Stages of Computer Forensics Process

The overall computer forensics process is sometimes viewed as comprising of four
stages:

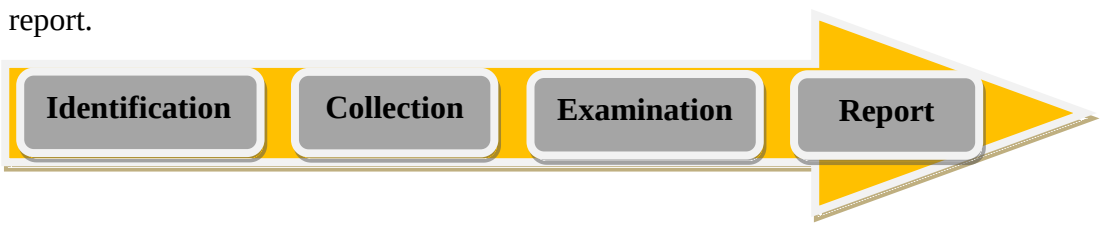
- **Assess the situation/ Identification:** Analyze the scope of the investigation and the
  action to be taken.

- **Acquire the data/ Collection:** Gather, protect, and preserve the original evidence.

- **Analyze the data/Examination:** Examine and correlate digital evidence with events of
  interest that will help you make a case.

- **Report the investigation:** Gather and organize collected information and write the final

report.



Assess the situation/ Identification

The first process of computer forensics is to identify the scenario or to understand the case. At this stage, the investigator has to identify the need of the investigation, type of incident, parties that involved in the incidence, and the resources that are required to fulfil the needs of the case.

Acquire the data/ Collection

The collection (chain of custody) is one of the important steps because your entire case is based on the evidence collected from the crime scene. The collection is the data acquisition process from the relevant data sources while maintaining the integrity of data. Timely execution of the collection process is crucial in order to maintain the confidentiality and integrity of the data. Important evidence may lose if not acted as required.

Analyze the data/Examination

The aim of the third process is to examine the collected data by following standard procedures, techniques, tools and methodology to extract the meaningful information related to the case. At this stage, the investigator searches for the possible evidence against the suspect, if any. Use the tools and techniques to analyze the data. Techniques and tools should be justified legally because it helps you to create and present your report in front of the court.

Report the investigation

This is the final and most important step in the investigation process. At this step, an investigator needs to document the process used for the above steps. The investigation report also consists of the documentation of how the tools and procedures were being selected. The objective of this step is to report and present the findings justified by the evidence. Every step mentioned above can be further divided into many parts and every part has its own standard operating procedures (SOP), we will discuss this in detail in the next unit.

1.8 Need of computer forensics

1. The world has become a global village since the beginning of computer, digital devices & the internet. Life seems impossible without these technologies, as they are necessary for our workplace, home, street, and everywhere. Information can be stored or transferred by desktop computers, laptop, routers, printers, CD/DVD, flash drive, or thumb drive. The variations and development of data storage and transfer capabilities have encouraged the development of forensic tools, techniques, procedures and investigators.
2. With the ever-increasing rate of cybercrimes, from phishing to hacking and stealing of personal information not only just limited to a particular country but globally at large, there is a need for forensic experts to be available in public and private organizations. To be able to handle this, it's vital for network administrator and security staff of networked organizations to have the knowledge to make sure that they have the laws relating to this on their fingertips. This would ensure that should need for the service avail itself, then they would come in and rescue the situation.
3. The survival and integrity of any given network infrastructure of any company or organization strongly depends on the application of computer forensics. They should be taken as the main element of computer and network security. It would be a great benefit for a company if it has knowledge of all the technical and legal aspects of this field. It will be of help in the provision of evidence and prosecution of the case in the court of law.
4. New laws aimed at the protection of customer's data are continuously being developed. Should they lose data, then naturally the liability goes to the company. Such cases, if they occur will automatically result in the company or organization being brought to the court of law for failure to protect personal data, this can turn out

to be very expensive. But through the application of forensic science, huge chunks of money can be saved by the firms concerned.

It simply means that there is a necessity in investment in either employing an expert in computer forensic in the firms or having part of their staff trained into this project so as to help in detection of such cases.

1.9 Rules of Computer Forensic

There are certain rules and boundaries that should be kept in mind while conducting an investigation.

Matthew Braid, in his AusCERT paper, 'Collecting Electronic Evidence after a System Compromise' has provided the rules of computer forensics:

1) **Minimize or eliminate the chances of examining the original evidence:**
   Make the accurate and exact copy of the collected information to minimize the option of examining the original. This is the first and the most important rule that should be considered before doing any investigation, create duplicates and investigate the duplicates. You should make the exact copy in order to maintain the integrity of the data.

2) **Don't Proceed if it is beyond your knowledge**
   If you see a roadblock while investigating, then stop at that moment and do not proceed if it is beyond your knowledge and skills, consult or ask an experienced to guide you in a particular matter. This is to secure the data, otherwise, the data might be damaged which is unbearable. Do not take this situation as a challenge, go and get additional training because we are in the learning process and we love to learn.

3) **Follow the rules of evidence**
   You might be worried because we have not discussed any rule of evidence yet, but the next topic will be about evidence. The rule of evidence must be followed during the investigation process to make sure that the evidence will be accepted in court.

4) **Create Document**
   Document the behaviour, if any changes occur in evidence. An investigator should document the reason, result and the nature of change occurred with the evidence. Let say, restarting a machine may change its temporary files, note it down.

5) **Get the written permission and follow the local security policy**
   Before starting an investigation process, you should make sure to have written permission with instruction related to the scope of your investigation. It is very important because during the investigation you need to get access or need to make copies of the sensitive data, if the written permission is not with you then you may find yourself in trouble for breaching the IT security policy.

6) **Be ready to testify**
   Since you are collecting the evidence then you should make yourself ready to testify it in the court, otherwise the collected evidence may become inadmissible.

7) **Your action should be repeatable**
   Do not work on trial-and -error, else no one is going to believe you and your investigation. Make sure to document every step taken. You should be confident enough to perform the same action again to prove the authenticity of the evidence.

8) **Work fast to reduce data loss**
   Work fast to eliminate the chances of data loss, volatile data may be lost if not collected in time. While automation can also be introduced to speed up the process, do not create a rush situation. Increase the human workforce where needed.

Always start collecting data from volatile evidence.

9) **Don't shut down before collecting evidence**
   This is a rule of thumb since the collection of data or evidence itself is important for an investigation. You should make sure not to shut down the system before you collect all the evidence. If the system is shut down, then you will lose the volatile data. Shutdown and rebooting should be avoided at all cost.

10) **Don't run any program on the affected system**
    Collect all the evidence, copy them, create many duplicates and work on them. Do not run any program, otherwise, you may trigger something that you don't want to trigger. Think of a Trojan horse.

1.10 Computer Forensics Team

As per Irfan Shakeel in his Book "Introduction to Computer Forensics & Digital Investigation" mention about the key people that a computer investigation firm should have. Which is as follows.

Law enforcement and security agencies are responsible for investigating computer crime, however, every organization should have the capability to solve their basic issues and investigation by themselves.

Even an organization can hire experts from small or mid-size computer investigation firms. Also, you can create your own firm that provides computer forensic services. To do so, you need a forensics lab, permission from the government to establish a forensics business, the right tools with the right people and rules/policies to run the business effectively and efficiently.

Without this ability, it is very hard for an organization to determine the fraud, illegal activities, policy, or network breach or even they will find it hard to implement the cybersecurity rules in the organization. The need for such abilities may vary and it depends on the nature of business, security threats and the possible loss.

Here are the key people that a computer investigation firm should have:

- **Investigators:** This is a group of people (number depends on the size of the firm) who handle and solve the case. It is their job to use forensic tools and techniques in order to find evidence against the suspect. They may call law enforcement agencies if required. Investigators are supposed to act immediately after the occurrence of the event that is suspected of criminal activity.
- **Photographer:** To record the crime scene is as important as investigating it. The photographer's job is to take photographs of the crime scene (IT devices and other equipment).
- **Incident Handlers (first responder):** Every organization, regardless of type, should have incident handlers in their IT department. The responsibility of these people is to monitor and act if any computer security incidence happens, such as breaching of network policy, code injection, server hijacking, RAT or any other malicious code installation. They generally use a variety of computer forensics tools to accomplish their job.
- **IT Engineers & technicians** (other support staff): This is the group of people who run the daily operation of the firm. They are IT engineers and technicians to maintain the forensics lab. This team should consist of a network administrator, IT support, IT security engineers and desktop support. The key role of this team is to make sure the smooth organizational functions, monitoring, troubleshooting, data recovery and to maintain the required backup.