

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

jose.cruz2@udc.edu

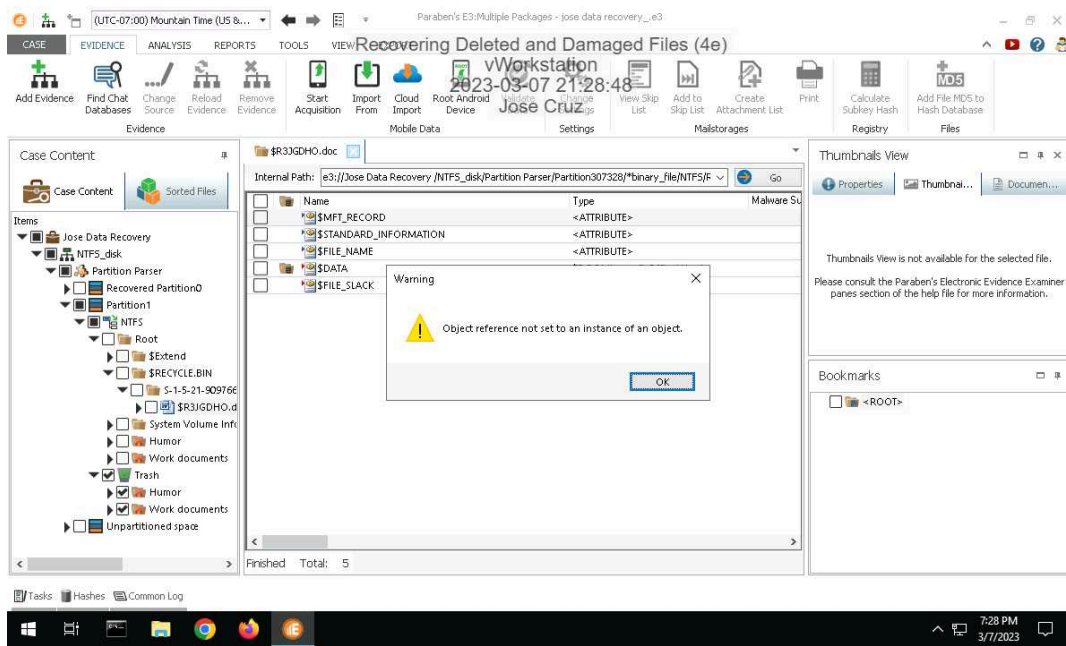
100%

Page 1 of 11

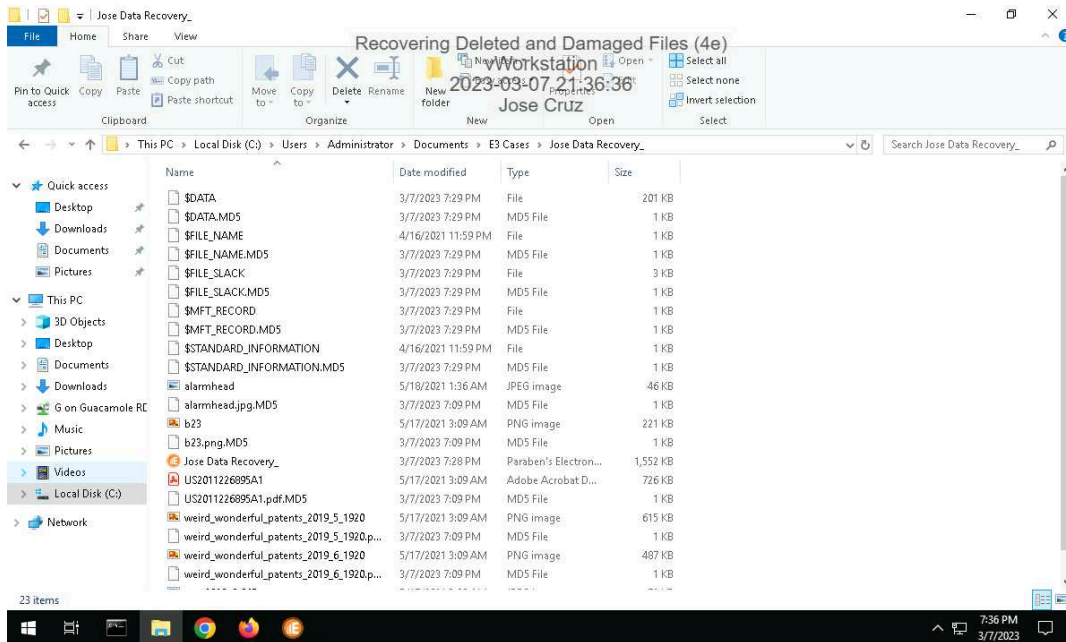
# Recovering Deleted and Damaged Files (4e)

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.

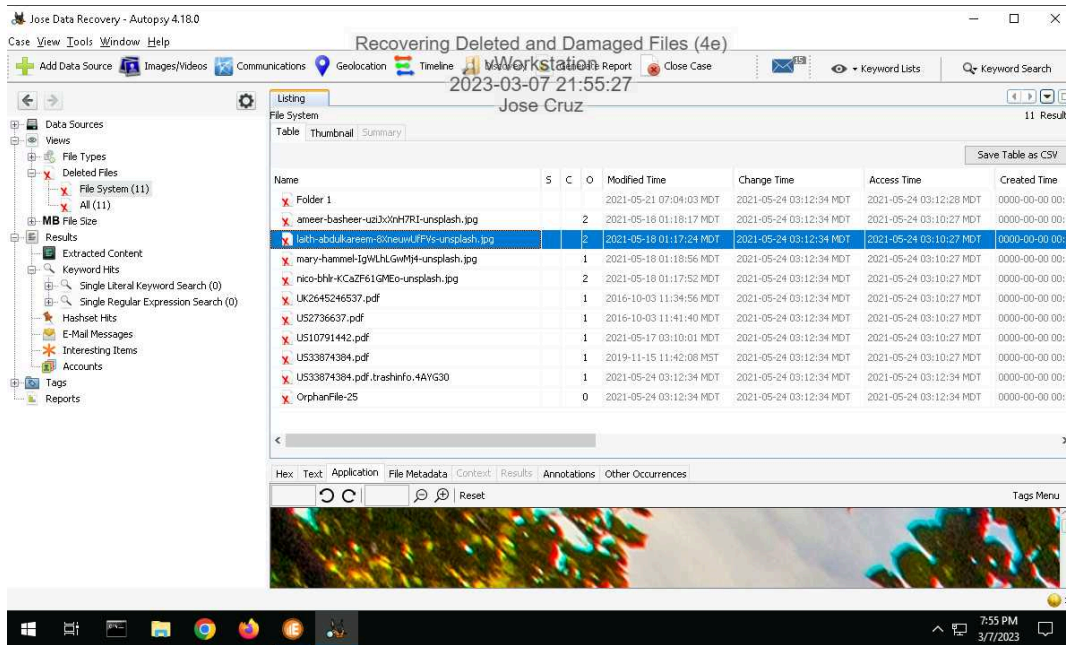


## Part 2: Recover Deleted Files from an Ext4 Drive Image with Autopsy

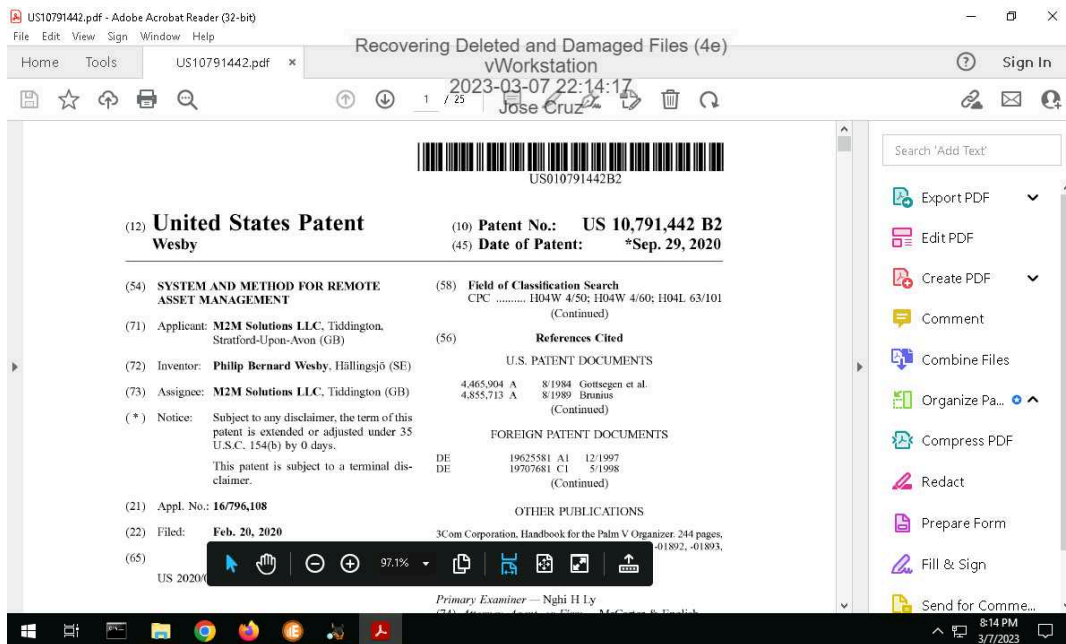
# Recovering Deleted and Damaged Files (4e)

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.



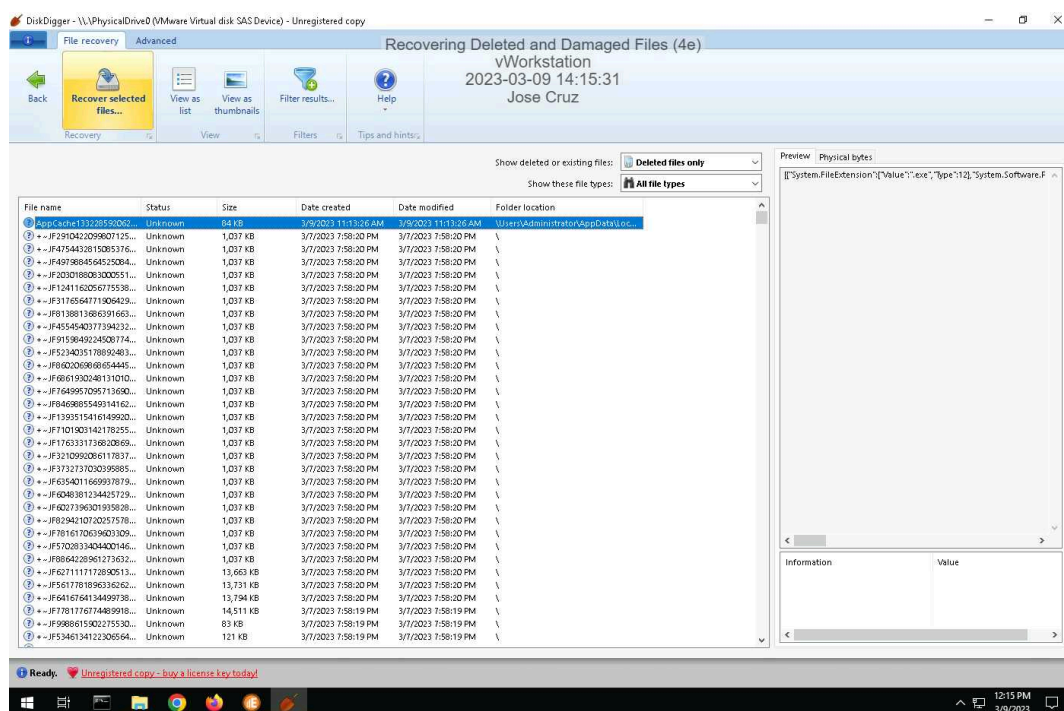
## 22. Make a screen capture showing the recovered patent file.



## 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.



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

[illegible]

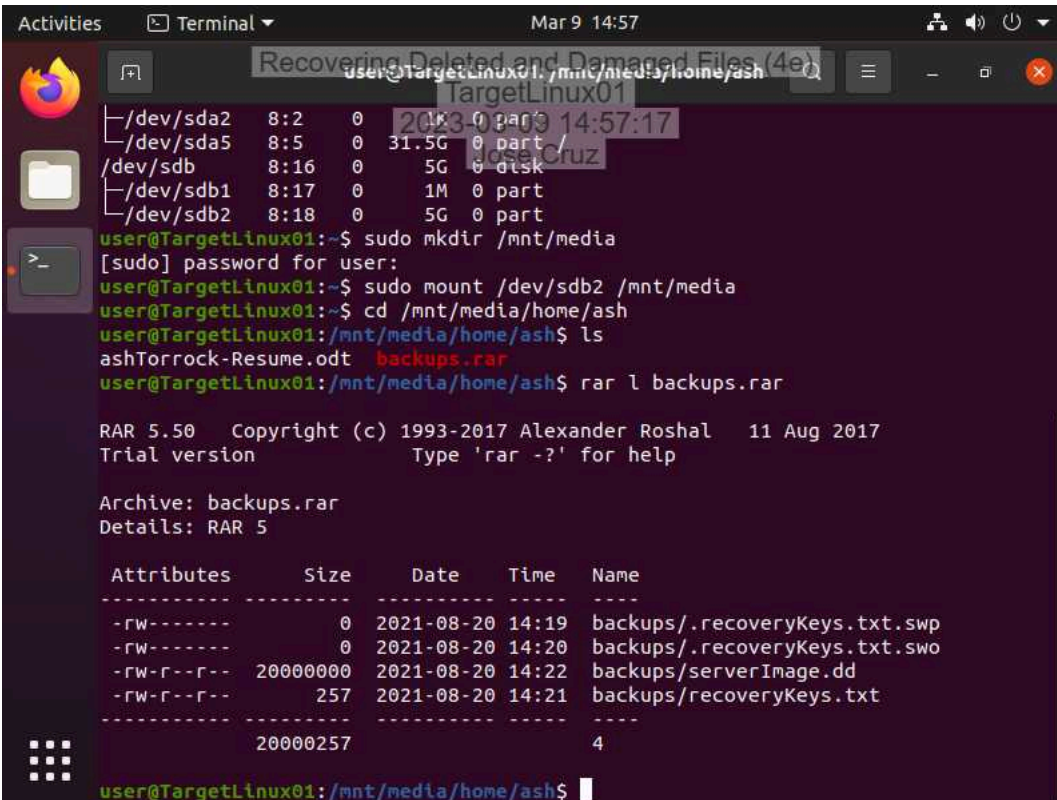
## Page 5 of 11



## 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 Linux system. The user is at the prompt `user@TargetLinux01: /mnt/media/home/ash`. The terminal output shows the following commands and results:

```
user@TargetLinux01:~$ sudo mkfs -t ext4 /dev/sdb2
[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
```

The output of the `rar l backups.rar` command is as follows:

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

Archive: backups.rar
Details: RAR 5

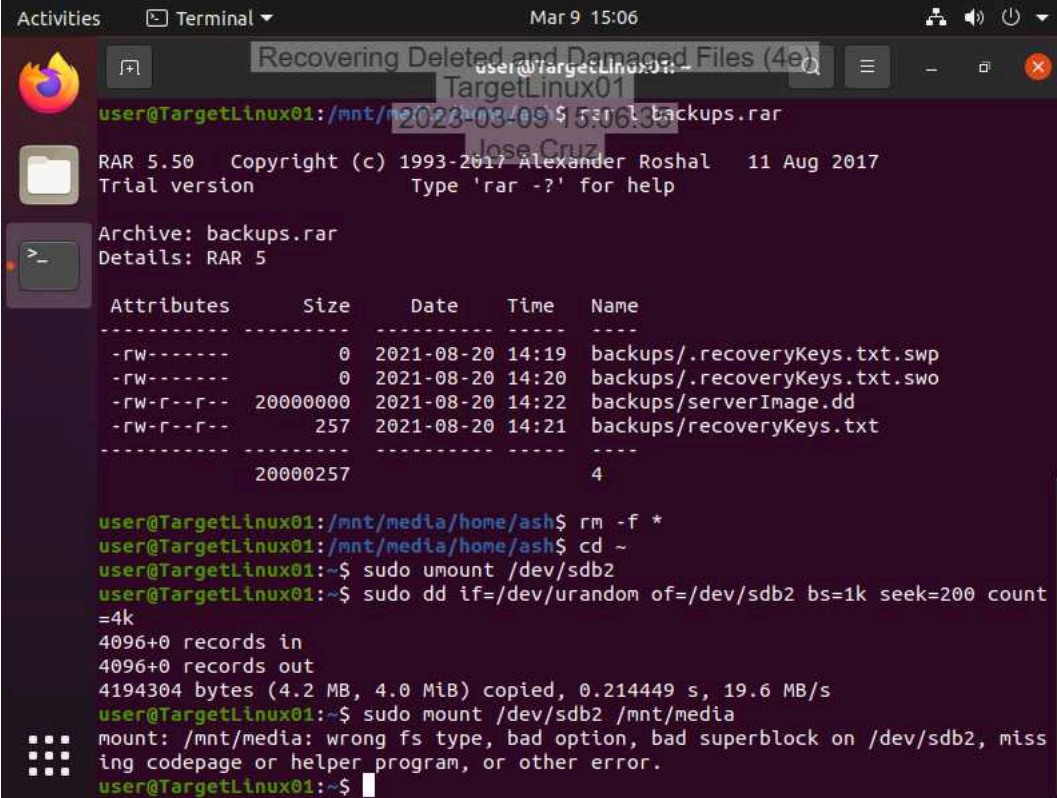
Attributes      Size      Date      Time      Name
-----
-rw-----      0      2021-08-20 14:19 backups/.recoveryKeys.txt.swp
-rw-----      0      2021-08-20 14:20 backups/.recoveryKeys.txt.swo
-rw-r--r-- 20000000 2021-08-20 14:22 backups/serverImage.dd
-rw-r--r--    257      2021-08-20 14:21 backups/recoveryKeys.txt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

The terminal prompt is now `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 on a system named 'TargetLinux01'. The user is in the directory /mnt/media/home/ash. They have just extracted a RAR archive named 'backups.rar'. The archive contains four files: two swap files (.txt.swp), a disk image (serverImage.dd), and a text file (recoveryKeys.txt). After listing the files, the user runs 'rm -f \*' to delete them, then 'cd ~' to return to the home directory. They then attempt to mount the /dev/sdb2 device to /mnt/media using 'sudo mount /dev/sdb2 /mnt/media'. The mount command 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: /mnt/media/home/ash$ 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

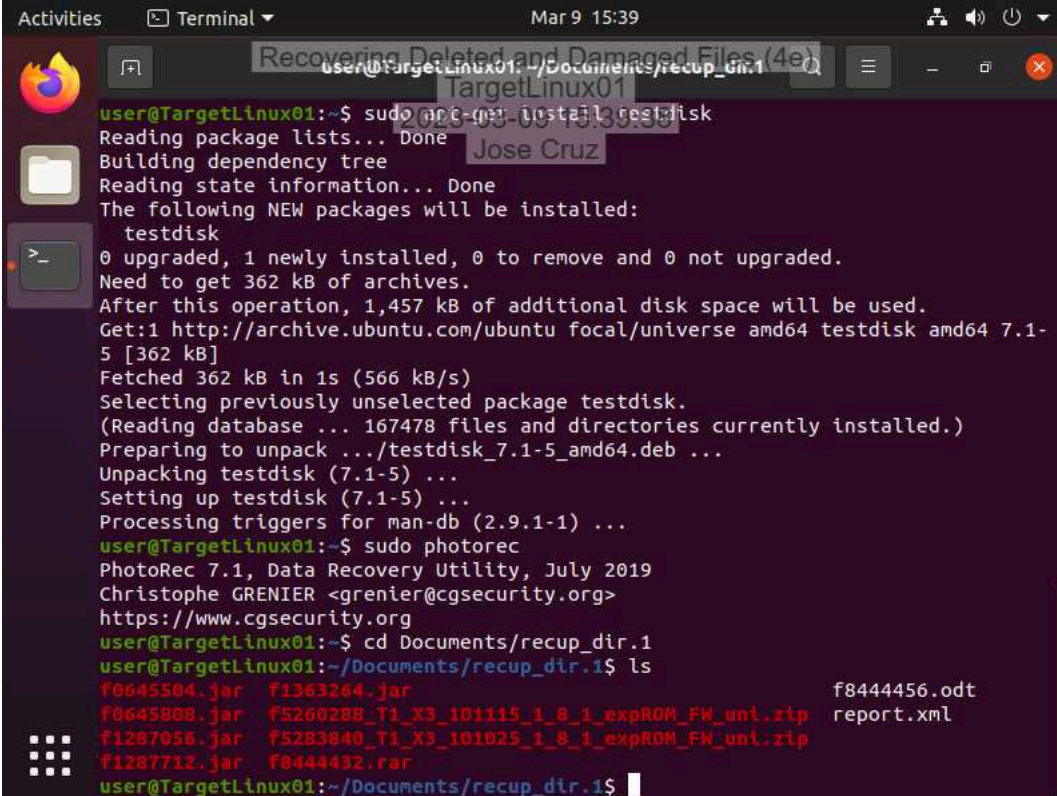
Attributes      Size      Date      Time      Name
-----
-rw-----      0      2021-08-20 14:19 backups/.recoveryKeys.txt.swp
-rw-----      0      2021-08-20 14:20 backups/.recoveryKeys.txt.swo
-rw-r--r-- 20000000      2021-08-20 14:22 backups/serverImage.dd
-rw-r--r--    257      2021-08-20 14:21 backups/recoveryKeys.txt
-----
                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, 0.214449 s, 19.6 MB/s
user@TargetLinux01: ~$ sudo mount /dev/sdb2 /mnt/media
mount: /mnt/media: wrong fs type, bad option, bad superblock on /dev/sdb2, miss
ing 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.



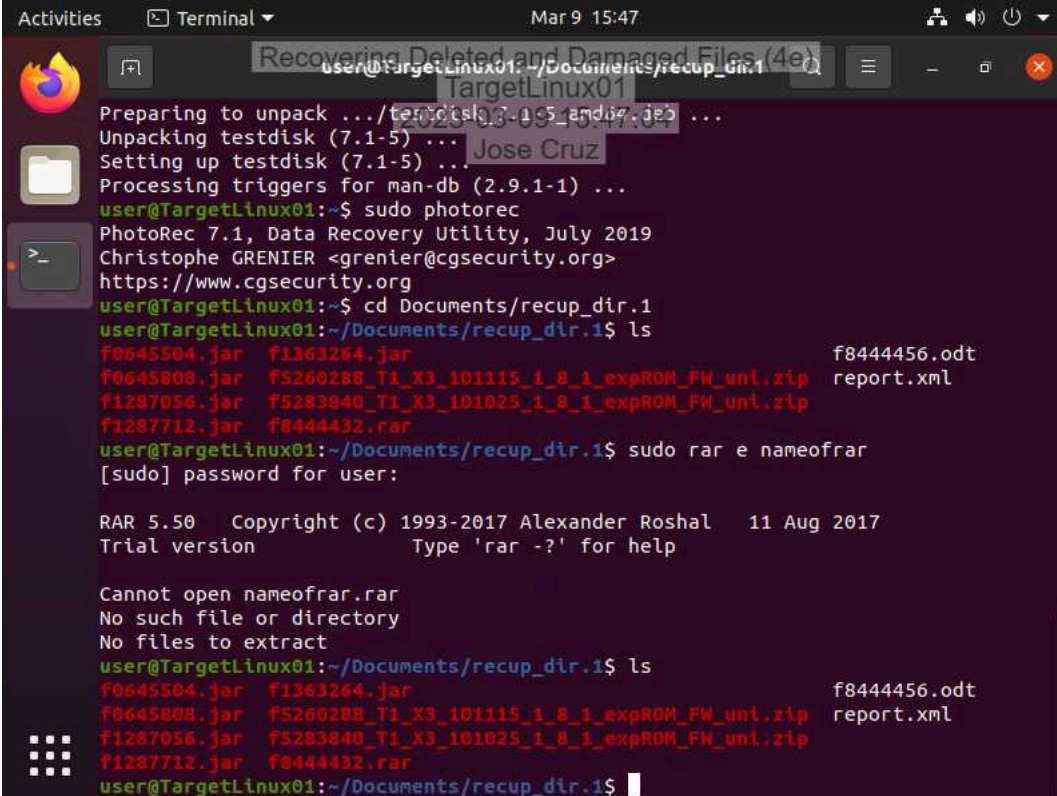
```
user@TargetLinux01:~/Documents/recup_dir.1$ sudo apt-get install testdisk
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  testdisk
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 362 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 (566 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.

A screenshot of a Linux terminal window titled "Recovering Deleted and Damaged Files (4e)". The terminal shows the user performing various recovery tasks. It starts with unpacking testdisk and setting up triggers. Then, the user runs 'sudo photorec', which displays version 7.1 and the author's information. Next, the user navigates to the 'Documents/recup\_dir.1' directory and lists the files, showing a list of .jar, .zip, and .rar files. Finally, the user attempts to create a RAR archive named 'nameofrar.rar' using 'sudo rar e', but it fails with an error message. The terminal output is as follows:

```
user@TargetLinux01:~/Documents/recup_dir.1$ ls
Preparing to unpack .../testdisk-7.1-1.tar.xz ...
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$ sudo rar e nameofrar
[sudo] password for user:

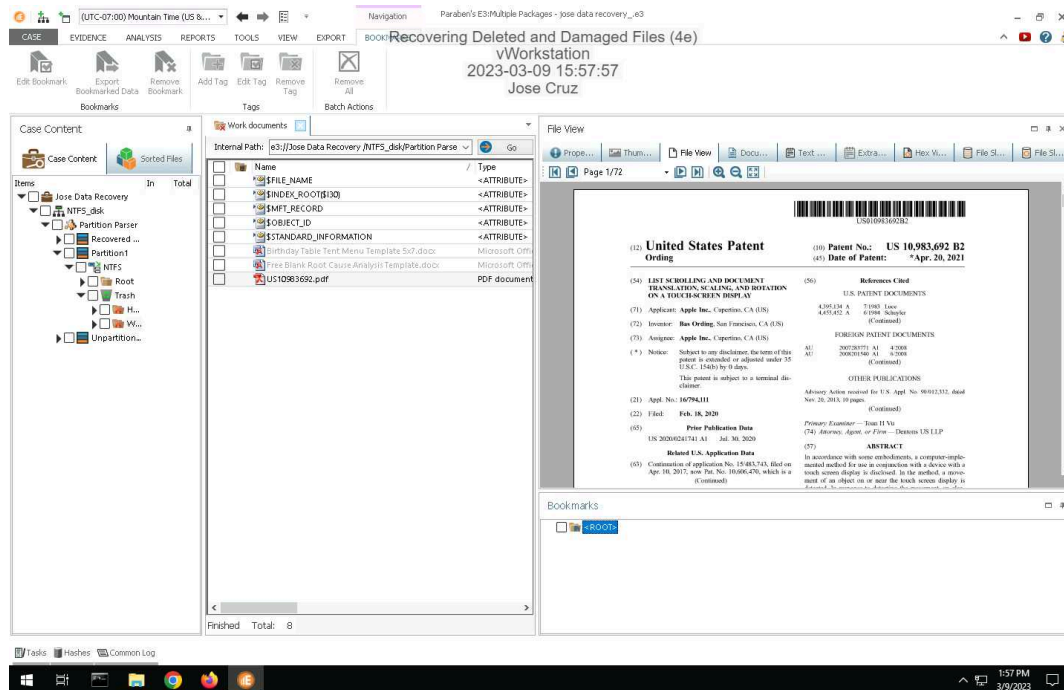
RAR 5.50 Copyright (c) 1993-2017 Alexander Roshal 11 Aug 2017
Trial version Type 'rar -?' for help

Cannot open nameofrar.rar
No such file or directory
No files to extract
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$
```

### 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.

