Unit 3: Investigation Process

3

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

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

- The process of investigation
- Different guidelines for digital evidence
- Understand step wise instruction of investigation in different scenarios

1.2 INTRODUCTION

Nowadays investigation is been carried out at a very fast pace. Thanks to technology that help investigating officer to gather the relevant information at very high speed and act upon it. Investigation process used needs to update and enhance with net types of technological advancement. In this chapter, we will understand the different investigation processes, guidelines

and standard operating procedure which investigation officer needs to be followed while dealing with cyber-crimes and other crimes where digital evidence are involved.[22]

1.3 ACPO GUIDELINES

The Association of Chief Police Officers (ACPO) was a not-for-profit private limited company that for many years led the development of policing practices in England, Wales, and Northern Ireland. It has contributed a lot in terms of guidelines for handling digital evidence.

The Association of Chief Police Officers (ACPO) Good Practice Guide for Computer-based Electronic Evidence [ACPO] –for reference

- No actions performed by investigators should change data contained on digital devices or storage media that may subsequently be relied upon in court.
- Individuals accessing original data must be competent to do so and have the ability to explain their actions.
- A trail or other record of applied processes, suitable for replication of the results by an independent third-party, must be created and preserved, accurately documenting each investigative step.
- The person in charge of the investigation has overall responsibility for ensuring the above-mentioned procedures are followed and in compliance with governing laws.

Apart from ACPO guidelines there are several guidelines out there and mainly used by Indian law enforcement agencies as given below.[23]

1.4 DIGITAL EVIDENCE GUIDELINES

- Identify the computer system, Secure the scene, preserve the traced evidence
- If the computer is switched off, then Photograph, label and document the system details on collection form and collect related software peripherals, removable media, passwords if any

[22] See the Digital Records Forensics Project website at <http://digitalrecordsforensics.org>

[23] Adams, Richard & Hobbs, Val & Mann, Graham. (2014). Journal of Digital Forensics, Security & Law. Journal of Digital Forensics, Security & Law. 8. 25-48

- If the computer is on and prompts for any password simply disconnect the power and then Photograph, label and document the system details on collection form and collect related software peripherals, removable media, passwords if any
- If it does not prompts for any password, then document screen, system time, network activity. Preserve the RAM content if needed using Authorized tools and procedures.
- Depending upon the case Scenario, the entire computer can be seized or any particular suspected hardware can be seized[24]

Following is the simple diagram which represents how exactly the cybercrime investigation is been carried out.[25]

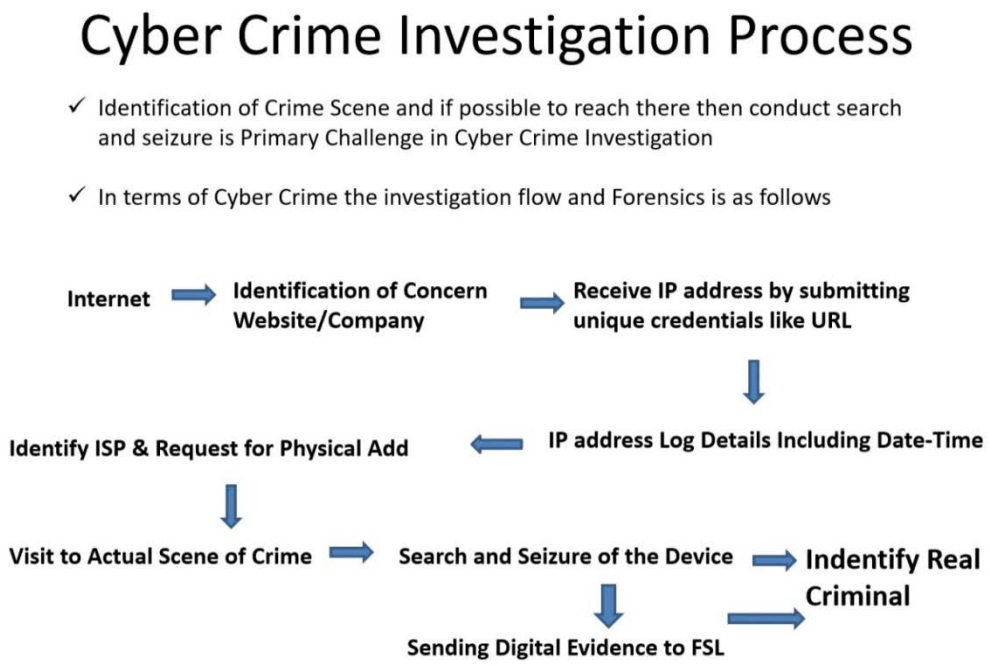

Figure 1.1 Cyber Crime Investigation Process

In the above diagram, the cyber space-related investigation is described. It mainly explains the flow of investigation where the place of incident is the internet.

Now let's understand the step by step approach of the investigating officer in crime investigation.

[24] Adams, R (2013) Doctoral Thesis. The Advanced Data Acquisition Model (ADAM): A process model fordigital forensic practice Murdoch University Retrieved from <http://researchrepository.murdoch.edu.au/14422/2/02Whole.pdf>

[25] Agarwal, A, Gupta, M, Gupta, S, & Gupta, S C (2011). Systematic digital forensic investigation model. International Journal of Computer Science and Security, 5(1), 118-130

1.5 STEPS IN CRIME SCENE INVESTIGATION

1. Identifying and securing the crime scene[26]
2. 'As is where is' documentation of the scene of the offence
3. Collection of evidence
4. Procedure for gathering evidences from switched-off Systems
5. Procedure for gathering evidence from live systems
6. Forensic duplication
7. Conducting interviews
8. Labelling and, documenting the evidence
9. Packaging, and transportation of the evidences

THE PROCESS OF EVALUATION OF THE SCENE OF OFFENCE

- Secure the Scene of Crime
- Identify all the potential evidences
- Conventional evidences like sticky slips, manuals, bank account numbers etc., to be part of the search process.
- If the system is OFF, leave it OFF
- Special care to be taken for perishable evidence eg., volatile data
- After identifying the scene of the offence, IO should secure it and, take note of every individual physically present at the scene of offence and, their role at the time of securing the scene of offence.
- From the information gathered and based on visual inspection of the scene of offence, IO should identify all the potential evidence. These physical evidences may include conventional physical evidences like the manuals, user guides and, other items left behind like passwords on slips, bank account numbers etc. it is also important to note the position of the various equipment and items at the scene of offence. For example,

[26] Ciardhuain, S O (2004) An extended model of cybercrime investigations. International Journal of Digital Evidence, 3(1)

a mouse on the left-hand side of the desktop possibly indicates the person operating the computer is a left-handed user.[27]

- While identifying the digital evidence, IO should make sure that the potentially perishable evidence is identified and, all the precautions are put in place for its preservation.

FOLLOWING IS THE PROCEDURE FOR CONDUCTING SEARCH

1. Secure the spot
2. Preserve the fingerprints
3. Restrict the access to a computer (s)
4. Don't accept the help of the suspect for operating computer.
5. Make the Computers Standalone (Remove LAN / Telephone / Wi-Fi / Blue tooth etc)
6. If the computer is/are "OFF"; don't turn "ON"
7. Some screen savers will show that computer is off hence to make sure by checking the light of CPU.
8. If the computer is "ON" then note down the date and time of computer system, don't try to correct it.
9. Documentation
10. Take the photograph of the Monitor screen
11. Don't shut down the computer in a normal manner but for shutting down pull the power cord from CPU and not from wall point.
12. Place the unformatted blank floppies in each drive for preventing accidental booting of the computer.
13. Photograph the scene, then disconnect all power source; unplug from wall and also from the back of the system.
14. Draw the sketch of the scene of the spot.
15. Label all the equipment, connectors and cables ends to allow reassemble as needed.
16. Seal all the ports and also screws of the CPU with paper seal.

[27] Freiling, F C, & Schwittay, B (2007) A common process model for incident response and computer forensics. Paper presented at the Conference on IT Incident Management and IT Forensics, Germany

17. Pack and seal the equipment carefully and a sample of the same seal must be sent to the FSL where the analysis of the CPU will be carried out.
18. Examine the persons, including suspect for the passwords, username etc.
19. Search the premises for the printouts, handwritten notes, diary, notebooks etc., for the passwords, username etc.
20. Search the premises for the software/programs, printouts, handwritten notes, financial transactions, books etc., which may be of vital importance to the investigation.
21. In personal search look for the pen/flash drives which might be attached to a key chain and may contain vital data.

PRELIMINARY INTERVIEWS AT THE SCENE OF OFFENCE

Following are some of the key questions which should be discussed during this phase of the investigation.[28]

- 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 OFFENCE, IO SHOULD GATHER THE FOLLOWING INFORMATION DURING THE INTERVIEWS PHASE

[28] Palmer, G (2001) A Road Map for Digital Forensic Research. Digital Forensics Research Workshop, Utica, New York

- 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

Let's take some examples in order to understand the investigation process of the different scene of the crime.[29]

SCENE OF OFFENCE: CYBER CAFÉ

1. Identify the number of computer systems present in the cyber café.
2. Identify the number of computer systems connected to the Internet.
3. Obtain details about the network topology and architecture (client — Server).
4. Obtain the CCTV/Web camera clippings, if any.
5. Whether any user management software is used by the cyber café owner?
6. Obtain the log register of Internet users for the relevant period.
7. Check the formatting of storage devices policy adopted by the cyber café owner.
8. Check the hardware replacements done by the cyber café owner.
9. Check the policy regarding removal media usage on the cyber café systems.

SCENE OF OFFENCE: HOME

1. Identify the type of connection (Wi-Fi/Ethernet).
2. How many computer systems are used for the Internet connection?
3. Location of the system and details of persons with access to system(s).
4. Obtain the details about the removable storage media (including external hard disk) used/owned by the user.
5. Obtain details about the network topology and architecture (client — Server), if any.
6. Obtain the details about other computer peripherals (printer/scanner/modem, etc.).

ISSUANCE OF THE PRESERVATION NOTICE

[29] Selamat, S R, Yusof, R, & Sahib, S (2008) Mapping process of digital forensic investigation framework. International Journal of Computer Science and Network Security, 8(10)

Preservation notice is the formal and legal document made in order to request to preserve the information which is important for further investigation. This is the vital document in the investigation process of the digital evidence.

Based on the information gathered, the IO should come out with issues to be complied immediately by issuing specific do's and don'ts to the complainant/company/agency.

e.g. stopping the access, taking backups, or preserving log information, etc. till further orders. For example, continuing access to the e-mail by the accused can enable him to delete the mails which are incriminating in nature.

A preservation notice needs to be sent to all affected parties to make sure that they do not delete any data that could be relevant to the case. It is ideal to issue this notice, which is necessary for preserving evidence.

GATHERING EVIDENCE

In this phase it is important to know the standard operating procedures for gathering information from different pieces of evidence. SOP gives step by step approach to gather evidence in a legal manner and preserve its admissibility by protecting the integrity of the evidence

PROCEDURE FOR GATHERING EVIDENCES FROM SWITCHED-OFF SYSTEMS

- Secure and take control of the scene of crime both physically and electronically.
- Make sure that the computer is switched OFF- some screen savers may give the appearance that the computer is switched OFF, but hard drive and monitor activity lights may indicate that the machine is switched ON.
- Be aware that some laptop computers may power ON by opening the lid.
- Remove the battery from laptop computers.
- Unplug the power and other devices from sockets.
- Never switch ON the computer, in any circumstances.
- Label and photograph (or video) all the components in-situ and if no camera is available, draw a sketch plan of the system.
- Label the ports and (in and out) cables so that the computer may be reconstructed at a later date, if necessary

- Carefully open the side casing of the CPU or laptop and identify the Hard disk. Detach the hard disk from the motherboard by disconnecting the data transfer cable and power cable.
- Take out the storage device (Hard disk) carefully and record unique identifiers like make, model, and serial number.
- Get the signature of the accused and witness on Hard disk, by using a permanent marker. Ensure that all items have signed and completed exhibit labels.
- Search scene of the crime for Non-electronic evidences like diaries, notebooks or pieces of paper with passwords.

PROCEDURE FOR GATHERING EVIDENCES FROM LIVE SYSTEMS (SWITCHED-ON SYSTEMS)

- Record what is on the screen by a photograph and by making a written note of the content of the screen.
- Do not touch the keyboard or click the mouse and if the screen is blank or a screen saver is present, the case officer should be asked to decide if they wish to restore the screen. If so, a short movement of the mouse will restore the screen or reveal that the screen saver is password protected. If the screen restores, photograph/video and note its content. If password protected is shown, continue as below without any further disturbing the mouse. Record the time and the activity of the use of the mouse in these circumstances.
- Take the help of technical expert to use live forensics tool to extract the information that is present in the temporary storage memory like RAM.
- If no specialist advice is available, remove the power supply from the back of the computer without closing down any programs. When removing the power supply cable, always remove the end attached to the computer and not that attached to the socket, this will avoid any data being written to the hard drive if an uninterruptible power protection device is fitted.

PROCEDURE FOR GATHERING EVIDENCES FROM MOBILE PHONES

- If the device is “OFF”, do not turn “ON”.
- With PDAs or cell phones, if the device is ON, leave ON. Powering down device could enable password, thus preventing access to evidence.
- Photograph device and screen display (if available).

- Label and collect all cables (including power supply) and transport with device.
- If device cannot be kept charged, analysis by a specialist must be completed prior to battery discharge or data may be lost.
- Seize additional storage media (memory sticks, compact flash, etc).
- Document all steps involved in the seizure of device and components.

USE OF FARADAY BAD IN MOBILE SEIZURE

Benefits for the investigator if a faraday bag is used are:

1) Potentially avoids the problem of the mobile phone becoming PIN locked.
2) Faraday Window ensures the examiner to view the phone in a 'faraday' condition, thus enabling an 'immediate preview of evidence'.
3) Re-usable
4) To prevent the data from the networks communicating with the device, therefore, stops any chance of evidence being tainted.
5) Prevents any chance of evidence being manipulated during covert acquisition.

After gathering the evidence it needs to be sent to Forensic lab for the analysis and reporting of it. With the evidence, the investigation officer needs to send certain points which act as guidelines for the forensic expert to retrieve the evidence from the sent media. Hence to get the best of the expert opinion IO should follow the following process.[30]

EXPERT OPINION FROM FORENSIC EXAMINER

- The forwarding letter to the FSL for scientific analysis and opinion should mention the following information.
- A brief history of the case
- The details of the exhibits seized and their place of seizure
- The model, make and description of the hard disk or any storage media
- The date and time of the visit to the scene of the crime
- The condition of the computer system (on or off) at the scene of the crime
- Is the photograph of the scene of crime is taken?

[30] Venter, J P (2006). Process flows for cyber forensics training and operations Retrieved from <http:researchspace.csir.co.za/dspace/bitstream/10204/1073/1/Venter_2006.pdf>

- Is it a stand-alone computer or a network?
- Is the computer has an Internet connection or any means to communicate with external computers?

MODEL QUESTIONS TO BE ASKED IN CASE OF "COMPUTER AS A TARGET" CYBERCRIME

- What type of operating system has been installed on the computer?
- When was the operating system installed?
- Please provide the user names/users present in the system
- What programs or software is installed on the computer?
- What is the IP address assigned to the system, if any?
- What is the MAC address of the system?
- Are there any information relating e-mail addresses present in the computer system?
- Are there any chat messenger software installed. If so, are there any chat IDs/profiles?
- Any suspicious or malicious software installed?
- Please provide the Internet history of the computer (Web sites accessed, files uploaded, downloaded, etc.)?
- Are there any firewall logs available in the system?

QUESTIONS TO BE ASKED IN CASE OF "SENDING THREATENING E-MAIL"

- Whether the sender's e-mail address is present in the seized hard disk.
- Whether the receiver's e-mail address is present in the seized hard disk.
- Whether the contents of the e-mail message (subject mail of case) is present in the hard disk.
- Any information relating to the IP addresses are available?

QUESTIONS TO BE ASKED IN CASE OF "COMPUTER AS AN INSTRUMENT/REPOSITORY"

- Which are the user accounts that are present on the computer?
- What financial applications/software applications are installed in the system?
- Are there any logs available for these applications?
- Please provide the list of files/filenames that were recently accessed
- What external devices (like thumb drives/external hard drives) were connected to the computer?

- Are there any databases and excel spreadsheets available inactive or deleted state?
- Are there any accounting packages/software installed?
- Are there any encrypted or password-protected files available? If so, please extract the content from them?
- Are there any pornographic images/videos present in the computer system?
- Was the system date and time changed at any point in time?

1.6 LET'S SUM UP

In this chapter, we have studied about the investigation process along with the ACPO guidelines. We also studied about the different guidelines with respect to digital evidence. Finally, we ended our discussion with the steps in crime scene investigation.

1.7 FURTHER READING

- Shon Harris; "All in One CISSP Guide, Exam Guide Sixth Edition", McGraw Hill, 2013.
- LNJN National Institute of Criminology and Forensic Science, "A Forensic Guide for Crime Investigators – Standard Operating Procedures", LNJN NICFS, 2016.
- Anthony Reyes, Jack Wiles; "The Best Damn Cybercrime and Digital Forensic Book", Syngress, USA, 2007.
- Cory Altheide and Halan Carvey; "Digital Forensics with Open Source Tools", Syngress Publication.

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is ACPO?

The Association of Chief Police Officers (ACPO) was a not-for-profit private limited company that for many years led the development of policing practices in England, Wales, and Northern Ireland. It has contributed a lot in terms of guidelines for handling digital evidence.

2. What are the guidelines for digital evidence?

- Identify the computer system, Secure the scene, preserve the traced evidence
- If the computer is switched off, then Photograph, label and document the system. details on collection form and collect related software peripherals, removable media, passwords if any.

- If the computer is on and prompts for any password simply disconnect the power and then Photograph, label and document the system details on collection form and collect related software peripherals, removable media, passwords if any.
- If it does not prompts for any password, then document screen, system time, network activity. Preserve the RAM content if needed using Authorized tools and procedures.
- Depending upon the case Scenario, the entire computer can be seized or any particular suspected hardware can be seized.

3. Explain the scene of offence in cyber café?

- Identify a number of computer systems present in the cyber café.
- Identify a number of computer systems connected to the Internet.
- Obtain details about the network topology and architecture (client — Server).
- Obtain the CCTV/Web camera clippings, if any.
- Whether any user management software is used by the cyber café owner?
- Obtain the log register of Internet users for the relevant period.
- Check the formatting of storage devices policy adopted by the cyber café owner.
- Check the hardware replacements done by the cyber café owner.
- Check the policy regarding removal media usage on the cyber café systems.

1.9 ACTIVITY

Briefly explain the steps in a Crime Scene Investigation along with a case study? (1000 – 1500 words)