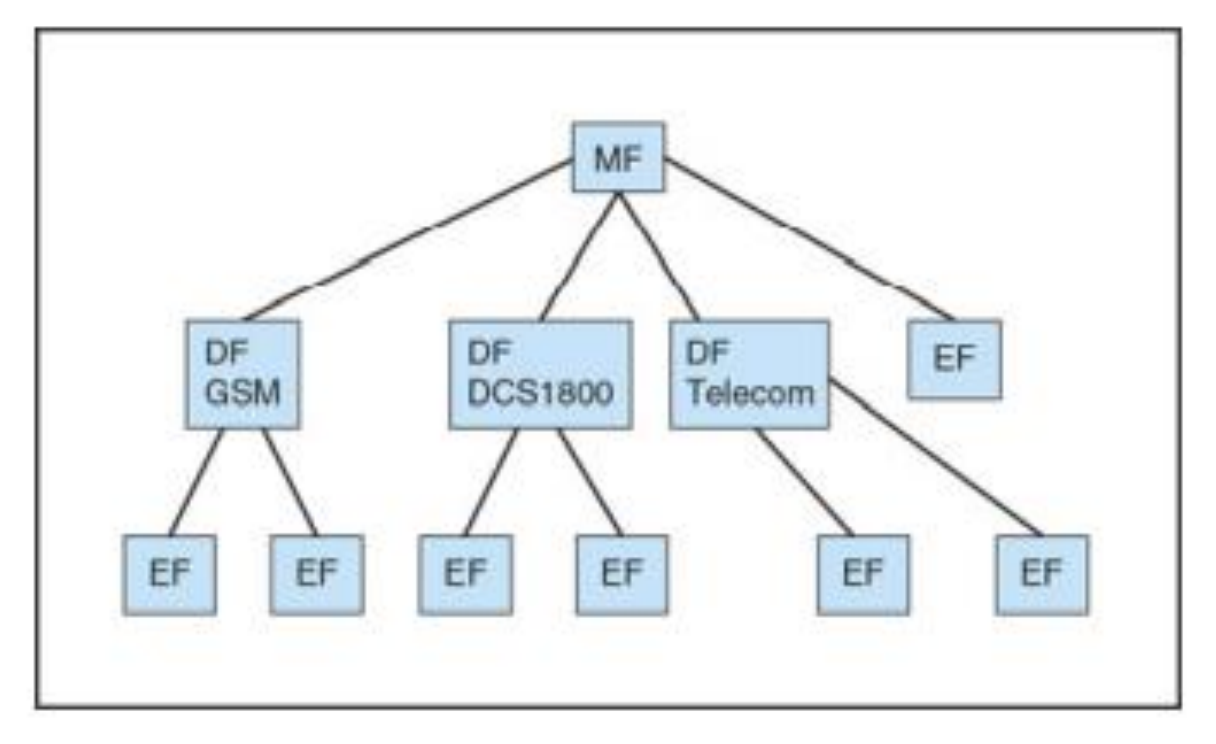
- You should check the following locations for information, keeping in mind that with mobile devices, often you need manufacturers’ tools:
- Internal memory
- SIM card
- Removable or external memory cards
- Network provider

- Because of the growing problem of mobile devices being stolen, service providers have started using remote wiping to remove a user's personal information stored on a stolen device, and this procedure often results in the loss of valuable information for investigations.
- Remote wiping is usually done to remove an account so that a thief can't use the phone and rack up charges.
- It also erases all contacts, the calendar, and other personal information, such as photos and bank logins, stored on the device.
- In some instances, it restores the device to the original factory settings.

- Depending on the device and service provider, the device owner or the service provider can do the remote wipe.
- Remote wiping can be used by device owners trying to protect their information.

- Memory storage on a mobile device is usually a combination of volatile and nonvolatile memory.
- Volatile memory requires power to maintain its contents, but nonvolatile memory doesn't.
- Although the 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.

- As mentioned, memory resides in the phone and in the SIM card, if the device is equipped with one.
- The file system for a SIM card is a hierarchical structure.
- This file structure begins with the root of the system (MF). The next level consists of directory files (DF), and under them are files containing elementary data (EF).



MF
DF GSM
DF DCS1800
DF Telecom
EF
EF
EF
EF
EF
EF
EF

- You can retrieve quite a bit of data from a SIM card, depending on whether the phone is GSM or CDMA. 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

- If power has been lost, you might need PINs or other access codes to view files.
- Typically, users keep the original PIN assigned to the SIM card, so when you're collecting evidence at the scene, look for users' manuals and other documentation that can help you access the SIM card.
- With most SIM cards, you have three attempts at entering an access code before the device is locked, which then requires calling the service provider to get the PIN unlock key (PUK) and waiting a certain amount of time before trying again. Common codes to try are 1-1-1-1 or 1-2-3-4.

MOBILE FORENSICS EQUIPMENT

- Mobile forensics is an evolving science, with the biggest challenge being constantly changing phone models.
- What works today might not work on a model that comes out tomorrow.

- 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.phonescoop.com.

- Next, make sure you have installed the mobile device forensics software.
- As mentioned, not all facilities are equipped with the necessary software because many tools are cost prohibitive.
- Some vendors offer tools that simply take pictures of screens as you scroll through them.
- Forensically, this approach isn’t the best, but you can use it if no other alternatives are available.

- The next step is to attach the phone to its power supply and connect the correct cables.
- Most phones now have a combination USB/power cable, and many are interchangeable.
- For older phones, often you have to rig cables together. Some vendors have toolkits with an array of cables you can use.

- After you’ve connected the device, start the forensics software and begin downloading the available information.
- If your forensics software doesn’t support the model you’re investigating, you might need to acquire other tools.
- Your main concern should be that the software is forensically sound.

- The general procedure is as follows:

1. Remove the device’s back panel.
2. Remove the battery.
3. 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.

- A variety of SIM card readers are available.
- Some are forensically sound and some are not; make sure you note this feature in your investigation log.
- After you view a message, the device shows the message as opened or read.
- For this reason, documenting messages that haven't been read is critical.
- Using a tool that takes pictures of each screen can be valuable because these screen captures can provide additional documentation.

MOBILE PHONE FORENSICS TOOLS AND METHODS

- The best method of retrieving information, of course, is acquiring a forensic image, which enables you to recover deleted text messages and similar data.
- With Android devices, the process can be as simple as using AccessData FTK(Forensic Tool Kit) Imager to perform a logical acquisition and a low-level analysis

- iPhone acquisition procedures are similar, and several good tools are available, such as MacLockPick 3.0 ,which is designed to deal with iPhones, iPads, iOS, and Mac OS X Lion (now macOS).
- It can also extract iPhoto information, handle plug-in apps, and pull the user’s online history.

- The NIST(National Institute of Standards and Technology) guidelines list six types of mobile forensics methods:
  - Manual extraction—This method involves looking at the device's content page by page and taking pictures. It's used if investigators can't do a logical or physical extraction.
  - Logical extraction—The mobile device is connected to a forensic workstation via a wired (USB cable, for example) or wireless (such as Bluetooth) connection, and then the file system information is extracted.

- Physical extraction—As with a logical extraction, the mobile device is attached to a forensic workstation. However, a forensic copy is made so that deleted files can be retrieved and other items decoded.
- Hex dumping and Joint Test Action Group (JTAG) extraction—Hex dumping involves using a modified boot loader to access the RAM for analysis .The JTAG extraction method gets information from the processor, flash memory, or other physical components. It's a highly invasive method

- Chip-off—This method requires physically removing flash memory chip and gathering information at the binary level.
- Micro read—This method looks at logic gates with an electron microscope and can be used even when data has been overwritten on magnetic media. It’s very expensive, however, so it’s typically used only in cases involving national security.
- Cloud Data Extraction

- Paraben Software a vendor of mobile forensics software, offers several tools, such as E3:DS, for mobile device investigations.
    - **E3-(Electronic Evidence Examiner for Device Seizure)**:
- It examines Internet of Things (IoT) devices, has a bootloader for locked mobile devices, and can perform data parsing and cloud data capture.
- Paraben offers different packages for a variety of uses.

- DataPilot has a collection of cables that can interface with phones made by Nokia, Motorola, Ericsson, Samsung, Audiovox, Sanyo, and others.
- Susteen Inc. also has a tool for mobile forensics analysis called Secure View 3.

- BitPim is a tool used to view data on many CDMA phones, including LG, Samsung, Sanyo, and others. It offers versions for Windows, Linux, and macOS.
- It’s not a forensics tool, but it can be used in read-only mode.
- In Windows, BitPim stores files in Documents\BitPim by default, so when you start a new case, make sure you move these files to another location first so that they’re not overwritten

- MOBILedit Forensic is a forensics software tool containing a built-in write-blocker.
- It can connect to phones directly via Bluetooth or a cable and can read SIM cards by using a SIM reader.
- It’s notable for being very user friendly.

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 network forensics specialists in law enforcement, legal firms, companies, and universities.

- When intruders break into a network, they leave a trail.
- 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, if a company's peak use is typically between 6 a.m. and 6 p.m., that's when you should expect spikes. If a usage spike occurs during the night, the network administrator should recognize it as unusual activity and take steps to investigate it.

THE NEED FOR ESTABLISHED PROCEDURES

- Network forensics examiners must establish standard procedures for how to acquire data after an attack or intrusion incident.
- Typically, network administrators want to find compromised machines, get them offline, and restore them as quickly as possible to minimize downtime.
- However, taking the time to follow standard procedures is essential to ensure that all compromised systems have been found and to ascertain attack methods in an effort to prevent them from happening again.

- Procedures must be based on an organization’s needs and should complement the network infrastructure.
- The increase in cybercrimes has prompted many groups to begin compiling procedures and protocols to follow when a network intrusion occurs.
- Network administrators need to learn how to stop intruders and determine how they got in; what they copied, altered, or deleted; and whether they’re still on the network.

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** refers to the process of securing a system, network, or application by reducing its vulnerability to attacks. The goal of hardening is to minimize potential weaknesses by configuring systems to prevent unauthorized access, reduce exposure to threats, and limit the potential damage from security breaches. Hardening typically involves removing unnecessary software, services, and permissions, applying security patches, and implementing strict access controls.

- 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

- 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 prevent someone from 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.

- **Testing networks** is as important as testing servers.
- You need to be up to date on the latest methods intruders use to infiltrate networks as well as methods internal employees use to sabotage networks.
- In the early and mid-1990s, approximately 70% of network attacks were caused by employees.
- Since then, this problem has been compounded by contract employees, who often have the same level of network privileges as full-time employees.

DEVELOPING PROCEDURES FOR NETWORK FORENSICS

- As you have seen, log files are often examined along with forensic image files collected from devices.
- To get these files, you need to establish a good working relationship with network administrators and technicians.
- Network forensics can be a long, tedious process, and unfortunately, the trail can go cold quickly.

- A standard procedure often used in network forensics is as follows:

1. Always use a standard installation image for systems on a network. This image isn't a bitstream image but an image containing all the standard applications used. You should also have MD5 and SHA-1 hash values of all application and OS files.

2. When an intrusion incident happens, make sure the vulnerability has been fixed to prevent other attacks from taking advantage of the opening.

3. Attempt to retrieve all volatile data, such as RAM and running processes, by doing a live acquisition before turning the system off.

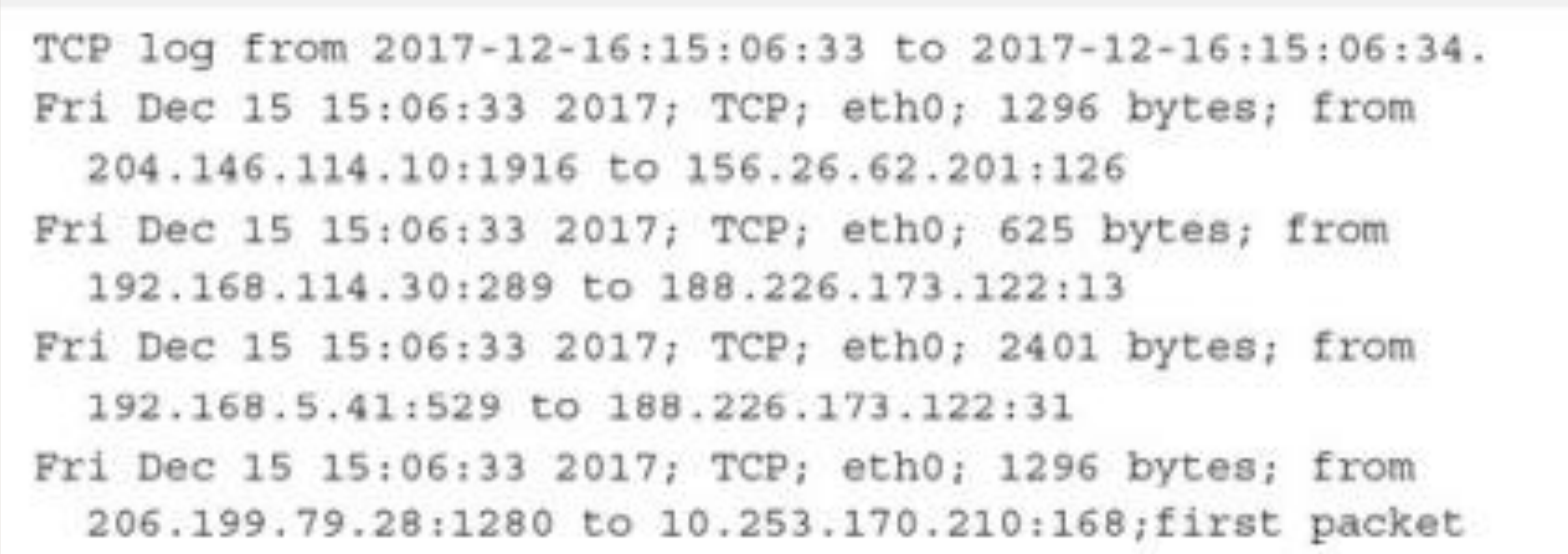
Acquire the compromised drive and make a forensic image of it

4. Compare files on the forensic image with the original installation image. Compare hash values of common files, such as Win.exe and standard dynamic link libraries (DLLs), and ascertain whether they have changed.

REVIEWING NETWORK LOGS

- Network logs record traffic in and out of a network.
- Network servers, routers, firewalls, and other devices record the activities and events that move through them.
- A common way of examining network traffic is running the tcpdump command-line program , which can produce hundreds or thousands of lines of records

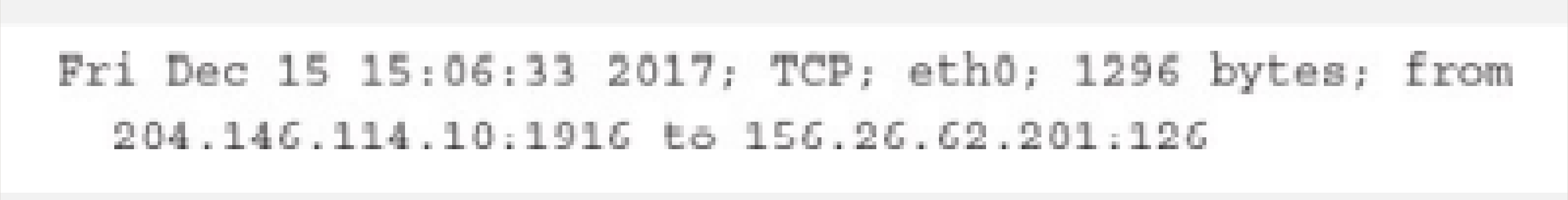
- A sample output:



```
TCP log from 2017-12-16:15:06:33 to 2017-12-16:15:06:34.
Fri Dec 15 15:06:33 2017; TCP; eth0; 1296 bytes; from
  204.146.114.10:1916 to 156.26.62.201:126
Fri Dec 15 15:06:33 2017; TCP; eth0; 625 bytes; from
  192.168.114.30:289 to 188.226.173.122:13
Fri Dec 15 15:06:33 2017; TCP; eth0; 2401 bytes; from
  192.168.5.41:529 to 188.226.173.122:31
Fri Dec 15 15:06:33 2017; TCP; eth0; 1296 bytes; from
  206.199.79.28:1280 to 10.253.170.210:168;first packet
```

- The first line of the output is simply the header.
- The rest of the lines follow the format time; protocol; interface; size; source and destination addresses.

- Take another look at the second line from the previous output:

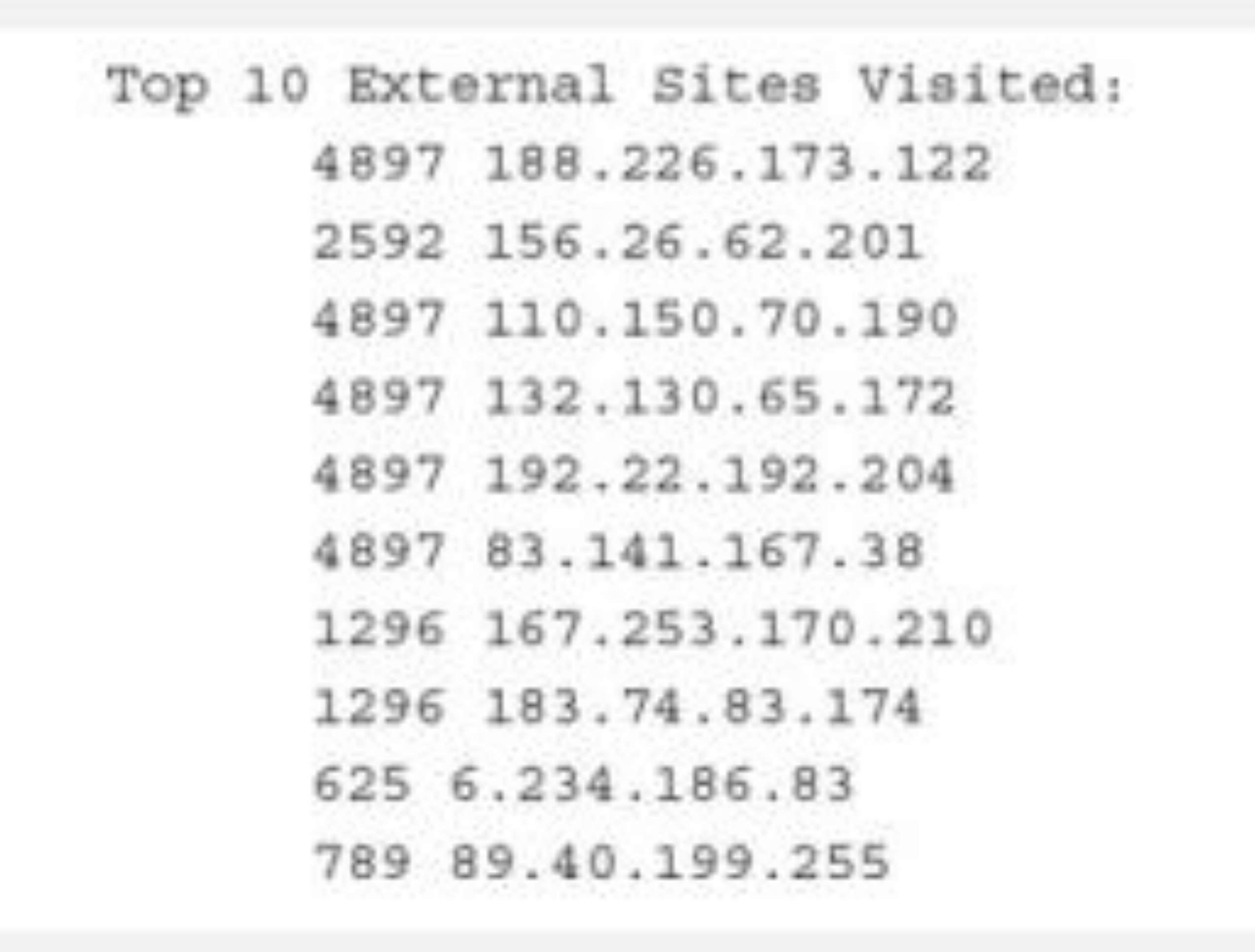


```
Fri Dec 15 15:06:33 2017; TCP; eth0; 1296 bytes; from
  204.146.114.10:1916 to 156.26.62.201:126
```

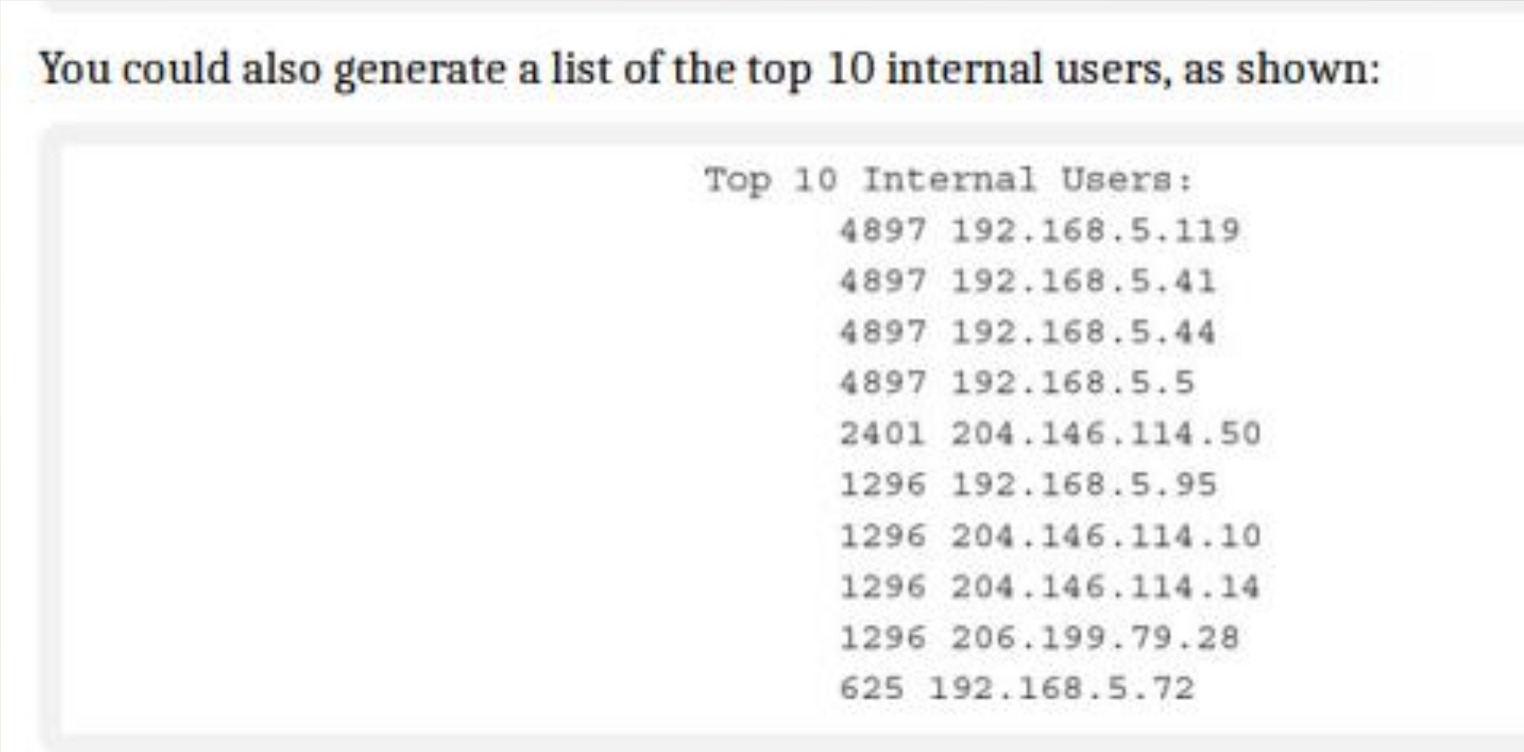
- This line shows that data was transmitted on Saturday, December 15, 2017, at 15:06:33. It was a TCP packet sent via the Ethernet 0 interface of 1296 bytes. The packet was sent from 204.146.114.10:1916 to 156.26.62.201:126. In these IP addresses, the numbers after the colon represent the port number.

- When viewing network logs, port information can give you clues to investigate.
- For example, you might notice that a particular IP address is coming in frequently on an unusual port.
- A receiving port above 1024, for example, should also raise a flag. You can check the Internet Assigned Numbers Authority Web site (www.iana.org/assignments/port-numbers) for a list of assigned port numbers.

- Using a network analysis tool such as Wireshark you could generate a list of the top 10 Web sites users in your network are visiting.
- As shown in the following output, the number of bytes being transferred is listed first, followed by the IP address of the site



```
Top 10 External Sites Visited:
     4897 188.226.173.122
     2592 156.26.62.201
     4897 110.150.70.190
     4897 132.130.65.172
     4897 192.22.192.204
     4897 83.141.167.38
     1296 167.253.170.210
     1296 183.74.83.174
     625 6.234.186.83
     789 89.40.199.255
```



You could also generate a list of the top 10 internal users, as shown:

```
Top 10 Internal Users:
      4897 192.168.5.119
      4897 192.168.5.41
      4897 192.168.5.44
      4897 192.168.5.5
      2401 204.146.114.50
      1296 192.168.5.95
      1296 204.146.114.10
      1296 204.146.114.14
      1296 206.199.79.28
      625 192.168.5.72
```

- These network logs can show you patterns, such as an employee transmitting data to or from a particular IP address frequently.
- Further investigation of the IP address could show that this employee is accessing an online shopping site during company time, for example.

- Automated software packages, such as Tripwire (www.tripwire.com), can tell you when suspicious network activity has occurred.
- Tripwire is an audit control program that detects anomalies in traffic and sends alerts automatically.

USING NETWORK TOOLS

- A variety of tools are available for network administrators to perform remote shutdowns, monitor device use, and more.
- Tools such as **Splunk** (www.splunk.com), **Spiceworks** (www.spiceworks.com), **Nagios** (www.nagios.org), and **Cacti** (www.cacti.net) help you monitor your network efficiently and thoroughly.
- For example, you can consult records that the tool generates to prove an employee ran a program without permission. You can also monitor your network and shut down machines or processes that could be harmful.

USING PACKET ANALYZERS

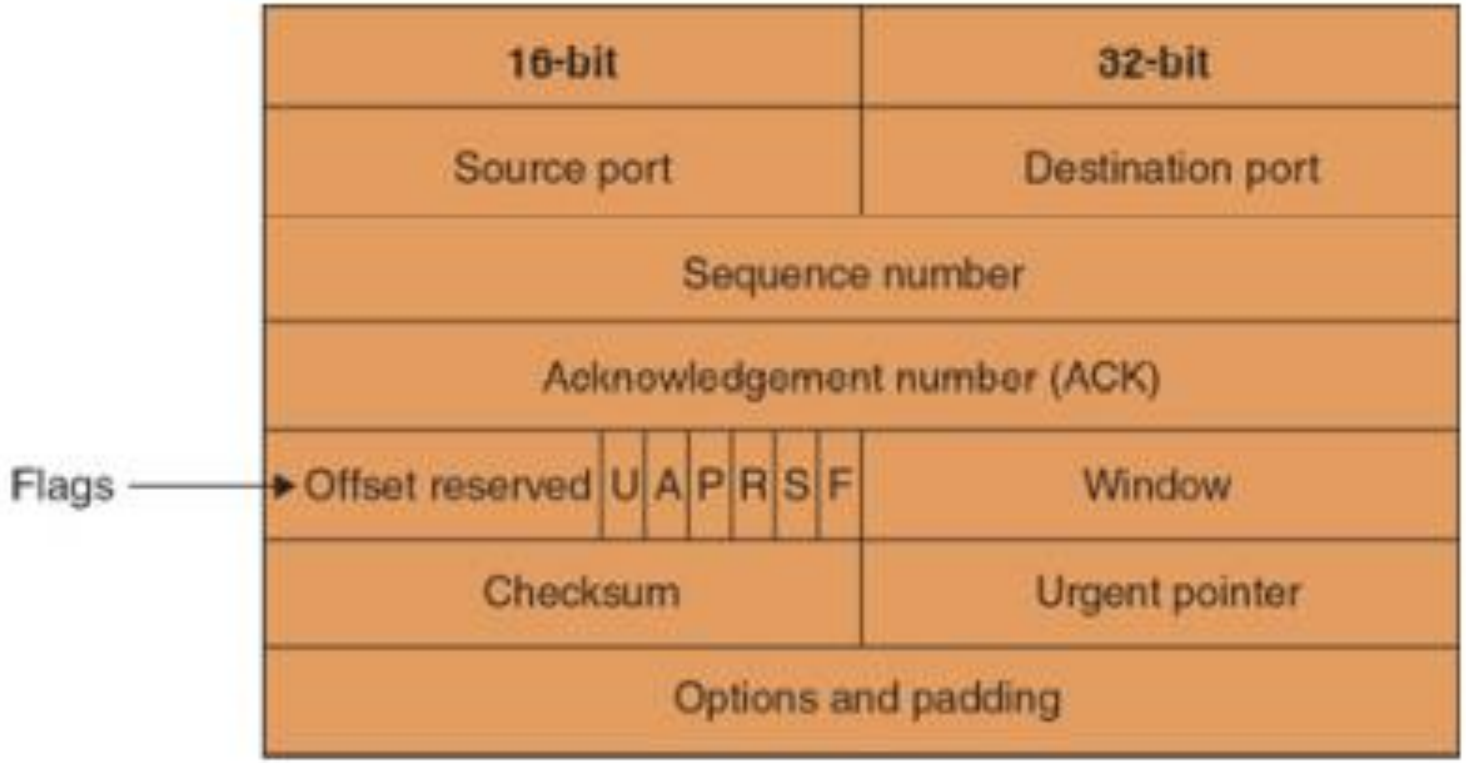
- Packet analyzers are devices or software placed on a network to monitor traffic.
- Most network administrators use them for increasing security and tracking bottlenecks..
- Most packet analyzers work at Layer 2 or 3 of the OSI model.
- To understand what’s happening on a network, often you have to look at the higher layers by using custom software that comes with switches and routers, however.

- Some analyzers perform packet captures, some are used for analysis, and some handle both tasks.
- Windows has many tools capable of capturing and analyzing packets, but you can’t feed the data they collect directly into other tools.
- Most tools can read anything captured in Pcap (packet capture) format.
- Programs such as tcpdump and Wireshark use the Pcap format, for example

EXAMPLE

- As a forensics expert, you must choose the tool that best suits your purposes.
- For example, if your network is being hit with SYN (the synchronize portion of the TCP handshake) flood attacks, you want to find packets with the SYN flag set.
- In a SYN flood attack, the attacker keeps asking your server to establish a connection.

- Although your server can handle thousands of connections, it can handle only a limited number of establishing connections.
- To find these packets, tcpdump and tethereal (a network protocol analyzer) can be programmed to examine TCP headers to find the SYN flag.



16-bit	32-bit
Source port	Destination port
Sequence number	
Acknowledgement number (ACK)	
Offset reserved U A P R S F	Window
Checksum	Urgent pointer
Options and padding	

A TCP header

- A suite of tools called Tcpreplay can be used to replay network traffic recorded in Libpcap format; you use this information to test network devices, such as IDSs, switches, and routers.
- Etherape is a tool for viewing network traffic graphically

WIRESHARK

- Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.

- It is used to track the packets so that each one is filtered to meet our specific needs.
- It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.

- Wireshark is a free to use application which is used to apprehend the data back and forth.
- It is often called as a free packet sniffer computer application.
- It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

USES OF WIRESHARK:

1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.