PART 2

Digital Investigations

CHAPTER 6

Conducting Digital Investigations

Eoghan Casey and Bradley Schatz

CONTENTS

The goal of any investigation is to uncover and present the truth. Although this chapter will deal primarily with truth in the form of digital evidence, this goal is the same for all forms of investigation whether it be in pursuit of a murderer in the physical world or trying to track a computer intruder online. As noted in the Introduction, when evidence is presented as truth of an allegation, it can influence whether people are deprived of their livelihoods and liberties, and potentially whether they live or die. This is reason enough to seek to use trusted methodologies and techniques to ensure that the analysis, interpretation, and reporting of evidence are reliable, objective, and transparent. This chapter compares several methodologies, highlighting commonalities and providing practical perspectives on approaches to uncover truths to serve justice. This chapter then covers how the scientific method can be applied in each step of a digital investigation.

An investigative scenario is provided at the end of this chapter to demonstrate how the methodologies can be applied to an actual case. This case example is based on abstracted lessons from various investigations. Any resemblance to actual incidents is coincidental.

Digital investigations inevitably vary depending on technical factors such as the type of computing or communications device, whether the investigation is in a criminal, civil, commercial, military, or other context, and case-based factors such as the specific claims to be investigated. Despite this variation, there exists a sufficient amount of similarity between the ways digital investigations are undertaken that commonalities may be observed. These commonalities tend to be observed from a number of perspectives, with the primary ways being process, principles, and methodology.

6.1 DIGITAL INVESTIGATION PROCESS MODELS

Early attempts to describe how one conducted a digital investigation tended to focus on practical stepwise approaches to solving particular investigative challenges, within the context of particular technical computing environments.

Digital Evidence and Computer Crime, Third Edition

For example, early descriptions of investigative procedures related to incident response provided practical guidance for investigating computer crime within networked computer systems (Madia, Prosise, & Pepe, 2003). However, the tasks described in these guidelines were not generally applicable to investigations of other types and within other contexts (Reith, 2002).

Numerous subsequent efforts determined that, when attempting to conceive of a general approach to describe the investigation process within digital forensics, one should make such a process generalizable. This led to the proposal of a number of models for describing investigations, which have come to be known as "process models."

The motivations for developing process models are numerous. Such process models serve as useful points of reference for reflecting on the state and nature of the field, as a framework for training and directing research, and for benchmarking performance against generally accepted practice. Using a formalized methodology encourages a complete, rigorous investigation, ensures proper evidence handling, and reduces the chance of mistakes created by preconceived theories, time pressures, and other potential pitfalls. Another purpose of these models is to refine our understanding of what is required to complete a comprehensive and successful investigation in a way that is independent of a particular technology in corporate, military, and law enforcement environments. An effective process model identifies the necessary steps to achieve goals, and can be applied to new technologies that become a source of digital evidence. Finally, these models are useful for the development of case management tools, Standard Operating Procedures (SOPs), and investigative reports.

Ultimately, these process models are intended to serve digital investigations, and not to dictate. Every investigation is unique and can bring unforeseeable challenges, so process models and other methodologies should not be viewed as an end-point but rather as a framework or foundation upon which to build. Furthermore, as with any tool, investigative process models can be useful under certain circumstances but have limitations. Therefore, it is important to be familiar with the various process models and the extent to which they apply to a given situation.

Process models have their origins in the early theories of computer forensics which defined the field in terms of a linear process. For example, in 1999, McKemmish defined forensic computing as follows:

> The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable.
>
> **(McKemmish, 1999)**

The above sequence of activities, *identification, preservation, analysis, and presentation*, arguably is the basis of the process model view of digital investigations,

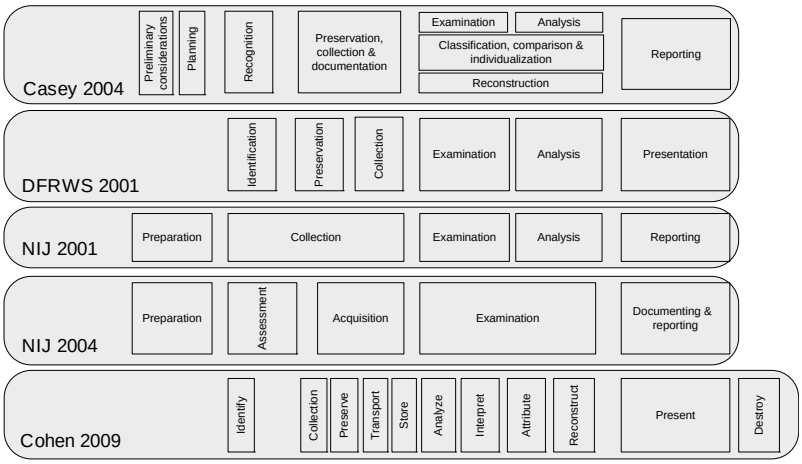

FIGURE 6.1

A comparison of terminology related to digital investigation process models.

when one looks beyond differences in terminology and granularity. However, certain process models address nuances that are important to consider when conducting a digital investigation. The results of a comparison of the terminology used for describing the steps of linear process models are presented in Figure 6.1. The most common steps for conducting a complete and competent digital investigation are:

- ***Preparation:*** Generating a plan of action to conduct an effective digital investigation, and obtaining supporting resources and materials.
- ***Survey/Identification:*** Finding potential sources of digital evidence (e.g., at a crime scene, within an organization, or on the Internet). Because the term *identification* has a more precise meaning in forensic science relating to the analysis of an item of evidence, this process can be more clearly described as *survey* of evidence. Survey is used throughout this chapter when referring to this step.
- ***Preservation:*** Preventing changes of *in situ* digital evidence, including isolating the system on the network, securing relevant log files, and collecting volatile data that would be lost when the system is turned off. This step includes subsequent *collection* or *acquisition*.[1]
- ***Examination and Analysis:*** Searching for and interpreting trace evidence. Some process models use the terms *examination* and *analysis* interchangeably.

[1] A nuance of the meaning of preservation is that it is used to refer in an inclusive way to prevention of changes to potential evidence, including collection and acquisition, whereas it is additionally used in some contexts to describe the evidence management activities related to storing and maintaining of digital evidence and provenance information once the potential evidence is in custody.

In this chapter, a clear distinction is made between these two steps in a digital investigation, where forensic examination is the process of extracting and viewing information from the evidence, and making it available for analysis. In contrast, forensic analysis is the application of the scientific method and critical thinking to address the fundamental questions in an investigation: who, what, where, when, how, and why.

- ***Presentation:*** Reporting of findings in a manner which satisfies the context of the investigation, whether it be legal, corporate, military, or any other.

Despite the similarities identified above, terminology is not well defined and is often inconsistent between process models, and the subtleties implied are not clearly perceivable. For example, the distinction between "examination" and "analysis" is unclear in many of these process models.

In general, the differences between these process models may be explained by the way they dissect the investigative process. Some models use broad categories, whereas others divide the process into more discrete steps. In many instances, the differences between models may be explained by a more refined viewpoint developed over time, with the promotion of subtasks to first-class citizens. For example, the "collection" step in the 2001 NIJ model was replaced with two discrete steps in the 2004 NIJ model: "assessment" and "acquisition."

6.1.1 Physical Model

Carrier's Integrated Digital Investigation Process model distinguishes itself by relating the digital investigative process with the more established investigative process associated with physical crime scenes, conceptualizing the computer or digital device itself as a crime scene (Carrier & Spafford, 2003). The overall process model has 17 phases organized into five groups: Readiness, Deployment, Physical Crime Scene Investigation, Digital Crime Scene Investigation, and Presentation, summarized in Table 6.1 for both physical and digital investigations.

This construct is useful from the physical perspective as all digital evidence ultimately exists in physical space.

> A computer being investigated can be considered a digital crime scene and investigations as a subset of the physical crime scene where it is located. Physical evidence may exist around a server that was attached by an employee and usage evidence may exist around a home computer that contains contraband. Furthermore, the end goal of most digital investigation is to identify a person who is responsible and therefore the digital investigation needs to be tied to a physical investigation.
>
> **(Carrier & Spafford, 2004)**

Table 6.1 Phases of Digital and Physical Investigations in Carrier's Integrated Digital Investigation Process Model

	Phase Goals (Physical)	Phase Goals (Digital)
Crime scene preservation	Securing entrances and exits and preventing physical changes to evidence	Preventing changes in potential digital evidence, including network isolation, collecting volatile data, and copying entire digital environment
Crime scene survey	Walking through scene, identifying obvious and fragile physical evidence	Identification of obvious evidence by searching in digital evidence (typically in lab)
Crime scene documentation	Photographs, sketches, maps of evidence, and crime scene	Photographs of digital devices and individuated descriptions of digital devices
Crime scene search and collection	In-depth search for physical evidence	Analysis of system for nonobvious evidence (typically in lab)
Crime scene reconstruction	Developing theories based on analysis results and testing against evidence	

Furthermore, by explicitly drawing a parallel between the handling of digital and physical crime scenes, this model encourages the transfer of mature crime scene investigation techniques from the physical forensic sciences to the digital. At the same time, it is important to keep in mind there are significant differences between digital and physical crime scenes that may limit the applicability of this process model in certain situations. Digital and physical crime scenes are compared here:

1. Physical crime scene investigators are in the crime scene itself, where they can see, smell, touch, hear, and taste evidence. Conversely, we view digital crime scenes through various layers of abstraction, including the operating system and forensic tools (Carrier, 2003). With virtualization, digital investigators can see certain aspects of the computer as the user saw them, but the majority of artifacts of forensic significance remain latent.
2. In traditional forensic sciences, there are two distinct realms: crime scene investigation and forensic laboratory processing. Initially, at a high level, a computer or other source of digital evidence can be thought of as a crime scene. However, at some point in the investigation, it becomes more like a specimen that is processed in a forensic laboratory. In both the physical and digital realms, procedures and expertise for processing a crime scene are distinct from processing a specimen in a laboratory environment. Carrier's model correctly considers the results of such laboratory analysis as input to the crime reconstruction process, but does not cover how this analysis is performed.

3. Digital crime scenes can be searched with a higher degree of thoroughness and specificity than physical ones. Although sniffer dogs, luminol, and other tools provide presumptive tests for certain substances, physical crime scene investigators cannot replicate and search an entire crime scene at the molecular level, whereas the physical properties of the digital crime scene allow a perfect duplicate of the crime scene to be made for later examination and analysis. Arguably, it is as economically infeasible to search the average digital crime scene completely at the bit level as it is to search a physical crime scene at the molecular level.

The differences between searching physical and digital crime scenes are significant, creating various challenges for digital investigators and legislators. The abstraction layers that translate raw data into a form that digital investigators can review may introduce errors (Carrier, 2003; Casey, 2002). The potential for error in data representation is unique to digital crime scenes and requires digital investigators to take extra precautions such as comparing the results of multiple tools and inspecting data at lower levels to double-check the veracity of the information that has been displayed through their forensic tools. In addition, digital investigators searching a digital crime scene may encounter information of a very personal nature and may even find evidence relating to other crimes. Legislators continue to wrestle with these issues as they consider how expectations of privacy and plain view apply to digital crime scenes.

6.1.2 Staircase Model

The investigative process model from the previous edition of this book, and depicted as a sequence of ascending stairs in Figure 6.2, provides a practical and methodical approach to conducting an effective digital investigation (Casey & Palmer, 2004). Digital investigators, forensic examiners, and attorneys work together to scale these steps from bottom to top in a systematic, determined manner in an effort to present a compelling story after reaching the final step of persuasion/testimony.

The categories in Figure 6.2 are intended to be as generic as possible. The unique methods and tools employed in each category tie the investigative process to a particular forensic domain. The terms located on the riser of each step are those more closely associated with the law enforcement perspective. To the right of each term is a more general descriptor that captures the essence of each step of the process.

Although depicted as a linear progression of events in Figure 6.2, the steps in this process often proceed simultaneously and it may be necessary to take certain steps more than once at different stages of an investigation or as new information emerges. Also, most steps are not only "digital forensic" in nature—many parts of the process function by applying and integrating methods and

FIGURE 6.2

Categories of the investigative process model (depicted as a flight of stairs) from *Digital Evidence and Computer Crime*, 2nd edition.

techniques in police science and criminalistics as aids. Finally, as with most processes, there is a relationship between successive steps. That relationship can often be described by the input and output expected at each stage, with products of one step feeding into the steps that follow.

One item of particular note and special importance stands out in this process model. First, case management is depicted as a handrail in Figure 6.2 because it plays a vital role in any investigation and spans across all the steps in the process model. It provides stability and enables investigators to tie all relevant information together, allowing the story to be told clearly. In many cases, the mechanisms used to structure, organize, and record pertinent details about all events and physical exhibits associated with a particular investigation are just as important as the information presented.

This model could be simplified by treating recovery, harvesting, reduction, organization, and search as subcomponents of the examination step. In addition, it could be made more comprehensive by adding a step to cover the transportation of evidence.

6.1.3 Evidence Flow Model

Ó Ciardhuáin's model goes beyond the steps required to preserve and examine digital evidence, incorporating nontechnical aspects of a digital investigation like authorization, notification, proof/defense, and transportation of

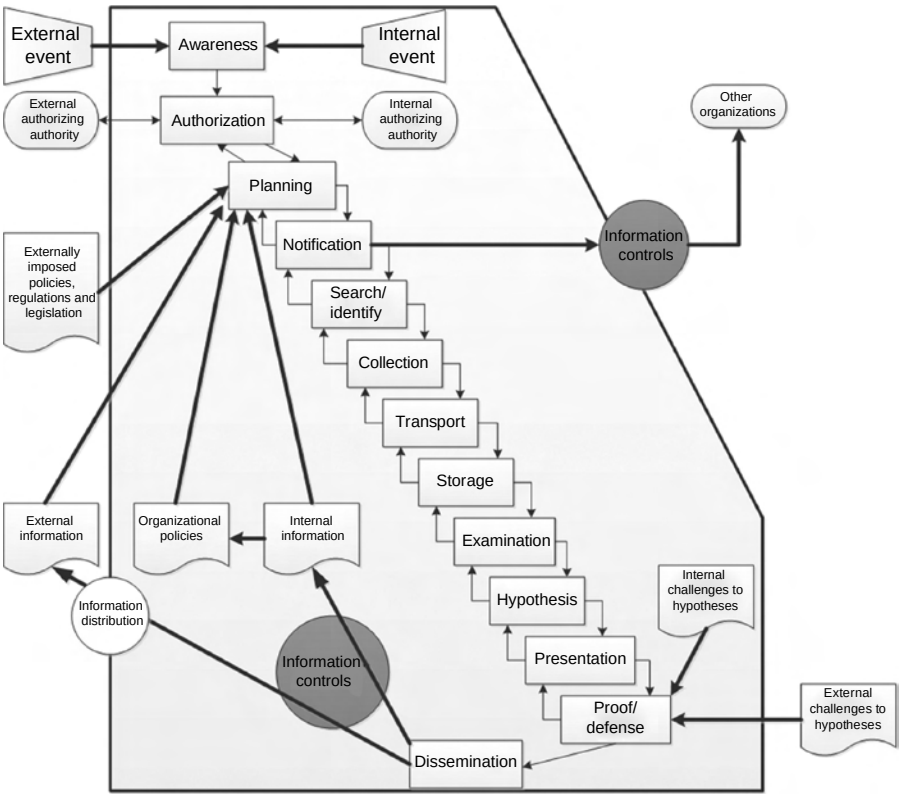

FIGURE 6.3
Ó Ciardhuáin's extended model of cybercrime investigations.

evidence (Ó Ciardhuáin, 2004). The main goal of this model is to completely describe the flow of information in a digital investigation, from the moment digital investigators are alerted until the investigation reaches its conclusion (Figure 6.3).

By concentrating on the flow of information, appropriate controls can be implemented at each step of the process to handle evidentiary data, written reports, or communications relating to the investigation. In this way, this model addresses the overall management of a case as well as individual tasks, and recognizes the importance of preventing information "leakage" in addition to maintaining the authenticity and integrity of digital evidence.

This process model is sufficiently general to be applied to any environment and technology. Its primary strength is the notion of a continuous flow of information, which emphasizes the importance of maintaining chain of custody, and protecting confidentiality and privacy.

One weakness of this model is that it excludes certain steps that are present in other models such as the return or destruction of evidence at the end of an investigation (Reith, Carr, & Gunsch, 2002). Furthermore, the terms used to describe each step are not clearly defined, making it difficult to compare with other models. For instance, it is not clear whether Ó Ciardhuáin excludes the preservation step present in other models because it is not considered necessary or because it is treated as part of the collection process. A further limitation of this model is that it does not define fundamental requirements or goals within each step in an investigation. As a result, different groups may decide on vastly different approaches at each step of a digital investigation, potentially even violating fundamental forensic principles.

6.1.4 Subphase Model

Beebe and Clark contend that most investigative process models are too high level and do not address the "more concrete principles of the investigation" (Beebe & Clark, 2005). Their solution is to create a multitiered framework, taking the steps common in other models and adding subphases with defined objectives to help investigators implement each step properly. In addition, this model defines overarching principles that apply to the entire process, such as repeatability and documentation. Interestingly, rather than treating evidence preservation as a separate step in the investigative process, Beebe and Clark define it as a principle that is "generally relegated to" the collection phase. They argue that the integrity of evidence must be maintained throughout the investigative process, and that "the analyst must be cognizant of which steps and processes modify working copies (e.g., file access times) and performs steps methodically from least invasive to most invasive and/or continually returns to use of clean copies."

The top-level steps used in this model are preparation, incident response, data collection, data analysis, findings presentation, and incident closure. As a proof of concept, Beebe and Clark use the analysis process, providing three objectives-based subphases, namely, survey, extract, and examine (abbreviated as SEE), with the following objectives for file system analysis:

1. Reduce the amount of data to analyze
2. Assess the skill level of the suspect(s)
3. Recover deleted files
4. Find relevant hidden data
5. Determine chronology of file activity
6. Recover relevant ASCII data
7. Recover relevant non-ASCII data
8. Ascertain Internet (non-e-mail) activity history
9. Recover relevant e-mail and attachments

10. Recover relevant "personal organizer" data (e.g., calendar, address books, etc.)
11. Recover printed documents
12. Identify relevant software applications and configurations
13. Find evidence of unauthorized system modification (e.g., Trojan applications)
14. Reconstruct network-based events

Beebe and Clark go on to suggest specific tasks within each of the above objectives, effectively providing a detailed protocol to follow when conducting a forensic examination of a hard drive.

There is much to be said for defining fundamental requirements or goals within each step of an investigation. This approach could lead to greater consistency and standardization in how digital investigations are conducted. However, this framework attempts to combine steps that are generally treated separately in other process models without explaining the rationale for doing so, and it is undermined by unorthodox use of terminology. For instance, the redefinition of "preservation" as an overarching principle rather than the process of acquiring data in a forensically sound manner introduces more confusion rather than clarity. Also, it is uncommon to treat examination as a subcomponent of analysis. The analysis of digital evidence is more commonly viewed as a separate process that involves hypothesis testing and event reconstruction among other things. Rather than attempting to invent new terminology and revise the high-level processes, the concept of objectives-based subphases could be applied to an established high-level investigation process model to help investigators implement each step properly.

6.1.5 Roles and Responsibilities Model

The FORZA model ascends to an even higher level of abstraction by providing a framework of roles and responsibilities in digital investigations (Ieong, 2006). The goal of this framework is to address not just the technical aspects of a digital investigation but also the legal and managerial issues. The FORZA model is based on the Zachman Framework, which was created to assist with the design, development, and management of enterprise IT architecture. Fundamentally, the FORZA model defines eight roles and provides six fundamental questions that each role must address in an investigation: who, what, how, when, where, and why (Figure 6.4).

This framework is useful for ensuring that all aspects of a complex digital investigation have been assigned to the appropriate individual(s) and that the expectations for each role are outlined. Because FORZA does not outline the process within each role, it is necessary to reference another process model for such details. For example, the investigative process models discussed above could be used to flesh out how digital investigators should carry out their responsibilities.

Table 2 – A high-level view of the FORZA framework

	Why (motivation)	What (data)	How (function)	Where (network)	Who (people)	When (time)
Case leader (contextual investigation layer)	Investigation objectives	Event nature	Requested initial investigation	Investigation geography	Initial participants	Investigation timeline
System owner (if any) (contextual layer)	Business objectives	Business and event nature	Business and system process model	Business geography	Organization and participants relationship	Business and incident timeline
Legal advisor (legal advisory layer)	Legal objectives	Legal background and preliminary issues	Legal procedures for further investigation	Legal geography	Legal entities and participants	Legal timeframe
Security/system architect/ auditor (conceptual security layer)	System/Security control objectives	System information and security control model	Security mechanisms	Security domain and network infrastructure	Users and security entity model	Security timing and sequencing
Digital forensics specialists (technical preparation layer)	Forensics investigation strategy objectives	Forensics data model	Forensics strategy design	Forensics data geography	Forensics entity model	Hypothetical forensics event timeline
Forensics investigators/system administrator/operator (data acquisition layer)	Forensics acquisition objectives	On-site forensics data observation	Forensics acquisition/ seizure procedures	Site network forensics data acquisition	Participants interviewing and hearing	Forensics acquisition timeline
Forensics investigators/ forensics analysts (data analysis layer)	Forensics examination objectives	Event data reconstruction	Forensics analysis procedures	Network address extraction and analysis	Entity and evidence relationship analysis	Event timeline reconstruction
Legal prosecutor (legal presentation layer)	Legal presentation objectives	Legal presentation attributes	Legal presentation procedures	Legal jurisdiction location	Entities in litigation procedures	Timeline of the entire event for presentation

FIGURE 6.4
High-level framework for FORZA model in Ieong (2006).

6.2 SCAFFOLDING FOR DIGITAL INVESTIGATIONS

When comparing the process models in the prior section, there are a number of discrepancies that are not explained by variations in terminology or how the investigative process has been dissected. These discrepancies, which include authorization and transportation, may be attributed to differences in perspective, and are related to orthogonal concerns such as noninvestigative occurrences and activities that support the investigative process. Although such occurrences and activities are not central to digital investigations, they provide necessary scaffolding to help build a solid case. This scaffolding also includes accusation/alert, threshold considerations, and case management.

Without an initial notification in the form of an accusation or alert, there is nothing to investigate. Then, in many situations, digital investigators must obtain written authorization to proceed. In addition, digital investigators will generally have to make some form of threshold assessment to decide what level of attention to give a certain case relative to all of the other cases they are handling. Transportation may seem like a minor issue until there is a problem such as lost or broken items containing digital evidence. Verification of the accuracy and completeness of results is needed in each phase of an investigation. Effective case management is one of the most important components of scaffolding, helping digital investigators bind everything together into a strong case.

6.2.1 Accusation or Incident Alert

Every process has a starting point—a place, event, or for lack of a better term, a "shot from a starting gun" that signals that the race has begun. This step can be signaled by an alarm from an intrusion detection system, a system administrator reviewing firewall logs, curious log entries on a server, or some combination of

indicators from multiple security sensors installed on networks and hosts. This initial step can also be triggered by events in more traditional law enforcement settings. Citizens reporting possible criminal activity will lead to investigative personnel being dispatched to a physical scene. That scene will likely contain exhibits of which some may be electronic, requiring part of the investigation to take a digital path. The prevalence of computers makes it increasingly likely that even traditional crimes will have related information derived from digital sources that require close scrutiny.

When presented with an accusation or automated incident alert, it is necessary to consider the source and reliability of the information. An individual making a harassment complaint because of repeated offensive messages appearing on his or her screen might actually be dealing with a computer worm/virus. An intrusion detection system alert may only indicate an attempted, unsuccessful intrusion or it might be a false alarm. Therefore, it is necessary to weigh the strengths, weaknesses, and other known nuances related to the sources and include human factors as well as digital.

In addition, to assess an accusation or alert thoroughly, some initial fact gathering is usually necessary before launching a full-blown investigation. Even technically proficient individuals sometimes misidentify normal system activity as a computer intrusion. Initial interviews and fact checking can correct such misunderstandings, clarify what happened, and help develop an appropriate response. To perform this fact gathering and initial assessment, it is usually necessary to enter a crime scene and scan or very carefully sift through a variety of data sources looking for items that may contain relevant information.

This is a very delicate stage in an investigation because every action in the crime scene may alter evidence. Additionally, delving into an investigation prematurely, without proper authorization or protocols, can undermine the entire process. Therefore, an effort should be made to perform only the minimum actions necessary to determine if further investigation is warranted. Although an individual investigator's experience or expertise may assist in forming internal conclusions that may have associated confidence levels, at this stage few firm, evidence-based conclusions will be drawn about whether a crime or an offense was actually committed.

6.2.2 Authorization

Before approaching digital evidence, it is important to be certain that the search is not going to violate any laws or give rise to liability. As noted in Chapter 3, there are strict privacy laws protecting certain forms of digital evidence like stored e-mail. Unlike the Fourth Amendment, which only applies to the government, privacy laws such as the Electronic Communications Privacy Act (ECPA) also apply to nongovernment individuals and organizations. If these

laws are violated, the evidence can be severely weakened or even suppressed. Because errors in this step can undermine the entire investigation, it is prudent to err on the side of caution when seeking authorization.

Computer security professionals should obtain instructions and written authorization from their attorneys before gathering digital evidence relating to an investigation within their organization. An organization's policy largely determines whether the employer can search its employees' computers, e-mail, and other data. However, a search warrant is usually required to access areas that an employee would consider personal or private unless the employee consents. There are some circumstances that permit warrantless searches in a workplace but corporate security professionals are best advised to leave this determination to their attorneys. If a search warrant is required to search an employee's computer and related data, it may be permissible to seize the computer and secure it from alteration until the police arrive.

As a rule, law enforcement should obtain a search warrant if there is a possibility that the evidence to be seized requires a search warrant. Although obtaining a search warrant can be time consuming, the effort is well spent if it avoids the consequences of not having a warrant when one is required. Sample language for search warrants and affidavits relating to computers is provided in the U.S. Department of Justice's (USDOJ) search and seizure manual to assist in this process. However, competent legal advice should be sought to address specifics of a case and to ensure that nuances of the law are considered.

Treating authorization as a discrete step at the start of an investigation does not consider the need for separate authorization to examine digital evidence or to disseminate information at the end of an investigation. For example, in the related area of electronic discovery, significant attention is paid to restricting the production of certain classes of documents identified by search of sets of electronic documents. Documents which are considered confidential or attracting legal privilege must be identified and excluded from production.

6.2.3 Threshold Considerations

Those involved in investigative activities are usually busy with multiple cases or have competing duties that require their attention. Given that investigative resources are limited, they must be applied where they are needed most. Therefore, digital investigators must establish thresholds in order to prioritize cases and make decisions about how to allocate resources. Threshold considerations vary with the associated investigative environment. Applied in law enforcement environments, threshold considerations include the likelihood of missing exculpatory evidence and seriousness of the offense. In civil, business, and military operations, suspicious activity will be investigated but policy, regulations, and continuity of operations may be the primary concern.

Regardless of environment, a form of triage is performed at this step in the process. Questions are asked that try to focus vital resources on the most severe problems or where they are most effective.

Factors that contribute to the severity of an offense include threats of physical injury, potential for significant losses, and risk of wider system compromise or disruption. Within an organization, if a security breach or policy violation can be contained quickly, if there is little or no damage, and if there are no exacerbating factors, a full investigation may not be warranted. The output of this step in the investigative process is a decision that will fit into two basic categories:

- Threshold considerations are not met—No further action is required. For example, available data and information are sufficient to indicate that there has been no wrongdoing. Document decisions with detailed justification, report, and reassign resources.
- Threshold considerations are met—Continue to apply investigative resources based on the merits of evidence examined to this point with priority based on initial available information. This step aims to inform about discernment based on practical as well as legal precedent coupled with the informed experience of the investigative team.

Expertise from a combination of training and on-the-job experience plays a tremendous role in effective triage.

6.2.4 Transportation

Moving evidence from the crime or incident scene back to the forensic laboratory or from one laboratory to another carries with it significant threats, the effects of which range from loss of confidentiality to destruction of evidence. One should keep in mind that one rarely gets a second chance to re-collect evidence that has been lost or rendered unusable.

When planning for movement of evidence, investigators should consider whether the evidence will be physically in the possession of the investigator at all times, environmental factors, and the potential consequence of chance events. For example, packing digital evidence into luggage that will be placed in the cargo hold of an airplane creates serious risks that can have an adverse impact on digital evidence such as loss of luggage, rough handling, and significantly different environmental conditions. Similarly, the heat that can quickly build up in automobiles in summer may result in lost bits in certain types of magnetic media.

Often evidence copies are required to be shared with other experts in other locations. Chain of custody is made simple by hand-to-hand delivery; however, this tends to be economically unfeasible in all but the same city. Courier services supporting service level agreements for person-to-person delivery, in tandem with tamper evident seals, are one strategy for maintaining

provenance. Another is shipping encrypted volumes through regular postal channels. Should the encrypted volume disappear along the way, with a proper key management scheme in place confidentiality is strongly protected.

6.2.5 Verification

Reviewing the information gathered in the survey phase for mistakes or oversights can help avoid confusion, criticisms, and missed evidence. Assessing the completeness and accuracy of acquired data and documenting its integrity are important considerations that support authentication. It is also necessary to verify that the results of forensic examination and analysis are correct. Approaches to verification include hash comparison, comparing results of multiple tools, checking data at a low level, and peer review.

6.2.6 Case Management

Case management plays a vital role in digital investigations, binding together all of the activities and outcomes. The purpose of effective case management is to ensure that a digital investigation proceeds smoothly and that all relevant information resulting from each step of the process is captured, documented, and woven together to create a clear and compelling picture of events relating to an offense or incident. The effectiveness of a digital investigation is heavily dependent on case management—particularly on keeping track of items of evidence, events, and important forensic findings. In addition, case management involves communication and prioritization, including sharing of information among digital investigators, managing the expectations of nontechnical stakeholders, and prioritizing and delegating administrative tasks among multiple digital investigators in a digital investigation.

Communication is a key component of case management. In more lengthy or complex digital investigations, daily or weekly status meetings may be needed to share details of progress, consolidate updated information, and discuss next steps in the investigation. Archiving digital evidence for future reference is another crucial consideration in managing an investigation effectively.

Without effective case management methods and supporting tools, investigative opportunities may be missed, digital evidence may be overlooked or lost, and crucial information may not be uncovered or may not be provided to decision makers.

6.3 APPLYING THE SCIENTIFIC METHOD IN DIGITAL INVESTIGATIONS

Although process models that define each step of an investigation can be useful for certain purposes, such as developing procedures, they are too complex and rigid to be followed in every investigation. In practice, most digital investigations

do not proceed in a linear manner and the common steps of preparation, survey, preservation, examination, and analysis are not neatly separated. All steps of the investigative process are often intertwined and a digital investigator may find the need to revisit steps in light of a more refined understanding of the case. Preparation is needed at every step of an investigation, rather than simply being a discrete step at the beginning. In addition, while identifying all potential sources of digital evidence, it may be necessary to preserve certain items immediately before volatile data are lost. Furthermore, some forensic analysis of computers may be required when trying to identify potential sources of digital evidence. This "feedback" is often essential to progress in a digital investigation and to refine the methods and findings in each step.

Many of these process models are limited in that they do not help digital investigators with some of the most important aspects of each step of an investigation, including the completeness and repeatability of each step. In addition, the process of obtaining reliable results in each step is not addressed directly in many of these investigative process models. The tenets of completeness, repeatability, and reliability apply to all aspects of a digital investigation, and not just to the forensic analysis steps. The scientific method provides the necessary structure to help digital investigators complete each step of an investigation in a repeatable manner to achieve reliable results.

Related to the above is the generally perceived need to transform the practice of digital forensics into a discipline based on the rigors of forensic science. Many process models claim to address this by providing a methodical, repeatable approach to the overarching investigative process. However, few process models attempt to address the foundation issue of the relationship between the scientific method and each step of a digital investigation.

While process models consider digital investigations in the large, in general they ascribe inordinate importance to each step, when one considers the typical amount of time spent by the digital investigator in performing the tasks of each step. In particular, the examination and analysis processes tend to consume by far the most resources in terms of a digital investigator's time, intellectual effort, and creativity. It is in these areas that process models tend to lack consistency, ranging from being silent to ambiguous, and from task focused to abstract.

In practice, digital investigators are better served by simpler methodologies that guide them in the right direction, while allowing them to maintain the flexibility to handle diverse situations. The scientific method provides such a simple, flexible methodology. The scientific method begins with fact gathering and validation, and proceeds to hypothesis formation and experimentation/testing, actively seeking evidence that disproves the hypothesis, and revising conclusions as new evidence emerges.

6.3.1 Formation and Evaluation of Hypotheses

From a practical viewpoint, at each stage of the investigative process a digital investigator is trying to address specific questions and accomplish certain goals relating to the case. These questions and goals will drive the overall digital investigation process and will influence specific tasks within each step. Therefore, it is important for digital investigators to have a robust and repeatable methodology within each step to help them accomplish the goals and address the questions that are necessary to solve the case.

Digital investigators are generally instructed to focus on specific issues in a case, sometimes with time constraints or other restrictions. For example, in order to find a missing person as quickly as possible, digital investigators may be compelled to progress rapidly through the preparation, survey, preservation, examination, and analysis steps at the expense of completeness and accuracy. Similarly, in a child exploitation case, digital investigators may initially concentrate their efforts on finding incriminating digital evidence. If, in the course of the investigation, there are some indications that encryption and wiping software was used on the defendant's computer, this may significantly alter the focus of the investigation to concentrate on evidence of concealment behavior. In certain cases, legal requirements will help digital investigators determine elements that are required to prove the crime. For instance, in the case of child pornography, there will be a distinction between whether files were accessed versus opened. In data breach cases, the key question will be whether personally identifiable information was taken from the compromised system.

In short, digital investigators face challenges throughout an investigation that they must puzzle through by applying their experience and intuition to form working theories, and to assess these theories against available information.

Carrier's Hypothesis Based Approach to digital forensic investigations (Carrier, 2006) provides an initial model which bridges digital investigation practices and computer science theory, demonstrating the role of the scientific method within a digital investigation. The approach defines a model of computer history based on a finite state machine view of computing and storage, describing the history of the state of a digital device in terms of low-level computations and storage operations (primitive history) and of user perceivable events and storage operations (complex histories). The history model is then related to the general scientific method of observation, hypothesis formulation, and predicting and testing, by casting the digital examination as a process of formulating and testing hypotheses about previous states and events.

While Carrier's model was a significant contribution to the theoretical foundations of the field, it provided little guidance on the application of the scientific method to the higher level investigative tasks undertaken in an investigation.

The remainder of this chapter shows how the scientific method is applied to each step of a digital investigation (preparation, survey, preservation, examination, and analysis), which can guide a digital investigator through almost any investigative situation, whether it involves a single compromised host, a single network link, or an entire enterprise.

1. ***Observation:*** One or more events will occur that will initiate your investigation. These events will include several observations that will represent the initial facts of the incident. Digital investigators will proceed from these facts to form their investigation. For example, a user might have observed that his or her web browser crashed when he or she surfed to a specific Web site, and that an antivirus alert was triggered shortly afterward.
2. ***Hypothesis:*** Based on the current facts of the incident, digital investigators will form a theory of what may have occurred. For example, in the initial observation described earlier, a digital investigator may hypothesize that the web site that crashed the user's web browser used a browser exploit to load a malicious executable onto the system.
3. ***Prediction:*** Based on the hypothesis, digital investigators will then predict where the artifacts related to that event may be located. Using the hypothesis, and knowledge of the general operation of web browsers, operating systems, and virii, a digital investigator may predict that there will be evidence of an executable download in the history of the web browser, and potentially, files related to the malware were created around the time of the incident.
4. ***Experimentation/Testing:*** Digital investigators will then analyze the available evidence to test the hypothesis, looking for the presence of the predicted artifacts. In the previous example, a digital investigator might create a forensic duplicate of the target system, and from that image extract the web browser history to check for executable downloads in the known timeframe. Part of the scientific method is also to test possible alternative explanations—if the original hypothesis is correct a digital investigator will be able to eliminate alternative explanations on the basis of available evidence (this process is called falsification).
5. ***Conclusion:*** Digital investigators will then form a conclusion based upon the results of their findings. A digital investigator may have found that the evidence supports the hypothesis, falsifies the hypothesis, or that there were not enough findings to generate a conclusion.

This general methodology can be repeated as many times as necessary to reach conclusions at any stage of a digital investigation. Applying this method to the survey process can help digital investigators locate all available sources of digital evidence at a crime scene. Applying this to the forensic preservation process will help digital investigators obtain a complete and accurate snapshot

of digital evidence relating to a crime or incident. Applying this to the forensic analysis process will help digital investigators test theories and come to reliable conclusions about what may have happened during a crime or incident. Its simplistic nature makes it useful as a grounding methodology for more complex operations, to prevent digital investigators from going down the rabbit hole of inefficient searches through the endless volumes of data that they will be presented with.

From this perspective, digital investigations are guided by identifying claims regarding events that have occurred which are relevant, and translating those claims into hypotheses. Typically these hypotheses will not be directly testable with regard to tracing evidence in the digital domain, and will need to be further translated into subhypotheses based on hypotheses about which applications a user employed, and the artifacts that application leaves behind. The following example demonstrates how a simple claim may be translated into numerous hypotheses and subhypotheses towards identifying theft of company proprietary information.

- Claim: Senior management stole proprietary data while exiting the business
- H0: Proprietary information was e-mailed out of the business or
- H1: Proprietary information was copied to a USB stick and taken out of the business or
- H3: …
- H0.1: Proprietary information was e-mailed by regular work e-mail
- H0.2: Proprietary information was e-mailed by private webmail
- H0.2.1: Records of webmail related to proprietary information will exist as webmail fragments in the filesystem of the employee's laptop.
- H0.2.2: Records of webmail related to proprietary information will exist as webmail fragments in the volume shadow copy of the filesystem of the employee's laptop.

Of particular significance in the scientific method is the weight attached to finding evidence which supports a particular hypothesis. Evidential artifacts found in the experimentation/testing process which are compatible with a particular hypothesis must not be taken as proof of the hypothesis; they merely support it, while evidence that supports an alternative hypothesis should be taken as undermining the primary hypothesis. Of course, finding multiple corroborating pieces of evidence produced by independent methods may give further weight to a hypothesis; however, a scientific test is only as good as the testing undertaken to refute a hypothesis. Attempting to refute the hypothesis will strengthen a hypothesis if those refutations fail, and digital investigators must use their best judgment when determining how much falsification testing is needed in a specific case.

CASE EXAMPLE

A claim was made that a party failed to meet conditions of a contract with another party by not sending an e-mail. The accused party claimed that the e-mail had been sent. An investigation ensued in which the forensic examiner was asked, "Was the e-mail sent on the claimed date?" From that claim, a hypothesis was generated that if the e-mail had been sent it would still be in the mailbox of the sender. This hypothesis was tested and an e-mail and related document were found in the sent items mailbox of the accused with the sent date as the claimed date of sending. The hypothesis was confirmed. However, the most that can be said is that that the evidence identified is compatible with the e-mail having been sent. Depending on the forum and strategy employed, such an answer may be sufficient; however, more definitive statements are typically preferable.

One may add weight by identifying corroborative evidence, such as e-mail server logs which corroborate the sending of the e-mail. However, such evidence was in this matter not available, so an attempt to refute the hypothesis by identifying alternate hypotheses and testing those gives further weight. In this case, the following alternate hypotheses were tested:

- H1: The e-mail was sent at a later time, and made to appear that it was sent at the time indicated by rolling back the clock of the computer on which it was composed.
- H2: The e-mail was sent at a later time, and made to appear that it was sent at the time indicated by rolling back the clock of another computer, then somehow imported into the accused's laptop.

The first hypothesis was tested by constructing and assessing the following subhypothesis:

H1.1: Out of order events, and events showing user manipulation of the clock, will be found in the Windows Vista event log of the accused's machine.

A search of the event log revealed no events compatible with H1.1.

The second hypothesis was tested by generating and assessing the following subhypothesis:

H2.1: Moving of a fraudulent e-mail composed on another machine would yield some discrepancies or inconsistencies in metadata associated with the e-mail message.

An experiment was designed to replicate the hypothetical actions and the e-mail message was investigated for inconsistent metadata. Of particular interest was the message ID metadata field associated with the message as it was stored within Microsoft Outlook. The message ID field of the e-mail was compared with that of other messages that were sent around the same time, and the embedded sequence numbers within all of the e-mails were found to be compatible with the times and dates of sending.

The above application of the scientific process to evaluating whether an e-mail was sent yielded no refutations and identified further corroborating evidence in support of the primary hypothesis.

There will come a time in the scientific process when digital investigators will believe that they have proved their hypotheses to some level of certainty. After digital investigators are satisfied that they have thoroughly tested their hypotheses, they will reach a conclusion. Although digital investigators may not be able to predict all potential defenses in a case, if alternative theories are suggested later, digital investigators have an obligation to reevaluate their findings.

6.3.2 Preparation

The general aim of preparing for a digital investigation is to create a plan of action to perform an effective digital investigation, and to obtain the necessary personnel and equipment. Preparation for the preservation step ensures that the best evidence can be preserved when the opportunity arises. When preparing to execute a search warrant, digital investigators will create a plan to deal with the specific location and expected evidential items. When preparing an

organization to deal with future incidents, digital investigators will gradually establish a framework that includes policies, procedures, properly trained personnel, and centralized logging to make their organization more ready operationally and technically. Before conducting a forensic examination, it is helpful to develop a strategy for processing available evidence and, in some cases, to create a detailed examination protocol for digital investigators to follow.

An example of applying the scientific method to preparation for the preservation step of a digital investigation is provided here:

- ***Observation:*** gathering information about the crime scene to anticipate what number and type of computer systems to expect, and whether full disk encryption is in use. This stage can involve interviewing people familiar with the location to be searched, and reviewing documentation such as IT network diagrams, asset inventory, and purchase orders for computers. When no inside knowledge is readily available, this observation process may require covert surveillance.
- ***Hypothesis/Predication:*** Based on the information gathered about the crime scene, digital investigators will form theories about the types of computer systems and internal components such as hard drive capacity and interface (e.g., ATA, SATA, serial attached SCSI).
- ***Experimentation/Testing:*** It may be possible to test some predictions about what will or will not be encountered at the crime scene. For instance, it may be possible to glean details about internal and public servers by examining e-mail headers and connecting to them over the Internet. In some cases, these types of intelligence gathering experiments may not be feasible, particularly when there is concern about alerting the subjects of the investigation. In other situations, such as in a corporate environment, digital investigators may already have access to the systems to be preserved, making it easier to prepare well in advance in anticipation of an actual incident.
- ***Conclusions:*** The outcome of this process should be a robust plan for preserving evidence at the crime scene. In some instances, digital investigators also need to prepare for some on-scene processing of digital evidence. For instance, when digital investigators are not authorized to collect every computer system, some on-scene keyword searching of many computers must be performed to identify which are relevant to the investigation.

PRACTITIONER'S TIP

Always prepare to encounter more computers and data than initially expected. Even in a corporate investigation, there may be additional computers or mobile devices, and larger capacity hard drives or quantities of log files, that digital investigators did not know about prior to arriving to collect and preserve digital evidence.

After a digital investigation, it is common to revise preparatory measures based on lessons learned. Procedures may be updated, additional equipment may be purchased, network logging may be augmented, and additional training may be obtained.

CASE EXAMPLE (VANCOUVER, 1999)

The investigation into the Starnet Internet gambling company provides a good example of the successes of proper preparation. The August 1999 raid of Starnet's offices in Vancouver, B.C., was the culmination of more then a year's worth of investigative effort and preparation by the Royal Canadian Mounted Police. Over one hundred personnel from all over Canada were brought together to search and seize Starnet's systems. Search teams were trained to implement standard operating procedures to ensure consistency and were given sufficient equipment to store the large amounts of data that were anticipated. As a result of this planning, Starnet's office building and the network it contained were secured in a few minutes. Although it took several days, digital evidence from more than 80 computers was preserved. In 2001, Starnet pled guilty to violating Section 202 (1) b of the Canadian criminal code by having a machine in Canada for gambling or betting.

6.3.3 Survey

With a plan in hand from the preparation step, digital investigators should be well prepared to recognize sources of digital evidence at the crime scene. The aim of the process is for digital investigators to find all potential sources of digital evidence and to make informed, reasoned decisions about what digital evidence to preserve at the crime scene.

- ***Observation:*** A methodical inspection of the crime scene should be performed in an effort to locate the expected items and to find unanticipated items. Carrier's Integrated Digital Investigation Process model encourages use of traditional approaches to searching the physical crime scene in a methodical manner. A comparable methodical approach to searching a digital crime scene should be used to find and assess potential sources of digital evidence.
- ***Hypothesis:*** Theories should be developed about why certain expected items are not present, and why certain unexpected items were found.
- ***Prediction:*** Ideas should be considered for where missing items may be found, and which items may contain potentially relevant data. When large quantities of computers or removable media are involved, it may be necessary to develop theories about which ones do and do not contain potentially relevant digital evidence.

CASE EXAMPLE

The CFO's old laptop had crashed and been replaced by a newer laptop. He did not know where his old laptop might be, and thought it had been thrown out. Because this item was critical to the investigation, digital investigators came up with a theory about where it might have been stored and interviewed the CFO. The CFO acknowledged that it might have been put in storage and had his assistant check. The CFO's old laptop was found.

- ***Experimentation/Testing:*** When digital investigators believe that certain items are not relevant to the case, some experimentation and testing is needed to confirm this belief. For example, it may be necessary to perform a triage search of these seemingly irrelevant systems or storage media for responsive evidence to ensure that they, in fact, do not contain anything of interest. When digital investigators believe that they have identified all sources of digital evidence, they can test this theory in various ways. For example, rather than simply relying on system administrators for details about how routine backups are made, digital investigators can actually check backup configurations and storage areas for useful information. Similarly, examining a computer for traces of attached USB devices may reveal additional removable storage media that were not found at the crime scene.

PRACTITIONER'S TIP

Backup tapes are an example of potential sources of digital evidence that are commonly missed. Some organizations store backup tapes in a remote location for disaster recovery purposes. It is not safe to assume that an inventory of backup tapes is complete or reliable, as old tapes may not have been disposed of and may contain useful information. Therefore, it is often necessary for digital investigators to visit the remote location where tapes are stored and assess how these tapes are handled. It may even be necessary to review the contents of miscellaneous tapes found in unlabeled boxes at a remote storage facility to determine whether they are potentially related to the matter under investigation.

- ***Conclusions:*** Based on the methodical assessment of available information, there is a high degree of confidence that an inventory has been made of all potentially relevant sources of digital evidence at the crime scene that need to be preserved.

Documentation permeates all steps of the investigative process but is particularly important in the digital evidence survey step. Digital investigators need to document evidence thoroughly and must be prepared to justify their actions. It is necessary to record details about each piece of seized evidence to help establish its authenticity and initiate chain of custody. For instance, numbering items, photographing them from various angles, recording serial numbers, and documenting who handled the evidence help keep track of where each piece of evidence came from and where it went after collection. Standard forms and procedures help in maintaining this documentation, and experienced investigators and examiners keep detailed notes to help them recall important details. Any notebook that is used for this purpose should be solidly bound and have page numbers that will indicate if a page has been removed.

In an organization, documentation relating to the survey phase may take the form of a map indicating where evidence is located on a network—a *digital*

evidence map. Such a map may include e-mail, log files, and backup tapes, may specify for how long each source of digital evidence is retained, and may reference procedures for collecting the evidence to help digital investigators handle the data properly (Casey, 1997).

Although a digital evidence map can be created during a digital investigation, it is more effective to create such a map within an organization prior to an incident or legal action. As such, the creation of a digital evidence map may occur in the preparation phase of a digital investigation, and can then be referenced in all subsequent incidents in order to streamline the survey phase. Organizations that identify key sources of data prior to a security breach, labor dispute, or civil discovery request put themselves in a better position to mitigate the increasing costs and penalties associated with such incidents (Casey, 2007). In addition, the process of creating a digital evidence map may highlight problems in an organization's current data sources that need to be resolved. After determining the kinds of data that exist on their IT systems, organizations generally find that they need to maintain certain information that they are not currently preserving, and decide to cull certain data sources that are accumulating and pose a risk by containing more data than necessary and being too costly to maintain and produce.

6.3.4 Preservation

Working from the known inventory of identified components, investigators must act to make sure that potentially volatile items are collected or acquired in such a way that captures their current state. Another way to put it is that proper actions must be taken to ensure the integrity of potential evidence, physical and digital. The methods and tools employed to ensure integrity are key here. Their accuracy and reliability as well as professional acceptance may be subject to question by opposing counsel if the case is prosecuted. These same criteria will give decision makers outside of court the necessary confidence to proceed on recommendations from their investigators.

To many practitioners in digital forensics, the preservation step is where digital forensics begins. It is generally the first stage in the process that employs commonly used tools of a particular type. The output of this stage is usually a set of duplicate copies of all sources of digital data. This output provides investigators with two categories of exhibits. First, the original material is cataloged and stored in a proper environmentally controlled location, in an unmodified state. Second, an exact duplicate of the original material is created that will be scrutinized as the investigation continues. Several examples of digital evidence preservation are provided here, and more detailed guidelines for handling the digital crime scene are covered in Chapter 7.

Consider examples of the scientific process applied to the preservation of common forms of digital evidence.

6.3.4.1 Hard Drives

- ***Observation:*** A hard drive has a SATA interface with a certain number of sectors documented on the label.
- ***Hypothesis:*** A complete and accurate duplicate of the hard drive can be obtained without altering the original.
- ***Prediction:*** The resulting forensic duplicate will have the same hash value as the original hard drive.
- ***Experimentation/Testing:*** Comparing the hash value of the forensic duplicate with that of the original hard drive confirms that they are the same. However, comparing the size of the forensic duplicate with the capacity of the hard drive reveals a discrepancy. Further experimentation is needed to determine that this discrepancy is caused by an incorrect number of sectors being detected by the acquisition method used. Using an alternative method to acquire data from the hard drive gives a complete and accurate duplicate of the digital evidence.
- ***Conclusions:*** There is a high degree of confidence that an accurate duplicate of all data on the hard drive was acquired in a forensically sound manner.

6.3.4.2 E-Mail on Server

- ***Observation:*** E-mail is stored on a server, including 30 days of deleted messages.
- ***Hypothesis:*** Extracting mailboxes for the individuals of interest in the investigation will provide a complete and accurate duplicate of relevant e-mail with minimal disruption to the server.
- ***Prediction:*** The resulting copies of mailboxes will contain all relevant e-mail.
- ***Experimentation/Testing:*** An inspection of mailboxes acquired from the server reveal large gaps in e-mail messages during periods of interest. Further testing is needed to determine that the acquisition method used did not capture messages that were deleted within the past 30 days. In addition, sampling of mailboxes on backup tapes finds messages that were deleted over 30 days before.
- ***Conclusions:*** There is a high degree of confidence that all available e-mail, including deleted items, was accurately acquired from backup tape and mailboxes on the server in a forensically sound manner, with minimal disruption to the server.

6.3.4.3 Mobile Device

- ***Observation:*** Mobile device has a digital camera that can take photographs and videos.
- ***Hypothesis:*** A complete and accurate duplicate of photographs and videos on the mobile device can be obtained with minimal alteration of the original device.

- ***Prediction:*** The forensic acquisition will contain all photographs and videos of the mobile device.
- ***Experimentation/Testing:*** The data acquired from the mobile device contain two photographs and one video, whereas a manual examination of the device shows many more photographs and videos of interest that were not acquired. Further testing is needed to determine that the acquisition method used did not capture multimedia stored outside of the default storage folder. In addition, performing experiments on a test device reveals that photographs and videos can be stored on a small removable storage card inserted into the mobile device. Although no such storage card was found in the original mobile device, further searching of the crime scene locates one that contains relevant photographs and videos.
- ***Conclusions:*** There is a high level of confidence that complete and accurate duplicates of all the photographs and videos were acquired from the mobile device and removable storage card in a forensically sound manner.

Prior to attempting to preserve digital evidence, it is most effective to prepare the necessary forensic preservation tools and techniques to handle various forms of evidence. During the preparation step of a digital investigation, activities such as testing tools and sanitizing and/or encrypting storage media can be performed to make preservation processes go more smoothly.

Management of primary evidence is also an activity which should be undertaken carefully and in a planned and methodical manner. Obviously, physical security is an important factor in assuring that primary evidence is not inadvertently modified or destroyed. Redundancy should be considered in the context of storage media employed, given the potential for hard disk drives to fail to spin up after being stored for long periods and DVDs to deteriorate.

6.3.5 Examination

Forensic examination is the process of extracting and viewing information from the evidence, and making it available for analysis.

Forensic examination of digital evidence is generally one of the most resource-intensive and time-consuming steps in a digital investigation. To produce useful results in a timely manner at different phases of an investigation, it is useful to employ three levels of forensic examination: (1) survey/triage forensic inspections, (2) preliminary forensic examination, and (3) in-depth forensic examination (Casey, Ferraro, & Nguyen, 2009). The basis of these levels is that it makes little sense to wait for a complete review of each piece of media when only a handful of them will provide data of evidentiary significance. Each level of forensic examination is defined here:

- ***Survey/Triage Forensic Inspection:*** Targeted review of all available media to determine which items contain the most useful evidence and require additional processing.
- ***Preliminary Forensic Examination:*** Forensic examination of items identified during survey/triage as containing the most useful evidence, with the goal of quickly providing investigators with information that will aid them in conducting interviews and developing leads.
- ***In-Depth Forensic Examination:*** Comprehensive forensic examination of items that require more extensive investigation to gain a more complete understanding of the offense and address specific questions.

> In some circumstances it is necessary to perform a survey/triage forensic inspection of all available items prior to examining particular items in more depth. For instance, when criminal activity originated from an organization or Internet café with hundreds of computers, it may be necessary to perform a survey/triage forensic inspection of each computer to identify those that may have been involved in the crime. In other circumstances it is more effective to focus on a few items initially, before performing a survey/triage forensic inspection of all available media. For example, in a child exploitation case involving several computers and a large amount of removable media, it can be most effective to perform survey/triage forensic inspections of the computers (because they generally contain the most information about user activities), then a preliminary forensic examination of the most relevant computer, and subsequently process the remaining items as needed. When a cellular telephone or other device containing volatile data is a potential source of evidence, performing a survey/triage forensic inspection immediately can reveal valuable information that may not be available later. Under certain circumstances, it may also be necessary to examine the network on which a computer resides to determine whether analysis of additional computers, logs, and other related data is required.
>
> **(Casey et al., 2009)**

When conducting a forensic examination, it is useful to consider Carrier's Integrated Digital Investigation Process model, which treats sources of digital evidence as individual crime scenes. By conceptually treating each source of digital evidence as a crime scene, digital investigators are encouraged to apply each step of the investigative process to each source of evidence and thereby develop a more comprehensive and methodical approach to a forensic examination. The rationale for this approach is that each source of digital evidence may require its own preparation, survey, and examination steps as summarized here:

- ***Preparation for Forensic Examinations:*** Prior to performing a forensic examination of digital evidence, it is advisable to prepare a plan of action

that outlines what steps will be taken and what processes will be performed on each item of digital evidence. Without such a plan, digital investigators may miss important items or could violate legal restraints. In addition, it may be necessary to prepare a forensic workstation with software and sanitized storage space to conduct a forensic examination.

- ***Survey in Forensic Examinations:*** Digital investigators will generally survey each source of digital evidence, including the contents of hard drives, mobile devices, log files, and other data to develop an overall familiarity with the *corpus delicti* (a.k.a. totality of the evidence) to find items of potential relevance to the investigation. For example, during a survey of storage media in a child exploitation investigation, digital investigators might observe incriminating or encrypted files that require additional attention. As another example, during a survey of computers in a network intrusion, digital investigators might find several systems that exhibit signs of being compromised.
- ***Forensic Examinations:*** Certain items within a source of digital evidence may require special processing so that they can be examined more easily. Such special items can include mailboxes, password-protected files, encrypted volumes, and unallocated space. For instance, to extract additional details, digital investigators might employ specialized examination procedures on pornographic digital photographs on a sexual predator's computer, malicious programs on a compromised server, or e-mail messages on an exemployee's mobile device. Some special items may even require some degree of independent preservation, survey, and examination in order to extract usable information from them.

Forensic examination of digital evidence, whether it is an entire hard drive or an individual's mailbox, generally involves some level of recovery, harvesting, organization, search, and reduction to produce a reduced dataset for forensic analysis as discussed further here. Once all sources of digital evidence and special items that require further processing have been examined, the results can be incorporated into the analysis process.

- ***Recovery:*** Data should be extracted from available sources, including items that have been deleted, hidden, camouflaged, or that are otherwise unavailable for viewing using the native operating system and resident file system. The objective is to recover all unavailable data whether or not they may be germane to the case or incident. In some instances, it may also be necessary to reconstitute data fragments to recover an item. The output provides the maximum available content for the investigators, like a complete data timeline and information that may provide insight into the motives of an offender if concrete proof of purposeful obfuscation is found and recorded.
- ***Harvesting:*** Data and metadata (data about data) should be gathered about all recovered objects of interest. This gathering will typically

proceed with little or no discretion related to the data content, its context, or interpretation. Rather, the investigator will look for categories of data that can be harvested for later analysis—groupings of data with certain class characteristics that, from experience or training, seem or are known to be related to the major facts of the case or incident known to this point in the investigation. At this stage in the process, actual reasoned scrutiny begins and concrete facts begin to take shape that support or falsify hypotheses built by the investigative team. For example, an accusation related to child pornography requires visual digital evidence most likely rendered in a standard computer graphics format like GIF or JPEG. Therefore, the investigators would likely be looking for the existence of files exhibiting characteristics from these graphic formats. That would include surface observables like the object's file type (expressed as a three-character alphanumeric designator in MS Windows-based file systems) or more accurately a header and trailer unique to a specific graphical format. In the case of incidents related to hacking, investigators might focus some attention on the collection of files or objects associated with particular rootkits or sets of executables, scripts, and interpreted code that are known to aid crackers in successfully compromising systems as discussed in Chapter 13. A familiarity with the technologies and tools used, coupled with an understanding of the underlying mechanisms and technical principles involved, is of more importance in this step. The general outputs expected here are large organized sets of digital data that have the potential for evidence. It is the first layer organizational structure that the investigators and examiners will start to decompose in the steps that follow.

- ***Organization and Search:*** A thorough analysis should be facilitated by organizing the reduced set of materials from the previous step, grouping, tagging, or otherwise placing them into meaningful units. At this stage, it may be advantageous to actually group certain files physically to accelerate the analysis stage. They may be placed in groups using folders or separate media storage, or in some instances a database system may be employed to simply point to the cataloged file system objects for easy, accurate reference without having to use rudimentary search capability offered by most host operating systems. The primary purpose of this activity is to make it easier for digital investigators to find and identify data during the analysis step and allow them to reference these data in a meaningful way in final reports and testimony. This activity may incorporate different levels of search technology to assist investigators in locating potential evidence. A searchable index of the data can be created to enable efficient review of the materials to help identify relevant, irrelevant, and privileged material. Any tools or technology used in this regard should be understood fully and the operation should follow as many accepted

standards as exist. The results of this stage are data organization attributes that enable repeatability and accuracy of analysis activities to follow.

- ***Reduction:*** Irrelevant items should be eliminated or specific items targeted in the collected data as potentially germane to an investigation. This process is analogous to separating the wheat from the chaff. The decision to eliminate or retain is made on the basis of external data attributes such as hashing or checksums, type of data (after type is verified), etc. In addition, material facts associated with the case or incidents are also brought to bear to help eliminate data as potential evidence. This phase remains focused primarily on the overall structure of the object and very likely does not consider content or context apart from examination of fixed formatted internal data related to standards (like headers and trailers). The result (output) of the work in this stage of the investigative process is the smallest set of digital information that has the highest potential for containing data of probative value. This is the answer to the question: "Where's the beef?" The criteria used to eliminate certain data are very important and might possibly be questioned by judge, jury, or any other authorized decision maker.

Applying the scientific method to the forensic examination process can be a time-consuming and repetitive process, but the effort is generally well spent, giving digital investigators the information they need to resolve a case. A less methodical or scientifically rigorous forensic examination may miss important information or may give erroneous results.

An illustrative example of how the scientific method is applied during the forensic examination process is provided here.

- ***Observation:*** A hard drive contains documents that are pertinent to the investigation.
- ***Hypothesis:*** All documents are stored in Microsoft Office formats, predominantly Word and Excel.
- ***Prediction:*** Extracting all Microsoft Office documents will result in all relevant documents being available for analysis.
- ***Experimentation/Testing:*** Forensic examination of other file types on the hard drive reveals that compressed archives (.ZIP files) contain many Microsoft Office documents that were not extracted originally. In addition, fragments of relevant documents are observed in unallocated space. Efforts to identify pertinent documents by keyword searching are successful in finding more items. However, further examination reveals relevant documents in unsearchable formats, including binary PDF and scanned TIFF files.
- ***Conclusions:*** There is a high level of confidence that the production of documents obtained from the hard drive is complete and accurate.

The scientific method helps both with specific tasks and with the overall forensic examination process. After repeated use of the scientific method, experienced practitioners develop robust forensic examination protocols that incorporate lessons learned from past experience. These protocols include steps for dealing with deleted data, unsearchable files, password-protected documents, various e-mail formats, and compressed and encrypted data. In this way, by enabling digital investigators to codify the results of previous forensic examinations, the scientific method is used to progressively improve forensic examination techniques to make them more complete, repeatable, and reliable.

In addition, given the potential for errors in the way that digital evidence is represented or translated by forensic tools, it is important to perform quality assurance during the forensic examination process. For instance, file system metadata such as date-time stamps need to be checked for accuracy, recovered deleted files need to be inspected to determine whether they contain data from the actual original file, and e-mail messages extracted from mailboxes need to be assessed to ascertain whether all items (e.g., message bodies, attachments, and calendar items) were extracted and whether associated metadata were represented correctly. The scientific method is useful for assessing the completeness and accuracy of the results of a forensic examination, and for detecting errors and omissions introduced by forensic tools or other abstraction layers. In addition to testing forensic tools using known datasets, controlled experiments can be performed using samples from the actual digital evidence to assess whether all information is being processed and presented correctly.

6.3.6 Analysis

The forensic analysis process is inseparable from the scientific method. By definition, forensic analysis is the application of the scientific method and critical thinking to address the fundamental questions in an investigation: who, what, where, when, how, and why.

This step involves the detailed scrutiny of data identified, preserved, and examined throughout the digital investigation. The techniques employed here will tend to involve review and study of specific, internal attributes of the data such as text and narrative meaning of readable data, or the specific format of binary audio and video data items. Additionally, class and individual characteristics found in this step are used to establish links, determine the source of items, and ultimately locate the offender. Ultimately, the information that has been accumulated during the digital investigation is combined to reconstruct a comprehensive understanding of events relating to the crime or incident. Generally, the subcategories of analysis include but are not limited to the following:

- ***Observation:*** Human readable (or viewable) digital data objects have substance that can be perceived as well as context that can be reconstructed.

That content and context of digital evidence may contain information that is used to reconstruct events relating to the offense and to determine factors such as means, motivation, and opportunity.

- ***Hypothesis:*** Develop a theory to explain digital evidence.
- ***Prediction:*** Based upon the hypothesis, digital investigators will then predict where they believe the artifacts of that event will be located.
- ***Experimentation/Testing:*** A very general term but applied here to mean any activity used to determine whether or not digital evidence is compatible with the working theory. These activities can include running experiments using a specific operating system or application to learn about their behavior and associated artifacts, or loading the subject system into a virtualized environment to observe it as the user would. In addition, unorthodox or previously untried methods and techniques might be called for during investigations. All proven methodologies began as experiments so this should come as no surprise, especially when applying the scientific method. What remains crucial is that all experimentation be documented rigorously so that the community, as well as the courts, and opposing experts have the opportunity to test it. Eventually, experimentation leads to falsification or general acceptance.
- ***Conclusions:*** The result of a thorough forensic analysis generally includes an investigative reconstruction based on fusion and correlation of information as detailed in Chapter 8. These fusion and correlation processes are subtly distinct. During the course of the investigation, data (information) have been collected from many sources (digital and nondigital). The likelihood is that digital evidence alone will not tell the full tale. The converse is also true. The data must be fused or brought together to populate structures needed to tell the full story. An example of fusion would be the event timeline associated with a particular case or incident. Each crime or incident has a chronological component where event or actions fill time slices. This typically answers the questions where, when, and sometimes how. Time slices representing all activities will likely be fused from a variety of sources such as digital data, telephone company records, e-mail transcripts, and suspect and witness statements. Correlation is related but has more to do with reasoned cause and effect. Do the data relate? Not only does event B follow event A chronologically, but the substance (e.g., narrative, persons, or background in a digital image) of the events shows with high probability (sometimes intuition) that they are related contextually.

The outcome of a thorough forensic analysis is validated facts and reasoned findings that digital investigators propose to submit to jurists or other decision makers as "proof positive," or proof to a high degree of certainty, for prosecution or acquittal.

A failure to assess digital evidence objectively and to utilize experimentation to validate a theory can lead to false conclusions and personal liability as demonstrated in the following example.

CASE EXAMPLE (LISER V. SMITH, 2003)

Investigators thought they had found the killer of a 54-year-old hotel waitress, Vidalina Semino Door, when they obtained a photograph of Jason Liser from an ATM where the victim's bank card had been used. Despite the bank manager's warning that there could be a discrepancy between the time indicated on the tape and the actual time, Liser's photograph was publicized and he was subsequently arrested but denied any involvement in the murder. A bank statement confirmed that Liser had been at the ATM earlier that night but that he had used his girlfriend's card, not the murder victim's. Investigators made an experimental withdrawal from the ATM and found that the time was significantly inaccurate and that Liser had used the ATM before the murder took place. Eventually, information relating to the use of the victim's credit card several days after her death implicated two other men who were convicted for the murder. Liser sued the District of Columbia and Jeffrey Smith, the detective responsible for the mistaken arrest, for false arrest and imprisonment, libel and slander, negligence, and providing false information to support the arrest. The court dismissed all counts except the negligence charge. The court felt that Smith should have made a greater effort to determine how the bank surveillance cameras operated or consulted with someone experienced with this type of evidence, noting, "The fact that the police finally sought to verify the information—and quickly and readily learned that it was inaccurate—*after* Liser's arrest certainly does not help their cause." Liser's lawsuit against Bank of America for negligence and infliction of emotional distress due to the inaccuracy in the timing mechanism was dismissed.

6.3.7 Reporting and Testimony

To provide a transparent view of the investigative process, final reports should contain important details from each step, including reference to protocols followed and methods used to seize, document, collect, preserve, recover, reconstruct, organize, and search key evidence. The majority of the report generally deals with the analysis leading to each conclusion and descriptions of the supporting evidence. No conclusion should be written without a thorough description of the supporting evidence and analysis. Also, a report can exhibit the investigator or examiner's objectivity by describing any alternative theories that were eliminated because they were contradicted or unsupported by evidence.

In some cases, it is necessary to present the findings outlined in a report and address related questions before decision makers can reach a conclusion. A significant amount of effort is required to prepare for questioning and to convey technical issues in a clear manner. Therefore, this step in the process includes techniques and methods used to help the analyst and/or domain expert translate technological and engineering details into understandable narrative for discussion with decision makers.

6.4 INVESTIGATIVE SCENARIO: SECURITY BREACH

An investigative scenario involving a network security breach is outlined here to demonstrate how the various steps in a digital investigation tie together. In this case, data thieves target the IT systems of Corporation X, a medium sized business that manufactures various parts for airplane engines.

6.4.1 Preparation and Case Management

Corporation X is well prepared to handle security breaches and has a case management system in place that is tied to their IT help desk. When a problem is reported to the help desk, a trouble ticket is generated that can be assigned to the information security group, at which point the incident is assigned a unique number in the case management system and all information relating to the investigation can be referenced using the incident number. The case management system helps organize information about all incidents in the organization, enabling digital investigators to search across all cases for similar characteristics (e.g., IP addresses of attackers and malware characteristics), and allowing management to generate statistics and metrics relating to incidents in the organization (e.g., incidents per month, total time spent on incident handling, and average time to resolution).

In addition to establishing a case management process and supporting systems, there are a number of steps that Corporation X has taken to prepare for a digital investigation. As part of the overall risk management process, Corporation X has identified all of the critical assets on their network along with related sources of digital evidence. By doing this, the organization can quickly assess the severity of a security breach on the basis of the systems that are targeted and can efficiently locate and preserve the primary sources of digital evidence that will be needed to investigate the incident. Part of the preparation process involved enhancing logging of system and network activities to provide more visibility. Incident response policy and procedures were also developed to formally outline the approval/authorization process for initiating an investigation, roles and responsibilities of the investigative team, and guidelines for digital investigators to preserve and examine data. Finally, Corporation X has two properly trained digital investigators, Jack and Jill, who are equipped with the necessary hardware and software to perform their jobs. These individuals have daily responsibilities to assist in the overall information assurance operations at Corporation X, including routinely monitoring logs that may alert them to a problem. In addition, Jack and Jill employ the scientific method when testing their hardware and software, running tests and experiments with sample datasets to ensure that the tools perform as expected.

6.4.2 Accusation or Incident Alert

In this case, Jill observes unusually high numbers of failed logon attempts to a server that contains plans and details of Corporation X's newest product, code named *FastJet*. She contacts the system administrator for the system and, after a quick review of recent system logs, he confirms that there has been unauthorized use of the administrator account on the system. There is a strong indication that a security breach has occurred.

6.4.3 Assessment of Worth

The server in question contains some of Corporation X's most valuable intellectual property. Theft of this information could result in a loss of competitive advantage and could reduce the overall value of the company. As a result, this breach is considered most serious and worth a full-scale investigation to determine whether the intruders stole sensitive information relating to the FastJet project.

6.4.4 Authorization

Jill informs Corporation X's management and attorneys of the developing situation and obtains approval to gather evidence and report back any findings.

6.4.5 Survey

If the organization had not been prepared, digital investigators would waste substantial time and effort trying to locate sources of digital evidence, and might ultimately find that there was insufficient information to reach any conclusions about the security breach. Fortunately, because Corporation X took steps to prepare their network and IT systems from a forensic standpoint, Jack has an abundance of log data to work with. Corporation X's digital evidence map, which Jack and Jill helped prepare, enables them to identify all relevant sources of information on the network in an efficient manner. In addition, all of the necessary documentation of the evidence, including chain of custody and evidence details, is initiated and maintained from this point forward.

Although the digital evidence map is a powerful tool in a digital investigation, Jill never assumes that it will enable her to identify all relevant sources of evidence. In this case, she asks the system administrator a few questions about the specific server and learns that he had set up his own logging mechanism to help him maintain the server. This logging mechanism proves to be a very useful source of evidence in the investigation.

6.4.6 Preservation

Jill instructs the system administrator of the compromised server to leave the systems running and unaltered so that Jack can take steps to preserve volatile data. The compromised system is centrally managed and can be accessed remotely to collect volatile data. However, some systems that are peripherally involved in the incident are not set up to support remote forensic processes, requiring the digital investigators to gain physical access to each of them in order to gather the necessary data. While Jack traveled to the location of the compromised systems, Jill took steps to freeze network-level logs to prevent them from being overwritten. Jill copied network-level logs onto a system dedicated to preserving evidence and documented their origin and integrity. Anticipating that the intruder would return, Jill also monitored network traffic to record the intruder gaining unauthorized access to compromised hosts from another system on the network.

Jack gained access to the compromised systems and followed standard operating procedures as discussed in Chapter 13 to confirm that the host had been compromised and to preserve related evidence.

Documentation associated with each item of evidence is maintained throughout the preservation process. In addition, Jill and Jack validate each source of digital evidence they preserve to ensure that they obtain a complete and accurate duplicate of the data with minimal impact to the original systems.

6.4.7 Transportation

One of the systems that Jack encounters out in the field needs to be transported back to their office for processing. Jack labels and packs all the components to ensure that they will not be damaged during transit, and to enable him to put the system back together when it arrives in their office. He also removes power from the hard drives and covers the SATA interface of each drive with evidence tape. In this way, someone would not be able to inadvertently start the system without breaking the evidence tape and plugging the hard drive back into the power supply.

6.4.8 Examination

Jack and Jill follow standard protocols they have developed over many digital investigations to extract useful information from all of the digital evidence they have preserved.

6.4.9 Analysis

A preliminary analysis of the digital evidence from the system revealed trace evidence attributing a point of origin, method of initiation, and activities of the intruder. The intruder had broken in through a recently publicized vulnerability

in the Oracle database software running on the server. The intruder had fixed the vulnerability to prevent others from exploiting it, installed a rootkit with a backdoor for regaining entry to the system, and started a sniffer to monitor network traffic. There was no evidence on the system that revealed the source of the attack or the intruder's IP address. Corporation X's firewall, intrusion detection system, and NetFlow logs did not appear to contain any entries that were obviously related to the intrusion.

Jack and Jill identified trace evidence compatible with the intruder using a stolen account on an internal system (192.168.0.5) to launch attacks against other hosts on the network. The firewall, intrusion detection system, and the router that generated NetFlow logs were not between the launch pad and the target hosts. This explained how the intruder had been able to target the vulnerable ports on the compromised systems even though they were protected by a firewall. This also explained why the intrusion detection systems and NetFlow logs did not contain any useful data.

The intruder had stored tools in a hidden directory of this stolen account but had not been able to erase system log files. The examiner collected the log files and contents of the stolen account as evidence. Logon records from the stolen account contained the IP address of a computer on a business partner's network—Business Z in San Francisco.

6.4.10 Reporting

Jack called his counterpart in Business Z on her mobile phone to inform her of the problem. She quickly determined that the Windows NT system in question (172.16.12.15) was running a Trojan horse program named Back Orifice and did not contain any log containing the intruder's IP address. Also, Business Z's intrusion detection system logs did not contain any alerts relating to the compromised Windows NT system, probably because connections between the Back Orifice client and server were encrypted. However, Business Z's NetFlow logs did show incoming connections to the compromised Windows NT system and subsequent outgoing connections to the machine on Corporation X's network.

The two digital investigators corrected the time zone difference between New York and San Francisco and confirmed that these connections corresponded to the logon records from the stolen account. They immediately contacted the ISP that the intruder was using and asked them to preserve evidence on their systems relating to the intrusions.

Jack and Jill wrote an internal report of the security breach for Corporation X's management and attorneys. The internal report also recommended that Corporation X install permanent network monitoring probes on all of their important network segments to ensure that attacks launched from systems within their network were logged in the future.

Based upon findings in the digital investigation, Corporation X reported the incident to the FBI and provided them with enough information to obtain subscriber details from the ISP used by the intruder. The FBI determined that the dial-up account used by the intruder had been stolen. Fortunately, the ISP had Automatic Number Identification (ANI) records that contained the intruder's home telephone number.

After performing a background check and further investigation to satisfying themselves that the resident of the house was responsible for the connections, the FBI obtained a search warrant and seized the suspect's computers. An examination of these computers revealed many links with Corporation X's compromised servers, including information relating to the FastJet project and sensitive data captured in sniffer logs. Faced with overwhelming evidence, the suspect admitted his involvement and provided the FBI with a list of his accomplices.

6.5 SUMMARY

This chapter provided a formalized process to help investigators reach conclusions that are reliable, repeatable, well documented, as free as possible from error, and supported by evidence. Heavy reliance on the scientific method helps overcome preconceived theories, encouraging digital investigators to validate their findings by trying to prove themselves wrong, leading to well-founded conclusions that support expert testimony.

The important concepts of case management and analysis were discussed along with each discrete step in the investigative process. The ultimate aim of investigative models is to help digital investigators take steps that are (1) generally accepted, (2) reliable, and (3) repeatable, and that lead to (4) logical, (5) well-documented conclusions of (6) high integrity. All six of these tenets have a common purpose—to form the most persuasive argument possible based upon facts, not supposition, and to do so considering the legal criteria for admissibility.

The success of each step of the investigative process is dependent on preparation in the form of policies, protocols, procedures, training, and experience. Anyone responding to an accusation or incident should already have policies and protocols to follow and should have the requisite knowledge and training to follow them. Similarly, anyone processing and analyzing digital evidence should have standard operating procedures, necessary tools, and the requisite training to implement them.

REFERENCES

Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, *2*(2), 146–166.

Carrier, B. (2003). Defining digital forensic examination and analysis tools using abstraction layers. *International Journal of Digital Evidence*, *1*(4).

Carrier, B. D. (2006). A hypothesis-based approach to digital forensic investigations. Ph.D. Dissertation, Purdue University.

Carrier, B. D., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, *2*(2).

Casey, E. (1997). *Digital evidence and computer crime* (1st ed.). London: Academic Press.

Casey, E. (2002). Error, uncertainty and loss in digital evidence. *International Journal of Digital Evidence*, *1*(2).

Casey, E. (2007). Digital evidence maps—A sign of the times. *Journal of Digital Investigation*, *4*(2).

Casey, E., Ferraro, M., & Nguyen, L. (2009). Investigation delayed is justice denied: Proposals for expediting forensic examinations of digital evidence. *Journal of Forensic Science*, *54*(6). November 2009.

Cohen, F. (2009). *Digital forensic evidence examination*. Fred Cohen & Associates.

Ieong, R. S. C. (2006). *FORZA*—Digital forensics investigation framework that incorporate legal issues. Proceedings of DFRWS2008. Available from http://www.dfrws.org/2006/proceedings/4-Ieong.pdf.

Madia, K., Prosise, C., & Pepe, M. (2003). *Incident response & computer forensics*. USA: McGraw.

McKemmish, R. (1999). *What is forensic computing? Trends and issues in crime and criminal justice* (Vol. 118). Canberra: Australian Institute of Criminology.

Ó Ciardhuáin, S. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence*, *3*(1).

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, *1*(3).