DFRWS2008 Rodeo Results

Eoghan Casey would like to thank the graduate student in his Fall 2008 course at Johns Hopkins University Information Security Institute for their in-depth analysis of this exercise.

Summary of Findings

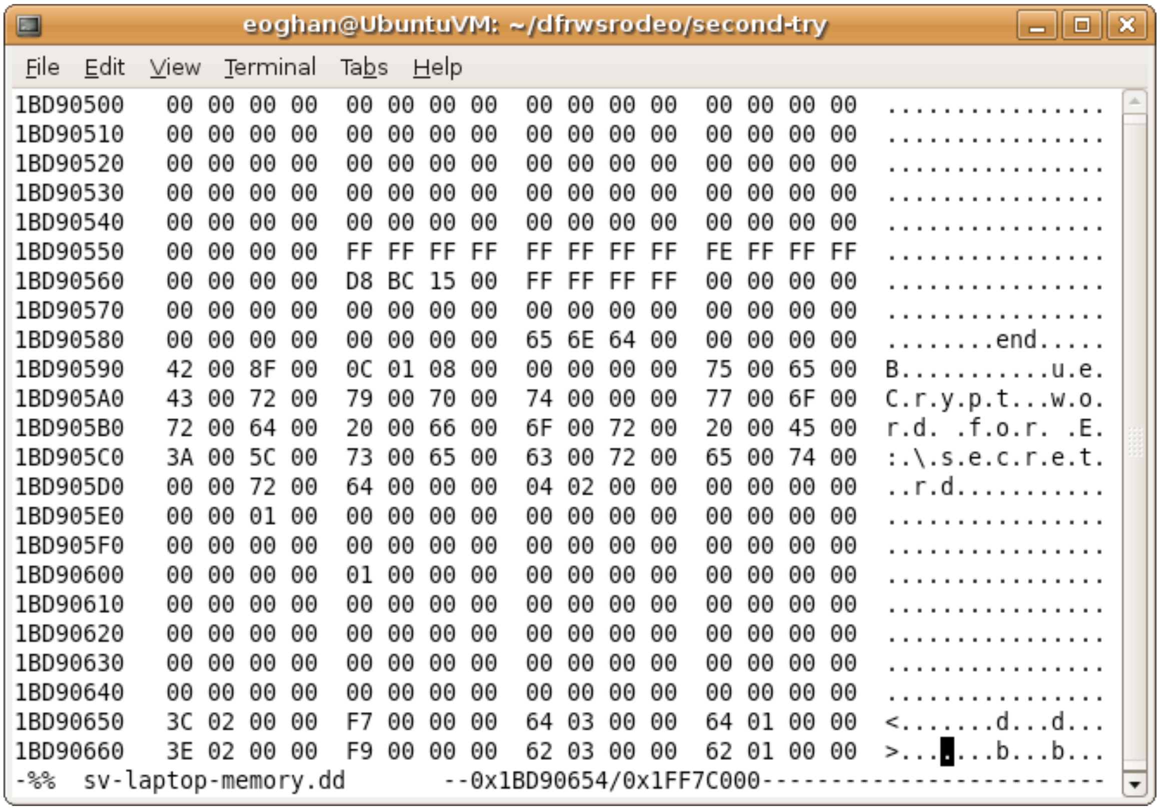
The materials provided in the DFRWS2008 Rodeo contain solid evidence that Mr. Vogon took photographs of confidential material, copied them to his local workstation, and used a custom built script as a covert channel to secretly upload this material to an unknown third-party source. In addition, the evidence reveals that Mr. Vogon attempted to conceal his activities using encryption and reformatting the thumb drive. The materials also contain information identifying potential accomplices.

Question 1

In regards to the USB thumb drive image that you have been provided with, were there any steps taken or actions performed to conceal the drive's contents? If so, what were they?

An initial review of the USB thumb drive shows that it contains an empty FAT16 file system. Further forensic analysis of unallocated space reveals files that can be salvaged using file carving techniques. The absence of file system entries for any of these files indicates that the thumb drive was reformatted.

The thumb drive also contains an encrypted container, and executable files stored on the thumb drive had been UPX compressed, which constitutes a form of concealment. Clues about the encrypted container can be found in the memory dump as shown here:


eoghan@UbuntuVM: ~/dfrwsrodeo/second-try
File Edit View Terminal Tabs Help

```
1BD90500   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
1BD90510   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
1BD90520   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
1BD90530   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
1BD90540   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
1BD90550   00 00 00 00  FF FF FF FF  FF FF FF FF  FE FF FF FF  ................
1BD90560   00 00 00 00  D8 BC 15 00  FF FF FF FF  00 00 00 00  ................
1BD90570   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
1BD90580   00 00 00 00  00 00 00 00  65 6E 64 00  00 00 00 00  ........end.....
1BD90590   42 00 8F 00  0C 01 08 00  00 00 00 00  75 00 65 00  B...........u.e.
1BD905A0   43 00 72 00  79 00 70 00  74 00 00 00  77 00 6F 00  C.r.y.p.t...w.o.
1BD905B0   72 00 64 00  20 00 66 00  6F 00 72 00  20 00 45 00  r.d. .f.o.r. .E.
1BD905C0   3A 00 5C 00  73 00 65 00  63 00 72 00  65 00 74 00  :.\.s.e.c.r.e.t.
1BD905D0   00 00 72 00  64 00 00 00  04 02 00 00  00 00 00 00  ..r.d...........
1BD905E0   00 00 01 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
1BD905F0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
1BD90600   00 00 00 00  01 00 00 00  00 00 00 00  00 00 00 00  ................
1BD90610   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
1BD90620   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
1BD90630   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
1BD90640   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
1BD90650   3C 02 00 00  F7 00 00 00  64 03 00 00  64 01 00 00  <.......d...d...
1BD90660   3E 02 00 00  F9 00 00 00  62 03 00 00  62 01 00 00  >.......b...b...
-%%  sv-laptop-memory.dd      --0x1BD90654/0x1FF7C000------------------------
```

Figure 1: Data captured in memory dump showing relationship between encryption and "E:\secret"

Questions 2 & 3

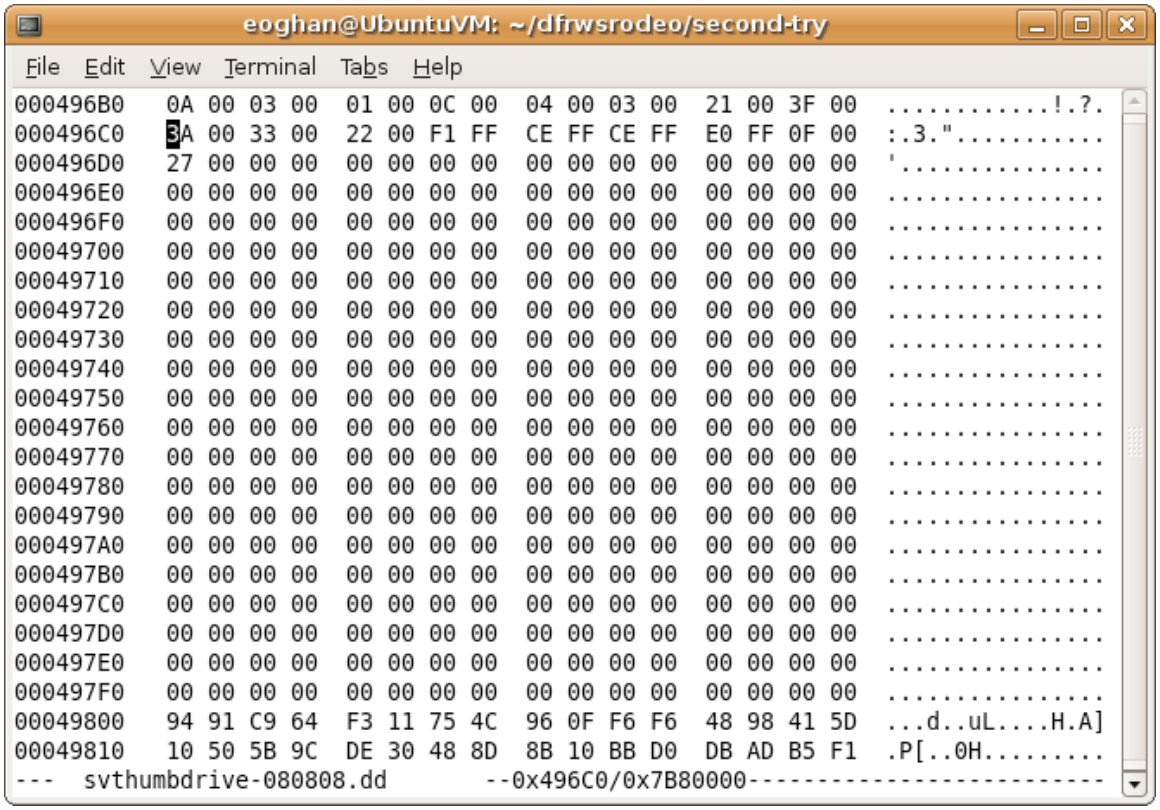
What files were found on this disk? How did you recover them? Please provide a full explanation for each file found on the USB thumb drive to include file type, contents and purpose.

All files on the thumb drive had to be salvaged using file carving techniques.

Name	**Description**
secret	Truecrypt Container
keyfile.wav	Keyfile for "secret" TrueCrypt container
xfer.pl	Perl script source code within Truecrypt container
Expedia Web page	Expedia trip summary showing purchase of three round trip tickets from Washington DC to Liberia Steve Vogon, Catherine Lagrande and Matthew Geiger.
PAR packed executable	Executable version of xfer.pl created using the Perl Archive toolkit (PAR)
upx.exe	Utility to UPX compress executables
wget.exe	Command line utility to access Web sites

	(referenced by xfer.pl Perl script)
libeay32.dll	Component of OpenSSL toolkit
ssleay32.dll	Component of OpenSSL toolkit
linintl3.dll	Required by wget
libiconv32.dll	Required by wget

Salvaging files from the thumb drive requires manual intervention because automated tools like foremost and scalpel cannot distinguish some of the file types. For instance, the start of the encrypted container is shown in **Figure 2**. The end of this encrypted container must be deduced from a known header signature indicating the start of another file type. As another example of the limitations of automated file carving techniques, the PAR file contains compressed data that is separately carved as a Zip file.


eoghan@UbuntuVM: ~/dfrwsrodeo/second-try
File Edit View Terminal Tabs Help

```
000496B0   0A 00 03 00  01 00 0C 00  04 00 03 00  21 00 3F 00  ............!.?.
000496C0   3A 00 33 00  22 00 F1 FF  CE FF CE FF  E0 FF 0F 00  :.3."...........
000496D0   27 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  '...............
000496E0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000496F0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00049700   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00049710   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00049720   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00049730   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00049740   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00049750   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00049760   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00049770   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00049780   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00049790   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000497A0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000497B0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000497C0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000497D0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000497E0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000497F0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00049800   94 91 C9 64  F3 11 75 4C  96 0F F6 F6  48 98 41 5D  ...d..uL....H.A]
00049810   10 50 5B 9C  DE 30 48 8D  8B 10 BB D0  DB AD B5 F1  .P[..0H.........
---  svthumbdrive-080808.dd       --0x496C0/0x7B80000------------------------
```

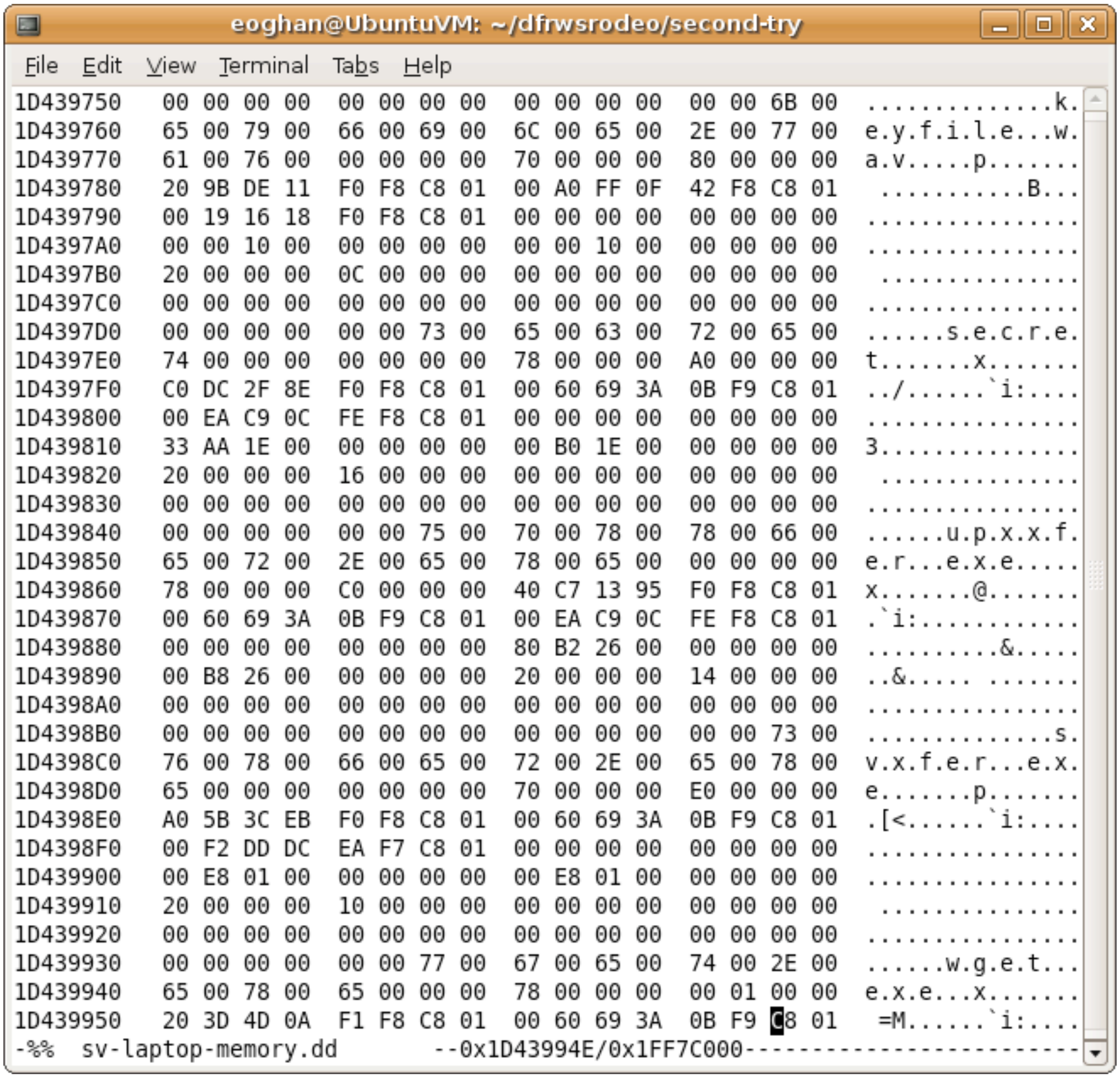
Figure 2: Start of encrypted container on thumb drive

Question 4

Did memory contain any references to remote systems, filenames, or data associated with the thumb drive? How did you recover this information?

Yes, the memory dump contains references to filenames and data associated with the thumb drive. For example, forensic examination of the memory capture using Volatility located Registry remnants of the removable media device “6f4e4ce6-6572-11dd-a440-000c29ac465b” (Offset 0x10106040) that can be tied to a partial volume directory listing of the thumb drive as shown in **Figure 3**. Various ASCII and Unicode strings in the memory dump also show filenames on the thumb drive, including traces of the xfer.pl script in use.

Forensic examination of the memory dump also provides some details about mounted drives, including T: as the TrueCrypt volume, E: as the thumb drive and X: as a mapped network share to a remote file server.


eoghan@UbuntuVM: ~/dfrwsrodeo/second-try
File Edit View Terminal Tabs Help

```
1D439750   00 00 00 00  00 00 00 00  00 00 00 00  00 00 6B 00  ..............k.
1D439760   65 00 79 00  66 00 69 00  6C 00 65 00  2E 00 77 00  e.y.f.i.l.e...w.
1D439770   61 00 76 00  00 00 00 00  70 00 00 00  80 00 00 00  a.v.....p.......
1D439780   20 9B DE 11  F0 F8 C8 01  00 A0 FF 0F  42 F8 C8 01   ...........B...
1D439790   00 19 16 18  F0 F8 C8 01  00 00 00 00  00 00 00 00  ................
1D4397A0   00 00 10 00  00 00 00 00  00 00 10 00  00 00 00 00  ................
1D4397B0   20 00 00 00  0C 00 00 00  00 00 00 00  00 00 00 00   ...............
1D4397C0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
1D4397D0   00 00 00 00  00 00 73 00  65 00 63 00  72 00 65 00  ......s.e.c.r.e.
1D4397E0   74 00 00 00  00 00 00 00  78 00 00 00  A0 00 00 00  t.......x.......
1D4397F0   C0 DC 2F 8E  F0 F8 C8 01  00 60 69 3A  0B F9 C8 01  ../......`i:....
1D439800   00 EA C9 0C  FE F8 C8 01  00 00 00 00  00 00 00 00  ................
1D439810   33 AA 1E 00  00 00 00 00  00 B0 1E 00  00 00 00 00  3...............
1D439820   20 00 00 00  16 00 00 00  00 00 00 00  00 00 00 00   ...............
1D439830   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
1D439840   00 00 00 00  00 00 75 00  70 00 78 00  78 00 66 00  ......u.p.x.x.f.
1D439850   65 00 72 00  2E 00 65 00  78 00 65 00  00 00 00 00  e.r...e.x.e.....
1D439860   78 00 00 00  C0 00 00 00  40 C7 13 95  F0 F8 C8 01  x.......@.......
1D439870   00 60 69 3A  0B F9 C8 01  00 EA C9 0C  FE F8 C8 01  .`i:............
1D439880   00 00 00 00  00 00 00 00  80 B2 26 00  00 00 00 00  ..........&.....
1D439890   00 B8 26 00  00 00 00 00  20 00 00 00  14 00 00 00  ..&..... .......
1D4398A0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
1D4398B0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 73 00  ..............s.
1D4398C0   76 00 78 00  66 00 65 00  72 00 2E 00  65 00 78 00  v.x.f.e.r...e.x.
1D4398D0   65 00 00 00  00 00 00 00  70 00 00 00  E0 00 00 00  e.......p.......
1D4398E0   A0 5B 3C EB  F0 F8 C8 01  00 60 69 3A  0B F9 C8 01  .[<......`i:....
1D4398F0   00 F2 DD DC  EA F7 C8 01  00 00 00 00  00 00 00 00  ................
1D439900   00 E8 01 00  00 00 00 00  00 E8 01 00  00 00 00 00  ................
1D439910   20 00 00 00  10 00 00 00  00 00 00 00  00 00 00 00   ...............
1D439920   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
1D439930   00 00 00 00  00 00 77 00  67 00 65 00  74 00 2E 00  ......w.g.e.t...
1D439940   65 00 78 00  65 00 00 00  78 00 00 00  00 01 00 00  e.x.e...x.......
1D439950   20 3D 4D 0A  F1 F8 C8 01  00 60 69 3A  0B F9 C8 01   =M......`i:....
-%%  sv-laptop-memory.dd       --0x1D43994E/0x1FF7C000------------------------
```

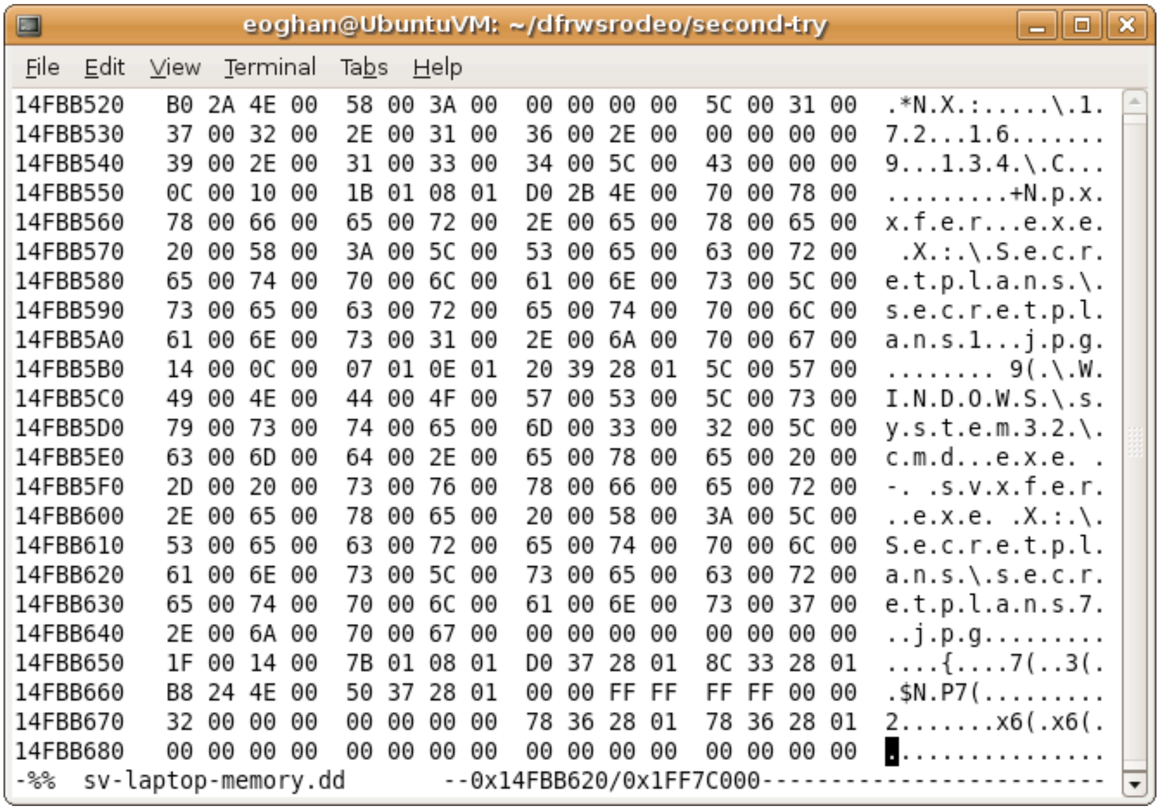
Figure 3: Reference to “keyfile.wav” and other filenames relating to files stored on the thumb drive

In addition, IP addresses can be extracted from the memory dump using regex search or a tool like Volatility. For example, using the Volatility tool, providing active network connectivity information, and identified a number of remote hosts. The primary host of interest in this case is 172.16.109.134, which was also identified as the original location of the confidential data being transmitted.

Questions 5 & 6

Based on your previous findings, please determine what Steve Vogon's intentions were? Did Steve Vogon act on his intentions? If so, what did he do? How can you prove this?

The evidence shows that Steve Vogon took files belonging to Saraquoit Corporation and used a customized program to transfer the files to a remote location on the Internet. More specifically, information captured in the memory dump shows files containing Saraquoit Corporation's intellectual property, including topsecret.gif and secretplans7.jpg, being copied from 172.16.109.34 in a folder named Secretplans mapped locally as the X: drive as shown in **Figure 4**.


eoghan@UbuntuVM: ~/dfrwsrodeo/second-try
File Edit View Terminal Tabs Help

```
14FBB520   B0 2A 4E 00  58 00 3A 00  00 00 00 00  5C 00 31 00  .*N.X.:.....\.1.
14FBB530   37 00 32 00  2E 00 31 00  36 00 2E 00  00 00 00 00  7.2...1.6.......
14FBB540   39 00 2E 00  31 00 33 00  34 00 5C 00  43 00 00 00  9...1.3.4.\.C...
14FBB550   0C 00 10 00  1B 01 08 01  D0 2B 4E 00  70 00 78 00  .........+N.p.x.
14FBB560   78 00 66 00  65 00 72 00  2E 00 65 00  78 00 65 00  x.f.e.r...e.x.e.
14FBB570   20 00 58 00  3A 00 5C 00  53 00 65 00  63 00 72 00   .X.:.\.S.e.c.r.
14FBB580   65 00 74 00  70 00 6C 00  61 00 6E 00  73 00 5C 00  e.t.p.l.a.n.s.\.
14FBB590   73 00 65 00  63 00 72 00  65 00 74 00  70 00 6C 00  s.e.c.r.e.t.p.l.
14FBB5A0   61 00 6E 00  73 00 31 00  2E 00 6A 00  70 00 67 00  a.n.s.1...j.p.g.
14FBB5B0   14 00 0C 00  07 01 0E 01  20 39 28 01  5C 00 57 00  ........ 9(.\.W.
14FBB5C0   49 00 4E 00  44 00 4F 00  57 00 53 00  5C 00 73 00  I.N.D.O.W.S.\.s.
14FBB5D0   79 00 73 00  74 00 65 00  6D 00 33 00  32 00 5C 00  y.s.t.e.m.3.2.\.
14FBB5E0   63 00 6D 00  64 00 2E 00  65 00 78 00  65 00 20 00  c.m.d...e.x.e. .
14FBB5F0   2D 00 20 00  73 00 76 00  78 00 66 00  65 00 72 00  -. .s.v.x.f.e.r.
14FBB600   2E 00 65 00  78 00 65 00  20 00 58 00  3A 00 5C 00  ..e.x.e. .X.:.\.
14FBB610   53 00 65 00  63 00 72 00  65 00 74 00  70 00 6C 00  S.e.c.r.e.t.p.l.
14FBB620   61 00 6E 00  73 00 5C 00  73 00 65 00  63 00 72 00  a.n.s.\.s.e.c.r.
14FBB630   65 00 74 00  70 00 6C 00  61 00 6E 00  73 00 37 00  e.t.p.l.a.n.s.7.
14FBB640   2E 00 6A 00  70 00 67 00  00 00 00 00  00 00 00 00  ..j.p.g.........
14FBB650   1F 00 14 00  7B 01 08 01  D0 37 28 01  8C 33 28 01  ....{....7(..3(.
14FBB660   B8 24 4E 00  50 37 28 01  00 00 FF FF  FF FF 00 00  .$N.P7(.........
14FBB670   32 00 00 00  00 00 00 00  78 36 28 01  78 36 28 01  2.......x6(.x6(.
14FBB680   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
-%%  sv-laptop-memory.dd      --0x14FBB620/0x1FF7C000------------------------
```

Figure 4: References in memory dump to 172.16.109.34 and Secretlplans

This finding is supported by artifacts from the SMB connection found at offset 0x226C8C0 in the memory dump, remnants of the filenames recovered from memory, and an active network connection on TCP 445 (SMB) recovered from the memory dump using the Volatility toolset.

Example: *\WINDOWS\system32\cmd.exe - copy X:\Secretplans\topsecret.gif T:*

Further forensic examination of the memory dump indicates that secretplans2.jpg, secretplans4.jpg, secretplans5.jpg and secretplans6.jpg were also copied.

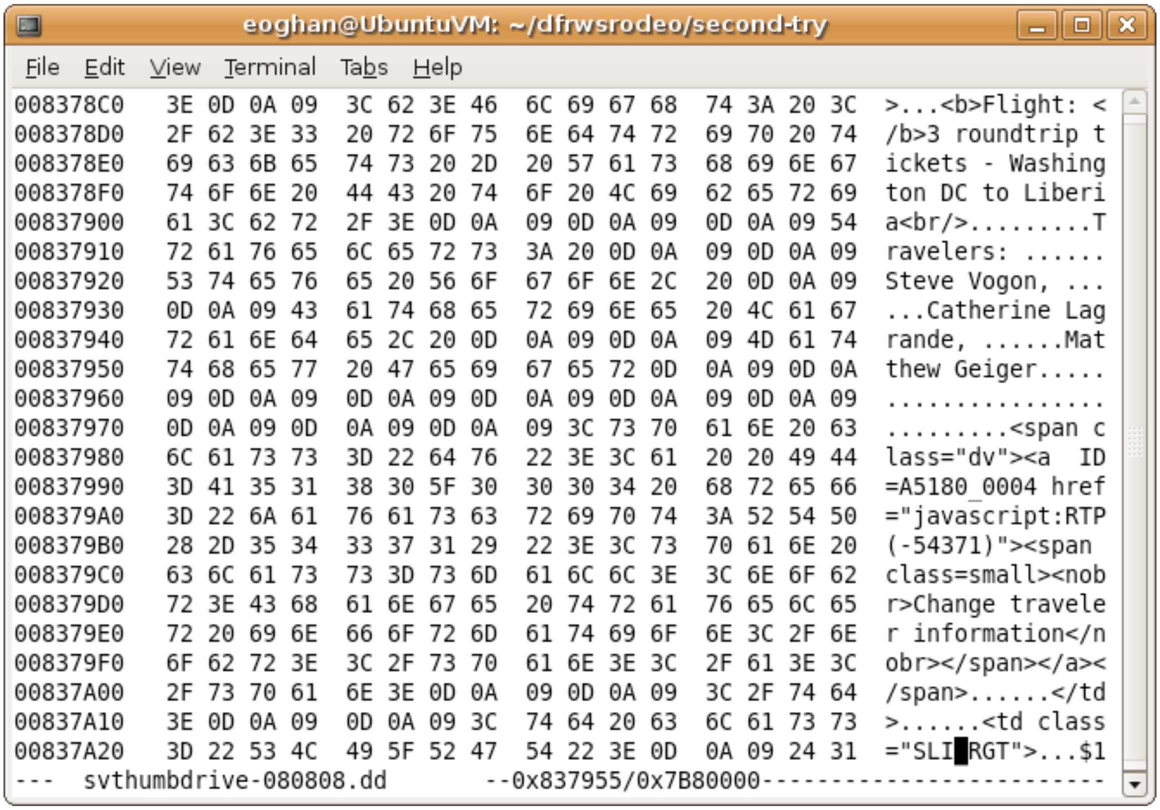
Artifacts in the memory dump indicate that the customized "xfer" program was executed. In addition to command line references to upxxfer.exe and svxfer.exe in memory, a reference to the Prefetch file "C:\WINDOWS\Prefetch\SVXFER.EXE-2DAB52DD.pf" was found, indicating that the svxfer.exe file was executed.

The memory dump also contains segments of HTTP communications to hosts listed in the xfer.pl program that included segments of the secretplans*N* .jpg and topsecret.gif files (e.g., offset 0x22EA8D0), which indicate that the transmissions were performed successfully. An examination of these segments find that they are in prefixed with a "Cval=" string are encoded in Base 64 which is consistent with the operation of the xfer.pl. When decoded, the results are consistent with JPEG files, and the header information states the source of the images as a "Canon PowerShot SD400" and that the photographs were taken at 21:48:41 on 10/22/2007. This camera may be tied to the Camera found at Steve Vogon's desk.

Question 7

While the above information is necessary, it is of no value if it cannot be tied to a specific individual. Saraquoit Corporation suspects that Steve Vogon was a disgruntled employee and may have performed malicious acts against the company. However, they need proof of this. Please provide detailed information based on your findings that would tie Steve Vogon (or others) to the contents on this thumb drive as well as the memory image.

Files salvaged from the thumb drive explicitly mention Steve Vogon by name, implicating him in the data theft scheme. The xfer.pl file has comments indicating "Developed for Steve Vogon" and error messages and input prompts that repeatedly used that name. Furthermore, the Expedia Web page salvaged from the thumb drive contains flight information for Steve Vogon, Catherine Lagrande and Matthew Geiger as shown in **Figure 5**.


eoghan@UbuntuVM: ~/dfrwsrodeo/second-try
File Edit View Terminal Tabs Help

```
008378C0   3E 0D 0A 09  3C 62 3E 46  6C 69 67 68  74 3A 20 3C  >...<b>Flight: <
008378D0   2F 62 3E 33  20 72 6F 75  6E 64 74 72  69 70 20 74  /b>3 roundtrip t
008378E0   69 63 6B 65  74 73 20 2D  20 57 61 73  68 69 6E 67  ickets - Washing
008378F0   74 6F 6E 20  44 43 20 74  6F 20 4C 69  62 65 72 69  ton DC to Liberi
00837900   61 3C 62 72  2F 3E 0D 0A  09 0D 0A 09  0D 0A 09 54  a<br/>.........T
00837910   72 61 76 65  6C 65 72 73  3A 20 0D 0A  09 0D 0A 09  ravelers: ......
00837920   53 74 65 76  65 20 56 6F  67 6F 6E 2C  20 0D 0A 09  Steve Vogon, ...
00837930   0D 0A 09 43  61 74 68 65  72 69 6E 65  20 4C 61 67  ...Catherine Lag
00837940   72 61 6E 64  65 2C 20 0D  0A 09 0D 0A  09 4D 61 74  rande, ......Mat
00837950   74 68 65 77  20 47 65 69  67 65 72 0D  0A 09 0D 0A  thew Geiger.....
00837960   09 0D 0A 09  0D 0A 09 0D  0A 09 0D 0A  09 0D 0A 09  ................
00837970   0D 0A 09 0D  0A 09 0D 0A  09 3C 73 70  61 6E 20 63  .........<span c
00837980   6C 61 73 73  3D 22 64 76  22 3E 3C 61  20 20 49 44  lass="dv"><a  ID
00837990   3D 41 35 31  38 30 5F 30  30 30 34 20  68 72 65 66  =A5180_0004 href
008379A0   3D 22 6A 61  76 61 73 63  72 69 70 74  3A 52 54 50  ="javascript:RTP
008379B0   28 2D 35 34  33 37 31 29  22 3E 3C 73  70 61 6E 20  (-54371)"><span
008379C0   63 6C 61 73  73 3D 73 6D  61 6C 6C 3E  3C 6E 6F 62  class=small><nob
008379D0   72 3E 43 68  61 6E 67 65  20 74 72 61  76 65 6C 65  r>Change travele
008379E0   72 20 69 6E  66 6F 72 6D  61 74 69 6F  6E 3C 2F 6E  r information</n
008379F0   6F 62 72 3E  3C 2F 73 70  61 6E 3E 3C  2F 61 3E 3C  obr></span></a><
00837A00   2F 73 70 61  6E 3E 0D 0A  09 0D 0A 09  3C 2F 74 64  /span>......</td
00837A10   3E 0D 0A 09  0D 0A 09 3C  74 64 20 63  6C 61 73 73  >......<td class
00837A20   3D 22 53 4C  49 5F 52 47  54 22 3E 0D  0A 09 24 31  ="SLI█RGT">...$1
---  svthumbdrive-080808.dd       --0x837955/0x7B80000------------------------
```

Figure 5: Web page on thumb drive with Expedia travel details

Finally, EXIF header information within digital photos transferred using the xfer.pl program show that they were taken using a Canon PowerShot SD40 camera. These photos could be compared with the camera found at Steve Vogon's desk to determine if this camera was used to take the photos of stolen intellectual information.