- 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.

2.7 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.

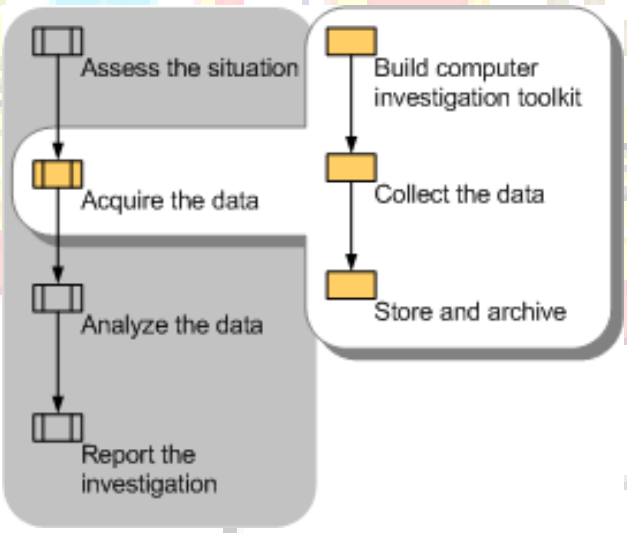

Figure 4: Acquisition phase of the computer investigation model

2.4.4 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.

2.4.4.1 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.

2.4.5 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:

7. 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.
8. 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.
9. 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™.

10. 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.
11. 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.
12. 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.

2.4.6 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.

2.8 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.

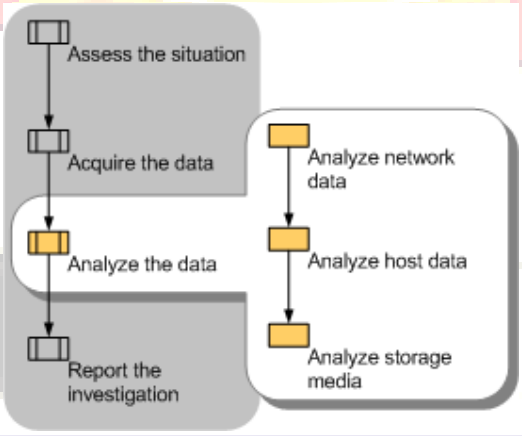

Figure 5: Analysis phase of the computer investigation model

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