Sanjana Asrani **DF**
D17B/01/Batch B **Lab 06: Scalpel & Foremost**

Aim: Data Carving using open source tools: Foremost, Scalpel.

Theory:

Theoretical Background:
Data carving stands as an indispensable technique in digital forensics and data recovery, particularly in scenarios where traditional file system structures are compromised or unavailable. It involves the extraction of specific files or fragments from raw data using file headers, footers, and internal data structures. This process, often referred to as "file carving," enables the recovery of valuable evidence files even when file system metadata such as Master File Table (MFT) entries are missing.
File carving tools operate by analyzing the signatures, headers, and footers of known file types within raw data. This allows them to identify the beginning and end of files, facilitating their extraction without reliance on file system information. While file carving can be conducted manually using hex editors, specialized open-source tools like Foremost and Scalpel streamline the process and enhance efficiency.

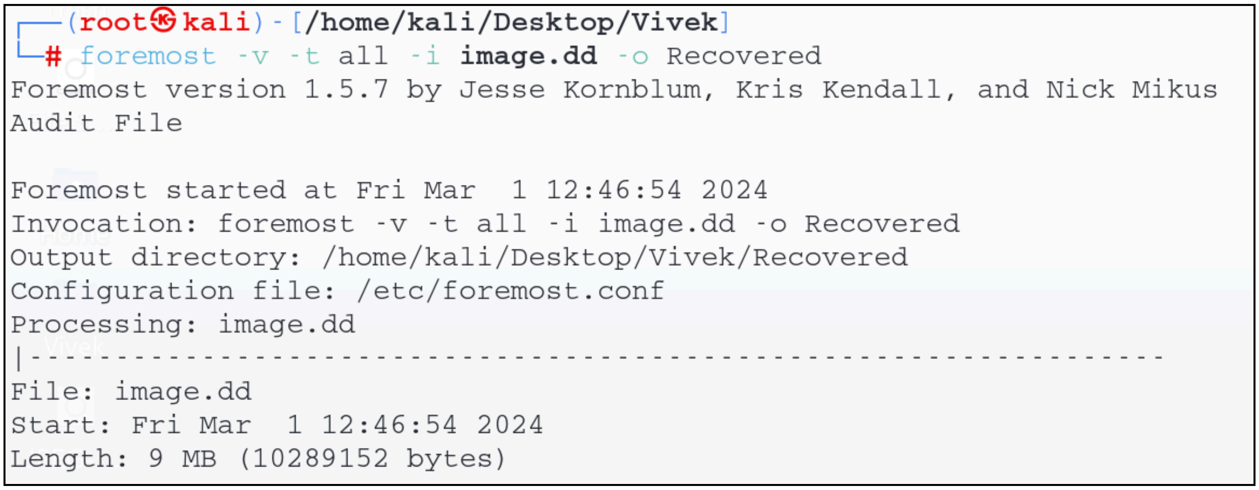
Foremost:
Foremost serves as a powerful forensic data recovery program tailored for Linux systems. Developed for law enforcement use, it's freely available and highly configurable. Foremost operates on the principle of file carving, enabling the recovery of a diverse range of file types, including documents, images, videos, and archives. Its versatility allows forensic examiners to specify recovery parameters, prioritize specific file types, and exclude irrelevant data, thereby enhancing efficiency and accuracy in investigations.

Scalpel:
Scalpel represents an evolution of file carving tools, introducing advancements in efficiency and accuracy. It conducts file carving in two phases: first, it identifies file headers and footers to create a metadata database, and then it carves files based on this database. Scalpel offers enhanced customization options, allowing users to recover specific file types efficiently. Additionally, its support for synthetic file naming and comprehensive configuration options streamlines the recovery process, making it a valuable asset in digital forensics and data recovery operations.

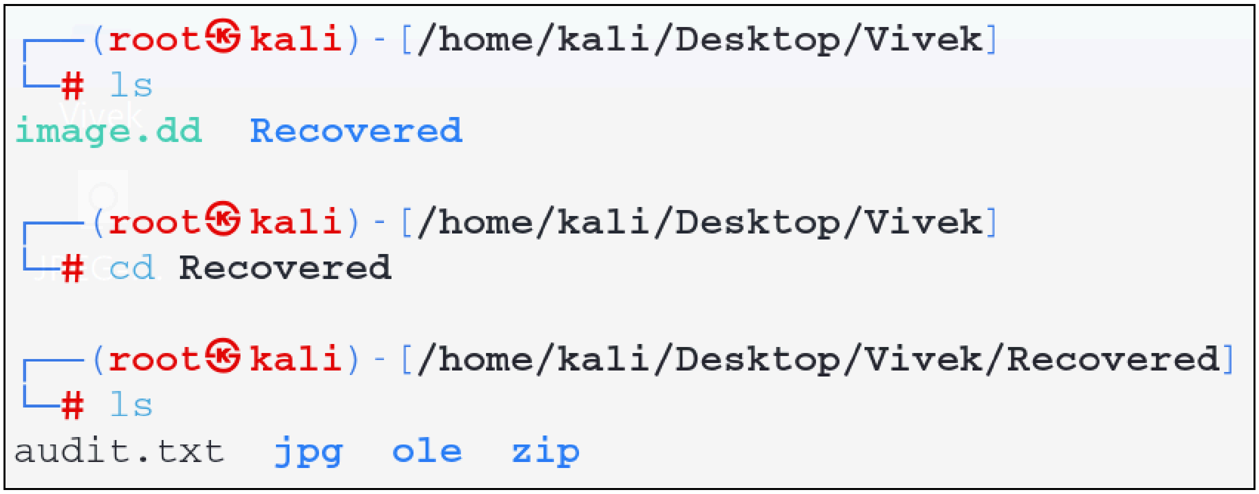
Practical Applications:
In forensic investigations, the utilization of tools like Foremost and Scalpel is instrumental in recovering crucial evidence from compromised or inaccessible storage media. Investigators can extract deleted files, fragments of documents, or multimedia content, aiding in the reconstruction of digital crime scenes and attribution of criminal activities. Beyond forensic applications, these tools find utility in general data recovery operations, assisting users in retrieving valuable files from damaged or corrupted storage devices.

Ethical and Legal Considerations:
Ensuring the integrity and chain of custody of recovered data is paramount in forensic investigations. Forensic examiners must meticulously document their procedures to ensure that recovered evidence remains admissible in legal proceedings. Additionally, respecting privacy rights and confidentiality agreements is crucial when handling recovered data, especially in cases involving sensitive information or personally identifiable data. Upholding ethical standards and adhering to legal frameworks is imperative to maintain trust and credibility in forensic investigations and data recovery operations.

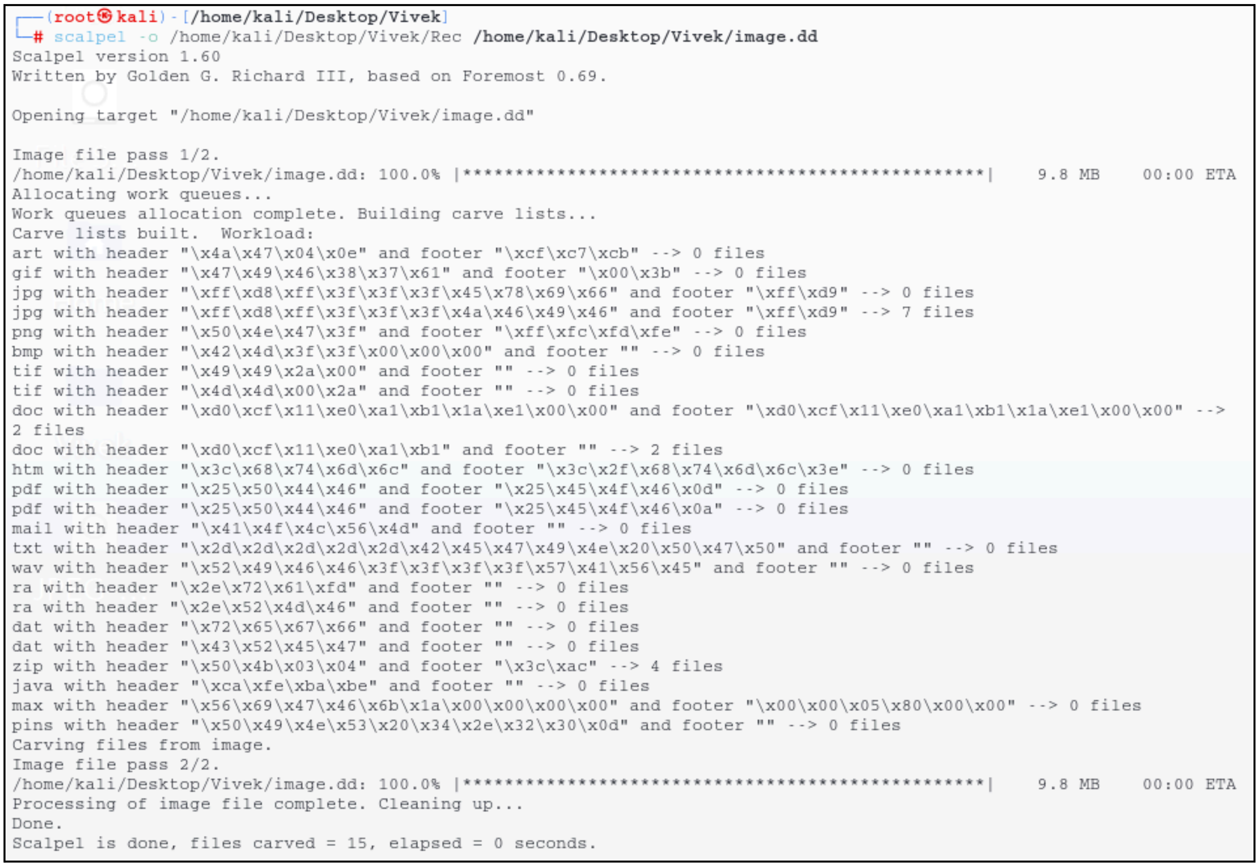
Practical:



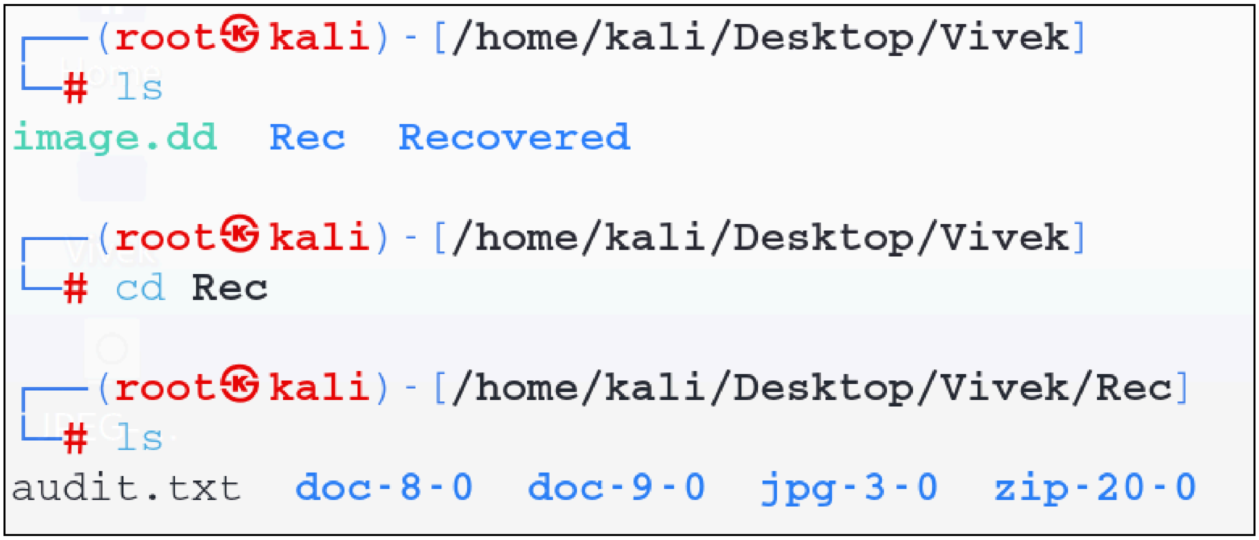
```
┌──(root㉿kali)-[/home/kali/Desktop/Vivek]
└─# foremost -v -t all -i image.dd -o Recovered
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Fri Mar  1 12:46:54 2024
Invocation: foremost -v -t all -i image.dd -o Recovered
Output directory: /home/kali/Desktop/Vivek/Recovered
Configuration file: /etc/foremost.conf
Processing: image.dd
|------------------------------------------------------------------
File: image.dd
Start: Fri Mar  1 12:46:54 2024
Length: 9 MB (10289152 bytes)
```



```
┌──(root㉿kali)-[/home/kali/Desktop/Vivek]
└─# ls
image.dd  Recovered

┌──(root㉿kali)-[/home/kali/Desktop/Vivek]
└─# cd Recovered

┌──(root㉿kali)-[/home/kali/Desktop/Vivek/Recovered]
└─# ls
audit.txt  jpg  ole  zip
```



```
┌──(root㉿kali)-[/home/kali/Desktop/Vivek]
└─# scalpel -o /home/kali/Desktop/Vivek/Rec /home/kali/Desktop/Vivek/image.dd
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/home/kali/Desktop/Vivek/image.dd"

Image file pass 1/2.
/home/kali/Desktop/Vivek/image.dd: 100.0% |**************************************************|    9.8 MB    00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built.  Workload:
art with header "\x4a\x47\x04\x0e" and footer "\xcf\xc7\xcb" --> 0 files
gif with header "\x47\x49\x46\x38\x37\x61" and footer "\x00\x3b" --> 0 files
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x45\x78\x69\x66" and footer "\xff\xd9" --> 0 files
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x4a\x46\x49\x46" and footer "\xff\xd9" --> 7 files
png with header "\x50\x4e\x47\x3f" and footer "\xff\xfc\xfd\xfe" --> 0 files
bmp with header "\x42\x4d\x3f\x3f\x00\x00\x00" and footer "" --> 0 files
tif with header "\x49\x49\x2a\x00" and footer "" --> 0 files
tif with header "\x4d\x4d\x00\x2a" and footer "" --> 0 files
doc with header "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" and footer "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" -->
2 files
doc with header "\xd0\xcf\x11\xe0\xa1\xb1" and footer "" --> 2 files
htm with header "\x3c\x68\x74\x6d\x6c" and footer "\x3c\x2f\x68\x74\x6d\x6c\x3e" --> 0 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0d" --> 0 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0a" --> 0 files
mail with header "\x41\x4f\x4c\x56\x4d" and footer "" --> 0 files
txt with header "\x2d\x2d\x2d\x2d\x2d\x42\x45\x47\x49\x4e\x20\x50\x47\x50" and footer "" --> 0 files
wav with header "\x52\x49\x46\x46\x3f\x3f\x3f\x3f\x57\x41\x56\x45" and footer "" --> 0 files
ra with header "\x2e\x72\x61\xfd" and footer "" --> 0 files
ra with header "\x2e\x52\x4d\x46" and footer "" --> 0 files
dat with header "\x72\x65\x67\x66" and footer "" --> 0 files
dat with header "\x43\x52\x45\x47" and footer "" --> 0 files
zip with header "\x50\x4b\x03\x04" and footer "\x3c\xac" --> 4 files
java with header "\xca\xfe\xba\xbe" and footer "" --> 0 files
max with header "\x56\x69\x47\x46\x6b\x1a\x00\x00\x00\x00" and footer "\x00\x00\x05\x80\x00\x00" --> 0 files
pins with header "\x50\x49\x4e\x53\x20\x34\x2e\x32\x30\x0d" and footer "" --> 0 files
Carving files from image.
Image file pass 2/2.
/home/kali/Desktop/Vivek/image.dd: 100.0% |**************************************************|    9.8 MB    00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 15, elapsed = 0 seconds.
```



```
┌──(root㉿kali)-[/home/kali/Desktop/Vivek]
└─# ls
image.dd  Rec  Recovered

┌──(root㉿kali)-[/home/kali/Desktop/Vivek]
└─# cd Rec

┌──(root㉿kali)-[/home/kali/Desktop/Vivek/Rec]
└─# ls
audit.txt  doc-8-0  doc-9-0  jpg-3-0  zip-20-0
```

Conclusion: