

Student: Jordan Calvert

Email: jordanryancalvert@gmail.com

Time on Task: 5 hours, 49 minutes

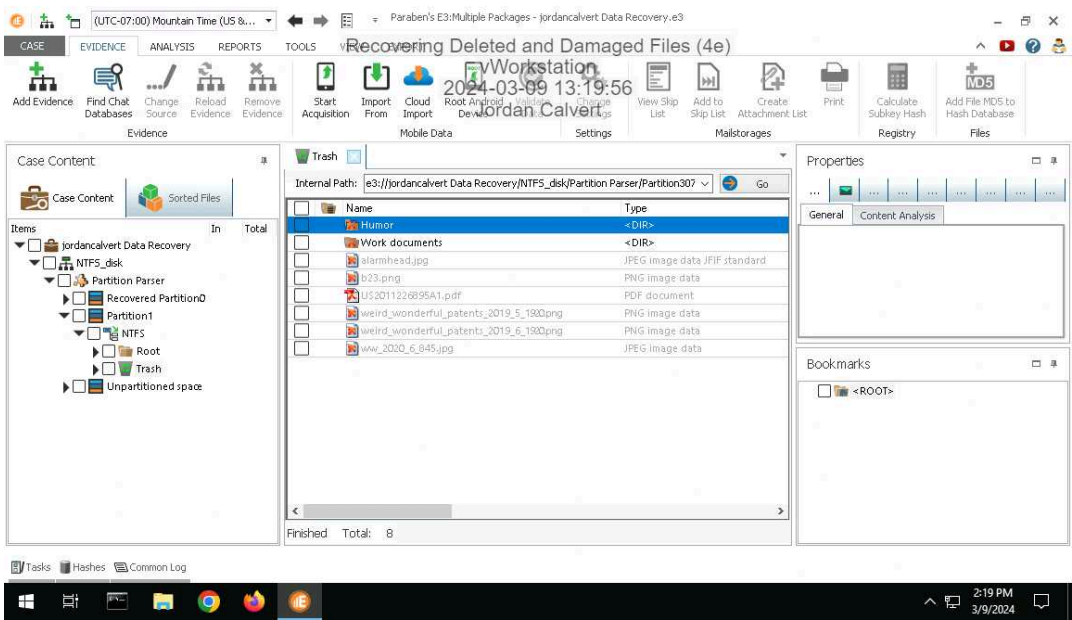
Progress: 100%

Report Generated: Wednesday, May 15, 2024 at 10:44 AM

Section 1: Hands-On Demonstration

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

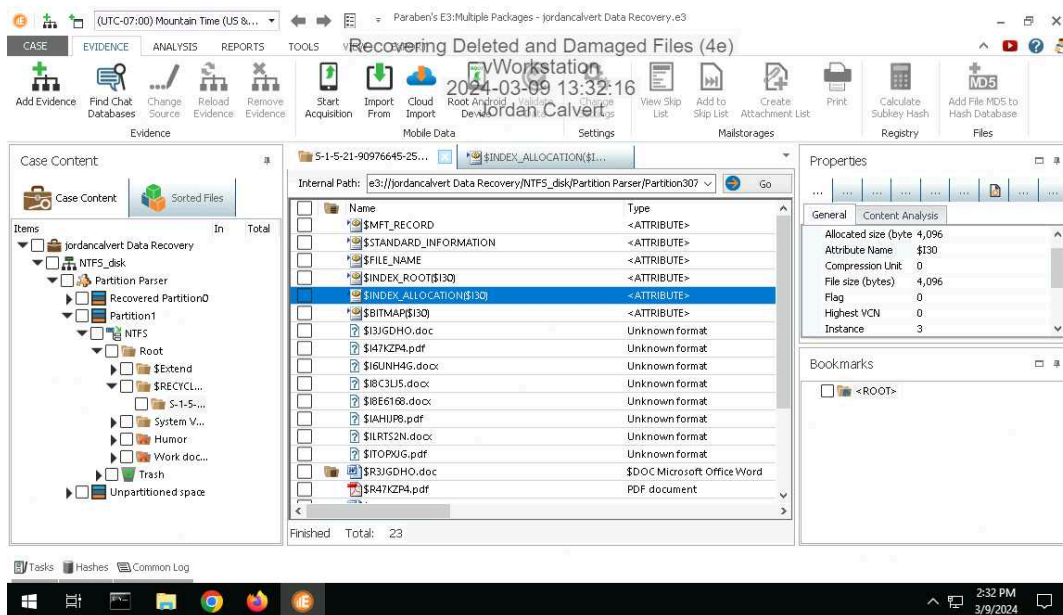
13. Make a screen capture showing the list of recovered files and folders in the E3 Trash folder.



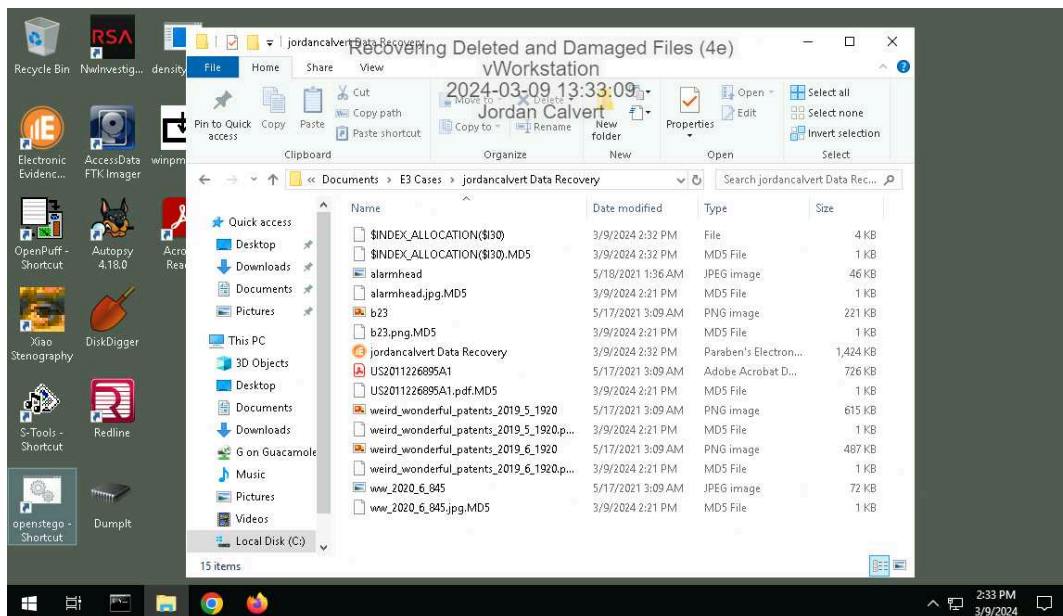
Recovering Deleted and Damaged Files (4e)

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.

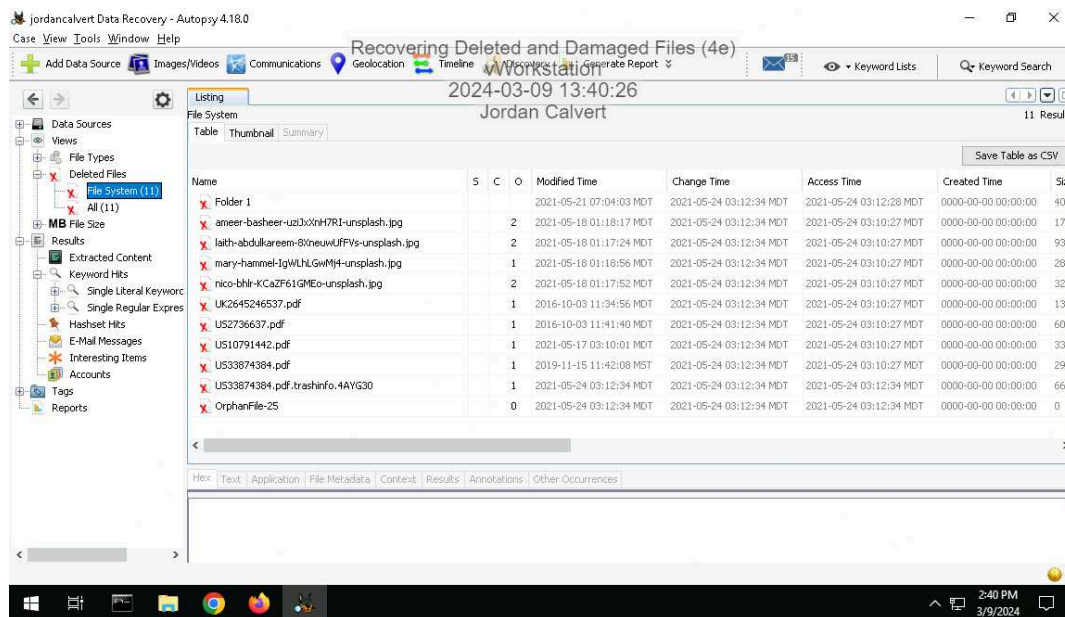


Part 2: Recover Deleted Files from an Ext4 Drive Image with Autopsy

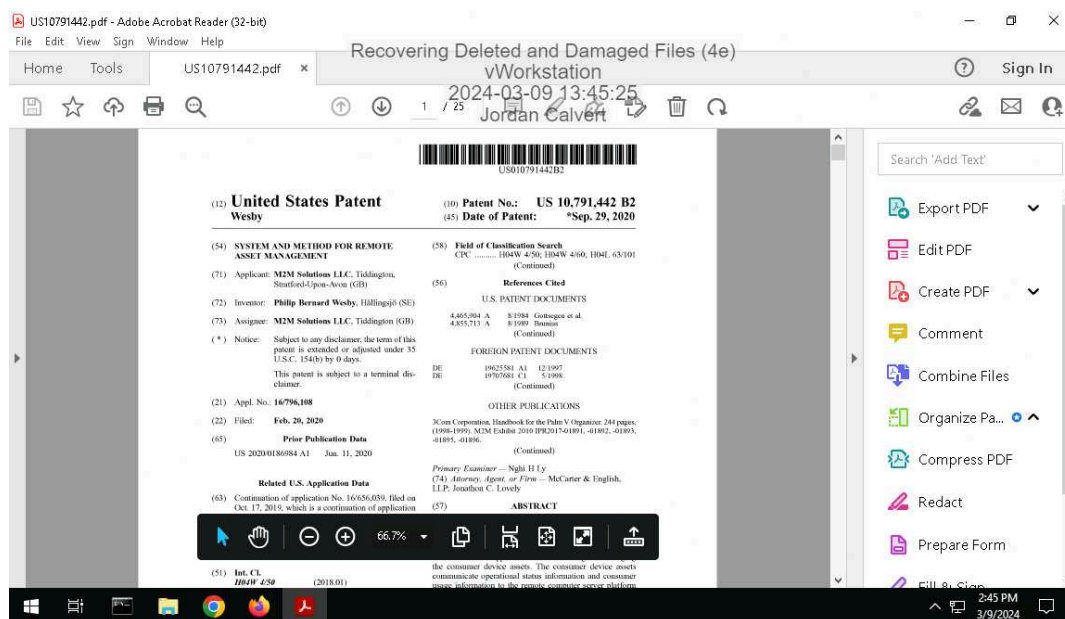
Recovering Deleted and Damaged Files (4e)

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.



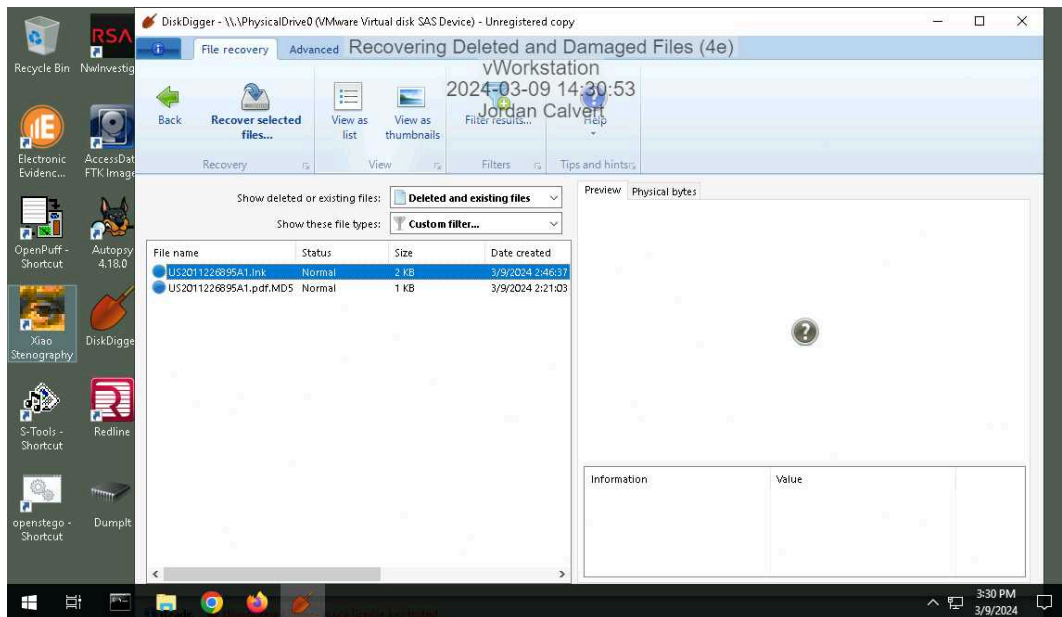
22. Make a screen capture showing the recovered patent file.



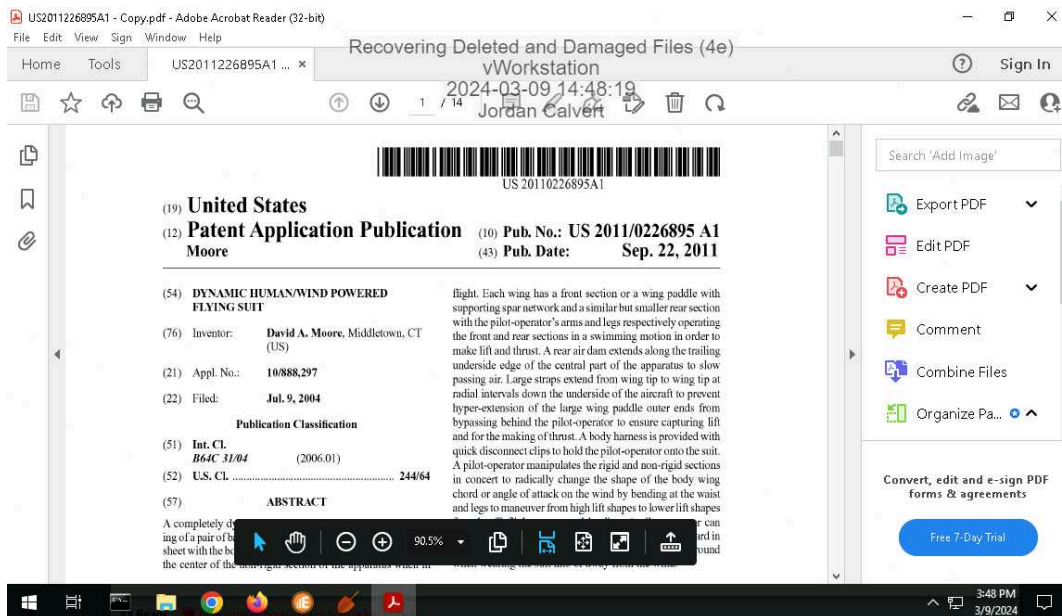
Section 2: Applied Learning

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.

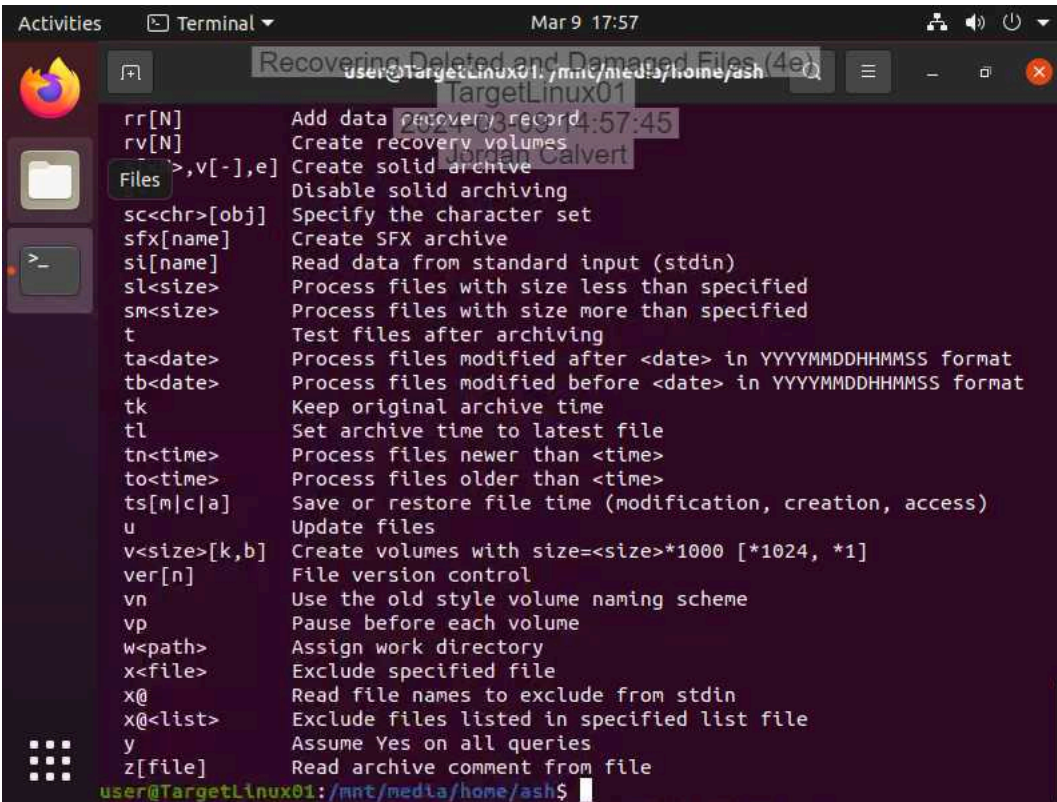


Part 2: Recover Deleted Files in Linux with PhotoRec

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**.



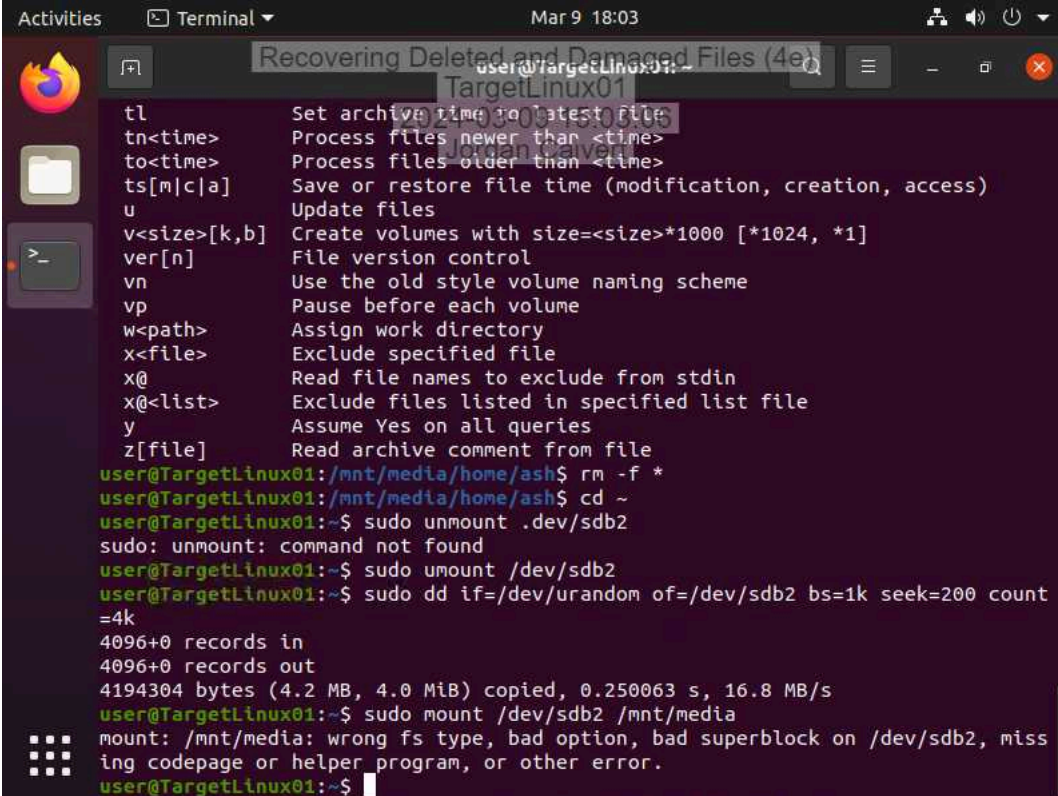
The screenshot shows a Linux terminal window titled "Recovering Deleted and Damaged Files (4e)". The terminal displays the contents of a RAR archive, listing various commands and their descriptions. The commands are listed in two columns, with the first column containing the command name and the second column containing the description. The commands are: rr[N], rv[N], >,v[-],e, sc<chr>[obj], sfx[name], si[name], sl<size>, sm<size>, t, ta<date>, tb<date>, tk, tl, tn<time>, to<time>, ts[m|c|a], u, v<size>[k,b], ver[n], vn, vp, w<path>, x<file>, x@, x@<list>, y, and z[file]. The terminal prompt is user@TargetLinux01:/mnt/media/home/ash\$.

```
rr[N]      Add data recovery record
rv[N]      Create recovery volumes
>,v[-],e  Create solid archive
          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
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)" showing a series of commands and their outputs. The user is on a system named "TargetLinux01". The commands and outputs are as follows:

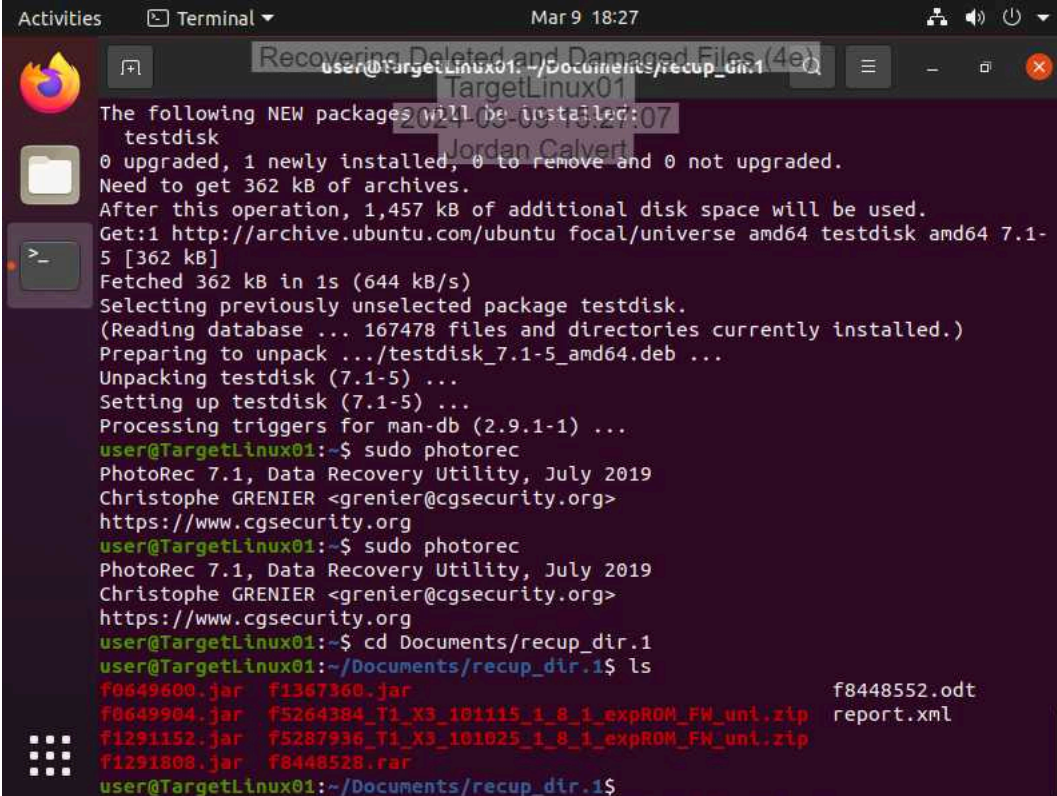
```
tl          Set archive time to latest file
tn<time>    Process files newer than <time>
to<time>    Process files older than <time>
ts[m|c|a]   Save or restore file time (modification, creation, access)
u           Update files
v<size>[k,b] Create volumes with size=<size>*1000 [*1024, *1]
ver[n]      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

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 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, 0.250063 s, 16.8 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.

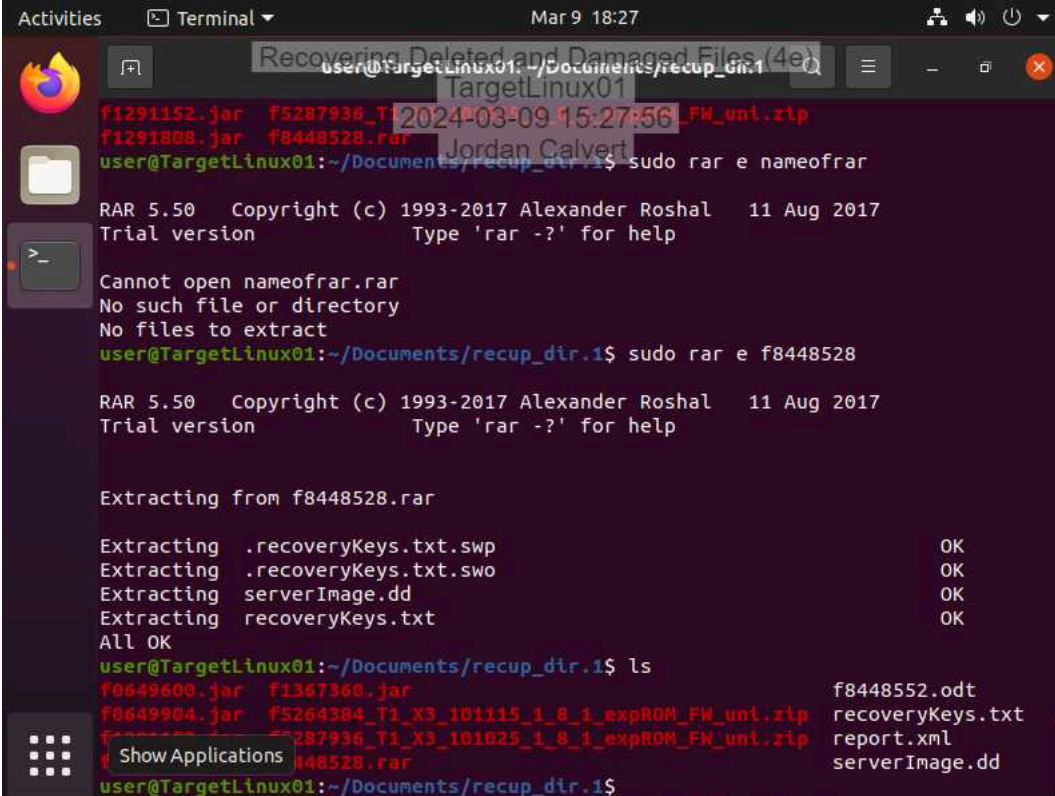


```
user@TargetLinux01: ~/Documents/recup_dir.1
The following NEW packages will be installed:
testdisk
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 362 kB of archives.
After this operation, 1,457 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal/universe amd64 testdisk amd64 7.1-5 [362 kB]
Fetched 362 kB in 1s (644 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:~$ 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
f0649600.jar  f1367360.jar  f8448552.odt
f0649904.jar  f5264384_T1_X3_101115_1_8_1_expROM_FW_uni.zip  report.xml
f1291152.jar  f5287936_T1_X3_101025_1_8_1_expROM_FW_uni.zip
f1291808.jar  f8448528.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)" with a search bar containing "TargetLinux01". The terminal shows a user at "TargetLinux01" in the directory "/Documents/recup_dir.1". The user lists files: f1291152.jar, f5287938_T1_X3_101025_1_8_1_expROM_FW_uni.zip, f1291808.jar, and f8448528.rar. They attempt to extract "nameofrar" with "sudo rar e nameofrar", which fails. Then they extract "f8448528" with "sudo rar e f8448528", which succeeds, showing a list of extracted files: .recoveryKeys.txt.swp, .recoveryKeys.txt.swo, serverImage.dd, and recoveryKeys.txt. Finally, they run "ls" showing a list of files including f0649600.jar, f1367360.jar, f0649904.jar, f5264384_T1_X3_101115_1_8_1_expROM_FW_uni.zip, f287938_T1_X3_101025_1_8_1_expROM_FW_uni.zip, f8448528.rar, f844852.odt, recoveryKeys.txt, report.xml, and serverImage.dd.

```
user@TargetLinux01:~/Documents/recup_dir.1$ ls
f1291152.jar  f5287938_T1_X3_101025_1_8_1_expROM_FW_uni.zip
f1291808.jar  f8448528.rar
user@TargetLinux01:~/Documents/recup_dir.1$ sudo rar e nameofrar
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$ sudo rar e f8448528
RAR 5.50   Copyright (c) 1993-2017 Alexander Roshal   11 Aug 2017
Trial version                               Type 'rar -?' for help

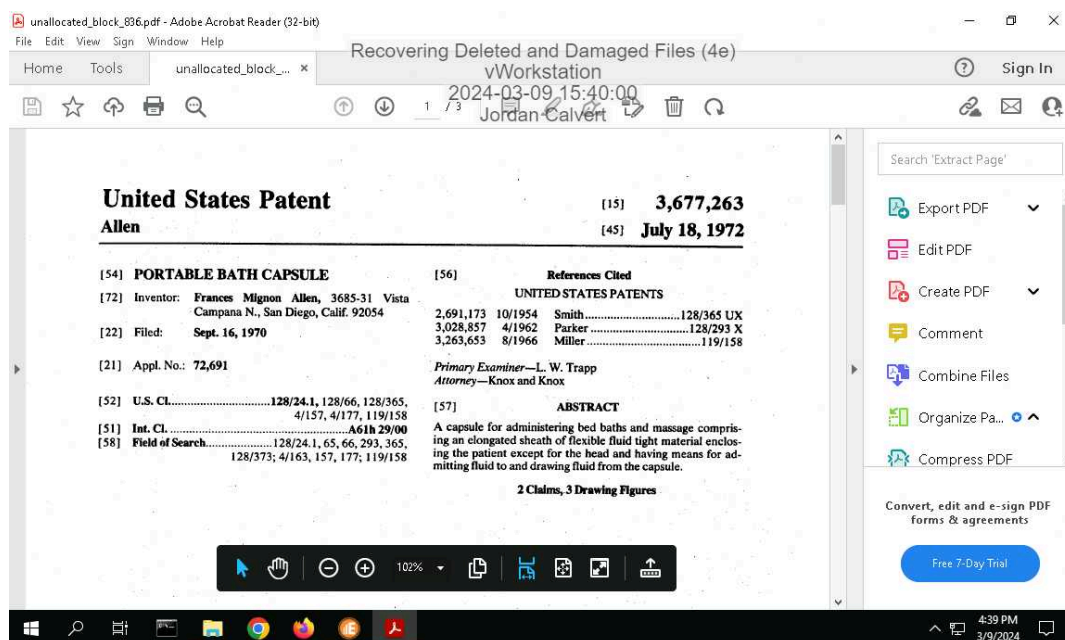
Extracting from f8448528.rar

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
f0649600.jar  f1367360.jar                                f844852.odt
f0649904.jar  f5264384_T1_X3_101115_1_8_1_expROM_FW_uni.zip  recoveryKeys.txt
f287938_T1_X3_101025_1_8_1_expROM_FW_uni.zip  report.xml
f8448528.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.

