

Digital Forensic and Investigation

A person in a grey suit is holding a magnifying glass over a tablet. The tablet screen displays binary code (0s and 1s) in various colors (red, blue, yellow). The background is dark with floating binary code and small square icons.

Sierra States University

[illegible]

Characteristics of network forensic

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 effective in network forensics, the following characteristics need to be developed;

- **Preparation:** The preparation stage is essential to ultimately arrive at a satisfactory conclusion of a case. A calm thought-out response with a proper evidence-collection process comes from extensive training and the knowledge of what to do in the event of the occurrence of most likely scenarios that are happening in the real world.

Trained personnel with the necessary tools and processes should be available to tackle any contingency. Just as organizations carry out fire drills on a regular basis, incident response drills should be institutionalized as part of the organization policy.

A situation where the investigator is unable to identify a compromised system could lead to years of data theft, resulting in bleeding of the organization and its ultimate and untimely demise. A scenario where an investigator is able to identify the problem but is unable to decide what action to take is equally bad. This is where preparation comes in. The key is knowing what to do in most situations.

Characteristics of network forensic (cont'd)

- **Information gathering/evidence gathering:** A comprehensive system to monitor network events & activity, store logs, and back them up is essential. Different inputs are generated by different event logging tools, firewalls, intrusion prevention & detection systems, and so on. These need to be stored and/or backed up at a secure location in order to prevent incidental or intentional tampering.
- **Understanding of human nature:** An understanding of human nature is critical. This helps the investigator to identify the motive to the attack, and anticipate and preempt the opponent's next move.
- **Instant action:** Based on the preparations done and the incident response planned, immediate action must be taken when a network compromise is suspected. Questions such as “Should the system be taken off the network?” or “Should we isolate it from the network and see what is going on?” , Should be already decided upon at the planning stage. At this stage, time is of essence and immediate action is required.

Characteristics of network forensic (cont'd)

- **Use of technology:** An investigator should have possess hands-on skill-sets. However, a thorough knowledge of the tools is a must. A number of hi-tech surveillance tools play an important role in network-based investigations. Specialized tools monitor network traffic, identify and retrieve hidden and cloaked data, analyze and visualize network logs and activities, and zero in on in-memory programs and malicious software and tools used by the bad guys.
- **Deductive reasoning:** A logical thought process, the ability to reason through all the steps involved, and the desire to see the case to its rightful conclusion are the skills that need in digital forensics. Questioning all the assumptions, questioning the unquestionable, understanding cause and effect, examining the likelihood of an event occurring, and so on are the hallmarks of an evolved investigator.

This page left blank intentionally

TAARA Framework

- **Trigger:** This is the incident that leads to the investigation.
- **Acquire:** This is the process that is set in motion by the trigger—this is predefined as a part of the incident response plan—and it involves identifying, acquiring, and collecting information and evidence relating to the incident. This includes getting information related to the triggers, reasons for suspecting an incident, and identifying and acquiring sources of evidence for subsequent analysis.

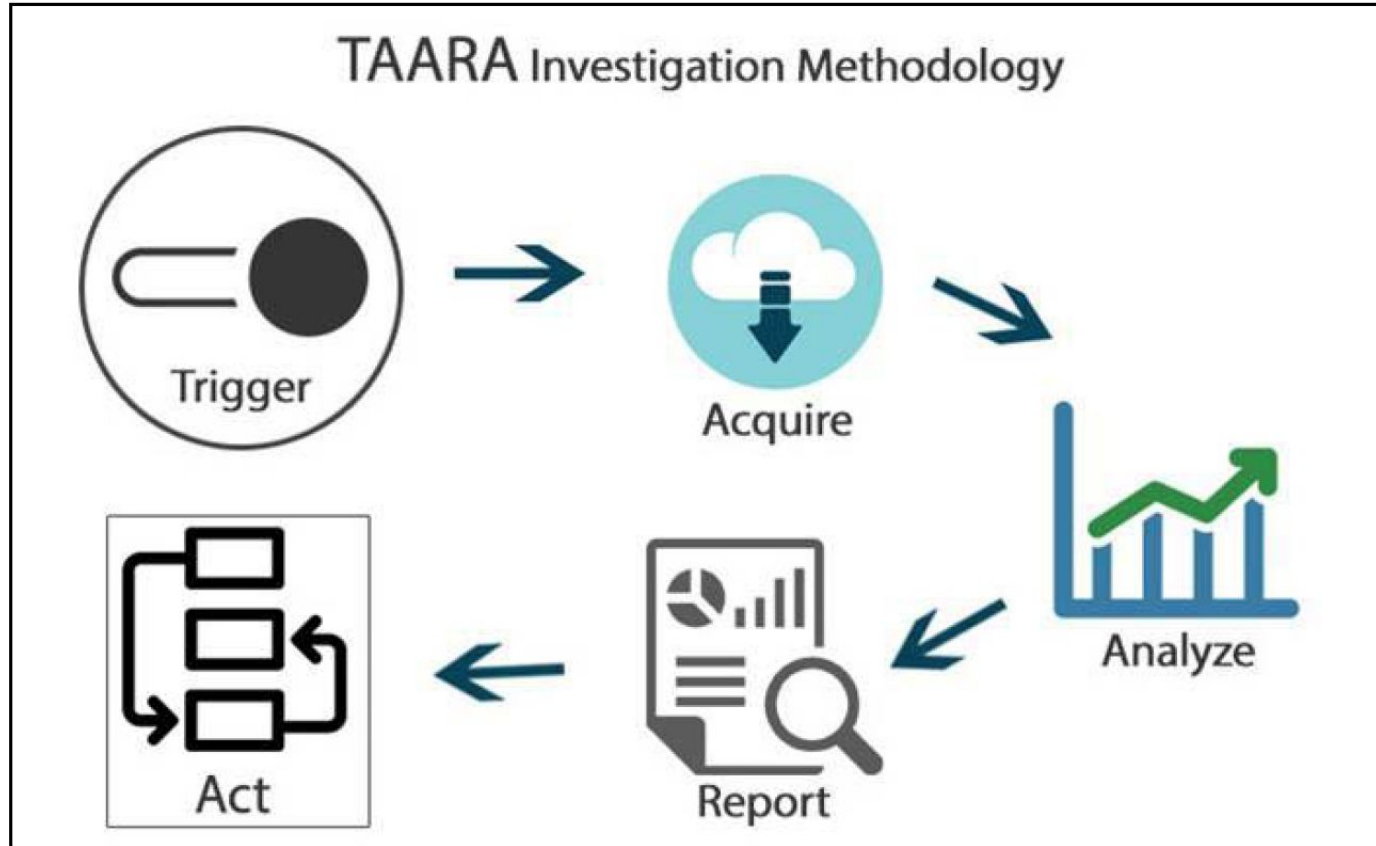
TAARA Framework (cont'd)

- **Analysis:** All the evidence that is collected so far is collated, correlated, and analyzed. The sequence of events is identified. Proper questions such as-
 - Whether the incident actually occurred or not
 - If it did, what exactly happened
 - How it happened
 - Who was involved
 - What is the extent of the compromise;-and so on are answered. Based on the information that is gathered during this stage, it may be necessary to go back to the acquire stage in order to gather additional evidence. Analysis is then initiated on the newly acquired evidence.

TAARA Framework (cont'd)

- **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.

TAARA Framework (cont'd)



Identifying threats to the enterprise - Internal

Disgruntled Employees

- Employees with intentions of damaging the enterprise
- Covert channel, Rogue AP

Lack of user training.

- Misuse, Malware infection
- Targeted by Social Engineering

Lack of access control

- Shared folder, Poorly managed access privileges

Lack of security policy

- BYOD (Bring your own device)

Lack of redundancy

- Single drive operation

Identifying threats to the enterprise - External

Poorly written Security Policies

- Outdated information systems(= vulnerabilities)
- Unattended unused open ports,
- Non-periodical IT Audits
- Legitimate backdoors
- Password complexity

Poorly written DRP(Disaster Recovery Plan)

- Natural disasters, Power outage

Identifying threats to the enterprise (cont'd)

	Intentional	Accidental
Internal	• Insider data theft • Insider sabotage • Information leakage • Assistance to outsiders • Sexual harassment within the enterprise • Tampering with sensitive data	• Accidental assistance to outsiders • Inadvertently letting malicious software loose on the network • Unintentional use of compromised software on bring your own device (BYOD) • Insiders social engineered to give away information such as passwords and so on
External	• Targeted phishing or spear phishing to extract confidential information • Network scans / OS fingerprinting / vulnerability assessments of outside-facing network components • Denial of Service attacks • State-sponsored surveillance	• An outsider accidentally stumbling onto sensitive data because of a flaw/vulnerability in the network • Accidental power outage • Natural disasters • An unsuspecting user's system can be taken over and used as part of a bot herd

This page left blank intentionally