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.

2.5 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.

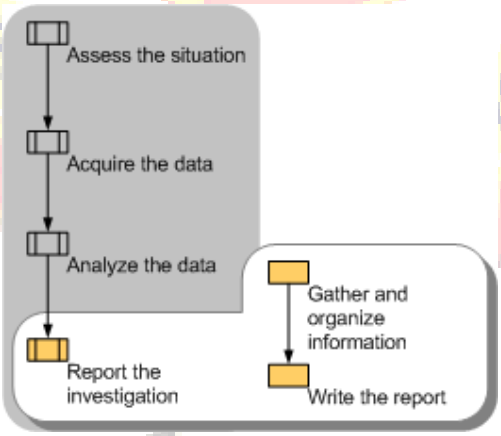

Figure 6: Reporting phase of the computer investigation model

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.

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.