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.

2.3 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.

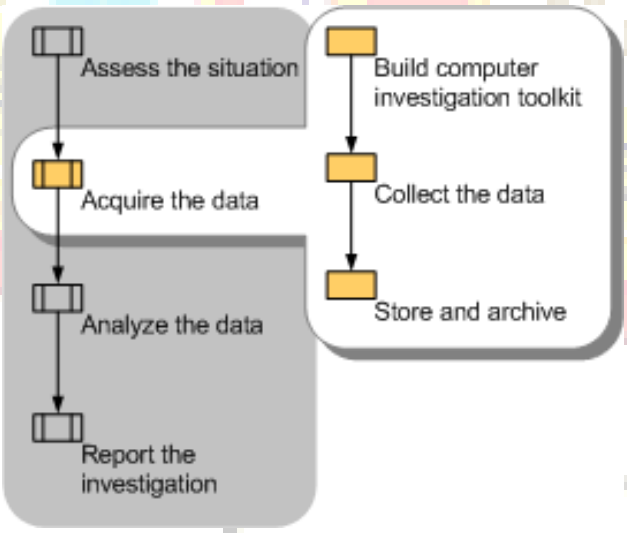

Figure 4: Acquisition phase of the computer investigation model

2.4.1 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.