

Recovering Deleted and Damaged Files (4e)

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

Student:

Jose Cruz

Email:

jose.cruz2@udc.edu

Time on Task:

14 hours, 14 minutes

Progress:

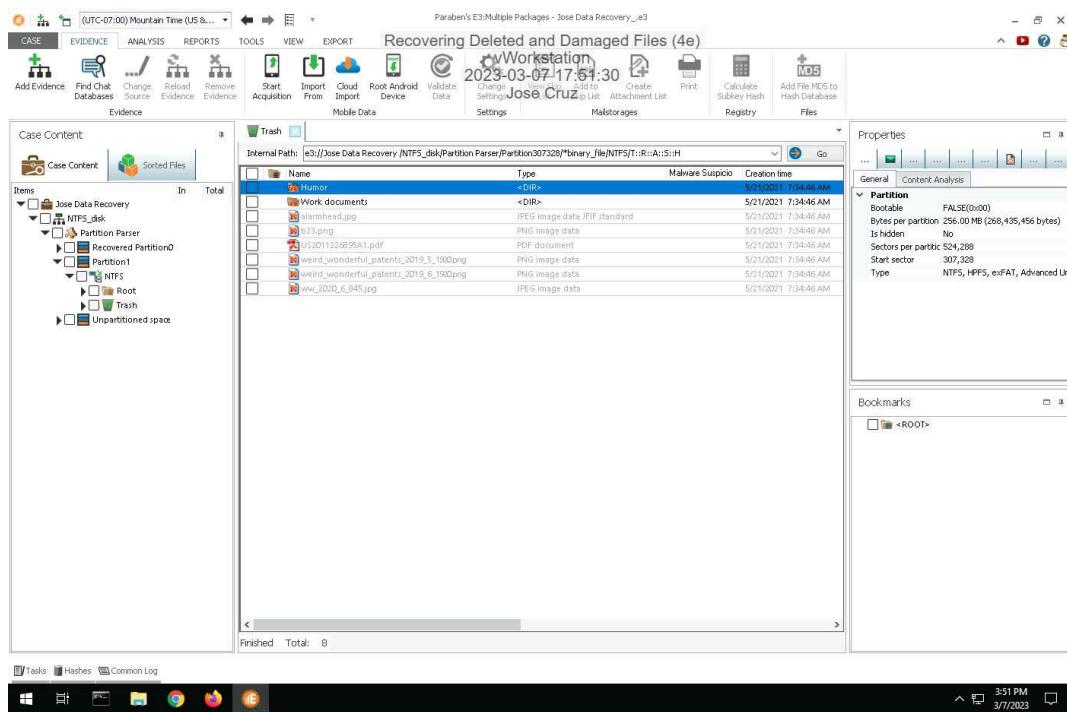
100%

Report Generated: Thursday, March 9, 2023 at 4:07 PM

Section 1: Hands-On Demonstration

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

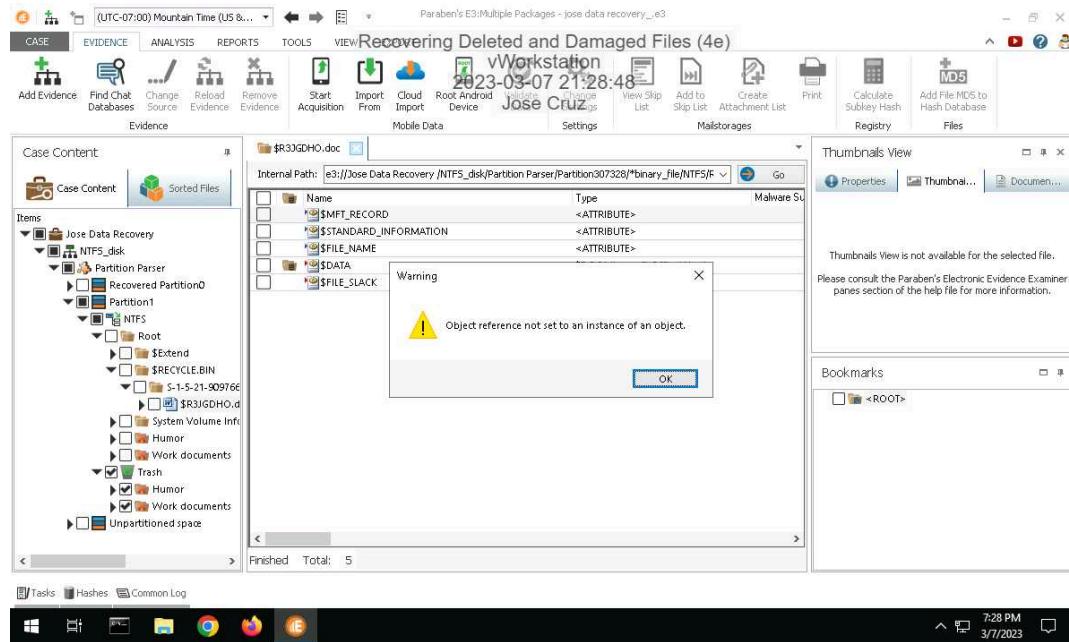
13. Make a screen capture showing the list of recovered files and folders in the E3 Trash folder.



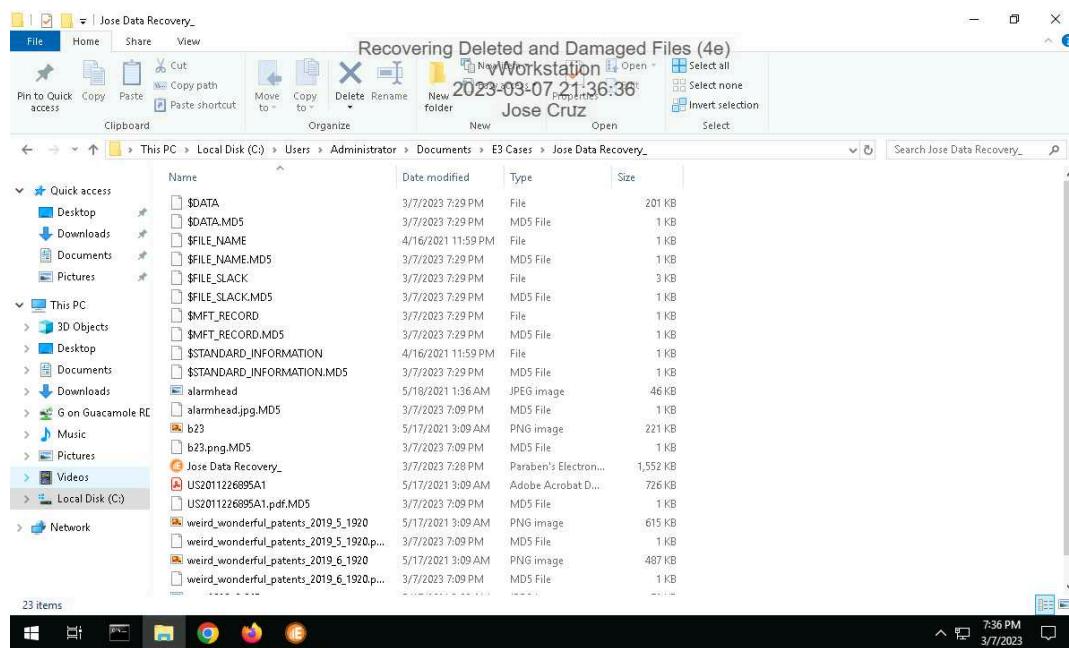
Recovering Deleted and Damaged Files (4e)

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.

The screenshot shows the Autopsy 4.18.0 interface with the title bar "Recovering Deleted and Damaged Files (4e)". The main window displays a table of recovered files under the "File System" tab. The table columns include Name, S, C, O, Modified Time, Change Time, Access Time, and Created Time. One file, "lath-abdullahreem-0x0newi#FVs-unplash.jpg", is highlighted in blue. The bottom right corner of the interface shows a small thumbnail preview of the image file.

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

The screenshot shows a patent document titled "United States Patent" for "SYSTEM AND METHOD FOR REMOTE ASSET MANAGEMENT". The patent number is US 10,791,442 B2, and the date of patent is *Sep. 29, 2020. The document includes sections for "FIELD OF CLASSIFICATION SEARCH", "REFERENCES CITED", and "FOREIGN PATENT DOCUMENTS". The right side of the interface features a toolbar with various PDF manipulation options like "Export PDF", "Edit PDF", and "Create PDF". The bottom status bar shows the file path "US10791442.pdf" and the date "3/7/2023".

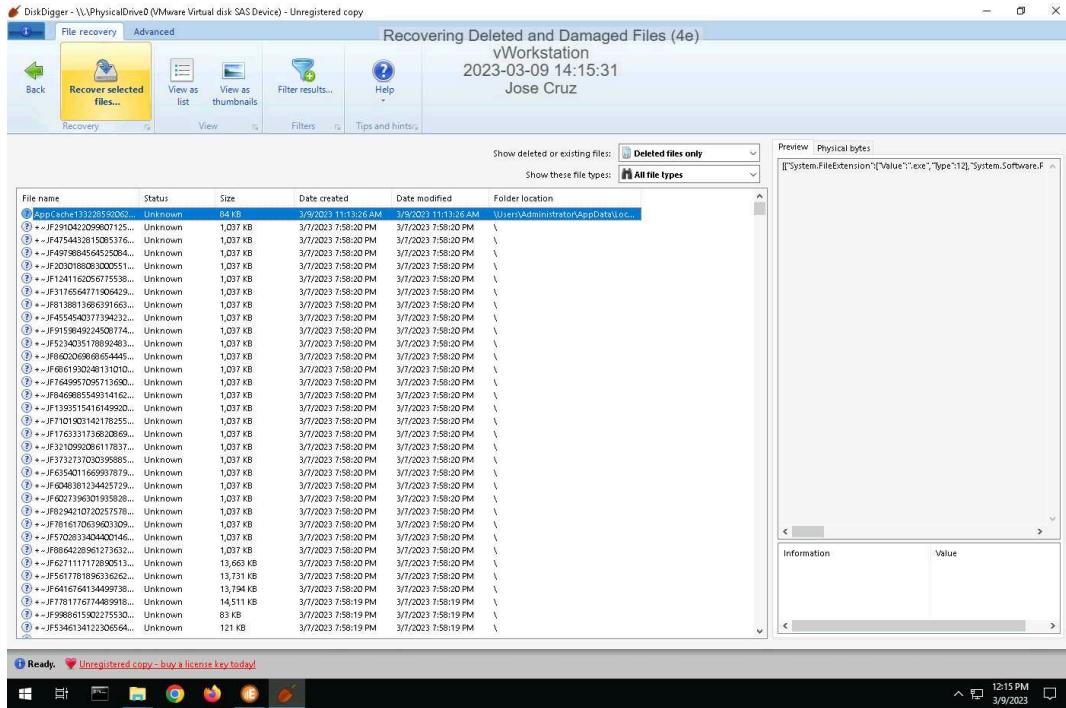
Recovering Deleted and Damaged Files (4e)

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

Section 2: Applied Learning

Part 1: Recover Deleted Files in Windows with DiskDigger

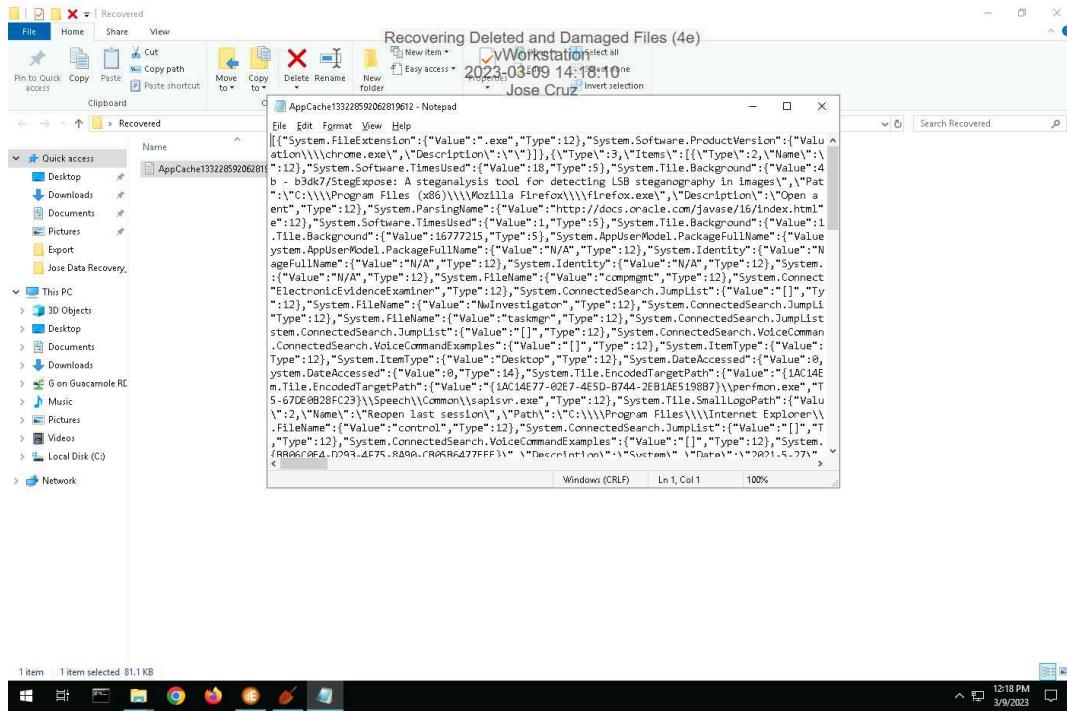
9. Make a screen capture showing the deleted patent file in DiskDigger.



Recovering Deleted and Damaged Files (4e)

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

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

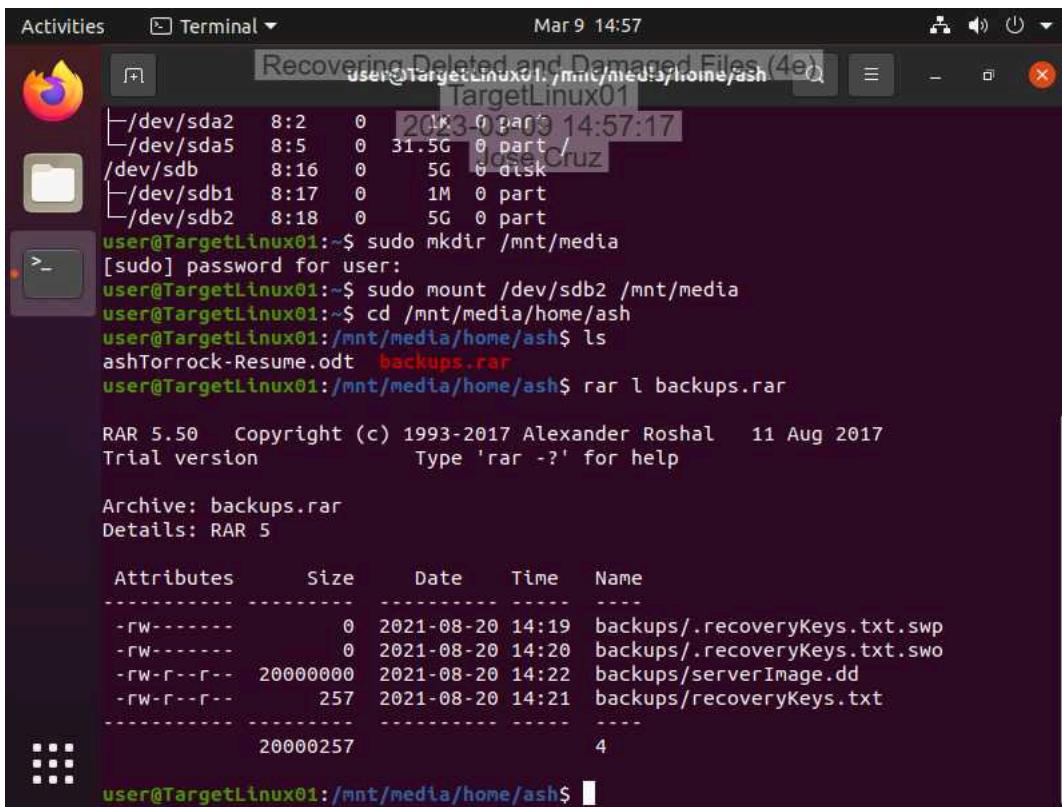


Part 2: Recover Deleted Files in Linux with PhotoRec

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)" running on a "TargetLinux01" system. The terminal displays the following command sequence and output:

```
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
```

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)" running on a "TargetLinux01" system. The user has extracted a RAR archive named "backups.rar" and listed its contents. The terminal then shows commands being run to clean up the media directory and attempt to mount the device /dev/sdb2. The final command, "sudo mount /dev/sdb2 /mnt/media", fails with the message "mount: /mnt/media: wrong fs type, bad option, bad superblock on /dev/sdb2, missing codepage or helper program, or other error."

```
Activities Terminal Mar 9 15:06
Recovering Deleted and Damaged Files (4e) user@TargetLinux01
TargetLinux01
user@TargetLinux01:/mnt/media$ ls
backups.rar
user@TargetLinux01:/mnt/media$ 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, 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.

The screenshot shows a terminal window on a TargetLinux01 system. The user runs the command `sudo apt-get install testdisk`, which installs the `testdisk` package. Afterward, the user runs `sudo photorec`, which performs a data recovery operation. Finally, the user lists the contents of the directory `recup_dir.1` using `ls`, showing several recovered files including `f0645504.jar`, `f1363264.jar`, `f0645808.jar`, `f5260288_T1_X3_101115_1_8_1_expoDM_FW_unt.zip`, `f1287056.jar`, `f5283840_T1_X3_101025_1_8_1_expoDM_FW_unt.zip`, `f1287712.jar`, `f8444452.rar`, and `f8444456.odt`.

```
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 (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_expoDM_FW_unt.zip report.xml
f1287056.jar  f5283840_T1_X3_101025_1_8_1_expoDM_FW_unt.zip
f1287712.jar  f8444452.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 desktop environment. The title bar reads "Recovering Deleted and Damaged Files (4e)". The terminal output is as follows:

```
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_expRDM_FW_uni.zip report.xml
f1287056.jar f5283840_T1_X3_101025_1_8_1_expRDM_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_expRDM_FW_uni.zip report.xml
f1287056.jar f5283840_T1_X3_101025_1_8_1_expRDM_FW_uni.zip
f1287712.jar f8444432.rar
user@TargetLinux01:~/Documents/recup_dir.1$
```

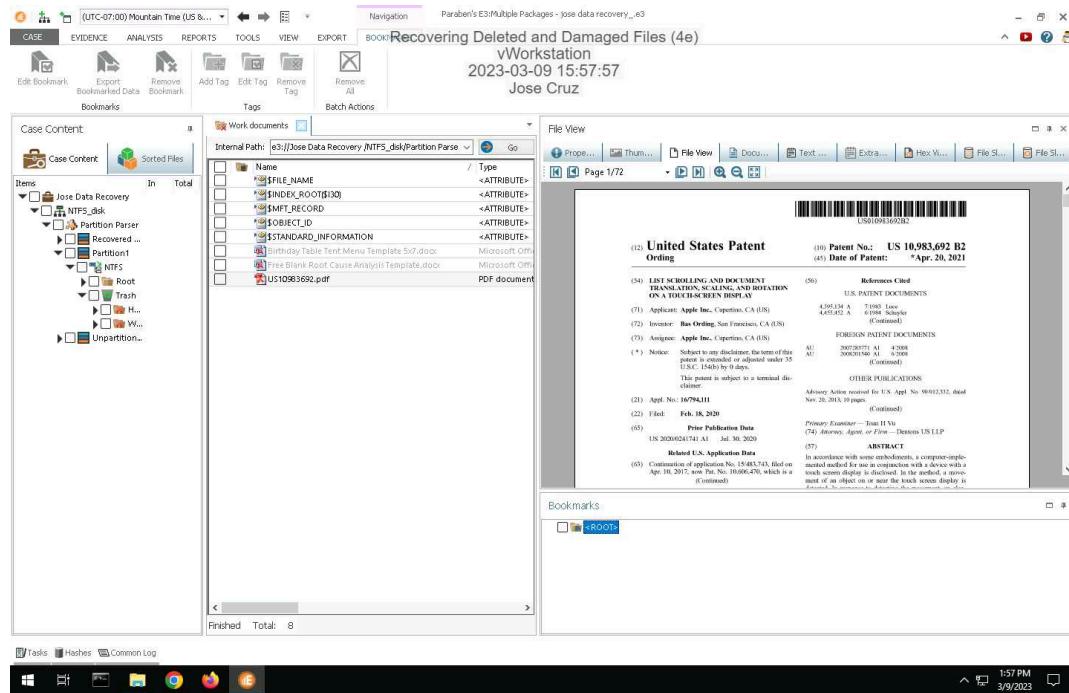
Recovering Deleted and Damaged Files (4e)

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

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.

The screenshot shows the Jose Data Recovery - Autopsy 4.18.0 interface. The main window displays a table titled "Recovering Deleted and Damaged Files (4e)" with 15 results. The table columns include Name, S, C, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and MD5 Hash. The table lists various files and folders, including ".Trash-0", ".Trash-1", and several image files like "anne-bagheri-up20x17Pv-unplash.jpg". Below the table is a detailed view of a patent document for "SYSTEM AND METHOD FOR REMOTE ASSET MANAGEMENT" (US 10,791,442 B2). The patent details the inventor (Philip Bernard Weller), the assignee (VTP Solutions LLC), and the filing date (Sep. 29, 2020). It includes figures, tables, and a summary of the invention.