

Digital Recovery Systems
Computer Examination Report
FINAL REPORT

ISSUE

The issue involved an email titled "Exit Time" sent by Timothy Rote, owner of Northwest Direct Teleservices, to Max Zweifel on October 2, 2003, from Mr. Rote's laptop computer. At issue also is a Microsoft Word document titled "Max term.doc" created on Mr. Rote's computer on October 1, 2003.

QUALIFICATIONS

I am a certified forensic computer examiner through the International Association of Computer Investigative Specialists (IACIS), with more than 440 hours of specialized training in the acquisition and analysis of computer evidence. That training was obtained through IACIS, the National White Collar Crime Center, AccessData Corporation, Guidance Software Inc., the Federal Bureau of Investigation and the Defense Computer Investigations Training Program.

ITEMS EXAMINED

- (1) Dell Inspiron 4000 laptop computer, model PP01L
Serial no. TW-0791UH-12800-141-5345
Containing IBM Travelstar hard drive, model DJSA-210
Serial no. HU-031YMK-47710-13P-5RM0

- (1) Unmarked green floppy diskette, Radio Shack brand
Double-sided, High-density MFD-2HD

ACQUISITION PROCESS

On June 3, 2005, I physically examined Mr. Rote's Dell laptop and found it to be of standard configuration with no unusual components. The laptop itself was mounted in a docking station with connections to a monitor, keyboard, mouse, printer and network cable for Internet access. At the time I examined it, the date and time settings on this computer were consistent with current Pacific Standard Time.

I removed the IBM Travelstar hard drive from the case and attached it to my forensic computer with a FireFly write-blocking device manufactured by Digital Intelligence Inc. I have personally tested this device and it does not allow any data to be written to the drive to which it is attached.

Digital Recovery Systems
Computer Examination Report
FINAL REPORT

I used the forensic program *EnCase* (version 3.22g) for the actual acquisition process. This program makes a bitstream image of all data on the hard drive, authenticated with CRC and HASH values. I stored the bitstream image on a separate hard drive that I had previously wiped of any residual data with the *EnCase* wipe drive function. I performed all further analysis on the image copy using the *Forensic Tool Kit (FTK)* software program by *AccessData*. I have received training in the use of both *EnCase* and *FTK*, and both are licensed in my name for my use.

I write-protected the unmarked green floppy diskette by sliding the write-protect switch on the diskette itself. This prevents any data from being written to the diskette during acquisition. Using the same method as noted above, I created a bitstream image of the entire diskette.

ANALYSIS

The email in question (Subject: "Exit Time") was stored in a Microsoft Outlook folder. The date on the email was shown as 10/2/03 at 11:46am. This is the date and time that would have been visible to sender and recipient when sending and receiving the message. Email programs like *Outlook* also create "header" data before a message is actually sent from the user's computer to their Internet Service Provider (ISP), where additional headers are added after it leaves the user's computer. This header data includes dates and times of message creation.

The header information attached to this email by the *Outlook* program lists dates and time for *Creation*, *Delivery*, *Submit* and *Modification*. The following dates and times were noted:

Creation	10/2/2003	11:44am
Delivery	10/2/2003	11:46am
Submit	10/2/2003	11:56am
Modification	4/29/2005	6:00pm

Regarding the Modification time and date, I asked Mr. Rote by telephone on June 9, 2005, if he had performed any action with this email recently. He told me that in April 2005 he had been cleaning up his Outlook folders and moved this particular saved email to a specific folder for storage purposes. This would account for the 2005 date. (see Attachment #1)

The Microsoft Word document (*Max term.doc*) was created and saved to the unmarked green floppy diskette. Within the text of the document is the date 10/1/03, which would have been typed by Mr. Rote when creating the document.

Digital Recovery Systems
Computer Examination Report
FINAL REPORT

Dates and times associated with the document file entry are as follows:

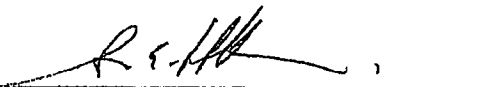
Create Date	10/1/2003	9:29am
Modification Date	10/1/2003	9:29am
Last Access Date	10/1/2003	

I examined the *metadata* within the document itself. *Metadata* is information about a particular file which is stored within the file's data itself by the program used to create the file. I found three instances in the document's data where the date **10/1/2003** existed. This was consistent with the other associated dates listed above. (See Attachment #2, 3 and 4)

CONCLUSIONS

Based on my examination of the email in question, it does appear that the "Exit Time" email message was created on and transmitted from this computer on October 2, 2003, with a copy of the message saved on Mr. Rote's computer, and subsequently moved to a storage folder on April 29, 2005.

Based on my examination of the Microsoft Word document "Max term.doc" the date and time evidence associated both with the file directory entry and the metadata within the file itself, it does appear that the document was created and saved on this floppy diskette on October 1, 2003.



Steven E. Williams CFCE
Digital Recovery Systems
3891 Kevington Ave.
Eugene OR 97405
(541) 968-2103

ATTACHMENT 01

AccessData FTK version 1.42 build 03 - 2.05 - F:\NWD 060505 Tim Rote Laptop and Floppy\FTK Workup\NWD\Diget1

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Bookmarks

- Email: 10/2/2003 email to Max Zwing
- Word Document:

Bookmark Name: Email
Bookmark Comment: 10/2/2003 email to Max Zwing

Bookmarked Files: 1

File Name	File Path
Message007	DELL InspironPart_1\WONAME-N...

Remember the position/selection

Include in Report Export Files

Subject: Exit Time

From: Timothy C. Rote

Date: 10/2/2003 11:46:00 AM

To: Max Zwing

Message Body

I don't think you are going to train the staff and transfer programs as requested, allowing us a full transition. Accordingly, we need to set your exit time for the middle of November. I'll be sending you a letter.

Outlook Header Information

Conversation Topic: Exit Time
 Subject: Exit Time
 From: Timothy C. Rote
 Sender Name: Timothy C. Rote
 To: Max Zwing
 Delivery Time: 10/2/2003 11:46:00 AM
 Creation Time: 10/2/2003 11:44:14 AM
 Modification Time: 4/29/2005 6:00:21 PM
 Submit Time: 10/2/2003 11:58:34 AM

1 Listed 0 Checked Total [DELL InspironPart_1\WONAME-N\F5 Document... Outlook.pst > Personal Folders > Top of Personal Folders > Inbox > Mail > Message007]

ATTACHMENT 03

AccessData FTK version 1.42 build 03.12.05 F:\NWD 060505 Tim Rote Laptop and Floppy\FTK Workup\NW Direct\

File Edit View Tools Help

Overview Explorer Graphics E-Mail Search Bookmark

Case

- DELL Inspiron
 - Part 1
 - NONAME-NTFS
 - UnpartSpace
 - Green Floppy
 - NONAME-FAT12
 - Max term.doc

Name	Value
Title	10/1/03
Subject	
Author	Northwest Direct Employee
Keywords	
Comments	
Template	Normal
LastAuthor	Northwest Direct Employee
Revision Number	2
Created	10/1/2003 9:29:00 AM
Last Saved	10/1/2003 9:29:00 AM
Page Count	1
Word Count	0
Char Count	0
App Name	Microsoft Word 9.0
Doc Security	0

List all descendants

Unfiltered Date File

6 Listed 0 Checked Total Green Floppy\NONAME-FAT12\Max term.doc > Summary Information

100%

ATTACHMENT 04

AccessData FTK version 1.42 build 03.12.05 - F:\NWD 060505.Tim Rote Laptop and Floppy\FTK Workup\NWD Direct

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Case

- DELL Inspiron
 - Part 1
 - NORNAME-NTFS
 - UnpartSpace
 - Green Floppy
 - NORNAME-FAT12
 - Max term.doc
 - ObjectPool

bjbrj

10/1/03 Mr. Max Zweig 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

descendants

File Name	Ext	Cr Date	Mod Date	Acc Date
CompObj		N/A	N/A	N/A
DocumentSummaryIn...		N/A	N/A	N/A
SummaryInformation		N/A	N/A	N/A
Table		N/A	N/A	N/A
ObjectPool		10/1/2003 9:29:34 AM	10/1/2003 9:29:34 AM	10/1/2003
WordDocument		N/A	N/A	N/A

6 Listed 0 Checked Total Green Floppy\NORNAME-FAT12\Max term.doc > Word Document

Start AccessData FTK v1.42 FTK Workup\NWD Direct 10/1/03