Computer Forensics Investigation Process

MODULE 2

Contents

Computer Forensics Investigation Process

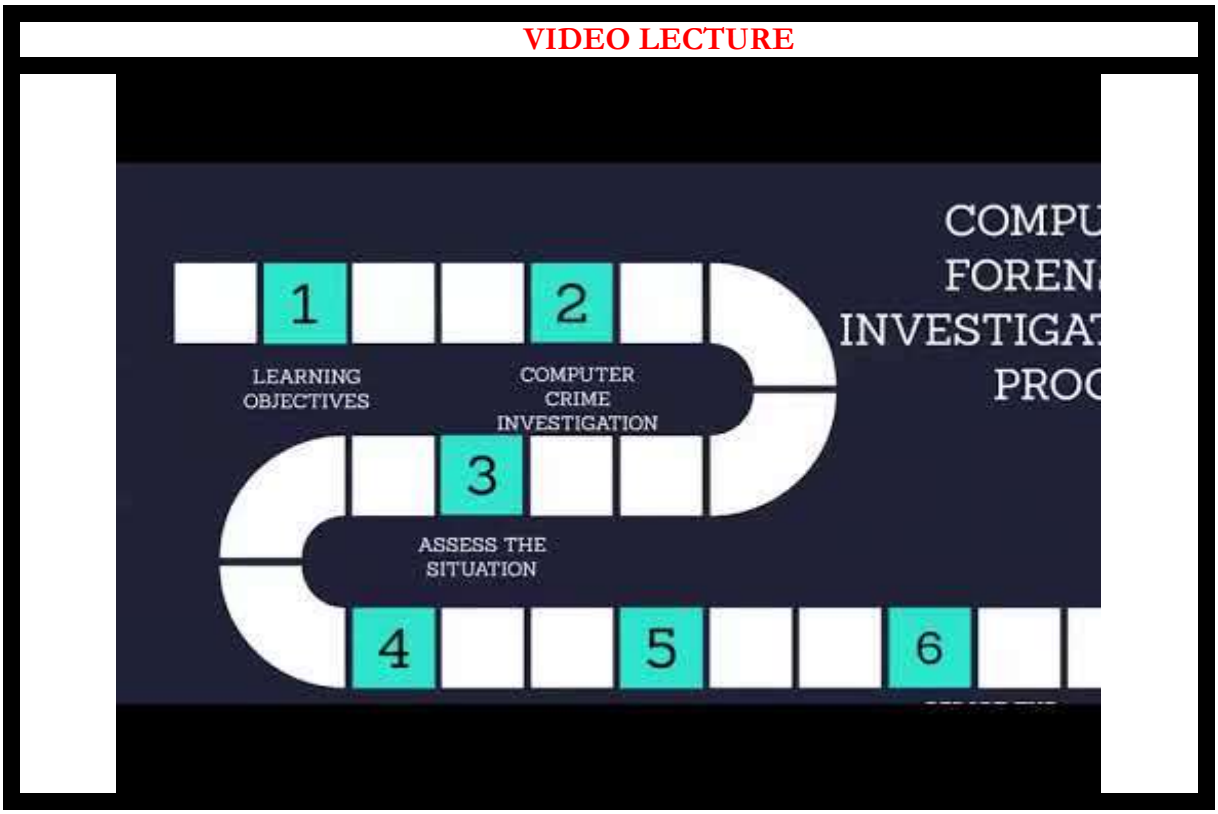
2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Define the process of investigating computer crime
- Apply initial decision-making process
- Assess the situation
- Notify decision makers and acquire authorisation
- Review policies and laws related to forensics investigation process
- Acquire the data
- Analyse the data
- Report the investigation

2.2 INTRODUCTION TO COMPUTER CRIME INVESTIGATION

VIDEO LECTURE



According to Warren G. Kruse II and Jay G. Heiser, authors of *Computer Forensics: Incident Response Essentials*, computer forensics is "the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis."

The computer investigation model shown in figure 1 organizes the different computer forensics elements into a logical flow[1].

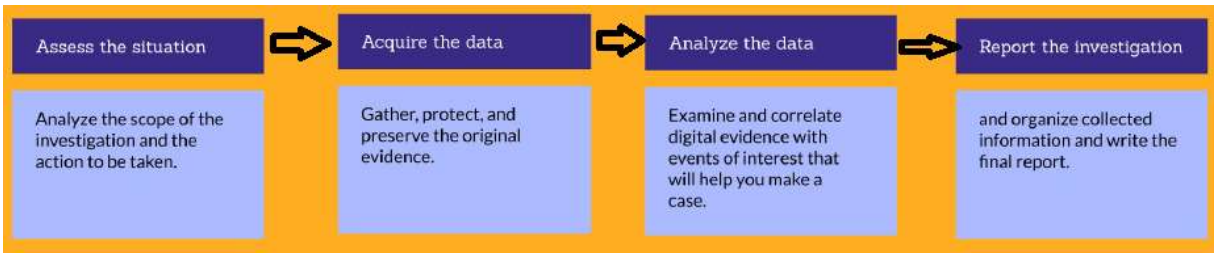


Figure 1: Computer investigation model

The four investigation phases and accompanying processes in the figure should be applied when working with digital evidence. The phases can be summarized as follows:

- **Assess the situation:** Analyze the scope of the investigation and the action to be taken.
- **Acquire the data:** Gather, protect, and preserve the original evidence.
- **Analyze the data:** 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.

Detailed information about each of the phases is provided in the proceeding sections of this unit.

2.2.1 Initial Decision-Making Process

Before you begin each of the general investigation phases you should apply the initial decision-making process shown in the figure 2.

Figure 2: Initial decision-making process

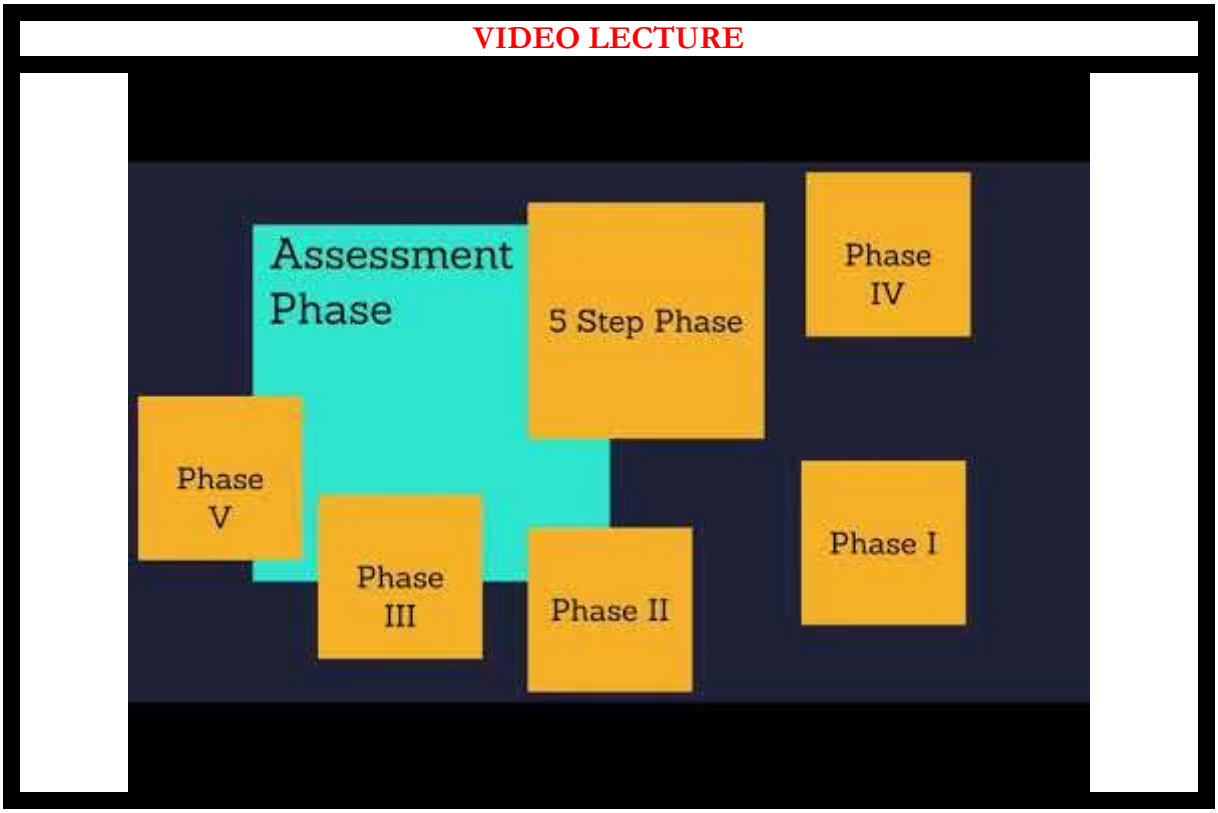
[1] http://www.microsoft.com/en-us/download/details.aspx?id=23378

You should determine whether or not to involve law enforcement with the assistance of legal advisors. If you determine that law enforcement is needed, then you need to continue the internal investigation unless law enforcement officials advise you otherwise. Law enforcement might not be available to assist in the investigation of the incident, so you must continue to manage the incident and investigation for later submission to law enforcement.

Depending on the type of incident being investigated, the primary concern should be to prevent further damage to the organization by those people(s) who caused the incident. The investigation is important, but is secondary to protecting the organization unless there are national security issues.

2.3 ASSESS THE SITUATION

VIDEO LECTURE



This section describes how to conduct a thorough assessment of the situation, how to establish scope, and the required resources for an internal investigation. Use the five-step process shown in the following figure.

Figure 3: Assesment phase of the computer investigation model

2.3.1 Notify Decision Makers and Acquire Authorization

To conduct a computer investigation, you first need to obtain proper authorization unless existing policies and procedures provide incident response authorization. Then you need to conduct a thorough assessment of the situation and define a course of action. Use the following best practices:

- If no written incident response policies and procedures exist, notify decision makers and obtain written authorization from an authorized decision maker to conduct the computer investigation.
- Document all actions you undertake that are related to this investigation. Ensure there is a complete and accurate documented summary of the events and decisions that occurred during the incident and the incident response. This documentation may ultimately be used in court to determine the course of action that was followed during the investigation.
- Depending on the scope of the incident and absent any national security issues or life safety issues, the first priority is to protect the organization from further harm. After the organization is secure, restoration of services (if needed) and the investigation of the incident are the next priorities.

Decisions you make may be questioned as much as the evidence. Because computer evidence is complex, different investigations (such as those conducted by an opposing party) may make different decisions and reach different conclusions.

2.3.2 Review Policies and Laws

At the start of a computer investigation, it is important to understand the laws that might apply to the investigation as well as any internal organization policies that might exist. Note the following important considerations and best practices:

- Determine if you have legal authority to conduct an investigation. Does your organization have policies and procedures that address the privacy rights of employees, contractors, or other persons using your network? Do any such policies and procedures specify the circumstances in which monitoring is allowed? Many organizations state in their policies and procedures that there is no expectation of privacy in the use of the organization's equipment, e-mail, Web services, telephone, or mail, and that the company reserves the right as a condition of employment to monitor and search these resources. Such policies and procedures should be reviewed by the organization's legal advisors, and all employees, contractors, and visitors should be notified of their existence. If you are uncertain about your authority, contact your management, your legal advisors, or (if necessary) your local authorities.

- Consult with your legal advisors to avoid potential issues from improper handling of the investigation. These issues may include:

    - Compromising customers' personal data.

    - Violating any state or federal law, such as federal privacy rules.

    - Incurring criminal or civil liability for improper interception of electronic communications. Consider warning banners.

    - Viewing sensitive or privileged information. Sensitive data that may compromise the confidentiality of customer information must only be made available as part of investigation-related documentation if it directly pertains to the investigation.

- Ensure the following customer privacy and confidentiality issues are addressed:

    - All data should be transferred securely, stored on local computers (not network servers), and should not be easily accessible.

    - All data (including documentation) should be maintained for the period specified by legal advisors or local policy after the computer investigation is closed. If the data is part of a potential criminal case, consult with the law enforcement agency investigating the case. If the case is a civil case, consult with your organization's legal advisors.

- Maintain digital copies of evidence, printouts of evidence, and the chain of custody for all evidence, in case of legal action. Preservation of the chain of custody is accomplished by having verifiable documentation that indicates who handled the evidence, when they handled it, and the locations, dates, and times of where the evidence was stored. Secure storage of evidence is necessary, or custody cannot be verified.

2.3.3 Identify Investigation Team Members

Determining who should respond to an incident is important to conducting a successful internal computer investigation. Ideally, team membership should be established before the team is needed for an actual investigation. It is important that investigation teams be structured appropriately and have appropriate skills. Your organization could establish team membership as part of a disaster recovery planning process. Use the following best practices as guidance for forming an investigation team:

- Identify a person who understands how to conduct an investigation. Remember that the credibility and skills of the person performing the investigation are often scrutinized if a situation results in legal proceedings in a court of law.
- Identify team members and clarify the responsibilities of each team member.
- Assign one team member as the technical lead for the investigation. The technical lead usually has strong technical skills and is experienced in computer investigations. In investigations that involve suspected parties who are technically skilled, you might need to select investigation team members who are more skilled than the suspected parties.
- Keep the investigation team as small as possible to ensure confidentiality and to protect your organization against unwanted information leaks.
- Engage a trusted external investigation team if your organization does not have personnel with the necessary skills.
- Ensure that every team member has the necessary clearance and authorization to conduct their assigned tasks. This consideration is especially important if any third-party personnel, such as consultants, are involved in the investigation.

Important The volatile nature of digital evidence makes it critical to conduct investigations in a timely manner. Be sure to secure availability of all team members for the duration of any investigation.

2.3.4 Conduct a Thorough Assessment

A thorough, clearly documented assessment of the situation is required to prioritize your actions and justify the resources for the internal investigation. This assessment should define the current and potential business impact of the incident, identify affected infrastructure, and obtain as thorough an understanding as possible of the situation. This information will help you define an appropriate course of action.

Use the following best practices to conduct a thorough assessment:

- Use all available information to describe the situation, its potential severity, potentially affected parties, and (if available) the suspected party or parties.

- Identify the impact and sensitivity of the investigation on your organization. For example, assess whether it involves customer data, financial details, health care records, or company confidential information. Remember to evaluate its potential impact on public relations. This assessment will likely be beyond the expertise of IT, and should be done in conjunction with management and legal advisors.

- Analyze the business impact of the incident throughout the investigation. List the number of hours required to recover from the incident, hours of downtime, cost of damaged equipment, loss of revenue, and value of trade secrets. Such an assessment should be realistic and not inflated. The actual costs of the incident will be determined at a later date.

- Analyze affected intangible resources, such as future impact on reputation, customer relationships, and employee morale. Do not inflate the severity of the incident. This analysis is for informational purposes only to help understand the scope of the incident. The actual impact will be determined at a later date. This assessment will likely be beyond the expertise of IT, and should be done in conjunction with management and legal advisors.

Use the following best practices to identify, analyze, and document the infrastructure and computers that are affected by the situation. Much of this guidance could have already been followed as part of a risk assessment process to prepare a disaster recovery plan.

- Identify the network(s) that are involved, the number of computers affected, and the type of computers affected.

- Obtain the network topology documentation, which should include a detailed network diagram that provides infrastructure information about servers, network hardware, firewalls, Internet connections, and other computers on the network.

- Identify external storage devices and any remote computers that should be included. External storage devices could include thumb drives, memory and flash cards, optical discs, and magnetic disks.

- Capture the network traffic over a period of time if live analysis is required. This type of analysis is only needed if you believe there is ongoing suspicious traffic on the network, and is typically only performed after auditing and logging have been exhausted as sources of evidence.

Important Network sniffing (capturing network traffic) can be a breach of privacy, depending on the scope of the capture. You should therefore be very cautious about deploying network capture tools on your network.

- Use tools to examine the state of software applications and operating systems on computers that are likely affected. Useful tools for this task include the Windows application logs, system logs, and Windows Sysinternals PsTools.

- Examine affected file and application servers.

Important Some of the information gathered during this assessment (such as running processes and data in memory) is captured by your tools in real time. You must ensure that any records or logs generated are securely stored to prevent losing this volatile data.

In addition, the following best practices can help you obtain a complete understanding of the situation.

- Build a timeline and map everything to it. A timeline is especially important for global incidents. Document any discrepancies between the date and time of hosts, such as desktop computers, and the system date and time.

- Identify and interview anyone who might be involved in the incident, such as system administrators and users. In some situations, such people might be external to the organization. Interviewing users and affected personnel often provides good results and insights into the situation. Interviews should be conducted by experienced interviewers.

- Document all interview outcomes. You will need to use them later to fully understand the situation.

- Retrieve information (logs) from internal and external facing network devices, such as firewalls and routers, which might be used in the possible attack path.

- Some information, such as IP address and domain name ownership, is often public by its nature. For example, you can use the *Whois* tool available at *https://www.whois.net/* and *https://www.arin.net/index.html* to identify an owner of an IP address.

2.3.5 Prepare for Evidence Acquisition

To prepare for the Acquire the Data phase, you should ensure that you have properly determined the actions and outcome of the Assess the Situation phase. A detailed document containing all information you consider relevant provides a starting point for the next phase and for the final report preparation. In addition, understand that if the incident becomes more than just an internal investigation and requires court proceedings, it is possible that all processes used in gathering evidence might be used by an independent third party to try and achieve the same results.

Such a document should provide detailed information about the situation and include the following:

- An initial estimate of the impact of the situation on the organization's business.

- A detailed network topology diagram that highlights affected computer systems and provides details about how those systems might be affected.

- Summaries of interviews with users and system administrators.
- Outcomes of any legal and third-party interactions.
- Reports and logs generated by tools used during the assessment phase.
- A proposed course of action.

Important Creating consistent, accurate, and detailed documentation throughout the computer investigation process will help with the ongoing investigation. This documentation is often critical to the project's success and should never be overlooked. As you create documentation, always be aware that it constitutes evidence that might be used in court proceedings. Before you begin the next phase, ensure that you have obtained a responsible decision maker's signoff on the documentation that you created during the assessment phase.

2.4 ACQUIRE THE DATA

This section discusses how to acquire the data that is necessary for the investigation. Some computer investigation data is fragile, highly volatile, and can be easily modified or damaged. Therefore, you need to ensure that the data is collected and preserved correctly prior to analysis. Use the three-step process shown in the following figure.

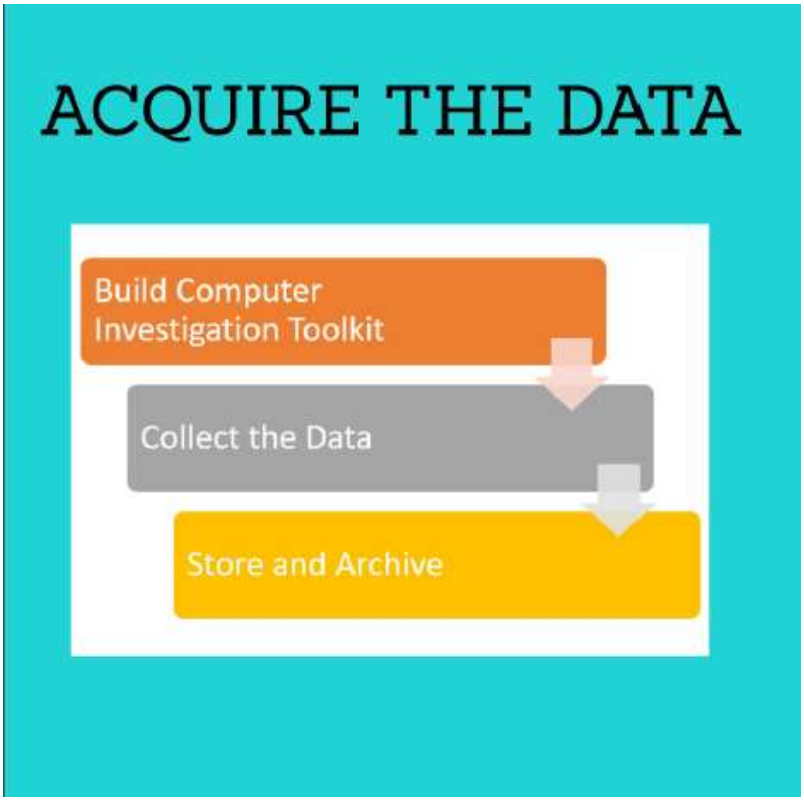
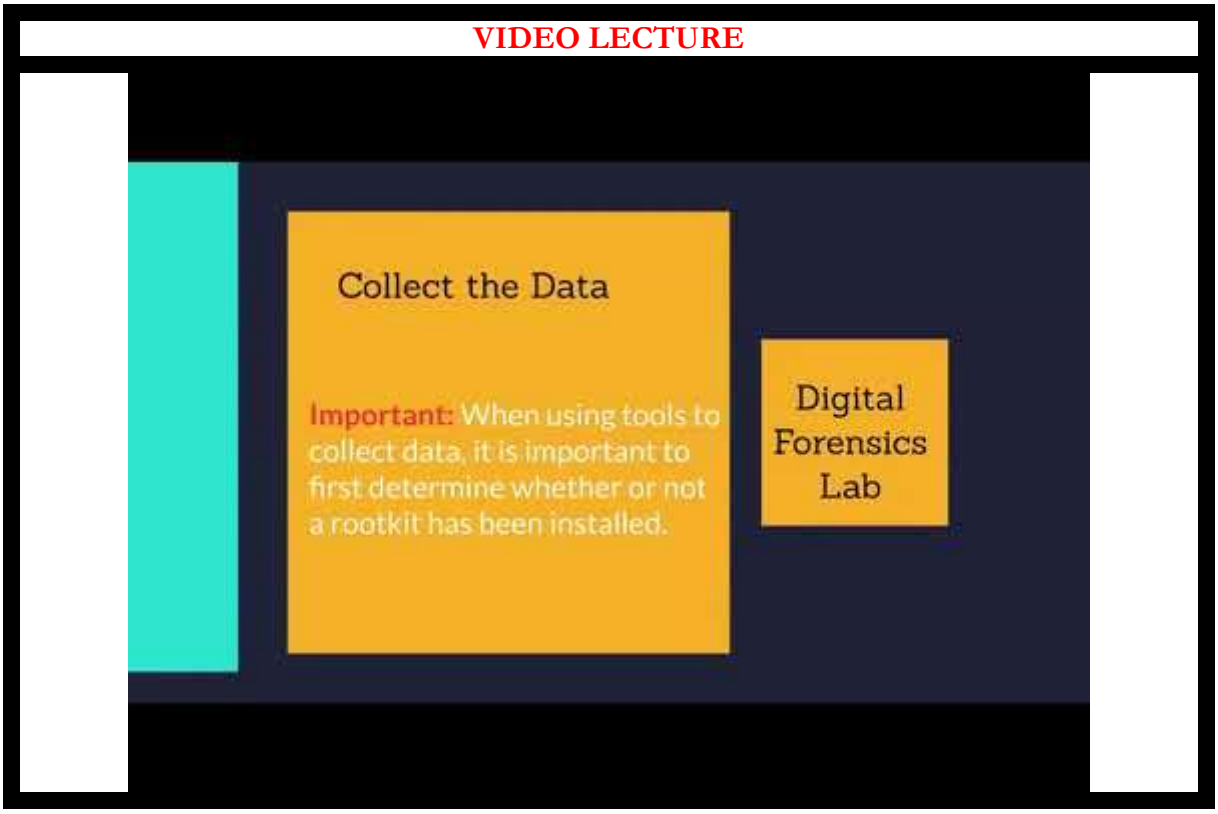


Figure 4: Acquisition phase of the computer investigation model

VIDEO LECTURE



2.4.1 Build Computer Investigation Toolkit

Your organization will need a collection of hardware and software tools to acquire data during an investigation. Such a toolkit might contain a laptop computer with appropriate software tools, operating systems and patches, application media, write-protected backup devices, blank media, basic networking equipment, and cables. Ideally, such a toolkit will be created in advance, and team members will be familiar with the tools before they have to conduct an investigation.

2.4.1.1 Preparing Your Organization for a Computer Investigation

To prepare your organization for an internal computer investigation, you should assemble a readily available computer investigation toolkit that includes software and devices you can use to acquire evidence. Such a toolkit might contain a laptop computer with appropriate software tools, different operating systems and patches, application media, backup devices, blank media, basic networking equipment, and cables. Preparing this toolkit can be an ongoing task as you find the need for various tools and resources, depending upon the investigations you need to conduct.

Use the following guidelines when building and using a computer investigation toolkit:

- Decide which tools you plan to use before you start the investigation. The toolkit will typically include dedicated computer forensics software, such as Sysinternals, Encase, The Forensic Toolkit (FTK) , or ProDiscover.

- Ensure that you archive and preserve the tools. You might need a backup copy of the computer investigation tools and software that you use in the investigation to prove how you collected and analyzed data.
- List each operating system that you will likely examine, and ensure you have the necessary tools for examining each of them.
- Include a tool to collect and analyze metadata.
- Include a tool for creating bit-to-bit and logical copies.
- Include tools to collect and examine volatile data, such as the system state.
- Include a tool to generate checksums and digital signatures on files and other data, such as the File Checksum Integrity Validator (FCIV) tool.
- If you need to collect physical evidence, include a digital camera in the toolkit.

In addition, ensure that your toolkit meets the following criteria:

- Data acquisition tools are shown to be accurate. Proving accuracy is generally easier if you use well-known computer forensics software.
- The tools do not modify the access time of files.
- The examiner's storage device is forensically sterile, which means the disk drive does not contain any data, before it is used. You can determine whether a storage device is forensically sterile by running a checksum on the device. If the checksum returns all zeros, it does not contain any data.
- The examiner's hardware and tools are used only for the computer investigation process and not other tasks.

2.4.2 Collect the Data

Data collection of digital evidence can be performed either locally or over a network. Acquiring the data locally has the advantage of greater control over the computer(s) and data involved. However, it is not always feasible (for example, when computers are in locked rooms or other locations, or when high availability servers are involved). Other factors, such as the secrecy of the investigation, the nature of the evidence that must be gathered, and the timeframe for the investigation will ultimately determine whether the evidence is collected locally or over the network.

Important When using tools to collect data, it is important to first determine whether or not a rootkit has been installed. Rootkits are software components that take complete control of a computer and conceal their existence from standard diagnostic tools. Because rootkits operate at a very low hardware level, they can intercept and modify system calls. You cannot find a rootkit by searching for its executable, because the rootkit removes itself from the list of returned search results. Port scans do not reveal that the ports the rootkit uses are open, because the rootkit

prevents the scanner from detecting the open port. Therefore, it is difficult to ensure that no rootkits exist.

When acquiring data over a network, you need to consider the type of data to be collected and the amount of effort to use. Consider what data you need to obtain that would support the prosecution of the offending parties. For example, it might be necessary to acquire data from several computers through different network connections, or it might be sufficient to copy a logical volume from just one computer.

The recommended data acquisition process is as follows:

1. Create accurate documentation that will later allow you to identify and authenticate the evidence you collect. Ensure that you note any items of potential interest and log any activities that might be of importance later in the investigation. Key to a successful investigation is proper documentation, including information such as the following:

    - Who performed the action and why they did it. What were they attempting to accomplish?

    - How they performed the action, including the tools they used and the procedures they followed.

    - When they performed the action (date and time) and the results.

2. Determine which investigation methods to use. Typically, a combination of offline and online investigations is used.

    - In offline investigations, additional analysis is performed on a bit-wise copy of the original evidence. (A bit-wise copy is a complete copy of all the data from the targeted source, including information such as the boot sector, partition, and unallocated disk space.) You should use the offline investigation method whenever possible because it mitigates the risk of damaging the original evidence. However, this method is only suitable for situations in which an image can be created, so it cannot be used to gather some volatile data.

    - In an online investigation, analysis is performed on the original live evidence. You should be especially careful when performing online analysis of data because of the risk of altering evidence that might be required to prove a case.

3. Identify and document potential sources of data, including the following:

    - Servers. Server information includes server role, logs (such as event logs), files, and applications.

    - Logs from internal and external facing network devices, such as firewalls, routers, proxy servers, network access servers (NAS), and intrusion detection systems (IDS) that may be used in the possible attack path.

- Internal hardware components, such as network adapters (which include media access control (MAC) address information) and PCMCIA cards. Also note external port types, such as Firewire, USB, and PCMCIA.

- Storage devices that need to be acquired (internal and external), including hard disks, network storage devices, and removable media. Don't forget portable mobile devices such as PocketPC, Smartphone devices, and MP3 players such as Zune™.

4. When you must capture volatile data, carefully consider the order in which you collect the data. Volatile evidence can be easily destroyed. Information such as running processes, data loaded into memory, routing tables, and temporary files can be lost forever when the computer is shut down.

5. Use the following methods to collect data from storage media and record storage media configuration information:

    - If you need to remove any internal storage devices, turn off the computer first. However, before you turn off the computer you should verify that all volatile data has been captured whenever possible.

    - Determine whether to remove the storage device from the suspect computer and use your own system to acquire the data. It may not be possible to remove the storage device because of hardware considerations and incompatibilities. Typically, you would not disconnect storage devices such as RAID devices, storage devices with a hardware dependency (for example, legacy equipment), or devices in network storage systems such as storage area networks (SANs).

    - Create a bit-wise copy of the evidence in a backup destination, ensuring that the original data is write-protected. Subsequent data analysis should be performed on this copy and not on the original evidence. Step-by-step guidance for imaging is beyond the scope of this guide but is an integral part of evidence collection.

Important Use industry accepted tools when acquiring a bit-wise copy. For example, EnCase FTK.

    - Document internal storage devices and ensure that you include information about their configurations. For example, note the manufacturer and model, jumper settings, and the size of the device. In addition, note the type of interface and the condition of the drive.

6. Verify the data you collect. Create checksums and digital signatures when possible to help establish that the copied data is identical to the original. In certain circumstances (for example, when a bad sector exists on the storage media) it may be impossible to create a perfect copy. Ensure that you have obtained the best copy possible with the available tools and resources. You can use the Microsoft File Checksum Integrity Verifier (FCIV) tool available at *http://www.microsoft.com/en-us/download/details.aspx?id=11533* to compute an MD5 or SHA1 cryptographic hash of the content of a file.

2.4.3 Store and Archive

When evidence is collected and ready for analysis, it is important to store and archive the evidence in a way that ensures its safety and integrity. You should follow any storage and archival procedures that exist within your organization.

Best practices for data storage and archival include the following:

- Physically secure and store the evidence in a tamperproof location.
- Ensure that no unauthorized personnel has access to the evidence, over the network or otherwise. Document who has physical and network access to the information.
- Protect storage equipment from magnetic fields. Use static control storage solutions to protect storage equipment from static electricity.
- Make at least two copies of the evidence you collected, and store one copy in a secure offsite location.
- Ensure that the evidence is physically secured (for example, by placing the evidence in a safe) as well as digitally secured (for example, by assigning a password to the storage media).
- Clearly document the chain of custody of the evidence. Create a check-in / check-out list that includes information such as the name of the person examining the evidence, the exact date and time they check out the evidence, and the exact date and time they return it.

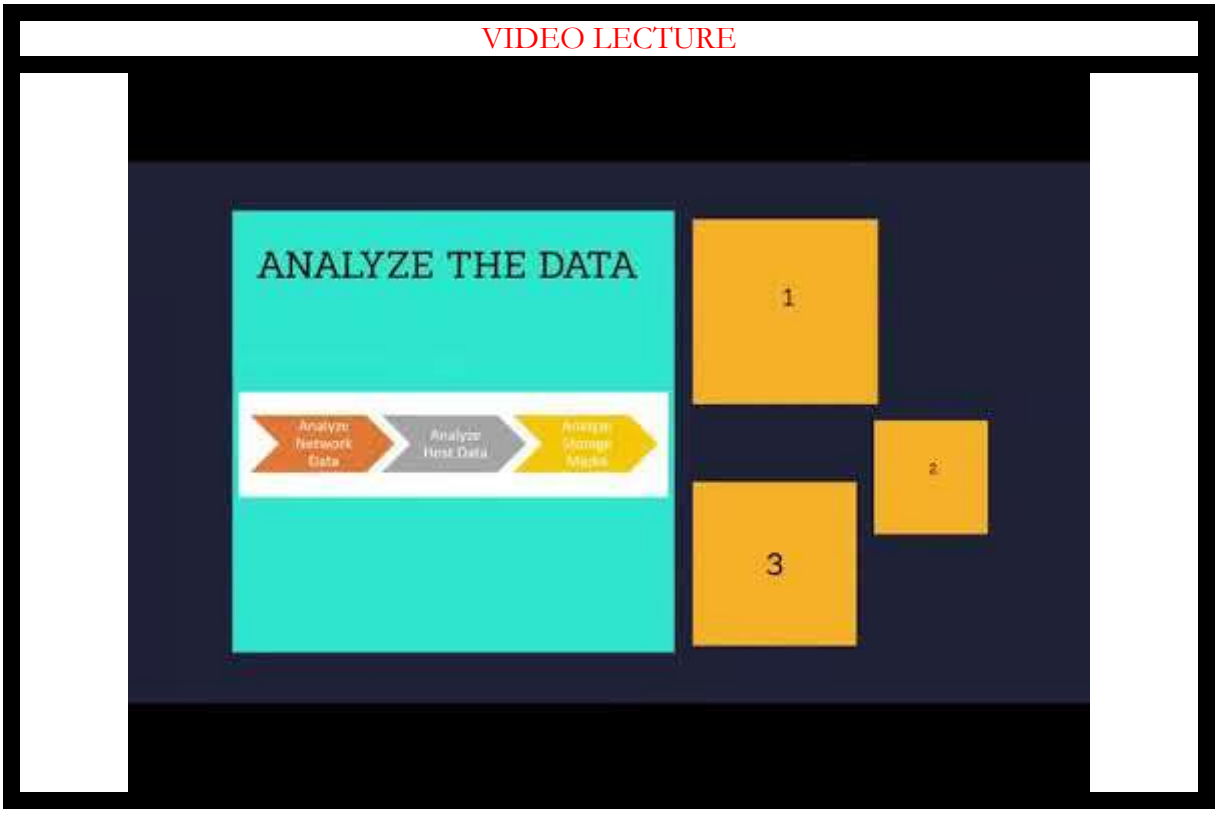
2.5 ANALYZE THE DATA

This section discusses different approaches and well-accepted industry best practices for analyzing the evidence that is gathered during the Acquire the Data phase of an internal investigation. Use the three-step process shown in the following figure.

Figure 5: Analysis phase of the computer investigation model

Important Online analysis of data, which examines a computer directly while it is running, is often necessary. Online analysis is typically performed because of time constraints on an investigation or to capture volatile data. You should be especially careful when performing online analysis to ensure that you minimize the risk to other evidence.

VIDEO LECTURE



2.5.1 Analyze Network Data

In many investigations it is not necessary to analyze network data. Instead, the investigations focus on and examine images of the data. When network analysis is required, use the following procedure:

1. Examine network service logs for any events of interest. Typically, there will be large amounts of data, so you should focus on specific criteria for events of interest such as username, date and time, or the resource being accessed.

2. Examine firewall, proxy server, intrusion detection system (IDS), and remote access service logs. Many of these logs contain information from monitored incoming and outgoing connections and include identifying information, such as IP address, time of the event, and authentication information. You might want to examine the log data in a tool that is suited for data analysis, such as Microsoft® SQL Server™ 2005.

3. View any packet sniffer or network monitor logs for data that might help you determine the activities that took place over the network. In addition, determine whether connections you examine are encrypted—because you will not be able to

read the contents of an encrypted session. However, you can still derive the time of the connection and whether a suspected party established a session with a specific server.

2.5.2 Analyze Host Data

Host data includes information about such components as the operating system and applications. Use the following procedure to analyze the copy of the host data you obtained in the Acquire the Data phase.

1. Identify what you are looking for. There will likely be a large amount of host data, and only a portion of that data might be relevant to the incident. Therefore, you should try to create search criteria for events of interest. For example, you might use the Microsoft Windows® Sysinternals Strings tool to search the files located in the \Windows\Prefetch folder. This folder contains information such as when and where applications were launched.

2. Examine the operating system data, including clock drift information, and any data loaded into the host computer's memory to see if you can determine whether any malicious applications or processes are running or scheduled to run. For example, you can use the Windows Sysinternals AutoRuns tool to show you what programs are configured to run during the boot process or login.

3. Examine the running applications, processes, and network connections. For example, you can look for running processes that might have an appropriate name but are running from non-standard locations.

2.5.3 Analyze Storage Media

The storage media you collected during the Acquire the Data phase will contain many files. You need to analyze these files to determine their relevance to the incident, which can be a daunting task because storage media such as hard disks and backup tapes often contain hundreds of thousands of files.

Identify files that are likely to be relevant, which you can then analyze more closely. Use the following procedure to extract and analyze data from the storage media you collected:

1. Whenever possible, perform offline analysis on a bit-wise copy of the original evidence.

2. Determine whether data encryption was used, such as the Encrypting File System (EFS) in Microsoft Windows. Several registry keys can be examined to determine whether EFS was ever used on the computer. If you suspect data encryption was used, then you need to determine whether or not you can actually recover and read the encrypted data. Your ability to do so will depend upon different circumstances, such as the version of Windows, whether or not it is a domain-joined computer, and how EFS was deployed. For more information about EFS see "The Encrypting File

System" on Microsoft TechNet. External EFS recovery tools are also available, such as Advanced EFS Data Recovery by Elcomsoft.

3. If necessary, uncompress any compressed files and archives. Although most forensic software can read compressed files from a disk image, you might need to uncompress archive files to examine all files on the media you are analyzing.

4. Create a diagram of the directory structure. It might be useful to graphically represent the structure of the directories and files on the storage media to effectively analyze the files.

5. Identify files of interest. If you know which files were affected by the security incident, you can focus the investigation on these files first. The hash sets created by the National Software Reference Library can be used to compare well-known files (such as operating system and application files) to the originals. Those files that match can normally be eliminated from the investigation. You can also use informational sites such as filespecs.com, Wotsit's Format, ProcessLibrary.com, and Microsoft DLL Help to help you categorize and collect information about existing file formats as well as to identify files.

6. Examine the registry, the database that contains Windows configuration information, for information about the computer boot process, installed applications (including those loaded during startup), and login information such as username and logon domain. For registry background information and detailed descriptions of registry content, see the Windows Server 2003 Resource Kit Registry Reference. Various tools are available for analyzing the registry, including RegEdit, which ships with the Windows operating system, Windows Sysinternals RegMon for Windows, and Registry Viewer by AccessData.

7. Search the contents of all gathered files to help identify files that may be of interest. Various intelligent searches can be performed using tools described in the "Tools" section in Appendix: Resources of this guide. For example, you can use the Windows Sysinternals Streams tool to reveal whether there are any NTFS alternate data streams used on files or folders. NTFS alternate data streams can hide information within a file by causing it to appear to contain zero bytes of data when viewed through Windows Explorer although the file actually contains hidden data.

8. Study the metadata of files of interest, using tools such as Encase by Guidance Software, The Forensic Toolkit (FTK) by AccessData, or ProDiscover by Technology Pathways. File attributes such as timestamps can show the creation, last access, and last written times, which can often be helpful when investigating an incident.

9. Use file viewers to view the content of the identified files, which allow you to scan and preview certain files without the original application that created them. This approach protects files from accidental damage, and is often more cost effective than

using the native application. Note that file viewers are specific to each type of file; if a viewer is not available, use the native application to examine the file.

After you analyze all of the available information, you may be able to reach a conclusion. However, it is important to be very cautious at this stage and ensure that you do not blame the wrong party for any damages. However, if you are certain of your findings, you will be ready to begin the Report the Investigation phase.

2.6 REPORT THE INVESTIGATION

This section discusses how to organize the information that you gather and the documentation that you create throughout a computer investigation, as well as how to write a final report. Use the two-step process shown in the following figure.

Figure 6: Reporting phase of the computer investigation model

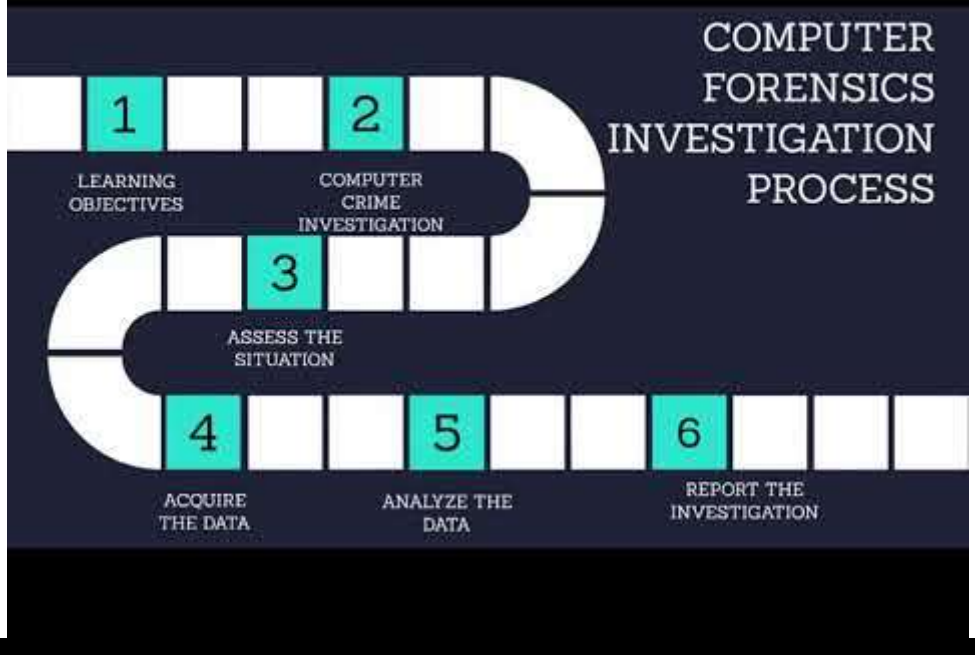
2.6.1 Gather and Organize Information

During the initial phases of a computer investigation you create documentation about the specific activities in each phase. From within this documentation you need to identify the specific information that is relevant to your investigation and organize it into appropriate categories. Use the following procedure to gather and organize the required documentation for the final report.

1. Gather all documentation and notes from the Assess, Acquire, and Analyze phases. Include any appropriate background information.
2. Identify parts of the documentation that are relevant to the investigation.
3. Identify facts to support the conclusions you will make in the report.
4. Create a list of all evidence to be submitted with the report.
5. List any conclusions you wish to make in your report.

6. Organize and classify the information you gather to ensure that a clear and concise report is the result.

VIDEO LECTURE



2.6.2 Write the Report

After you organize the information into appropriate categories, you can use it to write the final report. It is critical to the outcome of the investigation that the report is clear, concise, and written for the appropriate audience.

The following list identifies recommended report sections and information that should be included in these sections.

- **Purpose of Report**: Clearly explain the objective of the report, the target audience, and why the report was prepared.
- **Author of Report**: List all authors and co-authors of the report, including their positions, responsibilities during the investigation, and contact details.
- **Incident Summary**: Introduce the incident and explain its impact. The summary should be written so that a non-technical person such as a judge or jury would be able to understand what occurred and how it occurred.

- **Evidence**: Provide descriptions of the evidence that was acquired during the investigation. When describing evidence state how it was acquired, when, and who acquired it.

- **Details**: Provide a detailed description of what evidence was analyzed and the analysis methods that were used. Explain the findings of the analysis. List the procedures that were followed during the investigation and any analysis techniques that were used. Include proof of your findings, such as utility reports and log entries. Justify each conclusion that is drawn from the analysis. Label supporting documents, number each page, and refer to them by label name when they are discussed in the analysis. For example, "Firewall log from server, supporting document D." Also, provide information about those individuals who conducted or were involved with the investigation. If applicable, provide a list of witnesses.

- **Conclusion:** Summarize the outcome of the investigation. The conclusion should be specific to the outcome of the investigation. Cite specific evidence to prove the conclusion, but do not provide excessive detail about how the evidence was obtained (such information should be in the "Details" section). Include justification for your conclusion, along with supporting evidence and documentation. The conclusion should be as clear and unambiguous as possible. In many cases, it will be stated near the beginning of the report, because it represents the actionable information.

- **Supporting documents**: Include any background information referred to throughout the report, such as network diagrams, documents that describe the computer investigation procedures used, and overviews of technologies that are involved in the investigation. It is important that supporting documents provide enough information for the report reader to understand the incident as completely as possible. As mentioned earlier, label each supporting document with letters and number each page of the document. Provide a complete list of supporting documents.

    - If it is likely that the report will be presented to a varied audience, consider creating a glossary of terms used in the report. A glossary is especially valuable if the law enforcement agency is not knowledgeable about technical issues or when a judge or jury needs to review the documents.

2.7 SUMMARY

1. Computer forensics is "the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis.

2. Depending on the type of incident being investigated, the primary concern should be to prevent further damage to the organization by those people(s) who caused the incident.

3. To conduct a computer investigation, you first need to obtain proper authorization unless existing policies and procedures provide incident response authorization.

4. At the start of a computer investigation it is important to understand the laws that might apply to the investigation as well as any internal organization policies that might exist.

5. Preservation of the chain of custody is accomplished by having verifiable documentation that indicates who handled the evidence, when they handled it, and the locations, dates, and times of where the evidence was stored.

6. Determining who should respond to an incident is important to conducting a successful internal computer investigation.

7. The volatile nature of digital evidence makes it critical to conduct investigations in a timely manner.

8. Creating consistent, accurate, and detailed documentation throughout the computer investigation process will help with the ongoing investigation.

9. Your organization will need a collection of hardware and software tools to acquire data during an investigation. Such a toolkit might contain a laptop computer with appropriate software tools, operating systems and patches, application media, write-protected backup devices, blank media, basic networking equipment, and cables.

10. Data collection of digital evidence can be performed either locally or over a network.

11. When using tools to collect data, it is important to first determine whether or not a rootkit has been installed.

12. When evidence is collected and ready for analysis, it is important to store and archive the evidence in a way that ensures its safety and integrity.

13. In many investigations it is not necessary to analyze network data. Instead, the investigations focus on and examine images of the data.

14. The storage media you collected during the Acquire the Data phase will contain many files.

15. After you organize the information into appropriate categories, you can use it to write the final report. It is critical to the outcome of the investigation that the report is clear, concise, and written for the appropriate audience.

2.8 CHECK YOUR PROGRESS

1. Fill in the blanks

   i. Assign one team member as the _____ for the investigation.

   ii. EFS stands for _____.

   iii. During the initial phases of a computer investigation you create _____about the specific activities in each phase.

iv. If no written incident response policies and procedures exist, notify decision makers and obtain written authorization from an _____ decision maker to conduct the computer investigation.

v. After the organization is secure, _____and the_____ of the incident are the next priorities.

vi. Consult with your _____to avoid potential issues from improper handling of the investigation.

vii. Preservation of the _____is accomplished by having verifiable documentation that indicates who handled the evidence, when they handled it, and the locations, dates, and times of where the evidence was stored.

viii. Analyze the _____of the incident throughout the investigation.

ix. Capture the _____ over a period of time if live analysis is required.

x. _____ can be a breach of privacy, depending on the scope of the capture.

xi. A_____ is especially important for global incidents.

xii. _____users and affected personnel often provides good results and insights into the situation.

xiii. As you create documentation, always be aware that it constitutes _____that might be used in court proceedings.

xiv. _____ are software components that take complete control of a computer and conceal their existence from standard diagnostic tools.

xv. Include a tool to collect and analyze _____.

2. State True or False

i. The storage media you collected during the Acquire the Data phase will contain many files.

ii. Inflate the severity of the incident.

iii. Whenever possible, perform online analysis on a bit-wise copy of the original evidence.

iv. Maintain digital copies of evidence, printouts of evidence, and the chain of custody for all evidence, in case of legal action.

v. Engage a trusted external investigation team if your organization does not have personnel with the necessary skills.

vi. Retrieve information (logs) from internal and external facing network devices, such as firewalls and routers, might be used in the possible attack path.

2.9 ANSWERS TO CHECK YOUR PROGRESS

1. Fill in the blanks

   i. Technical lead

   ii. Encrypting File System.

   iii. Documentation

   iv. Authorized

   v. restoration of services , investigation

   vi. Legal advisors

   vii. Chain of custody

   viii. Business impact

   ix. Network traffic

   x. Network sniffing

   xi. Timeline

   xii. Evidence

   xiii. Rootkits

   xiv. Metadata

2. State true or false

   i. True

   ii. False

   iii. True

   iv. True

   v. True

   vi. True

2.10 SUGGESTED READING

1. Boiarkine, V., Carter, R., Chappell, L., Cullimore, P., Quilty, T., Slater, P., et al. (2007, Jan.). *Fundamental Computer Investigation Guide for Windows.* (S. Wacker, Red.)

Onttrek Nov. 12, 2015 uit http://www.microsoft.com/en-us/download/details.aspx?id=23378

2. Carvey, H. *Windows Forensic Analysis DVD Toolkit, Second Edition.* SYNGRESS.
3. Ligh, M. H., Case, A., Levy, J., & Walters, A. *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory 1st Edition.* Wiley.

2.11 MODEL QUESTIONS

1. What is computer forensics? Define.
2. What is network sniffing? List some popular tools used for packet sniffing.
3. What are the different phases of investigation process? Explain with the help of a diagram.
4. Why initial decision making process is important?
5. What are the different steps involved in the assessment of the situation?
6. What are the important guidelines for forming an investigating team?
7. What are the components of a computer investigation toolkit?
8. Explain the data acquisition process in detail.
9. List all the important sections that should be included in the investigation report.

References, Article source and Contributors

EXPERT PANEL

Dr. Jeetendra Pande, Associate Professor- Computer Science, School of Computer Science & IT, Uttarakhand Open University, Haldwani

Dr. Ajay Prasad, Sr. Associate Professor, University of Petroleum and Energy Studies, Dehradun

Dr. Akashdeep Bharadwaj, Professor, University of Petroleum and Energy Studies, Dehradun

Mr. Sridhar Chandramohan Iyer, Assistant Professor- Universal College of Engineering, Kaman, Vasai, University of Mumbai

Mr. Rishikesh Ojha, Digital Forensics and eDiscovery Expert

Ms. Priyanka Tewari, IT Consultant

Mr. Ketan Joglekar, Assistant Professor, GJ College, Maharastra

Dr. Ashutosh Kumar Bhatt, Associate Professor, Uttarakhand Open University, Haldwani

Dr. Sangram Panigrahi, Assistant Professor, Siksha 'O' Anusandhan,, Bhubaneswar

This MOOC has been prepared with the support of