Intro to Cyber Forensics Lab Grading Sheet

Project: LAB 4 - ANTI FORESICS
Member Name: **OLUWATOYOSI KEHINDE**
Member Name: **VINUSHA POTTOLA GOUD**
Member Name: **BOINAPELLY AKSHITH ROA**
Member Name: **AMANI PONMAN**
Member Name: **YADLAPALLI IAKSHMIDAR**

Executive Summary__________/ 4 points
+ ✓ -
❑ ❑ ❑ Executive summary is brief and focused to the point of the project
❑ ❑ ❑ The summary clearly illustrates the objectives of the laboratory exercise

Apparatus__________/ 4 points
❑ ❑ ❑ The apparatus are clearly illustrated and documented

Procedures__________/ 12 points
❑ ❑ ❑ Adequate information provided to allow re-creation of work
❑ ❑ ❑ Consistent level of coverage throughout the project – nothing overly detailed or omitted

Problem Solving__________/ 5 points
❑ ❑ ❑ All problems identified
❑ ❑ ❑ Alternative solutions identified
❑ ❑ ❑ Solutions attempted listed
❑ ❑ ❑ Final solution detailed (what fixed the problem and why?)

Conclusions & Recommendations__________/ 5 points
❑ ❑ ❑ Tie back to the learning objectives identified in the executive summary - <u>critical</u>
❑ ❑ ❑ Conclusions stated in a logical fashion
❑ ❑ ❑ Conclusions are viable based on the procedures and results
❑ ❑ ❑ Recommendations practical & relevant

Format & Grammar__________/ 5 points
❑ ❑ ❑ Table of Contents present
❑ ❑ ❑ Report written in past tense
❑ ❑ ❑ Proper voice (no I's, We's, Our's or The group)
❑ ❑ ❑ Paper easy to read (fonts, spacing, etc.)
❑ ❑ ❑ Proper credit given to sources in bibliography (APA style)
❑ ❑ ❑ Paper is cohesive and consistent in tone
________ Spelling & grammar errors: *minus one half point for each, up to a max deduction of 5 points – at that time, paper is returned for correction and re-submission with a one letter grade penalty.*

Final Score:________________/ 35

TABLE OF CONTENT

Following the procedures discussed in the lecture, the following solutions to the questions in the Lab 04-Anti-Forensics paper were found during the lab exercise.

Part 1 – Automated Nightmare?

1. Copy the contents of **to Lab05 folder** to Desktop.

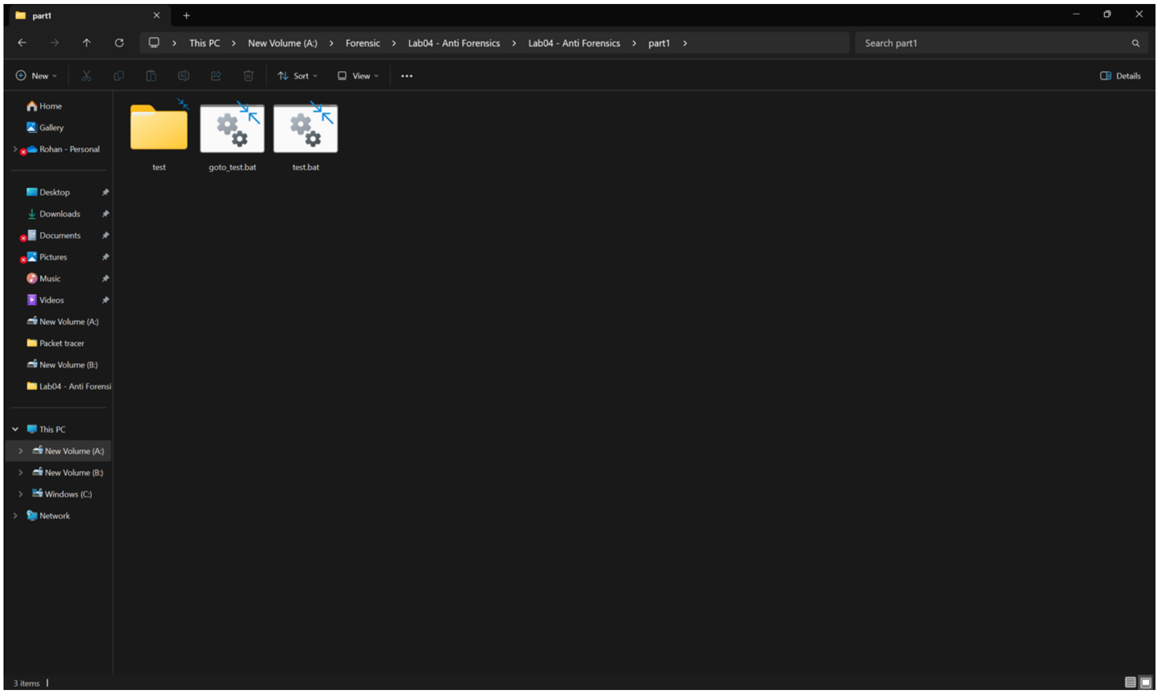
2. Go into the part1 folder and edit the test.bat file with Notepad.

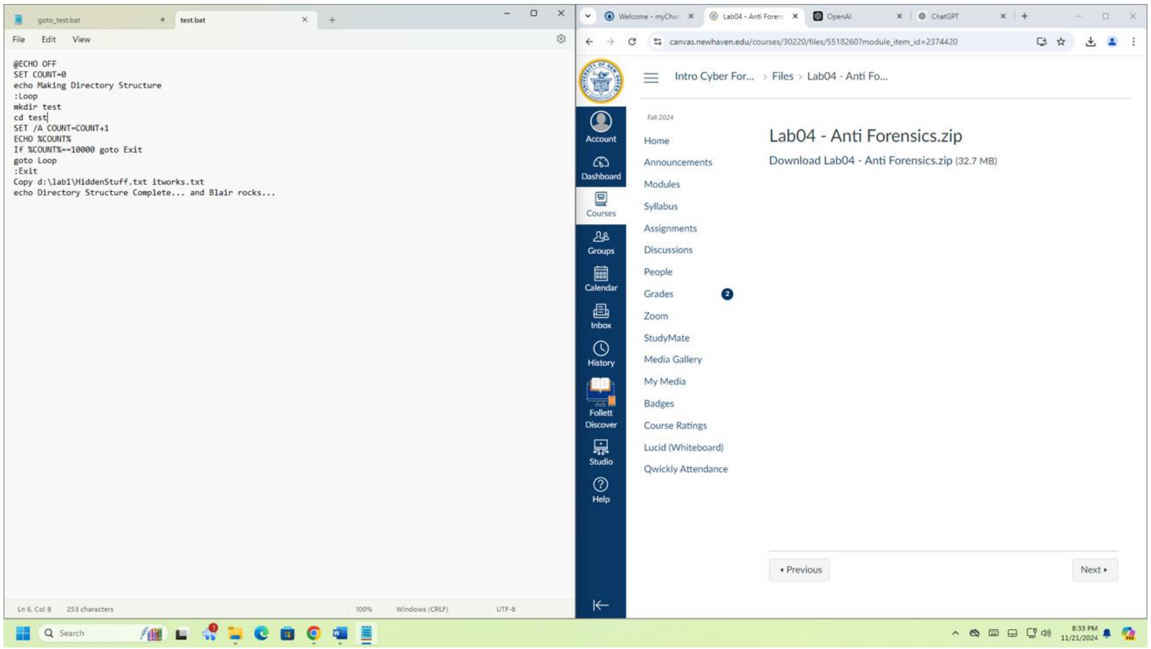
    a. **Briefly** describe what this batch file does:

    This Windows batch run regularly builds a folder called test inside itself up to 10,000 levels deep while maintaining count, resulting in a deeply nested directory structure. Following the loop's conclusion, it tries to move the HiddenStuff.txt file from d:\lab1 to the current directory, changing its name to itworks.txt. The successful message "Directory Structure Complete... and Blair rocks..." is printed at the end of the script. This script is entertaining or experimental, but if it is stopped before it is finished, it may cause system problems like disk space exhaustion.

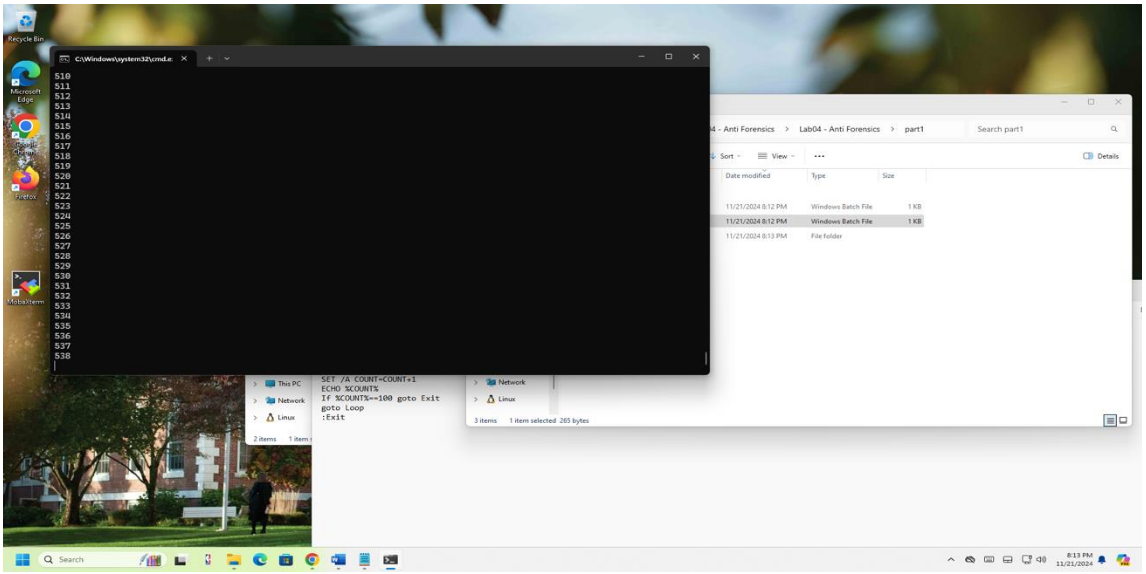
Close the test.bat file.

3. Run the test.bat file.



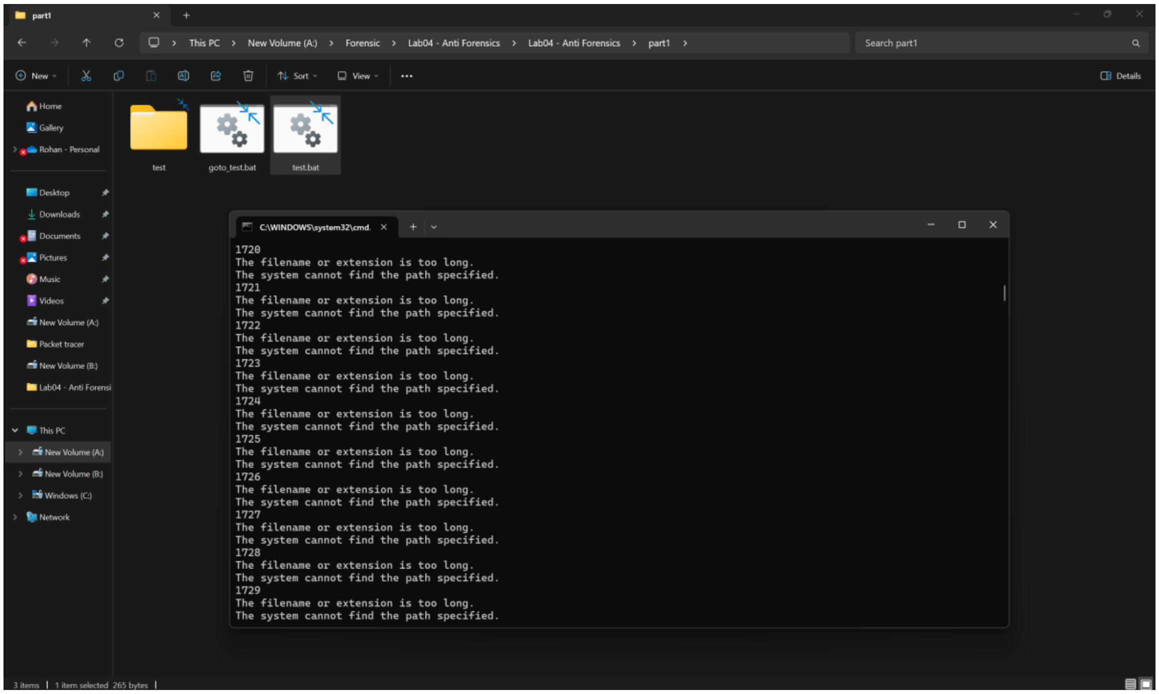


```
@ECHO OFF
SET COUNT=0
echo Making Directory Structure
:Loop
mkdir test
cd test
SET /A COUNT=COUNT+1
ECHO %COUNT%
If %COUNT%==10000 goto Exit
goto Loop
:Exit
Copy d:\lab1\HiddenStuff.txt itworks.txt
echo Directory Structure Complete... and Blair rocks...
```



```
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
```

```
SET /A COUNT=COUNT+1
ECHO %COUNT%
If %COUNT%==100 goto Exit
goto Loop
:Exit
```

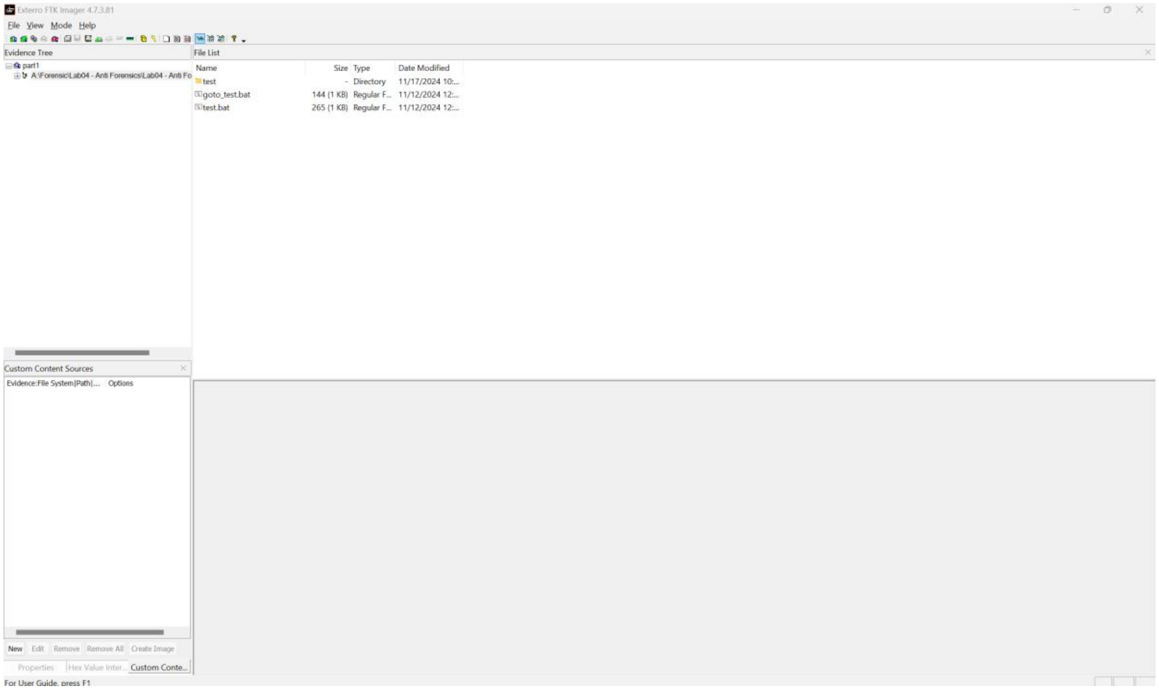


```
1720
The filename or extension is too long.
The system cannot find the path specified.
1721
The filename or extension is too long.
The system cannot find the path specified.
1722
The filename or extension is too long.
The system cannot find the path specified.
1723
The filename or extension is too long.
The system cannot find the path specified.
1724
The filename or extension is too long.
The system cannot find the path specified.
1725
The filename or extension is too long.
The system cannot find the path specified.
1726
The filename or extension is too long.
The system cannot find the path specified.
1727
The filename or extension is too long.
The system cannot find the path specified.
1728
The filename or extension is too long.
The system cannot find the path specified.
1729
The filename or extension is too long.
The system cannot find the path specified.
```

Forensic ToolKit (Install v1.62) – It is OK that it is not the FULL Version!
Examine the part1 folder using FTK by adding the folder to be analyzed.

1. What evidence was found?

   The presence of deeply nested directories should be disclosed by the analysis.
   The contents of HiddenStuff.txt are copied and renamed to itworks.txt if it is found in d:\lab1. The real creation times of the generated files and folders should be ascertained by looking at their metadata or timestamps.


Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
File List
Custom Content Sources
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1

part1
A:\Forensic\Lab04 - Anti Forensics\Lab04 - Anti Fo

Name	Size	Type	Date Modified
test	-	Directory	11/17/2024 10:...
goto_test.bat	144 (1 KB)	Regular F...	11/12/2024 12:...
test.bat	265 (1 KB)	Regular F...	11/12/2024 12:...

Evidence:File System|Path|...	Options

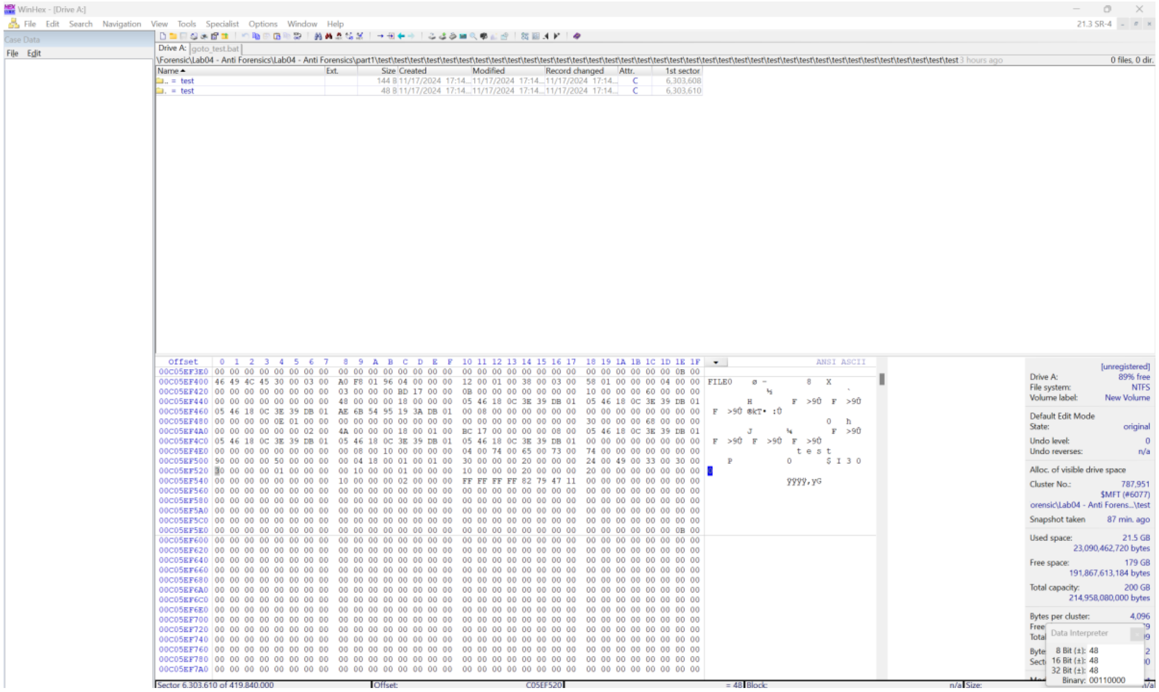
WinHex

1. Right Click on WinHex.exe and Run as Administrator
2. Open with WinHex (From the folder it is provided in, if you have license issue, delete the file WinHex.cfg from the WinHex Folder)
3. Tools → Open Disk (Choose C: partition).
4. Take a new volume snapshot (Tools | Disk Tools | Take New Volume Snapshot) in case WinHex is using an older one.
5. Browse to part1 folder using the Directory Browser (Ctrl+F7 if not already up).
6. Click through ALL the test folders created by the script until something bad happens…
   a. What happened?

Clicking on all 27 test folders resulted in an Error #1 popup stating, "Cannot open File". Please check the path and access rights.

7. If the deeply nested folder structure surpasses the system's resource or path length constraints, WinHex may crash or stop working.
   Although the exact number of folders visited varies from system to system, it typically takes between 255 and 260 nested directories before issues occur.

   a. Approximately how many folders did you go through before this?
      27


WinHex - [Drive A:]
File Edit Search Navigation View Tools Specialist Options Window Help
21.3 SR-4
Case Data
File Edit
Drive A: goto_test.bat

\Forensic\Lab04 - Anti Forensics\Lab04 - Anti Forensics\part1\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test 3 hours ago 0 files, 0 dir.

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
.. = test		144 B	11/17/2024 17:14...	11/17/2024 17:14...	11/17/2024 17:14...	C	6,303,608
. = test		48 B	11/17/2024 17:14...	11/17/2024 17:14...	11/17/2024 17:14...	C	6,303,610

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F  10 11 12 13 14 15 16 17  18 19 1A 1B 1C 1D 1E 1F   ANSI ASCII
00C05EF3E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 0B 00
00C05EF400  46 49 4C 45 30 00 03 00  A0 F8 01 96 04 00 00 00  12 00 01 00 38 00 03 00  58 01 00 00 00 04 00 00  FILE0   ø -        8   X
00C05EF420  00 00 00 00 00 00 00 00  03 00 00 00 BD 17 00 00  0B 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00           ½              `
00C05EF440  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00  05 46 18 0C 3E 39 DB 01  05 46 18 0C 3E 39 DB 01          H        F  >9Û  F  >9Û
00C05EF460  05 46 18 0C 3E 39 DB 01  AE 6B 54 95 19 3A DB 01  00 08 00 00 00 00 00 00  00 00 00 00 00 00 00 00   F  >9Û ®kT• :Û
00C05EF480  00 00 00 00 0E 01 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  30 00 00 00 68 00 00 00                          0   h
00C05EF4A0  00 00 00 00 00 00 02 00  4A 00 00 00 18 00 01 00  BC 17 00 00 00 00 08 00  05 46 18 0C 3E 39 DB 01          J        ¼         F  >9Û
00C05EF4C0  05 46 18 0C 3E 39 DB 01  05 46 18 0C 3E 39 DB 01  05 46 18 0C 3E 39 DB 01  00 00 00 00 00 00 00 00   F  >9Û  F  >9Û  F  >9Û
00C05EF4E0  00 00 00 00 00 00 00 00  00 08 00 10 00 00 00 00  04 00 74 00 65 00 73 00  74 00 00 00 00 00 00 00                    t e s t
00C05EF500  90 00 00 00 50 00 00 00  00 04 18 00 01 00 01 00  30 00 00 00 20 00 00 00  24 00 49 00 33 00 30 00      P          0         $ I 3 0
00C05EF520  30 00 00 00 01 00 00 00  00 10 00 00 01 00 00 00  10 00 00 00 20 00 00 00  20 00 00 00 00 00 00 00  0
00C05EF540  00 00 00 00 00 00 00 00  10 00 00 00 02 00 00 00  FF FF FF FF 82 79 47 11  00 00 00 00 00 00 00 00                  ÿÿÿÿ‚yG
00C05EF560  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF580  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF5A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF5C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF5E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 0B 00
00C05EF600  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF620  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF640  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF660  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF680  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF6A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF6C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF6E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF700  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF720  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF740  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF760  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF780  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00C05EF7A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

[unregistered]
Drive A: 89% free
File system: NTFS
Volume label: New Volume

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

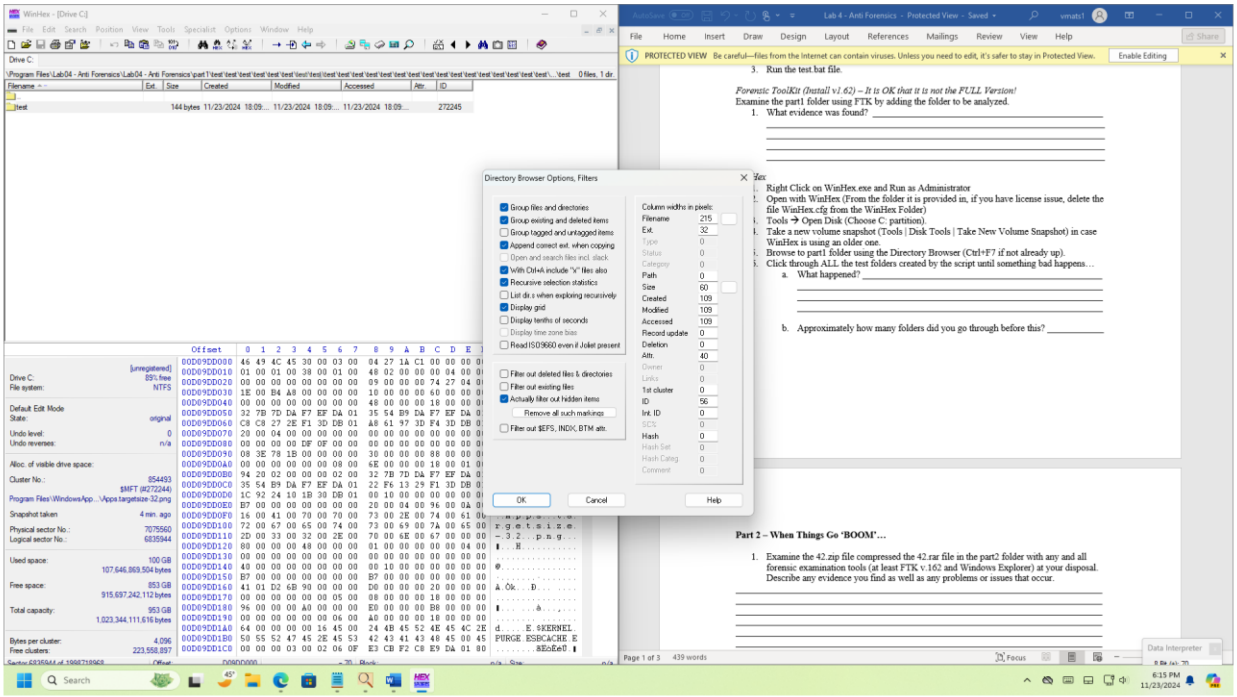
Alloc. of visible drive space
Cluster No.: 787,951
$MFT (#6077)
orensic\Lab04 - Anti Forens...\test
Snapshot taken 87 min. ago

Used space: 21.5 GB
23,090,462,720 bytes
Free space: 179 GB
191,867,613,184 bytes
Total capacity: 200 GB
214,958,080,000 bytes

Bytes per cluster: 4,096

Data Interpreter
8 Bit (±): 48
16 Bit (±): 48
32 Bit (±): 48
Binary: 00110000

Sector 6,303,610 of 419,840,000 | Offset: C05EF520 | = 48 | Block: n/a | Size: n/a


WinHex - [Drive C:]
File Edit Search Position View Tools Specialist Options Window Help
Drive C:

\Program Files\Lab04 - Anti Forensics\Lab04 - Anti Forensics\part1\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\...\test 0 files, 1 dir.

Filename	Ext.	Size	Created	Modified	Accessed	Attr.	ID
..							
test		144 bytes	11/23/2024 18:09:...	11/23/2024 18:09:...	11/23/2024 18:09:...		272245

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E
00D09DD000  46 49 4C 45 30 00 03 00  04 27 1A C1 00 00 00
00D09DD010  01 00 01 00 38 00 01 00  48 02 00 00 00 04 00
00D09DD020  00 00 00 00 00 00 00 00  09 00 00 00 74 27 04
00D09DD030  1E 00 B4 A8 00 00 00 00  10 00 00 00 60 00 00
00D09DD040  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00
00D09DD050  32 7B 7D DA F7 EF DA 01  35 54 B9 DA F7 EF DA
00D09DD060  C8 C8 27 2E F1 3D DB 01  A8 61 97 3D F4 3D DB
00D09DD070  20 00 04 00 00 00 00 00  00 00 00 00 00 00 00
00D09DD080  00 00 00 00 DF 0F 00 00  00 00 00 00 00 00 00
00D09DD090  08 3E 78 1B 00 00 00 00  30 00 00 00 88 00 00
00D09DD0A0  00 00 00 00 00 00 08 00  6E 00 00 00 18 00 01
00D09DD0B0  94 20 02 00 00 00 02 00  32 7B 7D DA F7 EF DA
00D09DD0C0  35 54 B9 DA F7 EF DA 01  22 F6 13 29 F1 3D DB
00D09DD0D0  1C 92 24 10 1B 30 DB 01  00 10 00 00 00 00 00
00D09DD0E0  B7 00 00 00 00 00 00 00  20 00 04 00 96 00 0A
00D09DD0F0  16 00 41 00 70 00 70 00  73 00 2E 00 74 00 61 00  ..a.p.p.s...t.a.
00D09DD100  72 00 67 00 65 00 74 00  73 00 69 00 7A 00 65 00  r.g.e.t.s.i.z.e.
00D09DD110  2D 00 33 00 32 00 2E 00  70 00 6E 00 67 00 00 00  -.3.2...p.n.g...
00D09DD120  80 00 00 00 48 00 00 00  01 00 00 00 00 00 04 00  ▮...H...........
00D09DD130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00D09DD140  40 00 00 00 00 00 00 00  00 10 00 00 00 00 00 00  @...............
00D09DD150  B7 00 00 00 00 00 00 00  B7 00 00 00 00 00 00 00  ................
00D09DD160  41 01 D2 6B 90 00 00 00  D0 00 00 00 20 00 00 00  A.Òk...Ð........
00D09DD170  00 00 00 00 00 00 05 00  08 00 00 00 18 00 00 00  ................
00D09DD180  96 00 00 00 A0 00 00 00  E0 00 00 00 B8 00 00 00  ▮.......à...,...
00D09DD190  00 00 00 00 00 00 06 00  A0 00 00 00 18 00 00 00  ................
00D09DD1A0  64 00 00 00 00 16 45 00  24 4B 45 52 4E 45 4C 2E  d.....E.$KERNEL.
00D09DD1B0  50 55 52 47 45 2E 45 53  42 43 41 43 48 45 00 45  PURGE.ESBCACHE.E
00D09DD1C0  00 00 00 03 00 02 06 0F  E3 CB F2 C8 E9 DA 01 80  ........ãËòÈéÚ.▮
```

[unregistered]
Drive C: 89% free
File system: NTFS

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Alloc. of visible drive space:
Cluster No.: 854493
$MFT (#272244)
Program Files\WindowsApp...\Apps.targetsize-32.png
Snapshot taken 4 min. ago
Physical sector No.: 7075560
Logical sector No.: 6835944

Used space: 100 GB
107,646,869,504 bytes
Free space: 853 GB
915,697,242,112 bytes
Total capacity: 953 GB
1,023,344,111,616 bytes

Bytes per cluster: 4,096
Free clusters: 223,558,897

Sector 6835944 of 1998718968 | Offset: D09DD000 | = 70 | Block: n/a | Size: n/a

Directory Browser Options, Filters

☑ Group files and directories
☑ Group existing and deleted items
☐ Group tagged and untagged items
☑ Append correct ext. when copying
☐ Open and search files incl. slack
☑ With Ctrl+A include "x" files also
☑ Recursive selection statistics
☐ List dir.s when exploring recursively
☑ Display grid
☐ Display tenths of seconds
☐ Display time zone bias
☐ Read ISO9660 even if Joliet present

☐ Filter out deleted files & directories
☐ Filter out existing files
☑ Actually filter out hidden items
Remove all such markings
☐ Filter out $EFS, INDX, BTM attr.

Column widths in pixels:

Filename	215
Ext.	32
Type	0
Status	0
Category	0
Path	0
Size	60
Created	109
Modified	109
Accessed	109
Record update	0
Deletion	0
Attr.	40
Owner	0
Links	0
1st cluster	0
ID	56
Int. ID	0
SC%	0
Hash	0
Hash Set	0
Hash Categ.	0
Comment	0

AutoSave
Lab 4 - Anti Forensics - Protected View - Saved
vmats1
File Home Insert Draw Design Layout References Mailings Review View Help
Share

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing

3. Run the test.bat file.

Forensic ToolKit (Install v1.62) – It is OK that it is not the FULL Version!
Examine the part1 folder using FTK by adding the folder to be analyzed.

1. What evidence was found? ____

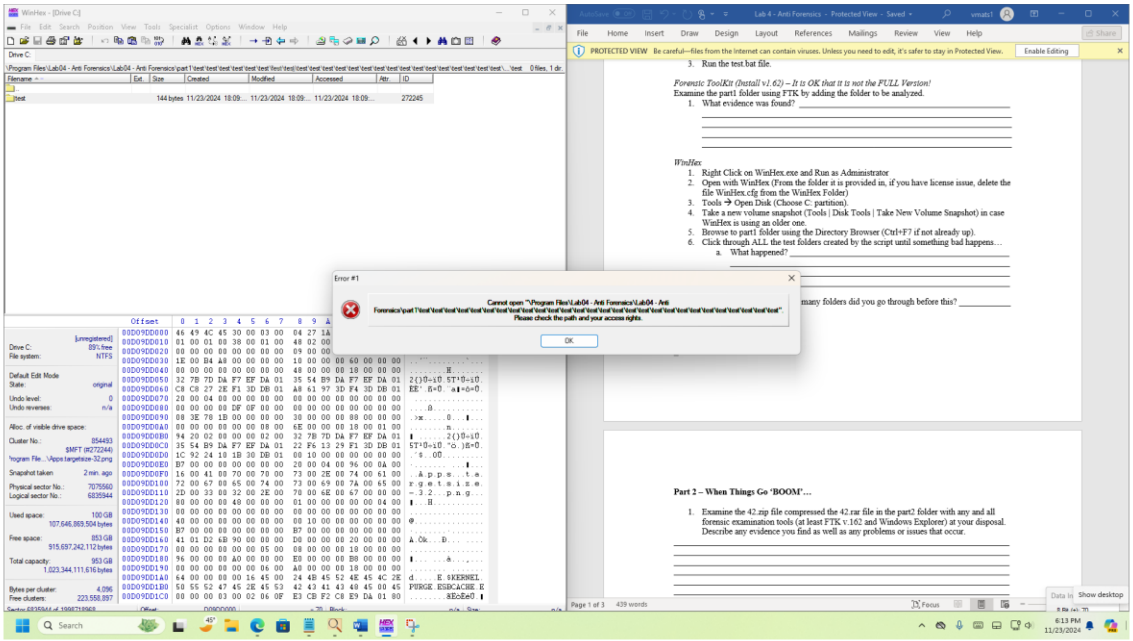
[WinH]ex

1. Right Click on WinHex.exe and Run as Administrator
2. Open with WinHex (From the folder it is provided in, if you have license issue, delete the file WinHex.cfg from the WinHex Folder)
3. Tools → Open Disk (Choose C: partition).
4. Take a new volume snapshot (Tools | Disk Tools | Take New Volume Snapshot) in case WinHex is using an older one.
5. Browse to part1 folder using the Directory Browser (Ctrl+F7 if not already up).
6. Click through ALL the test folders created by the script until something bad happens…
   a. What happened? ____
   b. Approximately how many folders did you go through before this? __________

Part 2 – When Things Go 'BOOM'…

1. Examine the 42.zip file compressed the 42.rar file in the part2 folder with any and all forensic examination tools (at least FTK v.162 and Windows Explorer) at your disposal. Describe any evidence you find as well as any problems or issues that occur.

____



\Program Files\Lab04 - Anti Forensics\Lab04 - Anti Forensics\part1\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\...\test 0 files, 1 dir.

Filename	Ext.	Size	Created	Modified	Accessed	Attr.	ID
..							
test		144 bytes	11/23/2024 18:09:...	11/23/2024 18:09:...	11/23/2024 18:09:...		272245

	[unregistered]
Drive C:	89% free
File system:	NTFS
Default Edit Mode	
State:	original
Undo level:	0
Undo reverses:	n/a
Alloc. of visible drive space:	
Cluster No.:	854493
	$MFT (#272244)
'rogram File...\Apps.targetsize-32.png	
Snapshot taken	2 min. ago
Physical sector No.:	7075560
Logical sector No.:	6835944
Used space:	100 GB
	107,646,869,504 bytes
Free space:	853 GB
	915,697,242,112 bytes
Total capacity:	953 GB
	1,023,344,111,616 bytes
Bytes per cluster:	4,096
Free clusters:	223,558,897

```
   Offset     0  1  2  3  4  5  6  7   8  9  A
00D09DD000  46 49 4C 45 30 00 03 00  04 27 1A
00D09DD010  01 00 01 00 38 00 01 00  48 02 00
00D09DD020  00 00 00 00 00 00 00 00  09 00 00
00D09DD030  1E 00 B4 A8 00 00 00 00  10 00 00 00 60 00 00 00  ..´¨........`...
00D09DD040  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00  ........H.......
00D09DD050  32 7B 7D DA F7 EF DA 01  35 54 B9 DA F7 EF DA 01  2{}Ú÷ïÚ.5T¹Ú÷ïÚ.
00D09DD060  C8 C8 27 2E F1 3D DB 01  A8 61 97 3D F4 3D DB 01  ÈÈ'.ñ=Û.¨a▮=ô=Û.
00D09DD070  20 00 04 00 00 00 00 00  00 00 00 00 00 00 00 00   ...............
00D09DD080  00 00 00 00 DF 0F 00 00  00 00 00 00 00 00 00 00  ....ß...........
00D09DD090  08 3E 78 1B 00 00 00 00  30 00 00 00 88 00 00 00  .>x.....0...▮...
00D09DD0A0  00 00 00 00 00 00 08 00  6E 00 00 00 18 00 01 00  ........n.......
00D09DD0B0  94 20 02 00 00 00 02 00  32 7B 7D DA F7 EF DA 01  ▮ ......2{}Ú÷ïÚ.
00D09DD0C0  35 54 B9 DA F7 EF DA 01  22 F6 13 29 F1 3D DB 01  5T¹Ú÷ïÚ."ö.)ñ=Û.
00D09DD0D0  1C 92 24 10 1B 30 DB 01  00 10 00 00 00 00 00 00  .'$..0Û.........
00D09DD0E0  B7 00 00 00 00 00 00 00  20 00 04 00 96 00 0A 00  ·....... ...▮...
00D09DD0F0  16 00 41 00 70 00 70 00  73 00 2E 00 74 00 61 00  ..A.p.p.s...t.a.
00D09DD100  72 00 67 00 65 00 74 00  73 00 69 00 7A 00 65 00  r.g.e.t.s.i.z.e.
00D09DD110  2D 00 33 00 32 00 2E 00  70 00 6E 00 67 00 00 00  -.3.2...p.n.g...
00D09DD120  80 00 00 00 48 00 00 00  01 00 00 00 00 00 04 00  ▮...H...........
00D09DD130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00D09DD140  40 00 00 00 00 00 00 00  00 10 00 00 00 00 00 00  @...............
00D09DD150  B7 00 00 00 00 00 00 00  B7 00 00 00 00 00 00 00  ·.......·.......
00D09DD160  41 01 D2 6B 90 00 00 00  D0 00 00 00 20 00 00 00  A.Òk....Ð... ...
00D09DD170  00 00 00 00 00 00 05 00  08 00 00 00 18 00 00 00  ................
00D09DD180  96 00 00 00 A0 00 00 00  E0 00 00 00 B8 00 00 00  ▮... ...à...¸...
00D09DD190  00 00 00 00 00 00 06 00  A0 00 00 00 18 00 00 00  ........ .......
00D09DD1A0  64 00 00 00 00 16 45 00  24 4B 45 52 4E 45 4C 2E  d.....E.$KERNEL.
00D09DD1B0  50 55 52 47 45 2E 45 53  42 43 41 43 48 45 00 45  PURGE.ESBCACHE.E
00D09DD1C0  00 00 00 03 00 02 06 0F  E3 CB F2 C8 E9 DA 01 80  ........ãËòÈéÚ.▮
```

Error #1

Cannot open "\Program Files\Lab04 - Anti Forensics\Lab04 - Anti Forensics\part1\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test\test".
Please check the path and your access rights.

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

3. Run the test.bat file.

Forensic ToolKit (Install v1.62) – It is OK that it is not the FULL Version!

Examine the part1 folder using FTK by adding the folder to be analyzed.

1. What evidence was found? ________________________________

WinHex

1. Right Click on WinHex.exe and Run as Administrator
2. Open with WinHex (From the folder it is provided in, if you have license issue, delete the file WinHex.cfg from the WinHex Folder)
3. Tools → Open Disk (Choose C: partition).
4. Take a new volume snapshot (Tools | Disk Tools | Take New Volume Snapshot) in case WinHex is using an older one.
5. Browse to part1 folder using the Directory Browser (Ctrl+F7 if not already up).
6. Click through ALL the test folders created by the script until something bad happens…
   a. What happened? ________________________________

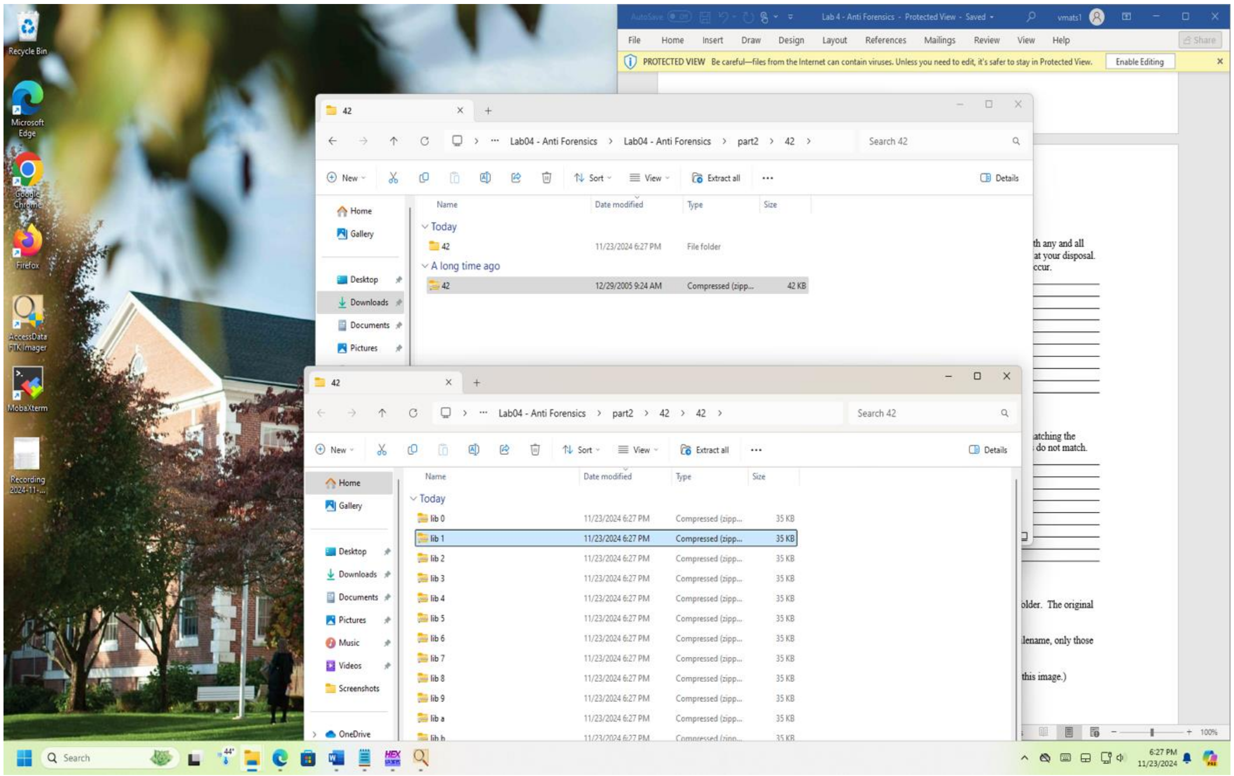
many folders did you go through before this? ____________

Part 2 – When Things Go 'BOOM'…

1. Examine the 42.zip file compressed the 42.rar file in the part2 folder with any and all forensic examination tools (at least FTK v.162 and Windows Explorer) at your disposal. Describe any evidence you find as well as any problems or issues that occur.

____

Page 1 of 3 439 words



Lab 4 - Anti Forensics - Protected View - Saved
PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.
Enable Editing
Recycle Bin
Microsoft Edge
Google Chrome
Firefox
AccessData FTK Imager
MobaXterm
Recording 2024-11-...

42
Lab04 - Anti Forensics > Lab04 - Anti Forensics > part2 > 42 >

Name	Date modified	Type	Size
Today			
42	11/23/2024 6:27 PM	File folder	
A long time ago			
42	12/29/2005 9:24 AM	Compressed (zipp...	42 KB

42
Lab04 - Anti Forensics > part2 > 42 > 42 >

Name	Date modified	Type	Size
Today			
lib 0	11/23/2024 6:27 PM	Compressed (zipp...	35 KB
lib 1	11/23/2024 6:27 PM	Compressed (zipp...	35 KB
lib 2	11/23/2024 6:27 PM	Compressed (zipp...	35 KB
lib 3	11/23/2024 6:27 PM	Compressed (zipp...	35 KB
lib 4	11/23/2024 6:27 PM	Compressed (zipp...	35 KB
lib 5	11/23/2024 6:27 PM	Compressed (zipp...	35 KB
lib 6	11/23/2024 6:27 PM	Compressed (zipp...	35 KB
lib 7	11/23/2024 6:27 PM	Compressed (zipp...	35 KB
lib 8	11/23/2024 6:27 PM	Compressed (zipp...	35 KB
lib 9	11/23/2024 6:27 PM	Compressed (zipp...	35 KB
lib a	11/23/2024 6:27 PM	Compressed (zipp...	35 KB
lib b	11/23/2024 6:27 PM	Compressed (zipp...	35 KB

6:27 PM 11/23/2024

WinHex version – v21.3

Part 2 – When Things Go 'LEFT'…

1. Examine the 42.zip file compressed the 42.rar file in the part2 folder with any and all forensic examination tools (at least FTK v.162 and Windows Explorer) at your disposal. Describe any evidence you find as well as any problems or issues that occur.

- The 42.rar and 42.zip files were extracted in phase 2. There were seven 'lib' folders in the 42 folders that required extraction.
- Every 'lib' folder contained a 'book' subdirectory, which contained books 0–9 and a–f. The extraction procedure went on. It takes awhile to extract each folder.
- While Access Data FTK 1.62 Demo looked through the 42.rar folder, Windows Defender found the "ZIP boom" virus. I turned on Windows Defender as a precaution. But the Windows security program took a while to start up.

Part 3 – 10 things I hate about hashes…

This semester you've already experienced the MD-5 hash of a disk image not matching the original hash. Briefly explain what you should do in the future when the hashes do not match.

When MD5 Hashes Do Not Match:

Explanation:
A mismatch shows that the data has been altered, either due to corruption, tampering, or errors during acquisition.

1. MD5 is slower than the SHA algorithm and other methods.
2. MD5 is less secure than the SHA algorithm due to its susceptibility to collision attacks.
3. It is possible to get the same hash function for two different inputs using MD5.
4. MD5 takes a lot of time.
5. Check the hash value after downloading the software again.
6. We should start over with a fresh copy if the visual verification is accurate.
7. Many individuals do not think about comparing hashes because of the difficulties.
8. Multiple hashing apps are needed to generate hashes.
9. The hash cannot contain null values.
10. It is time-consuming and necessitates a precise hash comparison.

Part 4 – Where did it go?

1. Use Autopsy for FAT to examine the warez.001 image in the part4 folder. The original MD-5 hash is 9af94f27b963f13025ab6f95ae2c3fdd.

Hash matched 9af94f27b963f13025ab6f95ae2c3fdd

2. Use the following page to:
    a. describe what is on the image (you don't have to list every filename, only those that are interesting or have value to the case)
    b. describe any form of anti-forensics that may be in use
        i. Data Hiding (There is no steganography or ADS on this image.)
        ii. Artifact Wiping
        iii. Trail obfuscation
        iv. Attacks against CF process/tools

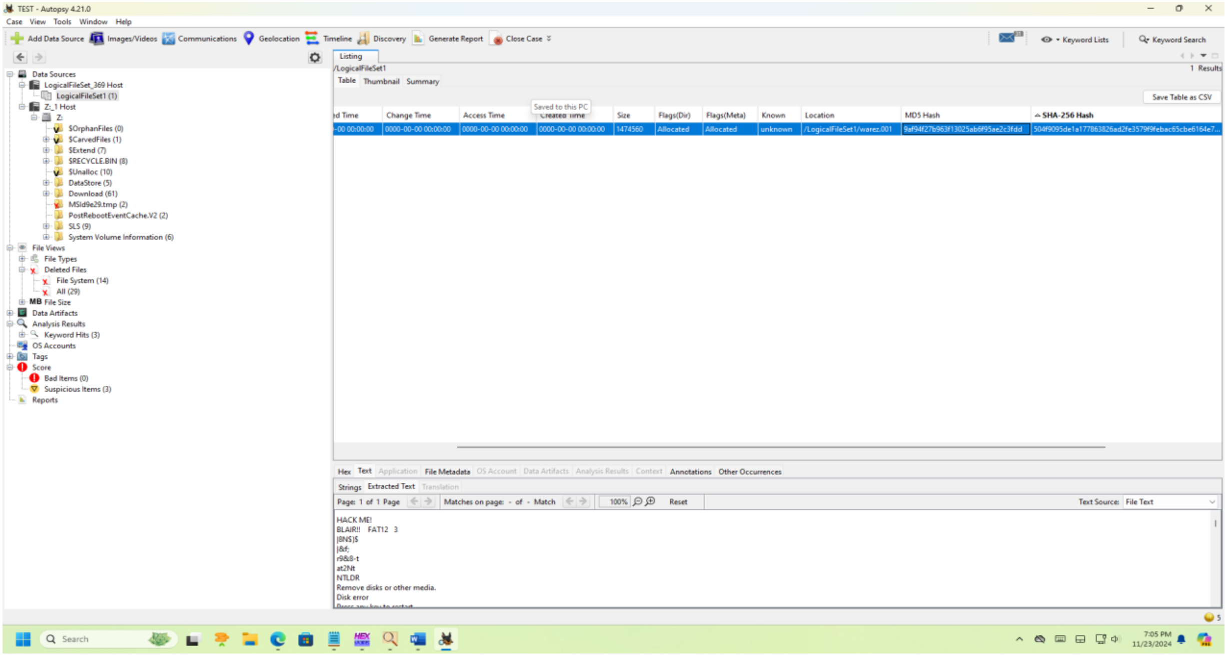
Part 4 Answers: - What did you find?

Autopsy Examination of warez.001:
What appears on the image:

```
HACK ME!
BLAIR!!   FAT12   3
|8N$}$
|&f;
r9&8-t
at2Nt
NTLDR
Remove disks or other media.
Disk error
Press any key to restart
This could be slack or this text could just kill this entire disk.  Either way, we'll soon find out.
```

```
WAREZ
43Sm
.jpg
43SM   JPG
45Sm
.jpg
145SM   JPG
53Sm
.jpg
153SM   JPG
61Sm
.jpg
61SM   JPG
23Sm
.jpg
223SM   JPG
37Sm
.jpg
237SM   JPG
44Sm
.jpg
244SM   JPG
49Sm
.jpg
49SM   JPG
54Sm
.jpg
254SM   JPG
55Sm
.jpg
255SM   JPG
57bg
Yellow
257BGY~1JPG
58Sm
℅.jpg
258SM   JPG
36Sm
.jpg
336SM   JPG
40Sm
.jpg
340SM   JPG
94Sm
.jpg
394SM   JPG
95Sm
.jpg
395SM   JPG
97bg
Black.
```

397BGB~1JPG
01Sm
.jpg
401SM   JPG
10Sm
.jpg
610SM   JPG
21Sm
.jpg
621SM   JPG
humb
s.db
THUMBS DB &
4QH7   Z6P

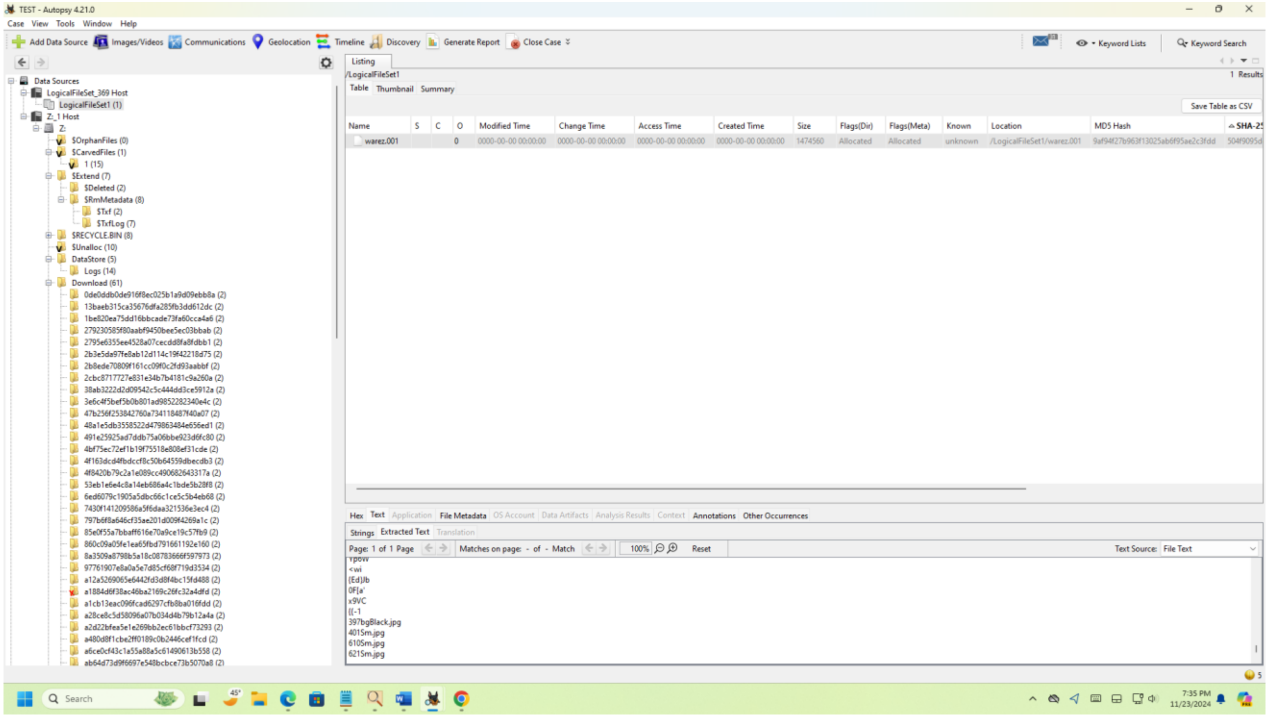


/LogicalFileSet1
1 Results

ed Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	SHA-256 Hash
-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1474560	Allocated	Allocated	unknown	/LogicalFileSet1/warez.001	9af94f27b963f13025ab6f95ae2c3fdd	504f9095de1a177863826ad2fe3579f9febac65cbe6164e7...

Page: 1 of 1 Page   Matches on page: - of - Match   100%   Text Source: File Text

```
HACK ME!
BLAIR!!   FAT12  3
|8N$}$
|&f;
r9&8-t
at2Nt
NTLDR
Remove disks or other media.
Disk error
Press any key to restart
```



```
Data Sources
  LogicalFileSet_369 Host
    LogicalFileSet1 (1)
  Z:_1 Host
    Z:
      $OrphanFiles (0)
      $CarvedFiles (1)
        1 (15)
      $Extend (7)
        $Deleted (2)
        $RmMetadata (8)
          $Txf (2)
          $TxfLog (7)
      $RECYCLE.BIN (8)
      $Unalloc (10)
      DataStore (5)
        Logs (14)
      Download (61)
        0de0ddb0de916f8ec025b1a9d09ebb8a (2)
        13baeb315ca35676dfa285fb3dd612dc (2)
        1be820ea75dd16bbcade73fa60cca4a6 (2)
        279230585f80aabf9450bee5ec03bbab (2)
        2795e6355ee4528a07cecdd8fa8fdbb1 (2)
        2b3e5da97fe8ab12d114c19f42218d75 (2)
        2b8ede70809f161cc09f0c2fd93aabbf (2)
        2cbc8717727e831e34b7b4181c9a260a (2)
        38ab3222d2d09542c5c444dd3ce5912a (2)
        3e6c4f5bef5b0b801ad9852282340e4c (2)
        47b256f253842760a734118487f40a07 (2)
        48a1e5db3558522d479863484e656ed1 (2)
        491e25925ad7ddb75a06bbe923d6fc80 (2)
        4bf75ec72ef1b19f75518e808ef31cde (2)
        4f163dcd4fbdccf8c50b64559dbecdb3 (2)
        4f8420b79c2a1e089cc490682643317a (2)
        53eb1e6e4c8a14eb686a4c1bde5b28f8 (2)
        6ed6079c1905a5dbc66c1ce5c5b4eb68 (2)
        7430f141209586a5f6daa321536e3ec4 (2)
        797b6f8a646cf35ae201d009f4269a1c (2)
        85e0f55a7bbaff616e70a9ce19c57fb9 (2)
        860c09a05fe1ea65fbd791661192e160 (2)
        8a3509a8798b5a18c08783666f597973 (2)
        97761907e8a0a5e7d85cf68f719d3534 (2)
        a12a5269065e6442fd3d8f4bc15fd488 (2)
        a1884d6f38ac46ba2169c26fc32a4dfd (2)
        a1cb13eac096fcad6297cfb8ba016fdd (2)
        a28ce8c5d58096a07b034d4b79b12a4a (2)
        a2d22bfea5e1e269bb2ec61bbcf73293 (2)
        a480d8f1cbe2ff0189c0b2446cef1fcd (2)
        a6ce0cf43c1a55a88a5c61490613b558 (2)
        ab64d73d9f6697e548bcbce73b5070a8 (2)
```

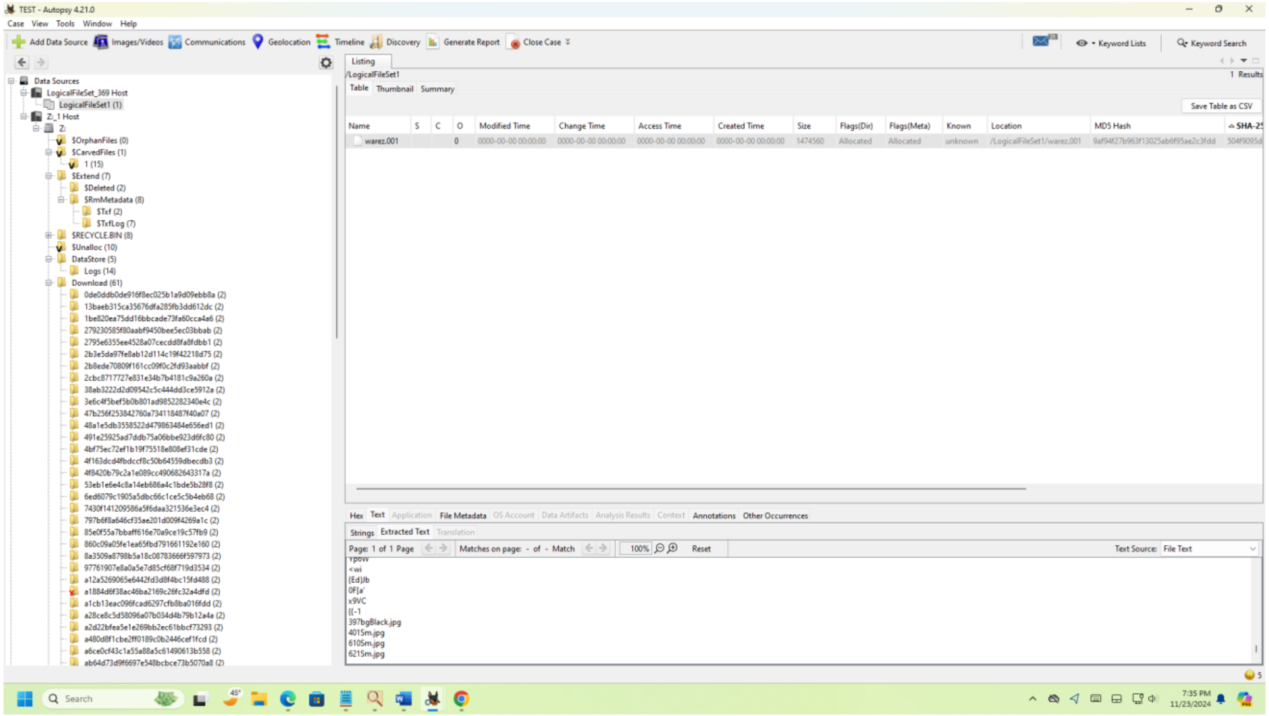
/LogicalFileSet1

1 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	SHA-2
warez.001			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1474560	Allocated	Allocated	unknown	/LogicalFileSet1/warez.001	9af94f27b963f13025ab6f95ae2c3fdd	504f9095d

Page: 1 of 1 Page Matches on page: - of - Match 100% Text Source: File Text

```
Ypow
<wi
{Ed)Jb
0F[a'
x9VC
{(-1
397bgBlack.jpg
401Sm.jpg
610Sm.jpg
621Sm.jpg
```


TEST - Autopsy 4.21.0

Data Sources
  LogicalFileSet_369 Host
    LogicalFileSet1 (1)
  Z:_1 Host
    Z:
      $OrphanFiles (0)
      $CarvedFiles (1)
        1 (15)
      $Extend (7)
        $Deleted (2)
        $RmMetadata (8)
          $Txf (2)
          $TxfLog (7)
      $RECYCLE.BIN (8)
      $Unalloc (10)
      DataStore (5)
        Logs (14)
      Download (61)
        0de0ddb0de916f8ec025b1a9d09ebb8a (2)
        13baeb315ca35676dfa285fb3dd612dc (2)
        1be820ea75dd16bbcade73fa60cca4a6 (2)
        279230585f80aabf9450bee5ec03bbab (2)
        2795e6355ee4528a07cecdd8fa8fdbb1 (2)
        2b3e5da97fe8ab12d114c19f42218d75 (2)
        2b8ede70809f161cc09f0c2fd93aabbf (2)
        2cbc8717727e831e34b7b4181c9a260a (2)
        38ab3222d2d09542c5c444dd3ce5912a (2)
        3e6c4f5bef5b0b801ad9852282340e4c (2)
        47b256f253842760a734118487f40a07 (2)
        48a1e5db3558522d479863484e656ed1 (2)
        491e25925ad7ddb75a06bbe923d6fc80 (2)
        4bf75ec72ef1b19f75518e808ef31cde (2)
        4f163dcd4fbdccf8c50b64559dbecdb3 (2)
        4f8420b79c2a1e089cc490682643317a (2)
        53eb1e6e4c8a14eb686a4c1bde5b28f8 (2)
        6ed6079c1905a5dbc66c1ce5c5b4eb68 (2)
        7430f141209586a5f6daa321536e3ec4 (2)
        797b6f8a646cf35ae201d009f4269a1c (2)
        85e0f55a7bbaff616e70a9ce19c57fb9 (2)
        860c09a05fe1ea65fbd791661192e160 (2)
        8a3509a8798b5a18c08783666f597973 (2)
        97761907e8a0a5e7d85cf68f719d3534 (2)
        a12a5269065e6442fd3d8f4bc15fd488 (2)
        a1884d6f38ac46ba2169c26fc32a4dfd (2)
        a1cb13eac096fcad6297cfb8ba016fdd (2)
        a28ce8c5d58096a07b034d4b79b12a4a (2)
        a2d22bfea5e1e269bb2ec61bbcf73293 (2)
        a480d8f1cbe2ff0189c0b2446cef1fcd (2)
        a6ce0cf43c1a55a88a5c61490613b558 (2)
        ab64d73d9f6697e548bcbce73b5070a8 (2)

/LogicalFileSet1

1 Results

Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Known | Location | MD5 Hash | SHA-2
warez.001 | | | 0 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 1474560 | Allocated | Allocated | unknown | /LogicalFileSet1/warez.001 | 9af94f27b963f13025ab6f95ae2c3fdd | 504f9095d

Page: 1 of 1 Page Matches on page: - of - Match 100% Text Source: File Text

Ypow
<wi
{Ed)Jb
0F[a'
x9VC
{(-1
397bgBlack.jpg
401Sm.jpg
610Sm.jpg
621Sm.jpg

7:35 PM
11/23/2024