**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**

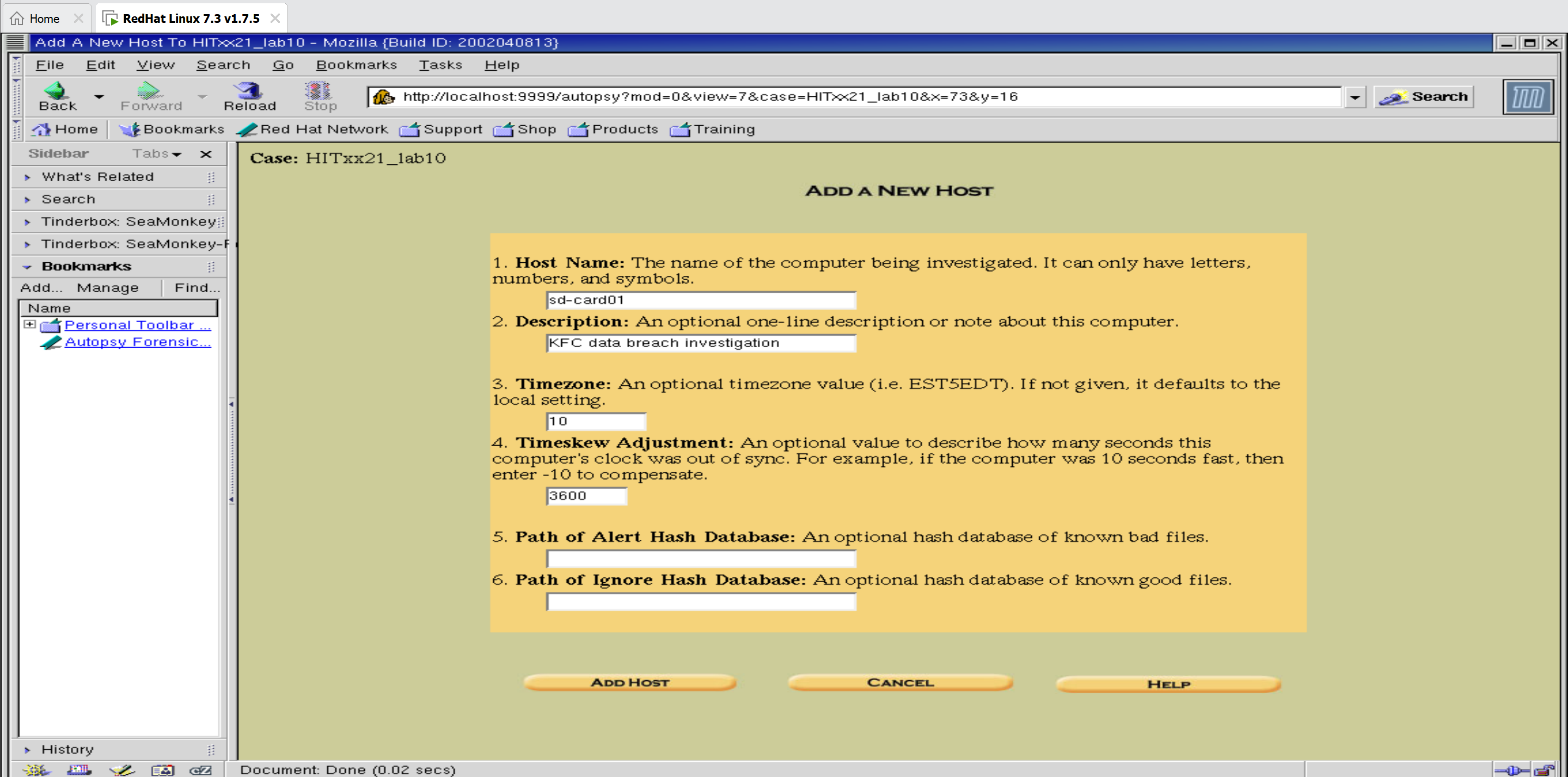
This lab was about performing digital forensic analysis on a disk image using the Autopsy tool – sleuth kit. The objective was to investigate a disk image, examine deleted files, recover a corrupted image, and understand the basics of file carving. It also included a small social engineering task. The 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**

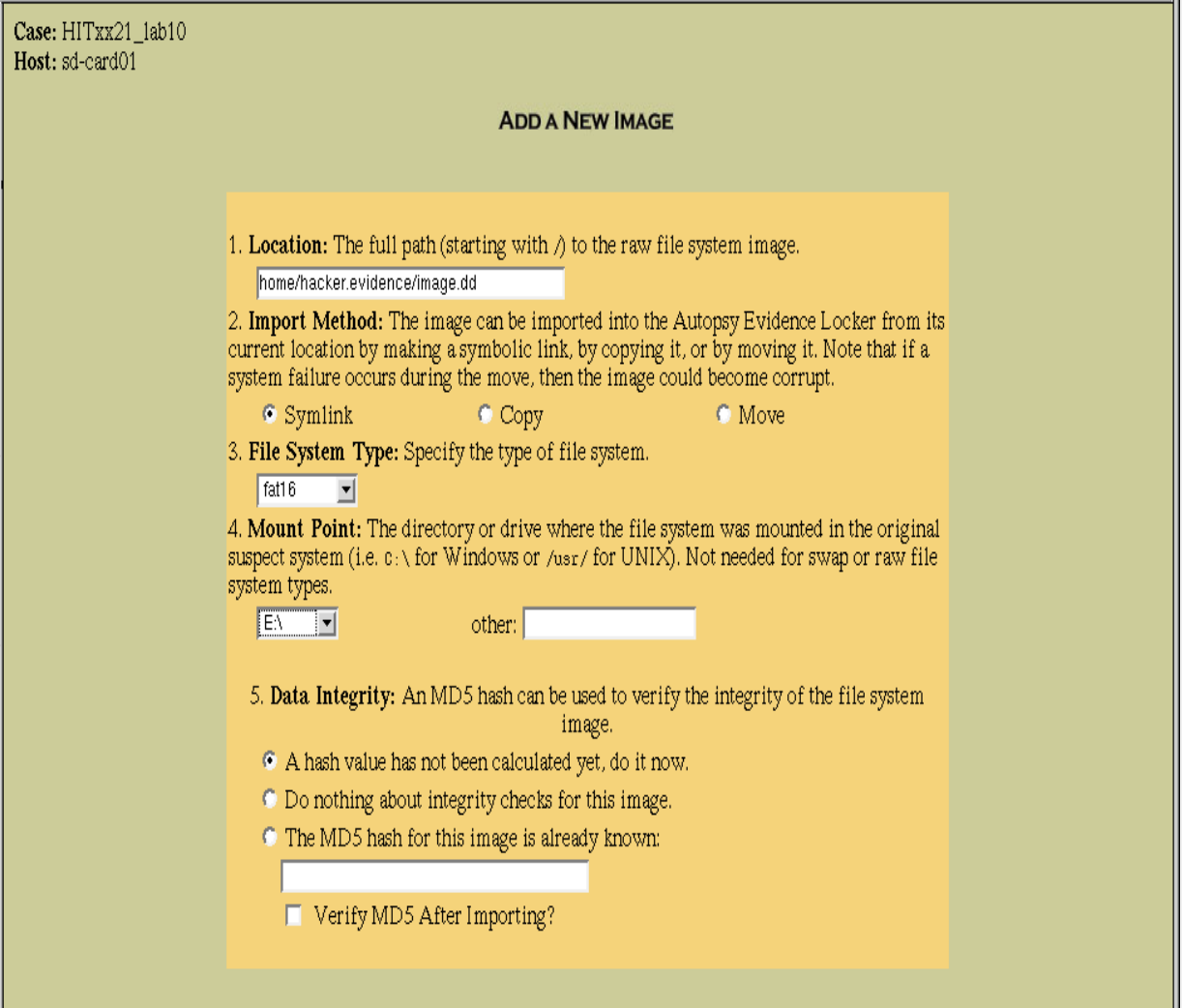
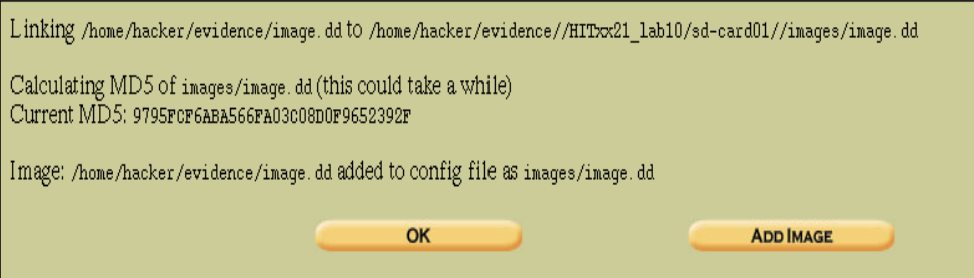
The lab was started by launching the RedHat Linux virtual machine and logging in as the "hacker" user. The graphical interface was started using the startx command, and Firefox was opened. A new case was created in Autopsy, and the case form was filled out. The host was added with timezone set to GMT+10 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**

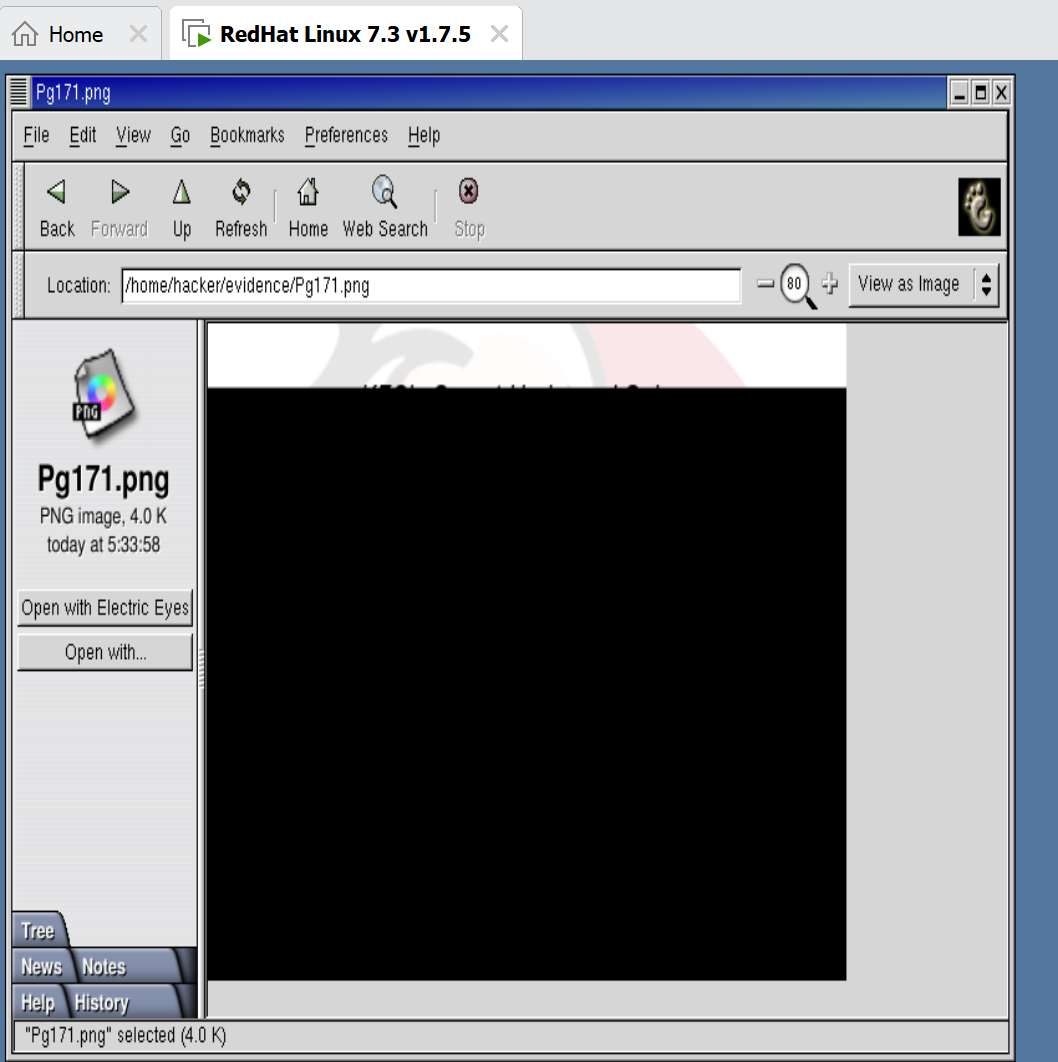
Autopsy case was created with timezone +10 and timeskew 3600.



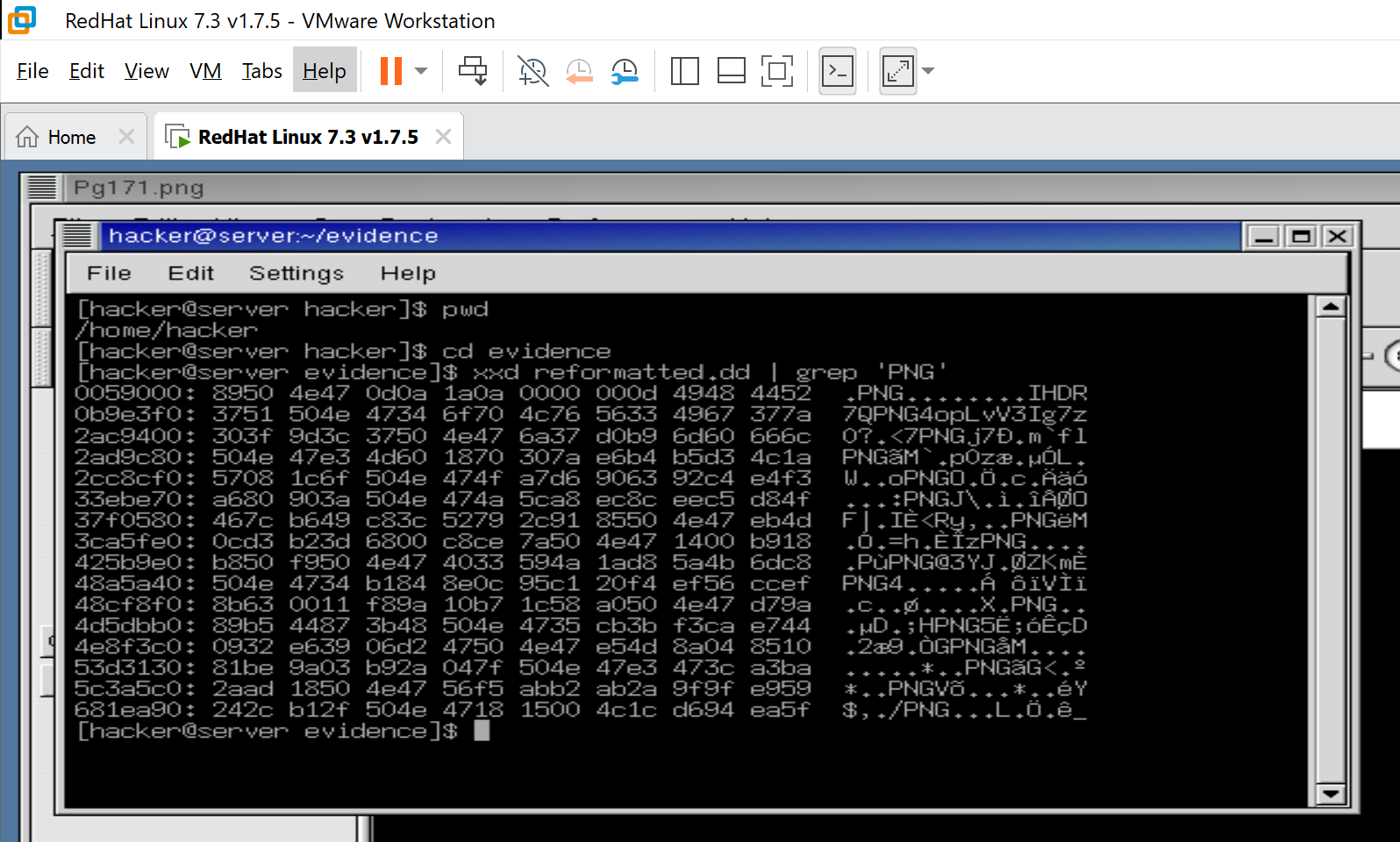
Disk image image.dd was added, and MD5 hash noted**. Current MD5: 9795FCF6ABA566FA03C08D0F9652392F**

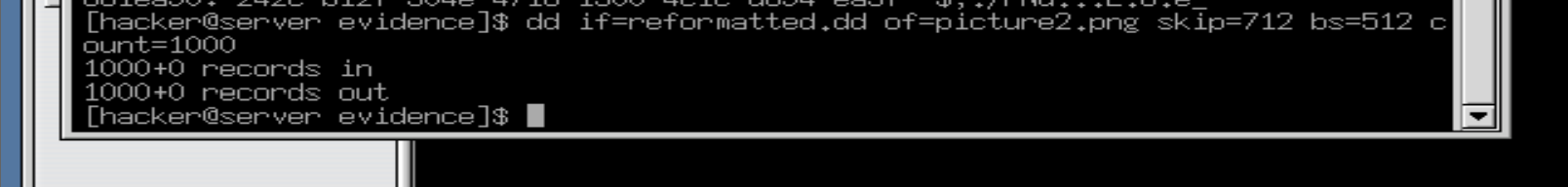
PgI71.png was found and recovered using icat, but the file was corrupted.



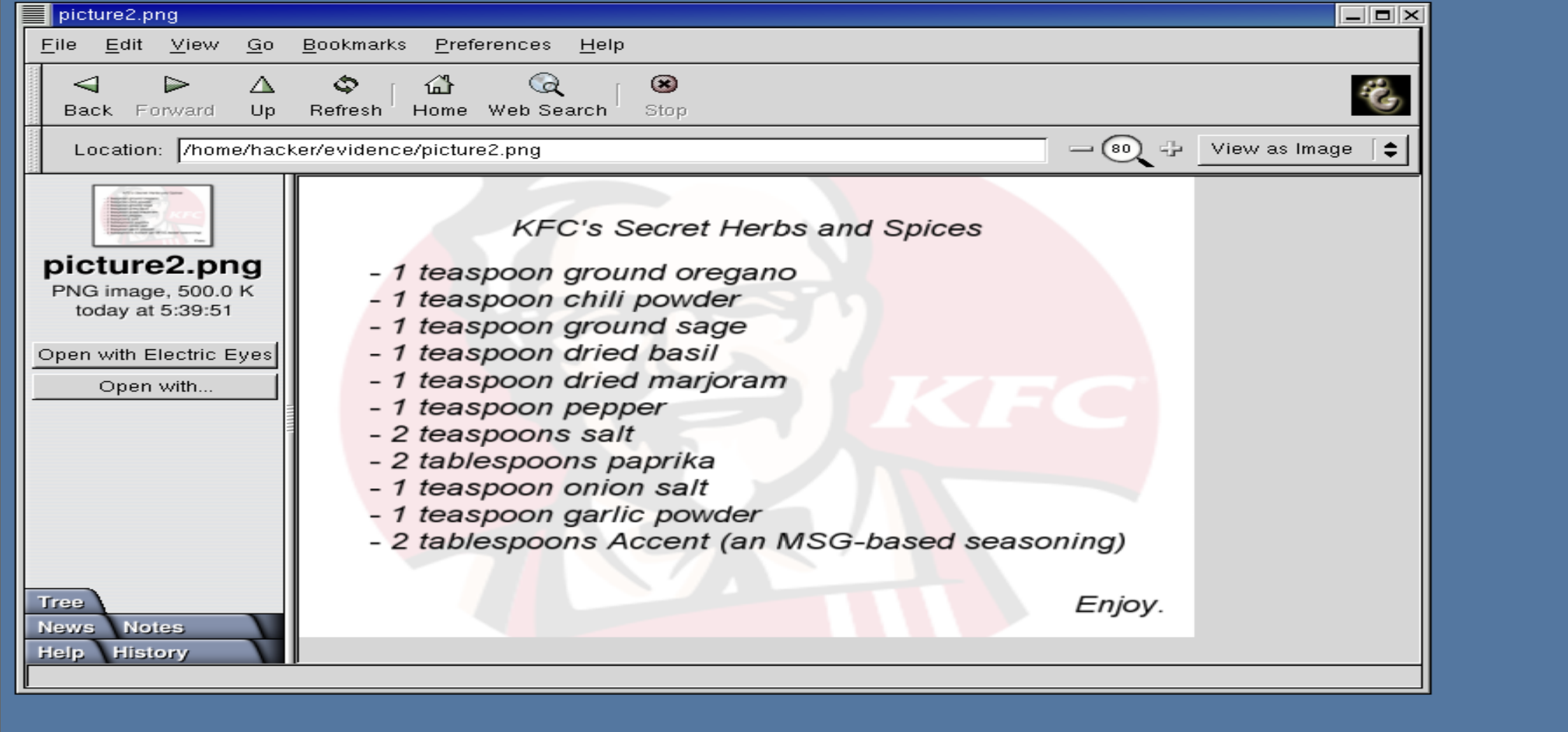
PNG signature was located in reformatted.dd at byte offset 364544 (sector 712).



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



Picture2.png successfully recovered and restored and displayed below



**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.