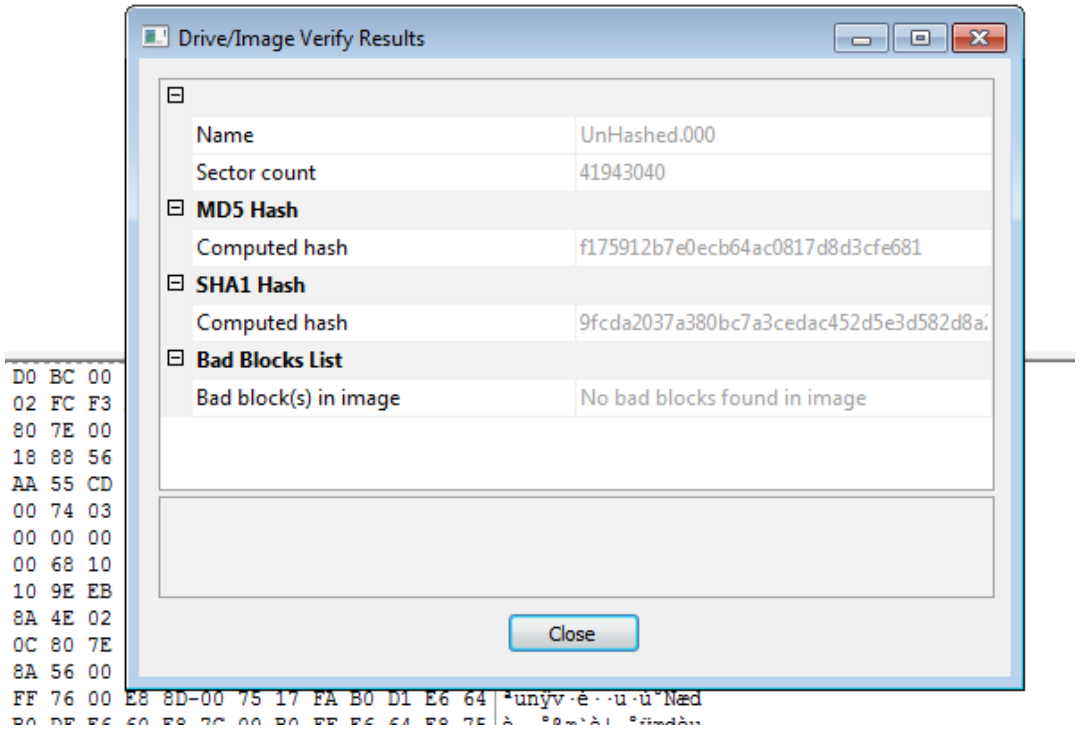
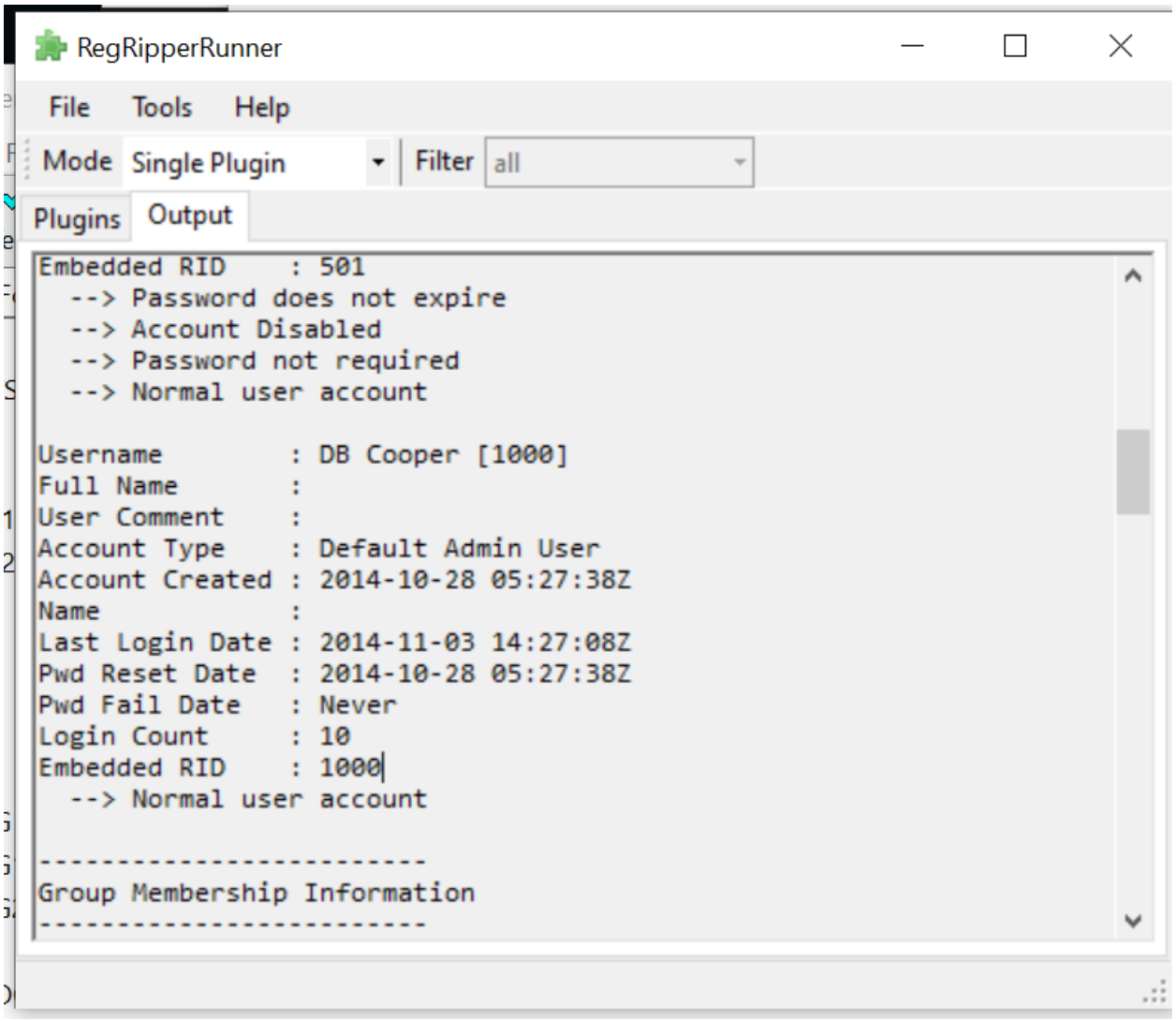
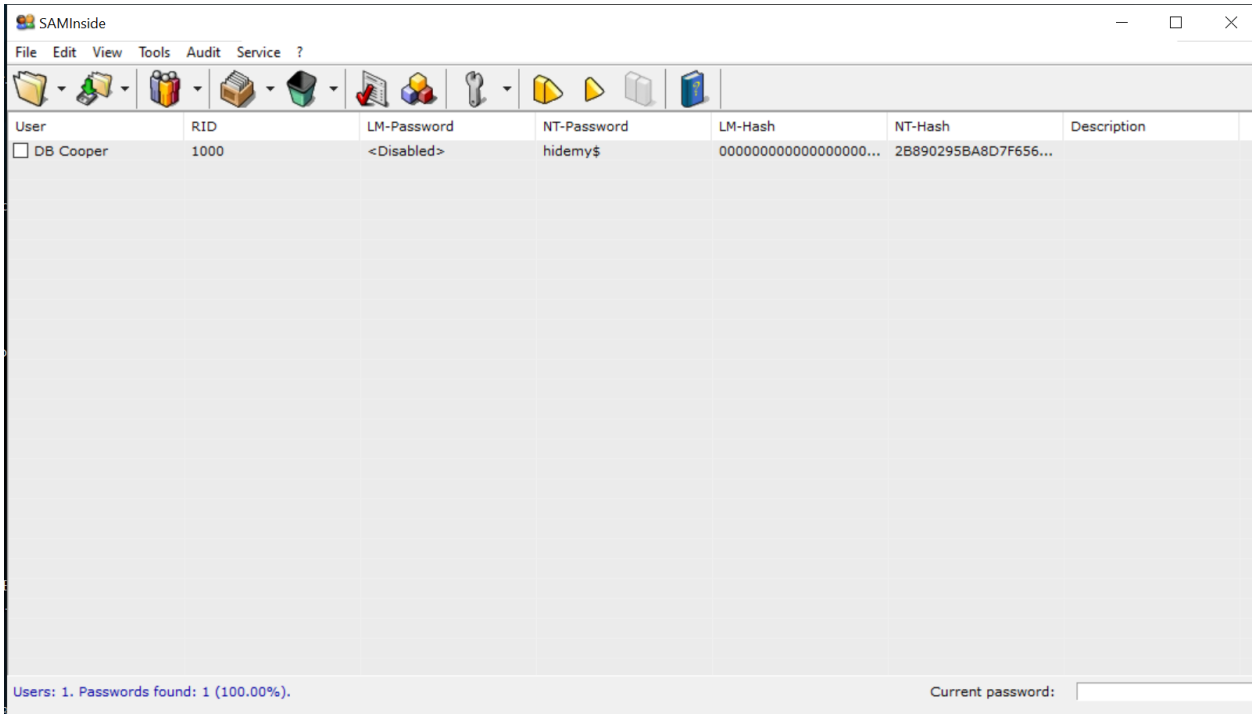
Bilal Anarwala
DB Cooper Lab

1. MD5 Hash
    a. The hash is f175912b7e0ecb64ac0817d8d3cfe681
    b. This hash was retrieved by imaging the contents of the DB Cooper Lab into a blank HDD using Paladin
        i. 

2. 

   a. The account name for the main user is DB Cooper
   b. This was gotten by using the SamParse plugin on RegRipper using the SAM file from the DB Cooper image

3. 

   a. Used SamInside to do a dictionary attack using the db cooper dictionary as well as the SAM and SYSTEM file from the DB Cooper lab image. The password is "hidemy$"

4.
```
File: C:\Users\Forensics User\Downloads\config\SOFTWARE

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
```

   a. The operating system is Windows 7 Ultimate
   b. The registered owner is "Windows User"
   c. This was gotten using RegRipperRunner on the config file that was extracted from the lab image
   d. Used regripper with the winver plugin to get this info

5. The operating system was installed on 11-30-2017

```
File: C:\Users\Forensics User\Downloads\config\SYSTEM

usbstor v.20200515
(System) Get USBStor key info

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
```

6.
   a. Yes there are two usb devices that were used on this computer. These two devices were both used on 11-03-2014. Got this using the usbstor plugin on regripper
   b. The serial numbers are
      i. 070B43740622B360&0
      ii. 2013070200000437&0
7. When it comes to finding the files accessed on it, I used the shellbags plugin on RegRipper to find that “secrets.zip” was used on the E drive (the USB).
   a.

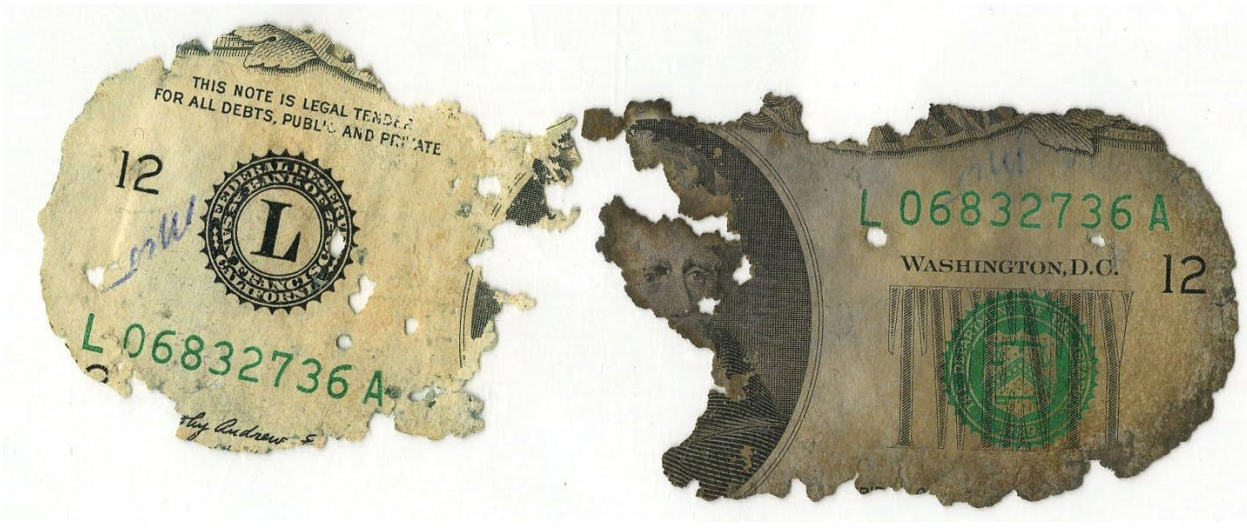
```
File: C:\Users\Forensics User\Downloads\UsrClass.dat

shellbags v.20200428
(USRCLASS.DAT) Shell/BagMRU traversal in Win7+ USRCLASS.DAT hives

MRU Time            |Modified            | Accessed            | Created             | Zip_Subfolder       | MFT File Ref |Resource
--------------------|--------------------|---------------------|---------------------|---------------------|--------------|------------
                    |                    |                     |                     |                     |              |Libraries [Desktop\0\]
                    |                    |                     |                     |                     |              |Libraries\CLSID_Documents Library [Desktop\0\0\]
2014-11-03 14:15:11 |                    |                     |                     |                     |              |Libraries\CLSID_Pictures [Desktop\0\1\]
                    |                    |                     |                     |                     |              |Control Panel [Desktop\1\]
2014-10-28 08:48:55 |                    |                     |                     |                     |              |Control Panel\System and Security [Desktop\1\0\]
                    |                    |                     |                     |                     |              |Control Panel\System and Security\CLSID_Backup
and Restore Center [Desktop\1\0\0\]
2014-10-28 08:50:17 |                    |                     |                     |                     |              |Control Panel\System and Security\CLSID_System
[Desktop\1\0\1\]
                    |                    |                     |                     |                     |              |My Computer [Desktop\2\]
                    |                    |                     |                     |                     |              |My Computer\C:\ [Desktop\2\0\]
2014-11-03 14:28:42 |                    |                     |                     |                     |              |My Computer\E:\ [Desktop\2\1\]
2014-11-03 14:28:55 |2014-10-31 16:11:14 | 2014-11-03 14:25:00 | 2014-11-03 14:25:00 |                     |              |My Computer\E:\secrets.zip [8714] [Desktop\2\1\0
\]
2014-11-03 14:33:12 |                    |                     |                     |                     |              |Users [Desktop\3\]
                    |                    |                     |                     |                     |              |Users\CLSID_Downloads [Desktop\3\0\]
2014-11-03 14:33:12 |                    |                     |                     |                     |              |Users\AppData [Desktop\3\1\]
2014-11-03 14:33:12 |                    |                     |                     |                     |              |Users\AppData\Local [Desktop\3\1\0\]
2014-11-03 14:33:12 |                    |                     |                     |                     |              |Users\AppData\Local\Microsoft [Desktop\3\1\0\0\]
2014-11-03 14:33:12 |                    |                     |                     |                     |              |Users\AppData\Local\Microsoft\Windows [Desktop\3
\1\0\0\0\]
2014-11-03 14:33:12 |                    |                     |                     |                     |              |Users\AppData\Local\Microsoft\Windows\Temporary
Internet Files [Desktop\3\1\0\0\0\0\]
2014-11-03 14:33:12 |                    |                     |                     |                     |              |Users\AppData\Local\Microsoft\Windows\Temporary
Internet Files\Low [Desktop\3\1\0\0\0\0\0\]
2014-11-03 14:33:12 |                    |                     |                     |                     |              |Users\AppData\Local\Microsoft\Windows\Temporary
Internet Files\Low\Content.IE5 [Desktop\3\1\0\0\0\0\0\0\]
2014-11-03 14:33:12 |                    |                     |                     |                     |              |Users\AppData\Local\Microsoft\Windows\Temporary
Internet Files\Low\Content.IE5\VSZDN07P [Desktop\3\1\0\0\0\0\0\0\0\]
2014-11-03 14:33:12 |                    |                     |                     |                     |              |Users\AppData\Local\Microsoft\Windows\Temporary
Internet Files\Low\Content.IE5\VSZDN07P\usback[1].zip [Desktop\3\1\0\0\0\0\0\0\0\0\]
```

8. Using PhotoRec filtering out PNG’s and JPEGs on the DB Cooper hard drive, it yielded these 4 photos.

a.


THIS NOTE IS LEGAL TENDER
FOR ALL DEBTS, PUBLIC AND PRIVATE
12
L
L 06832736 A
L 06832736 A
WASHINGTON, D.C.
12

b.

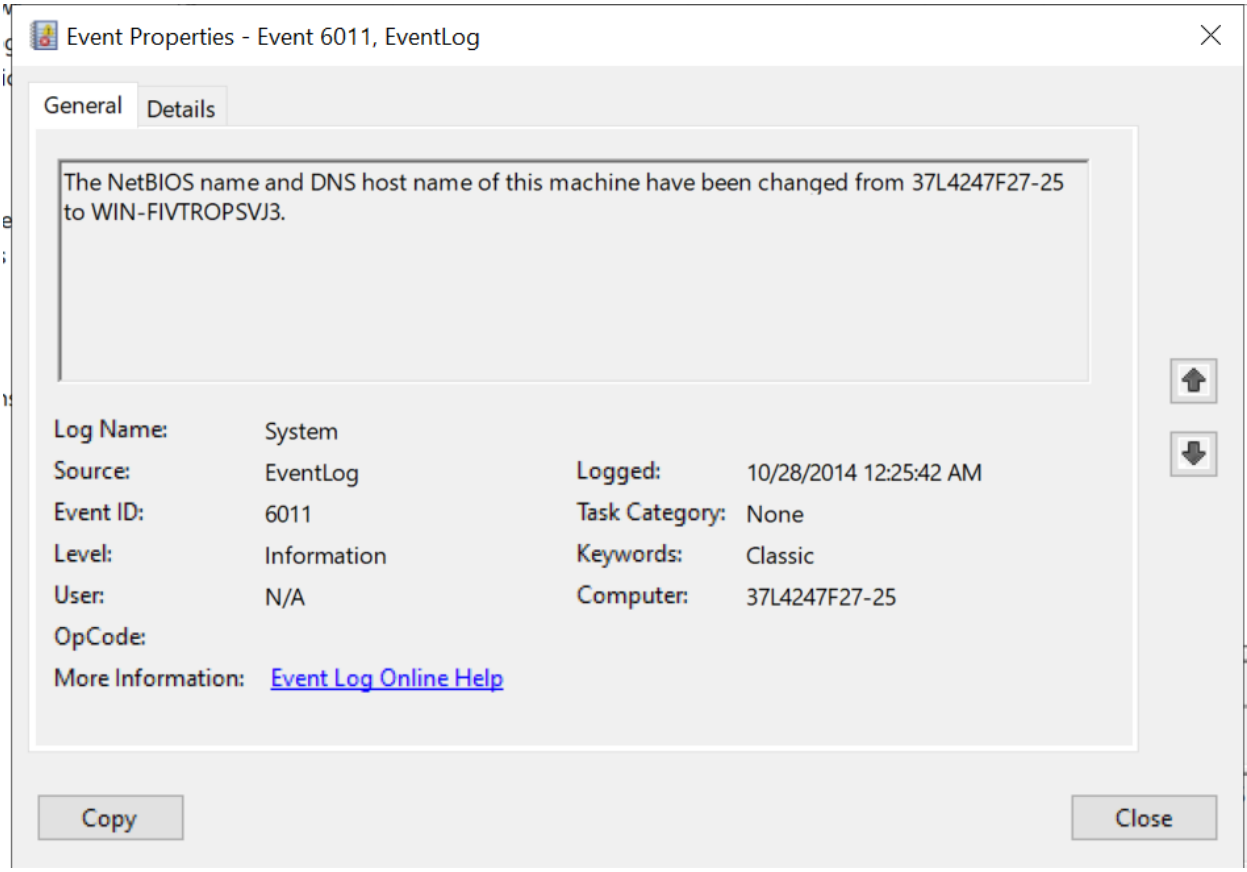

FOLLOW
THE MONEY

c. 

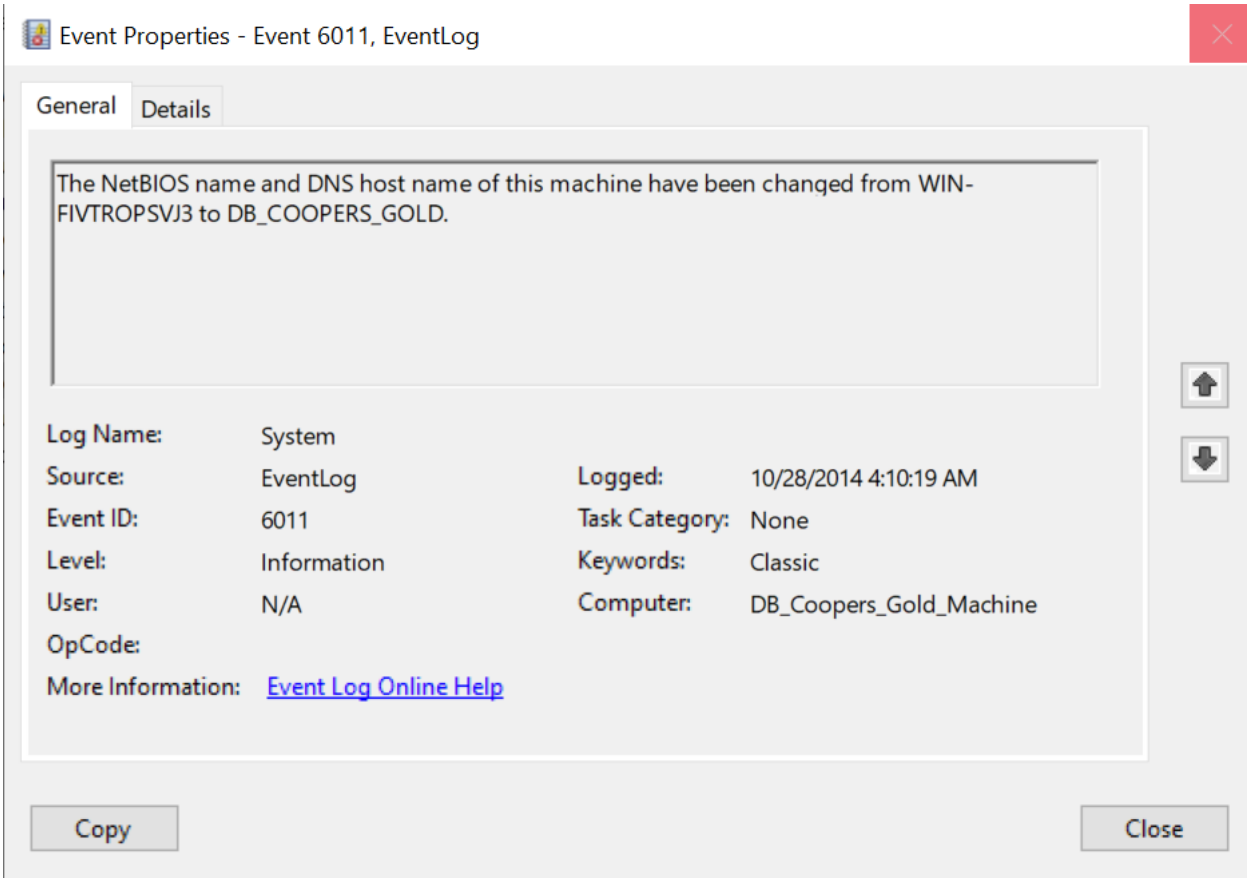
d. 

9. Using EventLog Explorer I was able to find out that the NETBIOS was initially changed to “WIN-FIVTROPSVJ3” and was subsequently changed to “DB_COOPERS_GOLD” Windows documentation pointed me to look for event ID 6011 which is there to log NETBIOS and DNS name changes.

a.

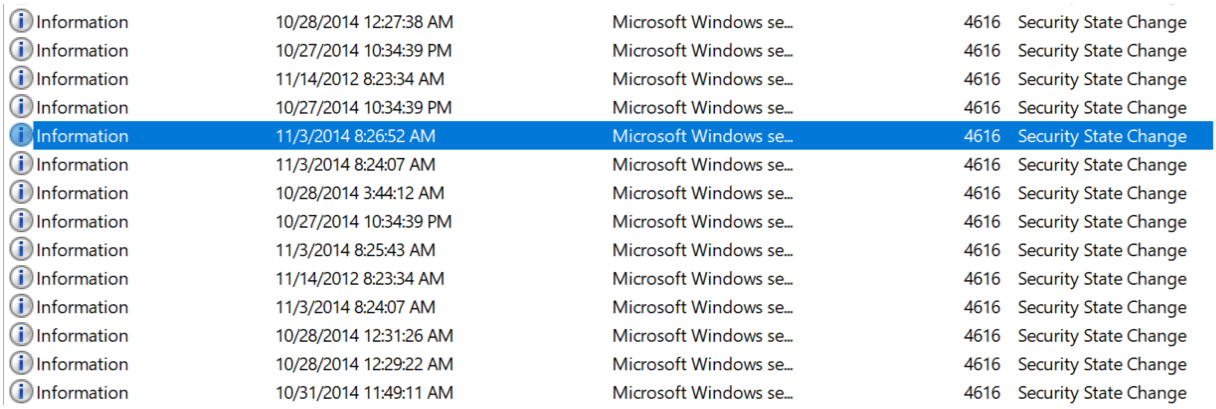

Event Properties - Event 6011, EventLog
General
Details
The NetBIOS name and DNS host name of this machine have been changed from 37L4247F27-25 to WIN-FIVTROPSVJ3.
Log Name: System
Source: EventLog
Logged: 10/28/2014 12:25:42 AM
Event ID: 6011
Task Category: None
Level: Information
Keywords: Classic
User: N/A
Computer: 37L4247F27-25
OpCode:
More Information: Event Log Online Help
Copy
Close

b.

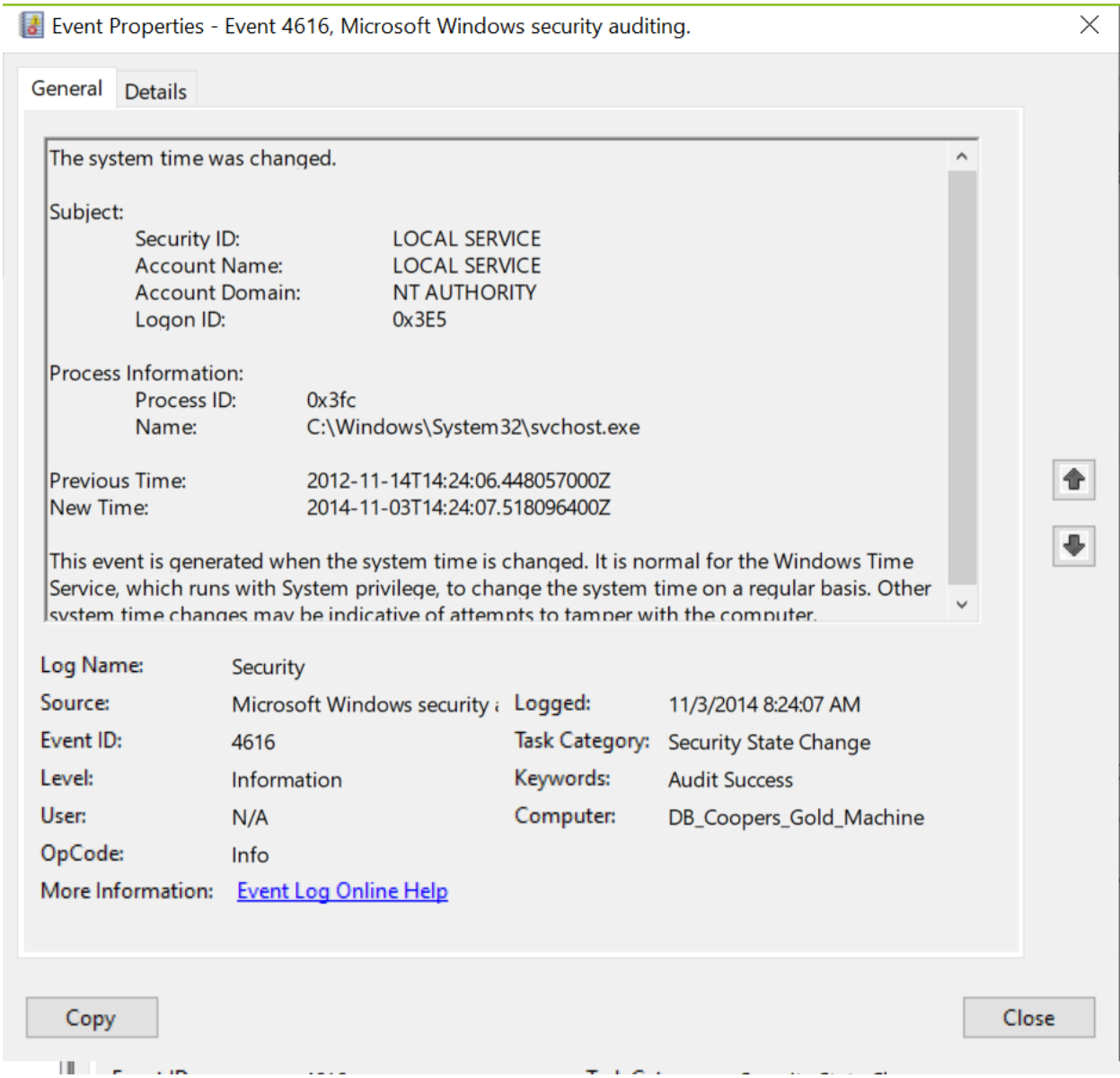


10. Within the security logs of the DB Cooper disk image, there were a handful of events within EventLog Explorer that indicated a time change. The biggest one is the time change from 11-14-2012 all the way to 11-3-2014. Just like the previous step, it was known (from a google search) that ID 4616 indicates a system time change so I knew what to look out for.

a.



Information	10/28/2014 12:27:38 AM	Microsoft Windows se...	4616	Security State Change
Information	10/27/2014 10:34:39 PM	Microsoft Windows se...	4616	Security State Change
Information	11/14/2012 8:23:34 AM	Microsoft Windows se...	4616	Security State Change
Information	10/27/2014 10:34:39 PM	Microsoft Windows se...	4616	Security State Change
Information	11/3/2014 8:26:52 AM	Microsoft Windows se...	4616	Security State Change
Information	11/3/2014 8:24:07 AM	Microsoft Windows se...	4616	Security State Change
Information	10/28/2014 3:44:12 AM	Microsoft Windows se...	4616	Security State Change
Information	10/27/2014 10:34:39 PM	Microsoft Windows se...	4616	Security State Change
Information	11/3/2014 8:25:43 AM	Microsoft Windows se...	4616	Security State Change
Information	11/14/2012 8:23:34 AM	Microsoft Windows se...	4616	Security State Change
Information	11/3/2014 8:24:07 AM	Microsoft Windows se...	4616	Security State Change
Information	10/28/2014 12:31:26 AM	Microsoft Windows se...	4616	Security State Change
Information	10/28/2014 12:29:22 AM	Microsoft Windows se...	4616	Security State Change
Information	10/31/2014 11:49:11 AM	Microsoft Windows se...	4616	Security State Change

b. 

11. Loading up the DB Cooper Timeline CSV into Timeline Explorer, I can see that there are two recent files that have been opened using Wordpad, “check SystemVolumeInformation.docx” as well as another file called “Docx4j_GettingStarted.docx”
    a. `File1: [REG_SZ] C:\Users\DB Cooper\Documents\Docx4j_GettingStarted.docx`
    b. `[REG_SZ] C:\Users\DB Cooper\AppData\Local\Temp\Temp1_secrets.zip\check SystemVolumeInformation.docx`
12. Using the web search feature on Autopsy, I can see that DB Cooper made a multitude of different searches. Examples include: “how to shred documents with sdelete”, “where to hide in belize”, “downloading a virus via dropbox”

a.

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				bing.com	chrome	Google Chrome	2014-11-03 08:20:28 CST	DB_Cooper_Lab.vmd
index.dat				google.com	how to shred documents with sdelete	Internet Explorer Analyzer	2014-11-03 14:30:23 CST	DB_Cooper_Lab.vmd
index.dat				google.com	where to hide in belize	Internet Explorer Analyzer	2014-11-03 14:29:54 CST	DB_Cooper_Lab.vmd
index.dat				google.com	dropbox.com	Internet Explorer Analyzer	2014-11-03 14:30:39 CST	DB_Cooper_Lab.vmd
index.dat				google.com	how to use truecrypt	Internet Explorer Analyzer	2014-11-03 14:29:44 CST	DB_Cooper_Lab.vmd
index.dat				google.com	where is db cooper now?	Internet Explorer Analyzer	2014-11-03 14:30:33 CST	DB_Cooper_Lab.vmd
index.dat				google.com	where to hide in belize	Internet Explorer Analyzer	2014-11-03 14:29:54 CST	DB_Cooper_Lab.vmd
index.dat				google.com	where is db cooper now?	Internet Explorer Analyzer	2014-11-03 14:30:33 CST	DB_Cooper_Lab.vmd
index.dat				bing.com	chrome	Internet Explorer Analyzer	2014-11-03 14:20:26 CST	DB_Cooper_Lab.vmd
index.dat				google.com	dropbox.com	Internet Explorer Analyzer	2014-11-03 14:30:39 CST	DB_Cooper_Lab.vmd
index.dat				google.com	how to shred documents with sdelete	Internet Explorer Analyzer	2014-11-03 14:30:23 CST	DB_Cooper_Lab.vmd
index.dat				google.com	how to use truecrypt	Internet Explorer Analyzer	2014-11-03 14:29:44 CST	DB_Cooper_Lab.vmd
index.dat				google.com	downloading a virus via dropbox	Internet Explorer Analyzer	2014-11-03 14:31:14 CST	DB_Cooper_Lab.vmd
index.dat				bing.com	chrome	Internet Explorer Analyzer	2014-11-03 14:20:26 CST	DB_Cooper_Lab.vmd
index.dat				google.com	where to hide in belize	Internet Explorer Analyzer	2014-11-03 14:29:54 CST	DB_Cooper_Lab.vmd
index.dat				google.com	where is db cooper now?	Internet Explorer Analyzer	2014-11-03 14:30:33 CST	DB_Cooper_Lab.vmd
index.dat				bing.com	chrome	Internet Explorer Analyzer	2014-11-03 14:20:26 CST	DB_Cooper_Lab.vmd
index.dat				google.com	dropbox.com	Internet Explorer Analyzer	2014-11-03 14:30:39 CST	DB_Cooper_Lab.vmd

13. Using the Web Downloads section of Autopsy, I can see that there were a total of 4 files that were downloaded.

a.

Web Downloads

Table | Thumbnail | Summary

Save Ta

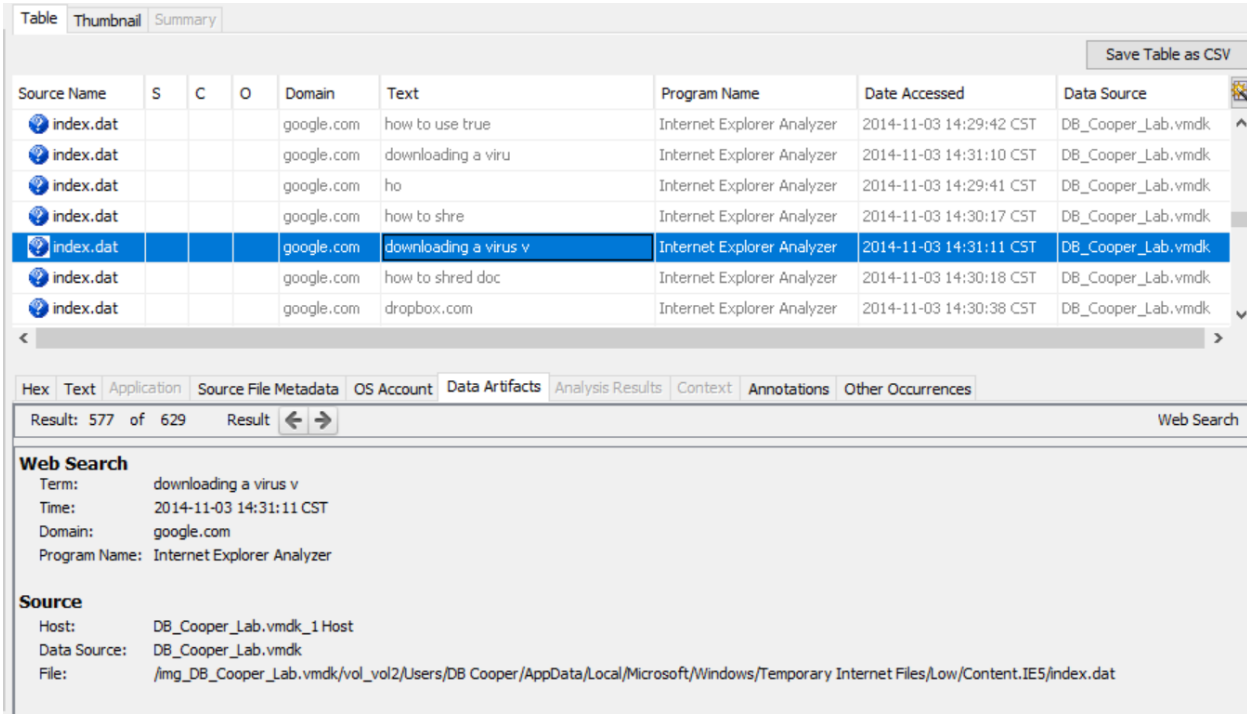
Source Name	S	C	O	Path	URL	Domain	Program Name	C
usback[1].zip:Zone.Identifier				/Users/DB Cooper/AppData/Local/Microsoft/Windows/Tem...				In
usback.exe:Zone.Identifier				/Users/DB Cooper/AppData/Roaming/usback.exe				In
IMG_3573.JPG:Zone.Identifier				/Users/DB Cooper/Downloads/IMG_3573.JPG				In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

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

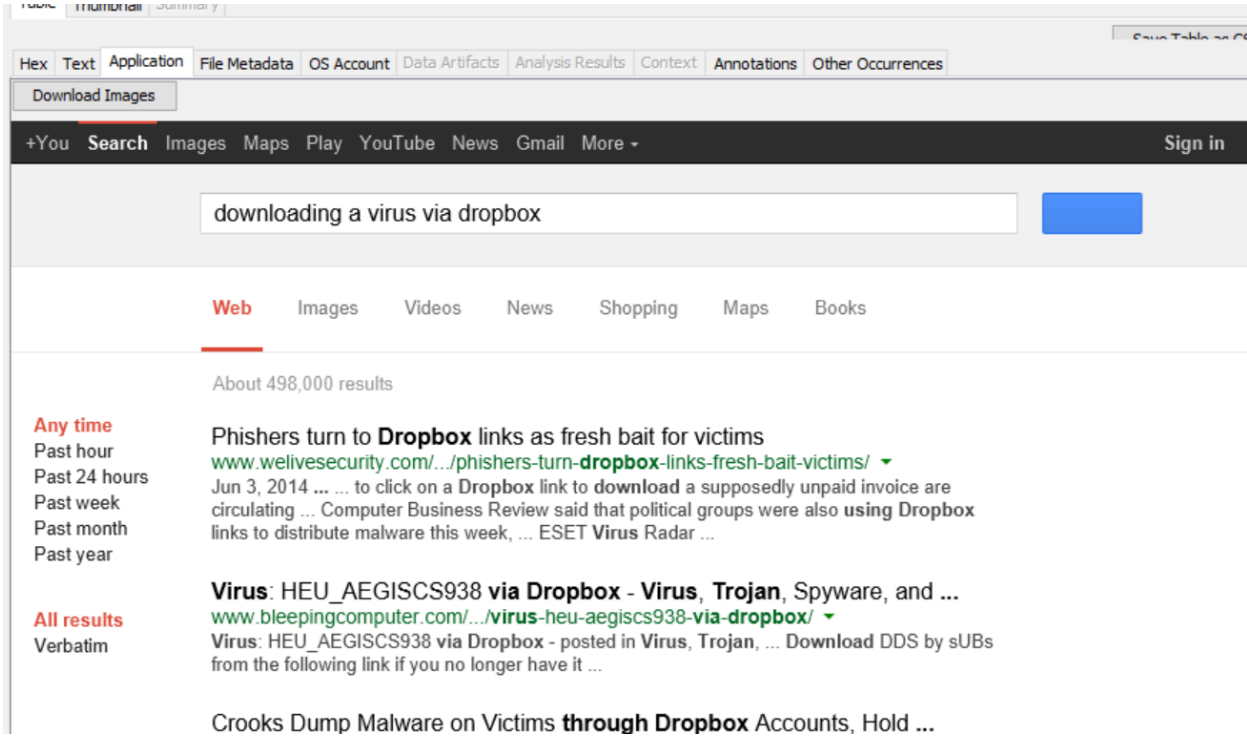
14. Going through DB Cooper's search history, there is a specific search that DB Cooper made on Google titled "downloading a virus" as well as "downloading a virus via dropbox". Looking through the websites visited during the date (11-03-2014) and around the time of the google search you find that Cooper visited a forum called

bleepingcomputer.com. Here you find a listing titled “Virus: HEU_AEGISCS938 via Dropbox " speaking of a virus called HEU AEGISCS**.** This got me searching his downloads within Autopsy and I found that there were 4 total web downloads that Cooper made. Within all of them, two of them were made during the same day that all of these searches were made. They were both the same file downloaded twice called “usback.exe” and “usback.zip”. It can be concluded that usback.exe is the virus due to this evidence.

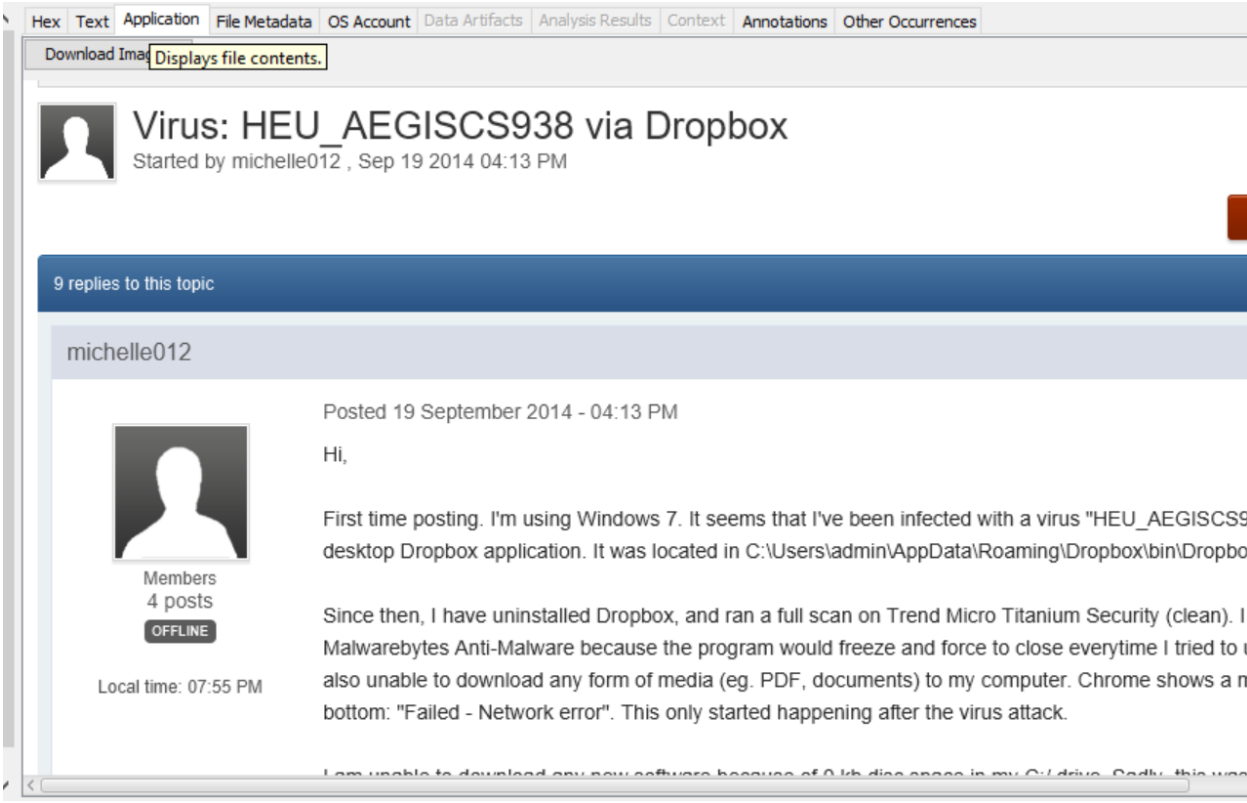
a.

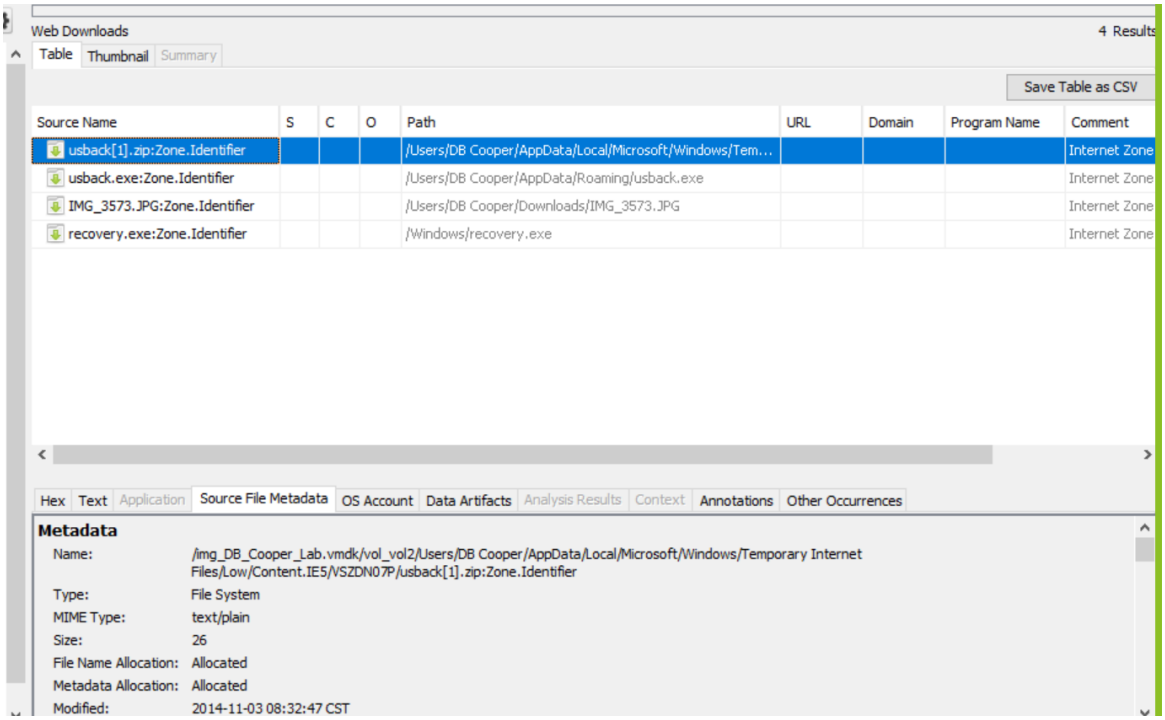


b.

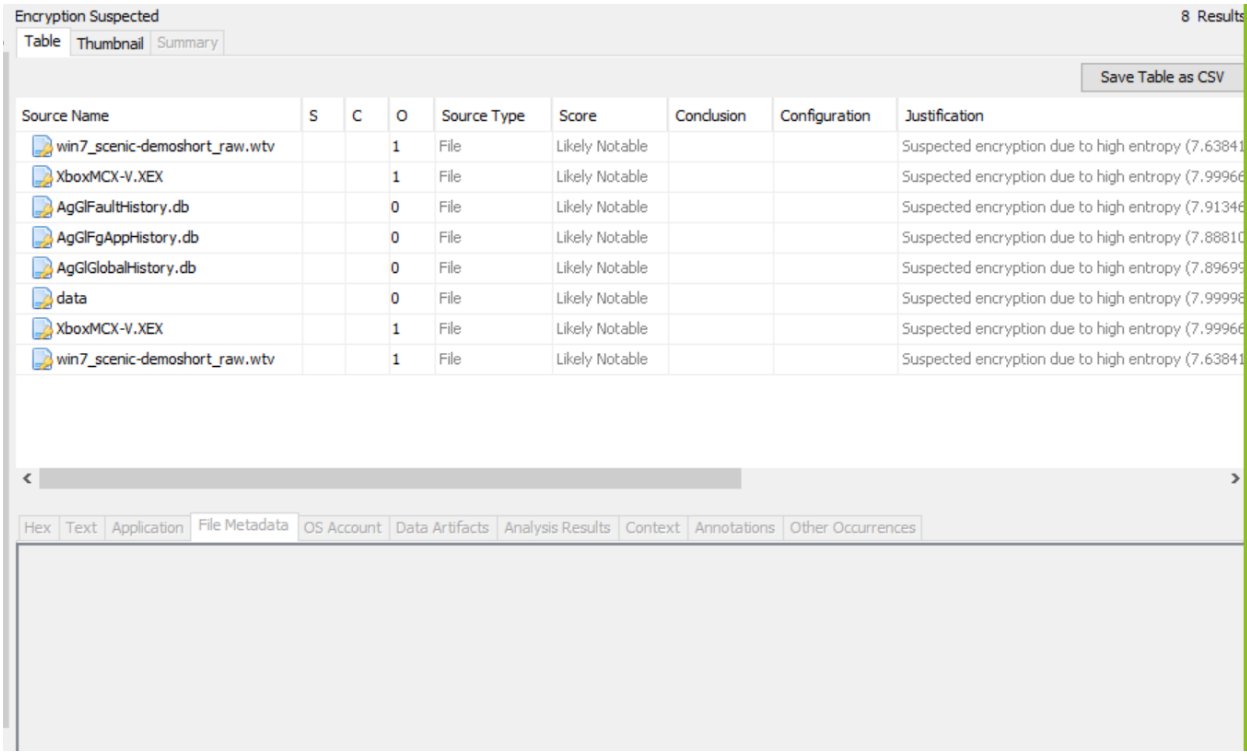

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Download Images
+You Search Images Maps Play YouTube News Gmail More
Sign in
downloading a virus via dropbox
Web Images Videos News Shopping Maps Books
About 498,000 results
Any time
Past hour
Past 24 hours
Past week
Past month
Past year
All results
Verbatim
Phishers turn to Dropbox links as fresh bait for victims
www.welivesecurity.com/.../phishers-turn-dropbox-links-fresh-bait-victims/
Jun 3, 2014 ... ... to click on a Dropbox link to download a supposedly unpaid invoice are circulating ... Computer Business Review said that political groups were also using Dropbox links to distribute malware this week, ... ESET Virus Radar ...
Virus: HEU_AEGISCS938 via Dropbox - Virus, Trojan, Spyware, and ...
www.bleepingcomputer.com/.../virus-heu-aegiscs938-via-dropbox/
Virus: HEU_AEGISCS938 via Dropbox - posted in Virus, Trojan, ... Download DDS by sUBs from the following link if you no longer have it ...
Crooks Dump Malware on Victims through Dropbox Accounts, Hold ...

c.

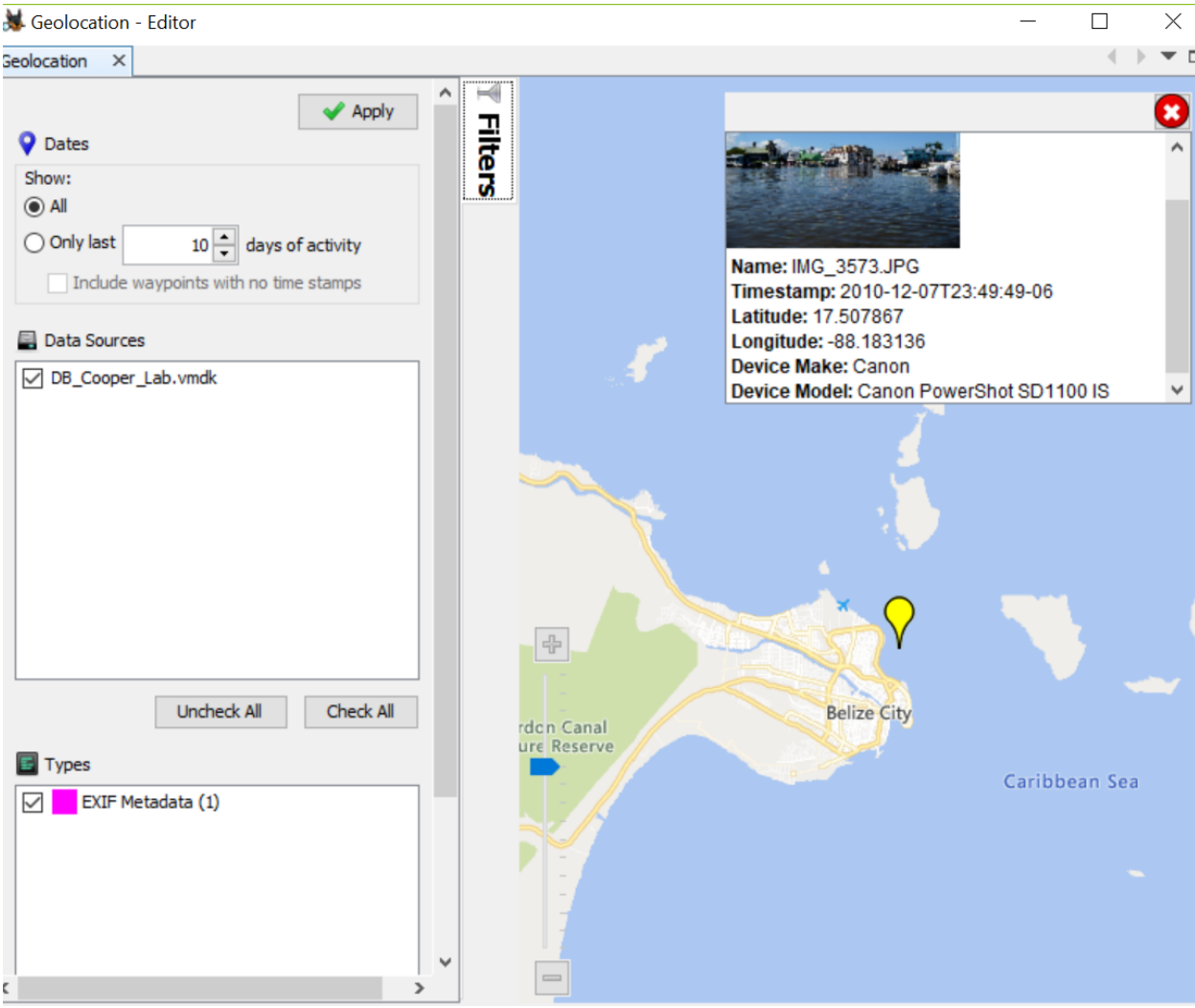

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Displays file contents.
Virus: HEU_AEGISCS938 via Dropbox
Started by michelle012 , Sep 19 2014 04:13 PM
9 replies to this topic
michelle012
Posted 19 September 2014 - 04:13 PM
Hi,
First time posting. I'm using Windows 7. It seems that I've been infected with a virus "HEU_AEGISCS9
desktop Dropbox application. It was located in C:\Users\admin\AppData\Roaming\Dropbox\bin\Dropbo
Since then, I have uninstalled Dropbox, and ran a full scan on Trend Micro Titanium Security (clean). I
Malwarebytes Anti-Malware because the program would freeze and force to close everytime I tried to
also unable to download any form of media (eg. PDF, documents) to my computer. Chrome shows a n
bottom: "Failed - Network error". This only started happening after the virus attack.
Members
4 posts
OFFLINE
Local time: 07:55 PM

d. 

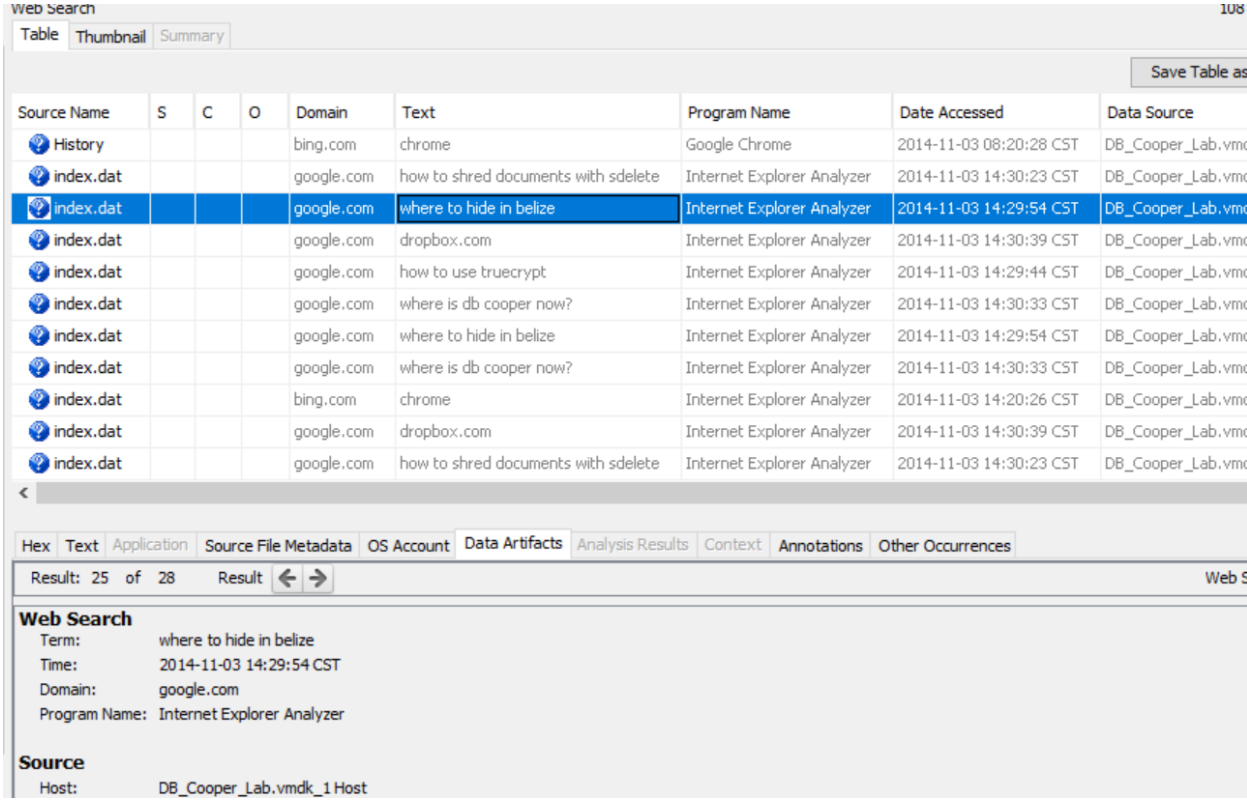
15. Yes there are. Within Autopsy, there is a section called “suspected encryption” that has a list of encrypted containers found within DB Cooper's laptop.

a. 

16. Using the Geolocation feature on autopsy, it finds a single image with metadata that is found in Belize. This tells us that DB Cooper is hiding somewhere in Belize. Also within DB Coopers’ search history, you can see a query titled “where to hide in Belize” backing the idea that Cooper is somewhere in Belize.

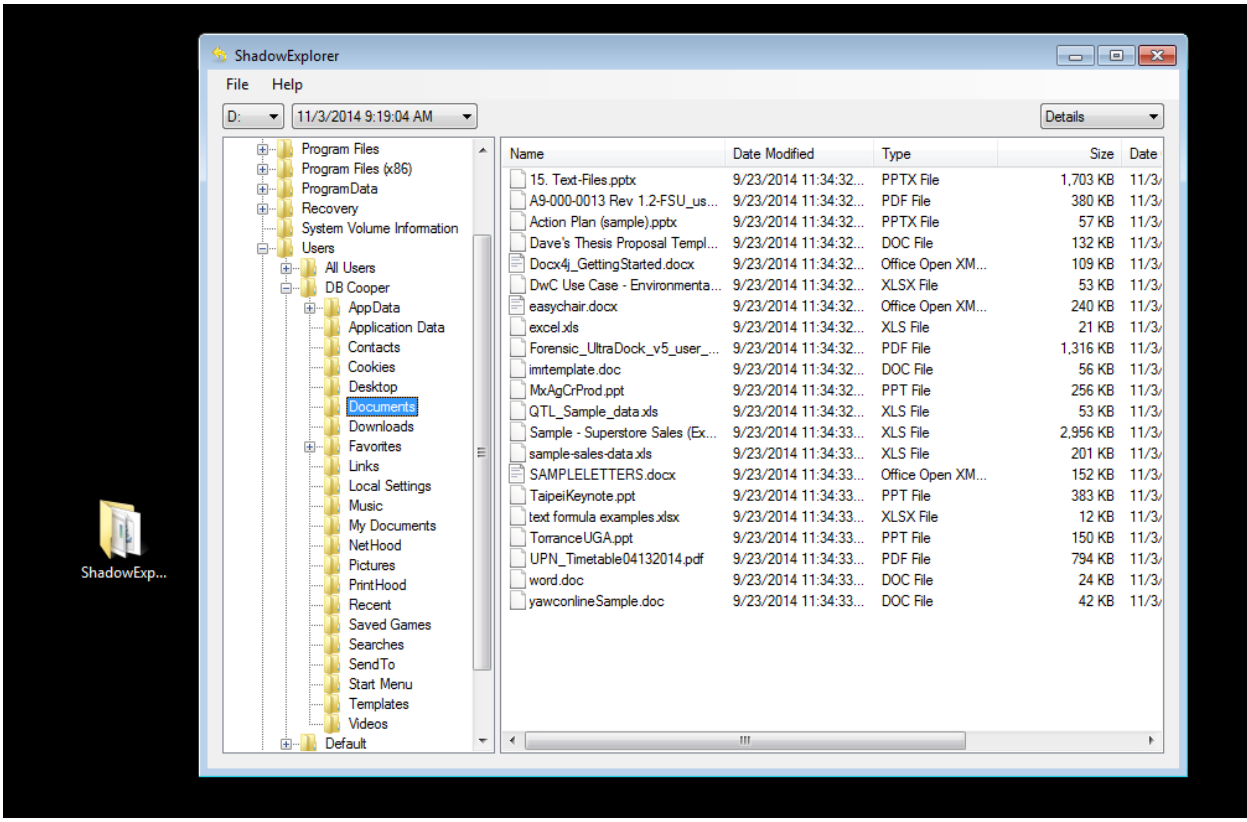
a. 
Geolocation - Editor
Geolocation
Apply
Dates
Show:
All
Only last
10
days of activity
Include waypoints with no time stamps
Data Sources
DB_Cooper_Lab.vmdk
Uncheck All
Check All
Types
EXIF Metadata (1)
Filters
Name: IMG_3573.JPG
Timestamp: 2010-12-07T23:49:49-06
Latitude: 17.507867
Longitude: -88.183136
Device Make: Canon
Device Model: Canon PowerShot SD1100 IS
Belize City
Caribbean Sea

b.



17. There are a handful of deleted documents that were found loading DB Cooper's hard drive using ShadowExplorer. Below is what was found. The names of these deleted files were also found within the logs of sdelete.

a.



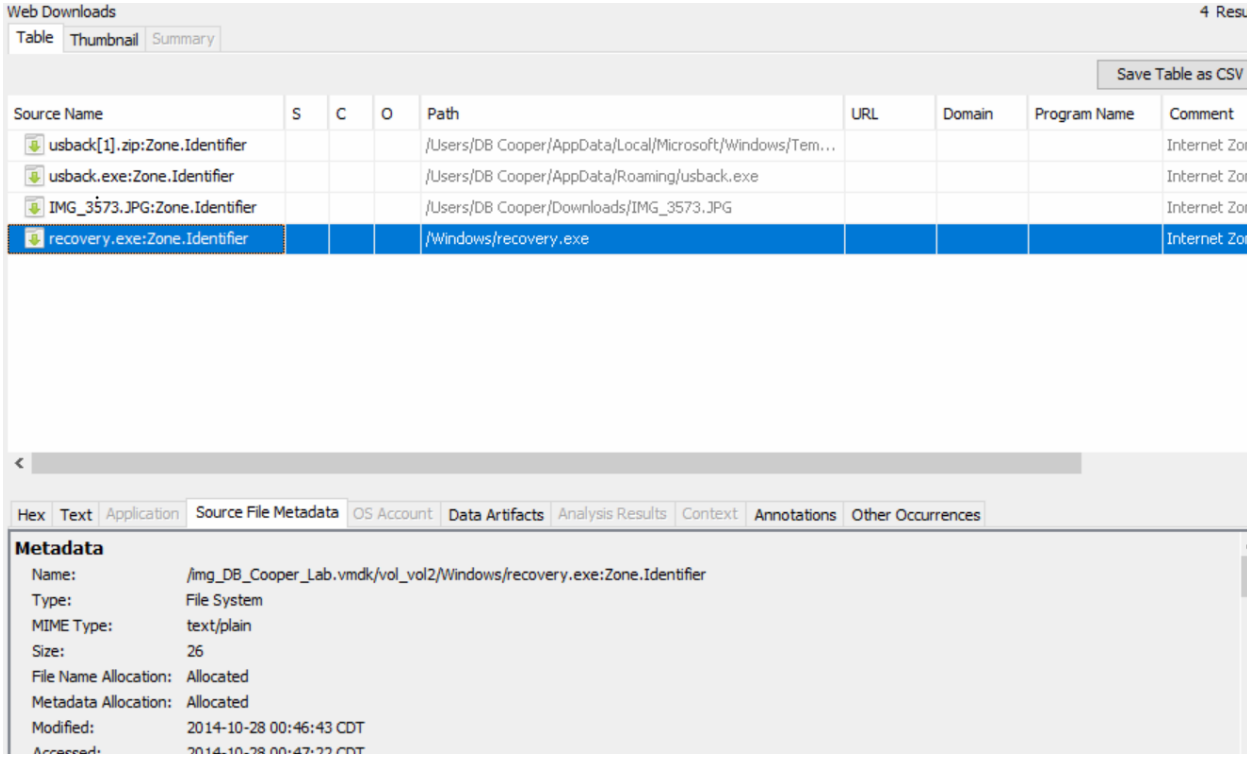
b.

\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\15. TEXT-FILES.PPTX
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\A9-000-0013 REV 1.2-FSU_USER_MANUAL.PDF
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\ACTION PLAN (SAMPLE).PPTX
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\DAVE'S THESIS PROPOSAL TEMPLATE_MSW04.DOC
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\DOCX4J_GETTINGSTARTED.DOCX
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\DWC USE CASE - ENVIRONMENTAL SAMPLE (EVENT).XLSX
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\EASYCHAIR.DOCX
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\EXCEL.XLS
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\FORENSIC_ULTRADOCK_V5_USER_MANUAL.PDF
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\IMRTEMPLATE.DOC
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\MXAGCRPROD.PPT
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\QTL_SAMPLE_DATA.XLS
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\SAMPLE - SUPERSTORE SALES (EXCEL).XLS
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\SAMPLE-SALES-DATA.XLS
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\SAMPLELETTERS.DOCX
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\TAIPEIKEYNOTE.PPT
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\TEXT FORMULA EXAMPLES.XLSX
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\TORRANCEUGA.PPT
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\UPN_TIMETABLE04132014.PDF
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\WORD.DOC
\DEVICE\HARDDISKVOLUME1\USERS\DB COOPER\DOCUMENTS\YAWCONLINESAMPLE.DOC

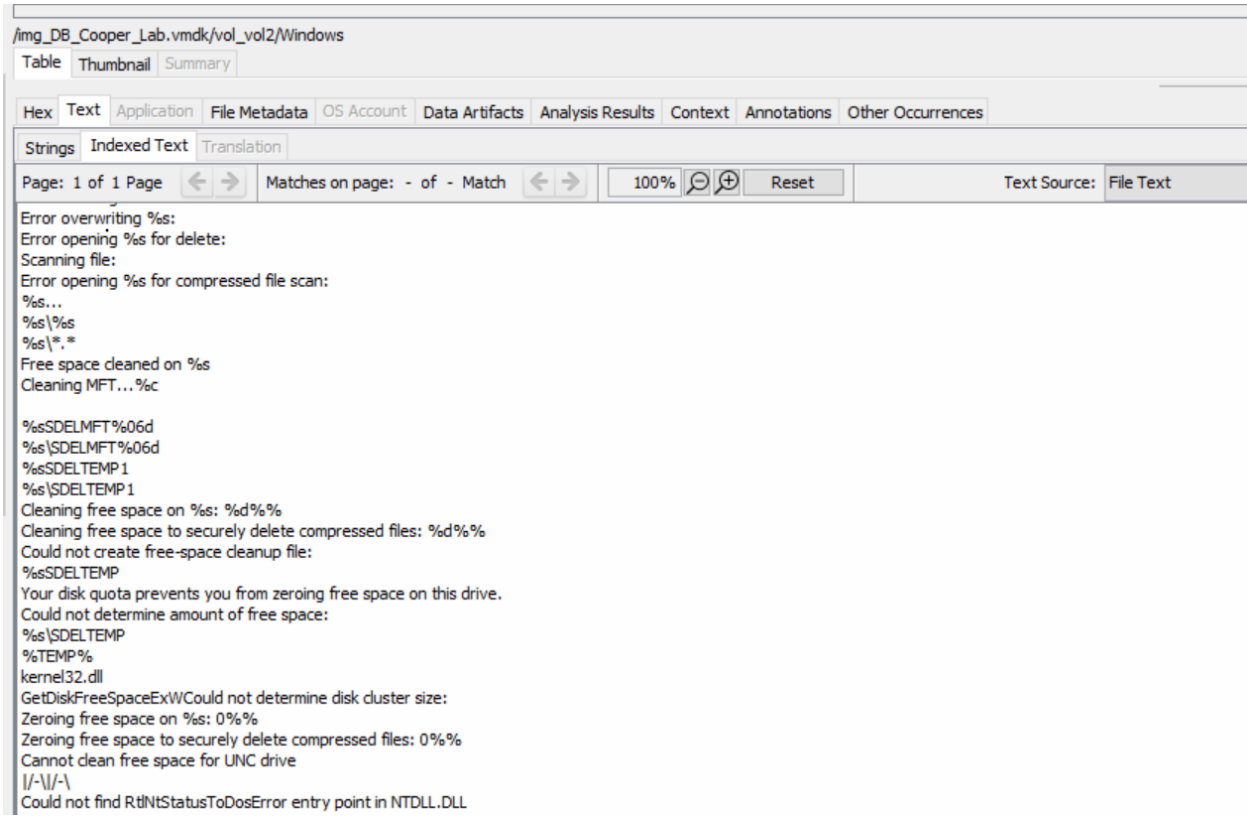
18. Checking DB Coopers search history, I can see that he made multiple Google searches on how to shred documents with one search stating “how to shred documents using sdelete” Checking the web downloads folder, there is one file named “recovery.exe” that was downloaded on 10-28-2014 which matches with the tip provided. When I navigate to Windows\recovery.exe you notice within the text of the file that it is actually sdelete and not recovery.exe. This tells us that Cooper most likely renamed the program to conceal the fact he was using sdelete. Finally, using the sysinterals plugin on RegRipper on the

ntuser.dat file from DB Cooper, it points out that sdelete is the scrubbing software used. By using ShadowExplorer, we can possibly get the deleted files back.

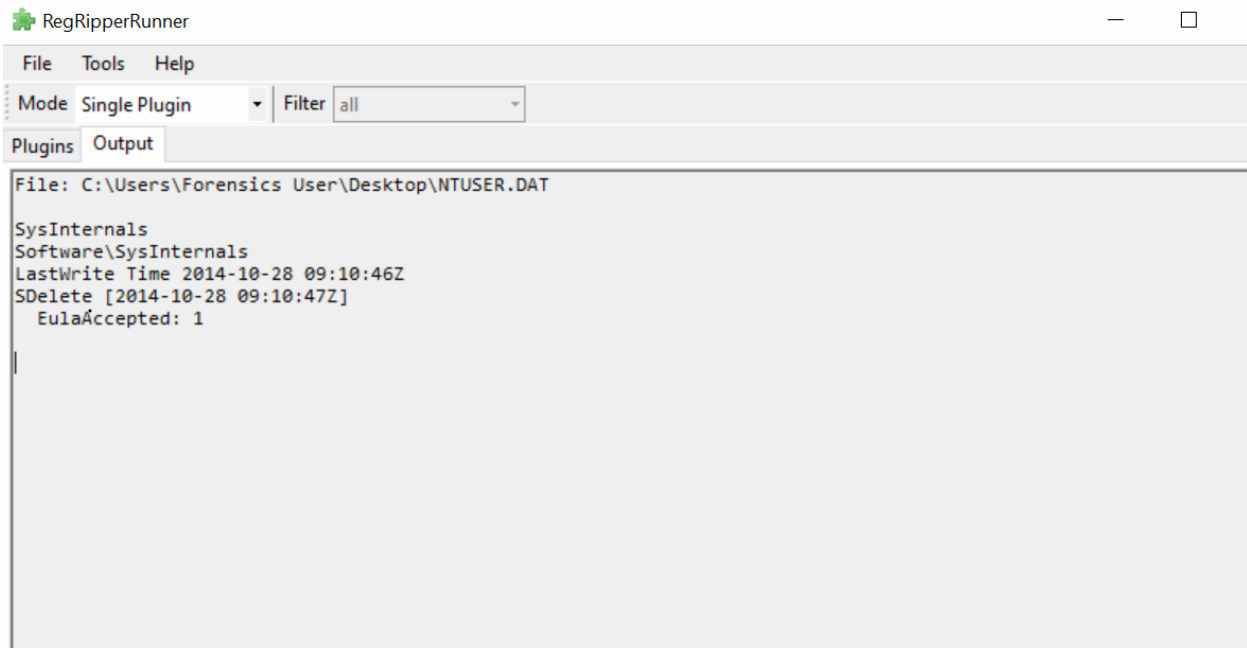
a.



b.

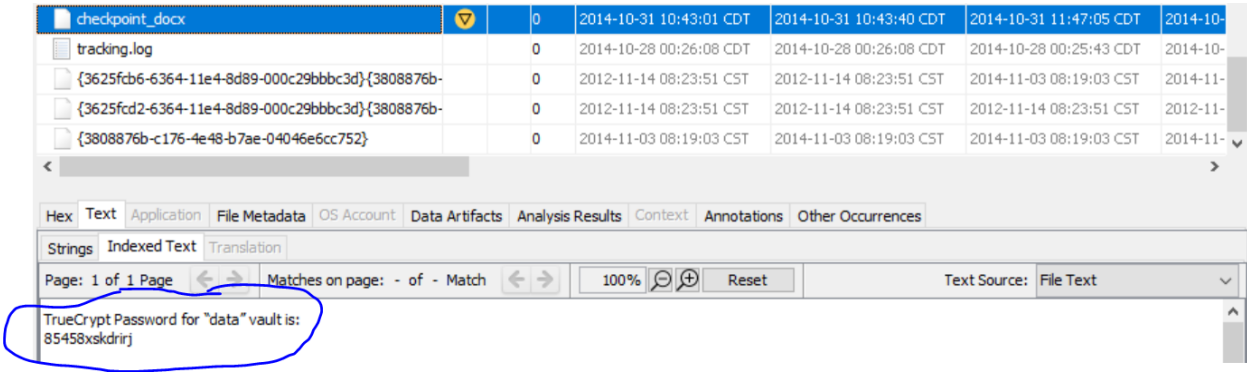


c.



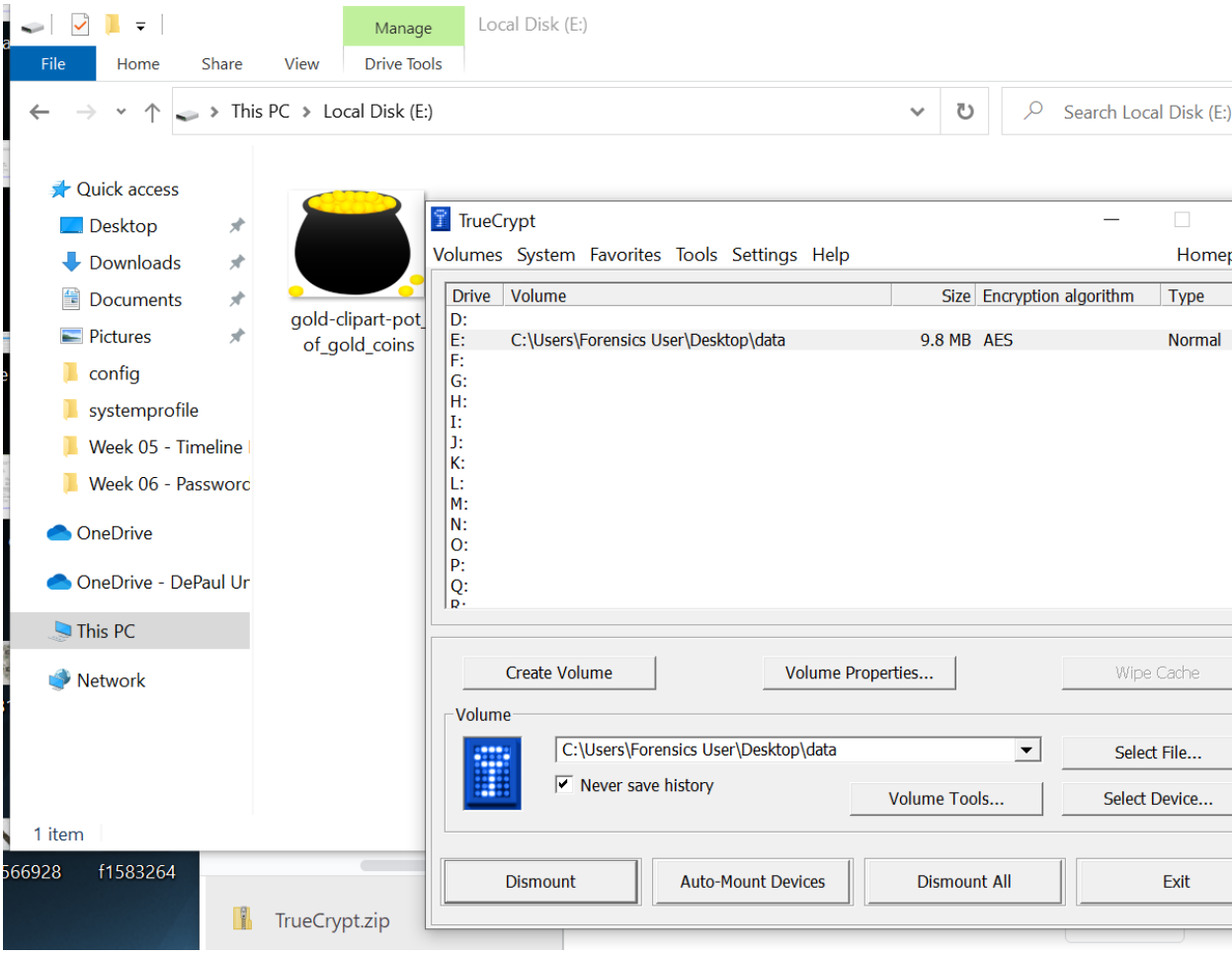
19. Hidden within SystemVolumeInformation in Autopsy is a file called “checkpoint_docx”, within this file lies the password for the TrueCrypt v7 container which is “85458xskdrirj”

a.



20. Knowing that I now had the password to the “data” file, I downloaded it onto my computer and mounted it with TrueCrypt. Using the supplied password, I was able to successfully mount the data container and it revealed the pot of gold

a.


Manage
Local Disk (E:)
File
Home
Share
View
Drive Tools
This PC
Local Disk (E:)
Search Local Disk (E:)
Quick access
Desktop
Downloads
Documents
Pictures
config
systemprofile
Week 05 - Timeline
Week 06 - Passworc
OneDrive
OneDrive - DePaul Ur
This PC
Network
gold-clipart-pot_of_gold_coins
1 item
566928
f1583264
TrueCrypt.zip
TrueCrypt
Volumes
System
Favorites
Tools
Settings
Help
Drive
Volume
Size
Encryption algorithm
Type
E:
C:\Users\Forensics User\Desktop\data
9.8 MB
AES
Normal
Create Volume
Volume Properties...
Wipe Cache
Volume
C:\Users\Forensics User\Desktop\data
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit