CEO Forensics, Inc.

DB Cooper vs. Boeing

Digital Forensics Analysis Report

Prepared For: Chad Gough
DePaul University
(555) 555-5555

Prepared By: Corinne Otten
CEO Forensics, Inc.
(666) 666-6666

Date: May 30, 2023

Signatures

The following author(s) of this document affirm that the information contained within is factual; based upon personal knowledge, acquired evidence, and familiarity with the matters recited herein. All of the evidence acquired during this matter and used for analysis is secured, resides on non-volatile media, and in the custody of Examiner Company.

This report is based on information and technology available to, and training completed by, the author(s) at the date of its submission. The below signed author(s) may supplement this report as and when it becomes necessary to do so and expressly reserve the right to do so.

A curriculum vitae, which includes prior testimony for the following author(s), accompanies this report.

Author	Signature
Corinne E. Otten	*Corinne E. Otten*

Executive Summary

Background

My company, CEO Forensics, Inc., was retained on May 1, 2023 by Client, Chad Gough, to review a laptop (Dell Latitude D610, SN X123Y456) believed to have been used by DB Cooper. Once it was determined that the laptop had been used by Mr. Cooper, I was to identify any existing evidence of the theft of $200,000 that occurred during the hijacking of a Boeing 727 aircraft in 1971 and, if possible, determine the current location of Mr. Cooper and the money.

Scope

I was asked to review the forensic image of the laptop, captured by agents in the field, identifying any data relevant to the case, including:

- User accounts and passwords
- Operating system
- System event logs
- External storage devices
- Timeline data
- Photographic and textual documentation
- Internet browsing and search history
- Deleted files
- Encrypted files

Materials Reviewed and Considered

In preparing this report, I reviewed and considered the following:

Image Name	Description	MD5 Hash
DBCooper.dd	Forensic image created from DB Cooper's Laptop	f175912b7e0ecb64ac0817d8d3cfe681
db_cooper_dictionary.txt	Dictionary provided by Chad Gough.	d16b36afb06f1e08b8a924e9320de342
DB_Cooper_Timeline.csv	Timeline generated by Log2timeline provided by Chad Gough	6a648c191009e8c3f15f4e19a8d99f3c

Software Tools and Utilities Used

All materials examined in this matter were analyzed using various closed and open-source utilities (listed in the table below). Unless specifically noted, all references to dates and times in this report have been converted to Central Standard Time (UTC/GMT -6 hours).

Tool/Utility Name	Description
4Discovery USB Historian	Parses registry and SETUP API log files for USB Device insertions
7Zip Forensic	File archiver
AccessDate FTK Imager 4.2.0.13	Forensic Imager
Arsenal Image Mounter	Mounts forensic images as an accessible logical drive
Autopsy Portable 4.19.3	Portable Linux-Based Forensic Suite
EaseUS Data Recovery	Recovers deleted data
Event Log Explorer	Processes and reviews log files
HxD	Hex editor

Jump List Explorer	Displays jumplist artifacts in a GUI
Paladin 8.1	Forensic imaging suite
Photo Recover 7.1	Data recovery software that recovers video, documents and archives
Plaso 1.5.1	Framework for artifact timeline creation and analysis
RegRipperRunner	Windows registry data extraction tool
SamInside	Password cracker
Shadow Explorer	Restore lost or damaged files from Shadow Copies
Sysinternals Strings	Searches for keywords in selected plaintext files
Veracrypt 1.25.9	Decrypts encrypted data
VMWare Workstation 17.0.1	Virtualization software
Zimmerman’s Registry Explorer 1.6.0.0	Views registry in Hive format and allows for searching

Findings and Conclusions

Overview

Based on the results of my findings and analysis below, there is evidence that the recovered laptop (Dell Latitude D610, SN X123Y456) was used by Mr. Cooper and that Mr. Cooper stole money. Further evidence supports that Mr. Cooper traveled to Belize to avoid capture.

Forensic Imaging/Data Collection

The forensic image (DBCooper.dd) was created using Paladin 8.1 in a VMWare virtual machine container. The MD5 hash of the forensic image is f175912b7e0ecb64ac0817d8d3cfe681 (**Question 1**). This was further validated by creating a second forensic image using AccessData FTK Imager. Logs are shown below.

Paladin Log from creation of forensic image:

```
dc3dd 7.2.646 started at 2023-05-18 21:15:05 +0000
compiled options:
command line: /usr/bin/dc3dd if=/dev/sda hash=md5 hash=sha1 of=/media/Evidence/2023-001_DBCooper/2023-001_DBCooper.000
log=/media/Evidence/2023-001_DBCooper/2023-001_DBCooper.log hlog=/media/Evidence/2023-001_DBCooper/2023-
001_DBCooper.log.hashes bufsz=512k
device size: 41943040 sectors (probed),   21,474,836,480 bytes
sector size: 512 bytes (probed)
 21474836480 bytes ( 20 G ) copied ( 100% ), 475.771 s, 43 M/s

input results for device `/dev/sda':
   41943040 sectors in
   0 bad sectors replaced by zeros
   f175912b7e0ecb64ac0817d8d3cfe681 (md5)
   9fcda2037a380bc7a3cedac452d5e3d582d8a2b0 (sha1)

output results for file `/media/Evidence/2023-001_DBCooper/2023-001_DBCooper.000':
   41943040 sectors out

dc3dd completed at 2023-05-18 21:23:01 +0000
```

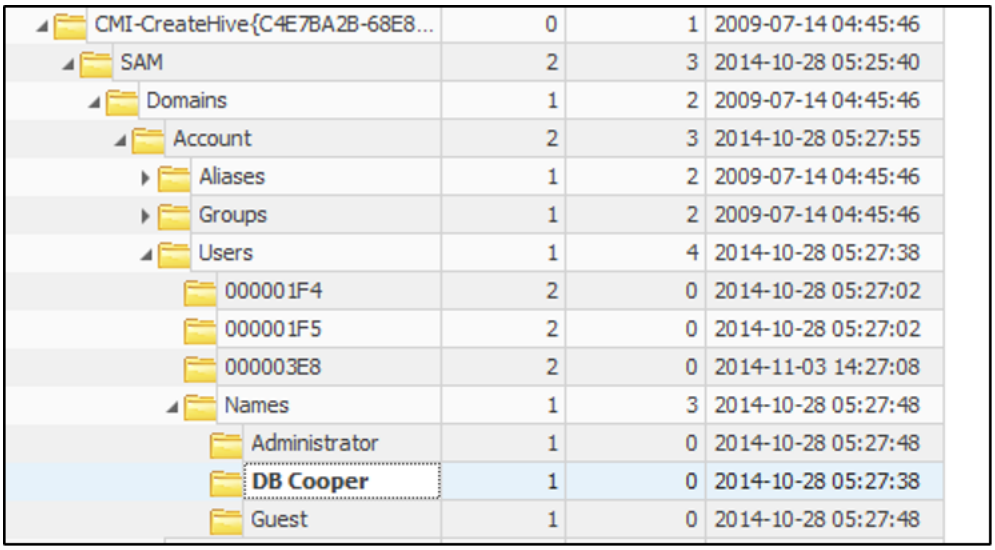
AccessData FTK Image Log from creation of forensic image:

```
Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 16,383
 Heads: 16
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 41,943,040
[Physical Drive Information]
 Drive Interface Type: ide
[Image]
 Image Type: VMWare Virtual Disk
 Source data size: 20480 MB
 Sector count:    41943040
[Computed Hashes]
 MD5 checksum:    f175912b7e0ecb64ac0817d8d3cfe681
 SHA1 checksum:   9fcda2037a380bc7a3cedac452d5e3d582d8a2b0
```

User Accounts and Profiles

The primary username was recovered by extracting the SAM file (\Windows\System32\config\SAM) from the forensic image with 7Zip and analyzing the SAM file with Zimmerman's Registry Explorer v.1.6.0. The user/account name for the main user account/profile is "DB Cooper" (**Question 2**).

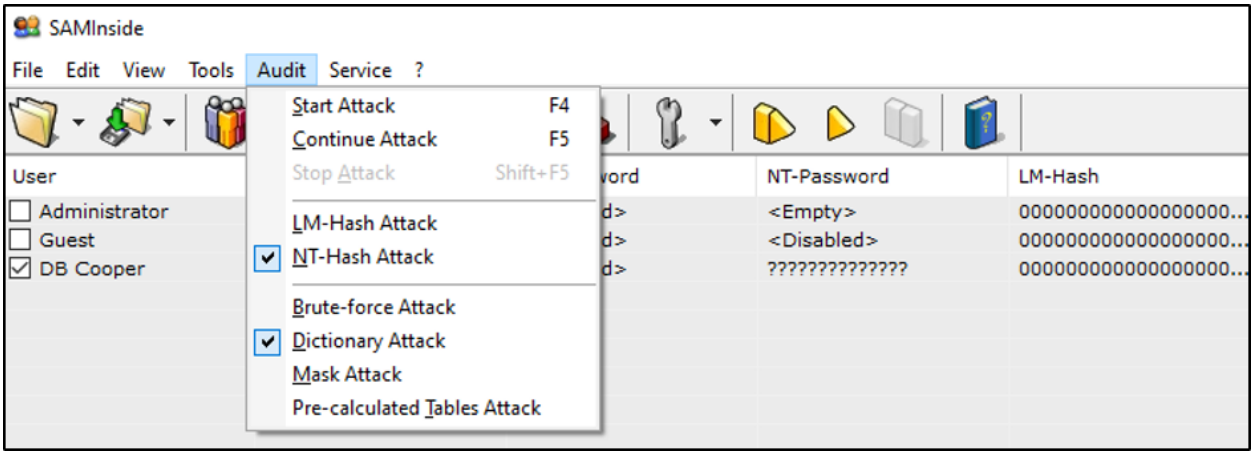
Zimmerman's Registry Explorer user account:



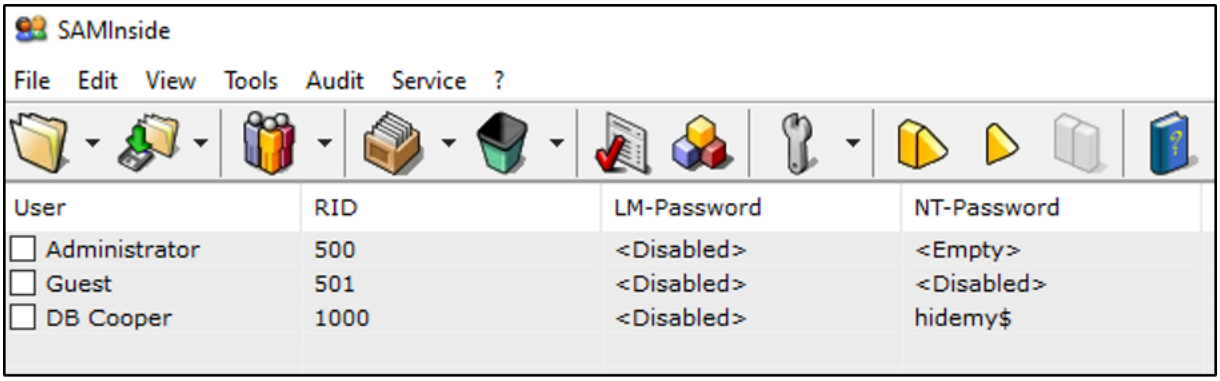
CMI-CreateHive{C4E7BA2B-68E8...	0	1	2009-07-14 04:45:46
SAM	2	3	2014-10-28 05:25:40
Domains	1	2	2009-07-14 04:45:46
Account	2	3	2014-10-28 05:27:55
Aliases	1	2	2009-07-14 04:45:46
Groups	1	2	2009-07-14 04:45:46
Users	1	4	2014-10-28 05:27:38
000001F4	2	0	2014-10-28 05:27:02
000001F5	2	0	2014-10-28 05:27:02
000003E8	2	0	2014-11-03 14:27:08
Names	1	3	2014-10-28 05:27:48
Administrator	1	0	2014-10-28 05:27:48
DB Cooper	1	0	2014-10-28 05:27:38
Guest	1	0	2014-10-28 05:27:48

The password was recovered by extracting the SAM and SYSTEM files (\Windows\System32\config\SAM and \Windows\System32\config\SYSTEM) using 7zip and processing them with the application SamInside. I set the software parameters to "NT Hash Attack" and "Dictionary Attack", loaded the dictionary file (db_cooper_dictionary.txt, MD5 d16b36afb06f1e08b8a924e9320de342) provided by Chad Gough. The password for the "DB Cooper" account is "hidemy$" (**Question 3**).

SamInside settings:



SamInside password results:



Operating System

I identified the operating system using RegRipperRunner with the WinVer plugin and the SOFTWARE file (\Windows\System32\config\SOFTWARE). The laptop operating system was Windows 7 Ultimate Edition (**Question 4**). The registered owner is "Windows User". The operating system was installed 11-30-2017 (**Question 5**).

RegRipperRunner winver plugin results:

```
winver v.20200525
(Software) Get Windows version & build info

ProductName              Windows 7 Ultimate
CSDVersion               Service Pack 1
BuildLab                 7601.win7sp1_rtm.101119-1850
BuildLabEx               7601.17514.amd64fre.win7sp1_rtm.101119-1850
RegisteredOrganization
RegisteredOwner          Windows User
InstallDate              2017-11-30 23:59:59Z
```

Removable Storage Analysis

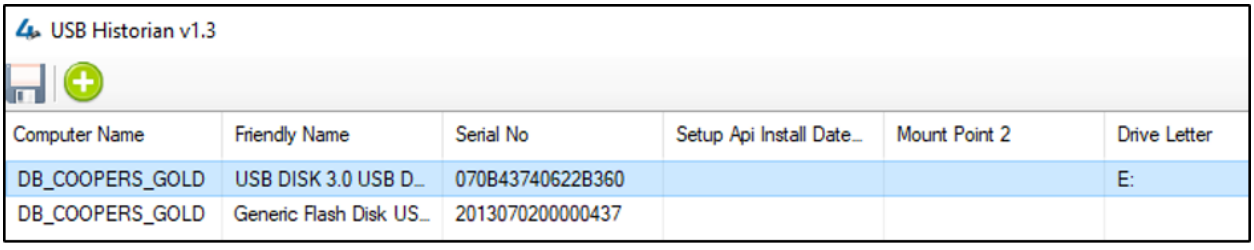
The laptop had two USB storage devices attached. This was determined using RegRipperRunner with the Usbstor plugin and the SYSTEM file (\Windows\System32\config\SYSTEM) (**Question 6**).

- USB 1: SN 070B43740622B360, used on 11-03-2014
- USB 2: SN 2013070200000437, used on 11-03-2014

RegRipperRunner usbstor plugin results:

```
USBStor
ControlSet001\Enum\USBStor

Disk&Ven_&Prod_USB_DISK_3.0&Rev_PMAP [2014-11-03 14:28:37]
  S/N: 070B43740622B360&0 [2014-11-03 14:28:37Z]
  Device Parameters LastWrite: [2014-11-03 14:28:37Z]
  LogConf LastWrite          : [2014-11-03 14:28:37Z]
  Properties LastWrite       : [2014-11-03 14:28:37Z]
    FriendlyName          : USB DISK 3.0 USB Device

Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07 [2014-11-03 14:25:13]
  S/N: 20130702000000437&0 [2014-11-03 14:25:14Z]
  Device Parameters LastWrite: [2014-11-03 14:25:14Z]
  LogConf LastWrite          : [2014-11-03 14:25:13Z]
  Properties LastWrite       : [2014-11-03 14:25:14Z]
    FriendlyName          : Generic Flash Disk USB Device
```

This was further validated with 4Discovery USB Historian:



Recently Accessed Files

I used the timeline provided by Chad Gough (DB_Cooper_Timeline.csv, MD5 6a648c191009e8c3f15f4e19a8d99f3c) to determine what had been opened from the USB devices. The original timeline file had too many events/lines to be opened in Excel or Libre Office, so I opened it in Notepad++ and split the file into multiple CSV files, organized by year.

DB Cooper opened two files with Windows Wordpad. This was determined by reviewing the DB_Cooper_Timeline.csv file for Wordpad related events. The timeline revealed Wordpad.exe had been executed twice. I then used Zimmerman's Registry Explorer to review the USER.NAT file to determine the user had opened (**Question 7 and 11**):

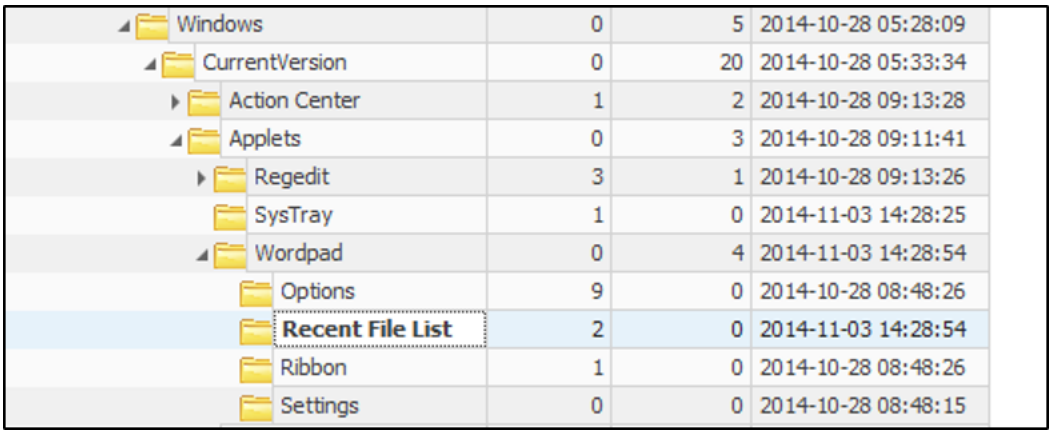
1. secrets.zip
2. Docx4j_GettingStarted.docx.

These two documents were also in the linked files list, indicating they had been recently accessed.

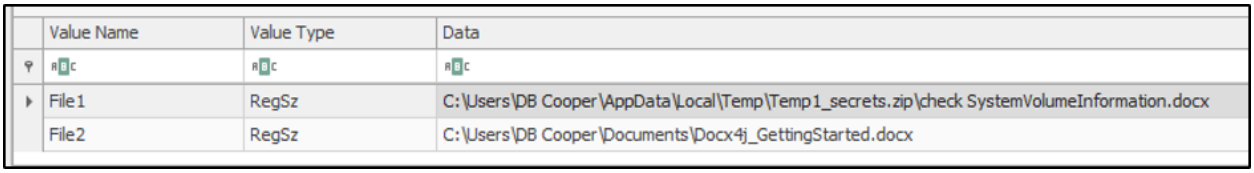
Linked List Displayed in 7Zip:

Name	Size	Packed Size	Modified	Created	Accessed	Metadata Cha...
AutomaticDestinations	14 848	20 480	2014-10-28 03:48	2014-10-28 00:28	2014-10-28 03:48	2014-10-28 03:48
CustomDestinations	34 706	45 104	2014-11-03 09:33	2014-10-28 00:28	2014-11-03 09:33	2014-11-03 09:33
desktop.ini	432	432	2014-10-28 00:28	2014-10-28 00:28	2014-10-28 00:28	2014-10-28 00:28
Docx4j_GettingStarted.lnk	2 609	4 096	2014-10-28 03:48	2014-10-28 03:48	2014-10-28 03:48	2014-10-28 03:48
secrets.lnk	426	426	2014-11-03 09:28	2014-11-03 09:28	2014-11-03 09:28	2014-11-03 09:28

Zimmerman's Registry Explorer Recent Files:



Windows	0	5	2014-10-28 05:28:09
CurrentVersion	0	20	2014-10-28 05:33:34
Action Center	1	2	2014-10-28 09:13:28
Applets	0	3	2014-10-28 09:11:41
Regedit	3	1	2014-10-28 09:13:26
SysTray	1	0	2014-11-03 14:28:25
Wordpad	0	4	2014-11-03 14:28:54
Options	9	0	2014-10-28 08:48:26
Recent File List	2	0	2014-11-03 14:28:54
Ribbon	1	0	2014-10-28 08:48:26
Settings	0	0	2014-10-28 08:48:15



Value Name	Value Type	Data
File1	RegSz	C:\Users\DB Cooper\AppData\Local\Temp\Temp1_secrets.zip\check SystemVolumeInformation.docx
File2	RegSz	C:\Users\DB Cooper\Documents\Docx4j_GettingStarted.docx

Recent Files in RegRipperrunner:

```
File: D:\Forensics\Project\DBCooper_Hives\NTUSER.DAT

recentdocs v.20200427
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time: 2014-11-03 14:28:45Z
  1 = secrets.zip
  0 = Docx4j_GettingStarted.docx

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.docx
LastWrite Time 2014-10-28 08:48:15Z
MRUListEx = 0
  0 = Docx4j_GettingStarted.docx

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.zip
LastWrite Time 2014-11-03 14:28:45Z
MRUListEx = 0
  0 = secrets.zip
```

Autopsy Shell Bag report showing files from the flashdrive mounted at E:

My Computer\E:\	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...	2014-11-03 14:28:42 CST
My Computer\E:\secrets.zi	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...	2014-11-03 14:28:55 CST

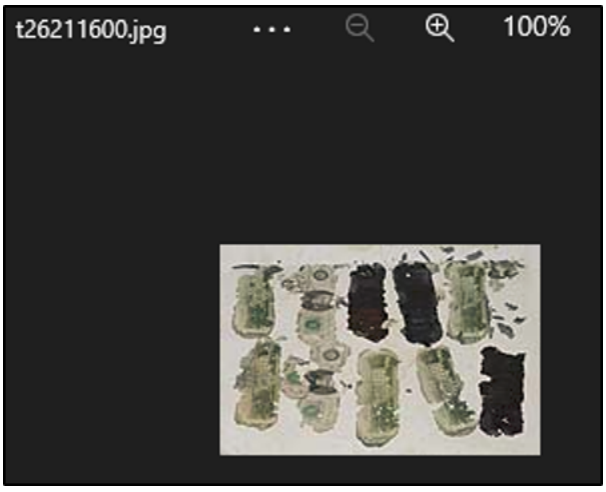
Photo Artifact Analysis

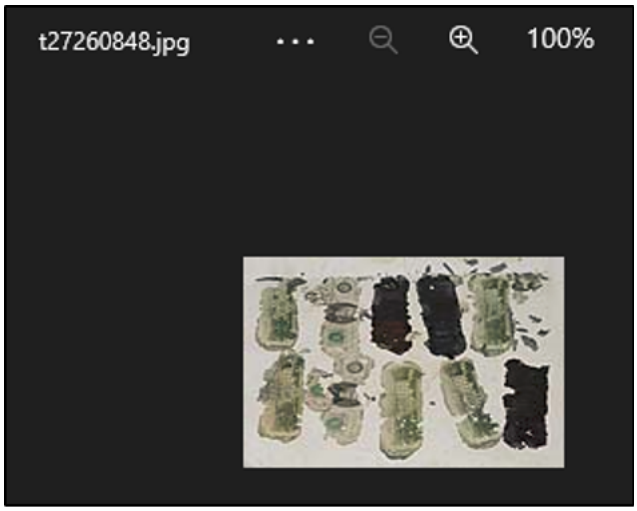
Based on a tip that DB Cooper had 4 (four) images on his computer depicting the stolen money, I ran Photo Recovery v7.1, searching specifically for image file types (jpg, png, tif). This recovered 19 images, only 2 (two) images were relevant.

Photo Recovery:

File family	Number of files recovered
png	10
jpg	9

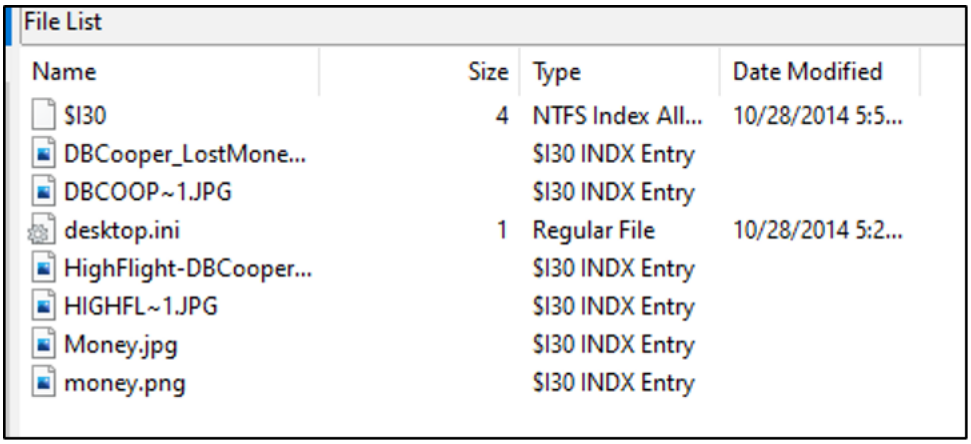
Two thumbnail images (t26211600.jpg and t27260848.jpg) showed burned money.



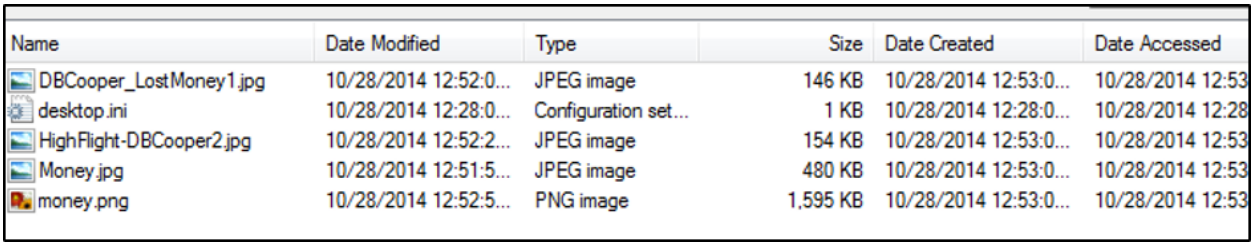


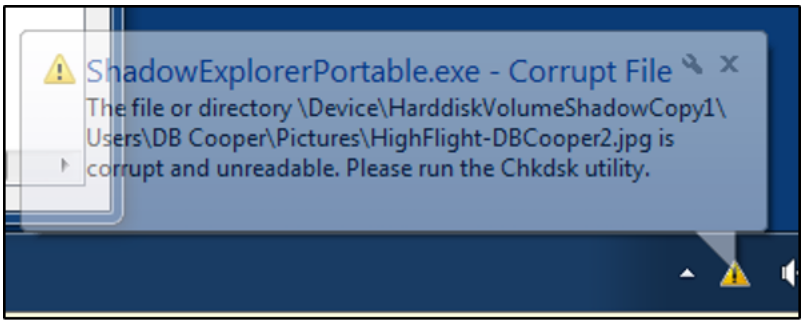
Looking at the disk image in AccessData FTK Imager shows multiple images that were previously in \Users\DB Cooper\Pictures (**Question 8**):

AccessData FTK Imager:

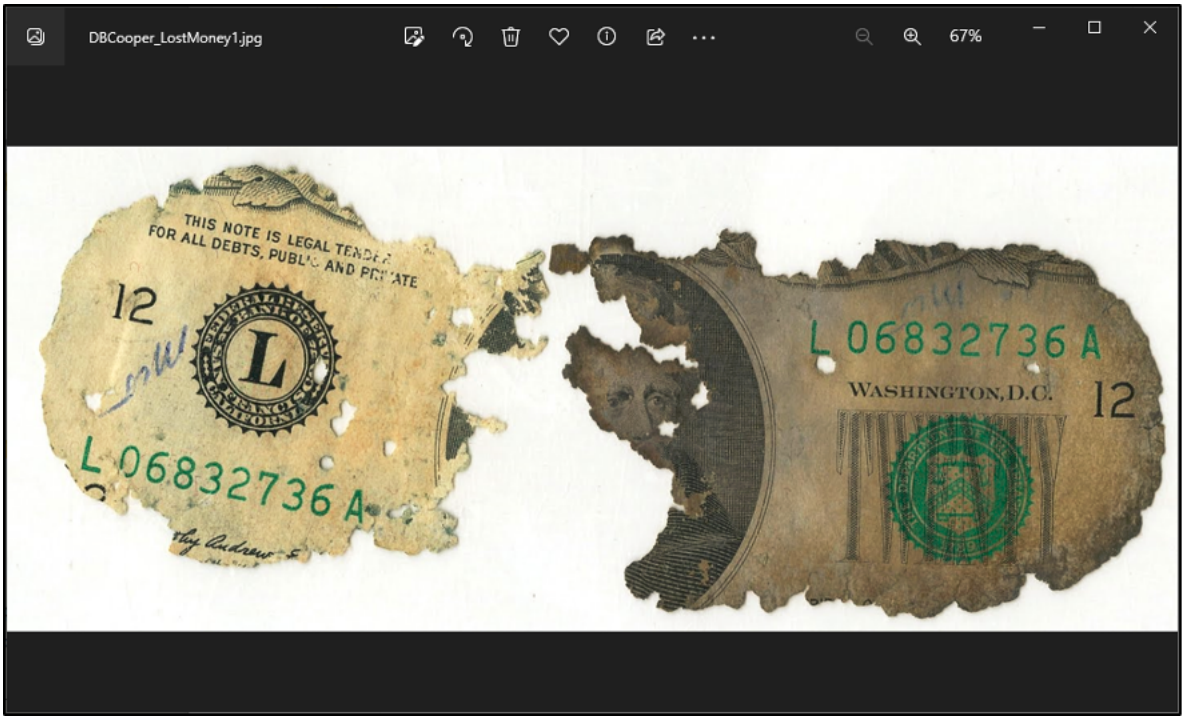


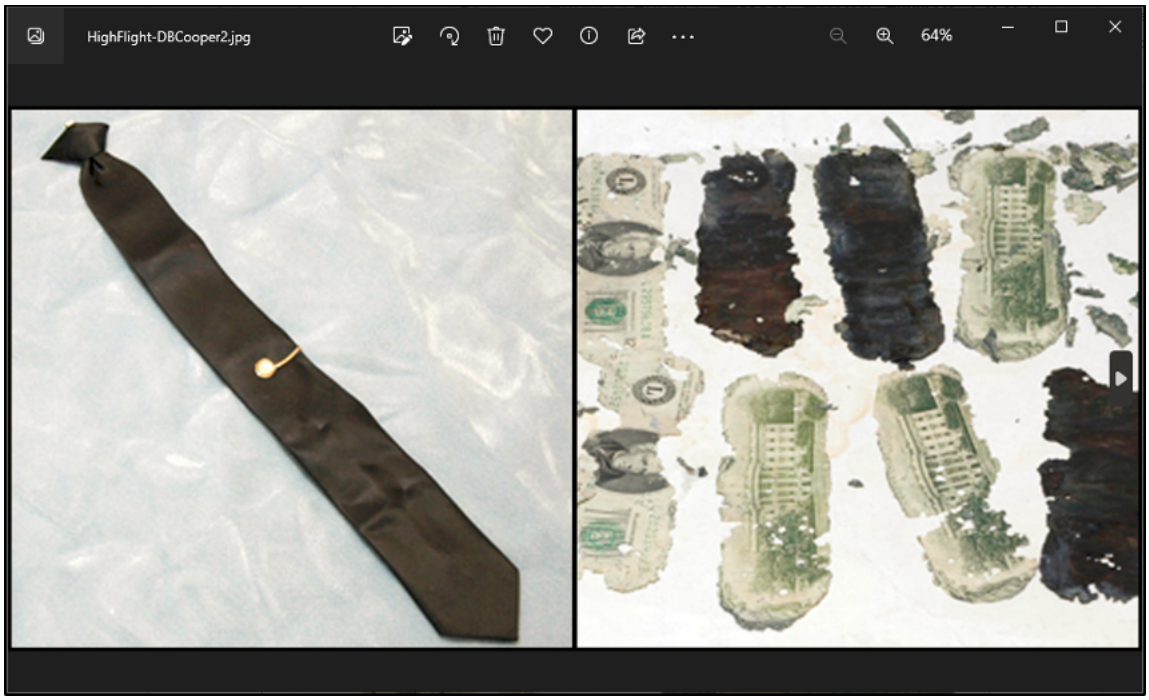
It appears that these images have been deleted from the system. I used Shadow Explorer to view shadow copies of the images. Shadow Explorer could export Money.jpg but could not export the other images as they were corrupted.

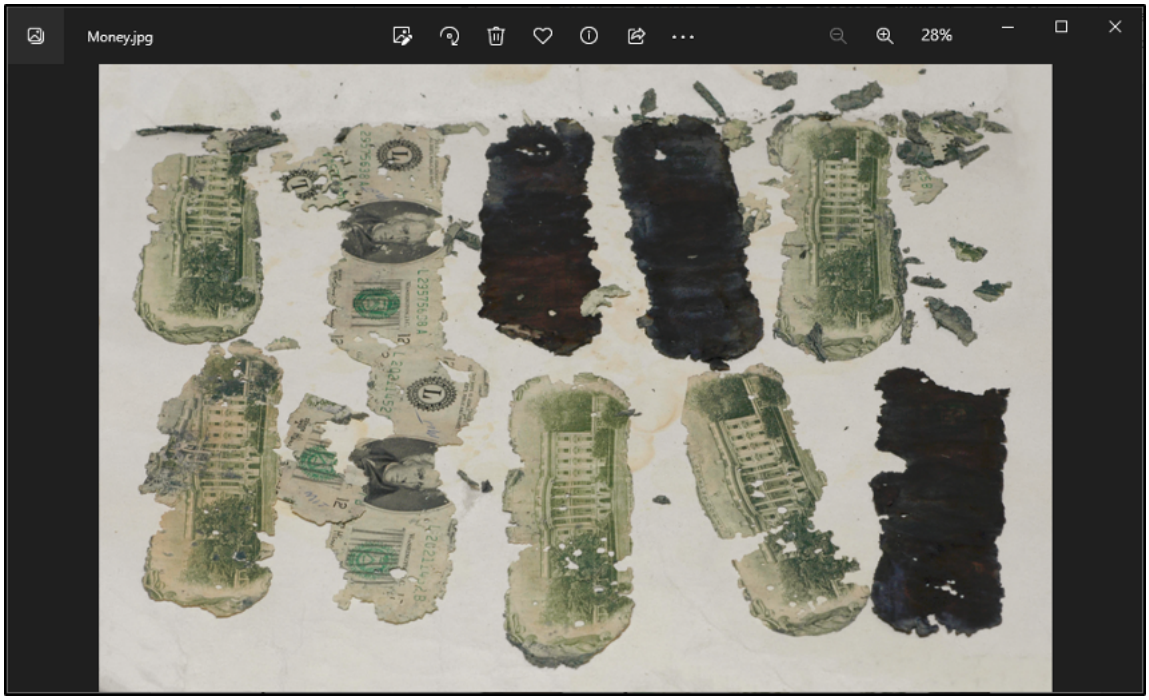




I used the free version of EaseUS Data Recovery to retrieve the three images that were corrupted.






Money.jpg
28%

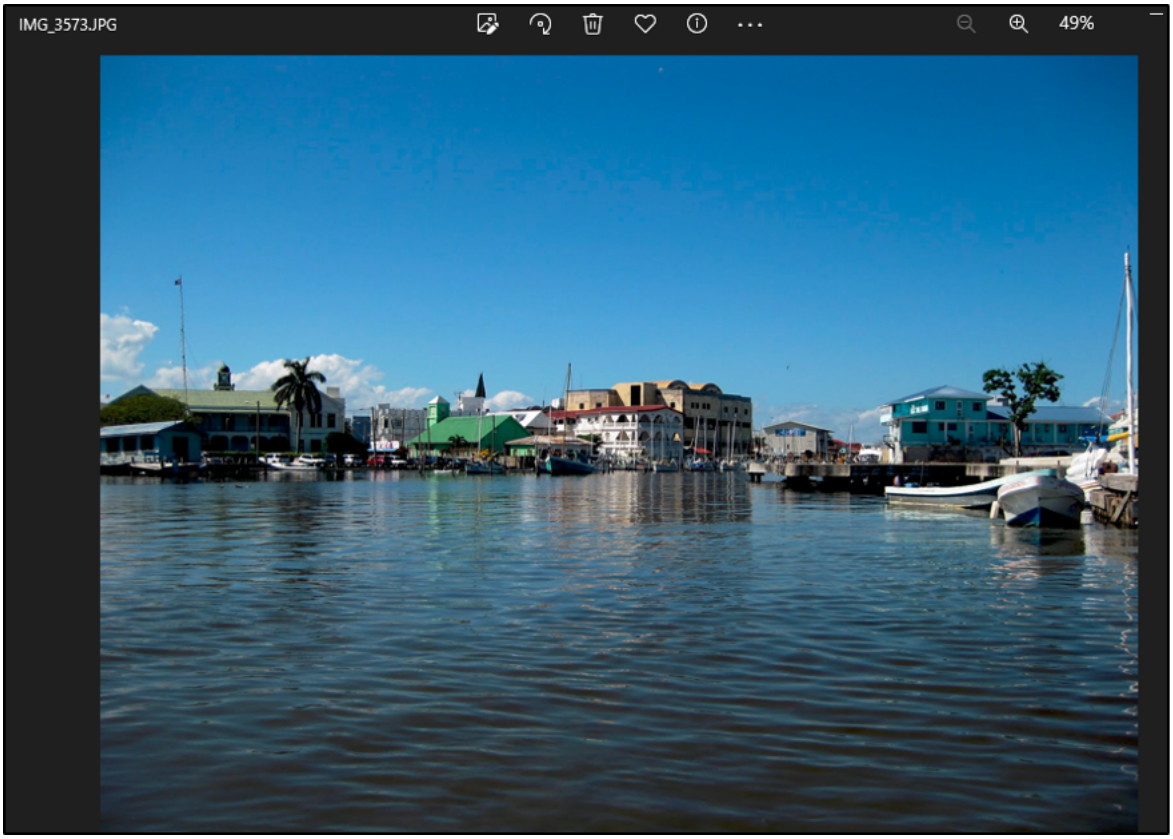

money.png
69%
FOLLOW
THE MONEY

I was also able to recover the image "IMG_3573.JPG" from DB Cooper/ Downloads folder. The image depicted a tropical marina.

7Zip Forensic:

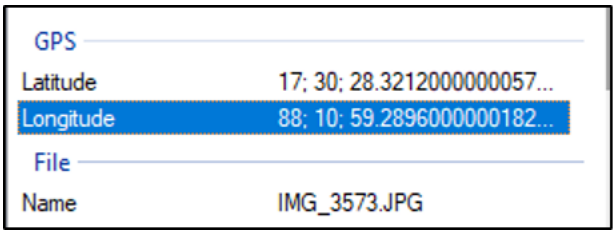
Name	Size	Packed Size	Modified	Created	Accessed	Metadata Cha...
desktop.ini	282	282	2014-10-28 00:28	2014-10-28 00:28	2014-10-28 00:28	2014-10-28 00:28
IMG_3573.JPG	218 430	221 184	2014-10-31 12:01	2014-11-03 09:16	2014-11-03 09:16	2014-10-31 12:01

Image file: IMG_3573.JPG:

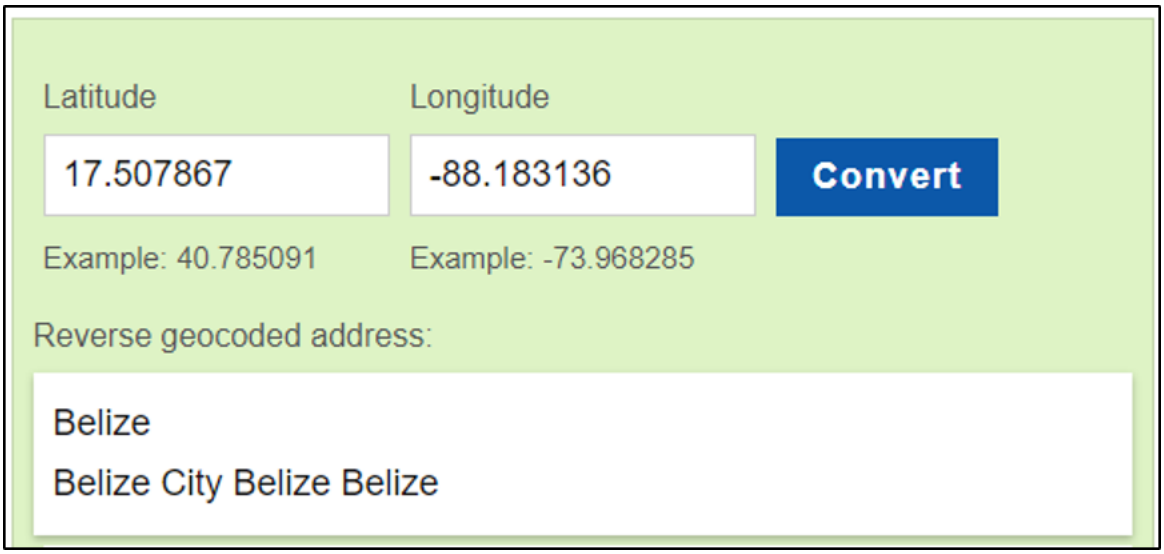


The geolocation data in the metadata of the image show the latitude and longitude (Latitude:17.507867, Longitude: -88.183136) that correspond to Belize. I believe this artifact indicates where DB Cooper is hiding with the money (**Question 16**). This theory was further supported by Internet

search histories that show that DB Cooper did a Google search: where to hide in Belize (see screenshots in Internet Browsing and Search History).



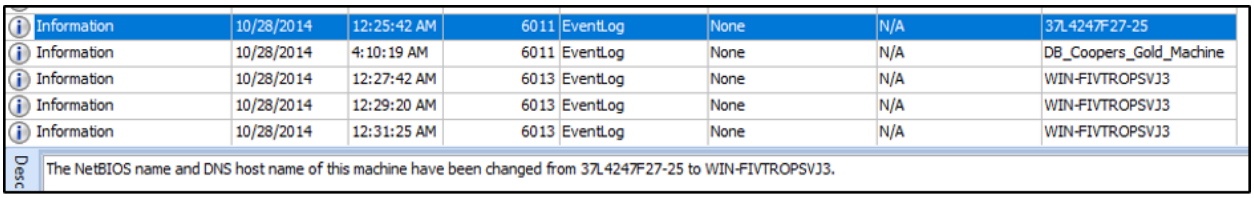
Results of Latlong.net Lookup:



NETBIOS and Computer Time

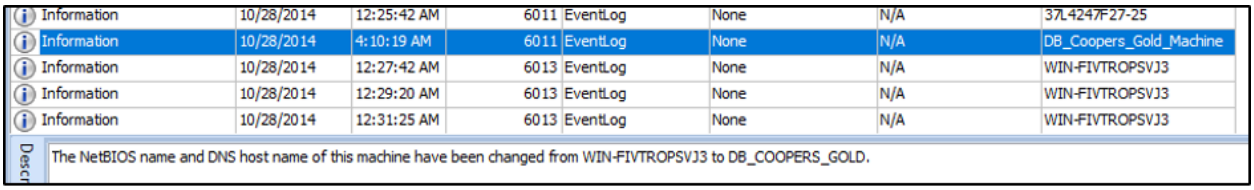
I reviewed the system logs (C:\Windows\System32\winevt\logs\system) with the application Event Log Explorer and found evidence that the computer name (NETBIOS) was changed. This was done by loading the system log and looking for a 6011 event (a 6011 event indicates a NETBIOS change). The name was changed twice, first from 37L4247F27-25 to WIN-FIVTROPSVJ3, and then from WIN-FIVTROPSVJ3 to DB_COOPERS_GOLD (**Question 9**).

Event Log Explorer:



Information	10/28/2014	12:25:42 AM	6011	EventLog	None	N/A	37L4247F27-25
Information	10/28/2014	4:10:19 AM	6011	EventLog	None	N/A	DB_Coopers_Gold_Machine
Information	10/28/2014	12:27:42 AM	6013	EventLog	None	N/A	WIN-FIVTROPSVJ3
Information	10/28/2014	12:29:20 AM	6013	EventLog	None	N/A	WIN-FIVTROPSVJ3
Information	10/28/2014	12:31:25 AM	6013	EventLog	None	N/A	WIN-FIVTROPSVJ3

Desc The NetBIOS name and DNS host name of this machine have been changed from 37L4247F27-25 to WIN-FIVTROPSVJ3.

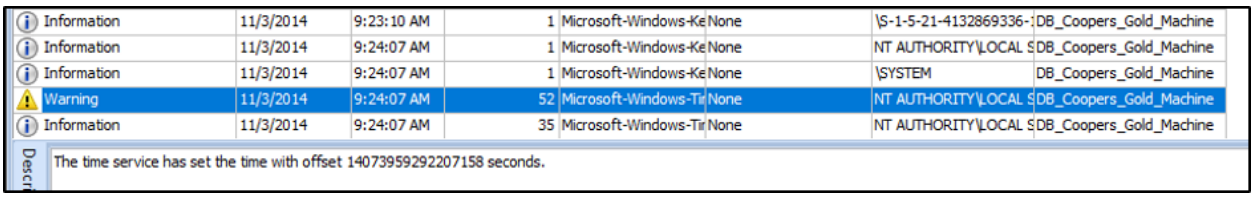


Information	10/28/2014	12:25:42 AM	6011	EventLog	None	N/A	37L4247F27-25
Information	10/28/2014	4:10:19 AM	6011	EventLog	None	N/A	DB_Coopers_Gold_Machine
Information	10/28/2014	12:27:42 AM	6013	EventLog	None	N/A	WIN-FIVTROPSVJ3
Information	10/28/2014	12:29:20 AM	6013	EventLog	None	N/A	WIN-FIVTROPSVJ3
Information	10/28/2014	12:31:25 AM	6013	EventLog	None	N/A	WIN-FIVTROPSVJ3

Descr The NetBIOS name and DNS host name of this machine have been changed from WIN-FIVTROPSVJ3 to DB_COOPERS_GOLD.

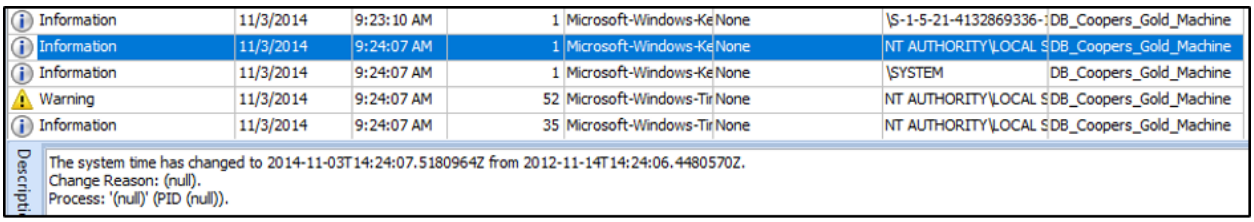
I also reviewed the system logs (C:\Windows\System32\winevt\logs\system) with the application Event Log Explorer and found evidence of time/date manipulation. This was done by loading the system log and identifying a 52 event (a warning that the time had been offset). The system time was changed from 2012-11-14T14:24:06.4480570Z to 2014-11-03T14:24:07.5180964Z (**Question 10**).

Event Log Explorer:



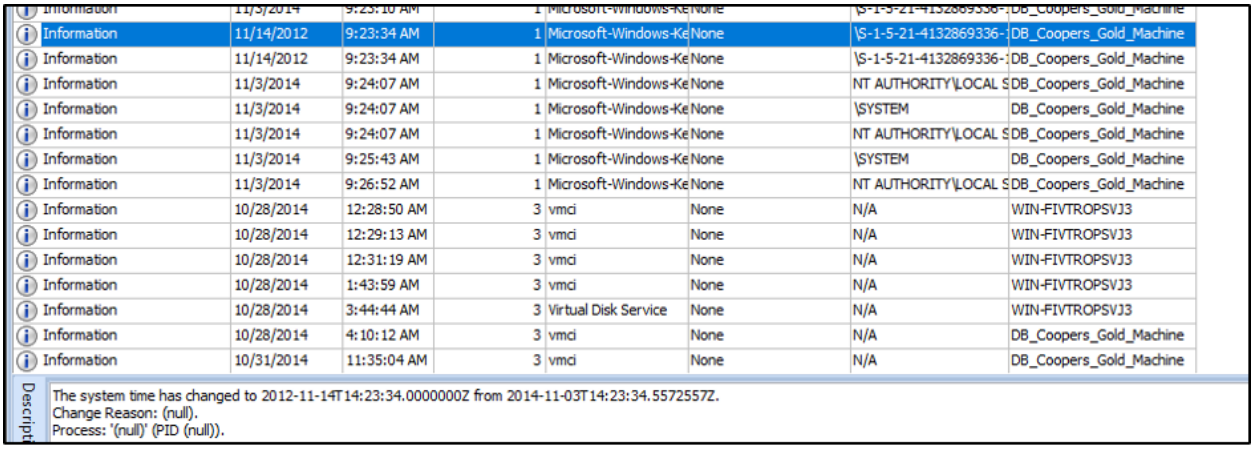
Information	11/3/2014	9:23:10 AM	1	Microsoft-Windows-Ke	None	\S-1-5-21-4132869336-	DB_Coopers_Gold_Machine
Information	11/3/2014	9:24:07 AM	1	Microsoft-Windows-Ke	None	NT AUTHORITY\LOCAL S	DB_Coopers_Gold_Machine
Information	11/3/2014	9:24:07 AM	1	Microsoft-Windows-Ke	None	\SYSTEM	DB_Coopers_Gold_Machine
Warning	11/3/2014	9:24:07 AM	52	Microsoft-Windows-Ti	None	NT AUTHORITY\LOCAL S	DB_Coopers_Gold_Machine
Information	11/3/2014	9:24:07 AM	35	Microsoft-Windows-Ti	None	NT AUTHORITY\LOCAL S	DB_Coopers_Gold_Machine

Descr The time service has set the time with offset 1407395929220715 8 seconds.



Information	11/3/2014	9:23:10 AM	1	Microsoft-Windows-Ke	None	\S-1-5-21-4132869336-	DB_Coopers_Gold_Machine
Information	11/3/2014	9:24:07 AM	1	Microsoft-Windows-Ke	None	NT AUTHORITY\LOCAL S	DB_Coopers_Gold_Machine
Information	11/3/2014	9:24:07 AM	1	Microsoft-Windows-Ke	None	\SYSTEM	DB_Coopers_Gold_Machine
Warning	11/3/2014	9:24:07 AM	52	Microsoft-Windows-Ti	None	NT AUTHORITY\LOCAL S	DB_Coopers_Gold_Machine
Information	11/3/2014	9:24:07 AM	35	Microsoft-Windows-Ti	None	NT AUTHORITY\LOCAL S	DB_Coopers_Gold_Machine

Descripti The system time has changed to 2014-11-03T14:24:07.5180964Z from 2012-11-14T14:24:06.4480570Z.
Change Reason: (null).
Process: '(null)' (PID (null)).



Information	11/14/2012	9:23:34 AM	1	Microsoft-Windows-Ke	None	\S-1-5-21-4132869336-	DB_Coopers_Gold_Machine
Information	11/14/2012	9:23:34 AM	1	Microsoft-Windows-Ke	None	\S-1-5-21-4132869336-	DB_Coopers_Gold_Machine
Information	11/3/2014	9:24:07 AM	1	Microsoft-Windows-Ke	None	NT AUTHORITY\LOCAL S	DB_Coopers_Gold_Machine
Information	11/3/2014	9:24:07 AM	1	Microsoft-Windows-Ke	None	\SYSTEM	DB_Coopers_Gold_Machine
Information	11/3/2014	9:24:07 AM	1	Microsoft-Windows-Ke	None	NT AUTHORITY\LOCAL S	DB_Coopers_Gold_Machine
Information	11/3/2014	9:25:43 AM	1	Microsoft-Windows-Ke	None	\SYSTEM	DB_Coopers_Gold_Machine
Information	11/3/2014	9:26:52 AM	1	Microsoft-Windows-Ke	None	NT AUTHORITY\LOCAL S	DB_Coopers_Gold_Machine
Information	10/28/2014	12:28:50 AM	3	vmci	None	N/A	WIN-FIVTROPSVJ3
Information	10/28/2014	12:29:13 AM	3	vmci	None	N/A	WIN-FIVTROPSVJ3
Information	10/28/2014	12:31:19 AM	3	vmci	None	N/A	WIN-FIVTROPSVJ3
Information	10/28/2014	1:43:59 AM	3	vmci	None	N/A	WIN-FIVTROPSVJ3
Information	10/28/2014	3:44:44 AM	3	Virtual Disk Service	None	N/A	WIN-FIVTROPSVJ3
Information	10/28/2014	4:10:12 AM	3	vmci	None	N/A	DB_Coopers_Gold_Machine
Information	10/31/2014	11:35:04 AM	3	vmci	None	N/A	DB_Coopers_Gold_Machine

Descripti

The system time has changed to 2012-11-14T14:23:34.0000000Z from 2014-11-03T14:23:34.5572557Z.
Change Reason: (null).
Process: '(null)' (PID (null)).

Internet History Analysis

I used JumpList Explorer to review the Custom Destination logs, this revealed the following Google searches (**Question 12**):

- downloading a virus via dropbox
- where is db cooper now?
- how to shred documents with sdelete
- where to hide in Belize

)\https://www.google.com/?gws_rd=ssl
)\http://www.bleepingcomputer.com/forums/t/549064/virus-heu-aegiscs938-via-dropbox
)\http://www.google.com/url?url=http://www.bleepingcomputer.com/forums/t/549064/virus-heu-aegiscs938-via-dropbox/&rct=j&frm=1&q=&esrc=s&sa=U&ei=sZFXVI-mLMLioA
)\https://www.google.com/search?hl=en&source=hp&q=downloading+a+virus+via+dropbox&gbv=2&oq=downloading+a+virus+via+dropbox&gs_l=heirloom-hp.3...2278.858
)\https://www.google.com/url?url=https://www.dropbox.com/&rct=j&frm=1&q=&esrc=s&sa=U&ei=jpFXVKOpL8ibNq-_gOgJ&ved=0CCMQFjAA&usg=AFQjCNHZkdzqnNjV_LVdy2
)\https://www.google.com/search?q=dropbox.com&hl=en&gbv=2&oq=&gs_l=
)\https://www.google.com/search?q=where+is+db+cooper+now%3F&hl=en&gbv=2&oq=&gs_l=
)\https://www.google.com/search?hl=en&source=hp&q=how+to+shred+documents+with+sdelete&gbv=2&oq=how+to+shred+documents+with+sdelete&gs_l=heirloom-hp.3.
)\https://www.google.com/search?hl=en&source=hp&q=where+to+hide+in+belize&gbv=2&oq=where+to+hide+in+belize&gs_l=heirloom-hp.3...1732.5304.0.5445.23.17.0.6.

The Autopsy logs also support the search history above:

Domain	Text	Program Name	Date Accessed	Data Source
google.com	downloading a virus v	Internet Explorer	2014-11-03 14:31:11 CST	DBCooper.dd
google.com	downloading a virus vi	Internet Explorer	2014-11-03 14:31:11 CST	DBCooper.dd
google.com	downloading a virus via dropbox	Internet Explorer	2014-11-03 14:31:14 CST	DBCooper.dd
google.com	downloading a virus via dropbox	Internet Explorer	2014-11-03 14:31:14 CST	DBCooper.dd

Web Search

Table | Thumbnail | Summary

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
index.dat				google.com	how to shred documents wi	Internet Explorer	2014-11-03 14:30:19 CST	DBCooper.dd
index.dat				google.com	how to shred documents with	Internet Explorer	2014-11-03 14:30:19 CST	DBCooper.dd
index.dat				google.com	how to shred documents with sdelete	Internet Explorer	2014-11-03 14:30:23 CST	DBCooper.dd
index.dat				google.com	how to shred documents with sdelete	Internet Explorer	2014-11-03 14:30:23 CST	DBCooper.dd
index.dat				google.com	how to shred documents with sdelete	Internet Explorer	2014-11-03 14:30:23 CST	DBCooper.dd
index.dat				google.com	how to u	Internet Explorer	2014-11-03 14:29:42 CST	DBCooper.dd

index.dat				google.com	how to use truecrypt	Internet Explorer	2014-11-03 14:29:44 CST	DBCooper.dd
index.dat				google.com	how to use truecrypt	Internet Explorer	2014-11-03 14:29:44 CST	DBCooper.dd
index.dat				google.com	how to use truecrypt	Internet Explorer	2014-11-03 14:29:44 CST	DBCooper.dd

index.dat				google.com	where is db cooper now?	Internet Explorer	2014-11-03 14:30:33 CST	DBCooper.dd
index.dat				google.com	where is db cooper now?	Internet Explorer	2014-11-03 14:30:33 CST	DBCooper.dd
index.dat				google.com	where is db cooper now?	Internet Explorer	2014-11-03 14:30:33 CST	DBCooper.dd

index.dat				google.com	where to hide in belize	Internet Explorer	2014-11-03 14:29:54 CST	DBCooper.dd
index.dat				google.com	where to hide in belize	Internet Explorer	2014-11-03 14:29:54 CST	DBCooper.dd
index.dat				google.com	where to hide in belize	Internet Explorer	2014-11-03 14:29:54 CST	DBCooper.dd

Autopsy also reveals the following downloads (**Question 13**):

Listing

Web Downloads

Table | Thumbnail | Summary

Source Name	S	C	O	Path
usback[1].zip:Zone.Identifier				/Users/DB Cooper/AppData/Local/Microsoft/Windows/Tem...
usback.exe:Zone.Identifier				/Users/DB Cooper/AppData/Roaming/usback.exe
IMG_3573.JPG:Zone.Identifier				/Users/DB Cooper/Downloads/IMG_3573.JPG
recovery.exe:Zone.Identifier				/Windows/recovery.exe

Malware Analysis

It is likely that DB Cooper's computer is infected by a virus (**Question 14**) that he downloaded via dropbox. He reviewed a forum online at http://www.bleepingcomputer.com/forums/t/549064/virus-heu-aegiscs938-via-dropbox. And Autopsy Internet History indicates he logged into a Dropbox account.

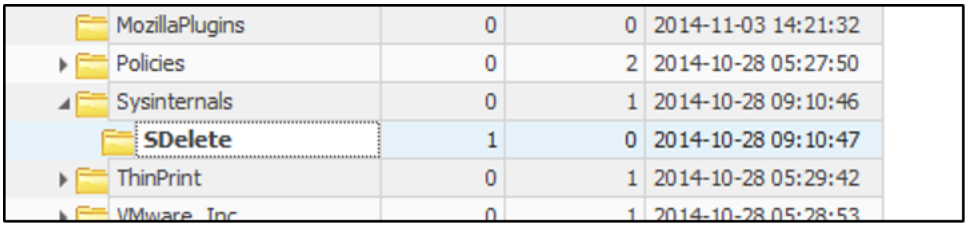
RegRipperRunner shows the following possible malware:

```
**Possible fileless malware found.
Microsoft\Windows\CurrentVersion\WSMAN\Plugin\Microsoft.PowerShell
LastWrite time: 2009-07-14 04:54:22Z
Value Name: ConfigXML
Data:              <PlugInConfiguration xmlns="http://schemas.microsoft.com/wbem/ws
XmlRenderingType="text" >                 <InitializationParameters>
<Resource ResourceUri="http://schemas.microsoft.com/powershell/microsoft.powershell
xmlns="http://schemas.microsoft.com/wbem/wsman/1/config/PluginConfiguration" Uri="ht
(AU;SA;GXGW;;;WD)"/>                          <Capability Type="Shell"/>

**Possible fileless malware found.
Wow6432Node\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
LastWrite time: 2014-10-28 06:24:54Z
Value Name: Path
Data: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

**Possible fileless malware found.
Wow6432Node\Microsoft\Windows\CurrentVersion\WSMAN\Plugin\Microsoft.PowerShell32
LastWrite time: 2009-07-14 04:54:22Z
Value Name: ConfigXML
Data: <PlugInConfiguration xmlns="http://schemas.microsoft.com/wbem/wsman/1/config/
Architecture="32" >                          <InitializationParameters>
<Resources>                               <Resource ResourceUri="http://schemas.micro
xmlns="http://schemas.microsoft.com/wbem/wsman/1/config/PluginConfiguration" Uri="ht
(AU;SA;GXGW;;;WD)"/>                                   <Capability Type="Shell"/>
```

Deleted Files

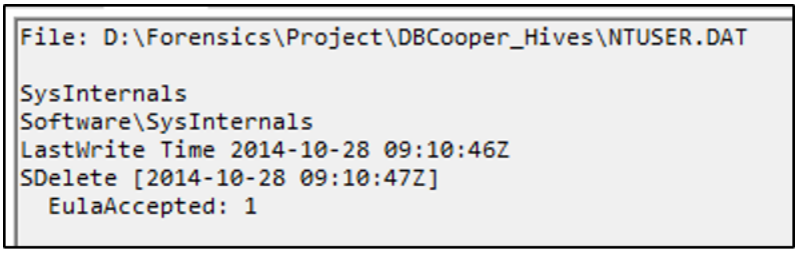
DB Cooper used software to delete files (**Question 17**). DB Cooper installed Sdelete on 10/28/2014 (**Question 18**).

Reviewing the NTUSER.DAT file in Zimmerman's Registry Explorer:

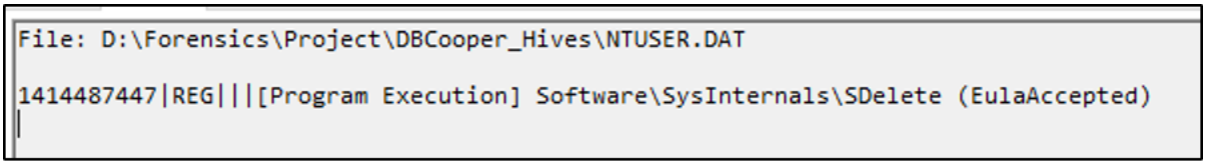


MozillaPlugins	0	0	2014-11-03 14:21:32
Policies	0	2	2014-10-28 05:27:50
Sysinternals	0	1	2014-10-28 09:10:46
SDelete	1	0	2014-10-28 09:10:47
ThinPrint	0	1	2014-10-28 05:29:42
VMware, Inc	0	1	2014-10-28 05:28:53

EULA for software installed on 10/28/2014:



```
File: D:\Forensics\Project\DBCooper_Hives\NTUSER.DAT

SysInternals
Software\SysInternals
LastWrite Time 2014-10-28 09:10:46Z
SDelete [2014-10-28 09:10:47Z]
  EulaAccepted: 1
```



```
File: D:\Forensics\Project\DBCooper_Hives\NTUSER.DAT

1414487447|REG|||[Program Execution] Software\SysInternals\SDelete (EulaAccepted)
```

DB Cooper deleted a large number of files, including many system files, as shown in the DB_Cooper_Timeline.csv file:

date	short
10/28/2014	DB CooZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZ 22317-7 USN_REASON_FILE_DELETE USN...
10/28/2014	DB CooZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZ 22317-7 USN_REASON_FILE_DELETE USN...
10/28/2014	DB CooZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZ 22317-7 USN_REASON_FILE_DELETE USN...
10/28/2014	DB CooZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZZ 22316-63 USN_REASON_FILE_DELETE USN_R...
10/28/2014	DB CooZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZZ 22316-63 USN_REASON_FILE_DELETE USN_R...
10/28/2014	DB CooZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZZ 22316-63 USN_REASON_FILE_DELETE USN_R...
10/28/2014	DB CooZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZ 34051-3 USN_REASON_FILE_DELETE USN_REA...
10/28/2014	DB CooZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZ 34051-3 USN_REASON_FILE_DELETE USN_REA...
10/28/2014	DB CooZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZ 34051-3 USN_REASON_FILE_DELETE USN_REA...
10/28/2014	DB CooZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZZ 34061-9 USN_REASON_FILE_DELETE...
10/28/2014	DB CooZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZZ 34061-9 USN_REASON_FILE_DELETE...
10/28/2014	DB CooZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZZ 34061-9 USN_REASON_FILE_DELETE...
10/28/2014	DB CooZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZ 35554-2 USN_REASON_FILE_DELETE USN_REASO...

I used Shadow Explorer to view the shadow copies of the images in User/DB Cooper/Pictures:

Name	Date Modified	Type	Size	Date Created
DBCooper_LostMoney1.jpg	10/28/2014 12:52:0...	JPEG image	146 KB	10/28/2014 12:53:0...
desktop.ini	10/28/2014 12:28:0...	Configuration set...	1 KB	10/28/2014 12:28:0...
HighFlight-DBCooper2.jpg	10/28/2014 12:52:2...	JPEG image	154 KB	10/28/2014 12:53:0...
Money.jpg	10/28/2014 12:51:5...	JPEG image	480 KB	10/28/2014 12:53:0...
money.png	10/28/2014 12:52:5...	PNG image	1,595 KB	10/28/2014 12:53:0...

I used Shadow Explorer to view the shadow copies of the documents in User/DB Cooper/Documents:

Name	Date Modified	Type	Size	Date Created	Date Accessed
15. Text-Files.pptx	9/23/2014 11:34:32...	PPTX File	1,703 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
A9-000-0013 Rev 1.2-FSU_us...	9/23/2014 11:34:32...	Chrome HTML ...	380 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
Action Plan (sample).pptx	9/23/2014 11:34:32...	PPTX File	57 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
Dave's Thesis Proposal Templ...	9/23/2014 11:34:32...	DOC File	132 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
Docx4j_GettingStarted.docx	9/23/2014 11:34:32...	Office Open XM...	109 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
DwC Use Case - Environmenta...	9/23/2014 11:34:32...	XLSX File	53 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
easychair.docx	9/23/2014 11:34:32...	Office Open XM...	240 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
excel.xls	9/23/2014 11:34:32...	XLS File	21 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
Forensic_UltraDock_v5_user_...	9/23/2014 11:34:32...	Chrome HTML ...	1,316 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
imrtemplate.doc	9/23/2014 11:34:32...	DOC File	56 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
MxAgCrProd.ppt	9/23/2014 11:34:32...	PPT File	256 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
QTL_Sample_data.xls	9/23/2014 11:34:32...	XLS File	53 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
Sample - Superstore Sales (Ex...	9/23/2014 11:34:33...	XLS File	2,956 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
sample-sales-data.xls	9/23/2014 11:34:33...	XLS File	201 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
SAMPLELETTERS.docx	9/23/2014 11:34:33...	Office Open XM...	152 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
TaipeiKeynote.ppt	9/23/2014 11:34:33...	PPT File	383 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
text formula examples.xlsx	9/23/2014 11:34:33...	XLSX File	12 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
TorranceUGA.ppt	9/23/2014 11:34:33...	PPT File	150 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
UPN_Timetable04132014.pdf	9/23/2014 11:34:33...	Chrome HTML ...	794 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
word.doc	9/23/2014 11:34:33...	DOC File	24 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22
yawconlineSample.doc	9/23/2014 11:34:33...	DOC File	42 KB	11/3/2014 8:16:22 ...	11/3/2014 8:16:22

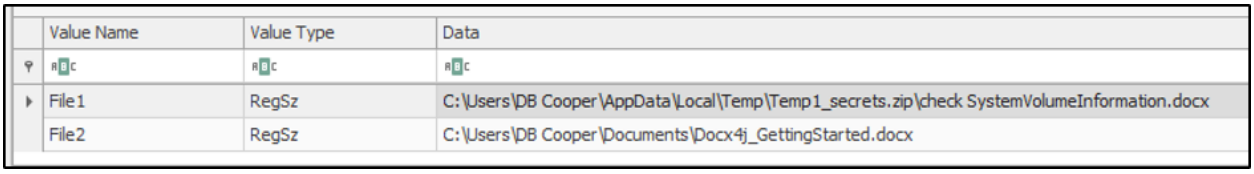
Encrypted Files

DB Cooper stored data in encrypted files (**Question 15**).

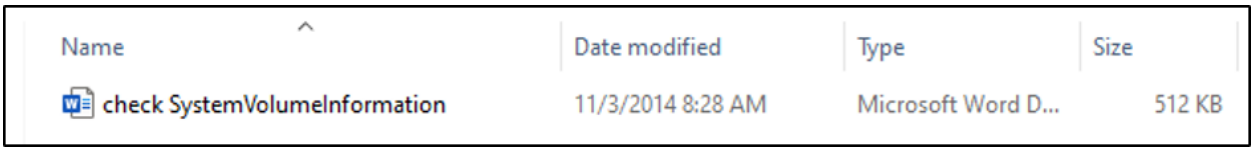
Autopsy shows suspected encrypted files:

Source Name	S	C	O	Source Type	Score	...	...	Justification
AgGlFaultHistory.db			1	File	Likely Notable			Suspected encryption due to high entropy (7.913463).
AgGlFgAppHistory.db			1	File	Likely Notable			Suspected encryption due to high entropy (7.888102).
AgGlGlobalHistory.db			1	File	Likely Notable			Suspected encryption due to high entropy (7.896992).
XboxMCX-V.XEX			2	File	Likely Notable			Suspected encryption due to high entropy (7.999667).
XboxMCX-V.XEX			2	File	Likely Notable			Suspected encryption due to high entropy (7.999667).
data			1	File	Likely Notable			Suspected encryption due to high entropy (7.999980).
win7_scenic-demoshort_raw.wtv			2	File	Likely Notable			Suspected encryption due to high entropy (7.638412).
win7_scenic-demoshort_raw.wtv			2	File	Likely Notable			Suspected encryption due to high entropy (7.638412).

One of the files accessed by DB Cooper on 11/03/214 using Wordpad was Temp1_secrets.zip. I was able to access the contents of that zip file to view the file check SystemVolumeInformation.docx. Following this pointer, using 7Zip, I found a file called checkpoint_docx in the System Volume Information directory. I exported that file but was unable to decrypt it with Veracrypt or Truecrypt (**Question 19 and 20**).



Value Name	Value Type	Data
File1	RegSz	C:\Users\DB Cooper\AppData\Local\Temp\Temp1_secrets.zip\check SystemVolumeInformation.docx
File2	RegSz	C:\Users\DB Cooper\Documents\Docx4j_GettingStarted.docx



Name	Date modified	Type	Size
check SystemVolumeInformation	11/3/2014 8:28 AM	Microsoft Word D...	512 KB

Findings and Conclusions

It is my conclusion, to a reasonable degree of certainty in my field of expertise that:

- DB Cooper stole money (see images) and used the laptop when planning where to hide with the money (Belize).
- He attempted to cover his digital footprint by deleting files with SDelete, downloading malware onto the computer, and changing the computer date and time.