LECTURE NOTES ON DIGITAL FORENSICS

Digital Forensics

AGNI DATTA

Lecture Notes collected from classes of Dr. Shishir Kumar Shandilya

DIGITAL FORENSICS

SCHOOL OF COMPUTER SCIENCE
VELLORE INSTITUTE OF TECHNOLOGY

Contents

Part I

Introduction to Digital Forensics:

Digital forensics is the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations. It involves the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

---

1 Importance of Computer Forensics:

The computer has invaded our very existence, become a part of our lives, and is an integral part of almost every case. Computer Forensics can help any organization in finding evidence in a variety of cyber crime cases. Crimes involving a computer can range across the spectrum of criminal activity, from child pornography to theft of personal data to destruction of intellectual property. Computer Forensics not only means recovering deleted files (documents, graphics, etc.), but also searching the slack and unallocated space on the hard drive-places where a plethora of evidence regularly resides. It is tracing Windows artefacts- those titbits of data left behind by the operating system-for clues of what the computer has been used for, and, more importantly, knowing how to find the artefacts, and evaluating the value of information. Forensic exams allow the processing of hidden files-files that are not visible or accessible to the user-that contain past usage information. It is reconstructing and analysing the date codes for each file-determining when each file was created, last modified, last accessed and when deleted. Computer forensics is being able to run a string-search for e-mail, when no e- mail client is obvious. An analysis will reveal Internet usage, recover data, and accomplish a full analysis even after the computer has been formatted. It is using industry-standard methodology, and with a concise report with clearly demonstrable results, something that is organized in a manner to make analysis easier.

---

2 Locard'S Exchange Principle:

Dr. Edmond Locard (13 December 1877 – 4 April 1966) was a pioneer in forensic science who became known as the "Sherlock Holmes of France". He formulated the basic principle of forensic science: "Every contact leaves a trace".

This became known as Locard's exchange principle. "Anyone, or anything that enters in the crime scene takes something from the crime scene with them and leaves something behind, and that both can be used as forensic evidence". Crime reconstruction involves examining the available physical evidence, those materials left at or removed from the scene, victim, or offender, for example fingerprints. These forensically established contacts are then considered in light of available and reliable witness, the victim, and a suspect's statements. From this, theories regarding the circumstances of the crime can be generated and falsified by logically applying the information of the established facts of the case.

---

3 Cardinal Rules of Digital Forensics:

Following are the cardinal rules of the Digital Forensics:

- ⋆ Never mishandle the evidence.
- ⋆ Never trust the subject machine or Operating system.
- ⋆ Never work on the original evidence.

---

4 Digital Evidence:

Digital evidence is defined as information and data of value to an investigation that is stored on, received or transmitted by an electronic device. This evidence can be acquired when electronic devices are seized and secured for examination.

Digital evidence:

- ⋆ Is latent (hidden), like fingerprints or DNA evidence,
- ⋆ Crosses jurisdictional borders quickly and easily,
- ⋆ Can be altered, damaged or destroyed with little effort,
- ⋆ Can be time sensitive.

Admissibility: Digital evidence is often ruled inadmissible by courts because it was obtained without authorization. In most jurisdictions a warrant is required to seize and investigate digital devices. In a digital investigation this can present problems where, for example, evidence of other crimes are identified while investigating another. Authentication: As with any evidence, the proponent of digital evidence must lay the proper foundation. Courts largely concerned themselves with the reliability of such digital evidence. Best evidence rule is a legal principle that holds an original copy of a document as superior evidence. The rule specifies that secondary evidence, such as a copy or facsimile, will be not admissible if an original document exists and can be obtained. "Secondary evidence" or copies of the content in the original document can be admitted as evidence. The best evidence rule is only applied in situations in which a party attempts to substantiate a non-original document submitted as evidence during a trial. Admissibility of documents before state court systems may vary.

Digital Evidence should be the following:

- ⋆ Admissible: Conform to legal requirements,
- ⋆ Authentic: Relevant to the case,
- ⋆ Complete: Not just extracts
- ⋆ Reliable: Collected and Handled appropriately,
- ⋆ Believable and understandable.

4.1 Legal Issues:

MAC details of the files as digital evidence in the seized original hard disk (hence its image too) must be earlier than the noticing / reporting of criminal incident as well as the date & time of its seizure. If it is not so, digital evidence will be diagnosed as a tampered evidence and court can not accept it as an admissible evidence.

4.2 Types of Digital Evidence:

4.2.1 Volatile (Non-persistent) Memory that loses its contents, as soon as power is turned off; e.g. Data stored in RAM (semiconductor storage) (System BIOS: CMOS RAM - battery powered)

4.2.2 Non-volatile (Persistent) No change in contents, even if power is turned off; e.g. Data stored in a tape / hard disk (magnetic storage), CD / DVD (optical storage), data cards, USB Thumb Drives – Flash memory).

4.3 Order of Volatility:

Higher Volatility to Lower Volatility List:

1. Registers & Cache
2. Routing Tables
3. ARP Cache
4. Process Table
5. Kernel Statistics & Modules
6. Main Memory (RAM)
7. Temporary System files
8. Secondary Memory
9. Router Configuration
10. Network Topology

4.4 Importance of Order of Volatility:

Current running state and system configuration details.

- ⋆ Activities performed/ In progress
- ⋆ Root cause of the incident
- ⋆ Timeline of the incident
- ⋆ Time, date, user responsible for the incident
- ⋆ Network connection details

Once system is shutdown / rebooted volatile data is lost for ever.

---

5 Procedure of Collecting Digital Evidence:

5.1 Order of Handling Data In Crime Scene:

- ⋆ Document the Crime Scene - OS (Version),
- ⋆ BIOS date & time (and difference, if any),
- ⋆ H/W and S/W Configuration,

- ⋆ IP / MAC address,
- ⋆ Computer System : Shutdown / Power Off ?
- ⋆ Identify Evidence & Authenticate through a Hashing Algorithm (MD5),
- ⋆ Always make the bit-stream copy (forensic image) of the seized storage media,
- ⋆ Label all the connecting cables and photograph them,
- ⋆ Document the chain of custody,
- ⋆ Preserve the evidence before packing for transportation,
- ⋆ Securely pack & transport the evidence to lab,
- ⋆ Store the seized evidence in a protected storage (air bubbled PVC, anti-static bag),
- ⋆ Transfer the Computer System to a secure location.

5.1.1 Document Everything:

The Crime Scene Computer forensics is a meticulous practice. When a crime involving electronics is suspected, a computer forensics investigator takes each of the following steps to reach — hopefully — a successful conclusion: Secure the area, which may be a crime scene. Document the chain of custody of every item that was seized. If someone is already working on the system then ask/ insist him/her to leave the terminal. Take photographs, note down the important things, if any. Bag, tag, and safely transport the equipment and e-evidence. Acquire the e-evidence from the equipment by using forensically sound methods and tools to create a forensic image of the e-evidence. Keep the original material in a safe, secured location. Design your review strategy of the e-evidence, including lists of keywords and search terms. Examine and analyse forensic images of the e-evidence (never the original!) according to your strategy. Interpret and draw inferences based on facts gathered from the e-evidence. Describe your analysis and findings in an easy-to-understand and clearly written report. Give testimony under oath in a deposition or courtroom.

5.1.2 Securing The Crime Scene:

Secure the area containing the equipment or the crime scene. Secure the entrances and exits to the digital scene. Move people away from computer and power supply as it may lead to contamination if anyone touches anything. Preventing changes in potential digital evidence, including network isolation, collecting volatile data, and copying entire digital environment is the goal of this phase. If there are any ongoing processes, they have to be captured so that to not cause loss of potential evidence.

5.1.3 Identifying The Evidence Sources:

Generating a plan of action to conduct an effective digital investigation, and obtaining supporting resources and materials is a part of this phase. Recognizing an incident from indicators and determining its type, which entails the preparation of tools, techniques, search warrants, and monitoring authorizations and management support. Finding potential sources of digital evidence (e.g., at a crime scene, within an organization, or on the Internet) is done.

What should be seized for the retrieval of evidence?

Examples:

⋆ Main unit, usually the box to which the monitor and keyboard are attached.

⋆ Monitor, keyboard and mouse (only necessary in certain cases.)

⋆ Power supply units.

⋆ Hard disks not inside the computer.

⋆ Dongles

⋆ Modems (some contain phone numbers).

⋆ External drives and other external devices.

⋆ Routers.

⋆ Digital cameras.

⋆ Back up tapes.

⋆ CDs/ DVDs.

⋆ Memory sticks, memory cards and all USB connected devices.

5.1.4 Document The Scene:

Photographs or videos of digital evidence are taken individually as well as crime scene and individuated descriptions of digital evidences are to be made. Each piece of digital evidence that is found during the analysis of the image must be clearly documented. Proper thorough chain of custody has to be maintained. Chain of custody is a form which documents the movement of evidence from its source to when it is presented in court.

It is essential that any items of evidence can be traced from the crime scene to the court room, and everywhere in between, known as CHAIN OF CUSTODY.

⋆ Positive control is the phrase most often used to describe the standard of care taken in the handling of potential evidentiality material (e.g., suspect computer systems, hard drives, and any backup copies).

⋆ Who handled the evidence?

⋆ What procedures were performed on the evidence?

⋆ When was the evidence collected and/or transferred to another party?

⋆ Where was the evidence collected and stored?

⋆ How was the evidence collected and stored?

⋆ For what purpose was the evidence collected?

5.1.5 Acquire The Evidence:

Analysis should always take place on a forensically sound copy, or image, of the seized data, rather than the original data itself. For this purpose a bit by bit copy of the evidence is to be made. The storage device is first connected to a “write blocking” device, which prevents any binary code from being altered or modified during the process. Then a mirror image or “clone” of the drive is created on a separate storage device to be examined later. During the acquisition process, such software creates a unique numerical code, called a verification “hash” of the media, which allows an analyst to later confirm that the image and its contents are accurate and unaltered. Data acquisition can be carried out either online (live) or offline (dead). A dead acquisition is carried out without the support of the suspect’s operating system while a live acquisition is carried out with the support of suspect operating system.

5.1.6 Photography and Videography:

Forensic photography, also referred to crime scene photography, is an activity that records the initial appearance of the crime scene and physical evidence, in order to provide a permanent record for the courts and for the record. Proper documentation is to be done and the evidences , the crime scene is to be photographed with a view to properly locate the things in and around the vicinity of the crime scene.

The following details/ steps need to be photographed sequentially with proper scale and labelling: When entering the scene of crime, photograph the scene to record the details of the crime scene. Photograph the live status of the system found at the scene, this includes current applications opened, cables/ USB attached, any running processes etc. After collection, the evidence is photographed with and without a scale and before and after packaging.

---

6 Communities' Works in Digital Forensics:

Communities working in Digital Forensics:

- ⋆ Law Enforcement (i.e. Police)
- ⋆ Military/Intelligence
- ⋆ Business & Industry
- ⋆ Academia/Researchers

---

7 Uses of Digital Forensics:

Digital forensics can be used in a variety of settings, including

- ⋆ Criminal Investigations
- ⋆ Civil Litigation
- ⋆ Intelligence
- ⋆ Administrative Matters

7.1 Criminal Investigation:

In today's digital world, electronic evidence can be found in almost any criminal investigation conducted.

- ⋆ Homicide, physical assault, robbery, and burglary are just a few of the many examples of "analogue" crimes that can leave digital evidence.
- ⋆ One of the major struggles in law enforcement is to change the paradigm of the police and get them to think of and seek out digital evidence.
- ⋆ Everyday digital devices such as cell phones and gaming consoles can hold a treasure trove of evidence.
- ⋆ Unfortunately, none of that evidence will ever see a courtroom if it's not first recognized and collected.
- ⋆ As time moves on and our law enforcement agencies are replenished with "younger blood," this will become less and less of a problem.

7.2 Civil Litigation:

Civil litigation is a legal process in which criminal charges and penalties are not at issue. When two or more parties become embroiled in such a non-criminal legal dispute, the case is presented at a trial where plaintiffs seek compensation or other damages from defendants.

The use of digital forensics in civil cases is big business. In 2011, the estimated total worth of the electronic discovery market is somewhere north of $780 million (Global EDD Group). As part of a process known as Electronic Discovery (e-Discovery), digital forensics has become a major component of much high dollar litigation. e-Discovery "refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case" In a civil case, both parties are generally entitled to examine the evidence that will be used against them prior to trial. This legal process is known as "discovery." Previously, discovery was largely a paper-based exercise, with each party exchanging reports, letters, and memos; however, the introduction of digital forensics and e-Discovery has greatly changed this practice. The proliferation of the computer has rendered that practice nearly extinct. Today, parties no longer talk about filing cabinets, ledgers, and memos; they talk about hard drives, spreadsheets, and file types. Some paper-based materials may come into play, but it's more the exception than the rule. Seeing the evidentiality landscape rapidly changing, the courts have begun to modify the rules of evidence. The rules of evidence, be they state or federal rules, govern how digital evidence can be admitted during civil litigation. The Federal Rules of Civil Procedure were changed in December 2006 to specifically address how electronically stored information is to be handled in these cases. Digital evidence can quickly become the focal point of a case, no matter what kind of legal proceeding it's used in. The legal system and all its players are struggling to deal with this new reality.

7.3 Intelligence:

- ⋆ Terrorists and foreign governments, the purview of our intelligence agencies, have also joined the digital age.
- ⋆ Terrorists have been using information technology to communicate, recruit, and plan attacks.
- ⋆ The armed forces are exploiting intelligence collected from digital devices brought straight from the battlefield.
- ⋆ This process is known as DOMEX (Document and Media Exploitation).
- ⋆ DOMEX is paying large dividends, providing actionable intelligence to support the soldiers on the ground army.

7.4 Administrative Matters:

- ⋆ Digital evidence can also be valuable for incidents other than litigation and matters of national security.
- ⋆ Violations of policy and procedure often involve some type of electronically stored information, for example, an employee operating a personal side business, using company computers while on company time.
- ⋆ That may not constitute a violation of the law, but it may warrant an investigation by the company.

8 Role of The Forensic Examiner in The Judicial System:

- ⋆ The digital forensics practitioner most often plays the role of an expert witness.
- ⋆ What makes them different than non expert witnesses? Other witnesses can only testify to what they did or saw. They are generally limited to those areas and not permitted to render an opinion.
- ⋆ Experts, by contrast, can and often do give their opinion. What makes someone an "expert?" In the legal sense, it's someone who can assist the judge or jury to understand and interpret evidence they may be unfamiliar with.
- ⋆ To be considered an expert in a court of law, one does not have to possess an advanced academic degree.
- ⋆ An expert simply must know more about a particular subject than the average lay person.
- ⋆ Under the legal definition, a doctor, scientist, baker, or garbage collector could be qualified as an expert witness in a court of law. Individuals are qualified as experts by the court based on their training, experience, education, and so on.

8.1 What separates a qualified expert from a truly effective one?

- ⋆ It is their ability to communicate with the judge and jury.
- ⋆ They must be effective teachers.
- ⋆ The vast majority of society lacks technical understanding to fully grasp this kind of testimony without at least some explanation.
- ⋆ Digital forensic examiners must carry out their duties without bias. Lastly, a digital forensics examiner must go where the evidence takes them without any preconceived notions.

---

9 Challenges In Digital Forensics:

9.1 Types of Evidences:

9.1.1 Real Evidence:

Real evidence is any evidence that speaks for itself without relying on anything else. In electronic terms, this can be a log produced by an audit function—provided that the log can be shown to be free from contamination.

9.1.2 Testimonial Evidence:

Testimonial evidence is any evidence supplied by a witness. This type of evidence is subject to the perceived reliability of the witness, but as long as the witness can be considered reliable, testimonial evidence can be almost as powerful as real evidence. Word processor documents written by a witness may be considered testimonial—as long as the author is willing to state that they wrote it.

9.1.3 Hearsay:

Hearsay is any evidence presented by a person who was not a direct witness. Word processor documents written by someone without direct knowledge of the incident is hearsay. Hearsay is generally inadmissible in court and should be avoided.

9.2 Evidence Handling:

Evidence handling has four primary areas in any incident response activity.

These areas are:

9.2.1 Collection, which has to do with searching for evidence, recognition and collection of evidence, and documenting the items of evidence. Always ensure the collection includes all of the available data and resources, such as the whole disk drive, not just the used portions. Always document the place, time, and circumstances of each data item collected for evidence.

9.2.2 Hardware evidence examination, which has to do with origins, significance, and visibility of evidence, often can reveal hidden or obscured information and documentation about the evidence. Dimensions, styles, sizes, and manufacturer of hard drives, other devices, or network items are all important evidence items.

9.2.3 Software and network evidence analysis, which is where the logs/records/software evidence is actually examined for the incident providing the significance criteria for inclusion and the probative value of the evidence. Always conduct this software and network analysis and interpretation separate from the hardware evidence examination.

9.2.4 Evidence reporting, it must be written documentation with the processes and procedures outlined and explained in detail in the reports. Pertinent facts and data recovered are the primary keys in the reports. Understand the documentation and reports will always be reviewed, critiqued, and maybe even cross-examined.

9.3 Technical Challenges In Evidence Handling:

As technology develops crimes and criminals are also developed with it. Digital forensic experts use forensic tools for collecting shreds of evidence against criminals and criminals use such tools for hiding, altering or removing the traces of their crime, in digital forensic this process is called Anti- forensics technique which is considered as a major challenge in digital forensics world.

Anti-forensics techniques are categorized into the following types:

9.3.1 Encryption:

It is legitimately used for ensuring the privacy of information by keeping it hidden from an unauthorized user/person. This helps protect the confidentiality of digital data either stored on computer systems or transmitted through a network like the internet. Unfortunately, it can also be used by criminals to hide their crimes.

9.3.2 Data Hiding in Storage Space:

Criminals usually hide chunks of data inside the storage medium in invisible form by using system commands, and programs.

9.3.3 Covert Channel:

A covert channel is a communication protocol which allows an attacker to bypass intrusion detection technique and hide data over the network. The attacker used it for hiding the connection between him and the compromised system.

9.3.4 Cloud Operation:

This allows the hackers to spoof their IP addresses and also makes forensics expert difficult tracking the actual presence of machine through which the malicious attack has been occurring.

9.3.5 Archival Time:

This small gap in time is crucial as it allows the offender to clean their digital trace and also destroy important evidence pertaining to the case. This time can also be the difference between apprehending a suspect and for him to be going free.

9.3.6 Skill Gap:

This mainly occurs when a digital forensic expert is lacking experience and knowledge when compared to their illegal counterparts. This is a major issue between the current landscape, as Black Hat and White Hat hackers have quite a known skill difference.

9.3.7 Steganography:

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of Steganography can be combined with encryption as an extra step for hiding or protecting data.

9.4 Legal Challenges in Digital Forensics:

The presentation of digital evidence is more difficult than its collection because there are many instances where the legal framework acquires a soft approach and does not recognize every aspect of cyber forensics. Besides, most of the time electronic evidence is challenged in the court due to its integrity. In the absence of proper guidelines and the non-existence of proper explanation of the collection, and acquisition of electronic evidence gets dismissed in itself.

9.4.1 Absence of Guidelines and Standards:

In India, there are no proper guidelines for the collection and acquisition of digital evidence. The investigating agencies and forensic laboratories are working on the guidelines of their own. Due to this, the potential of digital evidence has been destroyed.

9.4.2 Limitation of The Indian Evidence Act, 1872:

The Indian Evidence Act, 1872 have limited approach, it is not able to evolve with the time and address the E-evidence are more susceptible to tampering, alteration, transposition, etc. the Act is silent on the method of collection of e-evidence it only focuses on the presentation of electronic evidence in the court by accompanying a certificate as per subsection 4 of Sec. 65B. This means no matter what procedure is followed it must be proved with the help of a certificate.

9.4.3 Privacy Issues:

A major concern for people those who are affected by an incident. They do not want to raise a complaint due to the issue in privacy. This leads to a legal barrier between the process of evidence handling and evidence presentation in court.

9.4.4 Admissibility In Courts:

Due to lack of proper polices, the data collected can be proven inadmissible if any fault is found in the process of data accumulation.

9.4.5 Preservation of Electronic Evidence:

A major concern in the techniques of preservation used to store the digital evidence. Any changes and manipulations in the evidence will render the digital evidence inadmissible in court.

9.4.6 Power For Gathering Digital Evidence:

The digital forensic expert needs enough computing, legal and man power for the proper collection and preservation of data.

9.4.7 Analysing a Running Computer:

Analysis of a running computer is not easy and data collection can also cause changes in the current state of the running machine. The order of volatility needs to be followed otherwise there will a huge change the data collected. This will be inadmissible in court.

9.5 Resource Challenges in Digital Forensics:

As the rate of crime increases the number of data increases and the burden to analyse such huge data is also increases on a digital forensic expert because digital evidence is more sensitive as compared to physical evidence it can easily disappear. For making the investigation process fast and useful forensic experts use various tools to check the authenticity of the data but dealing with these tools is also a challenge in itself.

9.5.1 Change in Technology:

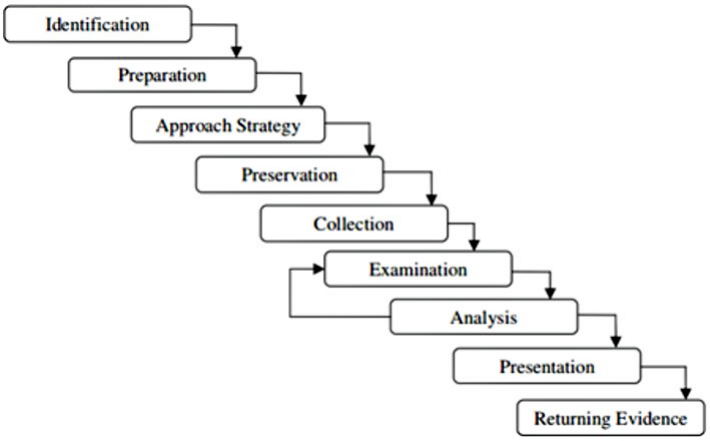
Due to rapid change in technology like operating systems, application software and hardware, reading of digital evidence becoming more difficult because new version software's are not supported to an older version and the software developing companies did provide any backward compatible's which also affects legally.

9.5.2 Volume and Replication:

The confidentiality, availability, and integrity of electronic documents are easily get manipulated. The combination of wide-area networks and the internet form a big network that allows flowing data beyond the physical boundaries. Such easiness of communication and availability of electronic document increases the volume of data which also create difficulty in the identification of original and relevant data.

---

10 A Flow of Evidence Diagram:



Part II

Incident Response:

Incident Response is an organized approach to addressing and managing the aftermath of a security breach or cyber-attack.

11 Incident Response:

Incident response is a key component of an enterprise business continuity and resilience program.

The increasing number and diversity of information security threats can disrupt enterprise business activities and damage enterprise information assets.

A sound risk management program can help reduce the number of incidents, but there are some incidents that can neither be anticipated nor avoided.

Therefore, the enterprise needs to have an incident response capability to detect incidents quickly, contain them, mitigate impact, and restore and reconstitute services in a trusted manner.

---

12 Incident:

- ⋆ An action likely to lead to grave consequences like,
- ⋆ Data loss may lead to commercial loss.
- ⋆ Confidentiality breached.
- ⋆ Political issues.
- ⋆ Network breakdown lead to service and information flow disruption.

---

13 Response:

- ⋆ An act of responding.
- ⋆ Something constituting a reply or a reaction.
- ⋆ The activity or inhibition of previous activity or any of its parts resulting from stimulation
- ⋆ The output of a transducer or detecting device resulting from a given input.
- ⋆ Ideally Incident Response would be a set of policies that allow an individual or individuals to react to an incident in an efficient and professional manner thereby decreasing the likelihood of grave consequences.

---

14 ISO 17799

- ⋆ Outlines Comprehensive Incident Response and Internal Investigation Procedures
- ⋆ Detailed Provisions on Computer Evidence Preservation and Handling

---

15 Purpose of Incident Response:

- ⋆ Minimize overall impact.
- ⋆ Hide from public scrutiny.
- ⋆ Stop further progression.
- ⋆ Involve Key personnel.
- ⋆ Control situation.

15.1 Minimize overall impact through,

- ⋆ Recover Quickly & Efficiently.
- ⋆ Respond as if going to prosecute.
- ⋆ If possible replace system with new one.
- ⋆ Priority one, business back to normal.

- ⋆ Ensure all participants are notified.
- ⋆ Minimize overall impact.
- ⋆ Recover Quickly & Efficiently.
- ⋆ Secure System.
- ⋆ Lock down all known avenues of attack.
- ⋆ Assess system for unseen vulnerabilities.
- ⋆ Implement proper auditing.
- ⋆ Implement new security measures.
- ⋆ Follow-up (A continuous process)
- ⋆ Ensure that all systems are secure.
- ⋆ Continue prosecution.
- ⋆ Securely store all evidence and notes.
- ⋆ Distribute lessons learned.

15.2 Identifying False Positives:

Each event that detection tools generate falls into one of four categories, depending on whether alert fired and whether something bad actually happened:

15.2.1 TRUE POSITIVES: Something bad happened, and the system caught it.

15.2.2 TRUE NEGATIVES: The activity is benign (gentle, kind), and no alert has been generated.

15.2.3 FALSE POSITIVES: The system alerts, but the activity was not actually malicious.

15.2.4 FALSE NEGATIVES: Something bad happened, but the system did not catch it.

Tools do not always alert when something bad happens, and just because they throw an alarm does not necessarily mean it is time to isolate a host or call the police.

Example:

Just because an IDS alerted that “the Web server has been hacked” does not mean that the Web server was actually hacked.

---

16 Signal to Noise Ratio:

EVERY ALERT IS IMPORTANT

16.1 To illustrate, consider the case of SOC A and SOC B.

In SOC A, the daily work queue contains approximately 100 reliable, high-fidelity, usable alerts. Each one is reviewed by an analyst. If incident response is necessary for a given alert, it is performed.

In SOC B, the daily work queue contains approximately 1,00,000 alerts, almost all of which are false positives. Analysts attempt to review them according to priority.

Because of the large volume (even for alerts of the highest priority), analysts cannot successfully review all of the highest-priority alerts.

Additionally, because of the large number of false positives, SOC B's analysts become desensitized to alerts and do not take them particularly seriously.

---

17 Triage:

The triage process happens between the moment when an alert is triggered and the time when an incident response process is initiated.

Not every alert generated by a SIEM product triggers an incident, some might prompt refinements of SIEM content or changes in security policy.

This process should include steps that allow security personnel to unambiguously determine whether the alert is an indicator of an incident, needs to be suppressed in the future, or requires further investigation or escalation.

Triage is the assessment of a security event to determine if there is a security incident its priority and the need for escalation.

As it relates to potential malware incidents the purpose of triaging may vary.

A few potential questions triaging may address are:

- ⋆ Is malware present on the system?
- ⋆ How did it get there?
- ⋆ What was it trying to accomplish?

---

18 Security Incident:

Understanding whether an event is an actual incident is not very simple and evident every time.

Event Correlation.

Here are a few tips for the verification:

- ⋆ Adjacent Data – Check the information adjacent to the event. For example, if an endpoint has a virus signature hit, look to see if there's evidence the virus is running before calling for further response metrics.
- ⋆ Intelligence Review – Understand the context around the intelligence. Just because an IP address was flagged as part of a botnet last week does not mean it still is part of a botnet today.
- ⋆ Initial Priority – Align with operational incident priorities and classify incidents appropriately. Make sure the right level of effort is applied to each incident.
- ⋆ Cross Analysis – Look for and analyse potentially shared keys, such as IP addresses or domain names, across multiple data sources for better data acuity.

Once an event is verified, the event becomes an investigation or an incident. All incidents must be investigated and tracked.

19 Classification of Types of Incidents:

Understand what types of attacks are likely to be used against your organization.

List of different attach by NIST is:

19.0.1 External/Removable Media: An attack executed from removable media (e.g., flash drive, CD) or a peripheral device.

19.0.2 Email: An attack executed via an email message or attachment (e.g. malware infection).

19.0.3 Attrition: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.

19.0.4 Improper Usage: Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.

19.0.5 Web: An attack executed from a website or a web-based application (e.g. drive-by download).

19.0.6 Loss or Theft of Equipment: The loss or theft of a computing device or media used by the organization, such as a laptop or smartphone.

19.0.7 Other: An attack that does not fit into any of the other categories.

20 Action on Security Incident:

20.1 Incident Scene Snapshot:

- ⋆ Record state of computer
- ⋆ Photos,
- ⋆ State of computer,
- ⋆ What is on the screen?
- ⋆ What is obviously running on the screen?
- ⋆ Xterm?
- ⋆ X-windows?
- ⋆ Should you port scan the affected computer?

Pros: You can see all active and listening ports.

Cons: It affects the computer and some backdoor log how many connections come into them and could tip off the bad guy.

20.2 Unplug Power from System:

This method may be the most damaging to effective analysis though there are some benefits.

Pros: Benefits include that you can now move the system to a more secure location and that you can physically remove the hard drive from the system

Cons: You lose evidence of all running processes and memory.

20.3 Unplug from The Network:

- ⋆ Unplug it from the network and plug the distant end into a small hub that is not connected to anything else.
- ⋆ Most systems will write error messages into log files if not on a network.
- ⋆ If you make the computer think it is still on a network, you will succeed in limiting the amount of changes to that system.

20.4 Backup or Analyse:

Set up in policy for your incident response:

- ⋆ It depends on the system and what you need it for.
- ⋆ To get BEST evidence BACKUP first at the cost of time to get answers.
- ⋆ To get FAST answers ANALYSE first at the cost of getting best evidence.
- ⋆ Label systems with priority. Some will need answers quicker than your ability to get best evidence.

---

21 Prioritizing Incidents:

- ⋆ An Incident's priority is usually determined by assessing its impact and urgency.
- ⋆ Urgency is a measure how quickly a resolution of the Incident is required.
- ⋆ Impact is measure of the extent of the Incident and of the potential damage caused by the Incident before it can be resolved.

---

22 Incident Prioritizing Table:

CATEGORY	DESCRIPTION
HIGH	The damage caused by the incident increases rapidly.
	Work that cannot be completed by the staff is highly time sensitive.
	A minor incident can be prevented from becoming a major incident by acting immediately.
	Several users with VIP status are affected.
MEDIUM	The damage caused by the incident increases considerably over time.
	A single user with VIP status is affected.
LOW	The damage caused by the incident only marginally increases over time.
	Work that cannot be completed by staff is not time sensitive.