Unit 2: Overview of First Responder

2

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Understand Cyber forensics investigation Phases
- The process of forensic duplication
- Role of First responder ,its toolkit and procedure

1.2 PHASES OF CYBER FORENSIC INVESTIGATION

We all know that cyber forensics is a branch of forensic science which mainly includes the different stages of digital evidence namely Identification, Acquisition, Analysis and Presentation.[52]

[52] Nelson, Bill. Guide to Computer Forensics and Investigations. Boston, MA: Thomson Course Technology, 2004 (ISBN 0-619- 13120-9)

Despite these stages, there are different phases of cyber forensics. Lets' us understand every phase in detail.

1. **PLANNING**

   In this phase, investigator does all the necessary arrangement to carry out the actual forensic investigation. This phase mainly consists of requirement and information gathering. This phase ensures high quality investigations output. In this phase, the forensic investigator gathers all related information of the incident actively and passively. He also prepares toolkit required for the investigation by understanding the scope. The forensic investigator obtains permission from authorities to conduct further steps. This permission is formerly known as Search Warrant. With the proper execution of the planning phase, the forensic investigator gets in-depth knowledge of facts of the case which is required to decide further approach. The key elements of this phase are interviewing the victims, identifying affected computing devices and deciding the digital forensic procedure to be used. In this process, the forensic investigator has given instructions, clarification and guidelines for performing activities. Allocation of roles and resources is been decided in this phase. Obtaining approval for forensic investigation is the key factor of this phase.[53]

2. **SEARCH AND IDENTIFICATION**

   This phase mainly deals with identifying the affected people and the infrastructure of the given incident. This can be done effectively with the proper inputs obtained from the previous phase. Different tools and methods can be used to identify the type of attack. Search facilitates examination of the suspected people as well as systems. This phase also contributes to deciding the scope of the overall investigation. Proper approval is a necessity to conduct this phase. The output of this phase clarifies the number of people and the system to be examined in further investigation.

3. **SEIZER**

[53] National Institute of Justice. Forensic Examination of Digital Evidence: A Guide for Law Enforcement <http://www.ncjrs.org/pdffiles1/nij/199408.pdf >

This phase starts with securing the crime scene. Before the actual examination of digital evidence in the forensic lab, it should be properly seized. There are different seizer procedures for different types of evidences. As per the requirement, scientific and legal seizer procedure is used like Isolation of system from the network, a photograph of the running machine skill. Applying forensic shutdown processes. Removing storage media like hard disk, memory card without any damage etc. The seizer memo is been created which is signed by the investigator and the witnesses. Seizer memo contains a brief description of evidence and procedure followed to seize particular evidence. The digital evidence collection form is been also prepared and filled accordingly for the sized evidence.[54]

4. ACQUIRE

The acquisition phase mainly consists of bit by bit forensic disk imaging, disk cloning, taking memory dump and creating evidence file suitable for analysis purpose. The hardware and software write blockers are used in this process to avoid any unintentional alteration or modification in digital evidence. To ensure the admissibility and integrity of the evidence a hash value is been calculated in this phase. There are different forensic tools available for different evidences to acquire entire evidence in a forensic manner.

The acquisition can be physical or logical. In a physical acquisition, the entire disk is been acquired. In a logical acquisition, logical partition of the disk is been acquired. In both cases write blocker are required. In this process, copies of evidence are made and its hash value is been verified.

5. COLLECT AND PRESERVE

In this phase, sealing, labelling and bagging of the evidence is been done at the crime scene. At most care is been taken while packing digital evidences is been taken in order to avoid physical damage during transportation. Chain of custody document is been created and properly filled. This document gives the information regarding accountability

[54] National Institute of Standards and Technology. CFTT Methodology Overview <http://www.cftt.nist.gov/Methodology_Overview.htm>

of the evidence in terms of who, when, why and for how much duration was handling that evidence. Properly sealed evidence is been created and preserved in an evidence storage box. The preserved evidence will be further transported to the location where the actual analysis will be carried out.

6. ANALYSIS

The acquired information needs forensic examination. When the evidence is been transported to the forensic lab before analysis, the hash value is been verified by the forensic experts. This helps to prove the integrity of digital evidence before analysis. Every file out there is with some purpose and proper analysis of the available data can reveal many ways to proceed in further investigation. For the said purpose, the appropriate techniques and tools need to be used to make a relevant mole-hill out of the mountain of the data, consistently yielding exemplary and concise results.

The examiner may use additional tools to recover deleted information. The used tools must be validated to ensure their reliability and correctness. Forensic expert analyze the evidence twice to verify the correctness of the findings. During analysis, the evidence found is been assembled to reconstruct event or actions to provide the facts.

7. REVIEW AND REPORT

After the examination is complete, the findings are reviewed and documented in the report. It includes a detailed description of the conducted steps during the investigation. The examination report typically contains following details:

Name of the examiner who did the examination, Date and time when is been done, Software and hardware that were used, their version numbers, Hash value verification and related clicked photographs.

The information related to the acquired evidence such as hard disk and mobile device details should be also included. The report generated should be easy to understand and explain in precise details. Further actions are determined after the report is reviewed

8. PRESENTATION

Presenting an understandable, defendable and complete report is the key to getting the desired outcome of the whole process. Expert witness testimony is one of the most important tasks of presentation finding. Success of the forensic investigation is very much dependent upon the way it has been presented and defended in a court of law.

1.3 FORENSIC DUPLICATION

Forensic duplication refers to bitstream imaging of data from the digital media in question. Data resides in all sorts of storage media present in computers, smartphones, GPS devices, USB drives, and so on.[55] We need to be able to get to this information in a manner that it does not change the information on the devices themselves. If the evidence is not collected properly, we face an issue where the results of the forensic exam will be put in doubt. Hence it is necessary to copy the data carefully in a forensically sound manner.

LOGICAL BACKUP	BITSTREAM IMAGING
A logical backup copies the directories and files of a logical volume. It does not capture other data that may be present on the media, such as deleted files or residual data stored in slack space.	Also known as disk imaging/ cloning/ bitstream imaging generates a bit-for-bit copy of the original media, including free space and slack space. Bitstream images require more storage space and take longer to perform than logical backups.

The Important thing required for forensic Investigation is Write blocker

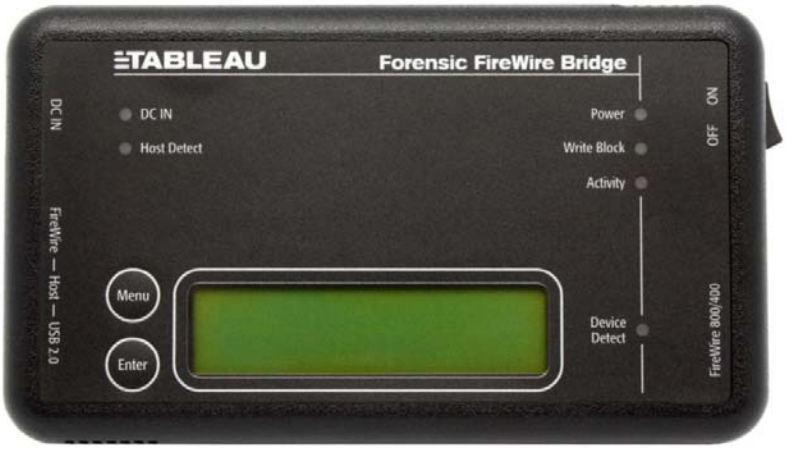
WRITE BLOCKER

[55] Kruse, Warren G., Heiser, Jay G.; Computer Forensics: Incident Response Essentials, Addison Wesley, Boston, Massachusetts, September 2001, ISBN: 0-201-70719-5

A write-blocker is hardware or software-based tool that prevents a computer from writing to computer storage media connected to it. Hardware write-blockers are physically connected to the computer and the storage media being processed to prevent any writes to that media.

Features:-

- Prevents any writes to the seized media
- Suspect hard disk connected to the forensic computer via a write blocker



Things to understand and remember about Digital evidence

- Almost every type of crime has digital evidence in it.
- The investigator must apply the same level of maturity, knowledge, security and safety while dealing with digital evidence likewise other traditional evidence
- Nature of Digital Evidence is delicate and fragile. Hence improper handling may result in damage or tampering of the evidence.
- Digital Evidence can be easily altered or manipulated without intention
- Never Assume Digital evidence is destroyed completely

RULES OF DIGITAL FORENSICS

- Never work on original evidence.
- Never mishandle evidence.
- Use proper software utilities to retrieve evidence from the media.
- Document everything while handling the suspected media.[56]

[56] Mandia, Kevin, Prosise, Chris; Incident Response: Investigating Computer Crime, New York, 2001, ISBN: 0-07-213182-9

THE FOUR PRINCIPLES FOR THE AUTHENTICATION AND INTEGRITY OF EVIDENCE ARE

PRINCIPLE 1:

No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

PRINCIPLE 2:

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

PRINCIPLE 3:

An audit trail or another record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

PRINCIPLE 4:

The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

HASHING

Hashing is a process of converting large, possibly variable-size amount of data into a small datum by well-defined procedure or mathematical function.[57]

Salient features of the process of the hashing

- The integrity of the seized evidence through the forensically proven procedure.
- Produces fixed length unique value representing the data on the seized media.
- Any changes in the evidence will result in a change in the hash value
- Hashing is a process of converting the large, possibly variable-size amount of data into a small datum by well-defined procedure or mathematical function.
- Hashing is mainly done to check the integrity of the data.
- Values returned after hashing is commonly called as hash values, hash sums or hashes
- Commonly used Hash functions are

[57] Nelson, Bill; Phillips, Amelia; Enfinger, Frank & Steuart, Chris; Guide to Computer Forensics and Investigations, Boston, Massachusetts, Course Technology, 2004, ISBN: 0-619-13120-9

- MD5 Hash Algorithm
- SHA1 Hash Algorithm
- While imaging the original Hard disk, a hash value is generated.
- After imaging, the hash value will be generated.
- The hash value of the original Harddisk = Hash value of the imaged Hard Disk, then we can say that the Message integrity is 100%

Commonly used Software for Imaging will calculate this Hash Values. Say for example

1. C-DAC's Cyber Check Suite
2. FTK Imager
3. Win Hex
4. Encase

1.4 INTRODUCTION TO FIRST RESPONDER

The first responder is the person who plays a vital role in the overall investigation. The tasks performed by the first responder are very much crucial for the investigation. Any mistake by the first responder may lead to tampering of the evidence or wrong direction of the investigation. Hence, the first responder is very much responsible for the further success of the investigation. The first responder is defined as a person who arrives first at the crime scene and accesses the victims computing devices after the incident. Protection, Integration and Preservation of the digital evidence are the key responsibilities of the first responder. He may be network administrator, investigation officer, law enforcement officer etc.[58]

Following are the important roles of First Responder:

- Identify the crime scene, affected people and affected computing devices.
- Protect the identified subject of the crime scene.
- Preserve the temporary and fragile evidence.
- Gather detailed information about the incident.
- Document all the findings.

[58] US Department of Justice; Electronic Crime Scene Investigation: A Guide for First Responders, Washington D.C., July 2001, NCJ-187736 <http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm>

- Seizer of the identified Digital Evidences.
- Package and transport of the Digital Evidence.

1.5 FIRST RESPONDER TOOLKIT

First Responder Toolkit defined as a collection of tools required to seize digital evidence in a genuine and presentable way. The toolkit helps First Responder to understand the limitations and capabilities of digital evidence at the time of collection.

The first responder is responsible to select a trusted forensic tool that gives the desired output. While creating first responder toolkit, the tools must be tested and validated before actual use. The details of every tool should be documented. Along with version name and hardware requirements. Multiple tools for similar functionality should be available in the toolkit. First responder toolkit should consist of a collection of following a different set of tools.

Disassembly Tools- Screw Drivers, Wire Cutters, Tweezers etc.

Documentation Tools- White Papers, Markers, Tag, Stick-on papers etc.

Packaging Tools- Evidence Bags, Bubble Wrap, Tape, Cable ties, Anti-static bubble wrap, Anti-static bags etc.

Forensic Equipment - Bootable Disk, External Hard Drives, Pen Drives, Write Blockers, Data Acquisition Software and Hardware field response Kit.

1.6 FIRST RESPONDER BASICS

THERE ARE SOME GROUND RULES OF FIRST RESPONSE[59]

Rule 1- The first responder must be competent and experience in handling technological gadgets.

Rule 2- The first responder should not do any such act which may tamper the digital evidence. The first responder should have knowledge of data acquisition technique mainly imaging and cloning.

[59] <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/394779/ediscovery-digital-forensic-investigations-3214.pdf>

Rule 3- He should secure the crime scene and maintain a secure state until the forensic team advises.

Rule 4- He should never take help of suspect to access the computing devices which may hold possible digital evidence.

Rule 5- He should document all the details of the crime scene and handed over those notes to forensic experts.

1.7 FIRST RESPONDER PROCEDURE

Following are different steps which should be taken by the first responder.[60]

Step 1. After planning for search and seizer and obtaining search warrant the first responder should secure and evaluate crime scene and conduct the initial search.

Step 2. In order to gather information regarding the incident, the first responder supposed to conduct the interviews.

Step 3. The first responder needs to photograph the crime scene and draw sketches of the scene.

Step 4. The first responder needs to document all the findings and create a note of it.

Step 5. The first responder needs to remove the storage device and note down its details.

Step 6. The first responder needs to exhibit numbering to the seized evidence and preserve them.

Step 7. Packaging and selling of the collected evidence should have been properly carried out with labelling upon it.

Step 8. The first responder should make sure that the evidence will be transported to a forensic lab safely.

SECURING CRIME SCENE

It is important to follow a certain procedure in order to secure the crime scene. Properly secured crime scene help forensic investigator to carry out further tasks.

[60] <https://forensiccontrol.com/resources/beginners-guide-computer-forensics/>

Following are some guidelines to the first responder in order to effectively secure the crime scene.

a. Understand and verify the type of incident and prepare accordingly.
b. Make sure that the premise is safe for investigators.
c. Find and help the victim.
d. Ensure that nobody will access the computer systems by isolating the people out there.
e. Document all connection of the suspected device and disconnect to make the system stand alone.
f. Observe the situation at the crime scene and note down all these observations.
g. Protect the fingerprints that can be found on the suspected computing devices.
h. All the forensic investigator should wear hand gloves and anti-static wrist belts.

COLLECTING PRELIMINARY INFORMATION

In order to collect initial information, the interviews of the related people should be carried out. For that questionnaire according the incident needs to be prepared. Search warrant act as permission to conduct the interviews. If required the written consent of the interviewer should be obtained before the interview. If required witness signature can also be obtained over the important documents such as search warrant, consent form etc. While conducting interviews different question should be asked to get detailed knowledge about certain facts e.g. owner and user of the computing device, internet service provider, purpose of using the system, offsite data storage, password required to access system software or data etc.

The first responder can also create a checklist of the expected information which needs to be collected as per the type of the incident.

Following are some of the key questions which should be discussed during this phase of the investigation.

- What steps were taken to contain the issue?
- Were there any logs (system access, etc.) present that cover the issue?
- Are there any suspicious entries present in them?
- Did anyone use the system after the issue occurred?

- Did you observe any similar instance before?
- Were there any alarms that were set off by the firewall/IDS/network security devices?
- Please give detailed documentation on the set of commands or processes run on the affected system or on the network after the issue occurred.
- Do they have similar systems in any of the branch/other offices?
- Whether log register of the Internet users/other users is maintained?
- Are there any questions about the issue that have not been answered?

At the scene of the offence, IO should gather the following information during the interviews phase

- Identify the complainant/owner (s) of the various devices and obtain the access details, usernames, and service providers' details.
- Gather information as provided in the questionnaire(s) above, on all the security systems.
- Identify the list of the people who can identify the network and a schematic diagram of the network.

DOCUMENTING THE SCENARIO

It is important to create certain records by documenting the crime scene. This may give certain findings which can be used further. All the observation of the crime scene should be properly documented such as the position of the screen, mouse and other components of the system. Listing down all the components and its connections help to understand the technique used by the criminal. Documenting also includes a detailed description of different facts of computing devices such as power status, storage devices etc. Photograph of the screen of running computing devices should be clicked and write down the notes of the observations in it. A video camera can

be used to capture the entire scene of the crime. A still camera should be used to take the photographs of the important object at the crime scene. Photography helps to notice even the smallest piece of evidence. In the documentation of the crime scene, sketches should be drawn for the layout of the area.

COLLECTING AND PRESERVING EVIDENCE

Nowadays there are many storage media available. As an Investigator one should know where the Digital Evidence is. The investigator should not ignore even a small piece of paper. It may contain valuable information that can be a Substantial Evidence to catch hold a criminal or culprit. This is a very important task for the Investigator.[61]

List of Storage Device to be collected from the scene of the offence

- CPU
- Hard Disk
- Floppy Drive
- CD's & DVD's Drive
- USB Memory Sticks
- Pen Drives
- Memory Cards
- Portable Hard Disks
- Tape Drives

The very important stage of Investigation is to isolate all the Memory Components from the Computer or computer Network. That simply means making computer Standalone. This has to be done in order to avoid manipulation, alteration or deletion of Digital Evidence. As far as possible cover the mouse and keyboard with polythene covers to preserve fingerprints.

[61] <https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics/Types>

PACKAGING AND TRANSPORTING EVIDENCE

PACKAGING

Following are the important points to be considered while packaging the evidence.

- Evidence should be properly documented
- The evidence should be labelled as per the type of evidence.
- The evidence should be inventoried
- Evidence should always be packed in antistatic packaging.
- Avoid folding, bending, or scratching the evidence.
- Seized / Confiscated Material should be properly packed in the box.
- Place labels (Exhibit No :) on the top of the package
- Check the size of the Hard Disk before seizing.
- Bring One Blank hard disk with the exact capacity (or more) that of suspect's HDD for forensic duplication process.

TRANSPORTATION

- The utmost care has to be taken while carrying the Seized components from one place to another.
- Ignorance while transportation may lead towards Tampering of Evidence
- Due to the sensitive and fragile nature of the computer evidence, place the computer in a box properly cushioned with non-static material.
- All the Seized Components should be packed with proper Packing material (Cello Tape, Boxes, Anti-Static Bags, Thermacol etc.)
- The Components should be kept properly.
- Store the computer is secure and dust-free place.
- The storage should not come in contact with water.
- Vibration Free Transportation.

- Evidence should not be kept in contact with any Electro-Magnetic field.
- As far as possible cover the mouse and keyboard with polythene covers to preserve fingerprints.
- Don’t bend the Pen drives, Floppy, CDs etc.
- Don’t place labels directly on Floppy drive/CD.
- Store it in normal temperature.

CRIME SCENE REPORTING

In order to explain what exactly has happened during the investigation, the investigator should document all the actions performed over the evidence. The overall responsibility of any changes in the evidence goes with the forensic investigator. Hence, the proper documentation is very much an important aspect of digital forensics.

Following are some of the key documents which every investigator should create during his investigation.

- Search warrant
- Chain of custody
- Digital evidence collection form
- Digital forensic report

Preparing a good and admissible report is the skilful work and the most important phase of the forensics process. The investigator’s knowledge is judged by what he writes. The court cases can be won or lost because of the reports and its quality. Hence the investigator should have the knowledge to represent the facts and findings in a simple and understandable manner through the report. The report should be written in such a way that it should speak for the investigator for itself and it will exist as an official record for that case.

SALIENT FEATURES OF GOOD REPORT

- It perfectly describes the incident and its details
- It should be easy to understand by decision-makers.
- It gives a clear picture of the investigation without any open-end conclusion.
- It defines the proper timeline of the investigation.
- It omits irrelevant information.
- It clearly states what the investigator has done, which facts are uncovered and how these facts lead to the final conclusion.
- It provides supporting material such as equation, data, tables and figures.
- Anyone who is new to the situation should be able to understand it through the report.

1.8 LET'S SUM UP

In this chapter, we have studied the different phases of cyber forensic investigation along with forensic duplication. We also studied the basics and toolkit of First Responder and have ended our discussion with the First Responder Procedure.

1.9 FURTHER READING

- "Electronic Crime Scene Investigation – A Guide for First Responders" by National Institute of Justice, USA; (http://www.ojp.usdoj.gov/nij)
- Mugisha, David. (2019). ROLE AND IMPACT OF DIGITAL FORENSICS IN CYBER CRIME INVESTIGATIONS. International Journal of Cyber Criminology. 47. 3.
- Resources.sei.cmu.edu (2019), https://resources.sei.cmu.edu/asset_files/Handbook/2005_002_001_14429.pdf (last visited Nov 25, 2019).

- Ncjrs.gov (2019), https://www.ncjrs.gov/pdffiles1/nij/187736.pdf (last visited Nov 25, 2019).

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are the different phases of cyber forensic investigation?

- Planning
- Search and Identification
- Seizer
- Acquire
- Collect and Preserve
- Analysis
- Review and Report
- Presentation

2. What are the ground rules of the first responder?

Rule 1- The first responder must be competent and experience in handling technological gadgets.

Rule 2- The first responder should not do any such act which may tamper the digital evidence. The first responder should have knowledge of data acquisition technique mainly imaging and cloning.

Rule 3- He should secure the crime scene and maintain a secure state until the forensic team advises.

Rule 4- He should never take help of suspect to access the computing devices which may hold possible digital evidence.

Rule 5- He should document all the details of the crime scene and handed over those notes to forensic experts.

3. What are the steps that needs to be taken by the first responder?

Following are different steps which should be taken by the first responder.

Step 1. After planning for search and seizer and obtaining search warrant the first responder should secure and evaluate crime scene and conduct the initial search.

Step 2. In order to gather information regarding the incident, the first responder supposed to conduct the interviews.

Step 3. The first responder needs to photograph the crime scene and draw sketches of the scene.

Step 4. The first responder needs to document all the findings and create a note of it.

Step 5. The first responder needs to remove the storage device and note down its details.

Step 6. The first responder needs to exhibit numbering to the seized evidence and preserve them.

Step 7. Packaging and selling of the collected evidence should have been properly carried out with labelling upon it.

Step 8. The first responder should make sure that the evidence will be transported to a forensic lab safely.

4. **What are the salient features of a good report?**

- It perfectly describes the incident and its details
- It should be easy to understand by decision-makers.
- It gives a clear picture of the investigation without any open-end conclusion.
- It defines the proper timeline of the investigation.
- It omits irrelevant information.
- It clearly states what the investigator has done, which facts are uncovered and how these facts lead to the final conclusion.
- It provides supporting material such as equation, data, tables and figures.
- Anyone who is new to the situation should be able to understand it through the report.

1.11 ACTIVITY

Briefly explain the procedure that needs to be undertaken by the First Responder along with a case study? (1000-1500 words)