

Student: Jake Simpson

Email: jaksimps@iu.edu

Time on Task: 1 hour, 19 minutes

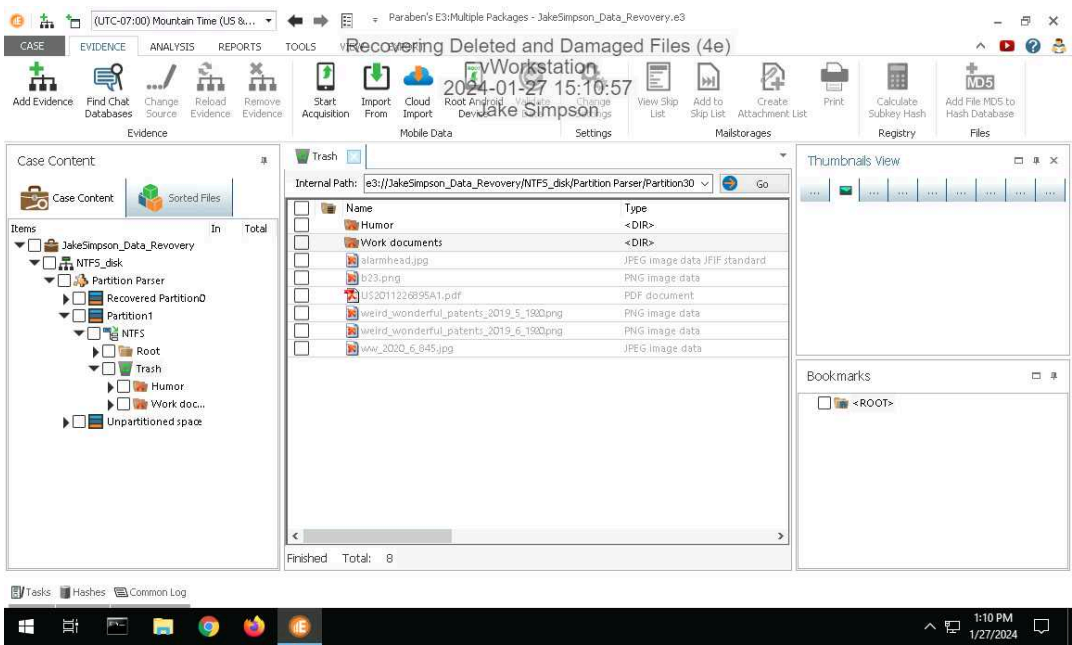
Progress: 100%

Report Generated: Saturday, January 27, 2024 at 4:04 PM

Section 1: Hands-On Demonstration

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

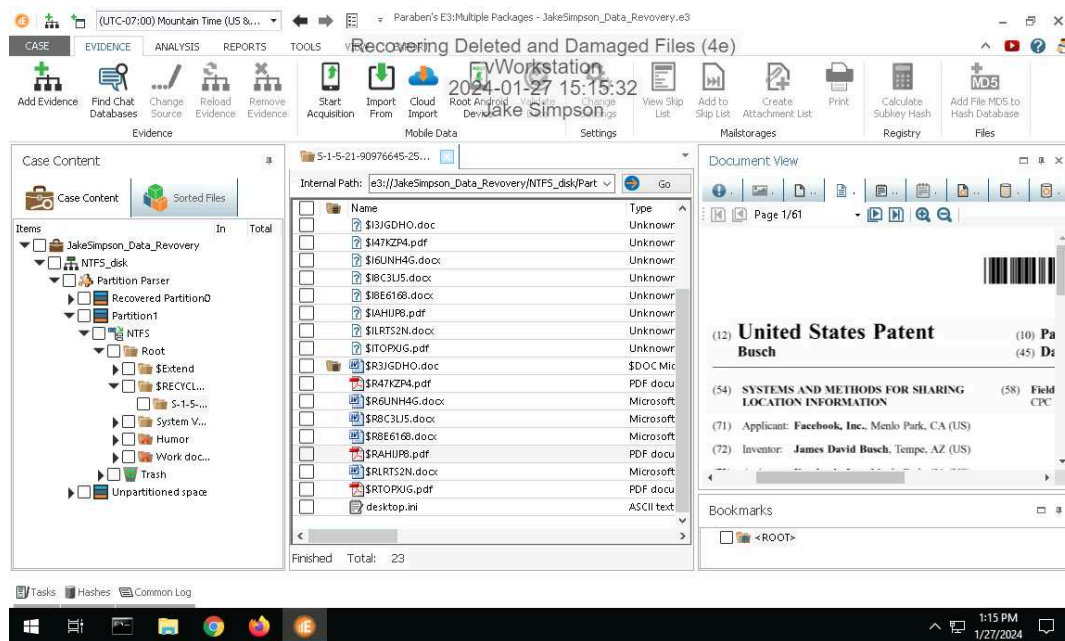
13. Make a screen capture showing the list of recovered files and folders in the E3 Trash folder.



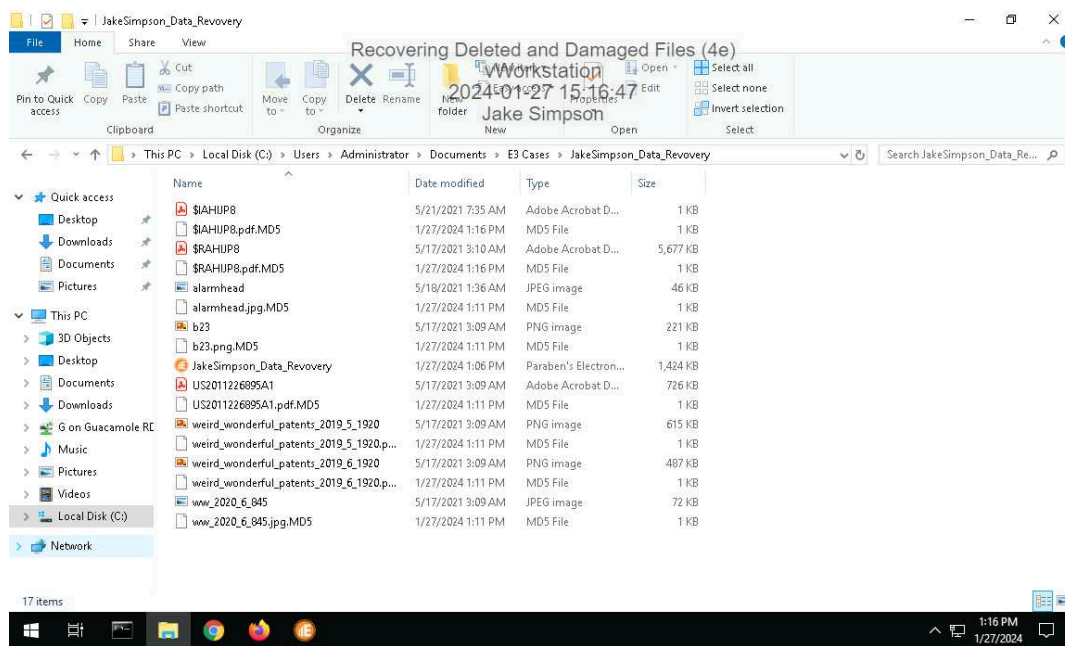
Recovering Deleted and Damaged Files (4e)

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.

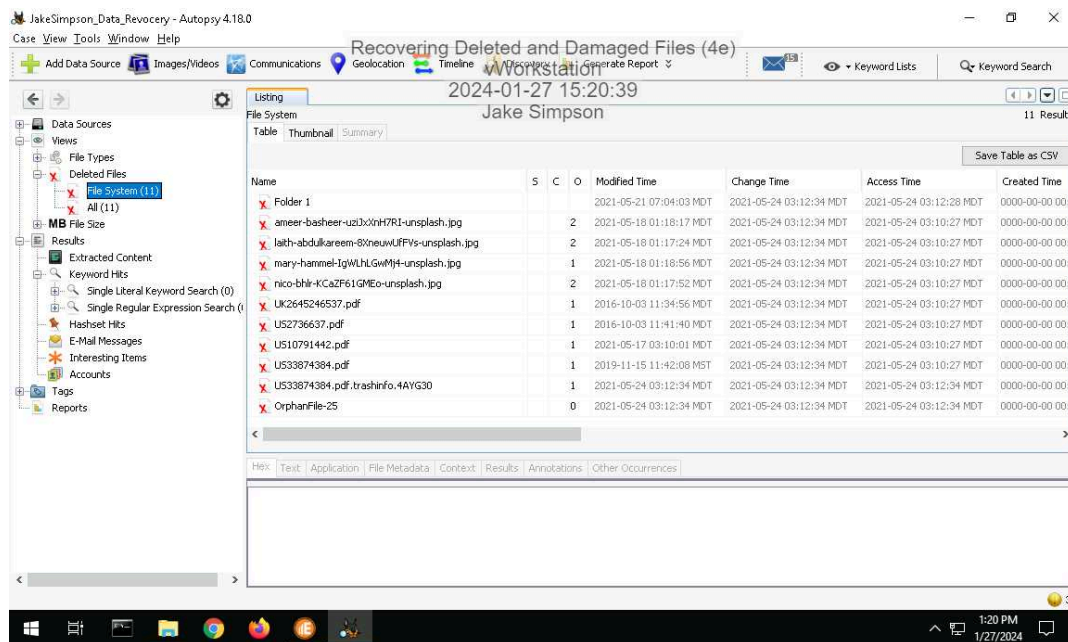


Part 2: Recover Deleted Files from an Ext4 Drive Image with Autopsy

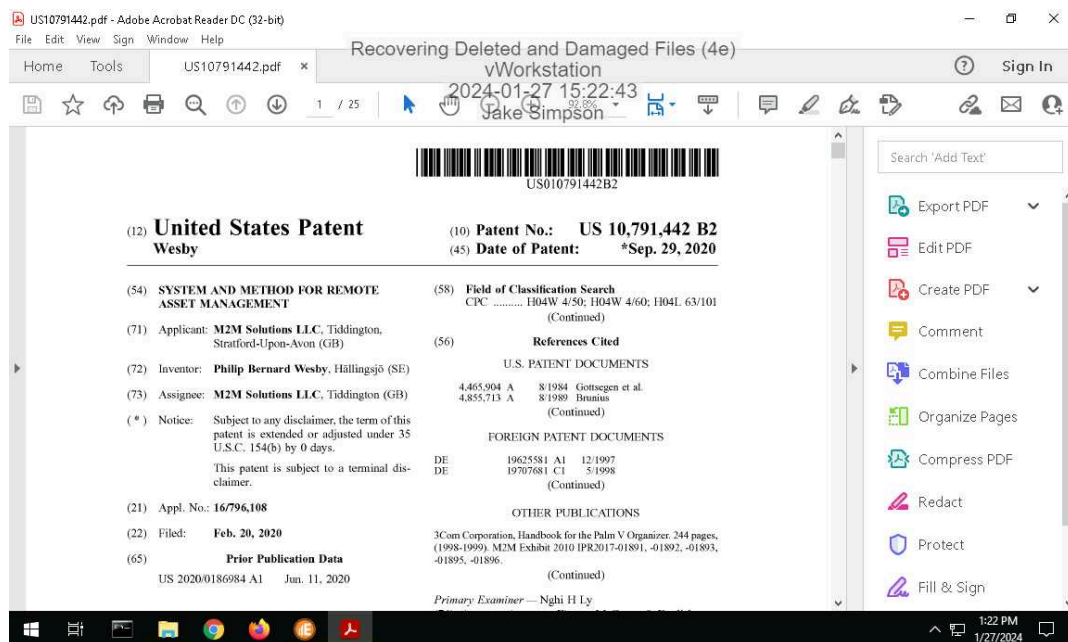
Recovering Deleted and Damaged Files (4e)

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.



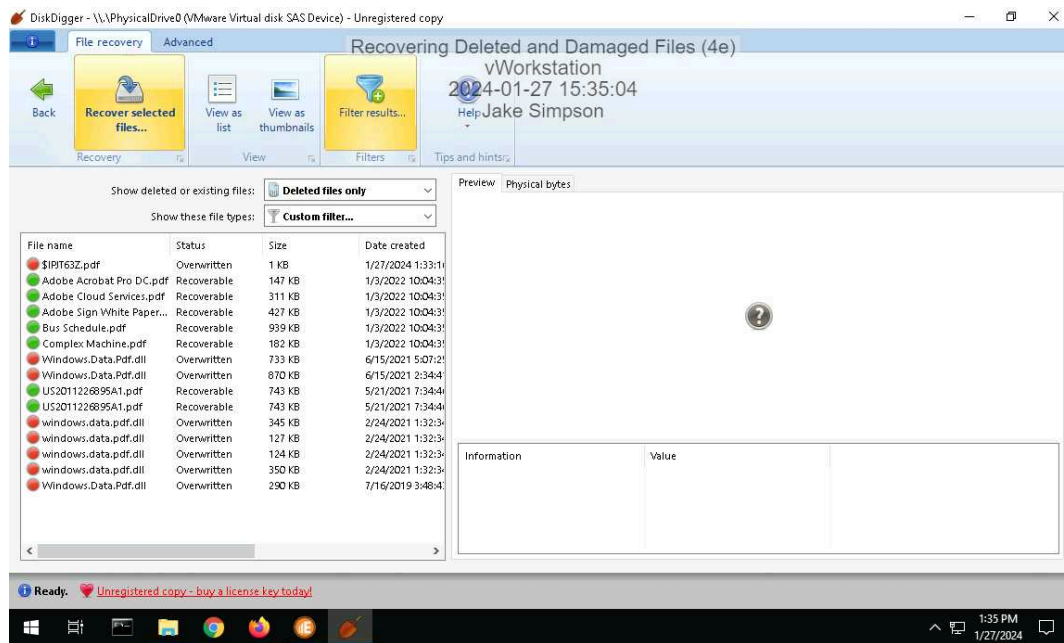
22. Make a screen capture showing the recovered patent file.



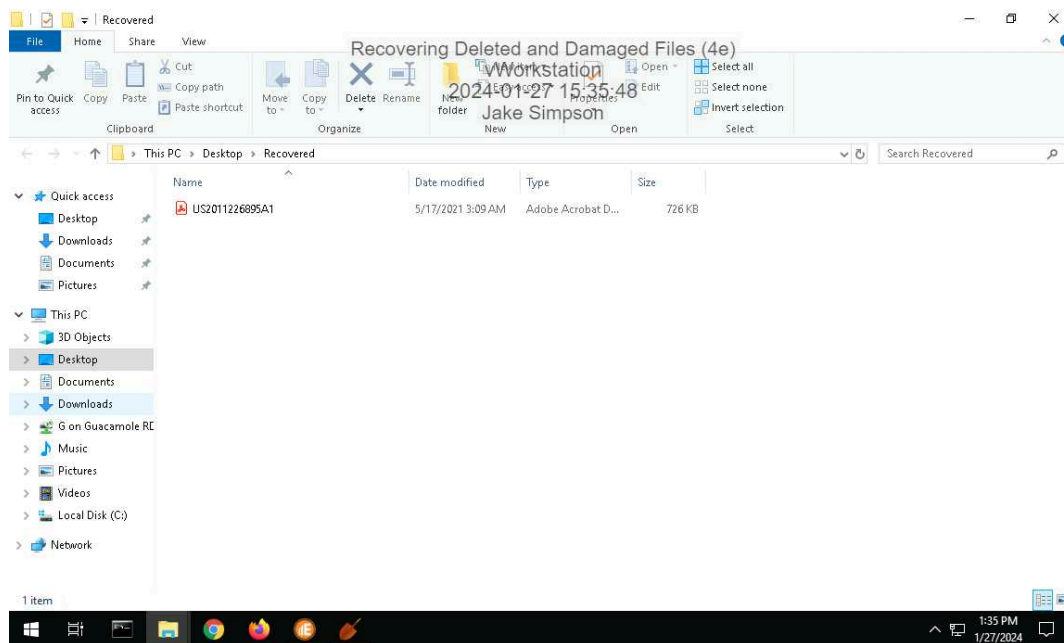
Section 2: Applied Learning

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.

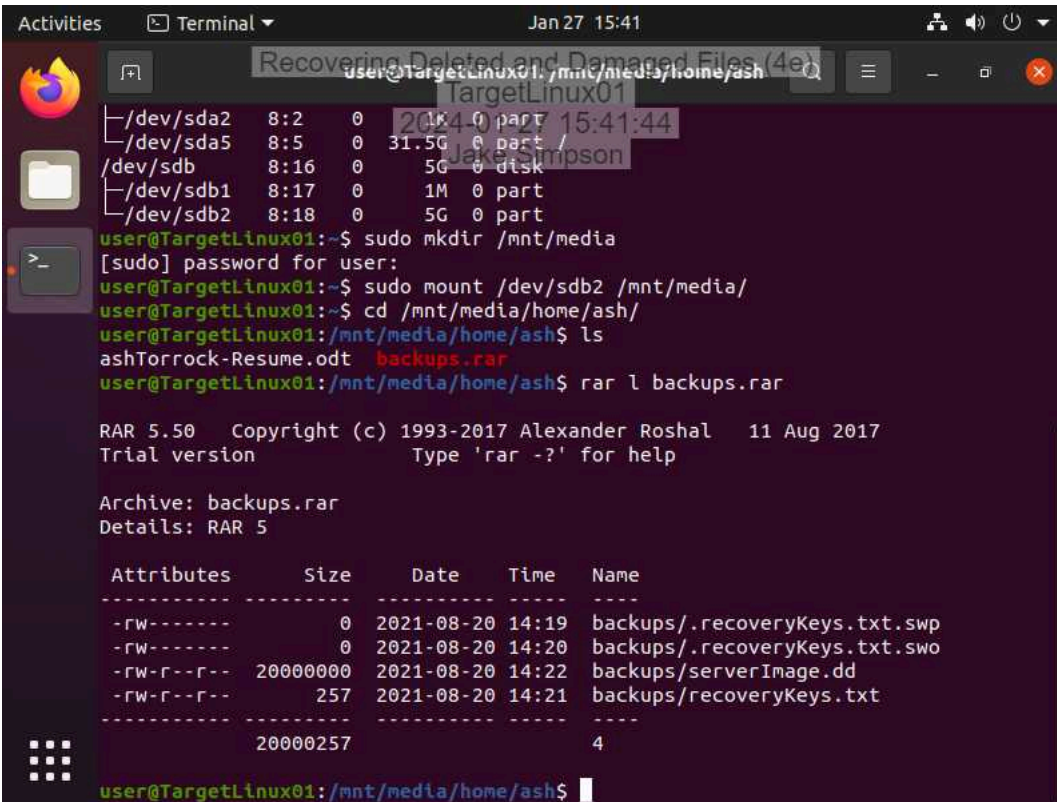


Part 2: Recover Deleted Files in Linux with PhotoRec

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 on a system named 'TargetLinux01'. The user is at the prompt 'user@TargetLinux01:~\$'. The terminal output shows the following commands and results:

```
user@TargetLinux01:~$ lsblk
lsblk output:
/dev/sda2 8:2 0 1M 0 part
/dev/sda5 8:5 0 31.5G 0 part
/dev/sdb 8:16 0 5G 0 disk
/dev/sdb1 8:17 0 1M 0 part
/dev/sdb2 8:18 0 5G 0 part

user@TargetLinux01:~$ sudo mkdir /mnt/media
[sudo] password for user:
user@TargetLinux01:~$ sudo mount /dev/sdb2 /mnt/media/
user@TargetLinux01:~$ cd /mnt/media/home/ash/
user@TargetLinux01:/mnt/media/home/ash$ ls
ashTorrock-Resume.odt backups.rar
user@TargetLinux01:/mnt/media/home/ash$ rar l 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

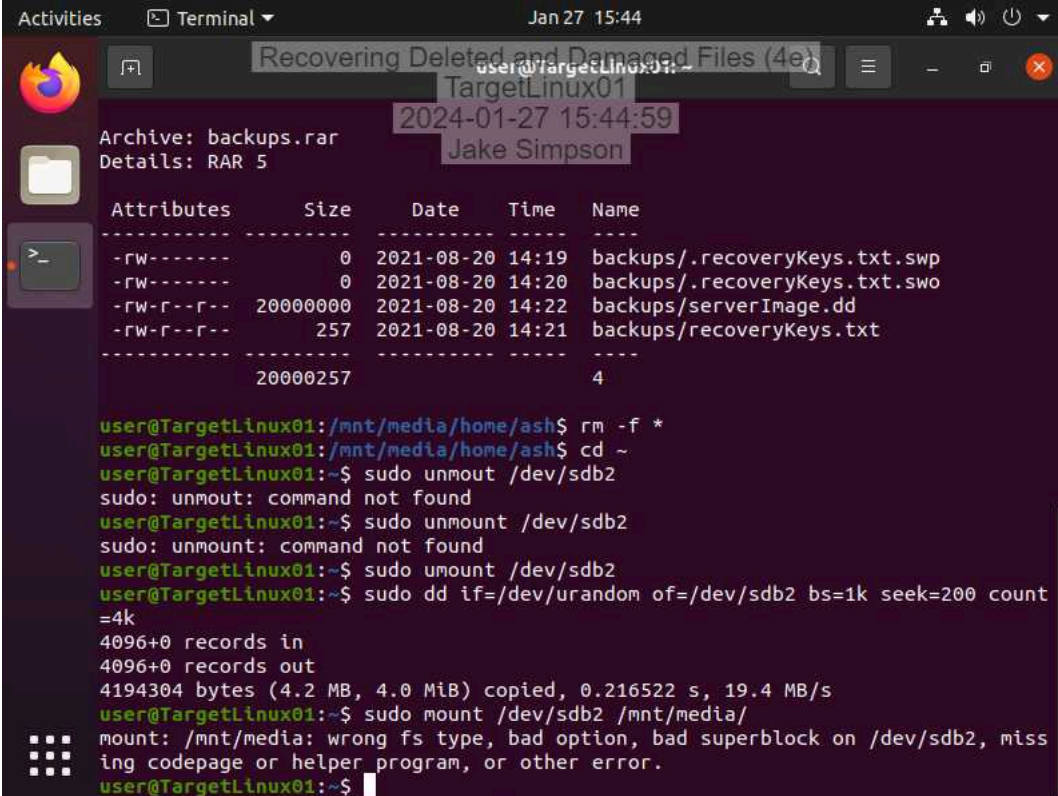
Attributes      Size      Date      Time      Name
-----
-rw-----      0      2021-08-20 14:19 backups/.recoveryKeys.txt.swp
-rw-----      0      2021-08-20 14:20 backups/.recoveryKeys.txt.swo
-rw-r--r-- 20000000 2021-08-20 14:22 backups/serverImage.dd
-rw-r--r--    257      2021-08-20 14:21 backups/recoveryKeys.txt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

user@TargetLinux01:/mnt/media/home/ash$
```


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.



The screenshot shows a terminal window titled "Recovering Deleted and Damaged Files (4e)" with the user "user@TargetLinux01". The terminal displays the output of the `rar` command for the file `backups.rar`, showing details of the RAR 5 archive. Below this, a table lists the files within the archive:

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

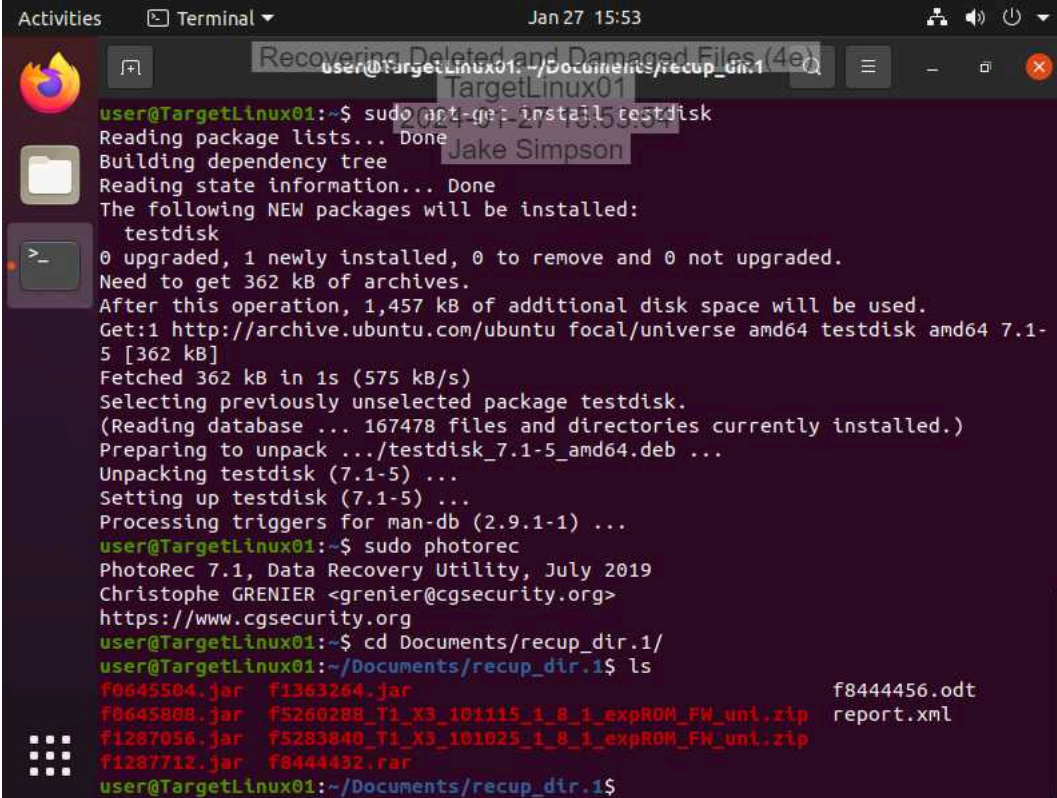
Following the table, the terminal shows a series of commands and their outputs:

```
user@TargetLinux01:/mnt/media/home/ash$ rm -f *
user@TargetLinux01:/mnt/media/home/ash$ cd ~
user@TargetLinux01:~$ sudo umount /dev/sdb2
sudo: umount: command not found
user@TargetLinux01:~$ sudo unmount /dev/sdb2
sudo: unmount: command not found
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, 0.216522 s, 19.4 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.

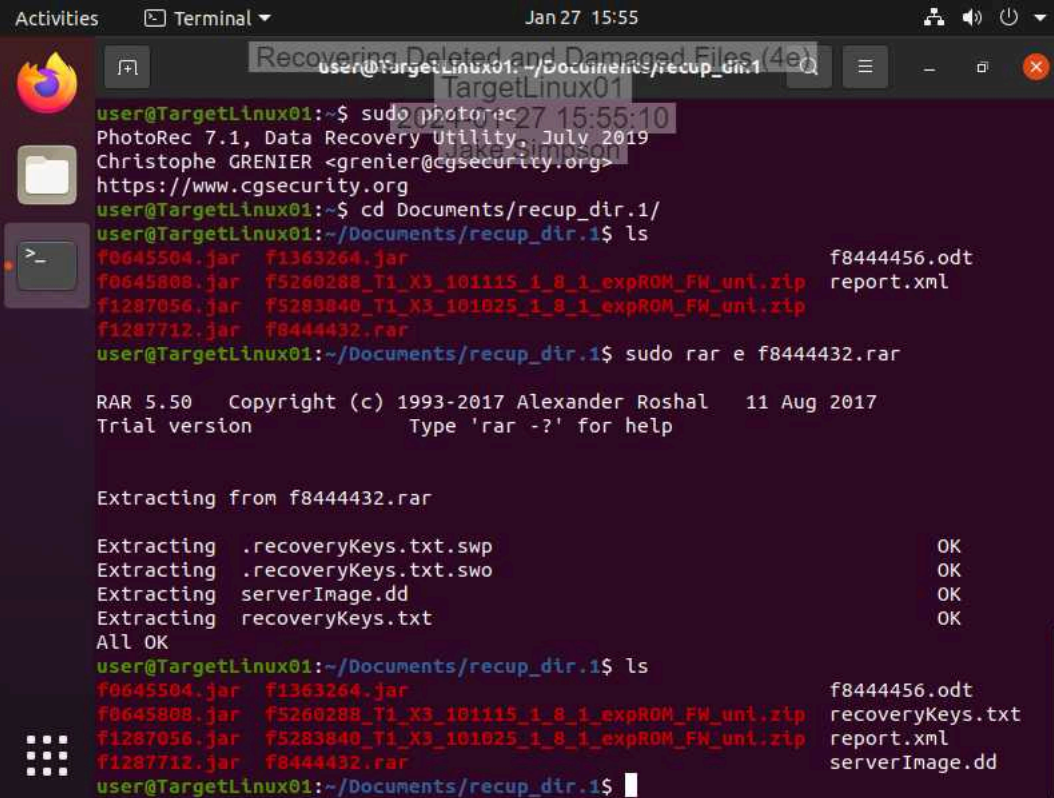


```
user@TargetLinux01: ~/Documents/recup_dir.1
user@TargetLinux01:~$ sudo apt-get install testdisk
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  testdisk
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 362 kB of archives.
After this operation, 1,457 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal/universe amd64 testdisk amd64 7.1-5 [362 kB]
Fetched 362 kB in 1s (575 kB/s)
Selecting previously unselected package testdisk.
(Reading database ... 167478 files and directories currently installed.)
Preparing to unpack .../testdisk_7.1-5_amd64.deb ...
Unpacking testdisk (7.1-5) ...
Setting up testdisk (7.1-5) ...
Processing triggers for man-db (2.9.1-1) ...
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.1/
user@TargetLinux01:~/Documents/recup_dir.1$ 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.1$
```

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.



The screenshot shows a terminal window on a Linux system. The user is in the directory `~/Documents/recup_dir.1`. They run `ls` and see a list of files including several .jar files, .zip files, and a .rar file. They then run `sudo rar e f8444432.rar` to extract the backup files. The output shows the extraction of `.recoveryKeys.txt.swp`, `.recoveryKeys.txt.swo`, `serverImage.dd`, and `recoveryKeys.txt`. Finally, they run `ls` again to see the extracted files.

```
user@TargetLinux01:~/Documents/recup_dir.1$ sudo photo-rec
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
user@TargetLinux01:~/Documents/recup_dir.1$ cd Documents/recup_dir.1/
user@TargetLinux01:~/Documents/recup_dir.1$ ls
f0645504.jar  f1363264.jar  f8444456.odt
f0645808.jar  f5260288_T1_X3_101115_1_8_1_expROM_FW_uni.zip  report.xml
f1287056.jar  f5283040_T1_X3_101025_1_8_1_expROM_FW_uni.zip
f1287712.jar  f8444432.rar
user@TargetLinux01:~/Documents/recup_dir.1$ sudo rar e f8444432.rar

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

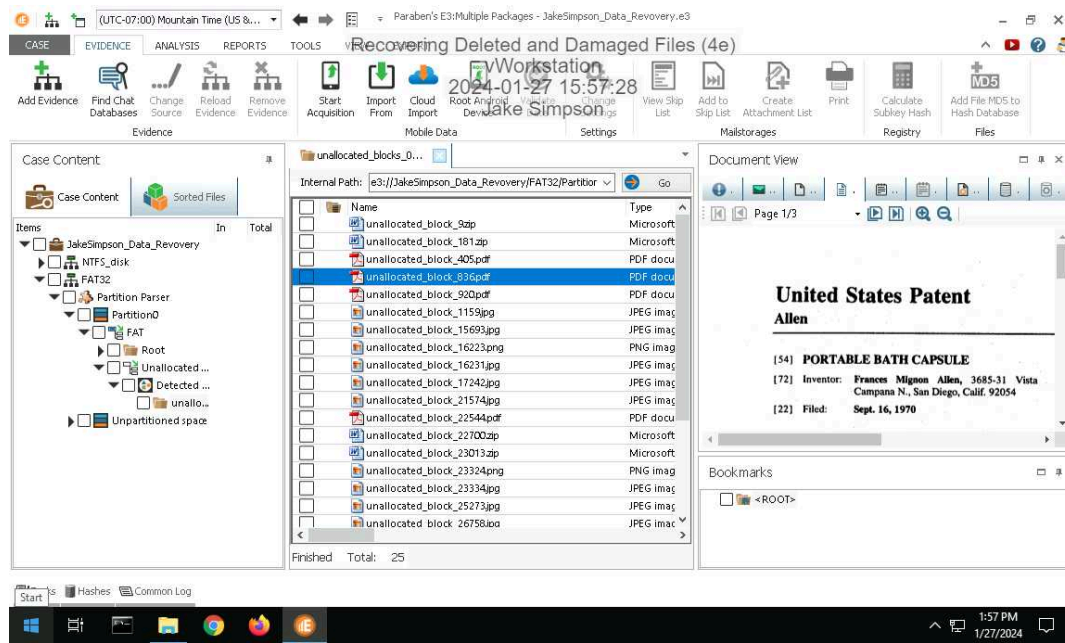
Extracting from f8444432.rar

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.1$ ls
f0645504.jar  f1363264.jar  f8444456.odt
f0645808.jar  f5260288_T1_X3_101115_1_8_1_expROM_FW_uni.zip  recoveryKeys.txt
f1287056.jar  f5283040_T1_X3_101025_1_8_1_expROM_FW_uni.zip  report.xml
f1287712.jar  f8444432.rar  serverImage.dd
user@TargetLinux01:~/Documents/recup_dir.1$
```


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

Recovering Deleted and Damaged Files (4e)

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

Make a screen capture showing the patent file recovered from the APFS drive image within Autopsy.

