15
Executive Fraud

The readers of this book will surely be aware of the recent outbreak of corporate fraud and accounting scandals within the executive ranks at major U.S. corporations. Enron, Tyco, AOL Time Warner, WorldCom (and these are real names now) are just the more well-known cases, and not by any means an exhaustive list. Well, we can say with some degree of satisfaction that computer security professionals do at least have a role to play in identifying, proving, and stopping this type of fraud.

This case study details the computer forensic procedures utilized to support a large-scale corporate fraud investigation aimed at many senior executives of an international company who were accused of fraudulently increasing corporate revenues in order to increase profits and subsequently their personal income.

Security professionals specializing in computer forensics and cyber crime investigations were asked to assist with the investigation. Computer forensics is a critical component of many corporate and law enforcement investigations. It is an excellent means of uncovering critical information and tracking the flow of information. However, computer forensic technicians must be knowledgeable in computer operating systems, system hardware, common business applications, and the function and design of hard drives. Because of these requirements, often—especially in larger companies—IT departments are responsible for providing computer forensic support to legal counsel or the internal audit director in support of an investigation.

We should define the term *computer forensics* here to make sure we're all speaking the same language. Computer forensics is most often thought of as involving the creation of a mirror image of a suspect's hard drive (and associated storage devices) and subsequent analysis of its logical file structure, unallocated file space, and file slack. This is a technical description of activities that a computer forensic professional may perform. In a larger sense, and as it is being used in this case study, **computer forensics** is the process of examining digital evidence for use in a criminal or other legal investigation.

15.1 INTRODUCTION: THE WHISTLE-BLOWER

A disgruntled employee at a large international company left a message on the company's fraud hot line indicating that he had information relating to fraudulent activities being conducted by many of the company's senior executives. Within hours the independent third party that managed the fraud hot line had contacted the disgruntled employee and the initial information was being gathered. Soon thereafter, the company's audit committee chairman was briefed on the initial allegation. Such allegations are not taken lightly in any case, but something about this caller and the information presented lent the accusation an extra bit of credibility, so a law firm was retained to conduct a full investigation.

Within 24 hours the law firm had its team of investigators in place. The initial efforts of the investigators were to meet with the disgruntled employee and collect any information relating to the fraud. The information gathered at this meeting suggested a fraud that could easily amount to millions of dollars.

The initial information identified several key executives in the company as potential conspirators in a plot to inflate corporate revenues in order to increase corporate profits and therefore the executives' annual salaries and bonuses. A lawyer representing the law firm hired to conduct the investigation assumed responsibility as the head of the investigation. A larger investigative team—consisting of more than 20 financial auditors, tax accountants, and corporate lawyers, as well as computer forensic professionals—was assembled.

Under the direction of counsel, three objectives were outlined for the investigative team.

1. To ascertain if any fraudulent activity had taken place.
2. To examine e-mails, internal communications, and the computer systems of all parties potentially involved, in an attempt to obtain proof and/or supporting documentation of the alleged fraud.
3. To identify the total financial extent of the alleged fraud—and ascertain how exactly the restatements, which certainly would follow, would be made.

This case study focuses on the second objective. We will operate under the assumption that the investigators determined that some amount of fraudulent activity had taken place. This is not a small assumption, and we make it here simply for brevity and to get to the heart of the case. We do not want to suggest, even in the current environment of corporate scandals, that allegations of fraud are immediately considered truth. Such allegations must be carefully investigated, and they certainly were in this case.

15.2 PREPARATION

The key to a successful computer forensic project is thorough preparation. Not only is preparation necessary for the most effective performance of the tasks at hand, but it is also critical for preserving any and all evidence for potential use in court. If there is even a hint that the evidence has been contaminated in any way, it cannot be used in efforts to prosecute the potentially guilty party.

ASIDE: Though it's not what we want, we will suppress the names of the senior executives involved in this case.

At the outset of the investigation in this case, we attempted to learn as much as possible about the many "suspect" systems to be analyzed, including the following:

- Size of the hard drive(s)
- Type of each hard drive—for example, Integrated Drive Electronics (IDE), Small Computer System Interface (SCSI)

- Operating systems
- Associated storage peripherals—for example, external hard drive(s), CDs, tapes
- Number of system users and their names

ASIDE: With any computer forensic examination you have both a suspect system and an analysis system. The **suspect system** is obviously the one that computer forensic analysis will be conducted *on*. The **analysis system** is the one that will be used to perform the analysis.

We worked with the client's IT assessment management team and obtained an inventory sheet that contained most of the information we needed. As you might imagine, they were very cooperative. Our primary concern was the size of the hard drives because we needed to prepare our analysis systems to ensure that we had the proper amount and type of hard drives for imaging the suspects' drives.

Once we were confident that we had the proper number and types of hard drives, we sanitized them and verified that they were in proper working order. Because we use the same analysis hard drives on multiple engagements, it is important for the drives to be wiped completely clean between engagements. Never should data from one job end up in the files of another job. If there is any doubt about the sanitization process, err on the side of caution and just buy brand-new drives. Actually, buying new drives is fairly common practice because whenever the investigation is being done as part of a criminal or legal action, the hard drive goes into evidence. We don't get these drives back, even after the case is over, because there may be an appeal down the road, for which the original evidence will need to be investigated.

A hard drive can be wiped clean in a variety of ways, such as through the Linux operating system's `DD` function or through commercially available software. The process involves writing a series of characters repeatedly over the entire hard drive and essentially "wiping" it clean of any data from a prior computer forensic analysis. This investigation required us to purchase several brand-new hard drives, but to take no chances, we wiped them clean as well. This added step ensured that no data would exist on our analysis drives until one of our team members placed it on the drive.

To use the Linux `DD` function to wipe a hard drive clean, you can utilize the following command:

```
# > dd if=/dev/urandom of=/dev/hda
```

where `/dev/hda` is the physical address of the analysis drive, and `urandom` is the built-in “random” number generator from Linux. This process should be repeated as many times as you desire. Many professionals sanitize their hard drives as many as three to nine times.

Upon examining the sanitized drive, you should see only a series of random characters throughout. No data should remain on the drive after this process is completed.

15.2.1 THE NATURE AND SOURCE OF THE ALLEGATION

One other essential preparation step was to work with the lead auditors and attorneys to ensure that all of our computer forensic technicians understood the nature and scope of the investigation and the purpose for conducting the computer forensics. Basically, we needed to ensure that everyone understood his or her own role and place within the overall team’s goals.

We approached the task by holding facilitated meetings first thing every morning. Our meetings provided an opportunity for the computer forensic technicians and the financial investigators to share information.

The meetings also provided us the opportunity to collaborate as a team on identifying the type of information we should search for during the computer forensic examination. For this particular project, the financial investigators suggested that Excel spreadsheets, Word documents, PowerPoint presentations, and e-mail correspondence would be the most likely places where evidence of fraud would turn up, as well as being the best indicators of who had taken part in the fraud.

From information gathered at these meetings, we collaborated on developing a list of key search terms that we would use for string searches later in the computer forensic process. The terms we chose were determined by the type of information being sought for use in an accounting fraud case. A lot of the words we came up with are what would be considered typical for a case of accounting fraud; others were specific to the industry, company, and executives involved. When developing a list of search terms, you will almost always include the names of the people being investigated, as well as other pertinent parties, such as customers, vendors, and business partners—that is, the names of any relevant entity. Sample search terms that could be utilized in an accounting fraud case are shown in Table 15.1.

One use for search terms, especially when they are to be used to search through e-mail, is to check whether the suspects have been communicating with each other about the investigation, or the potential for an investigation if they are caught. (Such evidence would prove premeditation, negating the "I didn't know it was against the rules" defense.) This is why the words *investigate* and *investigation* are included in the list of search terms.

One thing we should mention is that we collaborated with the lawyers and accountants on the development of search terms. Certainly we wanted the financial investigators' input on the kinds of evidence to look for specific to their industry. But this is not to suggest that they were controlling the forensic investigation. If there was any doubt about whether a term should be included or not included, we included it. The seriousness of the matter (and, we'd like to think, the professionalism of those involved allowed the situation to remain collaborative and not competitive).

Table 15.1 Possible Search Terms for Accounting-Fraud Cases

allowance	growth	overstatement
audit	incentive	per our discussion
beginning balance	income	prepaid
bonus	in connection	receivable
confirm	internal	repay
deduction	investigate	total
earned	investigation	year-end

15.3 Evidence Collection and Chain of Custody

A critical part of any computer forensic investigation is ensuring proper evidence collection and proper maintenance of the chain of custody of the evidence collected. **Positive control** is the phrase most often used to describe the standard of care taken in the handling of potential evidentiary material (e.g., suspect computer systems, hard drives, and any backup copies). You need to be sure that you can identify the who, what, when, where, how, and why of each piece of evidence or material that you collect during the investigation:

- **Who**. Who handled the evidence?
- **What**. What procedures were performed on the evidence?
- **When**. When was the evidence collected and/or transferred to another party?
- **Where**. Where was the evidence collected and stored?
- **How**. How was the evidence collected and stored?
- **Why**. For what purpose was the evidence collected?

If evidence must change hands multiple times, you may have a very long list of information to keep track of here.

At the beginning of the investigation in this case study we identified approximately 20 systems that required computer forensic analysis. Working with the client's IT department, however, we learned that the computers belonging to the people being investigated had recently been refreshed, and the old computers were still at the client site. That meant that we had to maintain positive control over approximately 40 computer systems.

The auditors on the team had already procured temporary office space near the client location to serve as the headquarters of the investigation. Because the investigative team members came from multiple firms, we needed a convenient space in which to work, and we certainly needed to be close to the client. The office space included a couple of offices that could serve as interview rooms, as well as a large conference room that would be the primary workspace. Before the team moved into that conference room, we had a locksmith install a new lock on the conference room door. (We joked that the owner of the facility might not be too happy that we were changing their locks, but the case warranted such action.) Only three keys to this door were produced, and all of them were marked "Do Not Copy." The keys were given to two of our investigators and the lead attorney. We all agreed to return the keys to the property owner at the end of the engagement.

The lead attorney expressed a lack of confidence in having the team's work papers secured by a simple door lock. The latch on the lock was so exposed that most of the team felt that any determined person could break into the room by simply using a credit card or wire coat hanger to move the latch away from the door frame and open the door. The security team was asked if anything else could be done to secure the room.

To add an extra layer of security, we recommended installing a miniature camera with a radar-based motion detector. The camera recorded to an extended-play VHS recorder and was turned on after hours, on weekends, and whenever any fewer than three team members were in the room. With the camera in place, we could monitor anyone entering, moving within, or leaving the room. We selected the radar-based motion detector because we needed to hide the entire apparatus in the conference room. During the day, many client personnel, including suspects, entered our room as a normal course of business, and we did not want any of them to know that the camera had been installed, so it needed to be out of sight. Further, if someone were to break into our room after hours, it was less likely they would uncover our camera and motion detector than if we had used an infrared-based motion detector that could not be hidden.

With the motion detector in place, the camera would automatically turn on when someone entered the room (and we wouldn't be recording hours and hours of no activity). For an extra level of protection, we added a battery backup to the camera and recorder in case power was cut to the room; our camera would run for an additional 60 hours on this battery (to cover a full weekend). In cases of fraud—especially when the dollar amounts involved start to rise—you don't take chances.

15.3.1 TAKE YOUR HANDS OFF THAT KEYBOARD AND SLOWLY BACK AWAY

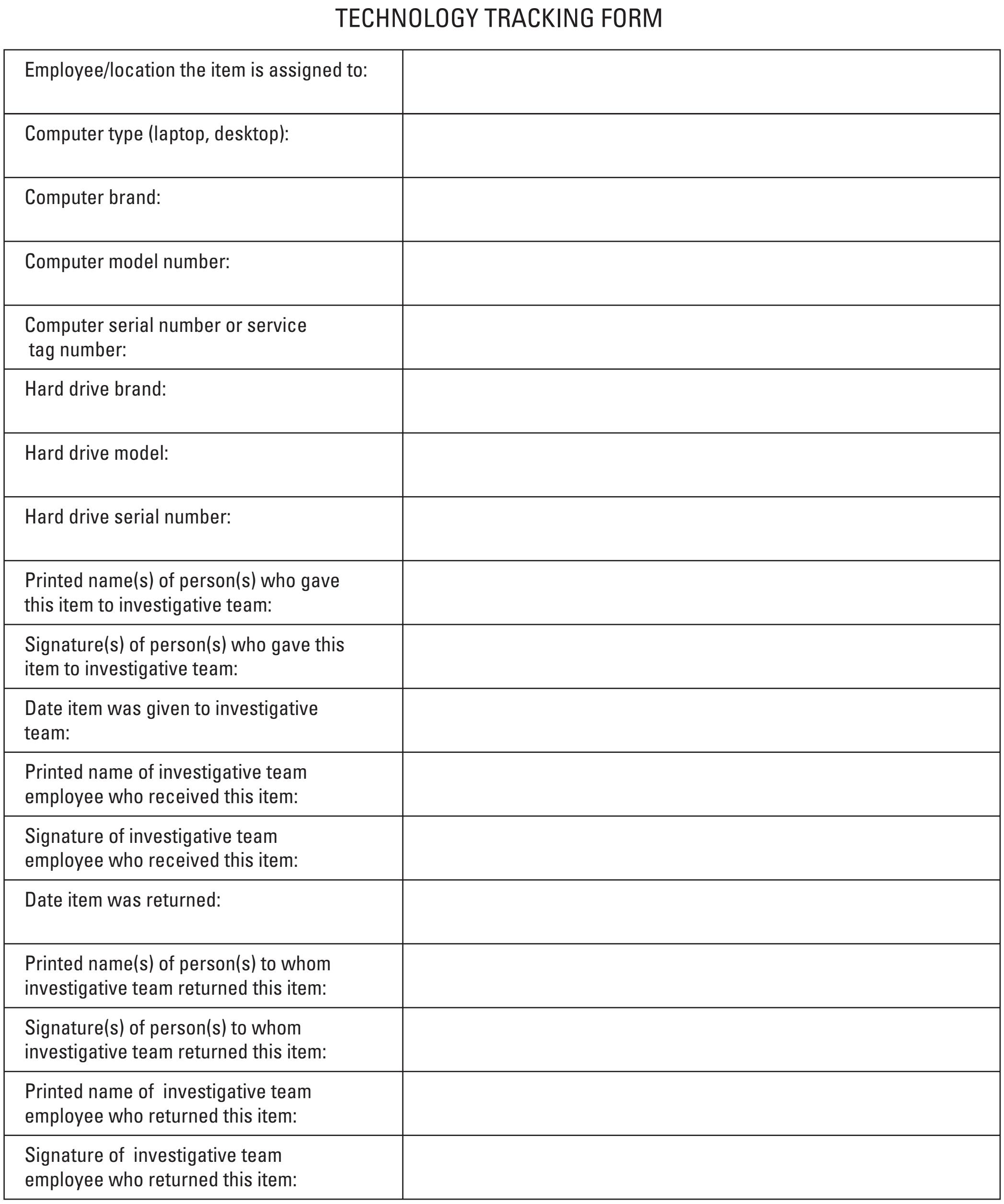
With the room secure, we proceeded to gather the computers and computer paraphernalia from the suspects. Several liaisons from the client's physical security team worked with us during this process. Their assistance proved an effective means of obtaining computer systems from company personnel (employees and executives), because those personnel were not expecting our request and were not prepared to resist the company's own physical security department. The fact that someone from the corporate security team was doing the confiscating made the process of turning over a computer system fairly tolerable. After all, yell all they might, the employees really had no choice. We needed this to be an exceptionally quick process because we wanted to mitigate the risk of anyone deleting pertinent files or e-mail from the systems we wanted to obtain. Therefore, we made the collection all at once, creating teams equal to the number of suspects.

Once the computers and all paraphernalia had been obtained by the liaison, with someone from our team present, we utilized a tracking form (see Figure 15.1) to ensure that we properly documented the chain of custody. Both team members (liaison and forensic investigator) signed our tracking form, as did the suspect. If anyone refused to sign the form, the refusal was noted and a witness (another employee who happened to be in the area) was asked to sign. (When faced with the threat of involving a witness, most suspects quietly signed.) This process was repeated when the computer was returned to the client.

15.4 DRIVE IMAGING

Imaging a suspect's hard drive is one of the most critical functions of the computer forensic process—arguably *the* most critical element. It is extremely important that no data be written to the suspect's hard drive during this process. To ensure the integrity of the 40+ hard drives to be imaged and analyzed in this case, we used the Linux `DD` function as the method for imaging.

Using Linux `DD` means attaching the suspect's hard drive to the analysis system and copying all of its data to a file on the analysis drive. Linux `DD` makes a bit-for-bit copy of the suspect's drive and writes all of the data to what is commonly



TECHNOLOGY TRACKING FORM

Employee/location the item is assigned to:	
Computer type (laptop, desktop):	
Computer brand:	
Computer model number:	
Computer serial number or service tag number:	
Hard drive brand:	
Hard drive model:	
Hard drive serial number:	
Printed name(s) of person(s) who gave this item to investigative team:	
Signature(s) of person(s) who gave this item to investigative team:	
Date item was given to investigative team:	
Printed name of investigative team employee who received this item:	
Signature of investigative team employee who received this item:	
Date item was returned:	
Printed name(s) of person(s) to whom investigative team returned this item:	
Signature(s) of person(s) to whom investigative team returned this item:	
Printed name of investigative team employee who returned this item:	
Signature of investigative team employee who returned this item:	

Figure 15.1 Chain of Custody Tracking Form

referred to as a **raw data file.** This file contains everything that was originally stored on the suspect's drive, including the logical file structure and unallocated space. By using a large hard drive (300GB) for our analysis drive, we were able to store up to five or six suspects' raw data files on a single drive.

Here's the command for using DD:

```
# > dd if=/dev/hda of=/mnt/image.dd
```

where /dev/hda is the physical address of the suspect's hard drive, and /mnt/image.dd is the raw data file to which the suspect's hard drive is being written.

It is imperative to validate that every bit and byte of the suspect's computer was properly copied to your analysis drive. To accomplish this validation, before using DD we used the MD5 checksum utility, called md5sum, that is built into Linux. We first performed a checksum on the suspect's hard drive, then we used DD to make the image, and finally we performed a checksum on the suspect's raw data file. The results of the two checksum operations were compared to make sure that the contents of the suspect's hard drive and our raw data file were identical.

Here's the command for using the Linux MD5 checksum utility:

```
# > md5sum /dev/hda
77538d7cdb02e592e1787f6905235b89 /dev/hda

# > md5sum /mnt/image.dd
77538d7cdb02e592e1787f6905235b89 /mnt/image.dd
```

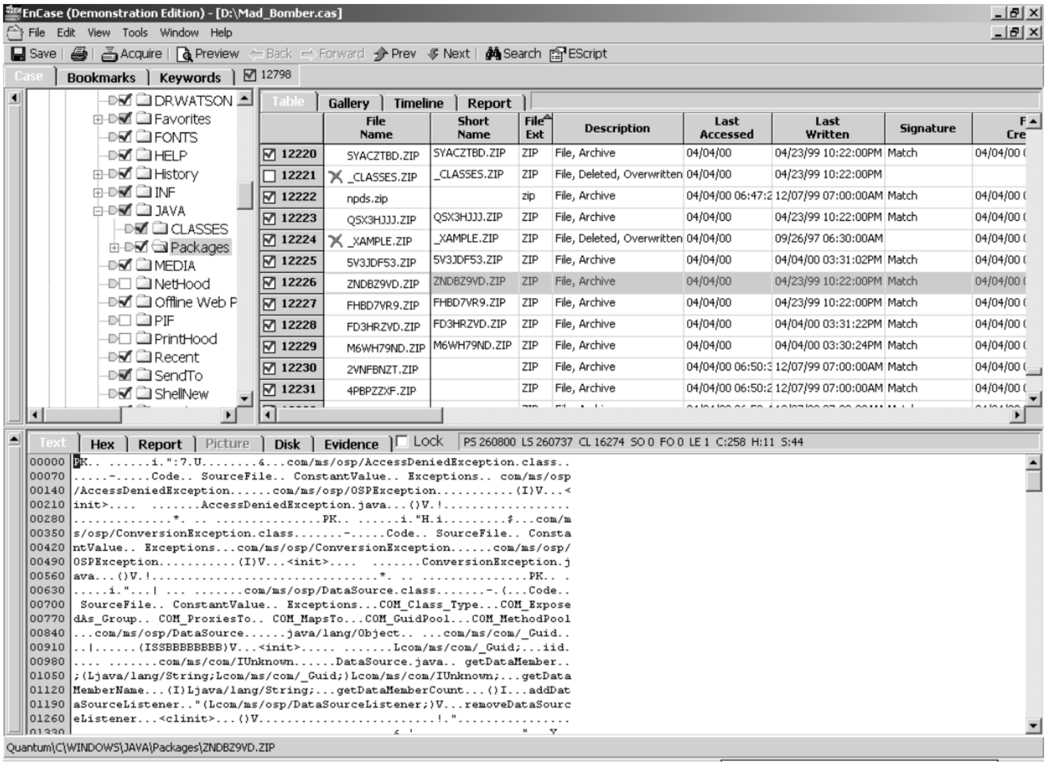
Comparing the results of the two checksum actions will tell you if the DD image copy is exactly the same as the original.

15.5 REVIEW OF THE LOGICAL FILE STRUCTURE

After imaging the suspect hard drives, we reviewed the logical file structure. To facilitate this process, our team used the EnCase Forensic Edition software. This is a licensed software tool. By using our Linux servers, previously used for hard drive imaging, as file servers (utilizing Samba as the mechanism for file sharing), our Windows-based analysis machines could access the raw data files that contained images of our suspects' hard drives.

With EnCase as our tool, we opened each raw data file and began our analysis. EnCase has the built-in technology to read the file and present the data as if it were actually connected to a hard drive. The view that is represented is similar to what an average Windows-based computer user sees when accessing the Windows Explorer utility (see Figure 15.2).

A review of logical file structure involves both automated and manual procedures. The computer forensic software being utilized facilitates the automated procedures. By using EnCase, we were able to search through the directories of


EnCase (Demonstration Edition) - [D:\Mad_Bomber.cas]
File Edit View Tools Window Help
Save Acquire Preview Back Forward Prev Next Search EScript
Case Bookmarks Keywords ☑ 12798
DRWATSON
Favorites
FONTS
HELP
History
INF
JAVA
CLASSES
Packages
MEDIA
NetHood
Offline Web P
PIF
PrintHood
Recent
SendTo
ShellNew
Table Gallery Timeline Report
Text Hex Report Picture Disk Evidence
□ Lock

	File Name	Short Name	File Ext	Description	Last Accessed	Last Written	Signature	F Cre
☑ 12220	SYACZTBD.ZIP	SYACZTBD.ZIP	ZIP	File, Archive	04/04/00	04/23/99 10:22:00PM	Match	04/04/00
□ 12221	_CLASSES.ZIP	_CLASSES.ZIP	ZIP	File, Deleted, Overwritten	04/04/00	04/23/99 10:22:00PM		
☑ 12222	npds.zip		zip	File, Archive	04/04/00 06:47:2	12/07/99 07:00:00AM	Match	04/04/00
☑ 12223	QSX3HJJJ.ZIP	QSX3HJJJ.ZIP	ZIP	File, Archive	04/04/00	04/23/99 10:22:00PM	Match	04/04/00
☑ 12224	_XAMPLE.ZIP	_XAMPLE.ZIP	ZIP	File, Deleted, Overwritten	04/04/00	09/26/97 06:30:00AM		04/04/00
☑ 12225	5V3JDF53.ZIP	5V3JDF53.ZIP	ZIP	File, Archive	04/04/00	04/04/00 03:31:02PM	Match	04/04/00
☑ 12226	ZNDBZ9VD.ZIP	ZNDBZ9VD.ZIP	ZIP	File, Archive	04/04/00	04/23/99 10:22:00PM	Match	04/04/00
☑ 12227	FHBD7VR9.ZIP	FHBD7VR9.ZIP	ZIP	File, Archive	04/04/00	04/23/99 10:22:00PM	Match	04/04/00
☑ 12228	FD3HRZVD.ZIP	FD3HRZVD.ZIP	ZIP	File, Archive	04/04/00	04/04/00 03:31:22PM	Match	04/04/00
☑ 12229	M6WH79ND.ZIP	M6WH79ND.ZIP	ZIP	File, Archive	04/04/00	04/04/00 03:30:24PM	Match	04/04/00
☑ 12230	2VNFBNZT.ZIP		ZIP	File, Archive	04/04/00 06:50:3	12/07/99 07:00:00AM	Match	04/04/00
☑ 12231	4PBPZZXF.ZIP		ZIP	File, Archive	04/04/00 06:50:2	12/07/99 07:00:00AM	Match	04/04/00

PS 260800 LS 260737 CL 16274 SO 0 FO 0 LE 1 C:258 H:11 S:44

```
00000 PK.. ......i.":7.U........&...com/ms/osp/AccessDeniedException.class..
00070 .....-.....Code.. SourceFile.. ConstantValue.. Exceptions.. com/ms/osp
00140 /AccessDeniedException......com/ms/osp/OSPException...........(I)V...<
00210 init>....  .......AccessDeniedException.java...()V.!..................
00280 ..............*. .. ................PK.. ......i."H.i.........$...com/m
00350 s/osp/ConversionException.class.......-.....Code.. SourceFile.. Consta
00420 ntValue.. Exceptions...com/ms/osp/ConversionException......com/ms/osp/
00490 OSPException...........(I)V...<init>....  .......ConversionException.j
00560 ava...()V.!...............................*. .. ...............PK.. .
00630 .....i."...| ... .......com/ms/osp/DataSource.class.......-.(...Code..
00700  SourceFile.. ConstantValue.. Exceptions...COM_Class_Type...COM_Expose
00770 dAs_Group.. COM_ProxiesTo.. COM_MapsTo...COM_GuidPool...COM_MethodPool
00840 ...com/ms/osp/DataSource......java/lang/Object.. ...com/ms/com/_Guid..
00910 ..|......(ISSBBBBBBBB)V...<init>..... .......Lcom/ms/com/_Guid;...iid.
00980 .... .......com/ms/com/IUnknown......DataSource.java.. getDataMember..
01050 ;(Ljava/lang/String;Lcom/ms/com/_Guid;)Lcom/ms/com/IUnknown;...getData
01120 MemberName...(I)Ljava/lang/String;...getDataMemberCount...()I...addDat
01190 aSourceListener.."(Lcom/ms/osp/DataSourceListener;)V...removeDataSourc
01260 eListener...<clinit>...()V.........................!."................
```

Quantum\C\WINDOWS\JAVA\Packages\ZNDBZ9VD.ZIP

Figure 15.2 EnCase Logical File Structure Review

the suspect's computer system and quickly locate any files that seemed pertinent to our investigation. As a follow-up method, we looked through the directories manually to identify any files that might not have been detected during our automated search with EnCase.

Each file we located that was deemed pertinent to our investigation was copied to the analysis drive, to be included in our computer forensic analysis report. When performing this step it is important to record the logical address of the file. This is the full path name; for example, the full path name of the `System32` directory on many Windows NT/2K/XP computers is `C:\Winnt\System32`.

15.6 REVIEW OF UNALLOCATED SPACE AND FILE SLACK

After completing the logical file structure review, we focused on analyzing the unallocated space and file slack. **Unallocated space**, also called *free space*, is defined as the unused portion of the hard drive; **file slack** is the unused space that is created between the end-of-file marker and the end of the hard drive cluster in which the file is stored. Sometimes data is written to these spaces that may be of value to investigators.

Using a software tool to facilitate the process is the easiest way to accomplish this portion of the analysis. As we had earlier, we used EnCase for this segment of the review. Our approach was twofold: (1) We extracted deleted files out of the unallocated space and subsequently reviewed them for appropriateness, and (2) we performed string searches through the unallocated space and file slack in an attempt to locate data related to the matter being investigated.

Even with the assistance of software tools, this process can be very time-consuming and potentially lengthy. The results of the extraction of deleted files can be voluminous. In this case several thousand files from each hard drive needed to be reviewed.

In addition, all of the identified files must be reviewed. We can't simply review until we find material that we're looking for, or material that helps our case, and stop. That would an unfair and incomplete evaluation of the potential evidence. Therefore, to expedite the process of reviewing files extracted from unallocated space, we use a software utility called dtSearch. With all of our extracted files in one location, we fed our search terms into dtSearch and had it scan through the files to find those that were pertinent to our investigation.

As in logical file structure review, when potential evidence is found, its address on the hard drive must be recorded. However, because unallocated space and file slack are outside of the logical addressing scheme in this review, we must record the physical address of any evidence, essentially including its cluster and sector address (e.g., cluster 11155, sector 357517).

15.7 SMOKING GUN

Although everyone on the investigative team wanted to find a smoking gun, such as an e-mail from a senior executive saying, "I'm going to lie about the numbers to increase my yearly bonus—the SEC be damned," no such e-mail was found. In addition, no single financial report, PowerPoint presentation, or word document clearly indicated that any individual was a party to fraud or that any fraud had indeed taken place.

Instead, the investigation was an iterative process in which we discovered information piece by piece—draft financial reports, reports marked confidential, e-mails between suspects—and shared it with the accountants to review. Each time we gave them some such material, they reviewed it and suggested that we look for more of the same.

Sometimes the accountants came to us with leads. For example, they might ask us to do a search on the name of an off-shore corporation to see what might turn up. In some cases, a great deal of relevant data was discovered; in other cases, nothing came up. In this back-and-forth process, the case for fraud was built.

15.8 REPORTING

When our analysis was complete, we began to draft a report. This is another critical step in the computer forensic process, and we wanted to make sure we got it right.

We met with the lead investigators and attorneys and provided them verbal reports of the results of our analysis, as well as our working papers. We had been working together, so they were aware of the findings for the most part, but a presentation still had to be made to ensure that there were no misunderstandings. In addition, though we had a report format (template) that we were comfortable with, we needed to know how the report should be labeled (e.g., confidential, sensitive, privileged, attorney/client privileged). This is an important consideration, that, in general, is best left to the lawyers.

We agreed to develop our report using Microsoft Word and to include links to pertinent files that would be stored on an accompanying CD-ROM. All the attorney would need to do is insert the CD in a computer, and the report would automatically open for viewing. The attorney could then easily review the report and choose to open any associated files she wished to view.

The report, as well as all data and work papers, would be on the CD-ROM. The written report could certainly be printed in hard copy; the sheer volume of the data, however, made hard copies of the data completely impossible.

15.9 LESSONS LEARNED

Although no smoking gun was found in this investigation, enough evidence was discovered (e.g., key electronic documents, e-mail, spreadsheets, PowerPoint presentations) that, when put together, identified how key executives had committed the fraud and had communicated about their activities. In this particular case, however, all of the information that we uncovered with computer forensics would have to fall into the category of circumstantial evidence. All of it was critical to allowing our team to complete the investigation. However, none of it contained the smoking gun that our computer forensic technicians were hoping for. Fortunately for the investigative team (and the company involved), a whistleblower and other company employees were willing to talk with the investigating team and provide information that was helpful in uncovering the details of the fraud.

For the sake of fairness, it must be stated that the investigation did exonerate certain of the suspects. And this is a major part of the role of computer forensic professionals. We are charged not only with presenting evidence that an incident did in fact occur, but also with presenting evidence suggesting that the incident did *not* occur, if that is indeed the case.

After the investigation was completed, the lead attorneys from the investigative team provided the complete report to the audit committee. The report outlined specifically which company employees—mainly executives—were involved in the fraud, without attempting to evaluate their culpability. (Lawyers have more leeway in assessing guilt than we do.) The report also contained information about internal control deficiencies that permitted the fraud to occur and ways to mitigate the risk of this type of fraud in the future.

The audit committee took swift and decisive action, firing all of the executives that were involved in the fraud and recommending significant changes to the company's internal financial reporting and control environment.