HR Forensic Solutions

DB Cooper Case

"Search for the treasure trove", an act well intended for this case in search of whereabouts of an individual named, DB Cooper. This case been a mystery for many years and only evidence to find clues is to delve meticulously into his Dell computer and conduct forensic analysis.

Prepared For: Professor Arlene Yetnikoff
DePaul University
(312) 362-5878

Prepared By: Helen Ramchandani
Examiner
(815) 540-5749

Date: February 9, 2021

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

Executive Summary

Background

An unidentified man, addressed as an alias named DB Cooper hijacked an aircraft, demanded ransom, and noted to be missing for many years. FBI investigations have been ongoing trying to locate this individual by interviewing many sources and receiving anonymous tips as to his possible whereabouts. One tip led to a retrieval of a Dell laptop belonging to DB Cooper. The laptop provides a source to obtain information, analyze raw data files, and extract artifacts to present as evidence.

Scope

Given the evidence, DB Cooper.vmdk file, this virtual disk file was uploaded to a VMware workstation and mounted to the DePaul Windows7 X 64 Forensic Workstation v3. In the forensic workstation, FTK Imager application was initiated to convert the “DB Cooper.vmdk” to an image file named, “newimage.E01”, an encase file format used by other forensic tools for analysis. In addition, backup files are kept on the host machine to ensure integrity of data and no compromised files created due to running of other application modules.

Materials Reviewed and Considered

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

Image Name	Description	MD5 Hash
DB Cooper Lab Image	Given .vmdk file, convert to encase format	f175912b7e0ecb64ac0817d8d3cfe681

Unless specifically noted, all references to dates and times in this report have been converted to Central Standard Time (UTC/GMT -6 hours). The forensic image referenced above were analyzed with FTK Imager, Registry Explorer, RegRipperRunner with plugins, Zimmerman's tools particularly evaluating the Timeline Explorer, PhotoRec, Autopsy and various opensource utilities.

Findings and Conclusions

Overview

The recovery of the data from DB Cooper's laptop involved executing many forensics tools, extracting files to produce artifacts pertinent to understanding his whereabouts.

Forensics Imaging/Data Collection

A handy tool for obtaining information and conducting forensic analysis is use of FTK imager. The file, "DB Cooper.vmdk" was uploaded to FTK imager to obtain MD5 and SHA1 hash of the image and snapshot presented below.

```
:reated By AccessData® FTK® Imager 4.2.0.13

:ase Information:
\cquired using: ADI4.2.0.13
:ase Number: DBCooper1
:vidence Number: 0125
Jnique description: Browse
:xaminer: HKR
Notes:

--------------------------------------------------------------

Information for C:\Users\Examiner\Results_output:

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

Image Information:
Acquisition started:   Mon Jan 25 17:10:01 2021
Acquisition finished:  Mon Jan 25 17:23:10 2021
Segment list:
 C:\Users\Examiner\Results_output.E01

Image Verification Results:
Verification started:  Mon Jan 25 17:23:10 2021
Verification finished: Mon Jan 25 17:27:29 2021
MD5 checksum:    f175912b7e0ecb64ac0817d8d3cfe681 : verified
SHA1 checksum:   9fcda2037a380bc7a3cedac452d5e3d582d8a2b0 : verified
SSSSSSSSSSS
```

Filesystem Analysis

Once encase format file retrieved, FTK Imager was used to extract information from the following registry hives such as NTUSER.DAT, SAM, SOFTWARE, SYSTEM. Each hive consists of tables storing data in NTFS file system. Registry Explorer tool was useful to upload the mention hives and peruse the registry files at system level. In addition, another helpful tool, RegRipperRunner with plugins was implemented to extract information in form of metadata, easier format to view data. This tool was used to obtain the DB Cooper's user account details.

```
Username        : DB Cooper [1000]
SID             : S-1-5-21-4132869336-1819149309-2426677690-1000
```

```
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Tue Oct 28 05:27:38 2014 Z
Name            :
Last Login Date : Mon Nov  3 14:27:08 2014 Z
Pwd Reset Date  : Tue Oct 28 05:27:38 2014 Z
Pwd Fail Date   : Never
Login Count     : 10
  --> Normal user account


Group Name    : Administrators [2]
LastWrite     : Tue Oct 28 05:27:38 2014 Z
Group Comment : Administrators have complete and unrestricted access to the computer/domain
Users :
  S-1-5-21-4132869336-1819149309-2426677690-500
  S-1-5-21-4132869336-1819149309-2426677690-1000
```

Note: Interestingly, the main user profile was set as default admin user allowing easy access to computer resources involving file system registries and directories.

RegRipper with plugin tool was used to obtain operating system information as well as install date.

```
   File: C:\Users\Examiner\Desktop\dbc\SOFTWARE

winver v.20081210
(Software) Get Windows version

ProductName = Windows 7 Ultimate
CSDVersion  = Service Pack 1
InstallDate = Thu Nov 30 23:59:59 2017
```

The registered owner belongs to “DB_Cooper_Gold”, data retrieved through Autopsy tool and documented as follows:

Result: 9 of 9 Result Operating System Informati

Type	Value	Source(s)
Name	DB_COOPERS_GOLD	Recent Activity
Domain		Recent Activity
Version	Windows_NT	Recent Activity
Processor Architecture	AMD64	Recent Activity
Temporary Files Directory	%SystemRoot%\TEMP	Recent Activity
Source File Path	/img_DB_Cooper_Lab.vmdk/vol_vol2/Windows/System32/config/SYSTEM	
Artifact ID	-9223372036854771910	

The install date of operating system,

```
File: C:\Users\Examiner\Desktop\dbc\SOFTWARE

winver v.20081210

InstallDate = Thu Nov 30 23:59:59 2017
```

One interesting point to note: the install date (November 30, 2017) is different than the date DB Cooper accessed his computer, the account date created was October 28, 2014 as highlighted above. The date difference indicates once DB Cooper completed his mission, his computer was set to factory settings, thus “InstallDate” of November 30, 2017 23:59:59.

Forensic Timeline Analysis

Obtaining a forensic timeline is important to establish and understand the events occurred in a structured format. To obtain a timeline, Plaso tool was used to parse artifacts on an image. However, there are three components to constructing a timeline, “log2timeline.exe”, “pinfo.exe”, and “psort.exe”. Due to the increase processing power, the (.plaso) file was obtained by Professor Arlene. Initiating the pinfo.exe command followed by the psort.exe command, resulted in a timeline, the data was transferred to a desirable output file (dbplasout.csv) for analysis. Running Zimmerman’s Timeline Explorer tool, accepts the file, “dbplasout.csv” file and outputs a timeline for review.

Executing Zimmerman’s Timeline Explorer tool was useful in viewing a concise timeline, filtering certain dates, and noting modified times to understand sequence of events.

Internet History Analysis

An important part of an investigation is to view web history providing a plethora of information. Using Autopsy forensic tool, under the “Extract Content” folder, an option called “Web

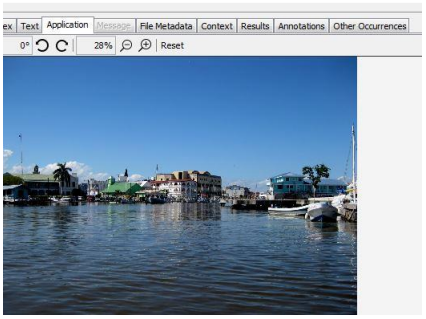
Searches” showed domains visited by Mr. Cooper using Internet Explorer browser.

History	www.bing.com	chrome	Chrome	2014-11-03 08:20:28 CST
index.dat	www.google.com	how to shred documents with sdelete	Internet Explorer	2014-11-03 14:30:23 CST
index.dat	www.google.com	where to hide in belize	Internet Explorer	2014-11-03 14:29:54 CST
index.dat	www.google.com	dropbox.com	Internet Explorer	2014-11-03 14:30:39 CST
index.dat	www.google.com	how to use truecrypt	Internet Explorer	2014-11-03 14:29:44 CST
index.dat	www.google.com	where is db cooper now?	Internet Explorer	2014-11-03 14:30:33 CST
index.dat	www.google.com	where to hide in belize	Internet Explorer	2014-11-03 14:29:54 CST
index.dat	www.google.com	where is db cooper now?	Internet Explorer	2014-11-03 14:30:33 CST
index.dat	www.bing.com	chrome	Internet Explorer	2014-11-03 14:20:26 CST
index.dat	www.google.com	dropbox.com	Internet Explorer	2014-11-03 14:30:39 CST
index.dat	www.google.com	how to shred documents with sdelete	Internet Explorer	2014-11-03 14:30:23 CST
index.dat	www.google.com	how to use truecrypt	Internet Explorer	2014-11-03 14:29:44 CST
index.dat	www.google.com	downloading a virus via dropbox	Internet Explorer	2014-11-03 14:31:14 CST
index.dat	www.bing.com	chrome	Internet Explorer	2014-11-03 14:20:26 CST

DB Cooper made many google searches and are the following: “How to shred documents with sdelete”, “where to hide in belize”, “dropbox.com”, “how to use truecrypt”, “where is db cooper now?”, and “downloading a virus via dropbox”. These web searches provide clues to his intentions and whereabouts.

Further clues were found on Mr. Cooper’s computer and retrieved as artifacts.

Executing Autopsy tool and viewing the EXIF metadata option, there was a file named, “IMG_3573.jpg” (picture shown below) followed by detailed information of latitude (17.507867) and longitude (-88.183136) coordinates suggesting location of Belize. Perhaps, this may be the location where DB Cooper is hiding. He made web searches using Google to search for “where to hide in Belize”.



Source File	S	C	O	Date Created	Latitude	Longitude	Device Model	Device Make	Data Source	Size	Path
IMG_3573.JPG			1	2010-12-07 23:49:49 CST	17.507867	-88.183136	Canon PowerShot SD1100 IS	Canon	DB_Cooper_Lab.vmdk	218430	/img_DB_Cooper_Lab.vmdk/vol_vol2/Users/DB Cooper/Downloads/IMG_3573.JPG

Accessing Autopsy forensic tool, I was able to retrieve an artifact relating to communication tools such as Document Writer, fax, Foxit Phantom PDF printer, and EverNote, to name a few. This suggests DB Cooper has some means of communication via the mediums listed below.

rag a column header here to group by that column

Value Name	Value Type	Data	Value Slack
Microsoft XPS Document Writer	RegSz	winspool,Ne00:	14-00-3F-00-0F-00
Fax	RegSz	winspool,Ne01:	00-00-00-00-00-00
NPI843346 (HP Color LaserJet CM2320nf MFP)#:2	RegSz	winspool,TPVM:	00-00-63-65-00-00
Fax#:5	RegSz	winspool,TPVM:	72-00-00-00-00-00
Foxit PhantomPDF Printer#:4	RegSz	winspool,TPVM:	64-69-61-33-33-34
Microsoft XPS Document Writer#:3	RegSz	winspool,TPVM:	6F-00-6F-00-6C-00
Print to Evernote#:1	RegSz	winspool,TPVM:	3A-31-00-00-00-00

Further evidence reveals DB Cooper had many encrypted files stored in containers. To view the files, Autopsy forensic tool was executed, selected the option “Encryption Suspected” tab under “Extracted Content” directory. There are nine encrypted entries consisting of databases, audio file formats, and data.

Table Thumbnail

Source File	S	C	O	Comment	Data Source
win7_scenic-demoshort_raw.wtv			2	Suspected encryption due to high entropy (7.638412).	DB_Cooper_Lab.vmdk
win7_scenic-demoshort_raw.wtv			2	Suspected encryption due to high entropy (7.638412).	DB_Cooper_Lab.vmdk
AgGlFgAppHistory.db			1	Suspected encryption due to high entropy (7.888102).	DB_Cooper_Lab.vmdk
AgGlFaultHistory.db			1	Suspected encryption due to high entropy (7.913463).	DB_Cooper_Lab.vmdk
AgGlGlobalHistory.db			1	Suspected encryption due to high entropy (7.896992).	DB_Cooper_Lab.vmdk
data			1	Suspected encryption due to high entropy (7.999980).	DB_Cooper_Lab.vmdk
XboxMCX-V.XEX			1	Suspected encryption due to high entropy (7.999667).	DB_Cooper_Lab.vmdk
win7_scenic-demoshort_raw.wtv			2	Suspected encryption due to high entropy (7.638412).	DB_Cooper_Lab.vmdk
XboxMCX-V.XEX			1	Suspected encryption due to high entropy (7.999667).	DB_Cooper_Lab.vmdk

In addition, there are many recovered deleted (system as well as application) files initiated by DB Cooper. Running Autopsy forensic tool, viewing the diagnostics there are many files (.docx, .doc, .xlsx, .ppt, .pptx, …) deleted, however, running “shadowcopyview-x64”, the once deleted files can be retrieved as seen below.

\Users\DB Cooper\Documents

Filename	Modified Time	Created Time	Entry Modified Time	File Size	Attributes	File Extension
15. Text-Files.pptx	9/23/2014 11:34:32...	11/3/2014 8:16:22 ...	9/23/2014 11:34:32...	1,743,039	A	pptx
A9-000-0013 Rev 1.2-FSU_user_man...	9/23/2014 11:34:32...	11/3/2014 8:16:22 ...	9/23/2014 11:34:32...	388,596	A	pdf
Action Plan (sample).pptx	9/23/2014 11:34:32...	11/3/2014 8:16:22 ...	9/23/2014 11:34:32...	57,947	A	pptx
Dave's Thesis Proposal Template_...	9/23/2014 11:34:32...	11/3/2014 8:16:22 ...	9/23/2014 11:34:32...	134,656	A	doc
Docx4j_GettingStarted.docx	9/23/2014 11:34:32...	11/3/2014 8:16:22 ...	9/23/2014 11:34:32...	111,590	A	docx
DwC Use Case - Environmental Sa...	9/23/2014 11:34:32...	11/3/2014 8:16:22 ...	9/23/2014 11:34:32...	53,931	A	xlsx
easychair.docx	9/23/2014 11:34:32...	11/3/2014 8:16:22 ...	9/23/2014 11:34:32...	245,234	A	docx
excel.xls	9/23/2014 11:34:32...	11/3/2014 8:16:22 ...	9/23/2014 11:34:32...	20,992	A	xls
Forensic_UltraDock_v5_user_manua...	9/23/2014 11:34:32...	11/3/2014 8:16:22 ...	9/23/2014 11:34:32...	1,347,230	A	pdf
imrtemplate.doc	9/23/2014 11:34:32...	11/3/2014 8:16:22 ...	9/23/2014 11:34:32...	57,344	A	doc
MxAgCrProd.ppt	9/23/2014 11:34:32...	11/3/2014 8:16:22 ...	9/23/2014 11:34:32...	262,144	A	ppt
QTL_Sample_data.xls	9/23/2014 11:34:32...	11/3/2014 8:16:22 ...	9/23/2014 11:34:32...	54,272	A	xls
Sample - Superstore Sales (Excel).xls	9/23/2014 11:34:33...	11/3/2014 8:16:22 ...	9/23/2014 11:34:33...	3,026,944	A	xls
sample-sales-data.xls	9/23/2014 11:34:33...	11/3/2014 8:16:22 ...	9/23/2014 11:34:33...	205,824	A	xls
SAMPLELETTERS.docx	9/23/2014 11:34:33...	11/3/2014 8:16:22 ...	9/23/2014 11:34:33...	155,440	A	docx
TaipeiKeynote.ppt	9/23/2014 11:34:33...	11/3/2014 8:16:22 ...	9/23/2014 11:34:33...	392,192	A	ppt
text formula examples.xlsx	9/23/2014 11:34:33...	11/3/2014 8:16:22 ...	9/23/2014 11:34:33...	11,438	A	xlsx
TorranceUGA.ppt	9/23/2014 11:34:33...	11/3/2014 8:16:22 ...	9/23/2014 11:34:33...	153,088	A	ppt
UPN_Timetable04132014.pdf	9/23/2014 11:34:33...	11/3/2014 8:16:22 ...	9/23/2014 11:34:33...	812,307	A	pdf
word.doc	9/23/2014 11:34:33...	11/3/2014 8:16:22 ...	9/23/2014 11:34:33...	24,064	A	doc
yawconlineSample.doc	9/23/2014 11:34:33...	11/3/2014 8:16:22 ...	9/23/2014 11:34:33...	42,496	A	doc

Investigators in this case received many tips from anonymous individuals providing information regarding DB Cooper. One tip mentions there are photographs taken of his money and kept in hidden files.

To locate these files, I initiated PhotoRec tool and transferred the information to a directory on the host drive. Began perusing the directory for images of evidence of money and retrieved this picture below.

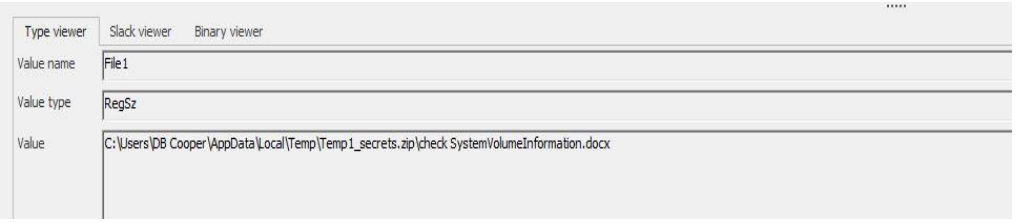
In addition, executing “shadowcopyview-x64” tool, I was able to recover another picture.

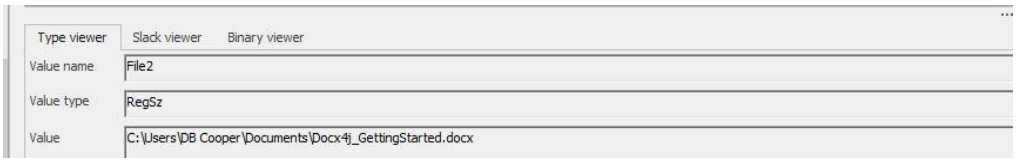
To recover the other 2 pictures, I boot up another virtual machine, imported “DB CooperLab.ova” file and able to retrieve more pictures listed below.

Interesting artifact to note is a tie with clip which can reveal clues to Mr. Cooper’s identity.

Another tip an investigator received involved DB Cooper used “scrubbing” software to delete certain files. Executing Autopsy, proceed to Windows directory, the Prefetch file are in this section. I exported the file from Autopsy to a (.csv) file named, “Prefetch_dbc.csv” to further investigate its contents. There is a “RECOVERY.EXE-B23669F0.pf “with the creation date of 10/28/2014. The software is call “RECOVERY.EXE”, an encrypted file requiring a password to access the executable file. The file located in the “Prefetch” directory and path is the following: /img_DB_Cooper_Lab.vmdk/vol_vol2/Windows/Prefetch/RECOVERY.EXE-B23669F0.pf.

An interesting tip received by investigators mentions DB Cooper kept password in a hidden file within encrypted containers. The first step was to explore the directories and locate any suspicious files. Assessed Registry Explorer tool and loaded NTUSER.DAT hive to check for current version of WordPad. There were two files obtained through the registry, “check SystemVolumeInformation.docx” and “Docx4j_GettingStarted.docx”.



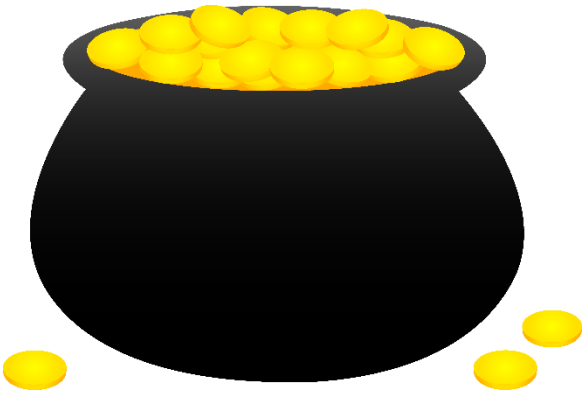


Once the two files were retrieved, next step was to access Autopsy forensic tool. Since the hidden file was named, “check SystemVolumeInformation.docx”, the clue was to check within “SystemVolumeInformation” directory for a file containing password to the TrueCrypt container. The file “checkpoint_docx” contained the password and its contents revealed the following:

TrueCrypt Password for “data” vault is:
85458xskdrirj

Now that the TrueCrypt password was obtained, next step was to access the “data” encrypted vault through Autopsy.

To obtain files from the “data” encrypted container, execute TrueCrypt tool, mount container to a selected drive, retrieve contents by supplying password obtained from “checkpoint_docx” file. Here is the pot of gold DB Cooper secretly stashed away!



Log Analysis

Interestingly, there is evidence of DB Cooper tampering with the NETBIOS. Perusing through SYSTEM hive in Registry Explorer, I was able to view the contents regarding NETBIOS and name has changed to “mssmbios”.

In table shown below, “Legacy” row, information is set to 1, acknowledging NetBios settings. Furthermore, the “Service” name set to “NetBios” as well as observing the “DeviceDesc” attribute indicates “NetBios Interface”, parameters of original NETBIOS settings.

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
Service	RegSz	NetBIOS	25-89-CB-01		
Legacy	RegDword	1			
ConfigFlags	RegDword	32			
Class	RegSz	LegacyDriver	69-00		
ClassGUID	RegSz	{8ECC055D-047F-11D1-A537-0000F8753ED1}	37-00-78-ED-2D-00		
DeviceDesc	RegSz	NetBIOS Interface			

In table listed below, the NETBIOS settings have been changed, viewing the “Legacy” row value set to 0 and “Service” name set to “mssmbios”. Also, viewing the “DeviceDesc” information data, the “mssmbios” is set to the root and initiating resources from Microsoft System Management.

rag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
HardwareID	RegMultiSz	ROOT\mssmbios	00-00-68-E5-37-00		
ConfigFlags	RegDword	0			
Legacy	RegDword	0			
DeviceReported	RegDword	1			
Service	RegSz	mssmbios	37-00		
Capabilities	RegDword	0			
ContainerID	RegSz	{00000000-0000-0000-FFFF-FFFFFFFFFFFF}	32-36-62-00-66-00		
ClassGUID	RegSz	{4d36e97d-e325-11ce-bfc1-08002be10318}	00-00-00-00-00-00		
Driver	RegSz	{4d36e97d-e325-11ce-bfc1-08002be10318}\0006	FF-FF-FF-FF		
Class	RegSz	System	00-00-01-00-FF-FF		
Mfg	RegSz	@machine.inf,%gendev_mfg%;(Standard system devices)	62-69-6C-69		
DeviceDesc	RegSz	@machine.inf,%root\mssmbios.devicedesc%;Microsoft System Manag...	23-00-00-00		

Furthermore, viewing the Zimmerman's Timeline Explorer and details of registry keys, Tsk:/Windows/System32/config/Software/.. shows a content modification time and in the long description section, note the change of the NETBIOS name to "mssmbios".

Details for super timeline entry. Line # 1460667, Inode: 0

Line #	1460667	Version	2
Timestamp	2014-11-03 14:32:00	File name	TSK:/Windows/System32/config/SOFTW/
Time zone	UTC	Inode	0
macb	m...	Notes	-
Source name	REG	Format	winreg/winreg_default
Source description	UNKNOWN	Extra	sha256_hash: 07b2f912ac9d927e085f1218ef5361fc88fc9841deee496b57b0c879ac85451a
Type	Content Modification Time		
User name	-		
Host name	DB_COOPERS_GOLD		
Short description	[HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\WDM] C:\Windows\System32\Drive		
Long description	[PROCESSORWMI]: [REG_SZ] LowDateTime:-1032902549 HighDateTime:30144695***Binary mof compiled successfully C:\Windows \system32\DRIVERS\en-US\mssmbios.sys.mui[MofResource]: [REG_SZ] LowDateTime:-1033215239 HighDateTime:30144695***Binary mof compiled successfully C:\Windows\system32\DRIVERS\intelppm.sys[PROCESSORWMI]: [REG_SZ] LowDateTime:308774759 HighDateTime:30016478***Binary mof compiled successfully C:\Windows\system32\DRIVERS\lsi_sas.sys[MofResource]: [REG_SZ] LowDateTime:-701916052 HighDateTime:30016498***Binary mof compiled successfully C:\Windows\system32\DRIVERS\mssmbios.sys[MofResource]: [REG_SZ] LowDateTime:-469323034 HighDateTime:30016498***Binary mof compiled successfully C:\Windows\system32\advapi32.dll[MofResourceName]: [REG_SZ] LowDateTime:-1239879408 HighDateTime:30016497***Binary mof compiled successfully C:\Windows\system32\en-US\advapi32.dll.mui [MofResourceName]: [REG_SZ] LowDateTime:-1055103539 HighDateTime:30144695***Binary mof compiled successfully SCSI \Disk&Ven_VMware_&Prod_VMware_Virtual_S\5&22be343f&0&000000_0-{05901221-D566-11d1-B2F0-00A0C9062910}: [REG_SZ] LowDateTime:803713417 HighDateTime:0***Binary mof compiled successfully USBSTOR \Disk&Ven_&Prod_USB_DISK_3.0&Rev_PMAP\070B43740622B360&0_0-{05901221 -D566-11d1-B2F0-00A0C9062910}: [REG_SZ] LowDateTime:803713417 HighDateTime:0***Binary mof compiled successfully		

Another interesting point to note, DB Cooper made changes to the timezone parameter settings within NTUSER.DAT file. One approach was to view the SYSTEM registry hive through RegRipper plugin tool, initiating “timezone” command.

```
File: C:\Users\Examiner\Desktop\dbc\SYSTEM

timezone v.20160318
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time Mon Nov  3 14:23:10 2014 (UTC)
  DaylightName   -> @tzres.dll,-161
  StandardName   -> @tzres.dll,-162
  Bias           -> 360 (6 hours)
  ActiveTimeBias -> 360 (6 hours)
  TimeZoneKeyName-> Central Standard Time
```

The time discrepancies from “DaylightName” to “StandardName” indicates difference between hardware clock settings and operating system clock. Also, the timestamps seen in Zimmerman’s Timeline Explorer showed a six hour difference, ahead of CST noted time.

Removable Storage Analysis

There are removable storage devices used by DB Cooper and information retrieved viewing SYSTEM registry hive through RegRipper with plugins tool by executing “usbdevices” command.

```
File: C:\Users\Examiner\Desktop\dbc\SYSTEM

usbdevices v.20140416
(System) Parses Enum\USB key for USB & WPD devices

VID_058F&PID_6387
LastWrite: Mon Nov  3 14:25:12 2014

  SN       : 2013070200000437
  LastWrite: Mon Nov  3 14:25:13 2014

VID_13FE&PID_5500
LastWrite: Mon Nov  3 14:28:35 2014
  SN       : 070B43740622B360
  LastWrite: Mon Nov  3 14:28:37 2014
```

Viewing the information, one device mentions vendor ID from Alcor Micro Corp. with corresponding product ID not known and serial number noted as 2013070200000437. The second USB device of vendor ID from Kingston Technology Company Inc. with corresponding product ID not known, however, serial number available and noted as 070B43740622B360.

In addition, I ran RegRipper with plugins tool initiating "USBstor" command, changes were made to each serial number by adding "&0" to end of number as well as device name assigned to "Generic Flash Disk USB Device" and "USB DISK 3.0 USB Device" respectively. Incidentally, both devices were last accessed and written on November 3, 2014.

```
  USBStor
ControlSet001\Enum\USBStor

Disk&Ven_&Prod_USB_DISK_3.0&Rev_PMAP [Mon Nov  3 14:28:37 2014]
  S/N: 070B43740622B360&0 [Mon Nov  3 14:28:37 2014]
  Device Parameters LastWrite: [Mon Nov  3 14:28:37 2014]
  LogConf LastWrite          : [Mon Nov  3 14:28:37 2014]
  Properties LastWrite       : [Mon Nov  3 14:28:37 2014]
    FriendlyName    : USB DISK 3.0 USB Device
    InstallDate     : Mon Nov  3 14:28:37 2014 UTC
    FirstInstallDate: Mon Nov  3 14:28:37 2014 UTC

Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07 [Mon Nov  3 14:25:13 2014]
  S/N: 2013070200000437&0 [Mon Nov  3 14:25:14 2014]
  Device Parameters LastWrite: [Mon Nov  3 14:25:14 2014]
  LogConf LastWrite          : [Mon Nov  3 14:25:13 2014]
  Properties LastWrite       : [Mon Nov  3 14:25:14 2014]
    FriendlyName    : Generic Flash Disk USB Device
    InstallDate     : Mon Nov  3 14:25:14 2014 UTC
    FirstInstallDate: Mon Nov  3 14:25:14 2014 UTC
```

To explore more storage devices on DB Cooper's system, accessed the "Shellbags" option in Autopsy, there are files accessed on USB devices and other important directory accesses. Viewing the table below, the line mentioned, "MyComputer\E:\secrets.zip" indicates "secrets.zip" files was accessed through USB drive (E) and last accessed on 11/03/2014 at 14:25:00 CST.

Listing
Shell Bags
25 Results
Table | Thumbnail
Save Table as CSV

Source File	S	C	O	Path	Key	Last Write	Data Source	Date Modified	Date Created	Date Accessed
NTUSER.DAT				Recycle Bin	Software\Microsoft\Windows\Shell\Bags\1\Desktop	2014-11-03 14:26:49 CST	DB_Cooper_Lab.vmdk			
NTUSER.DAT				Google Chrome.lnk	Software\Microsoft\Windows\Shell\Bags\1\Desktop	2014-11-03 14:26:49 CST	DB_Cooper_Lab.vmdk	2014-11-03 14:21:32 CST	2014-11-03 14:21:32 CST	2014-11-03 14:21:32 CST
UsrClass.dat				Libraries	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\0\		DB_Cooper_Lab.vmdk			
UsrClass.dat				Libraries\CLSID_Documents Library	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\0\0\		DB_Cooper_Lab.vmdk			
UsrClass.dat				Libraries\CLSID_Pictures	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\0\1\	2014-11-03 14:15:11 CST	DB_Cooper_Lab.vmdk			
UsrClass.dat				Control Panel	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\		DB_Cooper_Lab.vmdk			
UsrClass.dat				Control Panel\System and Security	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\	2014-10-28 08:48:55 CDT	DB_Cooper_Lab.vmdk			
UsrClass.dat				Control Panel\System and Security\CLSID_Backup and Restore Ce...	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\0\		DB_Cooper_Lab.vmdk			
UsrClass.dat				Control Panel\System and Security\CLSID_System	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\1\	2014-10-28 08:50:17 CDT	DB_Cooper_Lab.vmdk			
UsrClass.dat				My Computer	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\		DB_Cooper_Lab.vmdk			
UsrClass.dat				My Computer\C:\	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\0\		DB_Cooper_Lab.vmdk			
UsrClass.dat				My Computer\E:\	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\1\	2014-11-03 14:28:42 CST	DB_Cooper_Lab.vmdk			
UsrClass.dat				My Computer\E:\secrets.zip	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\1\0\	2014-11-03 14:28:55 CST	DB_Cooper_Lab.vmdk	2014-10-31 16:11:14 CDT	2014-11-03 14:25:00 CST	2014-11-03 14:25:00 CST

Malware Analysis

Malware is present in Mr. Cooper's computer system. Sysinternal Autoruns was initiated on the DB Cooper_Lab.vmdk, and within the DB Cooper directory, a file named "usback.lnk" was executed 11/03/2014 8:33 am.

Autoruns [DEPAULWIN4N6\Examiner] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Filter:
Everything | Logon | Explorer | Internet Explorer | Scheduled Tasks | Services | Drivers | Codecs | Boot Execute | Image Hijacks | AppInit | KnownDLLs | Winlogon | Wins

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				7/13/2009 10:49 PM	
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	11/20/2010 3:46 AM	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				10/27/2014 11:28 PM	
VMware User Process	VMware Tools Core Service	(Verified) VMware, Inc.	c:\program files\vmware\vmware tool...	3/21/2014 5:44 PM	
C:\Users\DB Cooper\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				11/3/2014 8:33 AM	
usback.lnk			c:\users\db cooper\appdata\roamin...	11/3/2014 8:33 AM	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				7/13/2009 10:49 PM	
Browser Customizations	Windows host process (Rundll32)	(Verified) Microsoft Windows	c:\windows\system32\rundll32.exe	7/13/2009 5:57 PM	
n/a	Windows host process (Rundll32)	(Verified) Microsoft Windows	c:\windows\system32\rundll32.exe	7/13/2009 5:57 PM	
Themes Setup	Microsoft(C) Register Server	(Verified) Microsoft Windows	c:\windows\system32\regsvr32.exe	7/13/2009 6:14 PM	
Windows Desktop Update	Microsoft(C) Register Server	(Verified) Microsoft Windows	c:\windows\system32\regsvr32.exe	7/13/2009 6:14 PM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				11/3/2014 8:21 AM	

The file, "usback.lnk" is a link file which is accessed often and contained in a zip file, "usback.zip". To view the programs run from the internet, I viewed NTUSER.DAT registry hive through RegRipper with plugins tool, initiating "typedurls" command showing internet connection was made several times to access execution of usback.zip.

```
File: C:\Users\Examiner\Desktop\Users\DB Cooper\NTUSER.DAT

typedurls v.20080324
(NTUSER.DAT) Returns contents of user's TypedURLs key.

TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time Mon Nov  3 14:32:39 2014 (UTC)
  url1 -> http://dl.dropboxusercontent.com/u/643261/usback.zip
  url2 -> https:///dl.dropboxusercontent.com/u/643261/usback.zip
  url3 -> http:///dl.dropboxusercontent.com/u/643261/usback.zip
  url4 -> http:///dl.dropboxusercontent.com/u/643261/usback1.zip
  url5 -> http://go.microsoft.com/fwlink/?LinkId=69157
```

The ”usback.zip” files are located in a storage container named “dropboxusercontent.com”. To further investigate, I ran Zimmerman Timeline Explorer forensic tool and retrieved some details of a virus. The first detail shows November 3, 2014 at 14:31:27, through private site of Internet Explorer, “betrad.com” was executed and its purpose is to write a program to local storage using JavaScript and emulate a browser. The private session creates a location (2014110320141104) by DB Cooper. He also initiates an internet connection to the domain, “bleepingcomputer.com”, navigates into the forum/t/549064/ directory and where the virus, “virus-heu-aegis938-via-dropbox” resides.

2014-11-03 14:31:27	MSIE Cache File URL record	WEBHIST	....	0	Location: PrivacIE:betrad.com/icon/*/ci.png Number of hits: 1 Ca
2014-11-03 14:31:27	MSIE Cache File URL record	WEBHIST	.a...	0	Location: :2014110320141104: DB Cooper@http://www.bleepingcomput
2014-11-03 14:31:27	MSIE Cache File URL record	WEBHIST	.a...	0	Location: :2014110320141104: DB Cooper@:Host: www.bleepingcomput
2014-11-03 14:31:27	MSIE Cache File URL record	WEBHIST	.a...	0	Location: :2014110320141104: DB Cooper@http://www.bleepingcomput
2014-11-03 14:31:27	MSIE Cache File URL record	WEBHIST	.a...	0	Location: :2014110320141104: DB Cooper@:Host: www.bleepingcomput
2014-11-03 14:31:27	MSIE Cache File URL record	WEBHIST	.a...	0	Location: Visited: DB Cooper@http://www.bleepingcomputer.com/for

```
Location: PrivacIE:betrad.com/icon/*/ci.png Number of hits: 1 Cached file size: 0
Location: :2014110320141104: DB Cooper@http://www.bleepingcomputer.com/forums/t/549064/virus-heu-aegiscs938-via-dropbox Number
Location: :2014110320141104: DB Cooper@:Host: www.bleepingcomputer.com Number of hits: 1 Cached file size: 0
Location: :2014110320141104: DB Cooper@http://www.bleepingcomputer.com/forums/t/549064/virus-heu-aegiscs938-via-dropbox Number
Location: :2014110320141104: DB Cooper@:Host: www.bleepingcomputer.com Number of hits: 1 Cached file size: 0
Location: Visited: DB Cooper@http://www.bleepingcomputer.com/forums/t/549064/virus-heu-aegiscs938-via-dropbox Number of hits:
```

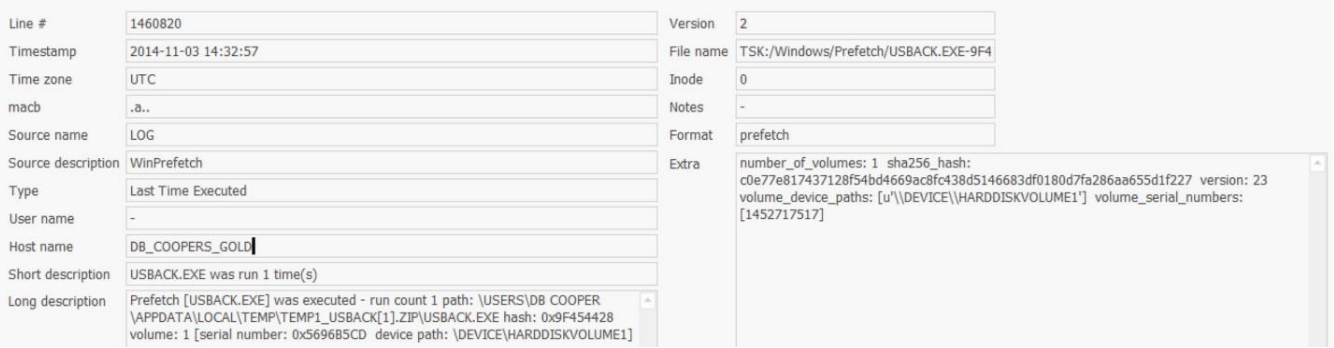
Final step is to make the usback.zip an executable file for execution to occur, thus, the virus file is “usback.exe” and activated once entering the command or selecting an option through a graphical user interface application.

Line #	1460820	Version	2
Timestamp	2014-11-03 14:32:57	File name	TSK:/Windows/Prefetch/USBACK.EXE-9F4
Time zone	UTC	Inode	0
macb	.a..	Notes	-
Source name	LOG	Format	prefetch
Source description	WinPrefetch	Extra	number_of_volumes: 1 sha256_hash: c0e77e817437128f54bd4669ac8fc438d5146683df0180d7fa286aa655d1f227 version: 23 volume_device_paths: [u'\\DEVICE\\HARDDISKVOLUME1'] volume_serial_numbers: [1452717517]
Type	Last Time Executed		
User name	-		
Host name	DB_COOPERS_GOLD		
Short description	USBACK.EXE was run 1 time(s)		
Long description	Prefetch [USBACK.EXE] was executed - run count 1 path: \USERS\DB COOPER \APPDATA\LOCAL\TEMP\TEMP1_USBACK[1].ZIP\USBACK.EXE hash: 0x9F454428 volume: 1 [serial number: 0x5696B5CD device path: \DEVICE\HARDDISKVOLUME1]		

An interesting point to note, ten seconds before "USBACK.exe" was to execute, Mr. Cooper made changes to NTUSER.DAT registry file, shown in the screenshot below.

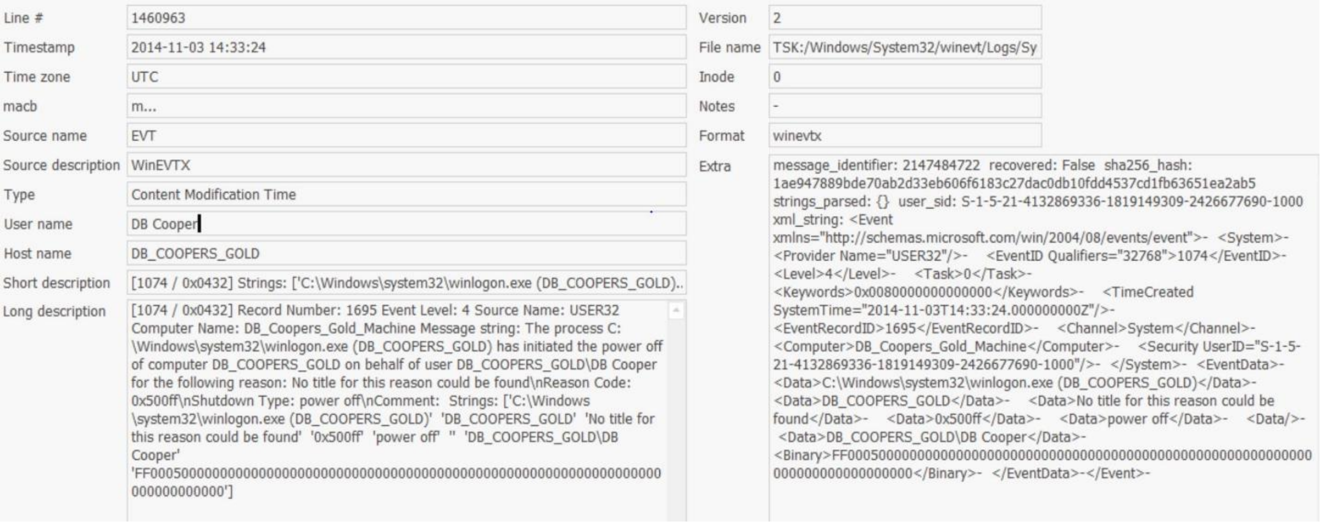
Line #	1460802	Version	2
Timestamp	2014-11-03 14:32:47	File name	TSK:/Users/DB Cooper/NTUSER.DAT
Time zone	UTC	Inode	0
macb	m...	Notes	-
Source name	REG	Format	winreg/winreg_default
Source description	UNKNOWN	Extra	sha256_hash: 03a6c1bbad1b3f916271d77c99b3602ba102aac05cda3502b4b34f2c10e09c06
Type	Content Modification Time		
User name	-		
Host name	DB_COOPERS_GOLD		
Short description	[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main] Anchor Underlin...		
Long description	[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main] Anchor Underline: [REG_SZ] yes Cache_Update_Frequency: [REG_SZ] Once_Per_Session Check_Associations: [REG_SZ] yes CompatibilityFlags: [REG_DWORD_LE] 0 Disable Script Debugger: [REG_SZ] yes Display Inline Images: [REG_SZ] yes Do404Search: [REG_BINARY] Enable Browser Extensions: [REG_SZ] yes FullScreen: [REG_SZ] no IE8RunOnceLastShown: [REG_DWORD_LE] 1 IE8RunOnceLastShown_TIMESTAMP: [REG_BINARY] IE8TourShown: [REG_DWORD_LE] 1 IE8TourShownTime: [REG_BINARY] Local Page: [REG_SZ] C:\Windows\system32\blank.htm NoUpdateCheck: [REG_DWORD_LE] 1 NotifyDownloadComplete: [REG_SZ] yes Play_Animations: [REG_SZ] yes Play_Background_Sounds: [REG_SZ] yes Save_Session_History_On_Exit: [REG_SZ] no Search Page: [REG_SZ] http://go.microsoft.com/fwlink/?LinkId=54896 Show_FullURL: [REG_SZ] no Show_StatusBar: [REG_SZ] yes Show_ToolBar: [REG_SZ] yes Show_URLToolBar: [REG_SZ] yes Show_URLinStatusBar: [REG_SZ] yes Start Page: [REG_SZ] http://www.google.com/ Start Page Redirect Cache: [REG_SZ] http://www.msn.com/?ocid=iehp Start Page Redirect Cache AcceptLangs: [REG_SZ] en-us Start Page Redirect Cache_TIMESTAMP: [REG_BINARY] UseClearType: [REG_SZ] no Use_DlgBox_Colors: [REG_SZ] yes Window_Placement: [REG_BINARY] XMLHTTP: [REG_DWORD_LE] 1		

Viewing Zimmerman's Timeline Explorer below, "USBACK.EXE" was executed on 11-03-2014 at 14:32:57 am (close to 8:33 am), one time run as indicated from Sysinternal Autoruns command.



Line #	1460820	Version	2
Timestamp	2014-11-03 14:32:57	File name	TSK:/Windows/Prefetch/USBACK.EXE-9F4
Time zone	UTC	Inode	0
macb	.a..	Notes	-
Source name	LOG	Format	prefetch
Source description	WinPrefetch	Extra	number_of_volumes: 1 sha256_hash: c0e77e817437128f54bd4669ac8fc438d5146683df0180d7fa286aa655d1f227 version: 23 volume_device_paths: [u'\\DEVICE\\HARDDISKVOLUME1'] volume_serial_numbers: [1452717517]
Type	Last Time Executed		
User name	-		
Host name	DB_COOPERS_GOLD		
Short description	USBACK.EXE was run 1 time(s)		
Long description	Prefetch [USBACK.EXE] was executed - run count 1 path: \USERS\DB COOPER \APPDATA\LOCAL\TEMP\TEMP1_USBACK[1].ZIP\USBACK.EXE hash: 0x9F454428 volume: 1 [serial number: 0x5696B5CD device path: \DEVICE\HARDDISKVOLUME1]		

Also, tech savvy DB Cooper initiated “winlogin.exe” using admin privileges to issue a command to power off his computer after infecting with malware. The date noted as 11-03-2014 14:33:24, a few seconds after the virus detected via observing Sysinternal Autoruns logs.



Line #	1460963	Version	2
Timestamp	2014-11-03 14:33:24	File name	TSK:/Windows/System32/winevt/Logs/Sy
Time zone	UTC	Inode	0
macb	m...	Notes	-
Source name	EVT	Format	winevtx
Source description	WinEVTX	Extra	message_identifier: 2147484722 recovered: False sha256_hash: 1ae947889bde70ab2d33eb606f6183c27dac0db10fdd4537cd1fb63651ea2ab5 strings_parsed: {} user_sid: S-1-5-21-4132869336-1819149309-2426677690-1000 xml_string: <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">- <System>- <Provider Name="USER32"/>- <EventID Qualifiers="32768">1074</EventID>- <Level>4</Level>- <Task>0</Task>- <Keywords>0x0080000000000000</Keywords>- <TimeCreated SystemTime="2014-11-03T14:33:24.000000000Z"/>- <EventRecordID>1695</EventRecordID>- <Channel>System</Channel>- <Computer>DB_Coopers_Gold_Machine</Computer>- <Security UserID="S-1-5-21-4132869336-1819149309-2426677690-1000"/>- </System>- <EventData>- <Data>C:\Windows\system32\winlogon.exe (DB_COOPERS_GOLD)</Data>- <Data>DB_COOPERS_GOLD</Data>- <Data>No title for this reason could be found</Data>- <Data>0x500ff</Data>- <Data>power off</Data>- <Data/>- <Data>DB_COOPERS_GOLD\DB Cooper</Data>- <Binary>FF000500000000000000000000000000000000000000000000000000000000000000000000000000000000</Binary>- </EventData>-</Event>-
Type	Content Modification Time		
User name	DB Cooper		
Host name	DB_COOPERS_GOLD		
Short description	[1074 / 0x0432] Strings: ['C:\Windows\system32\winlogon.exe (DB_COOPERS_GOLD)..		
Long description	[1074 / 0x0432] Record Number: 1695 Event Level: 4 Source Name: USER32 Computer Name: DB_Coopers_Gold_Machine Message string: The process C: \Windows\system32\winlogon.exe (DB_COOPERS_GOLD) has initiated the power off of computer DB_COOPERS_GOLD on behalf of user DB_COOPERS_GOLD\DB Cooper for the following reason: No title for this reason could be found\nReason Code: 0x500ff\nShutdown Type: power off\nComment: Strings: ['C:\Windows \system32\winlogon.exe (DB_COOPERS_GOLD)' 'DB_COOPERS_GOLD' 'No title for this reason could be found' '0x500ff' 'power off' '' 'DB_COOPERS_GOLD\DB Cooper' 'FF00050000000000000000000000000000000000000000000000000000000000000000000000']		

Here is an amazing artifact I found viewing Zimmerman’s Timeline Explorer suggesting DB Cooper monitored the effects of the hidden virus planted in his computer. This information is kept in a cache file URL record, 5 hits noted accessing the “USBACK.EXE” file, and date registered as 11/29/2014 at 14:24:20.

Details for super timeline entry. Line # 1461666, Inode: 0

Line #	1461666	Version	2
Timestamp	2014-11-29 14:24:20	File name	TSK:/Users/DB Cooper/AppData/Local/Mic
Time zone	UTC	Inode	0
macb	....	Notes	-
Source name	WEBHIST	Format	msiecf
Source description	MSIE Cache File URL record	Extra	cache_directory_index: -2 recovered: False sha256_hash: 9745d16f620bb9b625aa3cb5bc46979895c5f75213bf8dfd12c1362958a00848
Type	Expiration Time		
User name	-		
Host name	DB_COOPERS_GOLD		
Short description	Location: Visited: DB Cooper@http://www.bleepingcomputer.com/forums/t/549064/...		
Long description	Location: Visited: DB Cooper@http://www.bleepingcomputer.com/forums/t/549064/virus-heu-aegiscs938-via-dropbox Number of hits: 5 Cached file size: 0		

Findings and Conclusions

Helen Ramchandani- DePaul DB Cooper Report

1. What is MD5 hash for the forensic image?

To obtain the MD5 hash, I used FTK forensic application within the DePaul Windows Forensic Workstation. MD5 for forensic image retrieved, f175912b7e0ecb64ac0817d8d3cfe681, refer to Forensic Imaging/Data Collection section of report.

2. What is the user/account name for the main user account/profile?

To obtain this information, initiated "RegRipperRunner" tool with plugins and ran "samparse" command to extract information from SAM hive, results noted in Filesystem Analysis section of report.

3. What is the password for the user account?

Used SAMInside tool to recover passwords and initiated a NT hash attack and dictionary attack to obtain DB Cooper's password, "hidemy$".

User	RID	LM-Password	NT-Password	LM-Hash	NT-Hash	Description
Administrator	500	<Disabled>	<Empty>	00000000000000000000...	31D6CFE0D16AE931B...	Built-in account for ad...
Guest	501	<Disabled>	<Disabled>	00000000000000000000...	00000000000000000000...	Built-in account for gu...
DB Cooper	1000	<Disabled>	hidemy$	00000000000000000000...	2B890295BA8D7F656...	

4. What is Operating System version, and registered owner based on the Windows installation?

View the SOFTWARE registry hive through RegRipper tool, invoking "winver" command, refer to Filesystem Analysis of report.

5. When was the Operating System installed?

View the SOFTWARE registry hive through RegRipper tool, invoking "winver" command and refer to Filesystem Analysis of report.

6. Were any USB devices used on the computer? If so, when where the USB devices used and what are the serial numbers?

View the SYSTEM registry hive through RegRipper tool, invoked “usbdevices” command. I was able to view serial numbers and date “LastWrite” or accessed. Refer to Removable Storage Analysis section of report for details.

7. If any USB devices were used, can you determine what files and/or folders existed on USB devices and what may have been accessed from them?

Accessing “Shellbags” in Autopsy, to check for files accessed on USB devices are noted, refer to Removable Storage Analysis section of report.

8. The anonymous tip mentioned that DB Cooper may have had 4 photos of his money and that these photos may have been recently deleted... can you recover and produce them?

To produce the 4 pictures, Photorec, shadowcopyview-x64 tool, import “DB Cooper.ova” file to a forensic workstation as seen in section of Internet History Analysis of report.

9. Is there any evidence of the computer's (NETBIOS) name being changed? If so, what is the old/new name?

There is evidence of change in NETBIOS of Mr. Cooper’s computer and noted in Log Analysis section of report.

10. Is there any evidence of time/date manipulation?

There is evidence of time/date manipulation by viewing the time zone settings within the SYSTEM registry, refer to Log Analysis section of report.

11. What file(s) did DB Cooper open from the Windows WordPad?

Files DB Cooper accessed from Windows WordPad are retrieved and noted in Internet History Analysis of report.

12. What did DB Cooper search for on Google?

Using Autopsy forensic tool, under the “Extract Content” folder, an option called “Web

Searches" option provides web history visited by Mr. Cooper using Internet Explorer browser. Saved the results as a .csv file and named it "Web Search_google" and can refer to Internet History Analysis section of report.

13. Did DB Cooper download or run any programs from the Internet?

View the NTUSER.DAT registry hive through RegRipper and plugin tool, initiating "typedurls" command to view browsing history activity. Referring to Malware Analysis section, many programs were executed via internet.

14. Is DB Cooper's computer infected with a Virus? If so, what virus is it, when did he get infected, how did he get infected?

Sysinternal Autoruns tool was executed in the forensic workstation on the DB Cooper_Lab.vmdk file, within the DB Cooper directory, a file named "usback.lnk" was initiated 11/03/2014 8:33 am and referred to Malware Analysis section of report for details.

15. Is DB Cooper storing anything in encrypted containers?

DB Cooper many files of various types in encrypted containers and seen in Internet History Analysis of the report.

16. Can you find any artifacts that may show where DB Cooper is hiding?

There is a jpeg file along with information of longitude/latitude coordinates retrieved from Autopsy forensic tool suggesting the location of where DB Cooper maybe hiding, refer to Internet History Analysis section of report.

17. Are there any other files that DB Cooper deleted?

There is evidence that many files were deleted running shadow copy forensic tool can retrieve some of the files as seem in Internet History Analysis section of the report.

18. Investigators also received a tip that DB Cooper may have been using some secure deletion or scrubbing software on 10/28/2014? Can you confirm this tip? If so, what software was used and where is it located? Can you recover any of these documents?

DB Cooper used scrubbing software to delete files on 10/28/2014, information about software program noted in Internet History Analysis portion of report.

19. Another tip Investigators received is that DB Cooper may have been hiding files in TrueCrypt v7 container. Cooper apparently keeps the password for this container in a hidden location, but he may have accessed the password file using WordPad on 11/03/2014. The TrueCrypt container is also reported to be stored in a hidden location.

Password information was retrieved and location of container named “data” accessed, refer to information noted in Internet History Analysis portion of the report.

20. Rumor has it that DB Cooper stores a pot of gold in this TrueCrypt container. Can you located it and produce the hidden pot of gold?

The pot of gold was retrieved from TrueCrypt container given the password of the “data” vault, refer to Internet History Analysis section of report to view image of pot of gold.