Forensic Examination Report

By Justin McAnn **07/01/09**

All facts and statements contained within this Report are within my personal knowledge. If called as a witness at trial, I could testify to all matters referred to in this Report.

Narrative

I am a digital forensic examiner and I examined several of the computer data storage devices owned by Northwest Direct Teleservices ("NDT"). I have had extensive training in computer forensic examinations as well as advanced training in forensic examinations involving hacking and malware incidents. I am a certified security professional with over 12 years of experience working on computers and networks including administration, intrusions and forensic examination on hundreds of systems. My experience includes corporate forensic investigations, forensic examination consulting and electronic discovery services.

I received a copy of the Protective Order and I understand there are allegations between both the Claimant and Respondent where artifacts around the termination of Zwiezig are being disputed as well as the possible acts of pornography and the destruction of data on the data storage devices. I have been asked to conduct a forensic examination of various NDT data storage devices and other media to determine, based on the physical evidence, whether such allegations did or did not occur.

On December 12th, 2008 I arrived at the NDT Lawyer's office in Portland with the understanding based on the Stipulation Order that I would be creating forensic images of three data storage devices and a floppy disk. As I entered the office I was presented with a Dell Laptop, a Sony Workstation, a Green 2.5" Floppy Disk and a small box which I was told contained the third data storage device. I began by creating a bit stream image (forensic copy) of the data storage device (SN# ~13P-5RM0) from within the Dell Laptop. The data storage device was connected to a forensic system by means of a hardware write blocker to prevent any data changes to the original hard drive. After connected, the forensic image was created using software (AccessData FTK) which has been validated and verified forensically sound. When the data storage device was activated I noticed it produced a loud high pitched whine as it operated indicating the data storage device was severely worn and possibly damaged. The

Arb Ex 103
Page 1

forensic software had a difficult time taking a forensic copy of the data storage device and reported that there was damage to various "sectors" on the device which means some data would not be readable or recoverable, essentially destroyed. This is usually due to improper care and treatment of the data storage device over time. It doesn't completely stop a forensic copy from being taken so I completed the image of the data storage device and took a second image just in case it may be able to read more of the bad "sectors".

I proceeded to utilize the same forensic procedures of capturing a forensically sound copy of the second data storage device (SN# Y2VELLLE) from the Sony Workstation which finished successfully without issues. I continued on to the Green Floppy Disk. Floppy Disks have a built in switch on the back side of the disk which enables the disk to become Read-Only so no original data can be changed. A Forensic Copy was taken of the Green Floppy Disk successfully.

Finally, I opened the small box that was to contain the third data storage device however inside the small box was a CD-ROM Drive and not a hard drive. I consulted with NDT's Lawyers who were unable to find the final data storage device and thought it was misplaced.

On March 20th, 2009 I returned to the offices of the NDT Lawyer's in order to make a forensic image of the final missing data storage device. The original physical device was still not present and I was presented with a hard drive that supposedly contained a forensic image their forensic expert created of the final data storage device when it was in his possession. This is typically not the correct forensic procedure, utilizing a forensic image created by a third party without knowledge of their skill and physically over viewing the process. It was indicated to me that the original device was still not able to be found and this was the next best option for the evidence. I re-imaged their image of the final data storage device utilizing a write-blocker the same as if this was the original protecting the integrity of the image.

Findings

My analysis methodology begins by reviewing the termination letter (Exhibit #1:PG 2) found on the Green Floppy Disk for information about the creation, modification, storage and transfer of this termination letter named "max term.doc". My methodology is executed by identifying the information and then using that information to apply a timeline and search criteria for the document on the laptop data storage device which was originally introduced as the system the letter was created on.

Arb Ex 103
Page _____

Analyzing the termination letter on the Floppy Disk discovered file system and Microsoft Word metadata (Exhibit #1: PG 1) that indicates the document was written and saved on 10/1/03 at 9:29AM by an author named "Northwest Direct Employee". It was then transferred from a computer system it was created on to this Floppy Disk on 10/1/03 at 3:48PM.

Next I search for any artifacts of the letter. The keyword search utilized words and phrases from the termination letter content along with metadata and searches across every byte of data on the laptop storage device. When the search completed it found no search hits on the laptop data storage device. This is unusual as the amount of data written when simply creating a word document is abundant throughout the data storage device file system and registry, which is a database that stores configuration information and user activity. Unfortunately this laptop data storage device is small in size, only 10 gigabytes, and has been in use since the termination of Zweizig through 11/12/08. With five years of use after the fact nearly any artifacts that once existed would have easily been destroyed and overwritten.

No search results indicate the data has been destroyed or never existed on this laptop. I referred to the Registry above as a database which stores configuration information and user activity. The Registry stores a lot of the metadata such as author, initials and company of anyone who utilizes the Microsoft Word product. This data is embedded within the document when it is saved to the data storage device. In this case the Termination Letter contained the author as "Northwest Direct Employee" and the company as "Northwest Direct". Forensically I am able to open up the Registry on the laptop data storage device and compare the metadata to see if it matches. The analysis found that the author on this laptop under Tim Rote's account is "rotet" and the company is configured as "NWD" (Exhibit #4). This is supporting evidence that the Termination Document was not likely created on this laptop.

Further supporting evidence exists in the metadata of the Termination Letter on the Floppy Disk. According to Tim Rote's deposition (PG:92;10-16) he only saved the letter on the Floppy Disk however embedded within the Termination Letter the metadata includes the directory and filename of the letter on the data storage device where the document was created. In this case it was located at these locations:

C:\Documents and Settings\Owner\My Documents\Doc1.doc

C:\Documents and Settings\Owner\Application Data\Microsoft\Word\AutoRecovery save of Doc1.asd

This can occur even without the knowledge of the user writing the document as it is part of an automatic "Save" feature built into Microsoft Word. At set intervals it saves your document for the author so in case Microsoft Word or your computer happens to fail or "crash" it is able to recover the document you were working on, even if you didn't save it. The laptop data storage device did NOT contain an "Owner" profile as you see in the locations above again supporting the probability this document was created on an entirely different computer.

Without the correct computer system that created the Termination Letter there is no way to forensically corroborate the dates on the document to be truly accurate especially since producing false dates and times is as simple as changing the clock on your computer which could also be proven if the correct data storage device were forensically examined.

I continued on with my analysis and placed my focus on the presence, origin and background of accessing pornography on the Sony Workstation data storage device and the 120 gigabyte final data storage device. The methodology utilized to determine this is to first locate all pictures, active or deleted, and review them in a gallery type format. While performing this analysis very few pornographic pictures were discovered. Only one picture (Exhibit #2) existed within the relevant time frame Max Zweizig worked for NDT. This picture was located in the following directory and filename:

C:\Documents and Settings\NWT Employee\My Documents\My Pictures\c8.jpg

The picture exists under a profile named "NWT Employee". According to NDT's Forensic Expert's report at the time he performed his analysis the account was associated to JCioffi. My forensic analysis discovered the name associated with this account has since been removed. This data storage device has been in use since it was turned over by Zweizig and this is just one example of the data that has changed thereby destroying information that could be evidence for use in my examination. Without a name associated with the account there are no facts or proof that Zweizig was the owner of the NWT Employee account or of the picture. The user account NWT Employee has also since been deleted after Zweizig turned over the Sony Workstation. Additionally the account was deleted after NDT's Forensic Expert performed his forensic examination, which destroyed additional evidence about the account for my forensic examination to be able to analyze.

Whenever a picture is opened using the Microsoft Windows XP operating system a recording is made and stored within the profile of the user account that opened the picture. In this case the picture was accessed twice by the account "JCioffi" on 12/21/04 and 7/13/08 (Exhibit #3). That is two more times than the NWT Employee account has been recorded accessing the picture. There were no other links found on the data storage device that would be a shortcut to that file for others to click on.

Destruction

The final stipulation to examine is the alleged use of destructive computer programs that may have destroyed or tampered with NDT material. This examination analyzes the Sony Workstation data storage device and 120 gigabyte data storage devices again. The current forensic technologies allow examiners to see data that has been deleted just as if it hadn't been deleted. The methodology is to utilize that capability to identify any destructive applications such as file wiping utilities and evidence erasers. It also allows us to see very quickly if any files claimed to not exist are really there and easily recoverable.

As an experienced forensic examiner who specializes in incidents such as hacking and malware I am able to compare all files to a list of data destruction applications and quickly assess the presence of them on a data storage device. These two data storage devices contained no such applications with the exception of PGP. PGP stands for Pretty Good Privacy and is intended for encrypting sensitive documents. It is not considered a data destruction application however it does have the ability to wipe files. Since it is not a malicious tool, whenever someone utilizes PGP to wipe a file it leaves a very specific signature and artifacts behind. It will change the filename or directory that is wiped to a long string of repeating letters such as a file name "aaaaaaaaaaaaaaaaaaa". I examined the machine for any artifacts such as this and none existed.

Next I examined the data storage devices for the simple use and deletion of FoxPro files. The Sony Workstation only contained FoxPro files used from 12/01/03 which was after Zweizig had turned over the system to Tim Rote. This includes all deleted files so any deleted FoxPro files would not have been deleted by Zweizig.

The 120 gigabyte data storage device didn't contain any files visible to the typical user however forensic capabilities are able to see the hidden files in seconds. This data storage device contained two empty partitions which is an indication that the drive was "formatted" or deleted. According to the dates and timestamps on the partitions one partition was formatted on 11/12/03 at 11:26AM PST and the other on the same day at 12:31PM PST. Similar to the

Floppy Disk time stamps the dates and times associated with the formatting of the drive are directly related to the computer it was connected to at the time. Without knowing or having the computer to forensically examine, it is impossible to prove if the dates and times are accurate and true or if the clock was changed which impacted the recorded times.

The drive was not utilized after that point which means nearly none of the data that was on the drive prior to the formatting of the drive was destroyed. It simply wasn't able to be seen. I was able to see over 1900 FoxPro files and any data recovery or forensics application can quickly make them visible again with minimal effort.

Conclusion

Throughout the examination I have discovered many generalities without proof or fact based evidence. There are dates and times on the Termination Letter from a Floppy Disk but no proof from the laptop data storage device that supports the creation of that document at that time on that system. It is highly probable it wasn't created on the laptop data storage device provided but also possible that any evidence which could prove those dates are false has been destroyed as a result of utilizing the laptop for over five years since the Termination Letter was supposedly created.

There was one single pornographic picture that has a date and time stamp within the year 2003. The picture was underneath the profile of a generic user account indicating that there was no accountability as to who the owner was of that picture. Instead the only evidence we have is another non-generic account assigned to a JCioffi who accessed that pornographic picture twice while it never appeared to be accessed by the generic account, NWT Employee.

There was no data destruction application that impacted either of the two workstation data storage devices. The FoxPro application associated files hadn't been used in 2003 on the Sony Workstation after the initial 120 gigabyte data storage device failed. The only usage occurred after the return of the equipment from Zweizig. The 120 gigabyte data storage device failed according to both Rote and Zweizig's testimony in 5/03 which accurately aligns with the file dates and times on the data storage device visible to forensic examination technologies. From the data that is easily accessible on the 120 gigabyte data storage device it should not have taken any effort to do a recovery, no matter if the drive failed, was formatted or simply deleted.

why would there be any usage.

last talking about 120

In conclusion there aren't any hard facts, the basis of computer forensics, that can place any specific person at the keyboard WHEN and where they may have wrote a document,

viewed a picture or formatted a data storage device. I have provided hard facts that demonstrate the destruction of data on the data storage devices based on their usage over the past five years. This data destruction severely impacts my forensic examination in order to prove or disprove allegations. I also prove that it is highly probable the Termination Letter was not written on the laptop data storage device provided to me by NDT. Without the correct data storage device to forensically examine, the date and time of the document cannot be confirmed. We are left with a lack of evidence that could severely help or hinder this case.

Exhibit #1

Max term.doc

Metadata Page 1

File Created	10/01/03 03:48:00PM
Last Written	10/01/03 03:48:38PM
Logical Size	21,504
File Extents	1
References	0
Physical Location	16,896
Physical Sector	33
Evidence File	FloppyDisk
File Identifier	27
Code Page	0
Full Path	FloppyDisk\Max term.doc
Author	Northwest Direct Employee
LastAuthor	Northwest Direct Employee
Created	10/1/2003 9:29:00 AM
Last Saved	10/1/2003 9:29:00 AM

Arb Ex 103
Page 8

10/1/03

Mr. Max Zweizig
140 Ford Avenue
Woodbury, New Jersey 08096

Dear Max:

After the difficulties of the vacation, the failure to meet our clients expectations on dispositions (Allstate), the length I have to go just to get you to turn in time reports, the failures with Discover Card, your refusal to train personnel on the processing tasks, all against a back drop of being at 50% capacity as compared to our gross sales volume only one year ago, it is imperative that we both look for different alternatives. We are terminating our contract with you and this is notice pursuant to section 3 of the contract.

Considering your two-year tenure with the company, I want to allow you to stay on through November 15, 2003, providing that you immediately train Gunawan on the processing required for all of our clients and transfer all software applications you have developed while in our employe by 10/31/03. Said applications, all database files, all records, etc. need to be transferred to our Eugene facility by 10/31/03.

Ultimately Max, I believe the remote employee executive position I have allowed to date are not working out as productively as I expect they should be. You should pursue other employment and you have my endorsement and offer of a letter of recommendation, providing you meet the October 31, 2003 deadline in the previous paragraph.

Very truly yours,

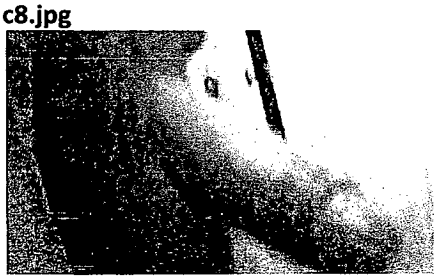
Timothy C. Rote

Arb Ex 103
Page 9

Exhibit #2

Name	File Created	Last Written	Logical Size	Full Path
c8.jpg	09/30/03 11:09:03AM	09/30/03 11:06:57AM	34,137	60GB VAIO\C:\Documents and Settings\NWT Employee\My Documents\My Pictures\c8.jpg

c8.jpg



Arb Ex 103
Page 10

Exhibit #3

LNK Files – Link or "Shortcut" file is a small file containing a target path to a file that the shortcut represents.

Recent – Recently accessed files

File Name	Last Accessed	File Created	Full Computer File Path
c8.jpg.lnk	12/21/04 03:39:28PM	12/21/04 03:39:28PM	60GB VAIO\C:\Documents and Settings\jcioffi\Recent\c8.jpg.lnk
c8.jpg.lnk	07/13/08 11:55:42AM	07/13/08 11:55:42AM	60GB VAIO\C:\Documents and Settings\jcioffi.NWT-1\Recent\ c8.jpg.lnk

Arb Ex 103
Page 11

Exhibit #4

Registry Key Locations and Registry Key Properties are in BOLD.

Name	**UserInitials**
File Type	BINARY
Description	File, Registry Entry
Logical Size	4
Initialized Size	4
Physical Size	4
Starting Extent	18NTRegistry-B639620
File Extents	1
References	0
Physical Location	639,620
Physical Sector	1,249
Evidence File	IBM Travelstar 10GB HDD (SN: HU-031YMK-47710-13P-5RM0) from Dell Inspiron 4000 (ST:6X6DJ01)
File Full Path	10GB Inspiron\C:\System Volume Information_restore{583ADD5F-1BFC-4EDE-B564-A2DBC1FB75DA}\RP1247\snapshot_REGISTRY_USER_NTUSER_S-1-5-21-2957982530-685884836-793787355-1137
Registry Key	**HKEY_Current_User\Software\Microsoft\Office\9.0\Common\UserInfo\UserInitials**

Registry Key Property

VALUE	F

Name	**UserName**
File Type	BINARY
Description	File, Registry Entry
Logical Size	12
Initialized Size	12
Physical Size	12
Starting Extent	18NTRegistry-B644340
File Extents	1
References	0
Physical Location	644,340
Physical Sector	1,258
Evidence File	IBM Travelstar 10GB HDD (SN: HU-031YMK-47710-13P-5RM0) from Dell Inspiron 4000 (ST:6X6DJ01)
File Identifier	3
Code Page	0
Full Path	NDT v Zweizig\IBM Travelstar 10GB HDD (SN: HU-031YMK-47710-13P-5RM0) from Dell Inspiron 4000 (ST:6X6DJ01)\C\System Volume Information_restore{583ADD5F-1BFC-4EDE-B564-A2DBC1FB75DA}\RP1247\snapshot_REGISTRY_USER_NTUSER_S-1-5-21-2957982530-685884836-793787355-1137
Registry Key	**HKEY_Current_User\Software\Microsoft\Office\9.0\Common\UserInfo\UserName**

Registry Key Property

VALUE	rotet

Arb Ex 103
Page 12

Name	**Company**
File Type	BINARY
Description	File, Registry Entry
Logical Size	8
Initialized Size	8
Physical Size	8
Starting Extent	18NTRegistry-B670100
File Extents	1
References	0
Physical Location	670,100
Physical Sector	1,308
Evidence File	IBM Travelstar 10GB HDD (SN: HU-031YMK-47710-13P-5RM0) from Dell Inspiron 4000 (ST:6X6DJ01)
Full Path	NDT v Zweizig\IBM Travelstar 10GB HDD (SN: HU-031YMK-47710-13P-5RM0) from Dell Inspiron 4000 (ST:6X6DJ01)\C\System Volume Information_restore{583ADD5F-1BFC-4EDE-B564-A2DBC1FB75DA}\RP1247\snapshot_REGISTRY_USER_NTUSER_S-1-5-21-2957982530-685884836-793787355-1137
Registry Key	**HKEY_Current_User\Software\Microsoft\Office\9.0\Common\UserInfo\Company**

Registry Key Property

VALUE	NWD

Arb Ex 103
Page 13