CS373 Defense Dark Arts
Weekly Write Up 2

Forensics

For week 2 of the course we discussed several security concepts & tools in the incident response and forensics category. This weeks post briefly discusses the steps in forensic analysis, the rules a forensic investigator should follow , the different tools that are used in capturing and analyzing evidence.

When performing a forensic investigation it is important to remember to be impartial. One should not assume the guilt or innocence of the party that is being investigated. The main task is to use the tools available to gather evidence that can be accepted by the court. By formulating preconceived notions of what happened may result in missing key evidence that disproves your notions. As per Dr Locard's principle every interaction leaves evidence and this is especially true with machines as well. Since this principle holds true it is of utmost importance that the investigator himself/herself document all the steps he/she takes while performing an investigation.

The general rule for starting an investigation is to gather the most volatile information first. There is an RFC that describes this and is cited here : [RFC3227]: https://tools.ietf.org/html/rfc3227.

The order of the volatility is the following:

1. registers, cache

2. routing table, arp cache, process table, kernel statistics, memory.

3. temporary file systems

4. Hibernation file

If one suspects a computer has been compromised in an attack, one should pull the network cable but not pull the power cable until you've collected a memory dump. If we pull the plug then all volatile information such as the memory dump will be lost and we may not be able to piece together the puzzle correctly. Here are things that are ranked lower in order of volatility

5. Disk images

6. Remote logging and monitoring of data that is relevant to the system.

7. Physical configuration & network topology

8. Backups

Volatility

Volatility is an open source that is used to analyse memory dumps.

[volatility]: http://www.volatilityfoundation.org/
[documentation]: https://github.com/volatilityfoundation/volatility/wiki
[cheat sheet]: https://downloads.volatilityfoundation.org//releases/2.4/CheatSheet_v2.4.pdf

Here are a list of different commands in volatility and what they do:

- `volatility -f memory_dump.mem imageinfo`

This command `imageinfo` helps to find out what kind of system it's from. This will give the output something like `suggested profiles: WinSP0x86`. We can copy that string into the rest of these commands.

- `volatility -f memory_dump.mem --profile=WinSP0x86 psscan`

`psscan` prints a list of proceses that were running at the time of the memory dump.

- `volatility -f memory_dump.mem --profile=WinSP0x86 dlllist -p 1234`

Given a process ID, `dlllist` will tell you what DLLs a process had loaded.

- `volalility -f memory_dump.mem --profile=WinSP0x86 mftparser`

This one reads the master file table block to give you a list of the files on the filesystem.

- `volatility -f memory_dump.mem --profile=WinSP0x86 timeliner --output=dump`

The timeliner prints out a timeline of everything that happened on the system (everything still in memory.. Running processes, filesystem events, etc.

Memory Capture Tool [FTK Imager]

[FTK Imager]: https://accessdata.com/product-download/ftk-imager-lite-version-3.1.1

The tool that was used in class is the FTK imager which captures memory. The main thing to remember is to not store the memory dump on the machine you are gathering memory from. Its essential to store the memory dump to an external hard drive for analysis.

Hard Disk Capture Tool

Based on the lectures these are the essential things to remember while dumping a disk:

1) Mounting a disk , access files on a disk results in changing the disk.
2) Take an image of the disk when the machine is off.

Write blockers costing an average of 300 dollars are used to ensure that any write commands are not being sent to the disk when a capture is in progress.

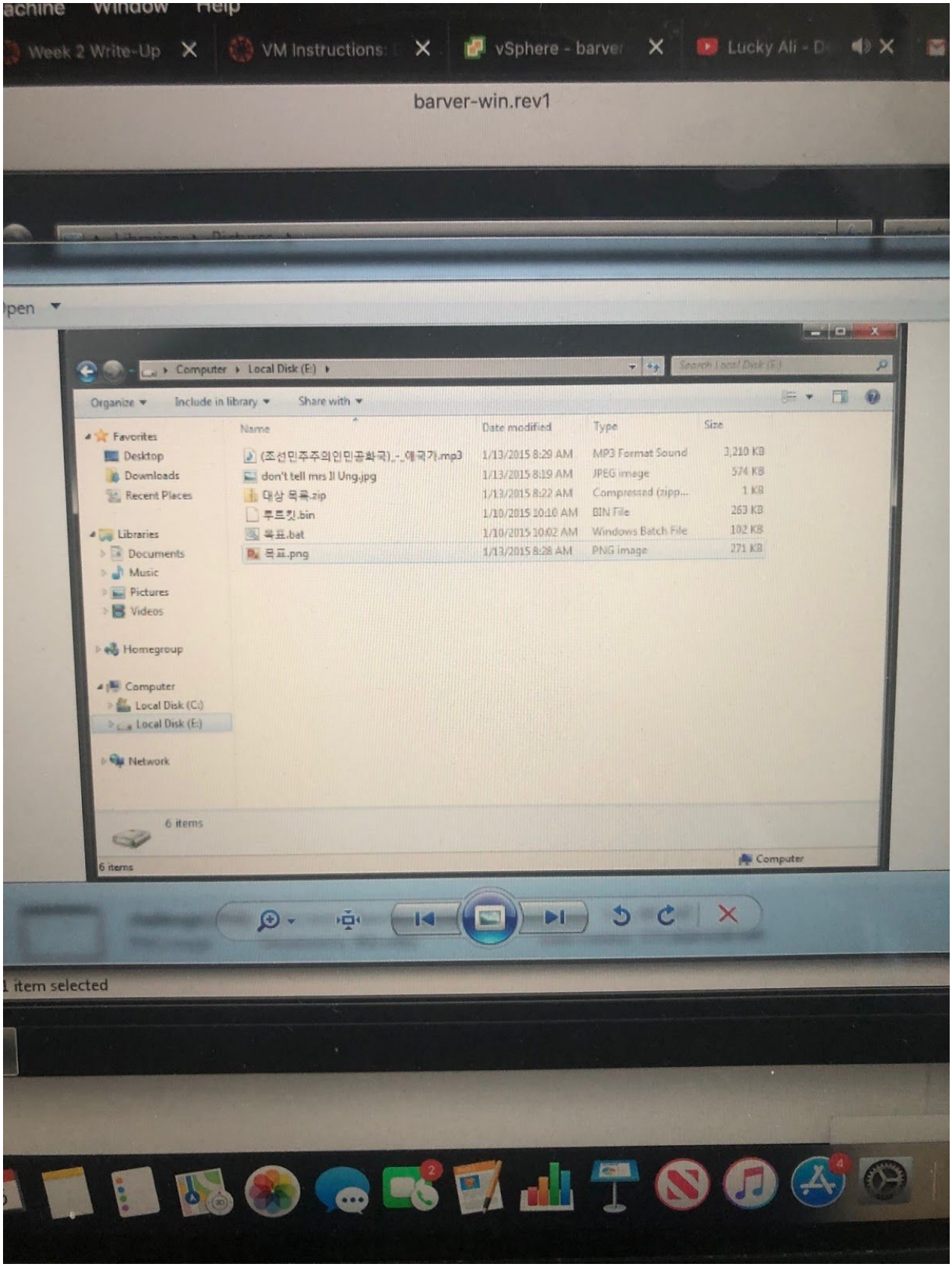
Recovering Data Tool

When a file is deleted from the system, it does not disappear right away. The reference to the file is removed but its contents linger around on the disk in unused blocks. The process of looking at the unused blocks on a disk and piecing together the deleted files is called carving. The tool that was used in class is called PhotoRec. It is cross platform and free to use.

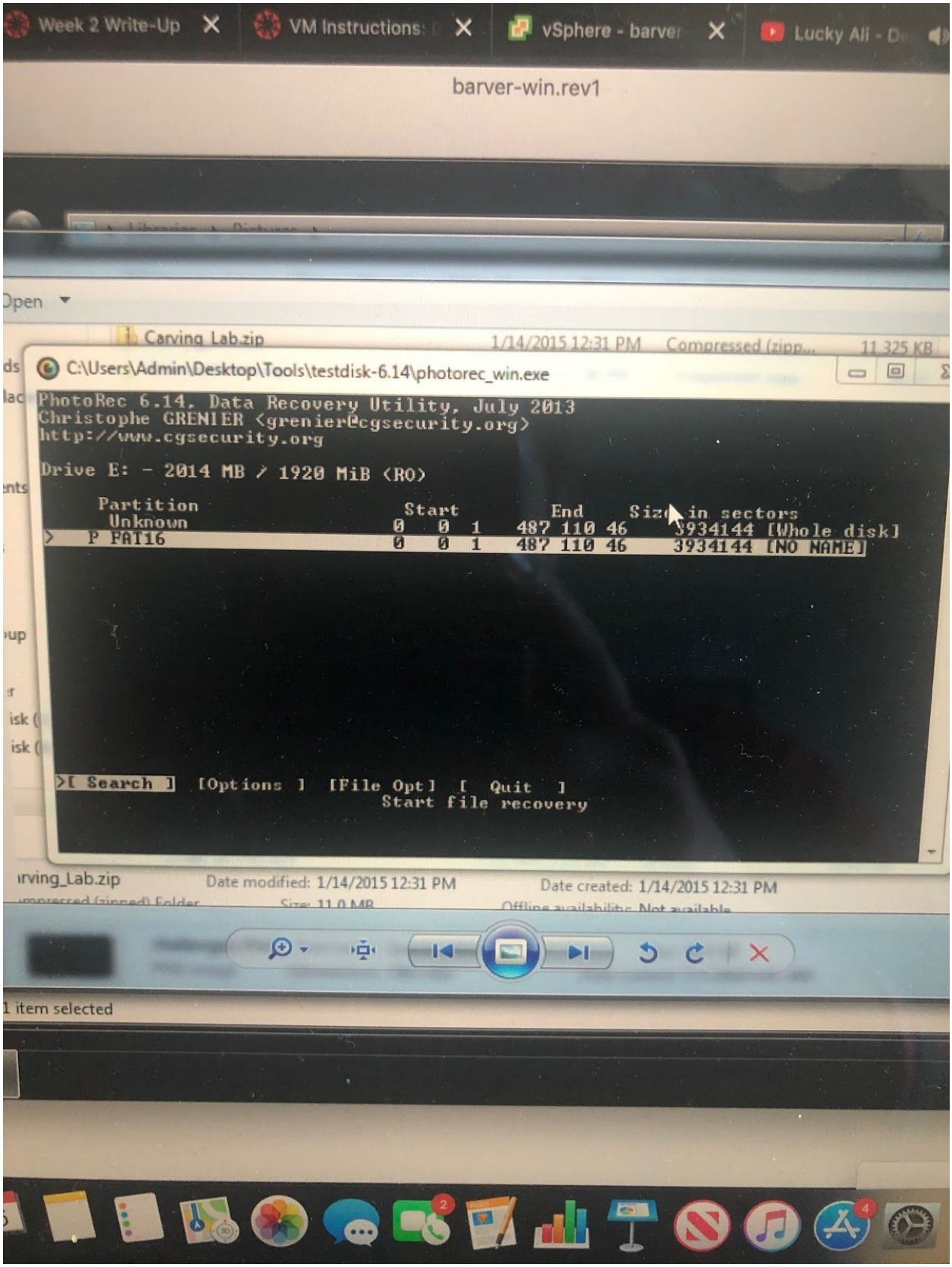
[PhotoRec]: https://www.cgsecurity.org/wiki/PhotoRec

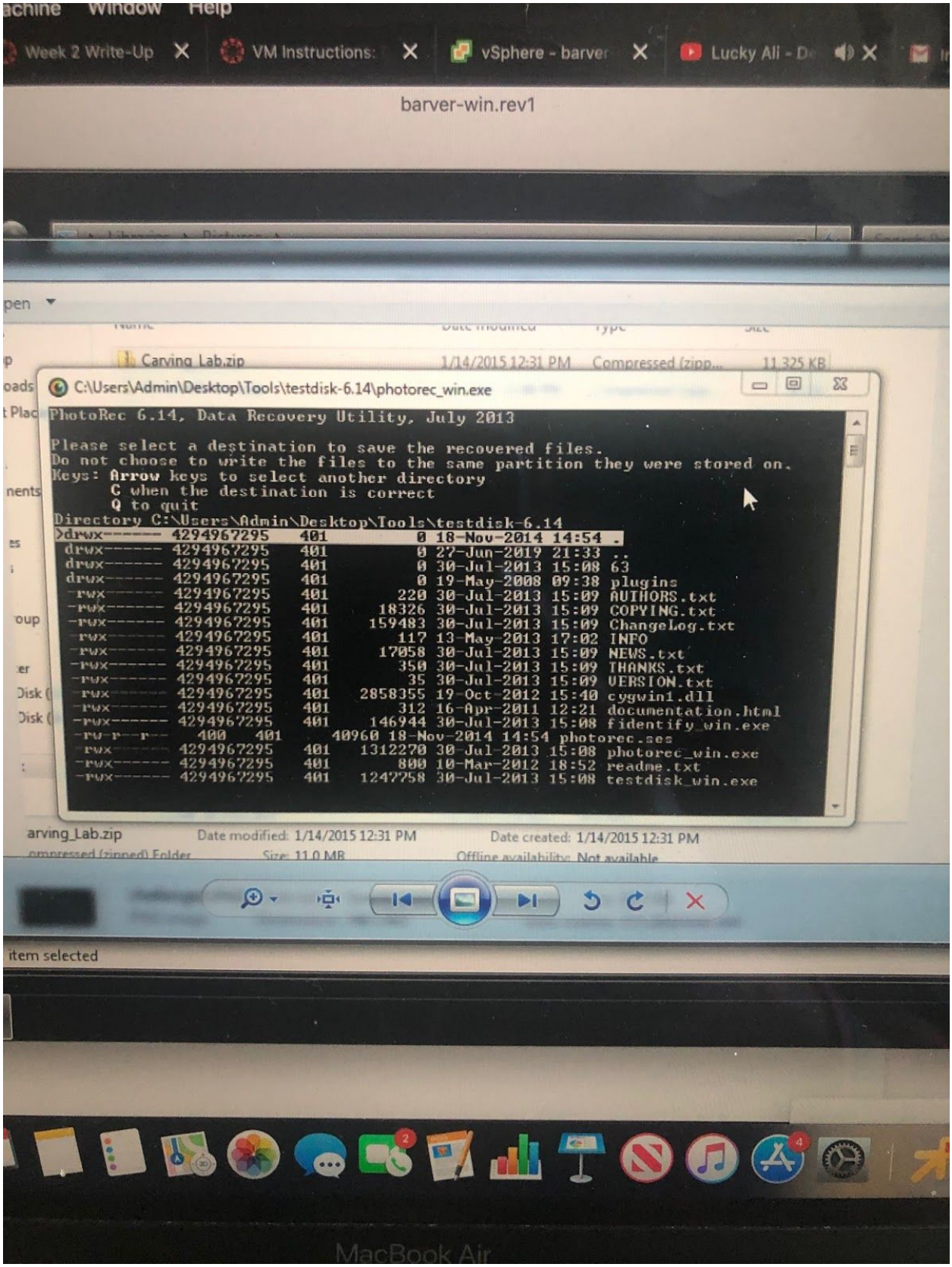
Challenge Discussion & Snapshots

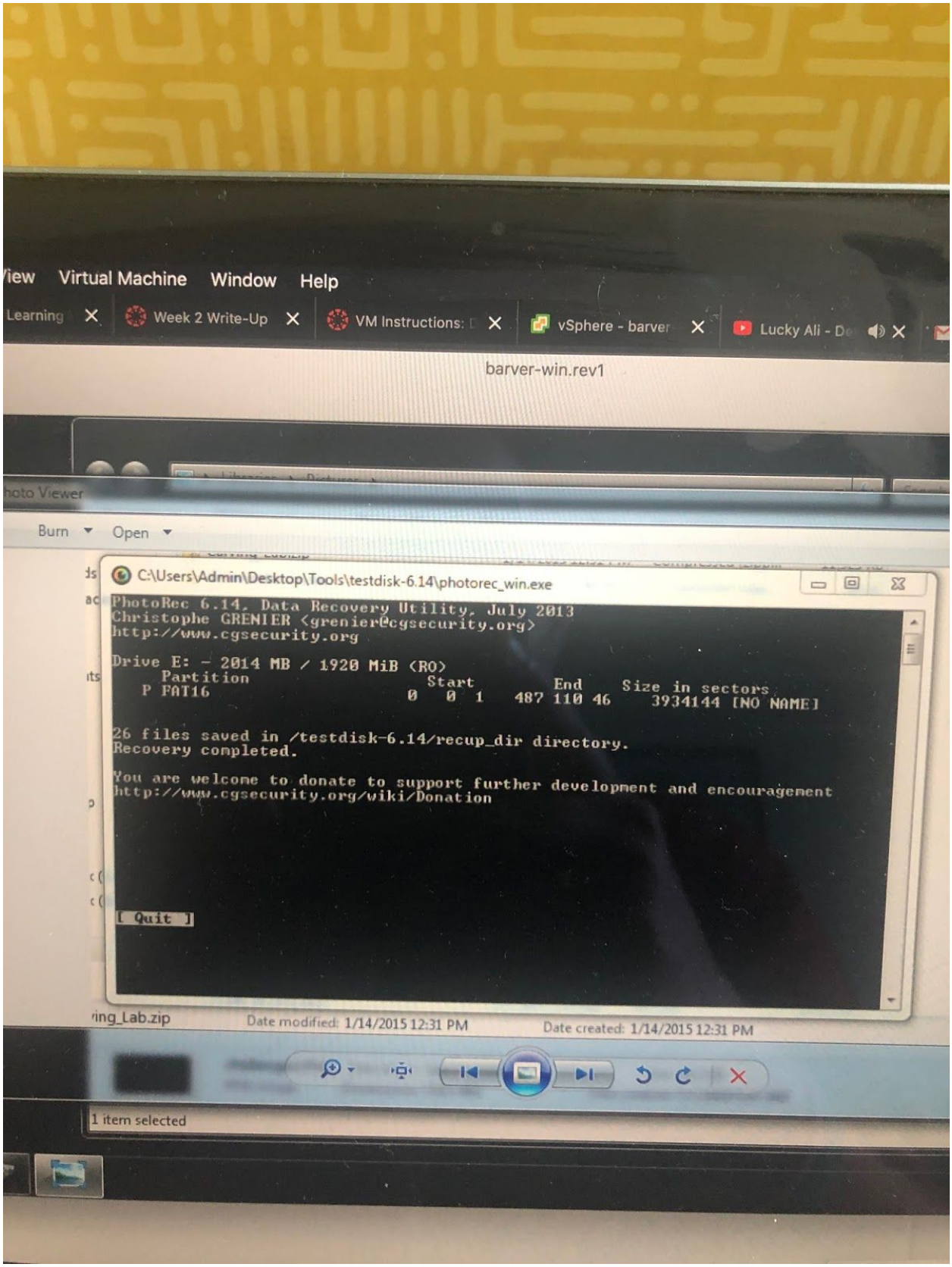
The provided image file was mounted using osfmount and the below contents collected:

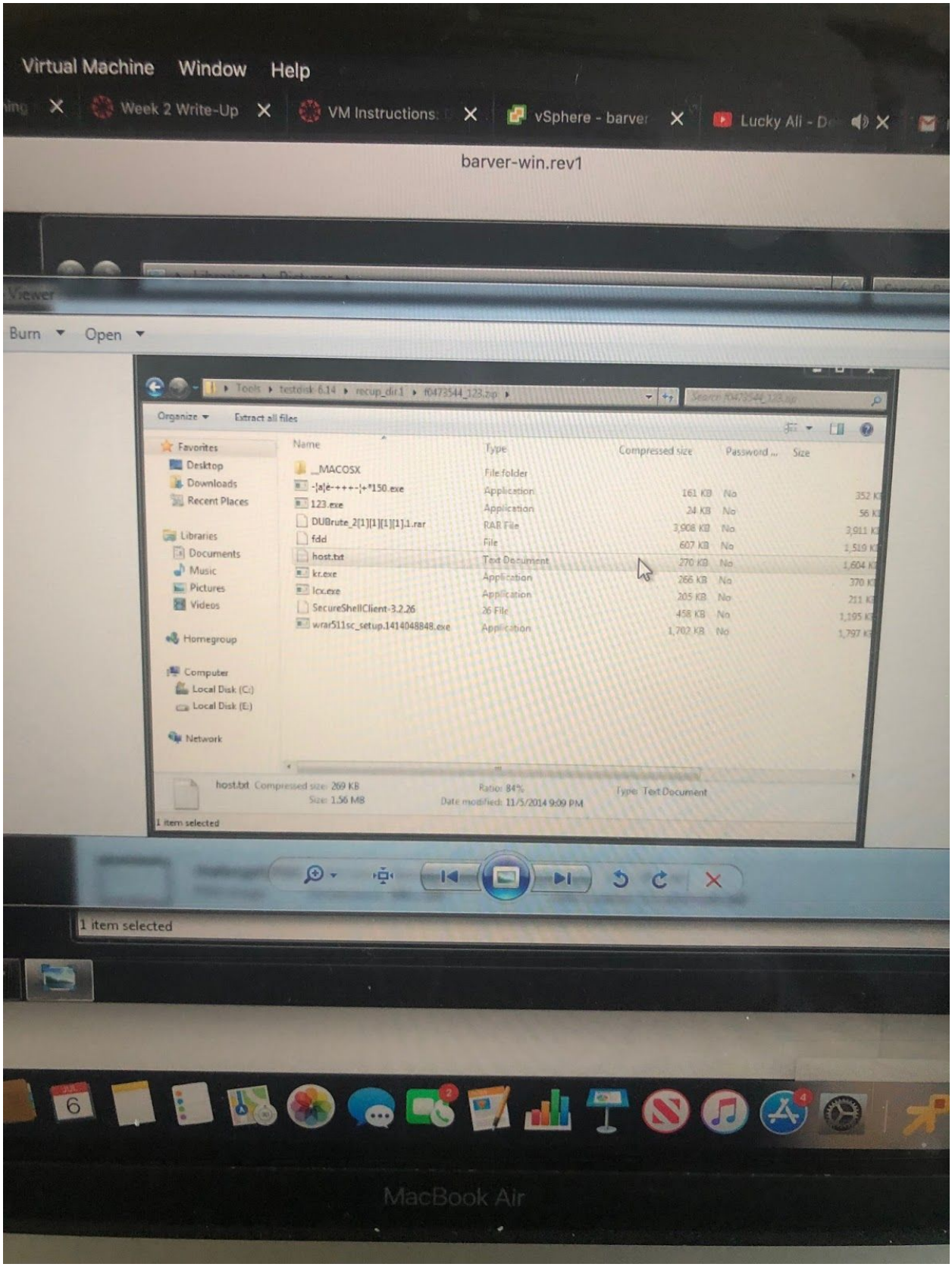

achine Window Help
Week 2 Write-Up
VM Instructions:
vSphere - barver
Lucky Ali - D
barver-win.rev1
pen
Computer ▸ Local Disk (E:) ▸
Organize
Include in library
Share with
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
Local Disk (E:)
Network
Name
Date modified
Type
Size
(조선민주주의인민공화국)_-_애국가.mp3 1/13/2015 8:29 AM MP3 Format Sound 3,210 KB
don't tell mrs Jl Ung.jpg 1/13/2015 8:19 AM JPEG image 574 KB
대상 목록.zip 1/13/2015 8:22 AM Compressed (zipp... 1 KB
루트킷.bin 1/10/2015 10:10 AM BIN File 263 KB
목표.bat 1/10/2015 10:02 AM Windows Batch File 102 KB
목표.png 1/13/2015 8:28 AM PNG image 271 KB
6 items
6 items
Computer
1 item selected

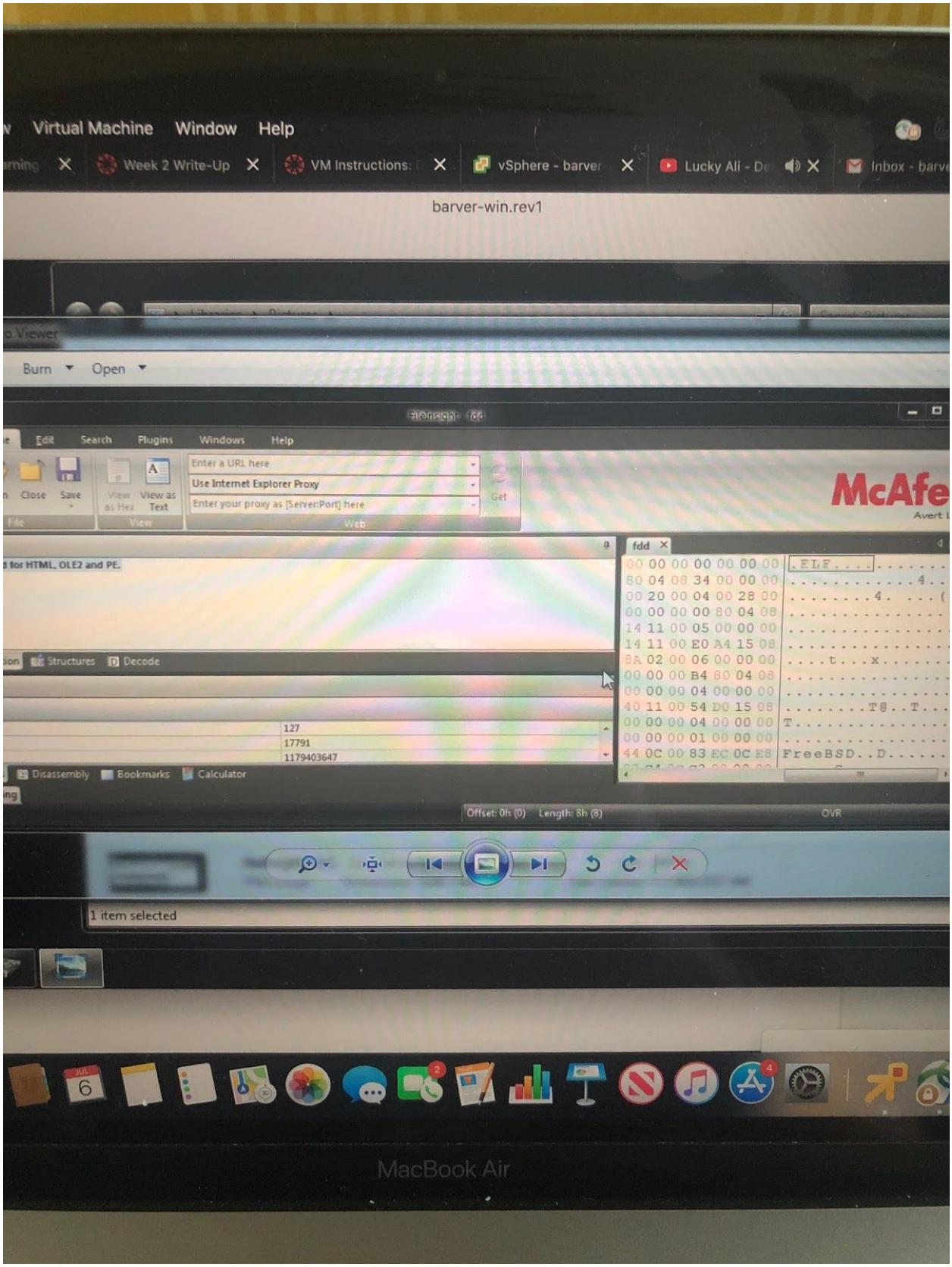
PhotoRec Tool was run and the following contents collected:


Week 2 Write-Up
VM Instructions:
vSphere - barver
barver-win.rev1
Carving_Lab.zip
1/14/2015 12:31 PM
Compressed (zipp...
11,325 KB
C:\Users\Admin\Desktop\Tools\testdisk-6.14\photorec_win.exe
PhotoRec 6.14, Data Recovery Utility, July 2013
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
Drive E: - 2014 MB / 1920 MiB (RO)
Partition Start End Size in sectors
Unknown 0 0 1 487 110 46 3934144 [Whole disk]
> P FAT16 0 0 1 487 110 46 3934144 [NO NAME]
>[Search] [Options] [File Opt] [Quit]
Start file recovery
Date modified: 1/14/2015 12:31 PM
Date created: 1/14/2015 12:31 PM
1 item selected


achine Window Help
Week 2 Write-Up
VM Instructions:
vSphere - barver
Lucky Ali - D
barver-win.rev1
Carving_Lab.zip
1/14/2015 12:31 PM
Compressed (zipp...
11,325 KB
C:\Users\Admin\Desktop\Tools\testdisk-6.14\photorec_win.exe
PhotoRec 6.14, Data Recovery Utility, July 2013
Please select a destination to save the recovered files.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
C when the destination is correct
Q to quit
Directory C:\Users\Admin\Desktop\Tools\testdisk-6.14
>drwx------ 4294967295 401 0 18-Nov-2014 14:54 .
drwx------ 4294967295 401 0 27-Jun-2019 21:33 ..
drwx------ 4294967295 401 0 30-Jul-2013 15:08 63
drwx------ 4294967295 401 0 19-May-2008 09:38 plugins
-rwx------ 4294967295 401 220 30-Jul-2013 15:09 AUTHORS.txt
-rwx------ 4294967295 401 18326 30-Jul-2013 15:09 COPYING.txt
-rwx------ 4294967295 401 159483 30-Jul-2013 15:09 ChangeLog.txt
-rwx------ 4294967295 401 117 13-May-2013 17:02 INFO
-rwx------ 4294967295 401 17058 30-Jul-2013 15:09 NEWS.txt
-rwx------ 4294967295 401 350 30-Jul-2013 15:09 THANKS.txt
-rwx------ 4294967295 401 35 30-Jul-2013 15:09 VERSION.txt
-rwx------ 4294967295 401 2858355 19-Oct-2012 15:40 cygwin1.dll
-rwx------ 4294967295 401 312 16-Apr-2011 12:21 documentation.html
-rwx------ 4294967295 401 146944 30-Jul-2013 15:08 fidentify_win.exe
-rw-r--r-- 400 401 40960 18-Nov-2014 14:54 photorec.ses
-rwx------ 4294967295 401 1312270 30-Jul-2013 15:08 photorec_win.exe
-rwx------ 4294967295 401 800 10-Mar-2012 18:52 readme.txt
-rwx------ 4294967295 401 1247758 30-Jul-2013 15:08 testdisk_win.exe
arving_Lab.zip
Date modified: 1/14/2015 12:31 PM
Date created: 1/14/2015 12:31 PM
item selected
MacBook Air


iew Virtual Machine Window Help
Learning
Week 2 Write-Up
VM Instructions:
vSphere - barver
Lucky Ali - De
barver-win.rev1
hoto Viewer
Burn
Open
C:\Users\Admin\Desktop\Tools\testdisk-6.14\photorec_win.exe
PhotoRec 6.14, Data Recovery Utility, July 2013
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
Drive E: - 2014 MB / 1920 MiB (RO)
Partition Start End Size in sectors
P FAT16 0 0 1 487 110 46 3934144 [NO NAME]
26 files saved in /testdisk-6.14/recup_dir directory.
Recovery completed.
You are welcome to donate to support further development and encouragement
http://www.cgsecurity.org/wiki/Donation
[Quit]
ring_Lab.zip
Date modified: 1/14/2015 12:31 PM
Date created: 1/14/2015 12:31 PM
1 item selected

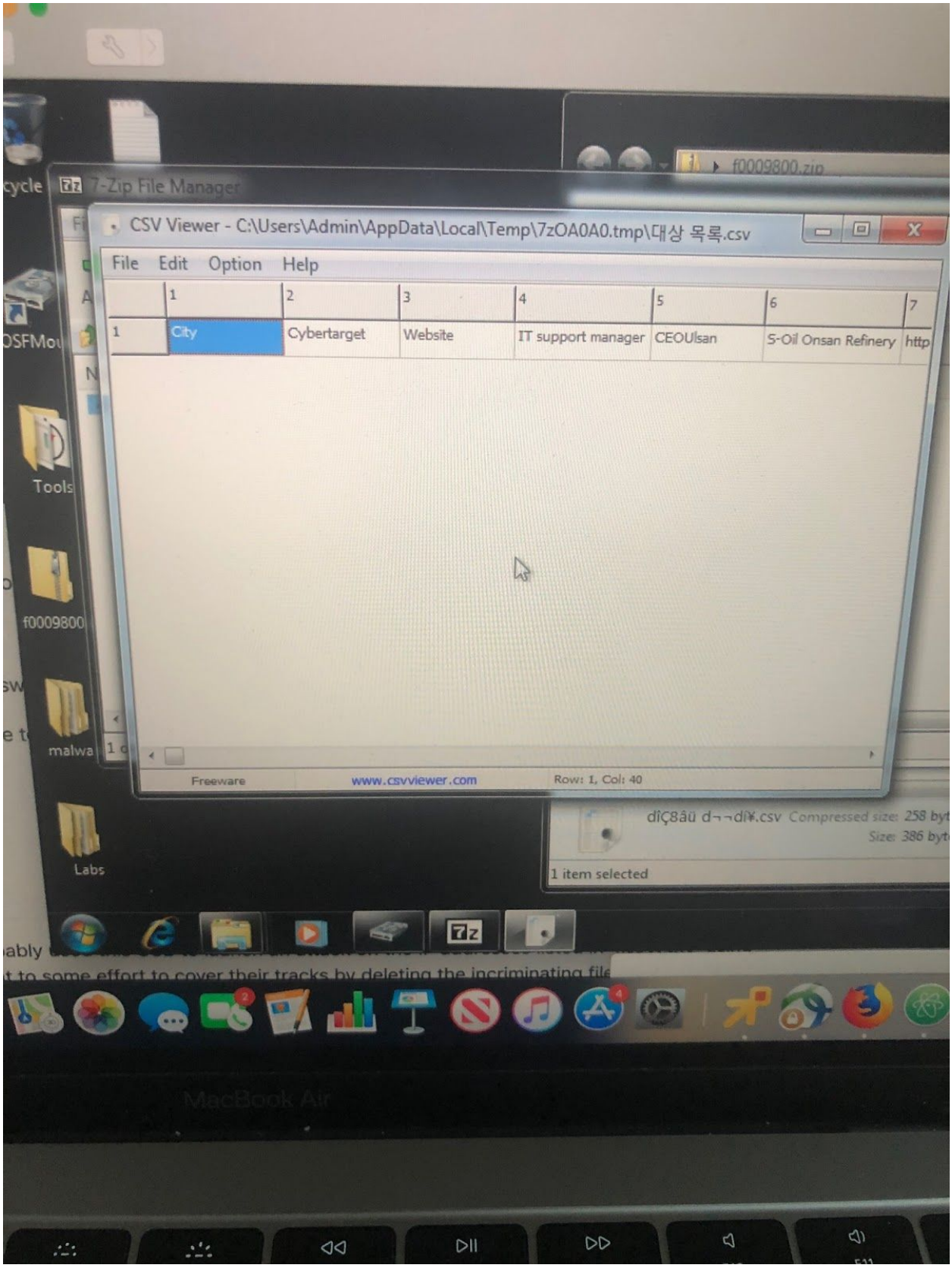

Virtual Machine
Window
Help
Week 2 Write-Up
VM Instructions
vSphere - barver
barver-win.rev1
Burn
Open
Organize
Extract all files
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
Local Disk (E:)
Network
Name
Type
Compressed size
Password ...
Size
_MACOSX
File folder
123.exe
DUBrute_2[1][1][1][1].1.rar
fdd
host.txt
Text Document
kr.exe
lcx.exe
SecureShellClient-3.2.26
wrar511sc_setup.1414048848.exe
host.txt Compressed size: 269 KB
Size: 1.56 MB
Ratio: 84%
Date modified: 11/5/2014 9:09 PM
Type: Text Document
1 item selected
1 item selected
MacBook Air


Virtual Machine
Window
Help
Week 2 Write-Up
VM Instructions:
vSphere - barver
Lucky Ali - De
Inbox - barve
barver-win.rev1
Burn
Open
Edit
Search
Plugins
Windows
Help
Enter a URL here
Use Internet Explorer Proxy
Enter your proxy as [Server:Port] here
Get
Close
Save
View as Hex
View as Text
File
View
Web
McAfe
Avert
for HTML, OLE2 and PE.
Structures
Decode
fdd
.ELF....
FreeBSD..D.....
127
17791
1179403647
Disassembly
Bookmarks
Calculator
Offset: 0h (0)
Length: 8h (8)
OVR
1 item selected
MacBook Air

The hints suggested I take a closer look at one of the jpeg images on the drive to find the password for the zip. I ran that file through the strings unix tool and luckily 1 line made sense:

0x00003B0: ‘pwd:infected123!’.

This data probably lies in the EXIF data of the jpeg file. The password was used the open the .csv file that was found using the osfmount tool:


7-Zip File Manager
f0009800.zip
CSV Viewer - C:\Users\Admin\AppData\Local\Temp\7zOA0A0.tmp\대상 목록.csv
File Edit Option Help
1 2 3 4 5 6 7
1 City Cybertarget Website IT support manager CEOUlsan S-Oil Onsan Refinery http
Freeware www.csvviewer.com Row: 1, Col: 40
1 item selected
Tools
f0009800
malwa
Labs
MacBook Air

Analysis

It seems that someone used the USB to launch an attack on the IP addresses found in the host.txt file using the DuBrute malware. There was also a list of passwords file found that so there might also have been some type of dictionary attack. One of the files was encrypted with a password that was found on the disk. The password was hidden in the jpeg file. This implies that it may have been received from another party.

Acknowledgements:

This post was based on the lectures provided by Christian Beek
Lead Scientist & Principal Engineer at McAfee