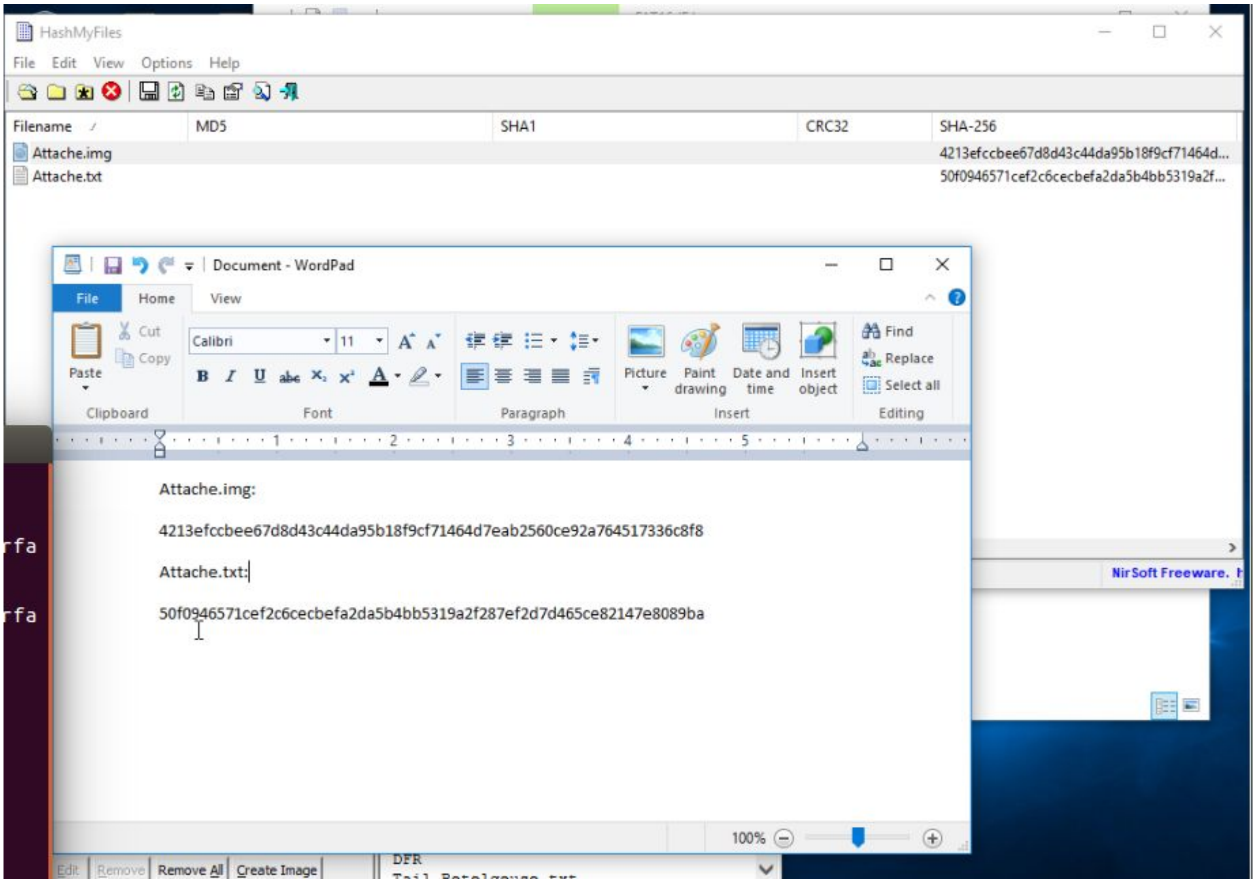
Lab 3 Report
Kevin Rineer
20 Sept 2017

The SHA-256 hashes of the image and log files are below:


HashMyFiles
File Edit View Options Help
Document - WordPad
File Home View
Paste Cut Copy
Calibri 11
Clipboard Font Paragraph Insert Editing
Picture Paint drawing Date and time Insert object
Find Replace Select all
100%
NirSoft Freeware.
Edit Remove Remove All Create Image

Filename	MD5	SHA1	CRC32	SHA-256
Attache.img				4213efccbee67d8d43c44da95b18f9cf71464d...
Attache.txt				50f0946571cef2c6cecbefa2da5b4bb5319a2f...

Attache.img:

4213efccbee67d8d43c44da95b18f9cf71464d7eab2560ce92a764517336c8f8

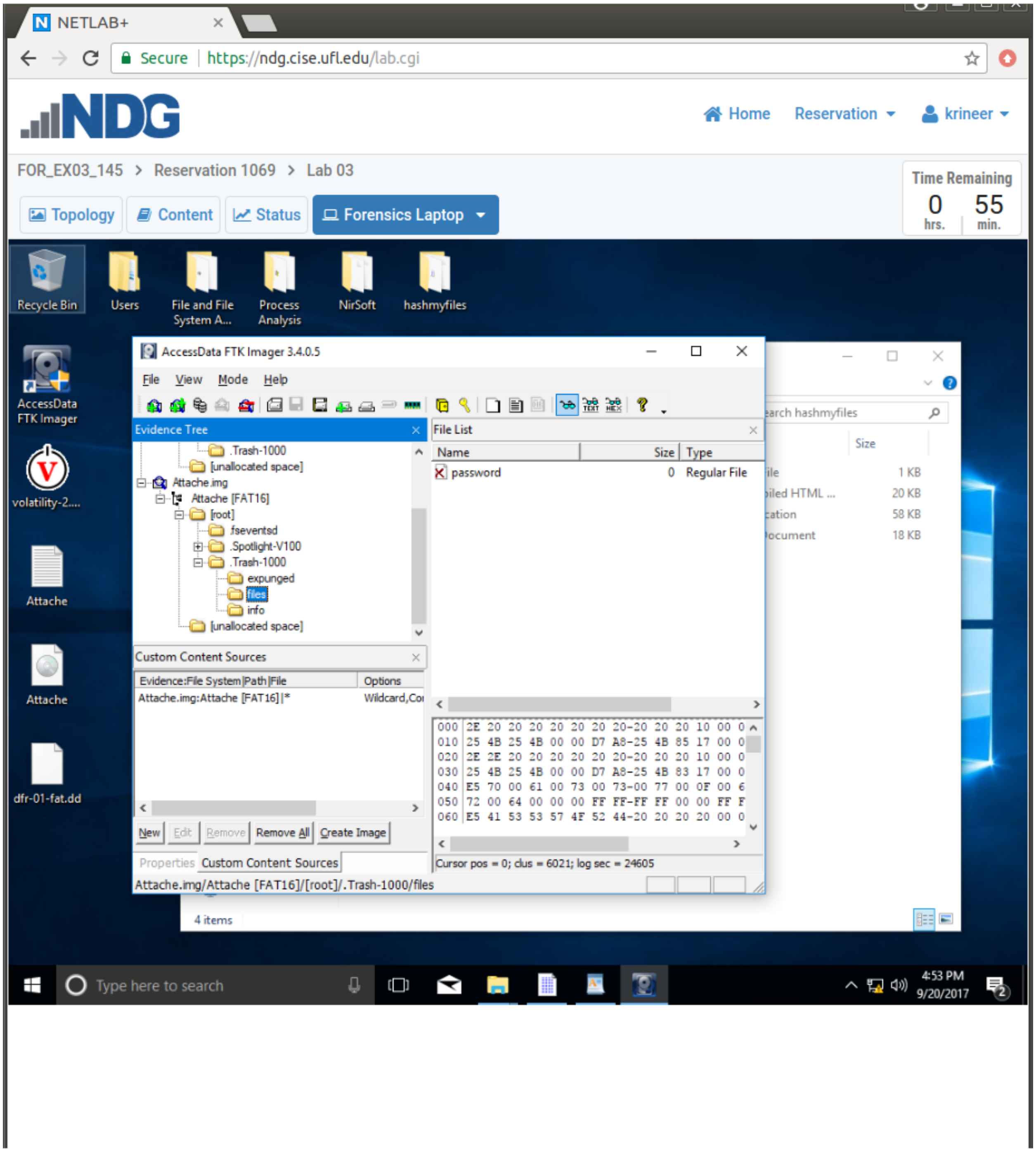
Attache.txt:

50f0946571cef2c6cecbefa2da5b4bb5319a2f287ef2d7d465ce82147e8089ba

These are used to confirm that the image and log files have not been written to in any way.

Lab 3 Report
Kevin Rineer
20 Sept 2017

The FTK image mounting for Attache.img seemed to succeed, but the deleted password seems to have been compromised by anti-forensic software as the file is 0 bytes.



Evidence:File System|Path|File	Options
Attache.img:Attache [FAT16]|*	Wildcard,Co

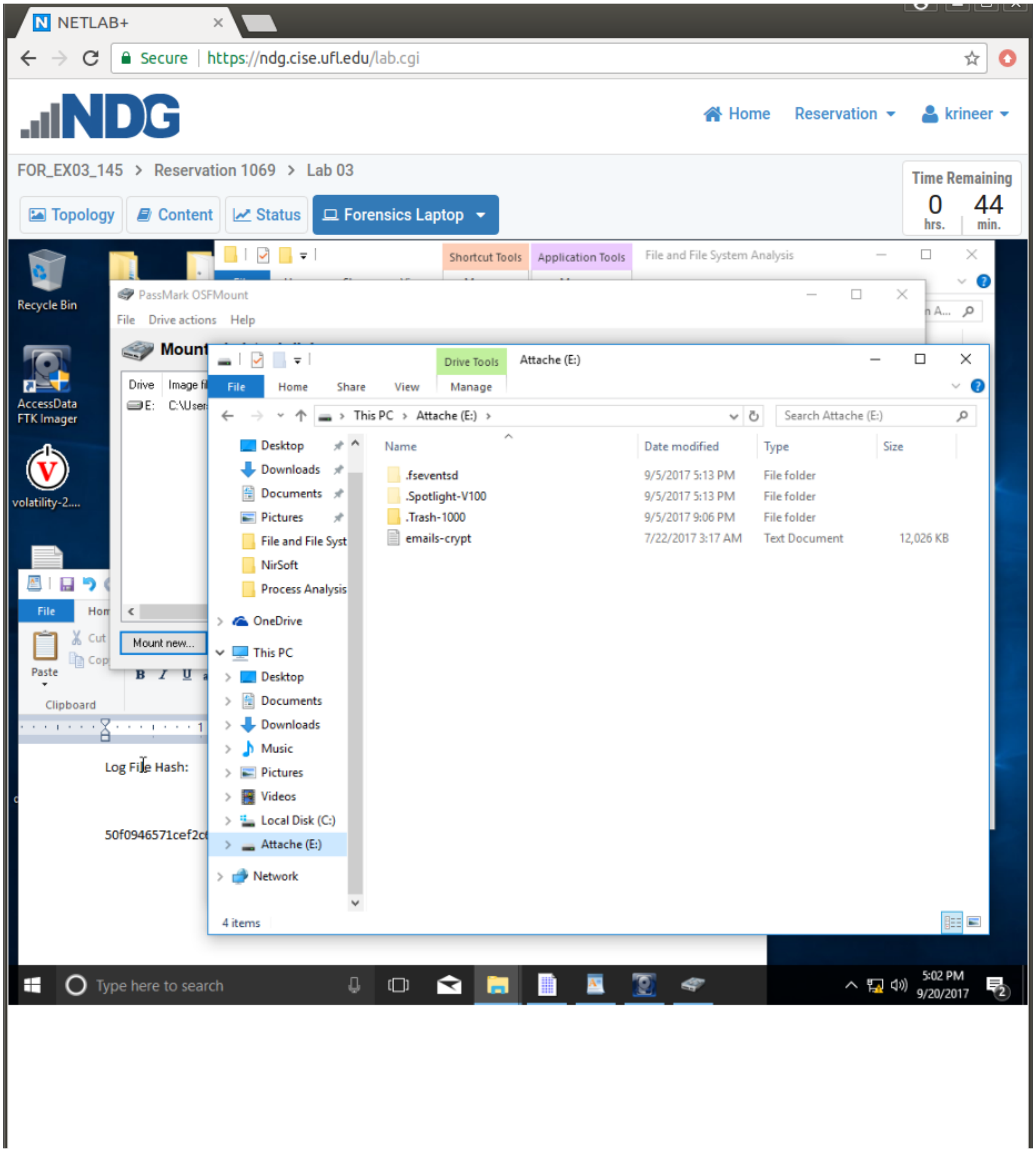
Name	Size	Type
password	0	Regular File

```
000 2E 20 20 20 20 20 20 20-20 20 20 10 00 0
010 25 4B 25 4B 00 00 D7 A8-25 4B 85 17 00 0
020 2E 2E 20 20 20 20 20 20-20 20 20 10 00 0
030 25 4B 25 4B 00 00 D7 A8-25 4B 83 17 00 0
040 E5 70 00 61 00 73 00 73-00 77 00 0F 00 6
050 72 00 64 00 00 00 FF FF-FF FF 00 00 FF F
060 E5 41 53 53 57 4F 52 44-20 20 20 20 00 0
```

Cursor pos = 0; clus = 6021; log sec = 24605

Attache.img/Attache [FAT16]/[root]/.Trash-1000/files

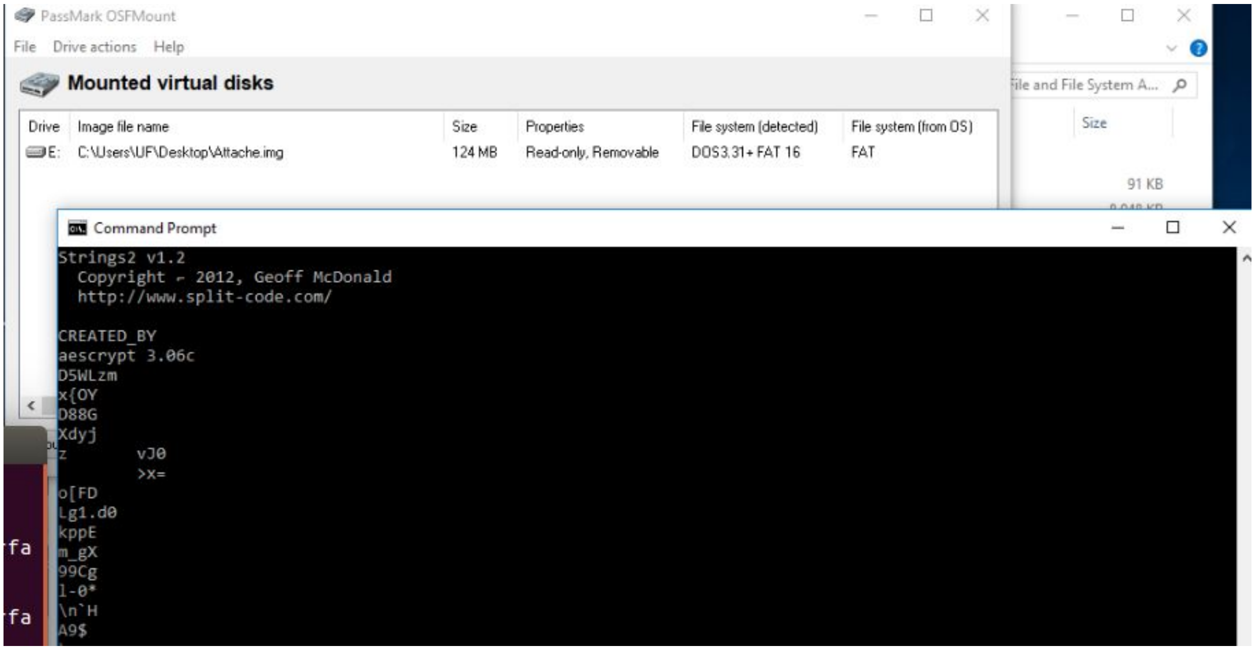
When using OSFMount to look at the logical drive when mount the Attache.img, a files called emails-crypt.txt was found. This file looks to be encrypted via aes. The file likely contained encrypted e-mails, however decryption could take some time if AES-256 is used. It is unfortunate we do not have the key for this encryption.



Name	Date modified	Type	Size
.fseventsd	9/5/2017 5:13 PM	File folder	
.Spotlight-V100	9/5/2017 5:13 PM	File folder	
.Trash-1000	9/5/2017 9:06 PM	File folder	
emails-crypt	7/22/2017 3:17 AM	Text Document	12,026 KB

Log File Hash:

50f0946571cef2c



Mounted virtual disks

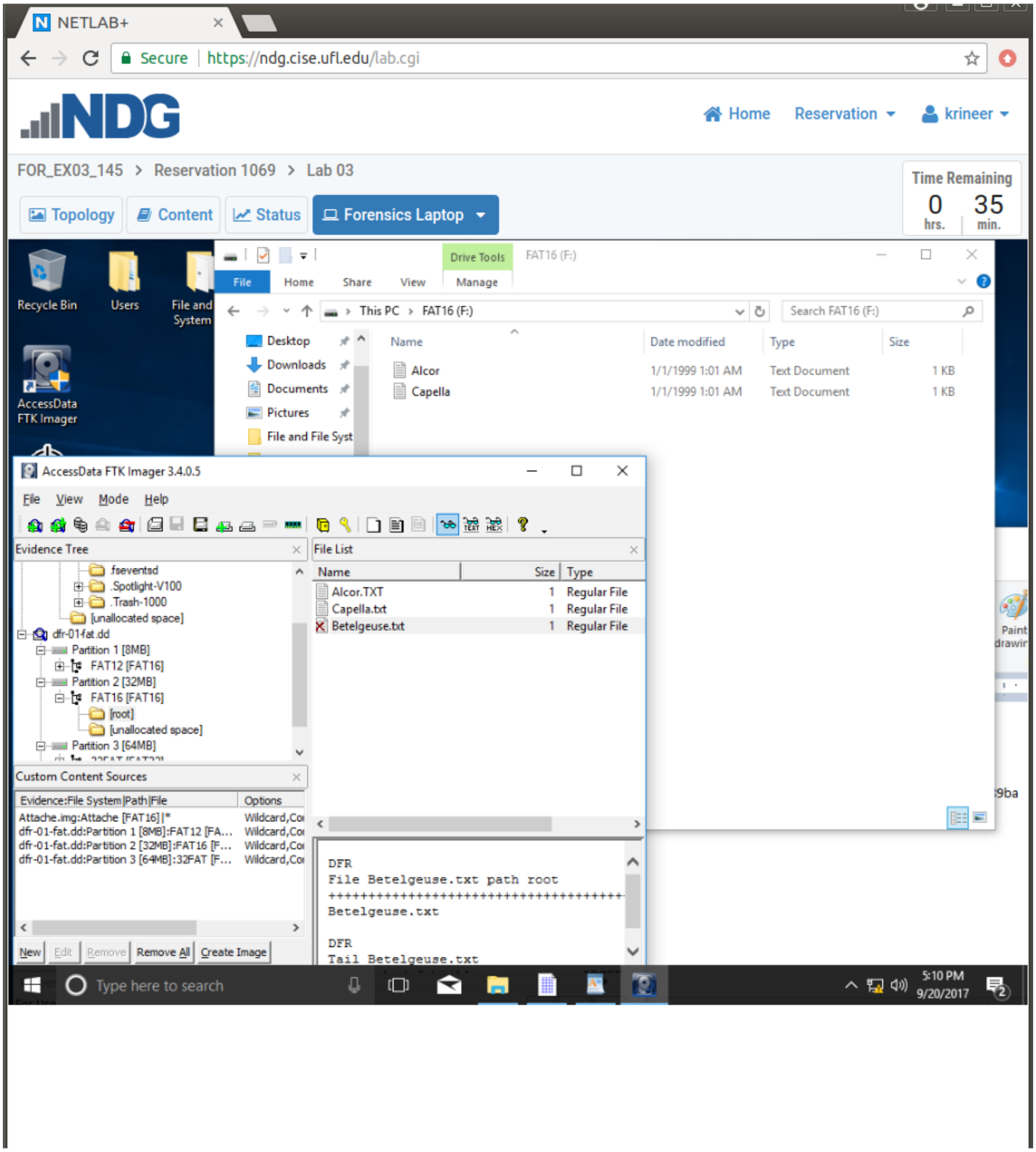
Drive	Image file name	Size	Properties	File system (detected)	File system (from OS)
E:	C:\Users\UF\Desktop\Attache.img	124 MB	Read-only, Removable	DOS3.31+ FAT 16	FAT

```
Strings2 v1.2
  Copyright - 2012, Geoff McDonald
  http://www.split-code.com/

CREATED_BY
aescrypt 3.06c
D5WLzm
x{OY
D88G
Xdyj
z       vJ0
        >x=
o[FD
Lg1.d0
kppE
m_gX
99Cg
l-0*
\n`H
A9$
```

Lab 3 Report
Kevin Rineer
20 Sept 2017

Using the dfr-01-fat.img and FTK Imager, logical drives for E: F: and G: were mounted for evidence collection. It can be seen from the screenshot below that the file Betelgeuse.txt was intended to be deleted by the user, however it is recoverable evidence.



Name	Date modified	Type	Size
Alcor	1/1/1999 1:01 AM	Text Document	1 KB
Capella	1/1/1999 1:01 AM	Text Document	1 KB

Name	Size	Type
Alcor.TXT	1	Regular File
Capella.txt	1	Regular File
Betelgeuse.txt	1	Regular File

Evidence:File System|Path|File	Options
Attache.img:Attache [FAT16]|*	Wildcard,Co
dfr-01-fat.dd:Partition 1 [8MB]:FAT12 [FA...	Wildcard,Co
dfr-01-fat.dd:Partition 2 [32MB]:FAT16 [F...	Wildcard,Co
dfr-01-fat.dd:Partition 3 [64MB]:32FAT [F...	Wildcard,Co

```
DFR
File Betelgeuse.txt path root
+++++++++++++++++++++++++++++++++++++
Betelgeuse.txt

DFR
Tail Betelgeuse.txt
```