Internet Security – COS80013 Lab - 10 Report

Internet Security – COS80013 Lab - 10 Report
Student ID: 104837257
Student Name: Arun Ragavendhar Arunachalam Palaniyappan
Lab Name: COS80013 Lab 10 – Disk Image Forensics Using sleuth kit

Date: 23 /05/2025
Tutor: Yasas Akurudda Liyanage Don

Title and Introduction

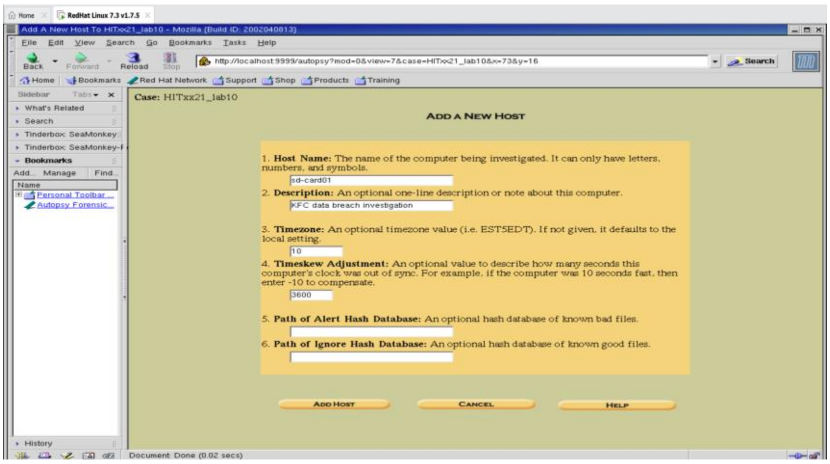
This lab was about performing digital forensic analysis on a disk image using the Autopsy tool – sleuth kit. The objective was to investigate a disk image, examine deleted files, recover a corrupted image, and understand the basics of file carving. It also included a small social engineering task. The goal was to see how forensic tools help recover and investigate data from a digital device, especially in cases where files were deleted, damaged, or hidden.

Methodology

The lab was started by launching the RedHat Linux virtual machine and logging in as the "hacker" user. The graphical interface was started using the startx command, and Firefox was opened. A new case was created in Autopsy, and the case form was filled out. The host was added with timezone set to GMT+10 and a timeskew value of 3600 seconds, accounting for daylight saving time. The disk image image.dd was loaded by navigating to the evidence directory in the console and copying the absolute path using pwd. After the image was added, the MD5 hash was recorded to ensure the evidence wasn't altered during analysis. File Analysis was started, and the file browser showed several deleted files. A file named PgI71.png was found with an iNode value of 54. To recover the file, the icat command was used from the console: icat image.dd 54 > Pg171.png. However, the file was found to be corrupted when opened. To try a lower-level recovery, a different disk image called reformatted.dd was used. The file signature for a PNG image was located using the command xxd reformatted.dd | grep 'PNG', which gave an offset of 364544 bytes or sector 712. Then, the following command was used to recover the file: dd if=reformatted.dd of=picture2.png skip=712 bs=512 count=1000. This recovered image was successfully opened on the desktop. The final part of the lab was a social engineering challenge. Using a browser and open-source search, the ingredients of the fragrance "Accent" were looked up and identified.

Data Recording and Screenshots

Autopsy case was created with timezone +10 and timeskew 3600.



http://localhost:9999/autopsy?mod=0&view=7&case=HITxx21_lab10&x=73&y=16

Case: HITxx21_lab10

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can only have letters, numbers, and symbols.
sd-card01

2. **Description:** An optional one-line description or note about this computer.
KFC data breach investigation

3. **Timezone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting.
10

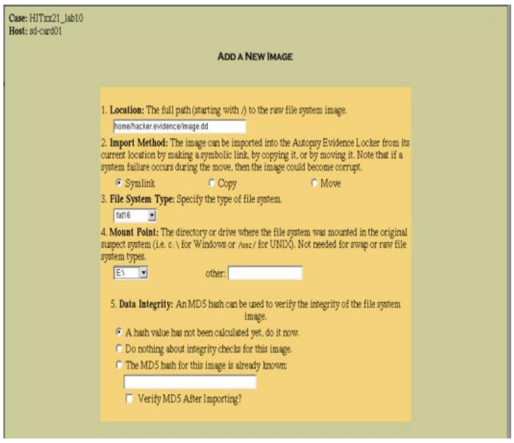
4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.
3600

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

Document: Done (0.02 secs)

Disk image image.dd was added, and MD5 hash noted. **Current MD5: 9795FCF6ABA566FA03C08D0F9652392F**



Case: HITxx21_lab10
Host: sd-card01

ADD A NEW IMAGE

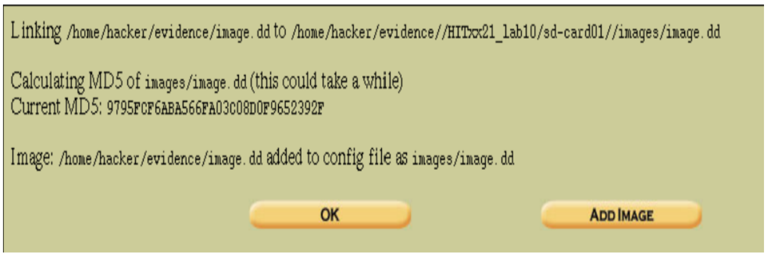
1. **Location:** The full path (starting with /) to the raw file system image.
home/hacker.evidence/image.dd

2. **Import Method:** The image can be imported into the Autopsy Evidence Locker from its current location by making a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
● Symlink ○ Copy ○ Move

3. **File System Type:** Specify the type of file system.
fat16

4. **Mount Point:** The directory or drive where the file system was mounted in the original suspect system (i.e. c:\ for Windows or /usr/ for UNIX). Not needed for swap or raw file system types.
E:\ other:

5. **Data Integrity:** An MD5 hash can be used to verify the integrity of the file system image.
● A hash value has not been calculated yet, do it now.
○ Do nothing about integrity checks for this image.
○ The MD5 hash for this image is already known:
□ Verify MD5 After Importing?

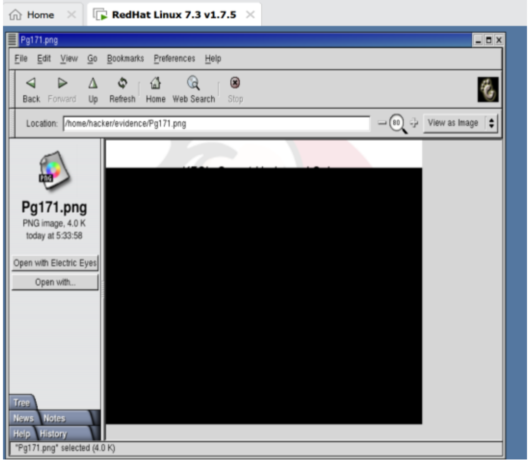


Linking /home/hacker/evidence/image.dd to /home/hacker/evidence//HITxx21_lab10/sd-card01//images/image.dd

Calculating MD5 of images/image.dd (this could take a while)
Current MD5: 9795FCF6ABA566FA03C08D0F9652392F

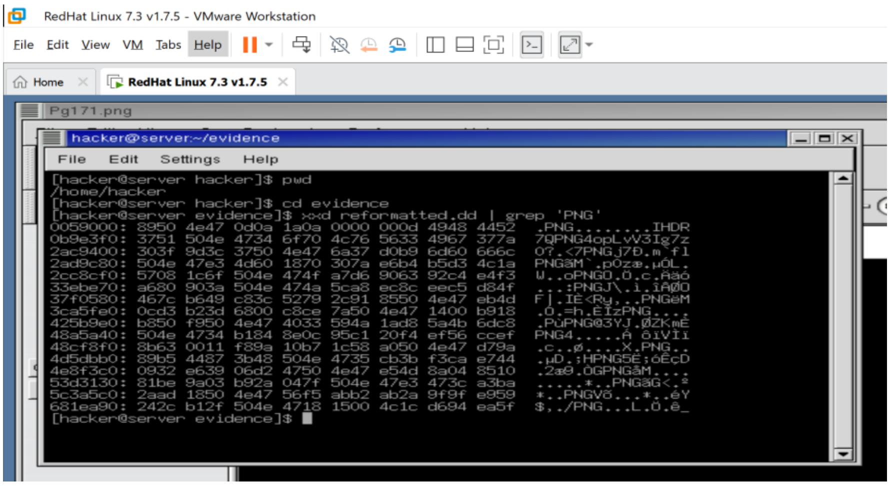
Image: /home/hacker/evidence/image.dd added to config file as images/image.dd

PgI71.png was found and recovered using icat, but the file was corrupted.



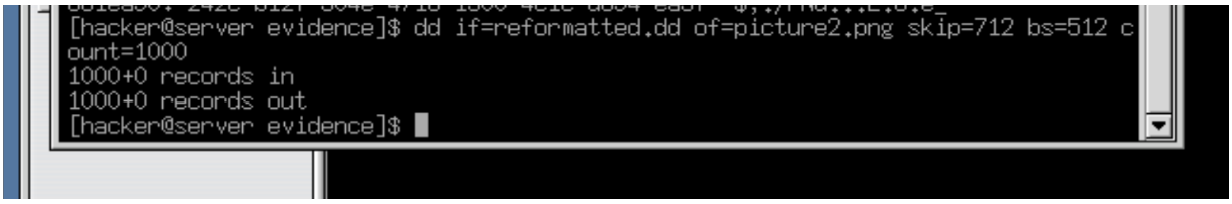
Home
RedHat Linux 7.3 v1.7.5
Pg171.png
File Edit View Go Bookmarks Preferences Help
Back Forward Up Refresh Home Web Search Stop
Location: /home/hacker/evidence/Pg171.png
View as Image
Pg171.png
PNG image, 4.0 K
today at 5:33:58
Open with Electric Eyes
Open with...
Tree
News Notes
Help History
"Pg171.png" selected (4.0 K)

PNG signature was located in reformatted.dd at byte offset 364544 (sector 712).



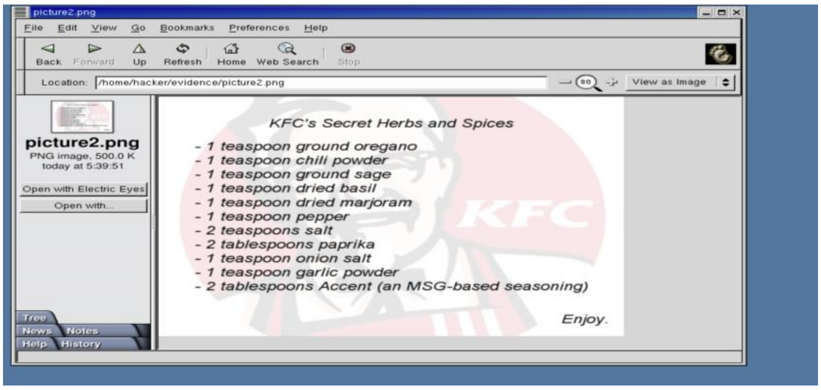
```
[hacker@server hacker]$ pwd
/home/hacker
[hacker@server hacker]$ cd evidence
[hacker@server evidence]$ xxd reformatted.dd | grep 'PNG'
0059000: 8950 4e47 0d0a 1a0a 0000 000d 4948 4452  .PNG........IHDR
0b9e3f0: 3751 504e 4734 6f70 4c76 5633 4967 377a  7QPNG4opLvV3Ig7z
2ac9400: 303f 9d3c 3750 4e47 6a37 d0b9 6d60 666c  0?.<7PNGj7Ð.m`fl
2ad9c80: 504e 47e3 4d60 1870 307a e6b4 b5d3 4c1a  PNGãM`.p0zæ.µÓL.
2cc8cf0: 5708 1c6f 504e 474f a7d6 9063 92c4 e4f3  W..oPNGO.Ö.c.Ääó
33ebe70: a680 903a 504e 474a 5ca8 ec8c eec5 d84f  ...:PNGJ\.ì.îÅØO
37f0580: 467c b649 c83c 5279 2c91 8550 4e47 eb4d  F|.IÈ<Ry,..PNGëM
3ca5fe0: 0cd3 b23d 6800 c8ce 7a50 4e47 1400 b918  .Ó.=h.ÈÎzPNG....
425b9e0: b850 f950 4e47 4033 594a 1ad8 5a4b 6dc8  .PùPNG@3YJ.ØZKmÈ
48a5a40: 504e 4734 b184 8e0c 95c1 20f4 ef56 ccef  PNG4.....Á ôïVÌï
48cf8f0: 8b63 0011 f89a 10b7 1c58 a050 4e47 d79a  .c..ø....X.PNG..
4d5dbb0: 89b5 4487 3b48 504e 4735 cb3b f3ca e744  .µD.;HPNG5Ë;óÊçD
4e8f3c0: 0932 e639 06d2 4750 4e47 e54d 8a04 8510  .2æ9.ÒGPNGåM....
53d3130: 81be 9a03 b92a 047f 504e 47e3 473c a3ba  .....*..PNGãG<.º
5c3a5c0: 2aad 1850 4e47 56f5 abb2 ab2a 9f9f e959  *..PNGVõ...*..éY
681ea90: 242c b12f 504e 4718 1500 4c1c d694 ea5f  $,./PNG...L.Ö.ê_
[hacker@server evidence]$
```

dd command recovered the file as picture2.png, which opened successfully.



```
[hacker@server evidence]$ dd if=reformatted.dd of=picture2.png skip=712 bs=512 c
ount=1000
1000+0 records in
1000+0 records out
[hacker@server evidence]$
```

Picture2.png successfully recovered and restored and displayed below



Location: /home/hacker/evidence/picture2.png

picture2.png
PNG image, 500.0 K
today at 5:39:51

KFC's Secret Herbs and Spices

- 1 teaspoon ground oregano
- 1 teaspoon chili powder
- 1 teaspoon ground sage
- 1 teaspoon dried basil
- 1 teaspoon dried marjoram
- 1 teaspoon pepper
- 2 teaspoons salt
- 2 tablespoons paprika
- 1 teaspoon onion salt
- 1 teaspoon garlic powder
- 2 tablespoons Accent (an MSG-based seasoning)

Enjoy.

Discussion and Application of Learnings

Learning 1

Autopsy was used to examine and recover deleted files from a disk image. The file list showed deleted entries, and their content could be explored or exported.

Real-World Application

Digital forensics teams use tools like Autopsy, sleuth kit to recover deleted evidence during investigations.

Learning 2

The icat command recovered a file using its inode number, but the result was corrupted. This showed that not all deleted files can be recovered cleanly using simple methods.

Real-World Application

When standard recovery fails, investigators need deeper tools or techniques to attempt file carving.

Learning 3

The lower-level file carving using dd helped recover the corrupted image by directly targeting its sector location.

Real-World Application

This method is used when files are partially overwritten or not properly indexed, especially in damaged or reformatted drives.

Learning 4

The MD5 hash helped verify that the disk image had not been altered during the analysis.

Real-World Application

Hashes are used in court and professional investigations to prove data integrity and chain of custody.

Learning 5

The final task showed how information can be gathered online using simple search methods, even without direct access to a system.

Real-World Application

Social engineering relies on public data, weak access controls, or human error to gather information.

Limitations

The lab was done in a safe test setup with small example files. Real investigations often involve bigger drives, hidden or encrypted data, and harder file systems. Autopsy can also be slow with large data. Some files needed manual recovery, which doesn't always work. Still, the lab clearly showed how basic forensic work can be done using free tools.