Computer and Network Forensics 14

14.1 Definition

The proliferation of computer technology, including wireless technology and telecommunication, the plummeting prices of these technologies, the miniaturization of computing and telecommunication devices, and the globalization forces have all together contributed to our ever-growing dependence on computer technology. This growing dependence has been a bonanza to computer criminals who have seen this as the best medium to carry out their missions. In fact, Richard Rubin [1] has called this new environment a tempting environment to cybercriminals, and he gives seven compelling reasons that cause such temptations. They are as follows:

- Speed. Both computer and telecommunication technology have greatly increased the speed of transmission of digital data, which means that one can violate common decency concerning transmission of such data speedily and not get caught in the act. Also, the act is over before one has time to analyze its consequences and one's guilt.
- Privacy and Anonymity. There is a human weakness that if no one is a witness to an act one has committed, then there is less to no guilt on the doer's part. Privacy and anonymity, both of which can be easily attained using this new technology, support this weakness enabling one to create what can be called "moral distancing" from one's actions.
- Nature of Medium. The nature of storage and transmission of digital information in the digital age is different in many aspects from that of the Gutenberg-print era. The electronic medium of the digital age permits one to steal information without actually removing it. This virtual ability to remove and leave the original "untouched" is a great temptation, creating an impression that nothing has been stolen.
- Aesthetic Attraction. Humanity is endowed with a competitive zeal to achieve far and beyond our limitations. So we naturally get an adrenaline high whenever we accomplish a feat that seems to break down the efforts of our opponents or

J.M. Kizza, *Guide to Computer Network Security*, Computer Communications and Networks, DOI 10.1007/978-3-319-55606-2_14

the walls of the unknown. It is this high that brings about a sense of accomplishment and creative pride whenever not so well-known creative individuals come up with elegant solutions to technological problems. This fascination and a sense of accomplishment create an exhilaration among criminals that mitigates the value and the importance of the information attacked and justifies the action itself.

- Increased Availability of Potential Victims. There is a sense of amusement and ease to know that with just a few key strokes, one's message and action can be seen and consequently felt over wide areas and by millions of people. This sense unfortunately can very easily turn into evil feelings as soon as one realizes the power he or she has over millions of invisible and unsuspecting people.
- International Scope. The global reach of cyberspace creates an appetite for greater monetary, economic, and political powers. The ability to cover the globe in a short time and to influence an entire global community can make a believer out of a nonbeliever.
- Enormous Powers. The international reach, the speed, and the distancing of one self from the act endow enormous powers to an individual which may lead to criminal activities.

There are reasons to believe Rubin because the rate of computer crime is on the rise. Fighting such rising crimes is a formidable task. It includes education, legislation, regulation, enforcement through policing, and forensics. In both computer forensics and network, the battle starts in the technical realms of investigative science that require the knowledge or skills to identify, track, and prosecute the cybercriminal. But before we discuss network forensics, which some call Internet forensics, let us start by looking at computer forensics. We will come back to network forensics in Sect. 14.3.

14.2 Computer Forensics

By definition, computer forensics is the application of forensic science techniques to computer-based material. This involves the extraction, documentation, examination, preservation, analysis, evaluation, and interpretation of computer-based material to provide relevant and valid information as evidence in civil, criminal, administrative, and other cases. In general, computer forensics investigates what can be retrieved from the computer's storage media such as hard disk and other disks. In Sect. 14.3, we will contrast it with network forensics. Because we are dealing with computer-based materials in computer forensic science, the focus is on the computer, first as a tool and as a victim of the crime. The computer as a tool in the crime is merely a role player, for example, as a communication tool, if the crime is committed using a computer network, or as a storage facility where the bounty is stored on the computer files. As a victim, the computer is now the target of the attack, and it becomes the focus of the forensic investigation. In either case, the computer is central to the investigations because nearly all forensic cases will

involve extracting and investigating data that is retrieved from the disks of the computer, both fixed and movable, and all its parts.

14.2.1 History of Computer Forensics

The history of computer forensics is tied up in the history of forensic science. According to Hal Berghel [2], the art of forensic science is actually derived from forensic medicine, an already recognized medical specialty. Forensic medicine's focus was autopsy examination to establish the cause of death. Although computers were in full use by the 1970s, mainly in big organizations and businesses such as banks and insurance companies, crimes involving computers as tools and as victims were very rare. One of the first recorded computer crimes during that time period was based on "interest rounding." Interest rounding was a round-robin policy used by banks to fairly distribute truncated floating point interest on depositors' accounts. The banks would round a depositor's interest points to a full cent. Anything less than a cent would be moved to the next account in a round-robin fashion.

Programmers, however, saw this as a source of ill-gotten wealth. They established an account to which they moved this less than a cent interest. With big banks with many depositors, this would add up. Because these programmers, like all computer criminals of the time, were highly educated, all computer crimes of the period were "white-collar" crimes. Law enforcement agencies of the time did not know enough about these types of computer crimes. Even the tools to gather evidence were not available. In a few cases where tools were available, they were often homemade [3].

It was not until the mid-1980s that some computer forensic tools such as X-Tree Gold and Norton Disk Editor became available. With these tools, investigators were able to recognize file types and were able to extract data on DOS-based disks. The 1990s saw heightened activities in computer crime and forensic investigations. The decade also produced an assortment of fine forensic tools that included the Forensic Toolkit.

Although the development of computer forensics started slow, it has now evolved as technology developed to where we are today. The increasing use of computers by law enforcement investigators and prosecutors and, as noted earlier, the widespread and rampant increase in computer-related crimes have led to the development of computer forensics. The primary focus and methodology, although still embedded in the basic physical forensics, have been tracing and locating computer hardware, recovering hidden data from the digital storage media, identifying and recovering hidden data, decrypting files, decomposing data, cracking passwords, and bypassing normal operating system security controls and permissions [4].

14.2.2 Elements of Computer Forensics

There are three key elements in any forensic investigations: the material itself, its relevance to the case in question, and the validity of any observations/conclusions reached by the examiner. Since computer forensics is very similar to ordinary physical forensics, these elements remain the same in computer forensics.

14.2.2.1 The Material

In both roles the computer plays in forensic science, the cases we have given above, the materials involved are both electronic and physical. Physical material investigation falls within the realms of the traditional police investigations where files and manila envelopes and boxes are all examined. The electronic form data is a little trickier to deal with. It may be data that does exist in hard copy, such as e-mail text, e-mail headers, e-mail file attachments, electronic calendars, Web site log files, and browser information. It may be deleted documents that must be recovered and reconstructed because deleted data does not necessarily disappear. Even when the reference to the deleted file is removed from the computer's directory, the bits that make up the file often remain on the hard drive until they are overwritten by new data. Beside deleted data, data also may be encrypted or password protected, making it more difficult to get in its original form.

If the computer is the focus of the investigation, then information from all system components is part of the required data. For example, network nodes and stand-alone personal computer operating systems create a great deal of administrative, management, and control information that is vital in the investigation.

14.2.2.2 Relevance

Once the existence of the material has been established, the next important step is to make sure that the material is relevant. The relevancy of the material will depend on the requesting agency, nature of the request, and the type of the case in question. The requesting agencies are usually one of the following:

- The victim
- Government
- Insurance companies
- The courts
- Private business
- Law enforcement
- Private individuals

We will talk more about relevancy when we discuss analysis of evidence.

14.2.2.3 Validity

The question of validity of data is tied up with the relevance of data. It is also based on the process of authentication of data. We are going to discuss this next.

14.2.3 Investigative Procedures

Both computer and network forensics (Sect. 14.3) methodologies consist of three basic components that Kruse and Heiser [5] both call the three As of computer forensic investigations. These are as follows: acquiring the evidence, taking care to make sure that the integrity of the data is preserved, authenticating the validity of the extracted data—this involves making sure that the extracted data is as valid as the original—and analyzing the data while keeping its integrity.

14.2.3.1 Looking for Evidence

As Kruse puts it, when dealing with computer forensics, the only thing to be sure of is uncertainty. So the investigator should be prepared for difficulties in searching for bits of evidence data from a haystack. The evidence usually falls into the following categories:

- Impressions: This includes fingerprints, tool marks, footwear marks, and other types of impressions and marks.
- Bioforensics: This includes blood, body fluids, hair, nail scrapings, and blood stain patterns.
- Infoforensics: This includes binary data fixed in any medium such as on CDs, memory, and floppies.
- Trace evidence: This includes residues of things used in the committing of a crime like arson accelerant, paint, glass, and fibers.
- Material evidence: This includes physical materials such as folders, letters, and scraps of papers.

As you start, decide on what the focus of the investigation is. At the start, decide on:

- What you have to work with: This may include written and technical policies, permissions, billing statements, and system application and device logs.
- What you want to monitor: This includes employer and employee rights, Internet e-mail, and chat room tracking.

Deciding what to focus on requires the investigator to make a case assessment that identifies the case requirements. To do this, the investigator must establish the following [3]:

- Situation—gives the environment of the case
- Nature of the case—broadly states the nature of the case
- Specifics about the case—states out what the case is about
- Types of evidence to look for—stating physical and electronic data and the materials to be collected and examined
- Operating system in use at the time of the incident
- Known disk formats at the time of the incident
- Location of evidence both physical and electronic

Once this information is collected, the investigation may start creating the profile of the culprit. At this point, you need to decide whether to let the suspect systems identified above run for a normal day, run periodically, or be pulled altogether if such actions will help the evidence-gathering stage. Pulling the plug means that you will make copies of the computer content and work with the copies while keeping the original intact. Make sure that the system is disconnected and that all that may be affected by the disconnection such as volatile data is preserved before the disconnection. Make duplication and imaging of all the drives immediately, and ensure that the system remains in its "frozen" state without being used during the investigation.

One advantage of pulling the plug is to "freeze" the evidence and prevent it from being contaminated with either new use or modifications or alterations. Also freezing the system prevents errors committed after the reported incident and before a full investigation is completed. However, freezing the system may result in several problems, including the destruction of any evidence of any ongoing processes.

On the other hand, working with a live system has its share of problems. For example, the intruder may anticipate a "live" investigation that involves an investigator working with a system still in operation. If the intruder anticipates such action, then he or she may alter the evidence wherever the evidence is well ahead of the investigator, thus compromising the validity of the evidence.

Whether you use a "live" system or a "frozen" one, you must be careful in the use of the software, both investigative and system software. Be careful and weigh the benefits of using software found on the system or new software. A number of forensic investigators prefer not to use any software found on the system for fear of using compromised software. Instead they use new software on the copy system, including system software. Another variation used by some investigators is to verify the software found on the system and then use it after. Each of these methods has advantages and disadvantages, and one has to be careful to choose what best serves the particular situation under review.

14.2.3.2 Handling Evidence

The integrity of the evidence builds the validity of such evidence and consequently wins or loses a case under investigation because it is this evidence that is used in the case to establish the facts upon which the merits, or lack of, are based. It is, therefore, quite important and instructive that extreme care must be taken when handling forensic evidence. Data handling includes extraction and the establishment of a chain of custody. The chain of custody itself involves packaging, storage, and transportation. These three form the sequence of events along the way from the extraction point to the courtroom. This sequence of events is traceable if one answers the following questions:

- Who extracted the evidence and how?
- Who packaged it?
- Who stored it, how, and where?
- Who transported it?

The answers to these questions are derived from the following information [3]:

- Case:
  - Case number—a number assigned to the case to uniquely identify the case
  - Investigator—name of the investigator and company affiliation
  - Nature of the case—a brief description of the case
- Equipment involved:
  - For all computing equipment, carefully describe the equipment including the maker, vendor, model, and serial number.
- Evidence:
  - Location where it is recorded
  - Who recorded it
  - Time and date of recording

This information may be filled in a form called the *chain-of-evidence* form.

14.2.3.3 Evidence Recovery

The process of evidence extraction can be easy or complicated depending on the nature of the incident and the type of computer or network upon which the incident took place. The million dollar question in evidence extraction is: What do I extract and what do I leave behind? To answer this question, remember that if you are in an area extracting data and you remove what you think is sufficient evidence only to come back for more, you may find that what you left behind is of no value anymore, a big loss. So the rule of thumb is extract and collect as much as you can so that the return trip is never needed.

What are the candidates for evidence extraction? There are many, including hardware such as computers, printers, scanners, and network connectors such as modems, routers, and hubs. Software items include system programs and logs, application software, and special user software. Documentation such as scrap paper and anything printed within the vicinity are also candidates and so are materials such as backup tapes and disks, CDs, cassettes, floppy and hard disks, and all types of logs.

In fact, according to Sammes and Jenkinson [6], an investigator should start the job only when the following items are at hand:

- An adequate forensic toolkit which may be a complete forensic computer workstation
- A search kit
- Search and evidence forms and sketch plan sheets
- Evidence bag
- Still, digital, and video cameras
- Disk boxes
- Mobile phone
- Blank floppy disks
- A flashlight

- Bitstream imaging tool
- Evidence container

With these at hand, the investigator then starts to gather evidence by performing the following steps [3]:

- Arrange for interviews with all parties involved in the case. This gives the investigator a chance to collect more evidence and materials that might help the case.
- Fill out the evidence form.
- Copy the digital evidence disk by making a bitstream copy or bit-by-bit copy of the original disk. This type of disk copying is different from a simple disk copy which cannot copy deleted files or e-mail messages and cannot recover file fragments. Bitstream copying then creates a bitstream image. As we will see in Sect. 14.4, there are several tools on the market to do this. Digital evidence can be acquired in three ways:
  - Creating a bitstream of disk-to-image file of the disk. This is the most commonly used approach.
  - Making a bitstream disk to disk used in cases that a bit-by-bit imaging cannot be done due to errors.
  - Making a sparse data copy of a file or folder.

Always let the size of the disk, the duration you have to keep the disk, and the time you have for data acquisition determine which extraction method to use. For large original source disks, it may be necessary to compress the evidence or the copy. Computer forensics compress tools are of two types: *lossless* compression which does not discard data when it compresses a file and *lossy* compression which loses data but keeps the quality of the data upon recovery. Only lossless compression tools such as WinZip or PKZip are acceptable in computer forensics. Other lossless tools that compress large files include EnCase and SafeBack. Compressed data should always have MD5, SHA-1 hash, or cyclic redundancy check (CRC) done on the compressed data for security after storage and transportation.

For every item of the evidence extracted, assign a unique identification number. Also for each item, write a brief description of what you think it is and where it was recovered. You may also include the date and time it was extracted and by whom. It is also helpful, where possible, to keep a record of the evidence scene either by taking a picture or by video. In fact where possible, it is better to videotape the whole process including individual items. This creates an additional copy, a video copy, of the evidence. After all the evidence has been collected and identified and categorized, it must be stored in a good clean container that is clearly labeled and safely stored. It is important to store the evidence at the most secure place possible that is environmentally friendly to the media on which the evidence is stored. For example, the place must be clean and dry. If the evidence was videotaped, the video must be stored in an area where video recordings can last the longest. Where it requires seizure of items, care must be taken to make sure that evidence is not

destroyed. If it requires dismantling the evidence object for easy moving and transportation, it is prudent that there be an identical reconstruction. Every electronic media item seized must be taken for examination.

When there is a need to deal with an unknown password, several approaches can be used. These include *second guessing*, use of *backdoors*, an undocumented key sequence that can be made available by manufacturers, and use of a *backup*.

And finally the investigator has to find a way of dealing with encrypted evidence. If the encrypting algorithm is weak, there are always ways and software to break such encryptions. However, if the algorithms are of a strong type, this may be a problem. These problems are likely to be encountered in encrypted e-mails, data files on hard drives, and hard disk partitions. Several products are available to deal with these situations [6]:

- For encrypted e-mails—use PGP.
- For encrypted hidden files—use Encrypted Magic Folders (http://www.pc-magic.com/des.htm).
- For hard drive encrypted files—use BestCrypt (http://www.jetico.com/encryption-bestcrypt/). Others are IDEA, Blowfish, DES, Triple DES, and CAST.

14.2.3.4 Preserving Evidence

There is no one standard way for securing evidence. Each piece of evidence, packing, and storage is taken on a case-by-case basis. Packaging the evidence is not enough to preserve its integrity. Extra storage measures must be taken to preserve the evidence for a long time if necessary. One of the challenges in preserving digital evidence is its ability to disappear so fast. In taking measures to preserve evidence, therefore, this fact must be taken into account. Evidence preservation starts at the evidence extraction stage by securing the evidence scene from onlookers and other interested parties. If possible, allow only those involved in the extraction to view it. Several techniques are used including the following:

- Catalogue and package evidence in a secure and strong antistatic, well-padded, and labeled evidence bag that can be secured by tape and zippers. Make sure that the packaging environment keeps the evidence uncontaminated by cold, hot, or wet conditions in the storage bag.
- Back up the original data including doing a disk imaging of all suspected media. Care must be taken especially when copying a disk to another disk; it is possible that the checksum of the destination disk always results in a different value than a checksum of the original disk. According to Symantec, the difference is due to differences in disk geometry between the source and destination disks [7]. Since Ghost, a Norton forensic product, does not create an exact duplicate of a disk but only recreates the partition information as needed and copies the contents of the files, investigators using Ghost for forensic duplication must be careful as it does not provide a true bit-to-bit copy of the original.
- Document and time-stamp, including the date, every and all steps performed in relation to the investigation, giving as many details as possible, however

insignificant the steps are. Note all network connections before and during the investigation.
- Implement a credible control access system to make sure that those handling the evidence are the only ones authorized to handle the evidence.
- Secure your data by encryptions, if possible. Encryption is very important in forensic science because it is used by both the investigator and the suspect. It is most commonly used by the suspect to hide content and by the investigator to ensure the confidentiality of the evidence. The integrity of the evidence is maintained when it has not been altered in any way. Encryption technology can also verify the integrity of the evidence at the point of use. Investigators must check to see that the encrypted system under examination has a key recovery system. It makes the job of the investigators ten times as more difficult if they encounter encrypted evidence. Data can become intercepted during transit.
- Preserve the evidence as much as possible by not adding or removing software, using only trusted tools, not using programs that use the evidence media.
- If possible validate and/or authenticate your data by using standards, such as Kerberos, and using digital certificates, biometrics, or timestamping. All these technologies are used in authentication, validation, and verification. The time when an object was signed always affects its trustworthiness because an expired or a revoked certificate is worthless. Timestamping is useful when collecting evidence because it provides incontestable proof that the digital evidence was in existence at a specific time and date and has not been changed since that date.

In addition to timestamping, the images of the hard drives and any volatile data saved before "freezing" the system, the following can also be time-stamped [5]:

- Ongoing collection of suspect activities including log files, sniffer outputs, and output from intrusion detection system
- Output from any reports or searches performed on a suspect machine, including all files and their associated access times
- Daily typed copies of investigator's notes

Note, however, that criminals can use all these same tools against investigators.

14.2.3.5 Transporting Evidence

Where it is necessary to transport the evidence either for safer security, more space, or to court, great care must be taken to safeguard the integrity of the evidence you have painstakingly collected and labored to keep safe and valid. Keep in mind that transportation pitfalls can be found across the transportation channel from the starting point all the way to the destination. Be aware that containers can be opened midway even from trusted individuals. So find the most secure, trusted, and verified way to transport the evidence. This may include constant and around-the-clock monitoring and frequent checks including signatures of all those handling the evidence along the way. The goal is to maintain a *chain of custody* to protect the

integrity of the evidence and to make it difficult for anybody to deny the evidence because it was tempered with.

Since during transportation the integrity of data may be affected, it is important to use strong data hiding techniques such as encryptions, steganography, password-protected documents, and other ways. Data hiding, a form of steganography, embeds data into digital media for the purpose of identification and annotation. Several constraints, however, affect this process: the quantity of data to be hidden, the need for invariance of this data under conditions where a "host" signal is subject to distortions, and the degree to which the data must be immune to interception, modification, or removal by a third party [8].

One of the important goals of data hiding in digital media in general and computer forensics in particular is to provide assurance of content integrity. Therefore, to ensure content integrity, the hidden data must stay hidden in a host signal even if that signal is subjected to degrading manipulation such as filtering, resampling, cropping, or lossy data compression.

Since data can be compromised during transit, there are ways to test these changes. Among these are the use of parity bits, redundancy checks used by communication protocols, and checksums. Even though these work, unfortunately they can all fall prey to deliberate attempts by hackers using simple utilities that can render them all useless. To detect deliberate attempts at data during transmission, a better technique is a cryptographic form of checksum called a hash function. Applying a hash function to data results in a *hash value* or a *message digest*. A robust hash algorithm such as MD5 and SHA-1 can deliver a computationally infeasible test of data integrity. Hash algorithms are used by examiners in two ways: to positively verify that data has been altered by comparing digests taken before and after the incident and to verify that evidence have not been altered.

Another way to safeguard evidence in transition, if it has to be moved either as a digital medium carried by somebody or electronically transferred, is data compression. As we have seen in Sect. 14.2.3.4, data compression can be used to reduce the size of data objects such as files. Since compression is a weak form of encryption, a compressed file can be further encrypted for more security.

14.2.4 Analysis of Evidence

After dealing with the extraction of evidence, identification, storage, and transportation, there now remains the most important and most time-consuming part of computer and network forensic science, that of analysis. As Kruse et al. noted, the most important piece of advice in forensics is "don't take anything for granted." Forensic evidence analysis is painstakingly slow and should be thorough. The process of analyzing evidence done by investigators to identify patterns of activity, file signature anomalies, unusual behaviors, file transfers, and several other trends to either support or reject the case is the most crucial and time-consuming in forensic investigation and should depend on the nature of the investigation and amount of data extracted. For example, non-litigation cases may not involve as

much care as the care needed for litigation ones because in litigation cases, there must be enough evidence of good quality to fend off the defense. According to Kruse, the following things should not be taken for granted [5]:

- Examine the shortcuts, Internet, recycle bins, and registry.
- Review the latest release of the system software with an eye on new methods of data hiding.
- Check every data tape, floppy disk, CD-ROM, DVD, and flash memory found during evidence extraction.
- Look in books, in manuals, under keyboards, on the monitor, and everywhere where people usually hide passwords and other pertinent information.
- Double-check the analysis.
- Reexamine every file and folder, log files, and print spooler.
- Recover any encrypted or archived file.

Once the evidence has been acquired and carefully preserved, then the analysis process begins. Make sure that all evidence is received at the examination center. All items must be in sealed evidence bags. An external examination of all items must be done before the internal examinations can begin. For disks and other recordable media, an imaging of each must be done. Currently tools to do this job include *DriveSpy*, *EnCase*, *CaptureIt*, *FTK Explorer*, and *dd* to name a few.

It is normal to start the hard drives with the following [9]:

- Hard drive physical analysis—seeking information of partitions, damaged sectors, and any data outside of the partitions
- Hard drive logical analysis—seeking information on active file metadata, context of information, file paths, file sizes, and file signatures
- Additional hard drive analysis—looking for active files, file system residues, erased files, electronic communications, and peripheral devices

After dealing with the hard drives, continue with other peripherals, documentation, and every other component that is relevant to the incident. The tools most used in this endeavor are discussed in Sect. 14.4. It is also important to note here that the amount of work done and sometimes the quality of the analysis done may depend on the platform you use. Forensic investigators are religiously devoted to their operating systems, but it is advisable to use whatever makes you comfortable.

The analysis itself should not be constrained; it should take any direction and any form. Specifically, it should focus on devices and on the storage media. Although we prefer the analysis to be loose and flowing, keeping close to the following guidelines is helpful [3]:

- Clearly know what you are looking for.
- Have a specific format for classifying data.
- Have and keep tools for data reconstruction.

- Request or demand for cooperation from agencies and departments, especially where you have to ask for help in evidence protection.
- Use only recently wiped media like disks as target media to store evidence. There are several tools to clean wipe a disk.
- Inventory the hardware and software on the suspect system because all may be part of the investigation.
- On the suspect system, remove the hard drive(s), noting the time and date in the system's CMOS.
- On the image disk:
  - List and check all directories, folders, and files.
  - Examine the contents of each. Where tools are needed to recover passwords and files, acquire such tools.
  - Note where every item found on the disk(s) was found and identify every executable, noting its function(s).

14.2.4.1 Data Hiding

While analyzing evidence data, it is very important to pay particular attention to data hiding. There are many ways data can be hidden in a file system including the following:

Deleted Files

Deleted files can be recovered manually using hex editor. When a file on a Windows platform is deleted, the first character of the directory entry is changed to a sigma character—hex value of E5. The operating system takes this sigma to indicate that the entry should not be displayed because the file has been deleted. The entry in the file allocation table (FAT) is also changed to zero, indicating unused sectors and therefore available to the operating system for allocation.

Similarly, MS-DOS does not remove data in clusters of files declared as deleted. It merely marks them as available for reallocation. It is, therefore, quite possible to recover a file that has been deleted, provided the clusters of the file have not been reused. DOS programs such as UNERASE and UNDELETE try to recover such files. But Norton Disk Editor is more effective.

Note that the operating system does not do anything to the data in these sectors until reallocating the sectors to another file. The data in the sectors are then overwritten. Before that, http://www.intergov.org/public_information/general_information/latest_web_stats.html data in these sectors can be reconstructed.

Hidden Files

Data hiding is one of the most challenging aspects of forensic analysis. With special software, it is possible to mark a partition "hidden" such that the operating system will no longer access it. Other hidden areas can be created by setting partition tables to start at head 0, sector 1 of a cylinder, and the first sector of the partition proper—the boot record—to start at head 1, sector 1 of the cylinder. The consequence of this is that there will invariably be a number of unused sectors at the beginning of each partition, between the partition table sector and the boot record sector [6].

In addition to these hidden areas, operating systems also hide files and filenames from users. Files and filenames, especially system files, are purposely hidden from users because we want the users not to be able to access those files from their regular display list. The filenames of system programs are usually hidden because average users do not have to know them and those who know them do not need to have them listed. When they need to see them, they can always list them.

Every operating system has a way of hiding and displaying hidden files. For example, Linux has a very simple way of "hiding" a file. Creating a file with an added period to the front of the filename which defines to Linux that the filename is "hidden" makes it hidden. To display Linux hidden files, add the **-a** flag (display all filenames) to the **ls** (list) command like "ls –a." This displays all of files in the current directory whether hidden or not. Similarly Unix does not display any files or directories that begin with the dot (.) character. Such files can be displayed by either the Show Hidden Files option or the -a switch of the ls command.

Because of these cases, it is, therefore, always prudent to assume that the candidate system has hidden files and data. Hidden data is always a clue for investigators to dig deeper. There are a number of ways to hide data including encryption; compression; codes; steganography; and using invisible names, obscure names, misleading names, and invisible names. We will discuss these throughout this chapter.

Slack Space

This is unused space in a disk cluster. Both DOS and Windows file systems use fixed-size clusters. During space allocation, even if the actual data being stored require less storage than the cluster size, an entire cluster is reserved for the file. Sometimes this leaves large swats of used space called *slack space*. When a file is copied, its slack space is not copied. It is not possible to eliminate all slack space without changing the partition size of the hard disk or without deleting or compressing many small files into a larger one. Short of eliminating these wasted spaces, it is good to have software tools to examine this slack space and find out how big it is and what is hidden in it. If this is not done, there is a risk of slack space containing remnants of hostile code or hidden confidential files.

Bad Blocks

A bad track is an area of the hard disk that is not reliable for data storage. It is possible to map a number of disk tracks as "bad tracks." These tracks are then put into a bad track table that lists any areas of the hard disk that should not be used. These "bad tracks" listed on the table are then aliased to good tracks. This makes the operating system avoid the areas of the disk that cannot be read or written. An area that has been marked as "bad" by the controller may well be good and could store hidden data. Or a good sector could be used to store incriminating data and then be marked as bad. A lot of data can be hidden this way in the bad sectors by the suspect. Never format a disk before you explore all the bad blocks because formatting a disk deletes any data that may be on the disk.

Steganography Utilities

Steganography is the art of hiding information in ways that prevent its detection. Steganography, an ancient craft, has seen a rebirth with the onset of computer technology with computer-based steganographic techniques that embed information in the form of text, binary files, or images by putting a message within a larger one in such a way that others cannot discern the presence or contents of the hidden message. The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. This is, therefore, a threat to forensic analysts as they now must consider a much broader scope of information for analysis and investigation. Steganalysis uses utilities that discover and render useless such covert messages.

Password-Cracking Software

This is software that once planted on a user's disk or finds its way to the password server tries to make any cryptosystems untrustworthy or useless by discovering weak algorithms, wrong implementation, or application of cryptalgorithms and human factor.

NTFS Streams

In NTFS (Windows NT File System), a file object is implemented as a series of streams. Streams are an NTFS mechanism allowing the association and linking of new data objects with a file. However, the NT NTFS has an undocumented feature that is referred to by different names, including alternate data streams, multiple data streams on the Microsoft TechNet CD, named data streams, and forked data streams. Whatever name it is called, this feature of NTFS is not viewable to ordinary NT tools. That means that data hidden in these streams are not viewable by GUI-based programs and Windows Explorer, for example. It is, however, easy to write in these streams using Windows Notepad. If this happens, however, then File Explorer has no mechanism to enumerate these additional streams. Therefore, they remain hidden to the observer. This is a security nightmare because these streams can be exploited by attackers for such things as denial-of-service and virus attacks. Also many network users can store data on an NT server that administrators are not aware of and cannot control.

Codes and Compression

There are two techniques combined here. Coding is a technique where characters of the data are systematically substituted by other characters. This technique can be used by system users to hide vital or malicious data. Data compression on the other hand is a way of reducing the size of data object like a file. This technique is also increasingly being used by suspects to hide data. Forensic investigators must find a way to decipher coded or compressed evidence. Uncompressing compressed data can reveal to investigators whether evidence is encrypted or not. To deal with all these, it is imperative that a forensic investigator acquires forensic tools that can decompress, decrypt, decode, and crack passwords and tools to uncover hidden data. We will survey these tools in Sect. 14.4.

Forensic analysis is done to positively identify the perpetrator and the method he or she is using or used to commit the act, to determine network vulnerabilities that allowed the perpetrator to gain access into the system, to conduct a damage assessment of the victimized network, and to preserve the evidence for judicial action, if it is necessary. These objectives which drive the analysis are similar in many ways to those set for physical forensics. So computer forensics examiners should and must develop the same level of standards and acceptable practices as those adhered to by physical investigators.

14.2.4.2 Operating System-Based Evidence Analysis

Most forensic analysis tools are developed for particular platforms. Indeed many forensic investigators prefer to work on specific platforms than on others. Let us briefly look at forensic analysis based on the following platforms:

Microsoft-Based File Systems (FAT8, FAT16, FAT 32, and VFAT)

Because most computer forensic tools so far are developed for Microsoft file systems, we will start with that. According to Bill Nelson et al., an investigator performing forensic analysis on a Microsoft file system must do the following [3]:

- Run an antivirus program scan for all files on the forensic workstation before connecting for a disk-to-disk bitstream imaging.
- Run an antivirus scan again after connecting the copied disk-to-disk bitstream image disk to all drives including the copied drive unless the copied volumes were imaged by EnCase or SaveSet.
- Examine fully the copied suspect disk noting all boot files in the root.
- Recover all deleted files, saving them to a specified secure location.
- Acquire evidence from FAT.
- Process and analyze all recovered evidence.

NTFS File System

Use tools such as DriveSpy to analyze evidence just like in FAT file systems.

Unix and Linux File Systems

Although forensic tools for Linux are still few, the recent surge in Linux use has led to the development of new tools, including some freeware such as the Coroner's Toolkit (TCT) and the Sleuth Kit (TSK). These tools and most GUI tools can also analyze Unix. These include EnCase, FTK, and iLook. Because most Unix and Linux systems are used as servers, investigators, according to Nelson et al., must use a live system. When dealing with live systems, the first task for the investigator is to preserve any data from all system activities that are stored in volatile memory. This saves the state of all running processes, including those running in the background. These activities include the following [3]:

- Console messages
- Running processes

- Network connections
- System memories
- Swap space

Macintosh File System
All system running Mac OS9X or later versions uses the same forensic tools such as Unix, Linux, and Windows. However, for older MAC systems, it is better to use tools like Expert Witness, EnCase, and iLook.

14.3 Network Forensics

In Sect. 14.2, we gave a definition for computer forensics that network forensics contrasts. Unlike computer forensics that retrieves information from the computer's disks, network forensics, in addition, retrieves information on which network ports were used to access the network. Dealing with network forensics, therefore, implies taking the problems of computer forensics and multiplying them one hundred times, a thousand times, and sometimes a million times over. Some of the things we do in computer forensics cannot be done in network forensics. For example, it is easy to take an image of a hard drive when we are dealing with one or two computers. However, when you are dealing with a network with five thousand nodes, it is not feasible. There are other differences. Network forensics, as Berghel observed, is different from computer forensics in several areas, although it grew out of it. And its primary objective, to apprehend the criminal, is the same. There are several differences that separate the two including the following:

- Unlike computer forensics where the investigator and the person being investigated, in many cases the criminals, are on two different levels with the investigator supposedly on a higher level of knowledge of the system, the network investigator and the adversary are at the same skills level.
- In many cases, the investigator and the adversary use the same tools: one to cause the incident and the other to investigate the incident. In fact, many of the network security tools on the market today, including NetScanTools Pro, Traceroute, and Port Probe, used to gain information on the network configurations, can be used by both the investigator and the criminal. As Berghel puts it, the difference between them is on the ethics level, not the skills level.
- While computer forensics, as we have seen in Sect. 14.3, deals with the extraction, preservation, identification, documentation, and analysis and it still follows well-defined procedures springing from law enforcement for acquiring, providing chain of custody, authenticating, and interpretation, network forensics on the other hand has nothing to investigate unless steps were in place (like packet filters, firewalls, and intrusion detection systems) prior to the incident.

However, even if network forensics does not have a lot to go after, there are established procedures to deal with both intrusive and nonintrusive incidents. For intrusive incidents, an analysis needs to be done.

14.3.1 Intrusion Analysis

Network intrusions can be difficult to detect let alone analyze. A port scan can take place without a quick detection, and more seriously a stealthy attack to a crucial system resource may be hidden by a simple innocent port scan. If an organization overlooks these simple incidents, it may lead to serious security problems. An intrusion analysis is essential to deal with these simple incidents and more serious ones like backdoors that can make reentry easy for an intruder, a program intentionally left behind to capture proprietary data for corporate espionage, or a program in waiting before launching a denial-of-service attack.

The biggest danger to network security is pretending that an intrusion will never occur. As we noted in Sect. 10.3, hackers are always ahead of the game; they intentionally leave benign or not easily detectable tools behind on systems that they want to eventually attack. Unless intrusion analysis is used, none of these may be detected. So the purpose of intrusion analysis is to seek answers to the following questions:

- Who gained entry?
- Where did they go?
- How did they do it?
- What did they do once into the network?
- When did it happen?
- Why the chosen network?
- Can it be prevented in the future?
- What do we learn from the incident?

Answers to these questions help us to learn exactly what happened, determine the intruder motives, prepare an appropriate response, and make sure it doesn't happen again. A thorough intrusion analysis requires a team of knowledgeable people who will analyze all network information to determine the location of evidence data. Such evidence data can reside in any one location of the network, including appliances and service files that are fundamental to the running of the network like [9]:

- Routers and firewalls.
- FTP and DNS server files.
- Intrusion detection systems monitor log files.
- System log files including security, system, remote access, and applications.
- Exchange servers.
- Servers' hard drives.

Intrusion analysis involves gathering and analyzing data from all these network points. It also consists of the following services [2]:

- Incident response plan
- Incident response
- Technical analysis of intrusion data
- Reverse engineering of attacker tools (reverse hacking)

All results of the analysis must be redirected to an external safe and secure place.

On systems such as Unix and Linux servers, the intrusion investigators must examine system log files to identify accounts used during the penetration. Investigators must also examine [3]:

- All running processes
- All network connections
- All deleted files
- All background processes
- File system
- Memory status
- Contents of each swap
- Backup media
- All files created or modified during the incident

These help the investigator to reconstruct the system in order to be able to determine what happened.

14.3.1.1 Incident Response Plan

The incident response plan should be based on one of the three philosophies: watch and warn, repair and report, and pursue and prosecute. In watch and warn, a monitoring and reporting system is set up to notify a responsible party when an incident occurs. This is usually a simple monitoring and reporting system with no actions taken beyond notifications. Some of these systems have now become real-time monitoring and reporting systems. The repair and report philosophy aims at bringing the system back to normal running as soon as possible. This is achieved through a quick identification of the intrusion, repairing all identified vulnerability, or blocking the attack and quickly reporting the incident to the responsible party. Finally, the pursue and prosecute philosophy involves monitoring for incidents, collection of evidence if an attack occurs, and reporting beyond technical staff that involves law enforcement and court charges.

The response plan should also outline the procedures to be taken and indicate the training needed. Under the procedures, everyone should know what he or she should do. The procedures should also indicate what level of priorities should receive the greatest level of attention. The response plan is important to an investigator because if the plan is good and it is followed, it should have documented the circumstances that may have caused the incident and what type of response was

immediately taken. For example, were the machines "frozen"? When and by whom? What immediate information about the attack and the attacker was known, who knew about it, and what was done immediately? What procedures were taken to deal with remote systems and connections to public networks? Disconnecting from the network can isolate the systems and keep the attackers from entering or sometimes exiting the network. However, severing all connections may not only disrupt the services, but it may also destroy the evidence. Communication is important, and there should be one designated person to handle all communication, especially to the public. Finally response plan information also consists of documentation of the activities on the system and networks as well as system configuration information before the incident. It also consists of support information such as a list of contacts and their responses; documentation on the uses of tools and by whom is also included [10]. Since different circumstances require different responses, the investigator needs to know what response was taken and have all the documentation of whatever was done.

14.3.1.2 Incident Response

Incident response is part of the security plan that must be executed whenever an incident occurs. Two items are important to an investigator in the incident response. These are incident notification and incident containment. In incident notification, what the investigator wants to know are as follows: Who knew first and what were the first responses? Who was notified in the process and what were the responses? It is common that the first person to notice the incident always deals with it. Usually employees "see" the incident in progress first and inform the "Techs" that the machines are running "funny" or slow. Incident notification procedures need to be built into the operating incident plan. The work of the response team may also be of interest to the investigator. The response team should get clear and precise information, and it should consist of people with the knowledge and skills needed to handle security incidents. It is this expertise that the investigator needs to tap into. Finally, since the reporting procedures require management to know immediately, the investigator may be interested in that trail of information. Also the response team may have information, preliminary at first but may improve later, of the extent of the attack. Usually they know who was affected and what actions were taken on their machines and tools. Also note if law enforcement agencies were contacted and what type of information was given.

Incident containment is required to stop the incident if possible but more so to minimize the effects of the incident. Rapid response is critical in today's automated attacks that are able to scan systems, locate vulnerabilities, and penetrate them with lightning speed and with limited human intervention. Incident containment is important to the investigator because it contains efforts taken to deny access to the system and the number of affected systems. The containment plan consists of the following response items: determination of affected systems, denying the attacker access to systems, elimination of rogue processes, and regaining control [10]. The documentation in each of these should provide the investigator with a trove of good information. The investigators should be particularly interested in the

plan's regaining of control because valuable evidence clues may be lost. To regain control means to bring the system back to the state it was in before the incident. The first effort in regaining control is to lock out the attacker. This is important because, when discovered, the attacker may try to destroy as much of the evidence as possible. Blocking the attacker's access may be achieved by blocking access at the firewall or a complete disconnection of the system. Actions that follow may include change of passwords, disabling of services, removal of backdoors, if those can be found, and monitoring of activities. In addition, if no further legal actions are required, the sanitation of the system may be required. However, if further legal recourse is anticipated, then this may be avoided for some time to allow the investigator to recover the evidence. After the evidence has been collected, then the rebuilding of the system involving the use of backups, applying security patches, and reloading of data begin. Since attacks can originate either from outside or internally, incident containment plans must be handled with care and secrecy in case the suspect is in the house.

14.3.1.3 Technical Analysis of the Intrusions

The most difficult, time-consuming, and technically challenging part of network forensics is the technical analysis of intrusions and intrusion data. Typically, unlike computer forensics where most of the evidence may reside on the victim machine, in network forensics, evidence does not reside on one hard drive or one machine; it may require to search many disks and many network computers. As we pointed out earlier, the investigator must have almost the same skills as the suspect and many times may use the same tools. In any case, as we discussed in Sect. 14.3.1, in any suspected incident occurring in a network environment, we may need to analyze the following network information to determine the location of pertinent information.

One of the most important and crucial source of logs on the Internet is the ISP. Since ISPs deal with lots of dial-up customers, each customer dialing in must be authenticated before a call is dynamically assigned an IP address by the Dynamic Host Configuration Protocol (DHCP) server. This IP address is associated with a DNS, thus allowing reverse lookup. The authentication is done by the Remote Authentication Dial-In User Service (RADIUS). However, RADIUS does not only authenticate calls, but it also maintains records that can be used to track down a suspect [5]. RADIUS information includes IP address assigned, connection time, telephone number used from a caller ID, and log-in name. ISPs maintain these logs for some time, sometimes up to a year, before purging them. However, investigators should not take this information as always valid. It can and it has been changed before. But as Kruse points out, the value of ISP information is to have the telephone number, date, and time of the incident. This can be followed by a subpoena.

Other good sources of investigator information are e-mail and new postings. Both these services offer good tracking attributes like:

- Store-and-forward architecture that moves messages of printable characters from network node to network node in a next-hop framework

- Human-readable message headers that contain the path between the sender and receiver

This information is useful to an investigator. For example, all e-mail servers have the ability to maintain a logging information. Let us look at this closely. E-mail programs, called clients, are based on application-level protocols. There are several of these protocols, including Post Office Protocol (POP), Internet Message Access Protocol (IMAP), Microsoft's Mail API (MAPI), and HTTP for Web-based mail. All outgoing e-mails use a different protocol called Simple Mail Transfer Protocol (SMTP). Unlike incoming protocols above used to receive e-mails, outgoing protocol SMTP does not require authentication. The SMTP at the client sends e-mail messages to the STMP at the mail server or at the ISP, which then relays e-mail messages to their destinations without any authentication. However, to give such e-mails some degree of trust, authentication protocols such as PGP or S/MIME (Secure/Multipurpose Internet Mail Extensions) are used on top of STMP. SMTP servers, however, maintain logging information which is more reliable than mail headers and may be useful to an investigator.

Another good source of information for forensic investigators is Usenet, a huge distributed news bulletin board consisting of thousands of news topics beautifully arranged. Throughout the news network are thousands of news servers running Network News Transfer Protocol (NNTP). In the header of each message news body, there is a path that forms the crest of the investigation. One can trace every NNTP host that the message has traversed in reverse chronological order. Also like mail servers, NNTP may or may not accept postings from nonmembers.

Finally, enormous amount of data can be gotten from monitoring systems like firewalls, intrusion detection systems, and operating system logs.

14.3.1.4 Reverse Hacking

Reverse engineering, commonly known as reverse hacking, is literally taking an offending package, breaking it up, and using it to try and trace the source of the attack. Antivirus writers have long used the technique by capturing the virus signature, usually a traffic package, breaking it up, and studying the patterns which then lead to an antivirus.

14.3.2 Damage Assessment

It has been difficult so far to effectively assess damage caused by system attacks. For the investigator, if the damage assessment report is available, it can provide a trove of badly needed information. It shows how widespread the damage was and who was affected and to what extent. Further it shows what data, system, services, and privileges were compromised. It is also from this report that the length of the incident can be established and the causes, vulnerability exploited, safeguards bypassed, and detection avoided. From this report, one can also be able to determine if the attack was manual or automated. If the source of the attack is indicated in the

report, then one can use it to trace network connections which may lead to other directions of the investigation.

To achieve a detailed report of an intrusion detection, the investigator must carry out a postmortem of the system by analyzing and examining the following [3]:

- System registry, memory, and caches. To achieve this, the investigator can use dd for Linux and Unix systems.
- Network state to access computer network accesses and connections. Here netstat can be used.
- Current running processes to access the number of active processes. Use ps for both Unix and Linux.
- Data acquisition of all unencrypted data. This can be done using MD5 and SHA-1 on all files and directories. Then store this data in a secure place.

14.4 Forensic Tools

Let us end this chapter by looking at the tools of the trade for forensic investigators. Like a hunter, forensic investigators rely on their tools. They succeed or fail based on their tools. Because of this, it is important that the investigators make sure that their tools are not only trusted but also that they work before they start the job.

Always try the tools on something before they are fully deployed for work. Make sure that the tools do exactly what you want them to do.

Following Hal Berghel's observations on differentiating computer forensics from network forensics, we are going to split the tools into two. In Sect. 14.4.1, we will discuss tools used mainly in computer forensics, and in Sect. 14.4.2, we will look at those used in network forensics.

Having done that, however, we do not want to look naive as if we do not know that the two disciplines are actually intertwined. Network forensics, for all its knowledge level requirements and tools sharing between the suspects and investigators, is still very much anchored in computer forensics. Many of the tools, as we will see are, therefore, used in both areas without a thought.

In addition, despite the latest call for their separation, which in many areas is still academic, many still treat the two areas as one. In fact, much of the current writing on the market has yet to differentiate the two. However, efforts are on to try and differentiate the two for better services.

14.4.1 Computer Forensic Tools

In Sect. 14.3, we indicated that computer forensics, as an established science, has been in use for some time. As it grow, it developed major tasks that must be performed to complete the job. A forensic tool must have at least one of these functionalities. Many major forensic tools have all of the functionalities below:

- Acquisition—where the main task is making a copy of the original suspect medium with the intention of preserving the integrity of the evidence. Copying can be done in a number of ways including physical, logical, and remote. In doing the acquisition, care must be taken to understand the file formats and also to do a thorough job of preservation and validation.
- Validation and discrimination—these two issues are very important in digital forensics because the case is won or lost based on how well these two were performed. Validation is very important to preserve the integrity and reliability of the evidence. Discrimination is also important because it establishes the relevance of the evidence through search and sort.
- Extraction—is another critical task in forensic investigation because, through it, we recover the evidence which makes up the case. To extract evidence from an evidence medium, one can use any of the following tasks: data viewing, decrypting (when the evidence is found to be encrypted), decompressing (when the evidence was compressed), keyword search, and bookmarking.
- Reconstruction—is a process of recreating what happened during the crime process. It is important to note here that before any reconstruction is made, a copy or two of the original evidence medium must have been made. This reconstruction process requires a few subtasks including disk-to-disk copy, image-to-disk copy, partition-to-partition copy, and image-to-partition copy.
- Reporting—no digital forensic case is done until a final report is written. So this task involves generating a final report.

Forensic tools are either software based or hardware based [5].

14.4.1.1 Software-Based Forensic Tools

Most, if not all, major forensic tools have the capabilities to all these major tasks. Most of the current major tools are software based. Currently, the major commercial forensic tools are (Table 14.1):

- EnCase—by Guidance Software (http://www.guidancesoftware.com/)
- FTK (Forensic Toolkit)—by AccessData (http://accessdata.com/products/computer-forensics/ftk)
- ProDiscover—by ProDiscover Forensics (http://www.techpathways.com/prodiscoverdft.htm)

14.4.1.2 Hardware-Based Forensic Tools

Although most forensic tools are software based, there is an ample supply of hardware-based forensic tools. Hardware tools are based on a workstation that can be stationary, portable, or lightweight. Lightweight workstations are based on laptops. The choice of the type of workstation an investigator uses is determined by the nature of the investigation and the environment of the incident location. There are fully configured turnkey workstations that can be bought, or the investigator can

Table 14.1 Functionalities of major forensic tools

	ProDiscover	FTK	EnCase
Acquisition	√	√	√
Validation and discrimination	√	√	√
Extraction	√	√	√
Reconstruction	√	√	√
Reporting	√	√	√

build his or her own. Hardware-based tools also include write blockers that allow investigators to remove and reconnect a disk drive on a system without having to shut the system down. These tools connect to the computer using FireWire, USB, or SCSI controllers.

14.4.2 Network Forensic Tools

Like in computer forensics, after collecting information as evidence, the next big decision is the analysis tools that are needed to analyze. This job is a lot easier if the system you are investigating was built up by you. Depending on the platform, you can start with *TCPdump* and the *strings* command. TCPdump will display individual packets or filter a few packets out of a large data set, and the string command gives a transcript of the information that passed over the network. Similarly *Snort* allows the investigator to define particular conditions that generate alarms or traps.

However, the job is not so easy if the investigator does not have any knowledge of the system. In this case, he or she is likely to depend on commercial tools. The forensic investigator's ability to analyze will always be limited by the capabilities of the system. Most commercial forensic tools perform continuous network monitoring based on observed data from internal and external sources. Monitoring examines the flow of packets into and out of every port in the network. With this blanket monitoring, it is possible to learn a lot about individual users and what they are doing and with whom. While analysis of individual traffic flows is essential to a complete understanding of network usage, with real-time monitoring on the way, network monitoring is going to require significant amounts of resources. One of the benefits of monitoring is the early warning intelligence-gathering technique sometimes called *recon probes*. A standard forensic tool such as TCPdump can provide the investigator with these probes. The probes can also come from other network monitoring tools such as firewalls and host-based and network-based intrusion detection systems.

Exercises

1. In your opinion, is computer forensics a viable tool in the fight against the cybercrime epidemic?
2. Discuss the difficulties faced by cybercrime investigators.

3. Differentiate between computer and network forensics.
4. Discuss the limitations of computer forensics in the fight against cybercrimes.
5. Many of the difficulties of collecting digital evidence stem from its ability to dry up so fast and the inability of investigators to move fast enough before the evidence disappears. Suggest ways investigators might use to solve this problem.
6. Handling forensic evidence in cybercrime situations must be done very carefully. Discuss the many pitfalls that an investigator must be aware of.
7. One of the methods used in extracting computer forensics evidence is to freeze the computer. While this is considered a good approach by many people, there are those who think it is a shoddy work. Discuss the merits and demerits of computer "freezing."
8. It is so much easier to extract evidence from a computer than from a network. Discuss the difficulties faced by investigators collecting evidence from a network.
9. Encryption can be used both ways: by the criminals to safeguard their data and by the investigators to safeguard their findings. Discuss the difficulties investigators face when dealing with encrypted evidence.
10. Discuss the many ways cybercriminals and other computer and network users may use to frustrate investigators.

Advanced Exercises

1. Hal Berghel meticulously distinguishes between computer forensics and network forensics by giving examples of the so-called "dual usage" network security tools. Study four such tools and demonstrate their "dual usage."
2. Discuss, by giving extensive examples, the claim put forward by Berghel that computer forensics investigators and network forensics investigators have similar levels of skills.
3. It has been stated on many occasions that "reverse hacking" is a good policy for network security. Define "reverse hacking" and discuss the stated opinion.
4. Study the new techniques of digital reconstruction and show how these new techniques are improving the fortunes of both computer and network forensics.
5. Discuss the future of both computer and network forensics in view of the observation that network forensics is but a small science soon to be forgotten.

References

1. Rubin R (1996) More distancing and the use of information: the seven temptations. In: Kizza JM (ed) Social and ethical effects of the computer revolution. McFarland & Company, Jefferson
2. "Intrusion Analysis." SANS. https://www.sans.org/curricula/intrusion-analysis
3. Nelson B, Amelia P, Frank E, Chris S (2004) Guide to computer forensics and investigations. Course Technologies, Boston

4. Berghel H. The discipline of internet forensics. Communications of the ACM, August 2003 46 (8)
5. Kruse W II, Jay GH (2002) Computer forensics: incident response essentials. Addison-Wesley, Reading
6. Sammes T, Brian J (2000) Forensic computing: a practitioner's guide. Springer, London
7. SymWise – Symantec Knowledge Base and MySymantec – Symantec Support. http://www.symantec.com/connect/articles/symwise-symantec-knowledgebase-and-mysymantec-symantec-support
8. Bender W, Gruhl D, Morimoto N, Lu A (1996) Techniques for data hiding. IBM Syst J 35 (3&4)
9. Wikipedia. Computer forensics. https://en.wikipedia.org/wiki/Computer_forensics
10. Pipkin DL (2000) Information security: protecting the global enterprise. Prentice Hall PTR, Upper Saddle River