Use foremost on recovered.img to see what files were previously deleted.

Run foremost for png files

```
franklin-wang@franklin-wang-VMware20-1:~$ sudo foremost -t png recovered.img
Processing: recovered.img
|**|
franklin-wang@franklin-wang-VMware20-1:~$ ls -l
total 124500
drwxrwxr-x 2 franklin-wang franklin-wang      4096 Feb 18 20:57 classDemos
-rw-rw-r-- 1 franklin-wang franklin-wang        33 Jan 23 10:57 completed.txt
drwxrwxr-x 2 franklin-wang franklin-wang      4096 Jan 23 09:53 Cryptography
-rw-r--r-- 1 root          root               1399 Jan 28 09:42 cwru.crt
-rw-r--r-- 1 root          root               1062 Jan 28 09:41 cwru.csr
-rw------- 1 root          root               1704 Jan 28 09:42 cwru.key
drwxr-xr-x 2 franklin-wang franklin-wang      4096 Jan 14 06:52 Desktop
drwxrwxr-x 2 franklin-wang franklin-wang      4096 Jan 23 10:59 docs
drwxr-xr-x 2 franklin-wang franklin-wang      4096 Jan 14 06:52 Documents
drwxr-xr-x 6 franklin-wang franklin-wang      4096 Apr 20 14:19 Downloads
drwxr-xr-x 2 franklin-wang franklin-wang      4096 Jan 23 10:53 logs
drwxrwxr-x 2 franklin-wang franklin-wang      4096 Apr 14 21:53 __MACOSX
drwxr-xr-x 2 franklin-wang franklin-wang      4096 Jan 14 06:52 Music
drwxr-xr-- 3 root          root               4096 Apr 20 14:31 output
drwxr-xr-x 2 franklin-wang franklin-wang      4096 Jan 14 06:52 Pictures
drwxr-xr-x 2 franklin-wang franklin-wang      4096 Jan 14 06:52 Public
-rw-rw-r-- 1 franklin-wang franklin-wang 127401472 Apr 14 11:10 recovered.img
drwx------ 4 franklin-wang franklin-wang      4096 Jan 22 19:04 snap
drwxr-xr-x 2 franklin-wang franklin-wang      4096 Jan 14 06:52 Templates
-rw-rw-r-- 1 franklin-wang franklin-wang       697 Mar 17 09:32 test.sql
```

Change ownership of output directory

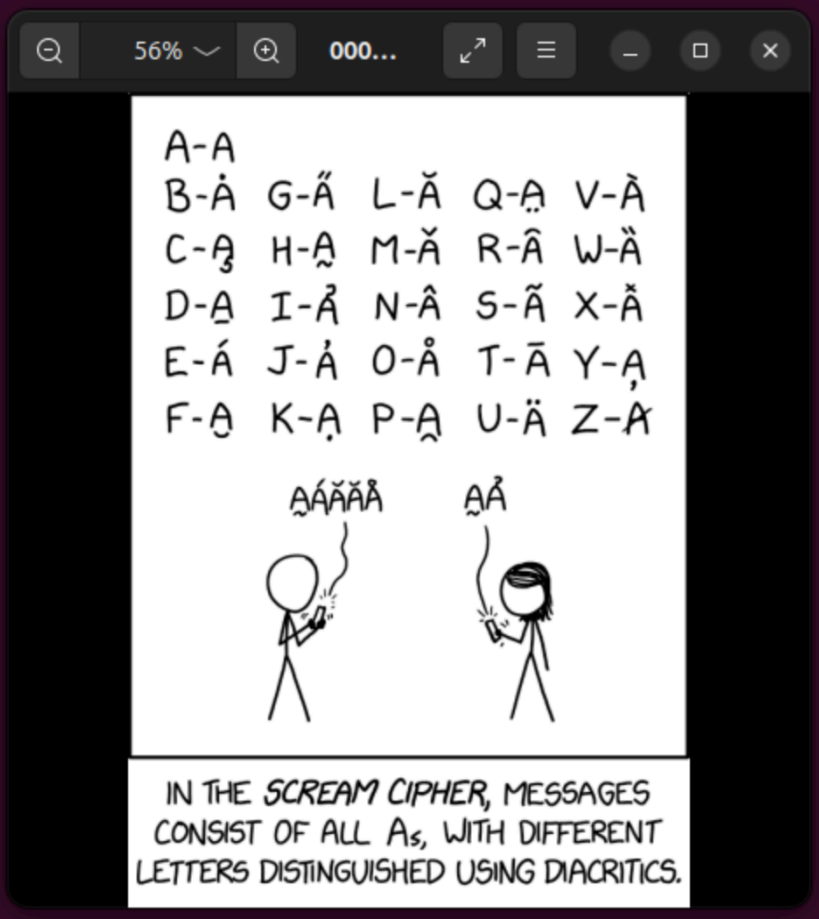
```
franklin-wang@franklin-wang-VMware20-1:~$ cd output
bash: cd: output: Permission denied
franklin-wang@franklin-wang-VMware20-1:~$ sudo chown -R franklin-wang: output
franklin-wang@franklin-wang-VMware20-1:~$ ls -d
.
franklin-wang@franklin-wang-VMware20-1:~$ ls
classDemos     cwru.crt  Desktop    Downloads  Music     Public          Templates
completed.txt  cwru.csr  docs       logs       output    recovered.img   test.sql
Cryptography   cwru.key  Documents  __MACOSX   Pictures  snap            Videos
franklin-wang@franklin-wang-VMware20-1:~$ ls -lt
total 124500
drwxr-xr-- 3 franklin-wang franklin-wang      4096 Apr 20 14:31 output
drwxr-xr-x 6 franklin-wang franklin-wang      4096 Apr 20 14:19 Downloads
drwxrwxr-x 2 franklin-wang franklin-wang      4096 Apr 14 21:53 __MACOSX
-rw-rw-r-- 1 franklin-wang franklin-wang 127401472 Apr 14 11:10 recovered.img
-rw-rw-r-- 1 franklin-wang franklin-wang       697 Mar 17 09:32 test.sql
drwxrwxr-x 2 franklin-wang franklin-wang      4096 Feb 18 20:57 classDemos
```

See the audit results

```
franklin-wang@franklin-wang-VMware20-1:~$ cd output/
franklin-wang@franklin-wang-VMware20-1:~/output$ ls
audit.txt  png
franklin-wang@franklin-wang-VMware20-1:~/output$ ca audit.txt
ca: command not found
franklin-wang@franklin-wang-VMware20-1:~/output$ cat audit.txt
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Sun Apr 20 14:31:56 2025
Invocation: foremost -t png recovered.img
Output directory: /home/franklin-wang/output
Configuration file: /etc/foremost.conf
------------------------------------------------------------------
File: recovered.img
Start: Sun Apr 20 14:31:56 2025
Length: 121 MB (127401472 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

0:      00008664.png          39 KB         4435968       (573 x 831)
Finish: Sun Apr 20 14:31:56 2025

1 FILES EXTRACTED

png:= 1
------------------------------------------------------------------

Foremost finished at Sun Apr 20 14:31:56 2025
```

View the recovered file

```
franklin-wang@franklin-wang-VMware20-1:~/output$ cd png/
franklin-wang@franklin-wang-VMware20-1:~/output/png$ ls
00008664.png
franklin-wang@franklin-wang-VMware20-1:~/output/png$ open 00008664.png
franklin-wang@franklin-wang-VMware20-1:~/output/png$
```



Running foremost to look for pdf files

```
franklin-wang@franklin-wang-VMware20-1:~$ sudo foremost -t pdf recovered.img
Processing: recovered.img
|**|
franklin-wang@franklin-wang-VMware20-1:~$ sudo chown -R franklin-wang: output
franklin-wang@franklin-wang-VMware20-1:~$ cd output/
franklin-wang@franklin-wang-VMware20-1:~/output$ cat audit.txt
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Tue May 20 19:48:37 2025
Invocation: foremost -t pdf recovered.img
Output directory: /home/franklin-wang/output
Configuration file: /etc/foremost.conf
------------------------------------------------------------------
File: recovered.img
Start: Tue May 20 19:48:37 2025
Length: 121 MB (127401472 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

0:      00004664.pdf           1 MB         2387968
Finish: Tue May 20 19:48:37 2025

1 FILES EXTRACTED

pdf:= 1
------------------------------------------------------------------

Foremost finished at Tue May 20 19:48:37 2025
```

View the deleted pdf file

Chain of custody

For chain of custody, you must document who accessed the evidence every location where the evidence was present, and what the person did with the evidence.