

Student:	Email:
Alexis Cherpes	cherpea@ferris.edu

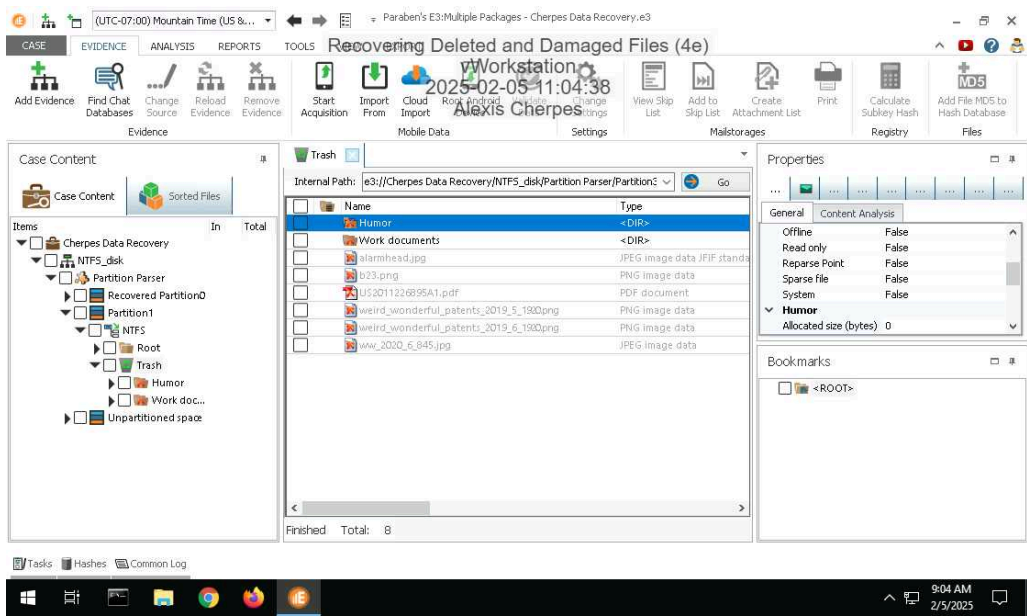
Time on Task:	Progress:
3 hours, 33 minutes	100%

Report Generated: Thursday, May 22, 2025 at 4:47 PM

Section 1: Hands-On Demonstration

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

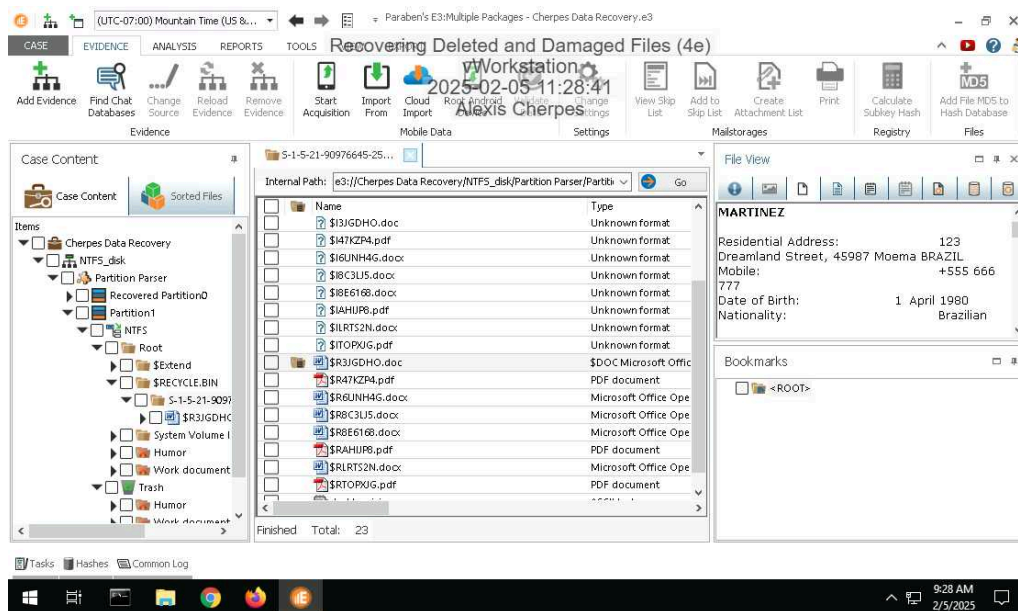
13. Make a screen capture showing the list of recovered files and folders in the E3 Trash folder.



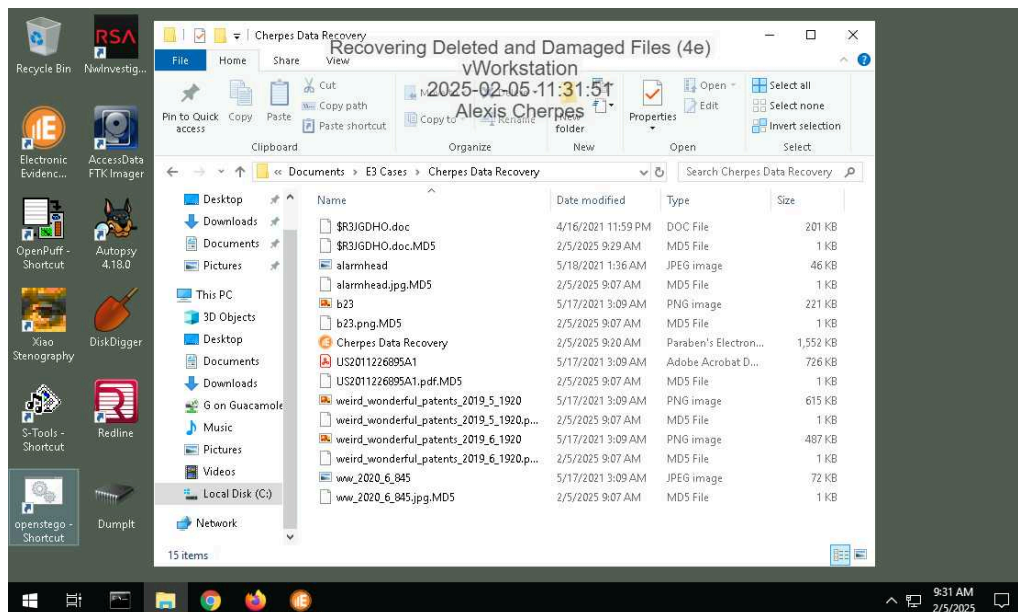
Recovering Deleted and Damaged Files (4e)

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.

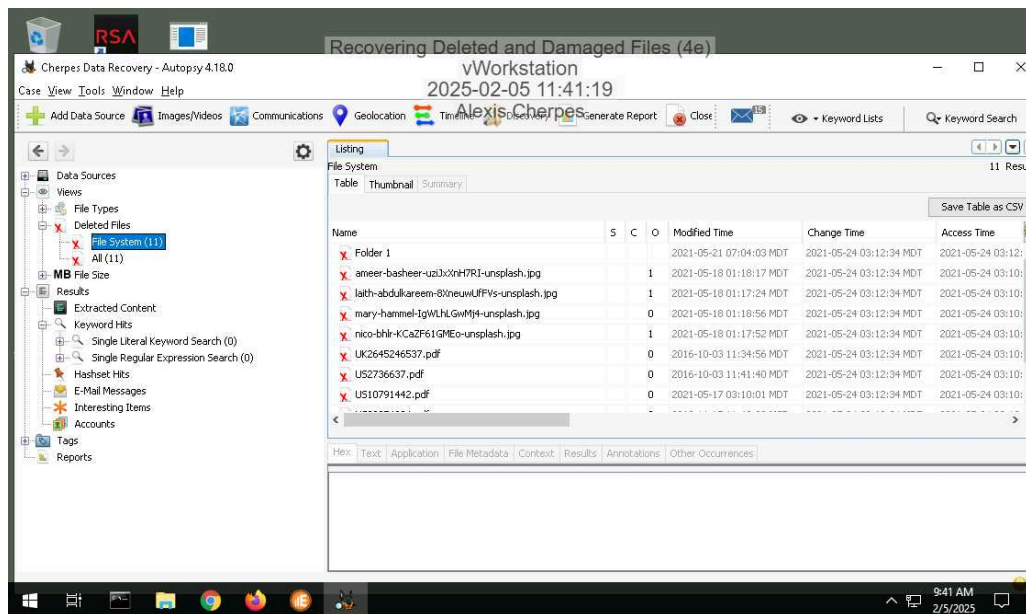


Part 2: Recover Deleted Files from an Ext4 Drive Image with Autopsy

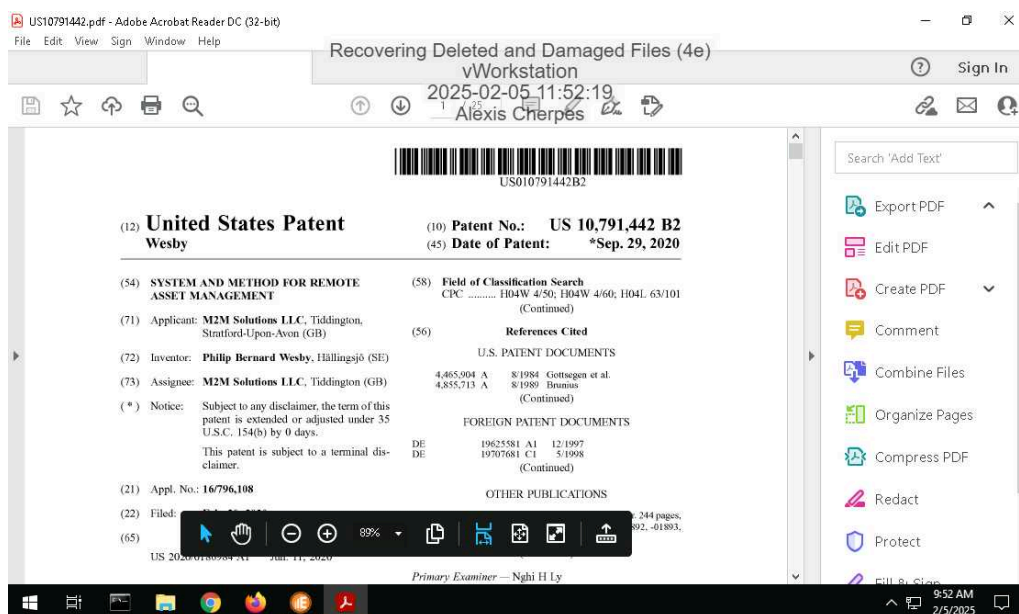
Recovering Deleted and Damaged Files (4e)

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.



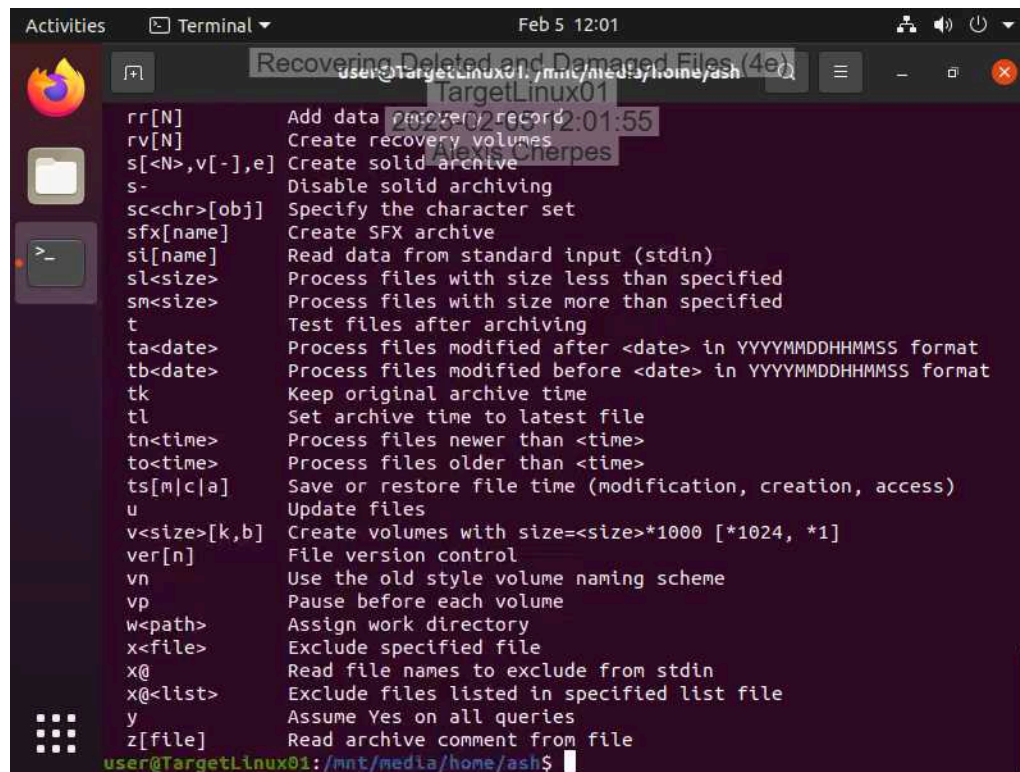
22. Make a screen capture showing the recovered patent file.



Section 2: Applied Learning

Part 1: Recover Deleted Files in Linux with PhotoRec

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 "Terminal" with the date and time "Feb 5 12:01". The user is logged in as "user@TargetLinux01" and is in the directory "/mnt/media/home/ash". The terminal displays the following command-line options for PhotoRec:

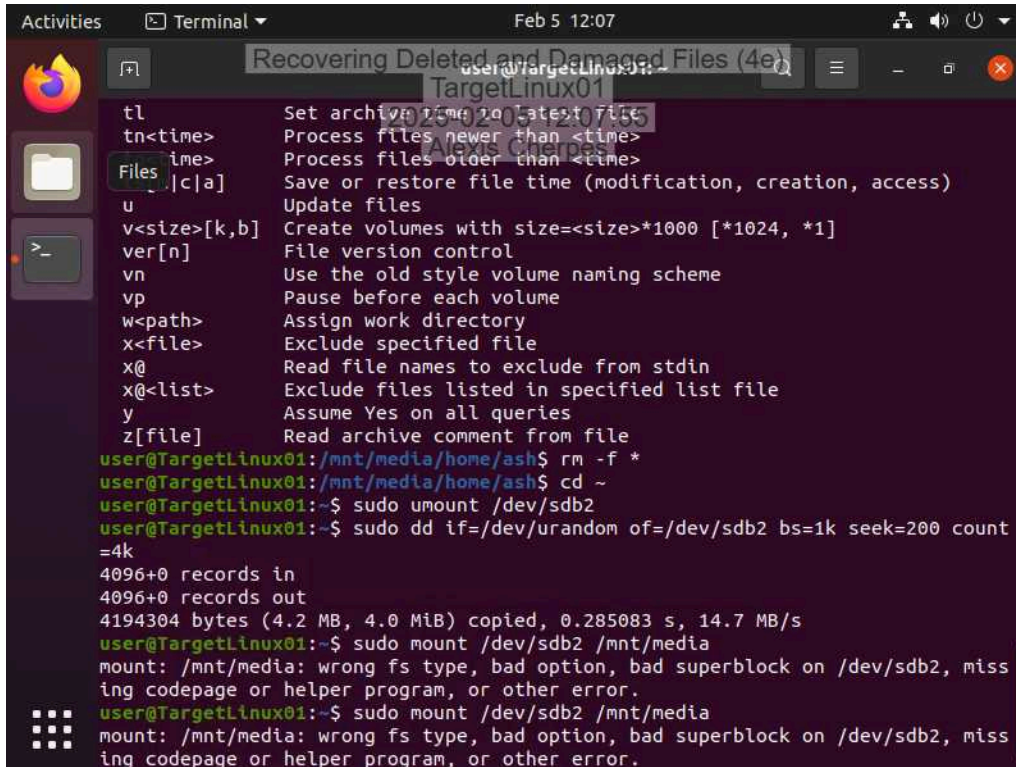
```
rr[N]      Add data recovery record
rv[N]      Create recovery volumes
s[<N>,v[-],e] Create solid archive
s-         Disable solid archiving
sc<chr>[obj] Specify the character set
sfx[name]  Create SFX archive
si[name]   Read data from standard input (stdin)
sl<size>   Process files with size less than specified
sm<size>   Process files with size more than specified
t          Test files after archiving
ta<date>   Process files modified after <date> in YYYYMMDDHHMMSS format
tb<date>   Process files modified before <date> in YYYYMMDDHHMMSS format
tk         Keep original archive time
tl         Set archive time to latest file
tn<time>   Process files newer than <time>
to<time>   Process files older than <time>
ts[m|c|a]  Save or restore file time (modification, creation, access)
u          Update files
v<size>[k,b] Create volumes with size=<size>*1000 [*1024, *1]
ver[n]     File version control
vn         Use the old style volume naming scheme
vp         Pause before each volume
w<path>    Assign work directory
x<file>    Exclude specified file
x@         Read file names to exclude from stdin
x@<list>   Exclude files listed in specified list file
y          Assume Yes on all queries
z[file]    Read archive comment from file
```

The prompt at the bottom is "user@TargetLinux01:/mnt/media/home/ash\$".

Recovering Deleted and Damaged Files (4e)

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

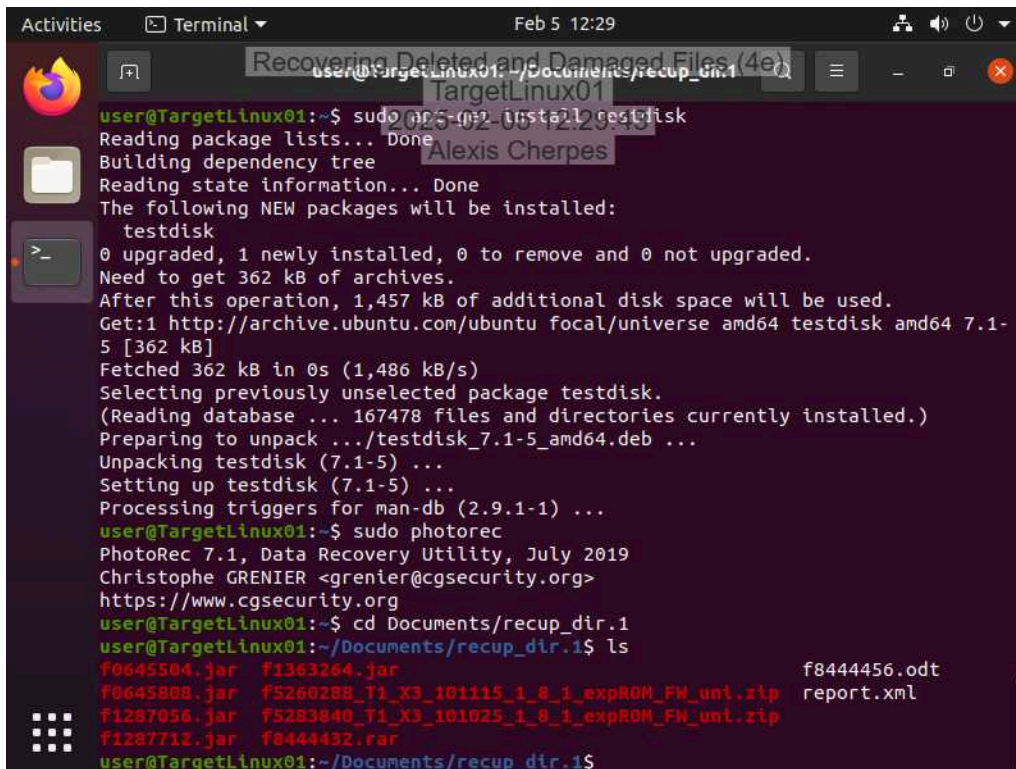
15. Make a screen capture showing the failed mount attempt on the /dev/sdb2 device.

A terminal window titled "Recovering Deleted and Damaged Files (4e)" on a system named "TargetLinux01". The terminal shows a list of ddrescue options (tl, tn, time, [c]a, u, v, ver, vn, vp, w, x, x@, x@<list>, y, z) and their descriptions. The user then runs a series of commands: 'rm -f *', 'cd ~', 'sudo umount /dev/sdb2', 'sudo dd if=/dev/urandom of=/dev/sdb2 bs=1k seek=200 count=4k', and 'sudo mount /dev/sdb2 /mnt/media'. The final two mount attempts fail with the error: "mount: /mnt/media: wrong fs type, bad option, bad superblock on /dev/sdb2, missing codepage or helper program, or other error."

```
Activities Terminal Feb 5 12:07
Recovering Deleted and Damaged Files (4e)
TargetLinux01
tl          Set archive time to latest file
tn<time>    Process files newer than <time>
time>       Process files older than <time>
[c]a        Save or restore file time (modification, creation, access)
u           Update files
v<size>[k,b] Create volumes with size=<size>*1000 [*1024, *1]
ver[n]      File version control
vn          Use the old style volume naming scheme
vp          Pause before each volume
w<path>     Assign work directory
x<file>     Exclude specified file
x@          Read file names to exclude from stdin
x@<list>    Exclude files listed in specified list file
y           Assume Yes on all queries
z[file]     Read archive comment from file

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, 0.285083 s, 14.7 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:~$ 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.
```

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

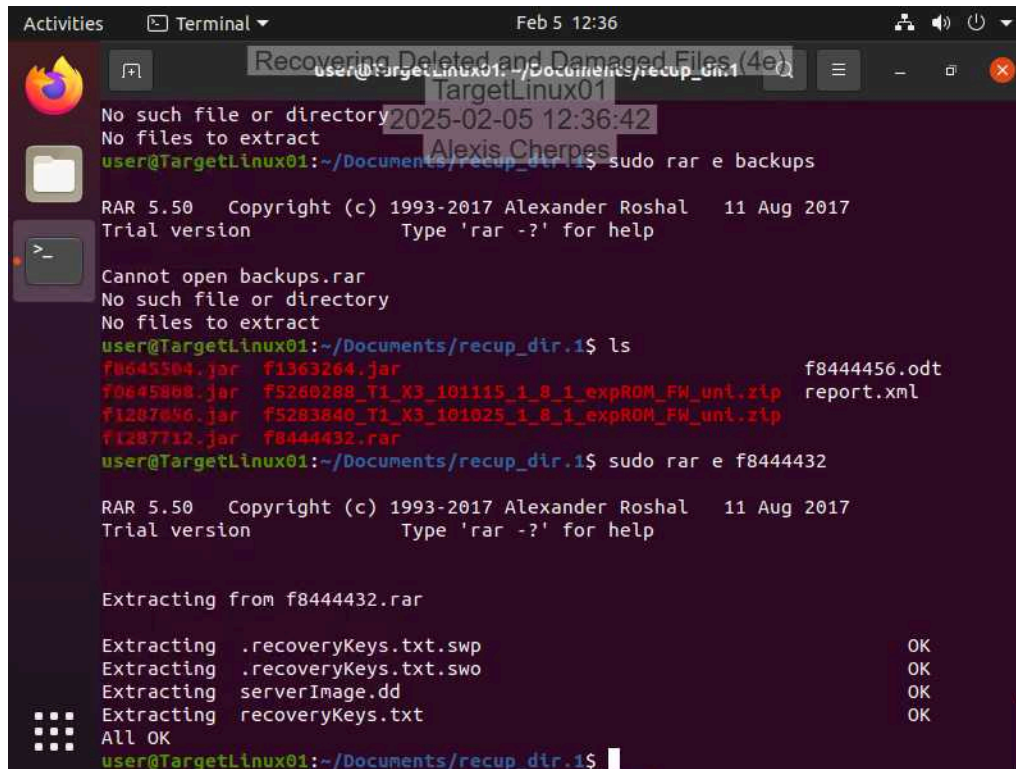
A terminal window titled "Recovering Deleted and Damaged Files (4e)" on a system named "TargetLinux01". The user runs 'sudo apt install testdisk', which shows the installation progress for 'testdisk'. Then, the user runs 'sudo photorec', which displays the PhotoRec version (7.1) and the user's name (Christophe GRENIER). Finally, the user runs 'cd Documents/recup_dir.1' and 'ls', which lists the recovered files: 'f0645504.jar', 'f1363264.jar', 'f8444456.odt', 'f0645808.jar', 'f5260288_T1_X3_101115_1_8_1_expROM_FW_unl.zip', 'report.xml', 'f1287056.jar', 'f5283840_T1_X3_101025_1_8_1_expROM_FW_unl.zip', 'f1287712.jar', and 'f0444432.rar'.

```
Activities Terminal Feb 5 12:29
Recovering Deleted and Damaged Files (4e)
TargetLinux01
user@TargetLinux01:~$ sudo apt 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 0s (1,486 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_unl.zip  report.xml
f1287056.jar  f5283840_T1_X3_101025_1_8_1_expROM_FW_unl.zip
f1287712.jar  f0444432.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 terminal window titled 'Recovering Deleted and Damaged Files (4e)' on a system named 'TargetLinux01'. The user is in the directory ~/Documents/recup_dir.1. The terminal shows the execution of 'sudo rar e backups', which fails with 'Cannot open backups.rar'. Then, 'ls' is run, listing several files including f8444432.rar. Finally, 'sudo rar e f8444432' is executed, successfully extracting files: .recoveryKeys.txt.swp, .recoveryKeys.txt.swo, serverImage.dd, and recoveryKeys.txt. The terminal output is as follows:

```
user@TargetLinux01:~/Documents/recup_dir.1$ sudo rar e backups
RAR 5.50 Copyright (c) 1993-2017 Alexander Roshal 11 Aug 2017
Trial version Type 'rar -?' for help

Cannot open backups.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_unl.zip report.xml
f1287046.jar f5283840_T1_X3_101025_1_8_1_expROM_FW_unl.zip
f1287712.jar f8444432.rar
user@TargetLinux01:~/Documents/recup_dir.1$ sudo rar e f8444432

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

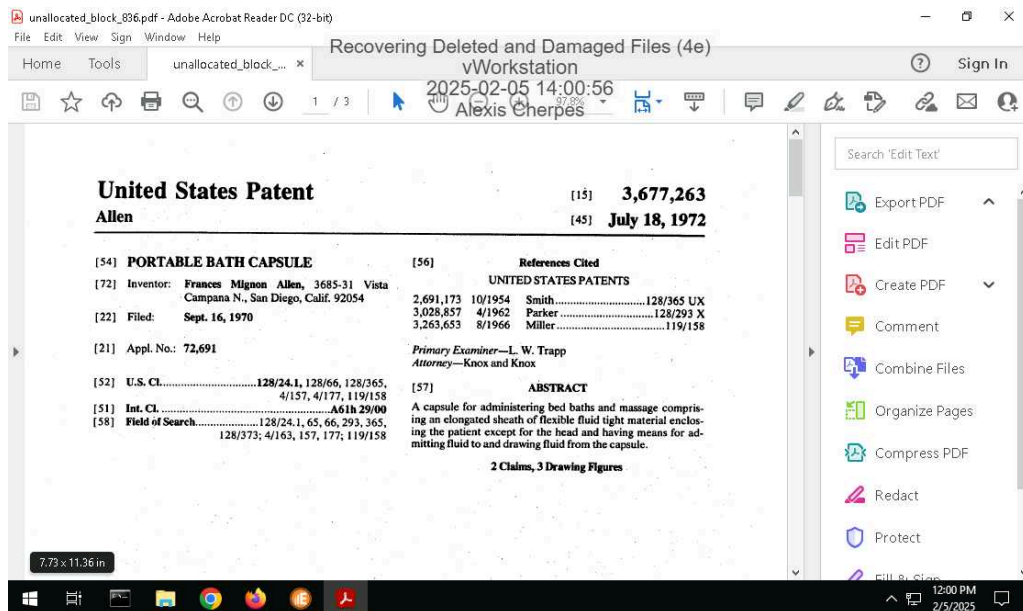
Extracting from f8444432.rar

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$
```

Section 3: Challenge and Analysis

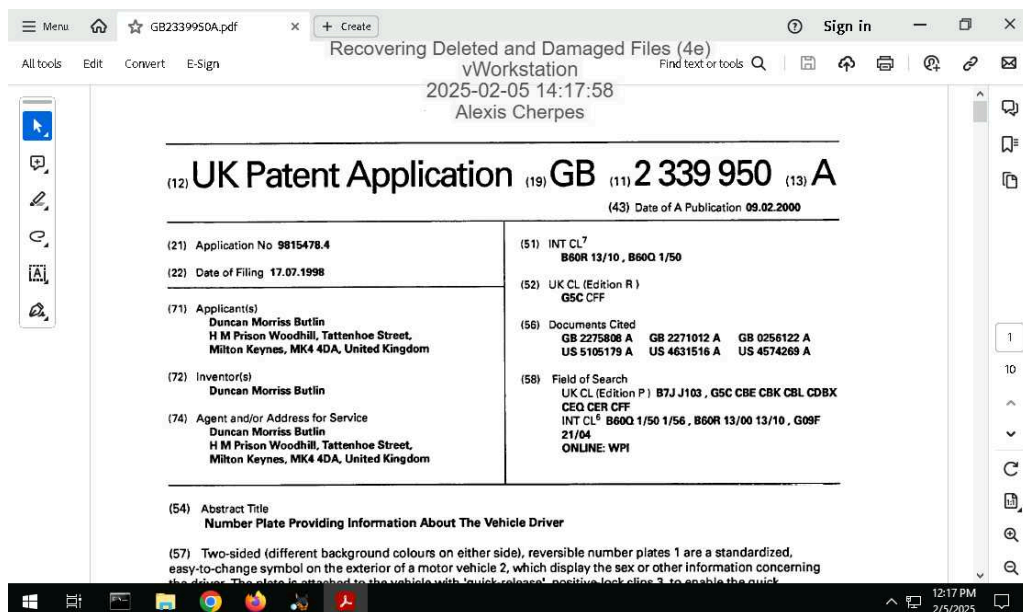
Part 1: Recover Deleted Files from a FAT Drive Image

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



Part 2: Recover Deleted Files from an APFS Drive Image

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



Recovering Deleted and Damaged Files (4e)

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