IA 311: Network Forensics

Lecture 5: Evidence Acquisition

Types of Evidence Acquisition

- Network forensics investigators refer to evidence acquisition as passive or active. That is:
  - Passive evidence acquisition
  - Active evidence acquisition

  - NOTE:
    - Despite the network evidence acquisition approach used by the network forensic investigator, the impact to the environment (the footprint) still exists/happens.

Types of Evidence Acquisition …

- Passive evidence acquisition
  - Is the practice of gathering forensic-quality evidence from networks without emitting data at Layer 2 and above.
    - Traffic acquisition is often classified as passive evidence acquisition.
- Active (on interactive) evidence acquisition
  - Is the practice of collecting evidence by interacting with stations on the network.
    - May include:
      - Logging into network devices via console or through a network interface.
      - Scanning the network ports to determine the current state.

Physical Interception

- Refers to the passive approach of acquiring network traffic by intercepting it as it is transmitted across **cables**, through **air**, or through **network equipment (**such as hubs and switches).
- NOTE:
  - This process can often be performed with very little impact (footprint).
  - The process of capturing traffic is also referred to as sniffing traffic.

Physical Interception …

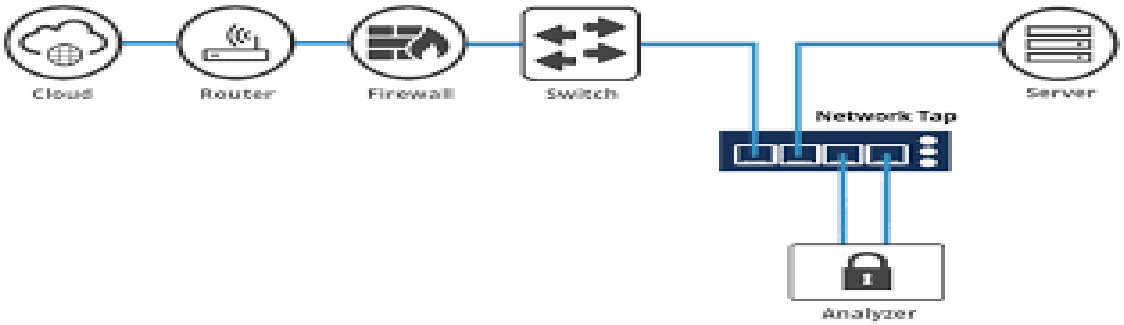
- This (physical interception) can be done via:
  - Cables
    - Copper cables
      - Coaxial
      - Twisted Pair (TP)
    - Optical cables (Fiber Optic Cables)
  - Radio Frequency (through the air)
  - Network equipment
    - Hubs
    - Switches

Traffic interception in cables

- A variety of tools can be used, including:
  - Inline network taps
  - Vampire taps
  - Induction coils

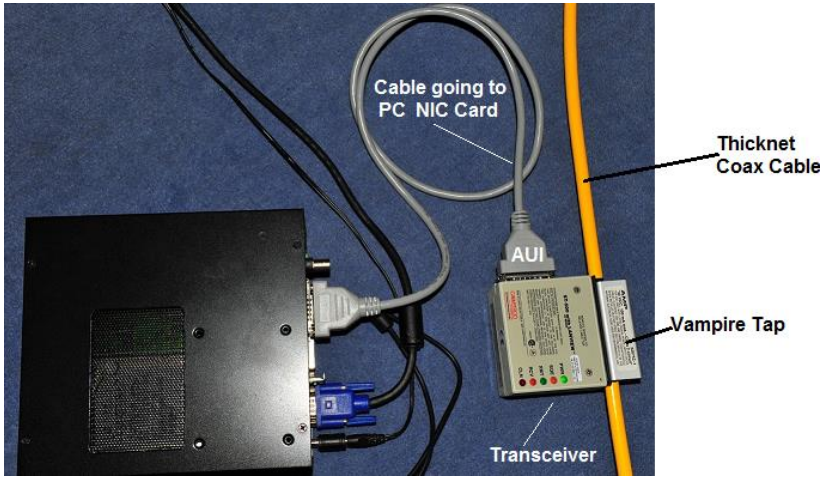
Inline network taps

- An inline network tap is a layer 1 (physical layer) device that can be inserted inline between two physically connected devices, allowing the packets to pass along and also physically replicating the packets to a separate port or multiple ports.
- The network taps usually have four ports - two connected inline to facilitate normal traffic flow, and two sniffing ports(these mirror the traffic – one for each direction).
- Insertion of the inline network tap usually causes a small disruption (as the cable must be separated to achieve the tap).
- Inline network taps can be applied to copper and fiber optic cables.



Vampire taps

- Refers to devices that pierce the shielding of copper wires in order to access the signal (traffic) within.
- This is as opposed to inline network tap, here the cable does not need to be separated for a vampire tap to be installed.
- The vampire tap, pierces/bites into the target cable, hence the name **vampire**.





Induction coils

- Induction coils are devices that transform the magnetism of weak signals to induce a much stronger signal in an external system.
  - Wires conducting voltages emit various electromagnetic signals outside of the intended channel.
  - Such electromagnetic radiation is more pronounced in unshielded wires such as UTP – this makes it possible to use an induction coil alongside such wires so as to translate the emitted signals into their original digital form.

Radio Frequency

- Since the 1990s, this approach has become an increasingly popular approach for transmission of data.
  - The RF waves travel through air – by nature this is a shared medium.
    - As a result the transmitted traffic can be observed and intercepted by all devices within range, making passive traffic acquisition very easy, both for investigators and attackers.

Radio Frequency …

- Take home clues to investigators:
  - The target of investigation may be able to access the Wireless LAN (WLAN) from a long distance, far outside the physical borders of a facility.
  - When one connects over wireless links, his/her activity can potentially be monitored from a great distance.
- Sometimes the transmitted traffic is encrypted:
  - Usually, there is commonly a single pre-shared key (PSK) for all stations.
    - Anyone who gains access to the encryption key can listen to all traffic relating to all stations involved.
    - It is also possible to passively capture encrypted Wi-Fi traffic and decrypt it offline later using the encryption keys.
      - Then, the investigator (*or attacker*) can analyse the decrypted data in the same manner as any other unencrypted network traffic.

Radio Frequency …

- Whether the 802.11 traffic is encrypted or not, one can gain a great amount of information by capturing and analysing the traffic. The traffic commonly includes:
  - Broadcast SSIDs (Service Set Identifiers)
  - WAP (Wireless Access Point) MAC addresses
  - Supported encryption/authentication algorithms
  - Associated client MAC addresses
  - In many cases, the full Layer 3+ packet contents
  - NOTE:
    - 802.11 shortly refers to an IEEE specification standard for implementation of wireless local area networks.

Radio Frequency …

- To capture wireless traffic, one needs the necessary hardware.
  - One can use commercial 802.11 network adapters for this purpose.
  - Examples include:
    - **AirPcap** USB adapter (Manufactured by Riverbed Technology)
      - This supports AirPcap tool on Windows OS.



    - **OpiPcap**
      - This is the alternative to the expensive AirPcap option.

Hubs

- They are unintelligent/dumb layer 1 devices that physically connect all devices on a network segment to one circuit.
  - It does not store enough information about what devices are connected to it or how.
  - Simply put: When a hub receives a frame, it retransmits it to all other ports.
    - That is, every device physically connected to the hub receives all the frames destined to every other device connected to the hub.
  - NOTE:
    - Currently, many devices labeled as hubs by the manufacturer are actually switches.
      - As an investigator/security expert, you should be able to identify which is which, so as to take advantage of hubs in the target network.

Hubs …

- Capturing network traffic using hubs:
  - Since the hub retransmits received frames to all devices physically connected to it – as an investigator, one can use one of the machines physically connected to the hub to capture the network segment's network traffic.
  - NOTE:
    - This should be used as an option only if a hub exists in the target network.
    - For security reasons, It is not recommended to install a hub in a network for the purpose of capturing network traffic.
      - This is because any (compromised) machine can be used to monitor the network segment.
        - » Any network traffic sent/received by every machine on the network segment can be seen and passively captured.

Switches

- These are the most common layer 2 devices.
- Like hubs, they connect multiple devices together to form a network segment or a LAN.
  - But, as opposed to hubs, switches use software to keep track of which devices are connected to which ports in its Content Addressable Memory (CAM) table.
    - The CAM table stores the devices' MAC addresses with corresponding switch ports.
    - When a switch receives a packet, it forwards it only to the destination device's port.
      - Individual devices do not physically receive each other's traffic.

Switches …

- Obtaining network traffic from switches:
  - Investigators can (and often do) capture network traffic by using switches.
    - This can be done by using switches that have sufficient software capabilities.
      - They can be configured to replicate traffic from one or more ports to other ports for aggregation and analysis.
        - » The terminologies used by Cisco for this capability is Switched Port Analyzer (SPAN) and Remote Switched Port Analyzer (RSPAN).
        - » The most vendor neutral term for this capability is **port mirroring**.
      - NOTE:
        - » Switches have varying mirroring capabilities.
          - You can not mirror four ports of an average of 50 Mbps each to one port, on a 100 Mbps switch – this is similar to making 100 Kg truck to carry 200 Kg – this is called **oversubscription** (some of mirrored packets will be dropped by the switch).

Switches …

- Once you have mirrored traffic from the ports of interest – you can connect a sniffer to the mirroring port and capture all of the traffic.
  - To accomplish such configuration (port mirroring), you should have administrative privileges.
- In some instances one can capture network traffic using switches without having administrative privileges:
  - Though not safest methods, these can be used by investigators in scenarios where the administrator is not trusted.
    - This can be done via the following attacks:
      - » MAC flooding
      - » ARP spoofing
    - Task: Read and be able to provide a short summary of each of these kinds of attacks.

Traffic Acquisition Software

- After getting physical access to network traffic, one needs software for recording and analyzing it.
  - The most common software libraries for such a purpose are:
    - Libpcap
    - WinPcap
  - The tools that are based on these libraries include:
    - TCPdump
    - Wireshark

Traffic Acquisition Software …

- Currently, the most popular packet sniffing and analysis tools are based on the libpcap libraries.
- As a result the tools are interoperable.
    - Packets captured by one tool can be read and analyzed by another tool.

Traffic Acquisition Software …

- Most libpcap based tools include specialized functionality, these include:
  - Ability to merge packet captures (i.e. mergecap)
  - Ability to split a capture up by TCP streams (i.e. tcpflow)
  - Ability to do regular expression searches on packet contents (i.e. ngrep)

Libpcap

- Its is a UNIX C library that provides an API for capturing and filtering data link layer frames from arbitrary (different) interfaces.
  - Previously, there were different distributions of UNIX OS, the need to inspect link-layer frames required distribution specific solutions to be developed to achieve the task.
  - libpcap solved the problem.
    - It provided a layer of abstraction that programmers could use to design portable packet capture and analysis tools.
    - It was initially released in 1994.

WinPcap

- It is a software library based on libpcap that was designed for Windows systems.
- It was published in 1999 by the Computer Networks Group (NetGroup).
  - The WinPcap project is now hosted by a site maintained by the **Riverbed Technology** (which is also the commercial sponsor of **Wireshark**).

The Berkeley Packet Filter (BPF) Language

- It is an extremely powerful filtering language included in libpcap.
  - In modern times, huge amounts of data tend to flow through networks - this language can be used by investigators to filter network traffic during captures and analysis.
    - By using BPF filters one can decide which traffic to capture and inspect and which traffic to ignore.
    - BPF allows one to filter traffic based on value comparisons in fields for Layer 2, 3 and 4 protocols.
  - BPF is widely used and supported by traffic capture and analysis tools.
    - Therefore, it is important for the network investigators be familiar with it.

TCPdump

- It is a tool for network traffic capturing, filtering and analysis.
  - It was designed as a UNIX tool.
- There are two ways in which tcpdump is most commonly used:
  - For on-the-fly analysis
    - This is for troubleshooting network issues.
      - It usually involves traffic capturing, filtering and analysis all performed simultaneously.
        - » This is suitable only when a quick glance at the data is needed.
  - For capturing traffic of interest passing on a target segment.
    - This is usually done over a longer period of time, whereby traffic is stored for offline analysis (+ even future correlation with other data).

TCPdump …

- Fidelity
  - Fidelity is similar to reliability, trustworthiness.
  - It is because of fidelity that tcpdump is said to be a powerful tool.
    - It is able to capture network traffic with high fidelity to an extent that the resulting packet capture can be used as evidence admissible in a court.
      - However the quality of the packet capture can be impacted by **hardware limitations** and **configuration constraints**.
        - » Hardware limitations example 01:
          - The clock speed of the processor (of the capturing machine) can limit tcpdump's packet capturing ability.
            - Packet capturing is a CPU-intensive activity – if the CPU is highly utilized it might eventually drop packets – thus some packets won't be captured.

TCPdump …

- Fidelity
  - Hardware limitations:
    - The clock speed of the processor (of the capturing machine) can limit tcpdump's packet capturing ability.
      - If the issue is just to get a sample of the network traffic , then this won't be much of an issue.
      - This would however be a critical issue if the goal is to get a high fidelity capture of the ongoing network traffic.
    - Disk space of the capturing machine
      - There should be sufficient disk space to store the traffic being captured.
      - To deal with this issue, it may be necessary to either filter traffic upon capture or provide more disk space.

TCPdump …

- tcpdump

```
# tcpdump -D

 1.eth0
2.eth1
3.usbmon1 (USB bus number 1)
4.usbmon2 (USB bus number 2)
5.usbmon3 (USB bus number 3)
```

```
# tcpdump -w 0001.pcap -i eth0

tcpdump: listening on eth0, link
4 packets captured
4 packets received by filter
0 packets dropped by kernel
```

```
# tcpdump -i eth0 port 22

tcpdump: verbose output suppressed, u
listening on eth0, link-type EN10MB (
10:37:49.056927 IP 192.168.0.2.ssh >
10:37:49.196436 IP 192.168.0.2.ssh >
10:37:49.196615 IP 192.168.0.1.nokia-
10:37:49.379298 IP 192.168.0.2.ssh >
10:37:49.381080 IP 192.168.0.2.ssh >
```

```
# tcpdump -c 5 -i eth0

tcpdump: verbose output suppr
listening on eth0, link-type
11:40:20.281355 IP 172.16.25.
11:40:20.281586 IP 172.16.25.
```

Wireshark (originally Ethereal) …

- It is a graphical (GUI), open source tool designed for capturing, filtering and analyzing network traffic.
  - A very good tool for beginner network forensics analysts.
  - Meanwhile it has great and extremely useful capabilities for experienced investigators.
  - One can use wireshark to capture packets from any system network interface provided that:
    - One has appropriate permissions and
    - The associate network card supports sniffing
  - Wireshark can display packets as they are captured in real time.
  - It is a very powerful protocol analyzer and uses a lot of processing power to achieve this.
    - NOTE:
      - Remember about the tcpdump load on CPU + packet loss/dropping.

Wireshark (originally Ethereal) …

- Wireshark capturing modes:
  - Promiscuous mode
  - Monitor mode
- Wireshark filter types:
  - Capture filters
  - Display filters

Wireshark (originally Ethereal) …

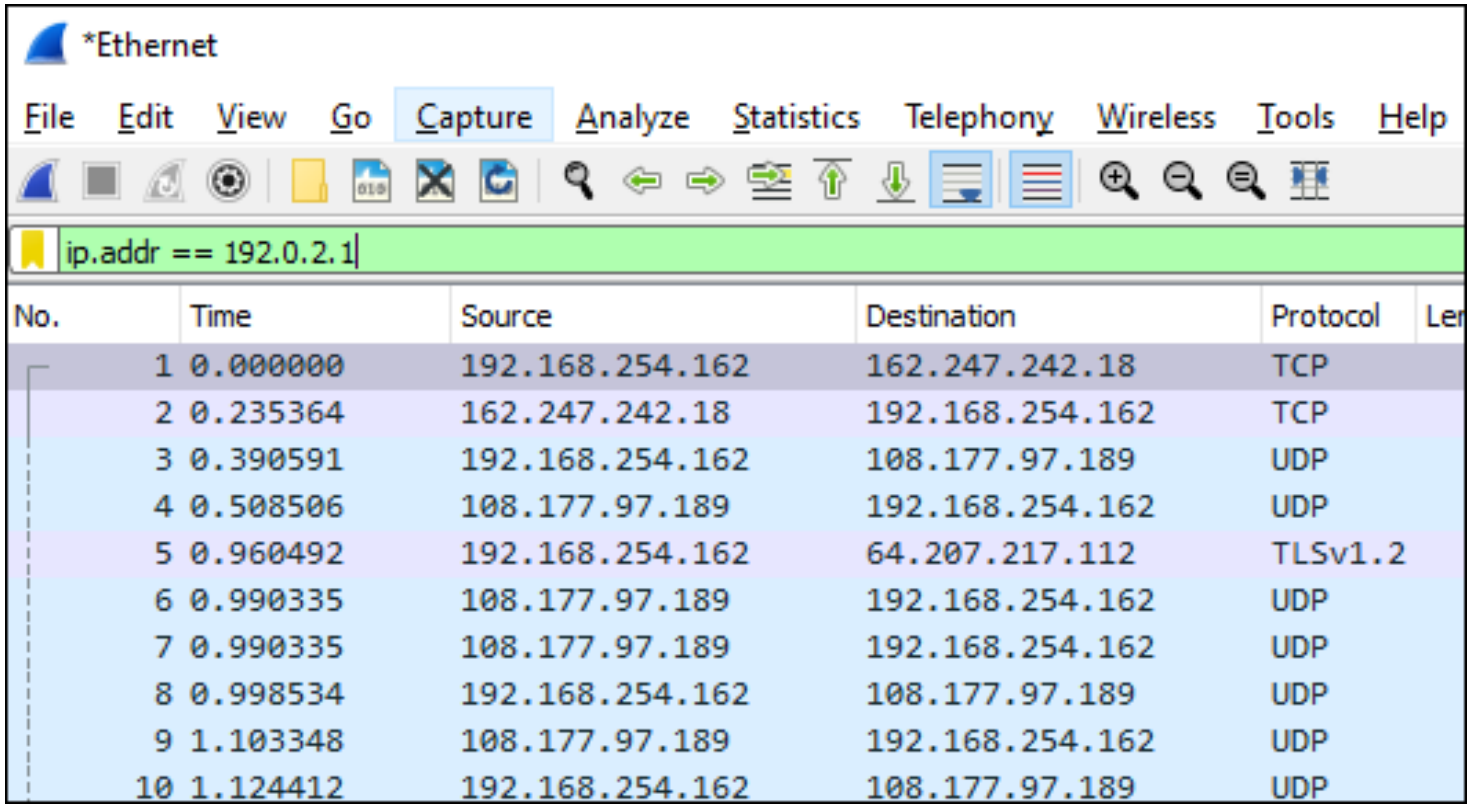
- Display filters examples:
  - Filter by IP address - displays all traffic from IP, be it source or destination
    - ip.addr == 192.168.1.1
  - Filter by source address - display traffic only from IP source
    - ip.src == 192.168.0.1
  - Filter by destination - display traffic only form IP destination
    - ip.dst == 192.168.0.1
  - Exclude IP address: remove traffic from and to IP address
    - !ip.addr ==192.168.0.1
  - Filter by MAC
    - eth.addr = 00:50:7f:c5:b6:78

Wireshark (originally Ethereal) …

- Display filters examples:
  - Filter TCP port
    - tcp.port == 80
  - Filter TCP port source
    - tcp.srcport == 80
  - Filter TCP port destination
    - tcp.dstport == 80
  - Find user agents
    - http.user_agent contains Firefox
  - Filter all http get requests
    - http.request
  - Filter all http get requests and responses
    - http.request or http.response

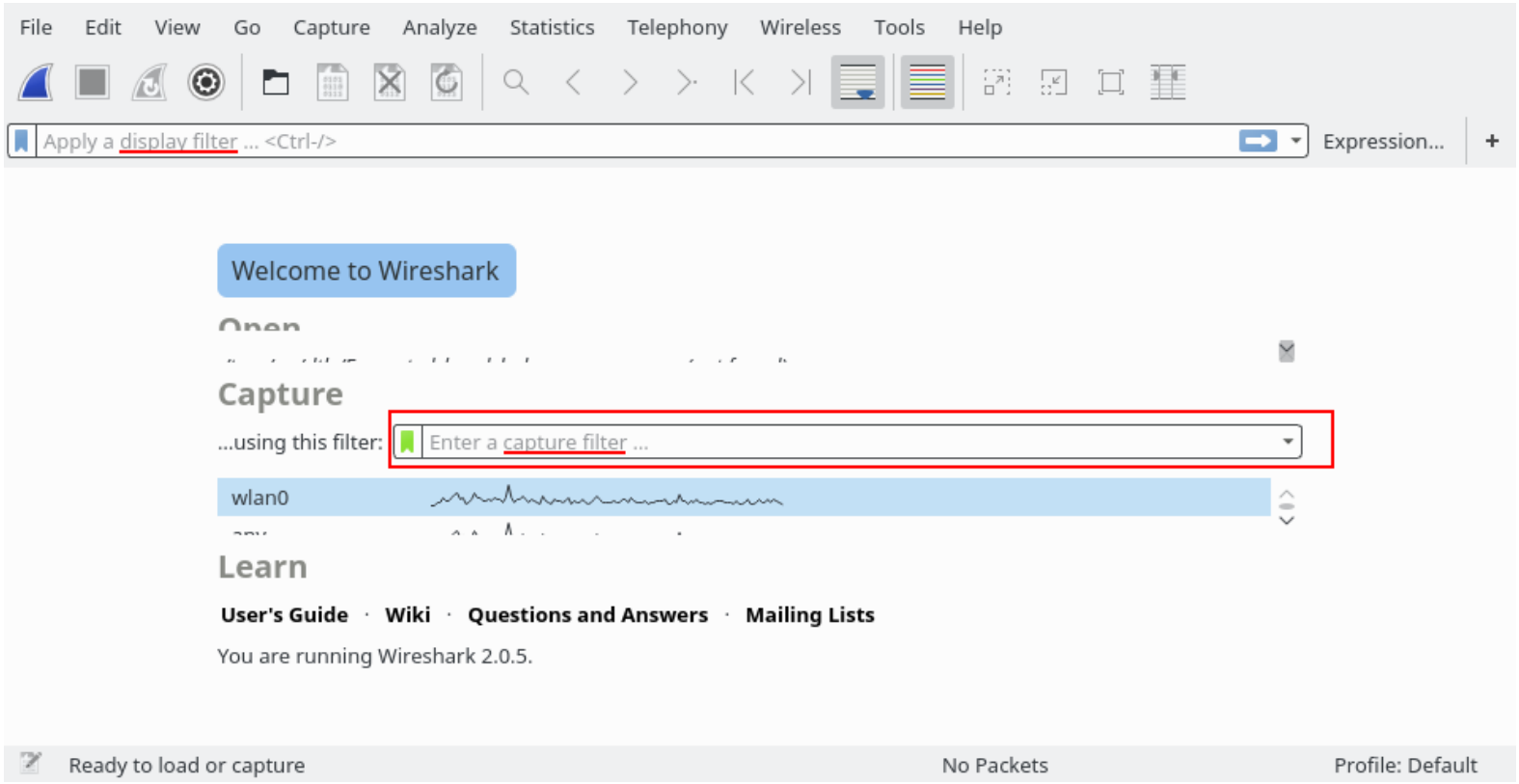
Wireshark (originally Ethereal) …

– Display filters examples:



Wireshark (originally Ethereal) …

– **Display** filters Vs. **Capture** filters



Wireshark (originally Ethereal) …

- Capture filters examples:
  - Capture only traffic to or from IP address 172.18.5.4:
    - host 172.18.5.4
  - Capture only DNS (port 53) traffic:
    - port 53
  - Capture except all ARP and DNS traffic:
    - port not 53 and not arp

tshark

- This is a command-line network protocol analysis tool that is part of the wireshark distribution.
  - It is libcap based (similar to wireshark).
  - It can read and save files in the same standard formats as wireshark.
  - It can be used not only for analysis, but for capturing packets as well.

dumpcap

- This is a command-line tool specifically designed for capturing packets, and comes in the wireshark distribution.
  - One is advised to use dumpcap for packet capturing, in case one is intending to use the wireshark distribution to perform an investigation.
    - Since it is specifically designed for packet capturing, it takes up fewer resources thereby maximizing capturing capabilities.

Recall: Active evidence acquisition

- It is the practice of collecting evidence by interacting with stations on the network.
  - This might involve gathering of evidence from network devices including firewalls, web proxies, logging servers, …
    - It is usually not possible to remove such devices from a network without causing serious damage to business operations.
    - Eventually, the evidence must be collected while the devices are live and on the network.
  - NOTE:
    - Active evidence acquisition modifies the environment (leaves footprints).
      - » The investigator should be highly aware of the various ways in which active evidence acquisition modifies the devices and the environment and work to minimize the impact.

Active Evidence Acquisition

- In active evidence acquisition, there is a number of common ways through which an investigator can gain access to live network-based devices.
  - This is through the use of common interfaces, these include:
    - Console
    - Secure shell (SSH)
    - Secure copy (SCP) and SSH File Transfer Protocol (SFTP)
    - Telnet
    - Simple Network Management Protocol (SNMP)
    - Trivial File Transfer Protocol (TFTP)
    - Web and proprietary interfaces

Active Evidence Acquisition …

- Inspection without Access
  - This is an approach of gaining information about a network device's configuration or state without accessing the device at all via an interface.
    - It can be due to a situation whereby the password to user interface in not available.
  - NOTE:
    - Gathering of extensive information about a device's configuration and state can be achieve through external inspection by using port scanning, vulnerability scanning and other methods.

Active Evidence Acquisition …

- Inspection without Access:
  - Port Scanning
    - Can use a tool like nmap.
      - Nmap is an effective tool for obtaining information about open ports and software versions of a device.
      - NOTE:
        - » Port scanning is an active process (as it will generate network traffic) and will therefore modify the state of the target device.
  - Vulnerability Scanning
    - This is the next level of active external inspection.
      - Vulnerability scanners test target systems for a wide variety of known vulnerabilities.
      - This approach also modifies the state of the target device, and it can even crash the target device.
        - » One is advised to be cautious (careful) in using this option.

Strategy

- Some tips for collecting evidence from network devices.
  - Goal:
    - To preserve evidence while minimizing investigators' footprint throughout the environment.
    - NOTE: The strategy might vary for each investigation.
- Tips:
  - Refrain from rebooting or powering down the device.
  - Connect via the console rather than over the network.
  - Record the system time.
  - Collect evidence according to level of volatility.
  - Record your investigative activities.

Strategy …

- Tips:
  - Refrain from rebooting or powering down the device.
    - A lot of network based evidence exists as volatile data in the memory of network devices.
      - Such data would not survive a reboot of the network device.
        - » Make sure that you capture all the volatile evidence you need before allowing the device to be rebooted.
  - Connect via the console rather than over the network.
    - Its is advised to connect via console rather than over the network.
      - Connecting over the network will generate network traffic which will eventually modify the state of the network devices' network connections.
        - » Connecting over the network might also alert an attacker on the network of your presence.
          - Connecting instead directly to the system console will minimize your network footprint.

Strategy …

- Tips:
  - Record the system time.
    - Always check to see what the time skew is between the network device you are investigating and a reliable source.
      - Even a small time skew can make it very difficult to correlate evidence.
        - » If you have access to a network device for an extended period of time, it is a good idea to collect the time at regular intervals because the time skew may change.
  - Collect evidence according to level of volatility.
    - This is a general rule of thumb for all digital forensic investigations:
      - *Collect the most volatile evidence first and work your way down to more persistent evidence*.
    - Reason:
      - This will increase your chances of capturing all the evidence you are after.

Strategy …

- Tips:
  - Record your investigative activities.
    - Record the interactions you made with the systems and network devises.
    - If one connects via a command line interface, one can record the commands using utilities such as “screen” or “script”.
      - These tools can help you clearly delineate/identify what footprints were the result of your own activities and what were those of the existing system.
  - NOTE:
    - As an investigator, one will always leave footprints.
      - The more places one looks for evidence, the more footprints one will leave.
        - » Fortunately, there are ways that you can minimize your impact on the environment.