

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.

2.5.4 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.

2.5.5 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.

2.5.6 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.

2.9 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.

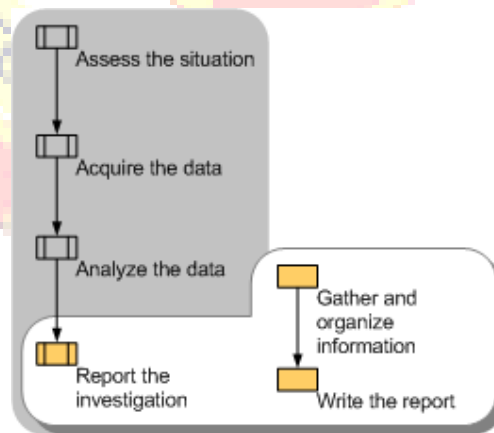


Figure 6: Reporting phase of the computer investigation model

2.6.3 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.

2.6.4 Write the Report

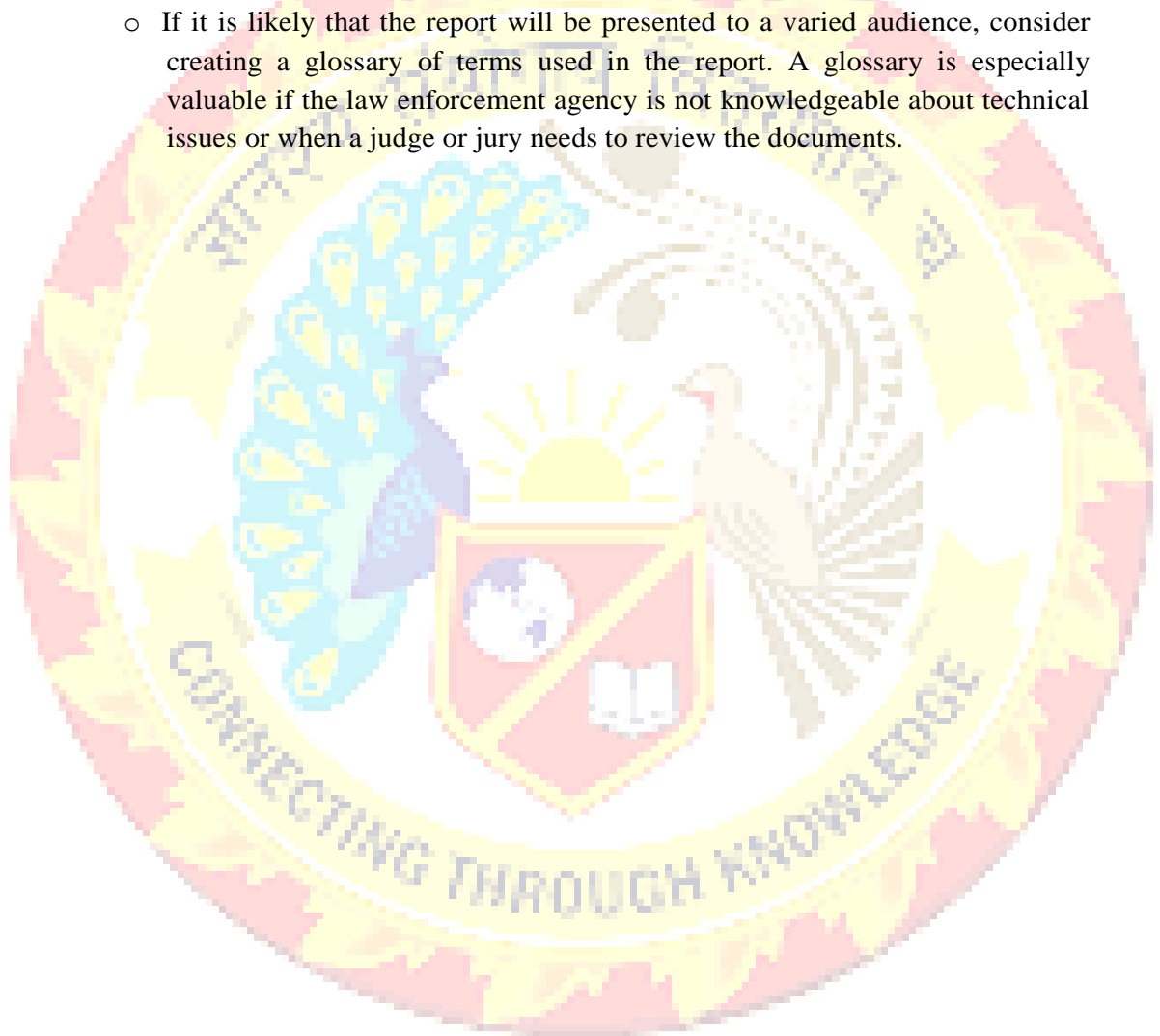
After you organize the information into appropriate categories, you can use it to write the final report. It is critical to the outcome of the investigation that the report is clear, concise, and written for the appropriate audience.

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.



Centurion

UNIVERSITY