Week 11: Network Forensics

Ayman El Hajjar

Email: a.elhajjar@westminster.ac.uk
Twitter: @azelhajjar

6COSC002W - Security and Forensics

29 March 2021

University of Westminster

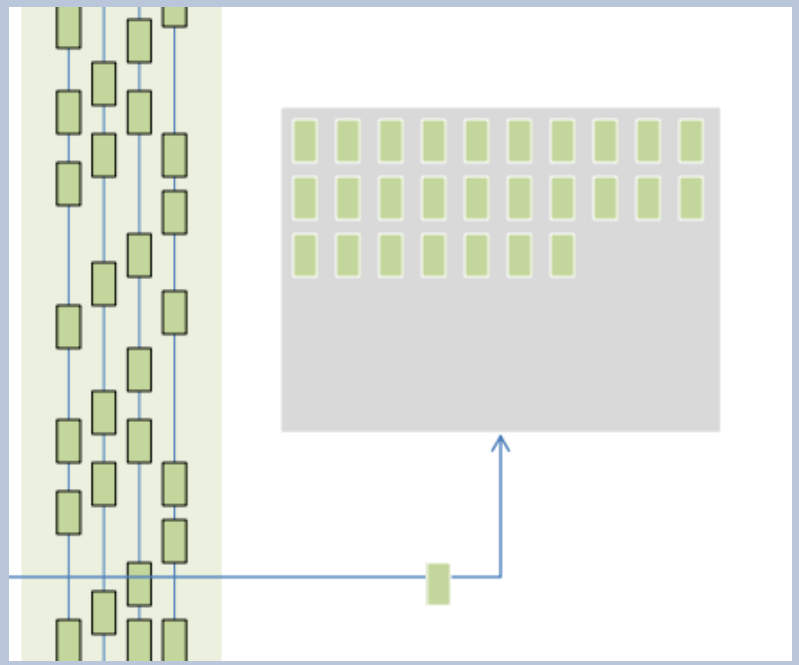
Session Overview

1. Network forensics methodologies
2. Sources of Network based evidence

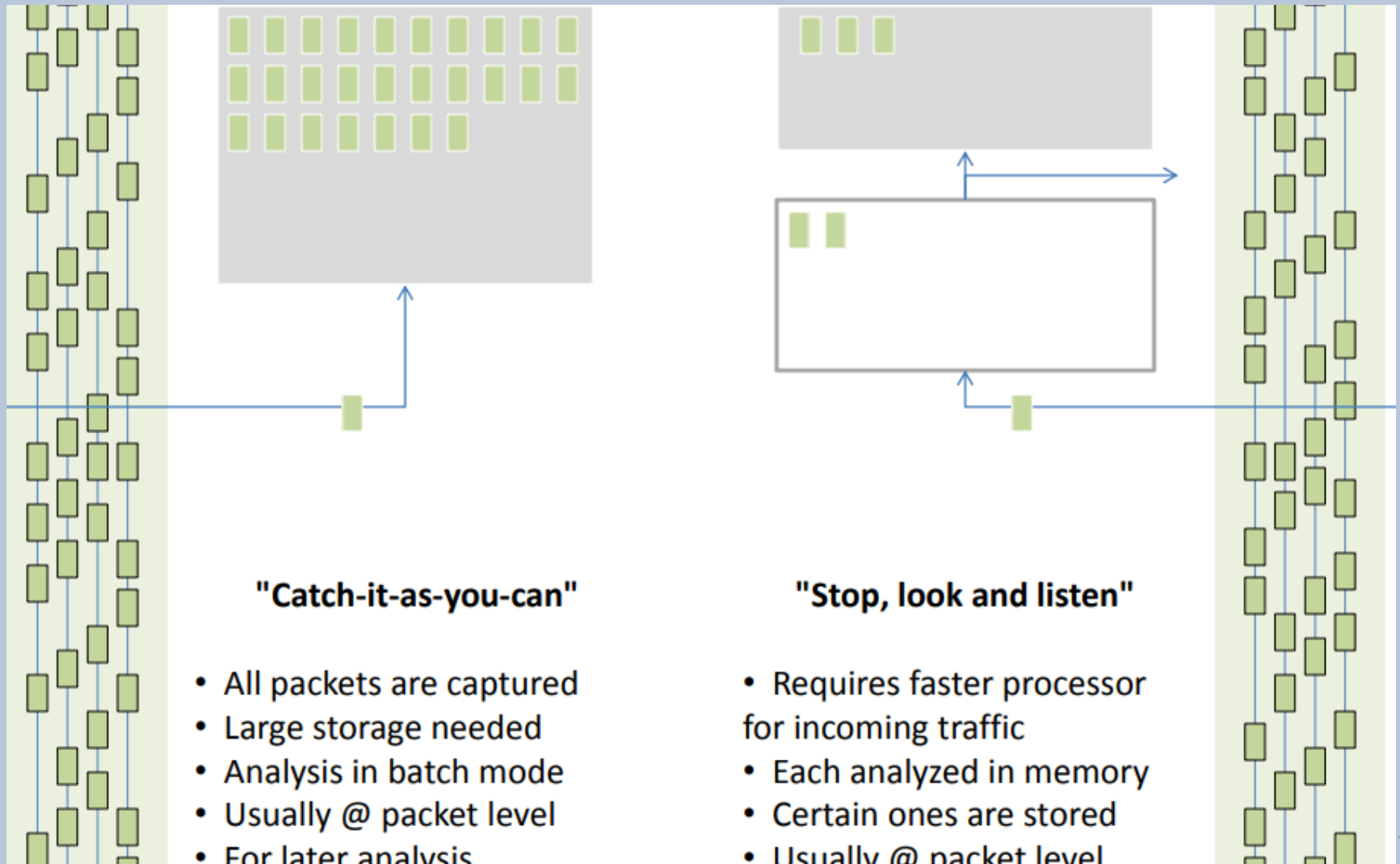
Network Forensics

What is Network forensics

Network forensics is categorized as a single branch of digital forensics; it includes the areas of monitoring and analyzing computer network traffic and allows individuals to gather information, compile evidence, and/or detect intrusions



Network forensics methods



"Catch-it-as-you-can"

- All packets are captured
- Large storage needed
- Analysis in batch mode
- Usually @ packet level
- For later analysis

"Stop, look and listen"

- Requires faster processor for incoming traffic
- Each analyzed in memory
- Certain ones are stored
- Usually @ packet level

007 characteristics in the network world

- In 007's world, everything begins with a trigger. The trigger is an event or incident that alerts the organization about unsavoury activities by persons known or unknown..
- This could be reactive or proactive.
- The investigator initiates a full-fledged information/evidence collection exercise using every sort of high-end technology available
- The evidence collection may be done from network traffic, endpoint device memory, and hard drives of compromised computers or devices.
- The information collected is carefully and painstakingly analysed with a view to extract evidence relating to the incident to help answer questions, as shown in the following diagram:

007 characteristics in the network world

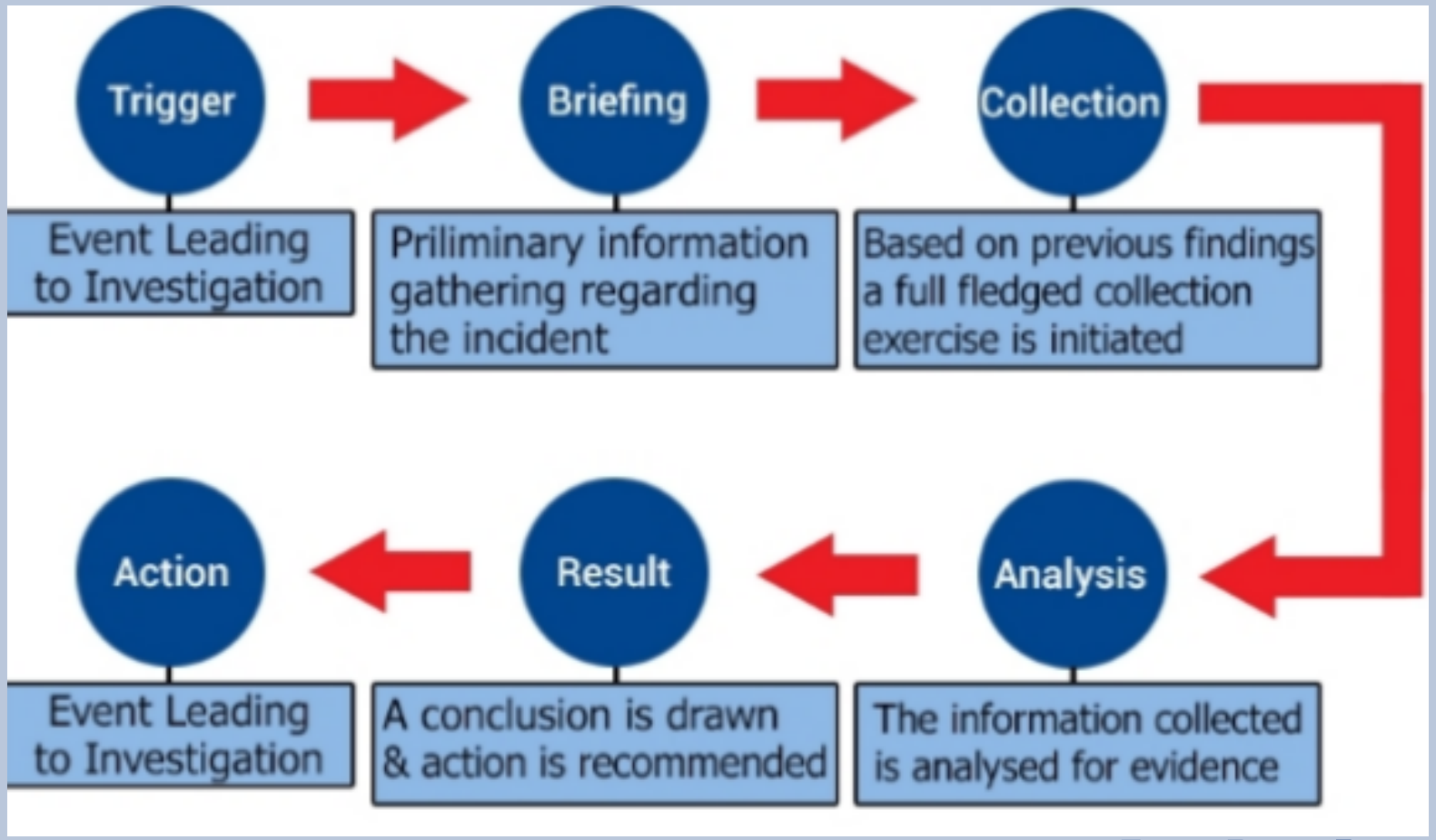
- The information collected is carefully and painstakingly analysed with a view to extract evidence relating to the incident to help answer questions, as shown in the following diagram:

007 characteristics in the network world

- An attempt is made to answer the following critical questions:
  - Who is behind the incident?
  - What actually happened?
  - When did it happen?
  - Where was the impact felt? Or which resources were compromised?
  - Why was it done?
  - How was it done?
- Based on the analysis result, a conclusion is drawn and certain recommendations are made.
- These recommendations result in an action.
- The action may include remediation, strengthening of defences, employee/insider termination, prosecution of suspects, and so on based on the objectives of the investigation.

Actions and recommendations process

- The following flow diagram neatly sums up the complete process:

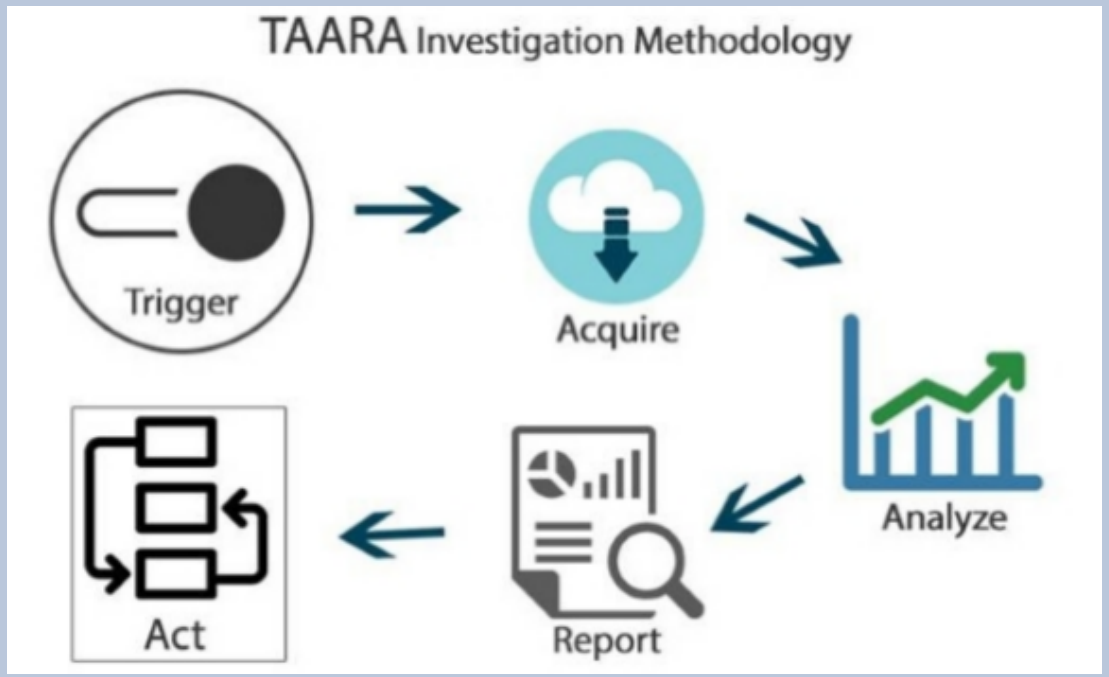


Satisfactory completion of case

- Network forensic investigations can be very time consuming and complex.
- These investigations are usually very sensitive in nature and can be extremely time critical as well.
- To be an effective network forensics Bond, we need to develop the following characteristics:
  - Preparation
  - Information gathering/evidence gathering
  - Understanding of human nature
  - Instant action
  - use of technology
  - Deductive reasoning

The TAARA methodology for network forensics

- There is a considerable overlap between incident response and network forensics in the corporate world, with information security professionals being tasked with both the roles.
- To help simplify the understanding of the process, we have come up with the easy-to-remember TAARA framework:



The TAARA methodology is composed off:

- Trigger: This is the incident that leads to the investigation.
- Acquire: This is a predefined incident response plan—and it involves identifying, acquiring, and collecting information and evidence relating to the incident.
- Analysis: All the evidence that is collected so far is collated, correlated, and analysed. The sequence of events is identified.
- Report: Based on the preceding analysis, a report is produced before the stakeholders in order to determine the next course of action.
- Action: The action recommended in the report is usually implemented during this stage.

Sources of Network-Based Evidence

- Every environment is unique. However similarities in network equipment and common design strategies for network infrastructure exist.
- There are many sources of network-based evidence in any environment, including routers, web proxies, intrusion detection systems, and more.
  - How useful is the evidence on each device?
  - This varies depending on the type of investigation, the configuration of the specific device, and the topology of the environment.

Evidence on the wire

- Physical cabling is used to provide connectivity between stations on a LAN and the local switches, as well as between switches and routers.
- Network cabling typically consists of copper, in the form of either twisted pair (TP) or coaxial cable.
- Both copper and fibre-optic mediums support digital signalling.

Forensics value

- Network forensic investigators can tap into physical cabling to copy and preserve network traffic as it is transmitted across the line.
- Two types of taps exist:
  - vampire tamps: Puncture the insulation and conncet to wire
  - Infrastructure taps, Replicate signals to a passive station without degrading the original signal.

Evidence in the Air

- An increasingly popular way to transmit station-to-station signals is via "wireless" networking, which consists of radio frequency (RF)
- The wireless medium has made networks very easy to set up.
- As a result, enterprises and home users can deploy wireless networks without the expense and hassle of installing cables

Forensics value

- Wireless access points broadcast all signals so that any station within range can receive them.
- As a result, it is often trivial for investigators to gain access to traffic traversing a wireless network.
- Investigators can still gather a lot of information from encrypted wireless networks.

Evidence in the Router

- Routers connect different subnets or networks together and facilitate transmission of packets between different network.
- Routers add a layer of abstraction that enables stations on one LAN to send traffic destined for stations on another LAN.
- Internetworking using routers allows the entire global Internet to happen thorugh a complex multilayer web of routers.

Forensics value

- Routers have routing tables.
- Routing tables map ports on the router to the networks that they connect.
- This allows a forensic investigator to trace the path that network traffic takes to traverse multiple networks.

Evidence in the authentication servers

- Authentication servers are designed to provide centralized authentication services to users throughout an organization.
- This allows enterprises to streamline account provisioning and audit tasks.

Forensics value

- Authentication servers typically log successful and/or failed login attempts and other related events.
- Investigators can analyse authentication logs to identify
  - brute-force password-guessing attacks
  - account logins at suspicious hours or unusual locations
  - unexpected privileged logins, which may indicate questionable activities.

Evidence in the Central log servers

- Central log servers aggregate event logs from a wide variety of sources, such as authentication servers, web proxies, firewalls, and more.
- Individual servers are configured to send logs to the central log server, where they can be timestamped, correlated, and analysed by automated tools and humans far more easily than if they resided on disparate systems.

Forensics value

- Central log servers are designed to help security professionals identify and respond to network security incidents.
- Even if an individual server is compromised, logs originating from it may remain intact on the central log server.

Evidence in the firewall

- Firewalls are specialized routers designed to perform deeper inspection of network traffic in order to make more intelligent decisions as to what traffic should be forwarded and what traffic should be logged or dropped.
- Modern firewalls are designed to make decisions based not only on source and destination IP addresses, but also based on the packet payloads, port numbers, and encapsulated protocols.

Forensics value

- Firewalls can be configured to produce alerts and log allowed or denied traffic, system configuration changes, errors, and a variety of other events.
- These logs can help operators manage the network and also serve as evidence for forensic analysts

Identifying sources of evidence

- For any successful investigation, it is extremely important to successfully collect, collate, preserve, and analyze the evidence.
- To begin with, we need to identify the sources of evidence for any investigation.
- The sources of evidence can be easily divided into the following two categories
  - Evidence obtainable from within the network
  - Evidence from outside the network

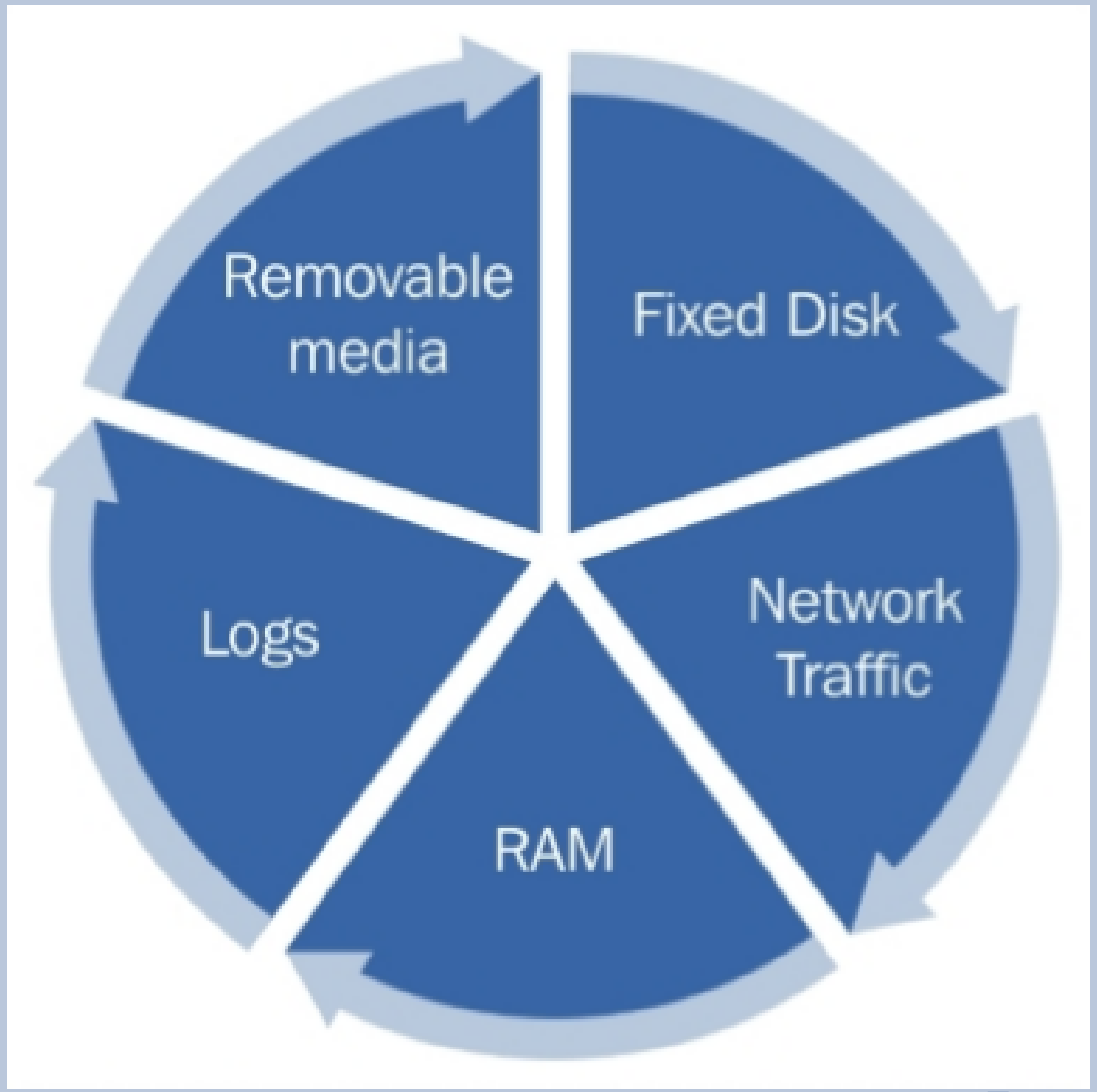
Evidence obtainable from within the network

- Evidence from network & device logs:
  - A log is a record of all the activities and outcomes performed by a device or by outside agents on a device.
  - Al the incoming or outgoing events are logged on a system.
  - Logs are a crucial part of the investigation ecosystem.
  - Devices such as firewalls, intrusion prevention and detection systems, anti-virus servers, and so on generate logs. Other logs include operating system event logs, application logs, and so on
- Network traffic
  - Network traffic is transmitted in packets.
  - The data is split up and transmitted in the form of packets that need to be captured and reconstructed for analysis

Evidence obtainable from within the network

- Memory of the individual computers under investigation
  - Volatile memory can be a valuable source of evidence. A lot of malware may only reside in the memory of a computer, which is under investigation.
  - Computers with whole disk encryption (WDE) may save the key on a USB stick and the key will only be accessible to the investigator if it is grabbed from the volatile memory.
- Evidence residing on the hard drives of individual computers under investigation
  - Substantial evidential data resides on the hard drives of compromised computers.
  - Traces of internet activity, web mail communications, efforts to cover tracks and obfuscate evidence, and so on will all be found post an investigation of hard drive contents.

Evidence obtainable from within the network



Evidence from outside the network

- Internet service provider (ISP) logs
  - These logs are a detailed record of access to various Internet resources that are provided by the ISP.
  - This can include details related to log on, log off, user names, resources accessed, online content, online activity, IP addresses, date and time of usage, as well as the duration of usage.
- Evidence on mobile devices
  - When hand-held devices such as phones or tablets are used to access network resources, evidence of their interaction is created on these devices.
  - This too may be required from an investigation perspective.

Challenges Relating to Network Evidence

- Network-based evidence poses special challenges in several areas. below are some of them:
- Acquisition
  - It can be difficult to locate specific evidence in a network environment.
  - Networks contain so many possible sources of evidence that sometimes pinpointing the correct location of the evidence is tricky.
  - Difficulty gaining access to it for political or technical reasons
- Content
  - Network devices may or may not store evidence with the level of granularity desired.
  - Network devices often have very limited storage capacity.

Challenges Relating to Network Evidence

- Storage
  - Storage Network devices commonly do not employ secondary or persistent storage.
  - The data they contain may be so volatile as to not survive a reset of the device.
- Privacy
  - Depending on jurisdiction, there may be legal issues involving personal privacy that are unique to network-based acquisition technique
- Seizure
  - seizing a network device can be much more disruptive than seizing a hard drive.
  - In the most extreme cases, an entire network segment may be brought down indefinitely.

References

- Network forensics by Ric Messier (Website link for book)
- Infosec resources (Infosec resources website)