

Student:

Email:

Vishal Singh Bhardvaj

Time on Task:

Progress:

2 hours, 2 minutes

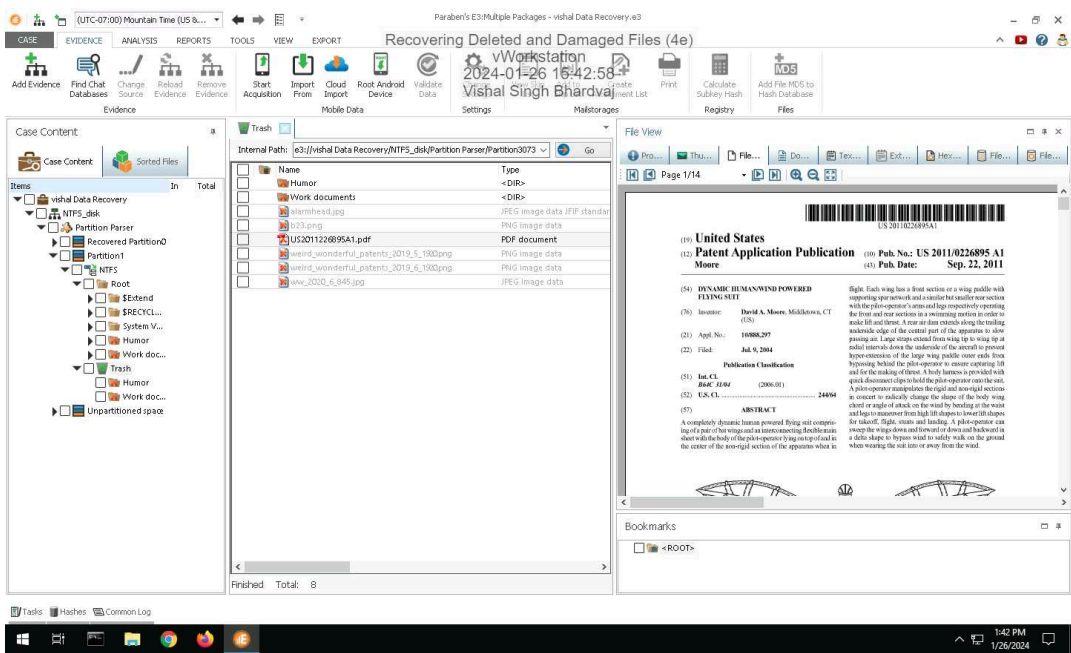
100%

Report Generated: Friday, January 26, 2024 at 5:29 PM

Section 1: Hands-On Demonstration

Part 1: Recover Deleted Files from an NTFS Drive Image with E3

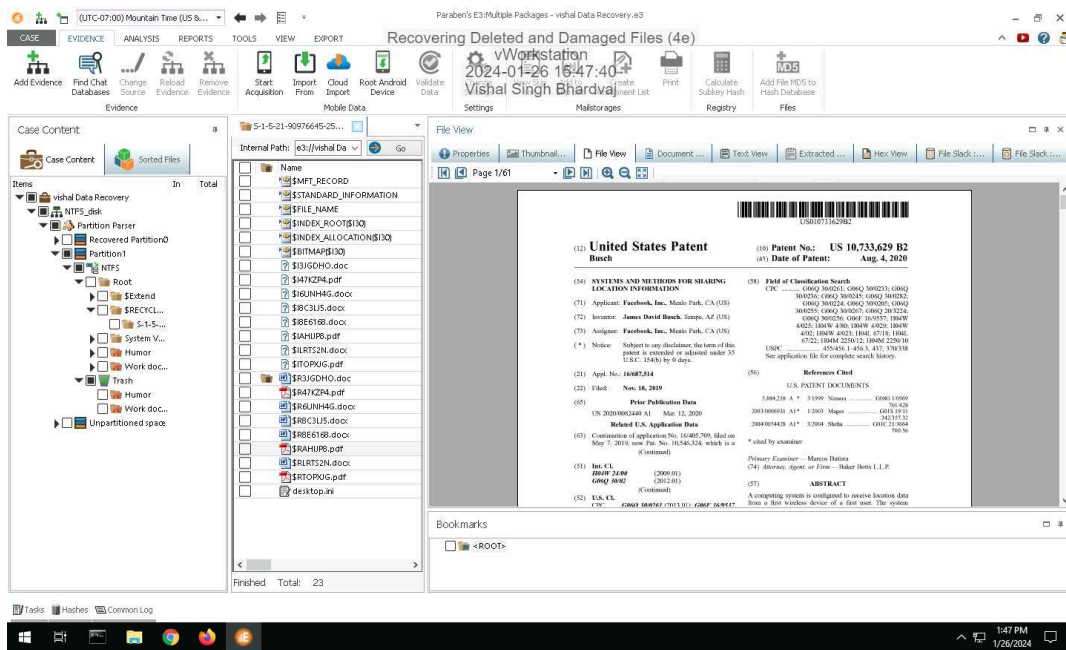
13. Make a screen capture showing the list of recovered files and folders in the E3 Trash folder.



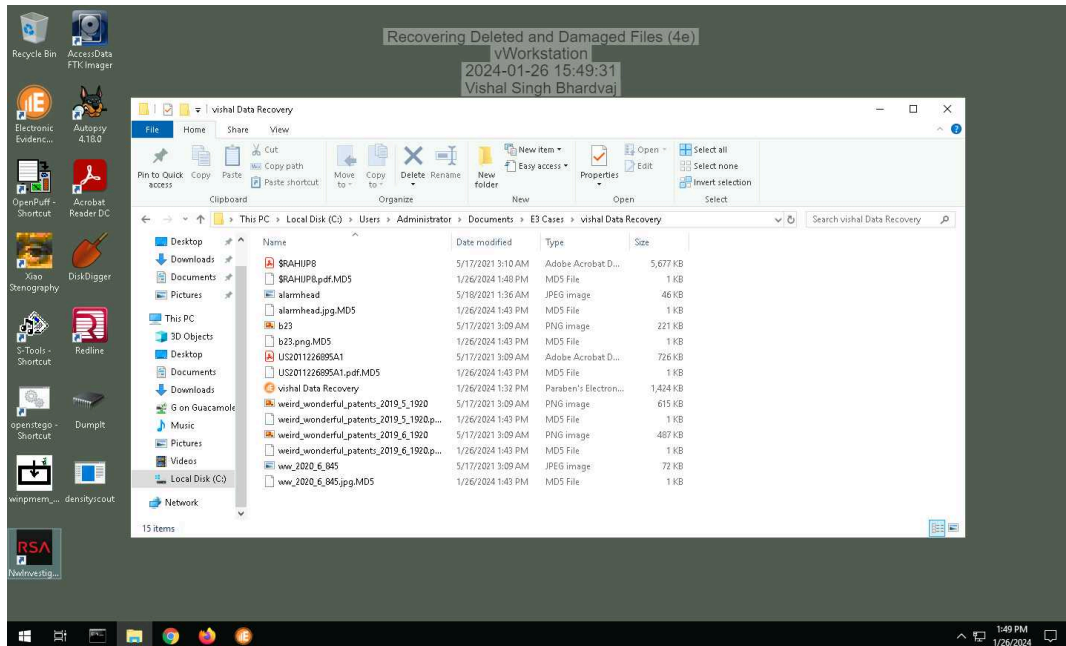
Recovering Deleted and Damaged Files (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 03

20. Make a screen capture showing the patent file in the File Viewer.



25. Make a screen capture showing the recovered files in the File Explorer.

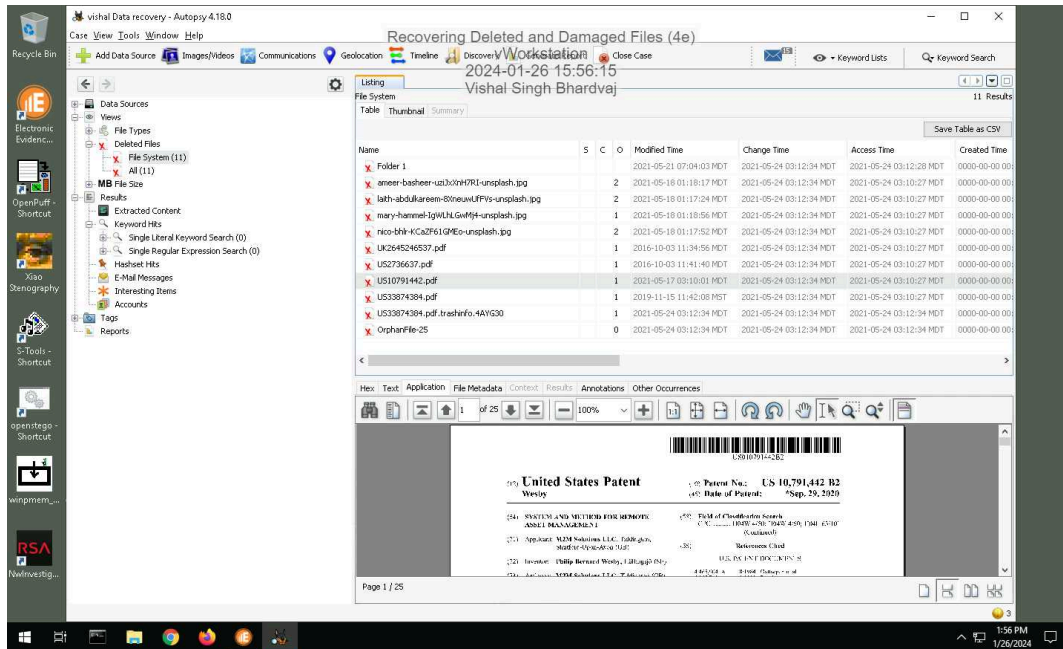


Part 2: Recover Deleted Files from an Ext4 Drive Image with Autopsy

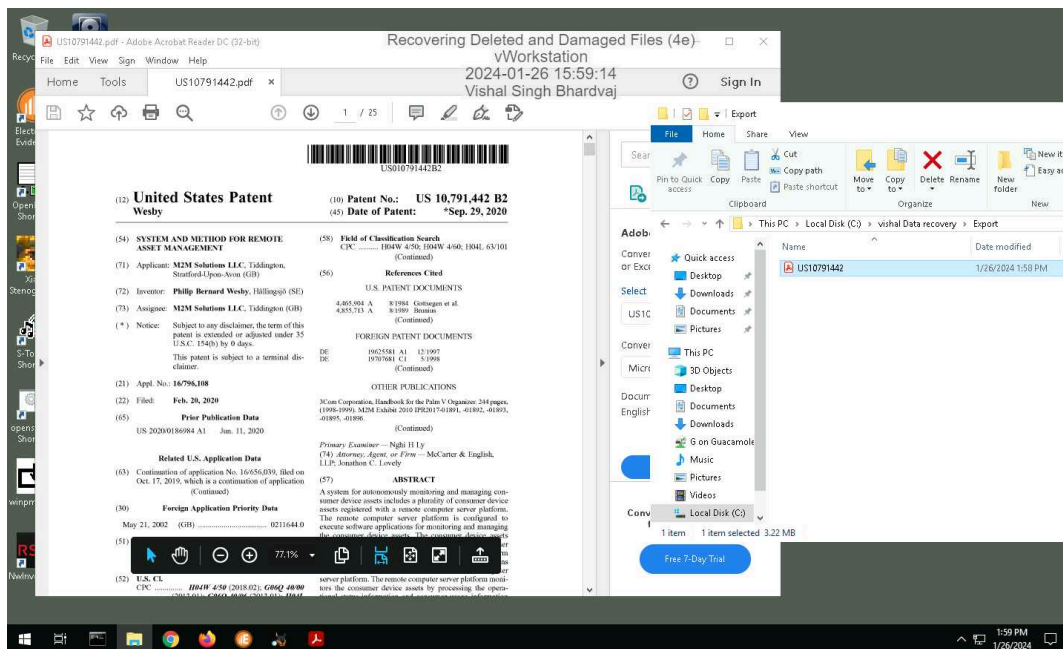
Recovering Deleted and Damaged Files (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 03

14. Make a screen capture showing the contents of the list of deleted files in Autopsy.



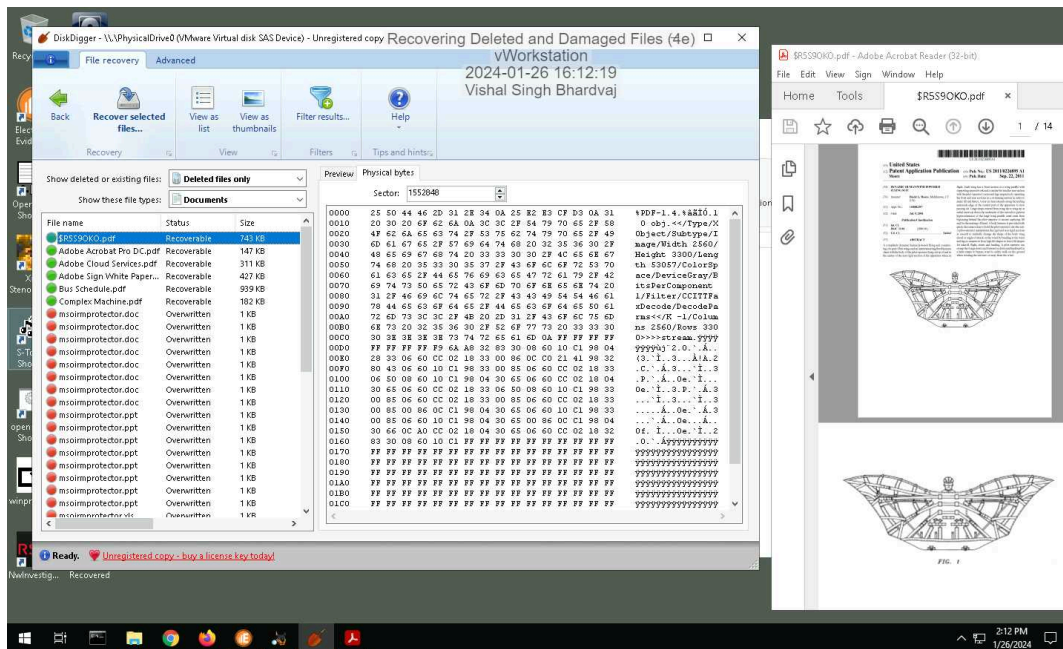
22. Make a screen capture showing the recovered patent file.



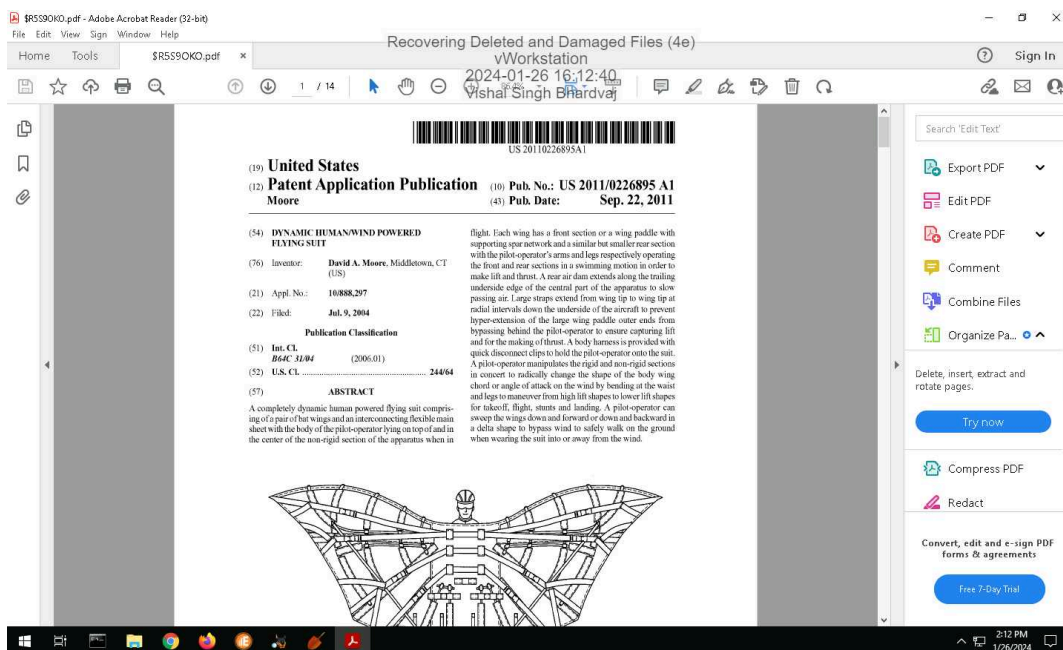
Section 2: Applied Learning

Part 1: Recover Deleted Files in Windows with DiskDigger

9. Make a screen capture showing the deleted patent file in DiskDigger.



15. Make a screen capture showing the recovered patent file.

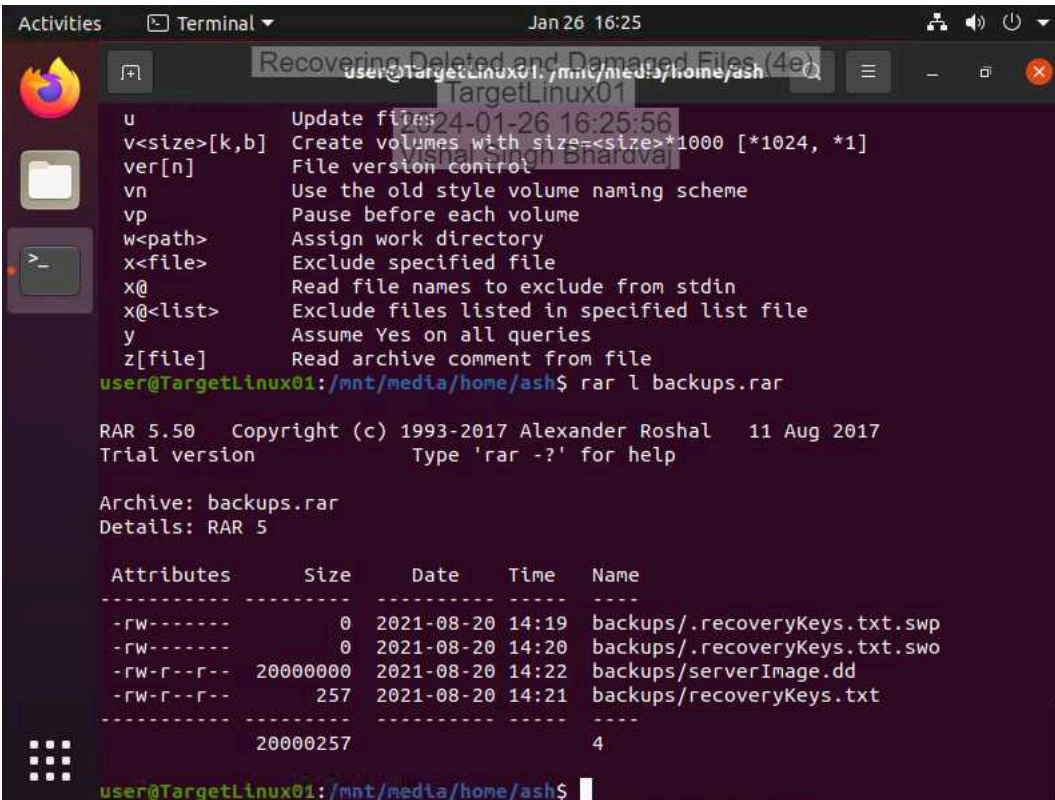


Part 2: Recover Deleted Files in Linux with PhotoRec

Recovering Deleted and Damaged Files (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 03

9. Make a screen capture showing the contents of the RAR archive in the `/mnt/media/home/ash` directory.



The screenshot shows a terminal window titled "Recovering Deleted and Damaged Files (4e)" with the user "user@TargetLinux01" in the directory "/mnt/media/home/ash". The terminal displays the output of the command `rar l backups.rar`. The output shows the RAR version (5.50), copyright information, and a list of files in the archive. The files are:

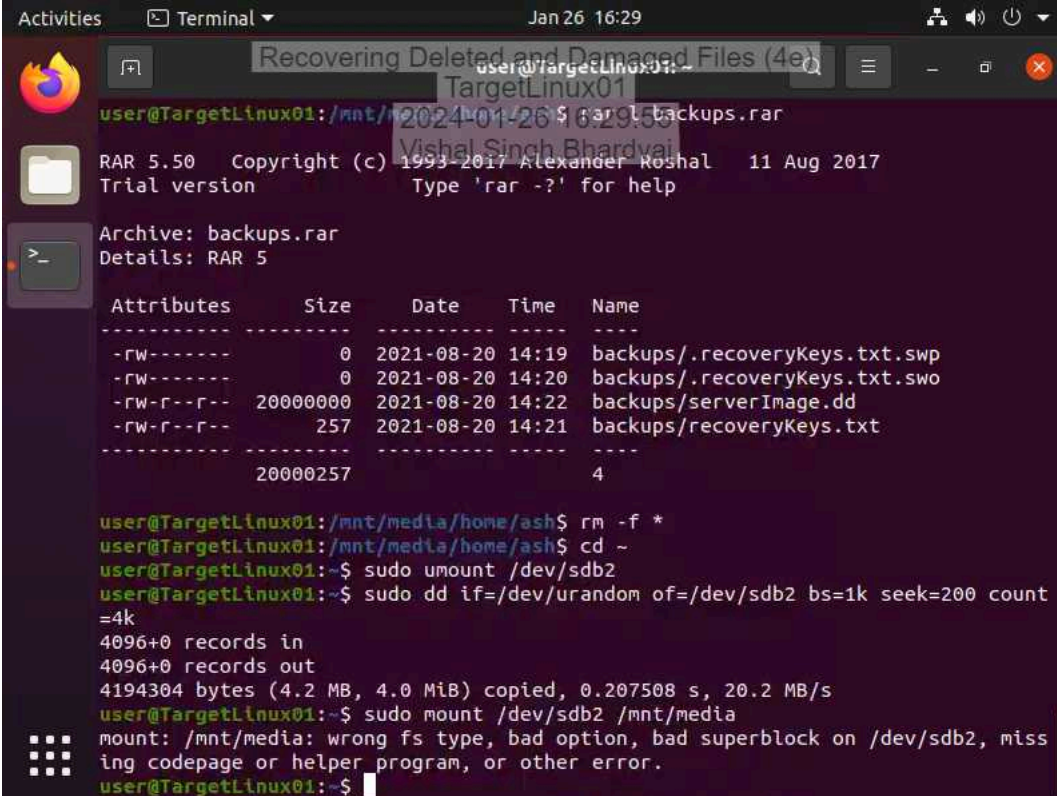
Attributes	Size	Date	Time	Name
-rw-----	0	2021-08-20	14:19	backups/.recoveryKeys.txt.swp
-rw-----	0	2021-08-20	14:20	backups/.recoveryKeys.txt.swo
-rw-r--r--	20000000	2021-08-20	14:22	backups/serverImage.dd
-rw-r--r--	257	2021-08-20	14:21	backups/recoveryKeys.txt
20000257		4		

The terminal prompt is `user@TargetLinux01:/mnt/media/home/ash$`.

Recovering Deleted and Damaged Files (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 03

15. Make a screen capture showing the failed mount attempt on the /dev/sdb2 device.

A terminal window titled 'Terminal' with a date and time of 'Jan 26 16:29'. The prompt is 'user@TargetLinux01:~'. The user runs 'rar x backups.rar', which extracts files. A table of extracted files is shown. Then, the user runs 'rm -f *', 'cd ~', 'sudo umount /dev/sdb2', and 'sudo dd if=/dev/urandom of=/dev/sdb2 bs=1k seek=200 count=4k'. Finally, the user runs 'sudo mount /dev/sdb2 /mnt/media', which fails with the error: 'mount: /mnt/media: wrong fs type, bad option, bad superblock on /dev/sdb2, missing codepage or helper program, or other error.'

```
user@TargetLinux01:~$ rar x backups.rar
RAR 5.50 Copyright (c) 1993-2017 Alexander Roshal 11 Aug 2017
Trial version
Type 'rar -?' for help

Archive: backups.rar
Details: RAR 5

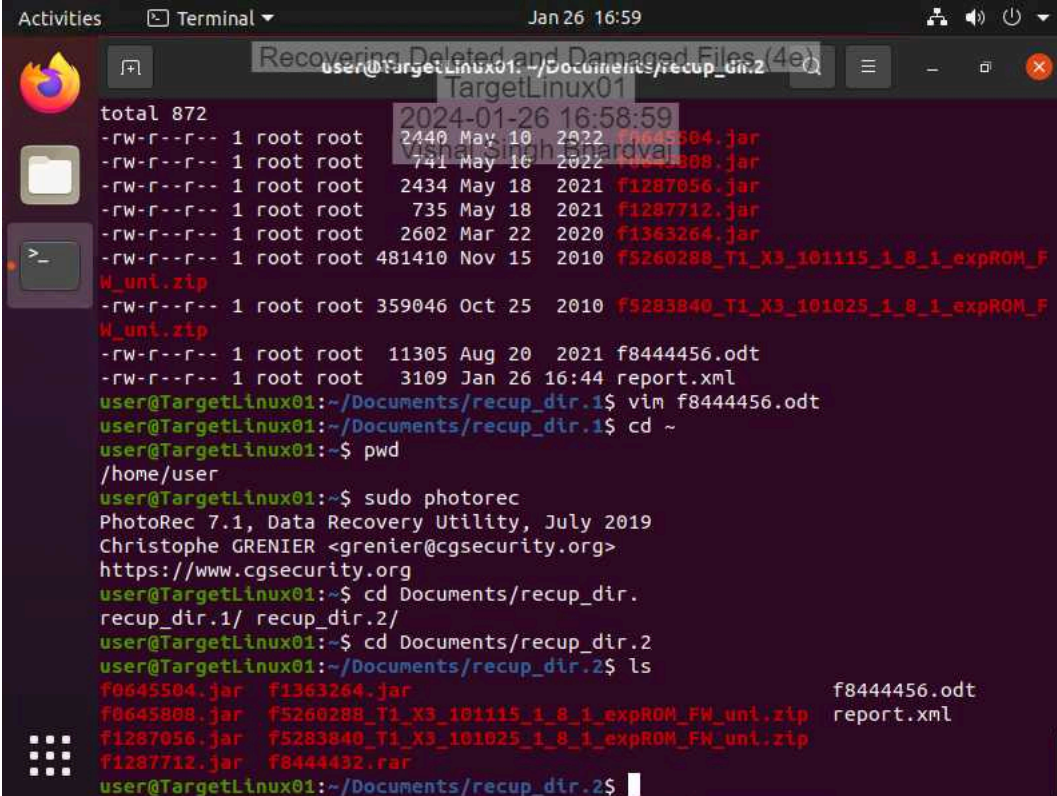
Attributes      Size      Date      Time      Name
-----
-rw-----      0      2021-08-20 14:19 backups/.recoveryKeys.txt.swp
-rw-----      0      2021-08-20 14:20 backups/.recoveryKeys.txt.swo
-rw-r--r-- 20000000      2021-08-20 14:22 backups/serverImage.dd
-rw-r--r--    257      2021-08-20 14:21 backups/recoveryKeys.txt
-----
                20000257                4

user@TargetLinux01:/mnt/media/home/ash$ rm -f *
user@TargetLinux01:/mnt/media/home/ash$ cd ~
user@TargetLinux01:~$ sudo umount /dev/sdb2
user@TargetLinux01:~$ sudo dd if=/dev/urandom of=/dev/sdb2 bs=1k seek=200 count=4k
4096+0 records in
4096+0 records out
4194304 bytes (4.2 MB, 4.0 MiB) copied, 0.207508 s, 20.2 MB/s
user@TargetLinux01:~$ sudo mount /dev/sdb2 /mnt/media
mount: /mnt/media: wrong fs type, bad option, bad superblock on /dev/sdb2, missing codepage or helper program, or other error.
user@TargetLinux01:~$
```

Recovering Deleted and Damaged Files (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 03

32. Make a screen capture showing the compressed files recovered by PhotoRec.

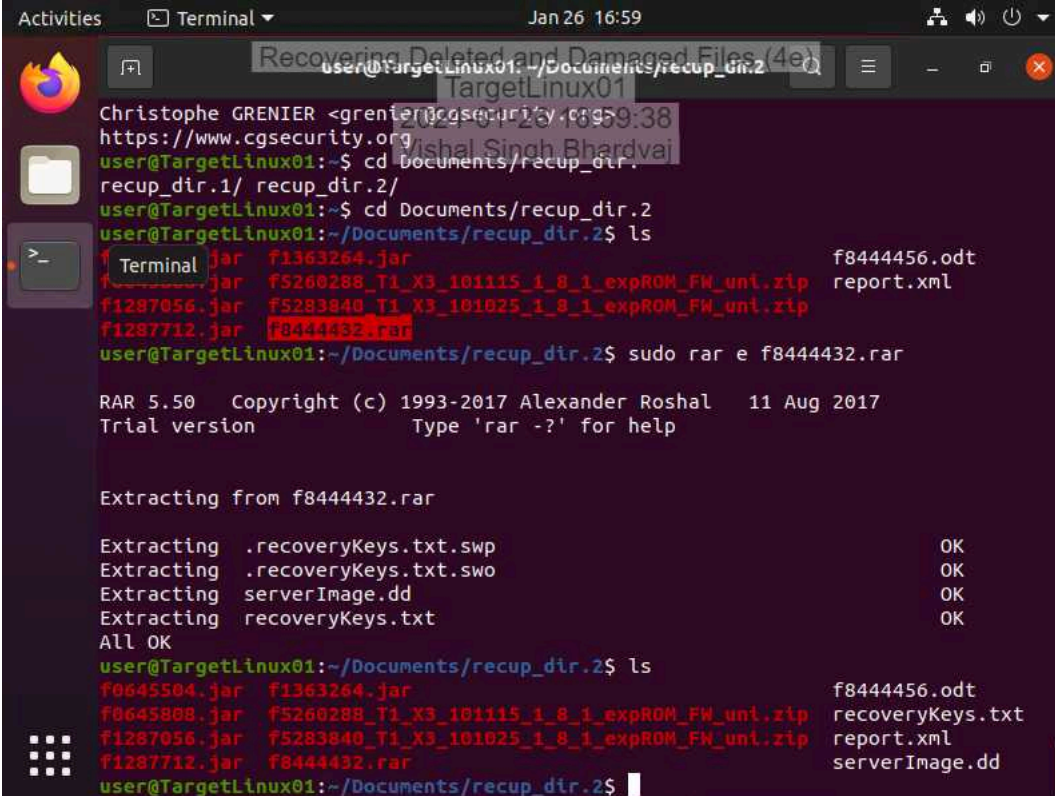


```
user@TargetLinux01: ~/Documents/recup_dir.2
2024-01-26 16:58:59
Total: 872
-rw-r--r-- 1 root root 2440 May 10 2022 f0645504.jar
-rw-r--r-- 1 root root 741 May 16 2022 f0645808.jar
-rw-r--r-- 1 root root 2434 May 18 2021 f1287056.jar
-rw-r--r-- 1 root root 735 May 18 2021 f1287712.jar
-rw-r--r-- 1 root root 2602 Mar 22 2020 f1363264.jar
-rw-r--r-- 1 root root 481410 Nov 15 2010 f5260288_T1_X3_101115_1_8_1_expROM_FW_uni.zip
-rw-r--r-- 1 root root 359046 Oct 25 2010 f5283840_T1_X3_101025_1_8_1_expROM_FW_uni.zip
-rw-r--r-- 1 root root 11305 Aug 20 2021 f8444456.odt
-rw-r--r-- 1 root root 3109 Jan 26 16:44 report.xml
user@TargetLinux01:~/Documents/recup_dir.1$ vim f8444456.odt
user@TargetLinux01:~/Documents/recup_dir.1$ cd ~
user@TargetLinux01:~$ pwd
/home/user
user@TargetLinux01:~$ sudo photorec
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
user@TargetLinux01:~$ cd Documents/recup_dir.
recup_dir.1/ recup_dir.2/
user@TargetLinux01:~$ cd Documents/recup_dir.2
user@TargetLinux01:~/Documents/recup_dir.2$ ls
f0645504.jar f1363264.jar f8444456.odt
f0645808.jar f5260288_T1_X3_101115_1_8_1_expROM_FW_uni.zip report.xml
f1287056.jar f5283840_T1_X3_101025_1_8_1_expROM_FW_uni.zip
f1287712.jar f8444432.rar
user@TargetLinux01:~/Documents/recup_dir.2$
```

Recovering Deleted and Damaged Files (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 03

35. Make a screen capture showing the backup files recovered from the RAR archive.

A terminal window titled 'Terminal' with a date and time of 'Jan 26 16:59'. The window shows a user at 'TargetLinux01' in the directory '~/Documents/recup_dir.2'. The user lists files, including 'f1363264.jar', 'f5260288_T1_X3_101115_1_8_1_expROM_FW_uni.zip', 'f1287056.jar', 'f5283840_T1_X3_101025_1_8_1_expROM_FW_uni.zip', and 'f1287712.jar'. They then run 'sudo rar e f8444432.rar'. The output shows 'RAR 5.50 Copyright (c) 1993-2017 Alexander Roshal 11 Aug 2017 Trial version'. It then lists files being extracted from 'f8444432.rar': '.recoveryKeys.txt.swp', '.recoveryKeys.txt.swo', 'serverImage.dd', and 'recoveryKeys.txt'. Finally, the user lists the directory again, showing the recovered files: 'f0645504.jar', 'f1363264.jar', 'f0645808.jar', 'f5260288_T1_X3_101115_1_8_1_expROM_FW_uni.zip', 'f1287056.jar', 'f5283840_T1_X3_101025_1_8_1_expROM_FW_uni.zip', 'f1287712.jar', and 'f8444432.rar'.

```
user@TargetLinux01:~/Documents/recup_dir.2$ ls
f1363264.jar      f8444456.odt
f5260288_T1_X3_101115_1_8_1_expROM_FW_uni.zip  report.xml
f1287056.jar      f5283840_T1_X3_101025_1_8_1_expROM_FW_uni.zip
f1287712.jar      f8444432.rar
user@TargetLinux01:~/Documents/recup_dir.2$ sudo rar e f8444432.rar

RAR 5.50   Copyright (c) 1993-2017 Alexander Roshal   11 Aug 2017
Trial version                Type 'rar -?' for help

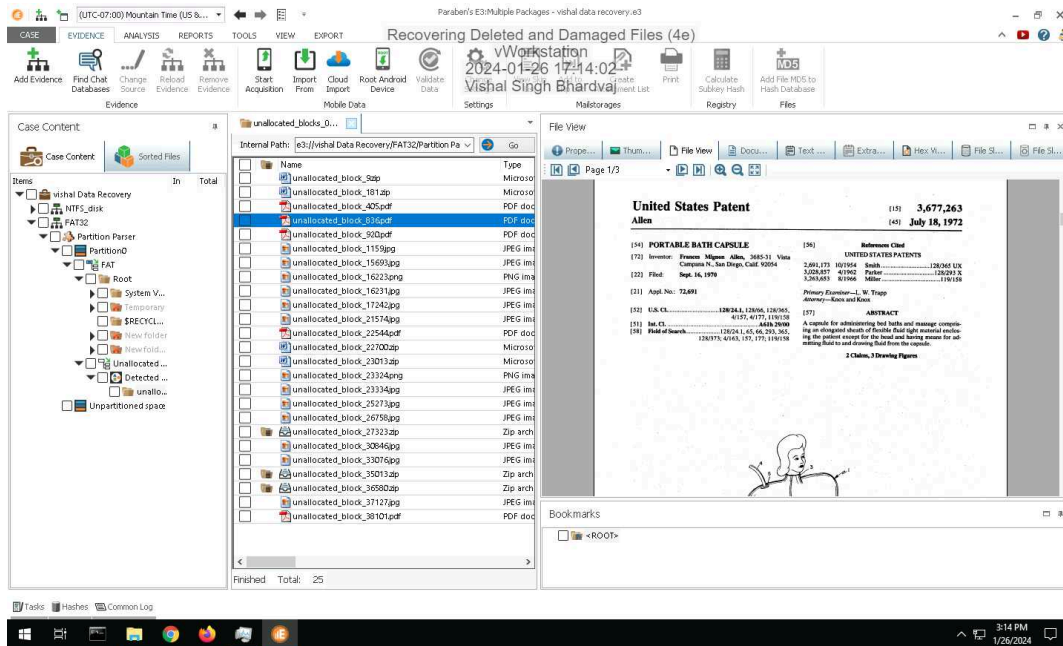
Extracting from f8444432.rar

Extracting .recoveryKeys.txt.swp                OK
Extracting .recoveryKeys.txt.swo                OK
Extracting serverImage.dd                      OK
Extracting recoveryKeys.txt                    OK
All OK
user@TargetLinux01:~/Documents/recup_dir.2$ ls
f0645504.jar  f1363264.jar      f8444456.odt
f0645808.jar  f5260288_T1_X3_101115_1_8_1_expROM_FW_uni.zip  recoveryKeys.txt
f1287056.jar  f5283840_T1_X3_101025_1_8_1_expROM_FW_uni.zip  report.xml
f1287712.jar  f8444432.rar      serverImage.dd
user@TargetLinux01:~/Documents/recup_dir.2$
```


Section 3: Challenge and Analysis

Part 1: Recover Deleted Files from a FAT Drive Image

Make a screen capture showing the patent file recovered from the FAT32 drive image within E3.



Part 2: Recover Deleted Files from a APFS Drive Image

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 03