

# Recovering Deleted and Damaged Files (4e)

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

Student:  
Samman Chouhan

Email:  
schouhan1@hawk.iit.edu

Time on Task:  
2 hours, 2 minutes

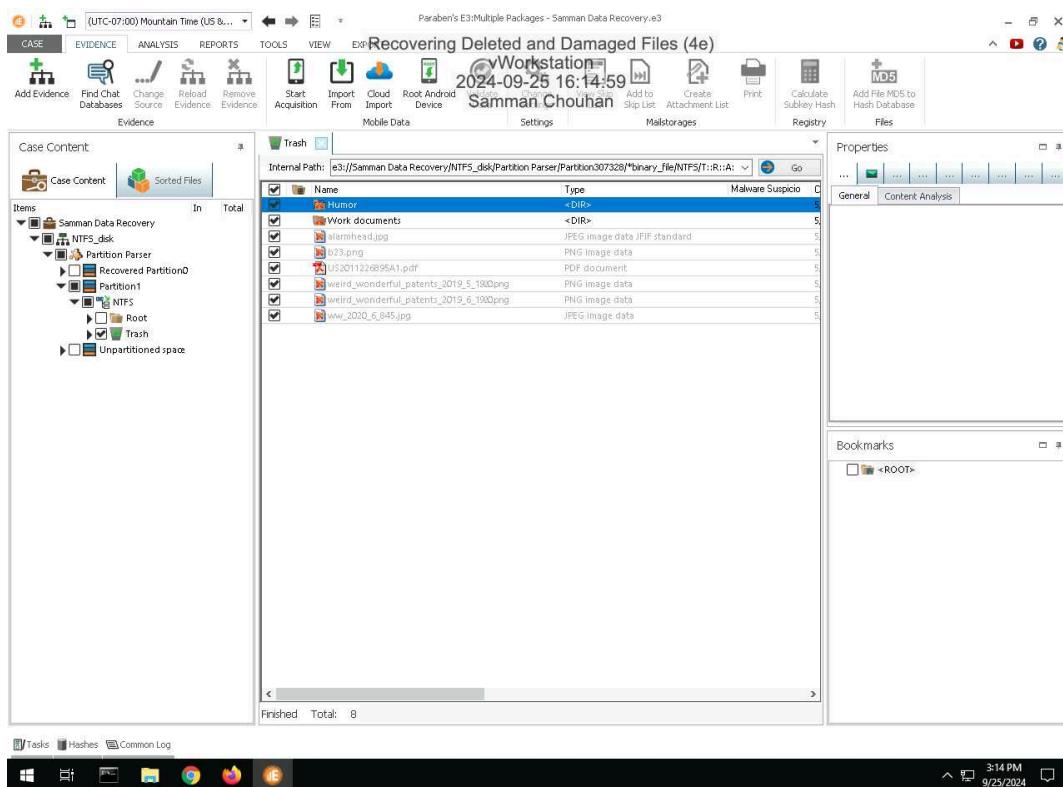
Progress:  
100%

Report Generated: Wednesday, September 25, 2024 at 7:09 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.

The screenshot displays the Paraben's E3 Multiple Packages - Samman Data Recovery software interface. The main window is titled "Recovering Deleted and Damaged Files (4e)". The interface is divided into several panes:

- Case Content:** Shows a tree view of the recovered files. The "NTFS\_disk" is expanded, showing "Partition Parser", "Recovered Partition0", "Partition1", and "NTFS". The "NTFS" folder is further expanded, showing "Root", "\$Extend", "\$RECYCL...", "System V...", "Humor", "Work doc...", "Trash", and "Unpartitioned space".
- Internal Path:** Shows the path "e3://Samman Data Recovery/NTFS\_disk/Partition Par...".
- File List:** A table listing recovered files. The file "\$RAHUR8.pdf" is selected. The table has columns for "Name" and "Type".
- Document View:** Displays the content of the selected PDF file, "United States Patent Busch". The document includes a title, a list of claims, and a table of contents.

The file list shows the following files:

Name	Type
\$MFT_RECORD	<ATTRIBUTE>
\$STANDARD_INFORMATION	<ATTRIBUTE>
\$FILE_NAME	<ATTRIBUTE>
\$INDEX_ROOT(\$I30)	<ATTRIBUTE>
\$INDEX_ALLOCATION(\$I30)	<ATTRIBUTE>
\$BITMAP(\$I30)	<ATTRIBUTE>
\$3IGDHO.doc	Unknown form
\$47XZM4.pdf	Unknown form
\$6UNH4G.doc	Unknown form
\$8C3US.doc	Unknown form
\$8E610B.doc	Unknown form
\$8AHUR8.pdf	Unknown form
\$8RTS3N.doc	Unknown form
\$8TOPXUG.pdf	Unknown form
\$83IGDHO.doc	DOC Microsoft
\$847XZM4.pdf	PDF document
\$86UNH4G.doc	Microsoft Office
\$8C3US.doc	Microsoft Office
\$8E610B.doc	Microsoft Office
\$8AHUR8.pdf	PDF document
\$8RTS3N.doc	Microsoft Office
\$8TOPXUG.pdf	PDF document
desktop.ini	ASCII text

The document viewer shows the following text:

**United States Patent**  
**Busch**

(12) **United States Patent** (10) **Patent**  
(45) **Date**

(54) **SYSTEMS AND METHODS FOR SHARING LOCATION INFORMATION** (58) **Field of CPC**

(71) Applicant: **Facebook, Inc.**, Menlo Park, CA (US)  
(72) Inventor: **James David Busch**, Tempe, AZ (US)  
(73) Assignee: **Facebook, Inc.**, Menlo Park, CA (US)

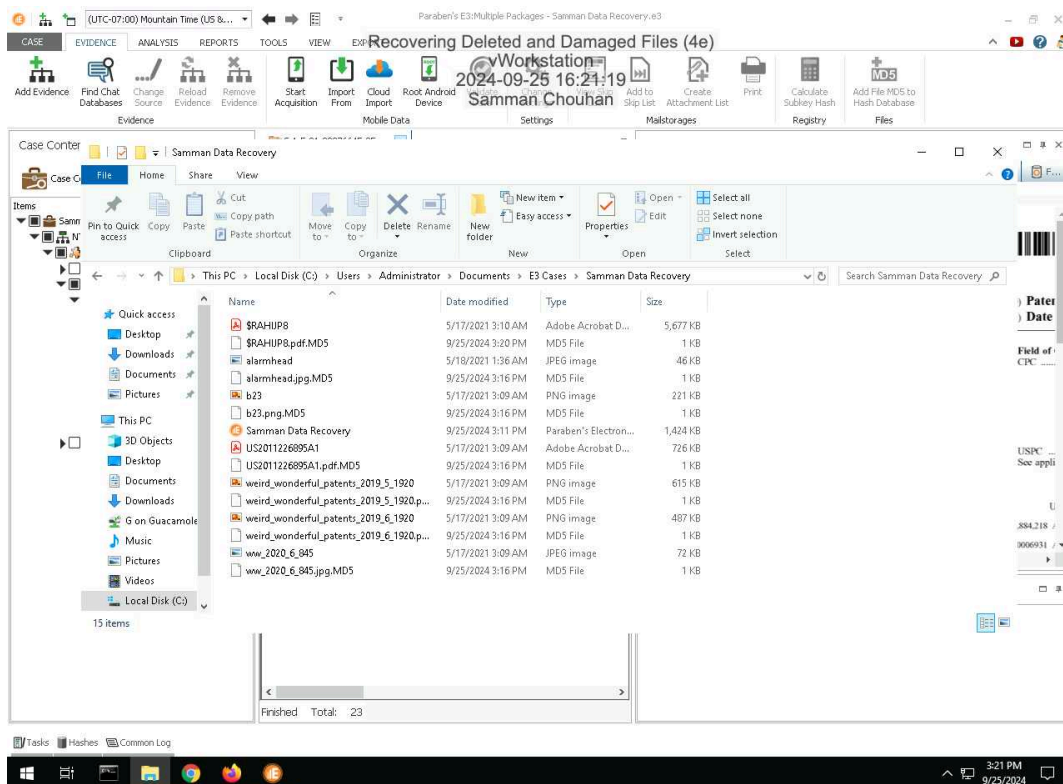
(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(h) by 0 days. USPC: See appli

(21) Appl. No.: **16/887,514** (56) **U**  
(22) Filed: **Nov. 18, 2019**  
(65) **Prior Publication Data** 5,884,218 /  
US 2020/0082440 A1 Mar. 12, 2020 2003/0006931 /

# Recovering Deleted and Damaged Files (4e)

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

## 25. Make a screen capture showing the recovered files in the File Explorer.

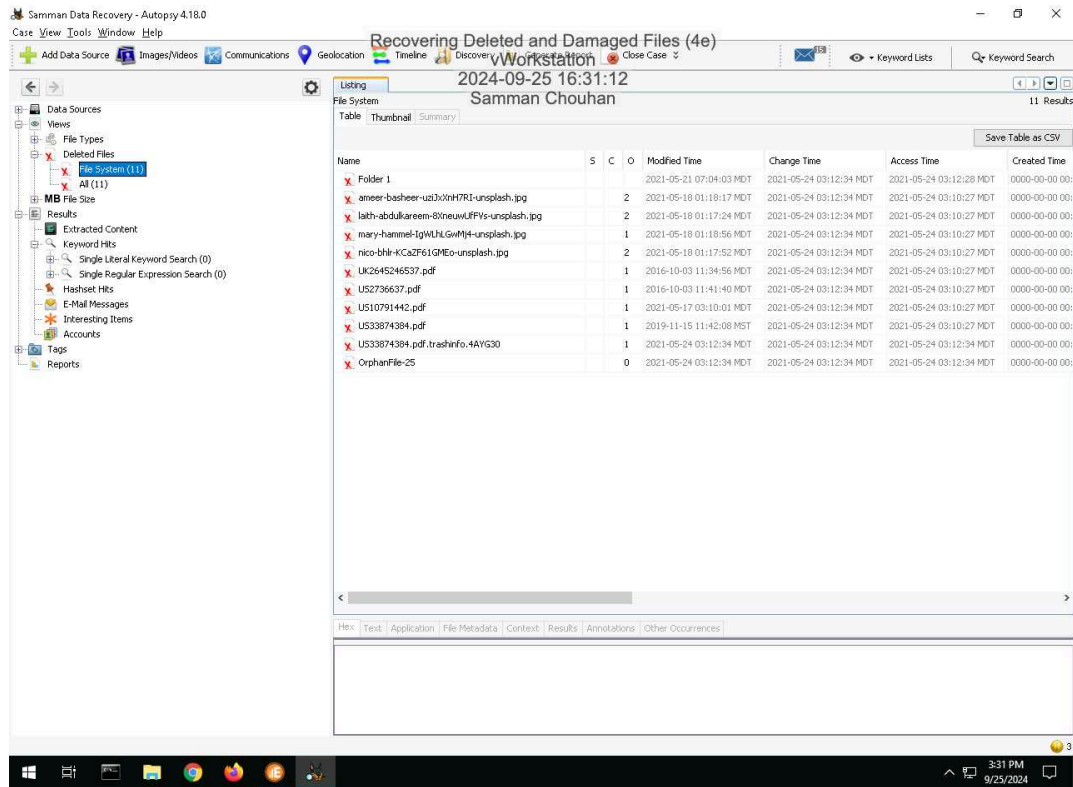


## Part 2: Recover Deleted Files from an Ext4 Drive Image with Autopsy

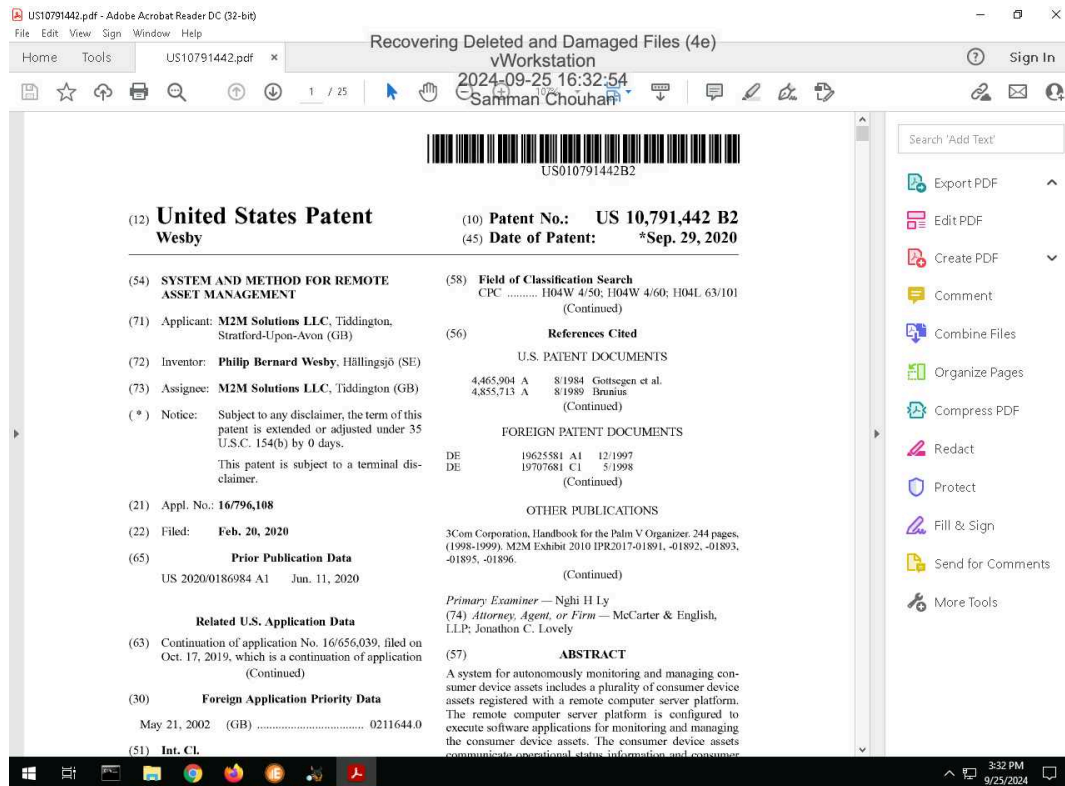
# Recovering Deleted and Damaged Files (4e)

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.



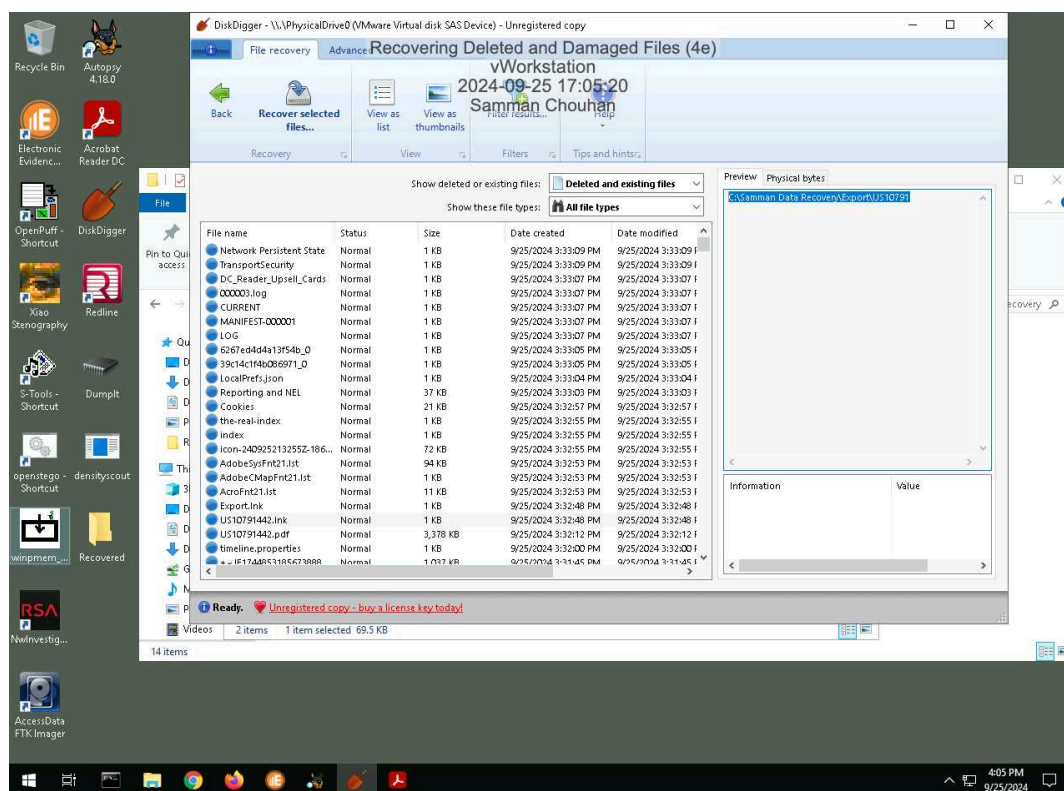
### 22. Make a screen capture showing the recovered patent file.



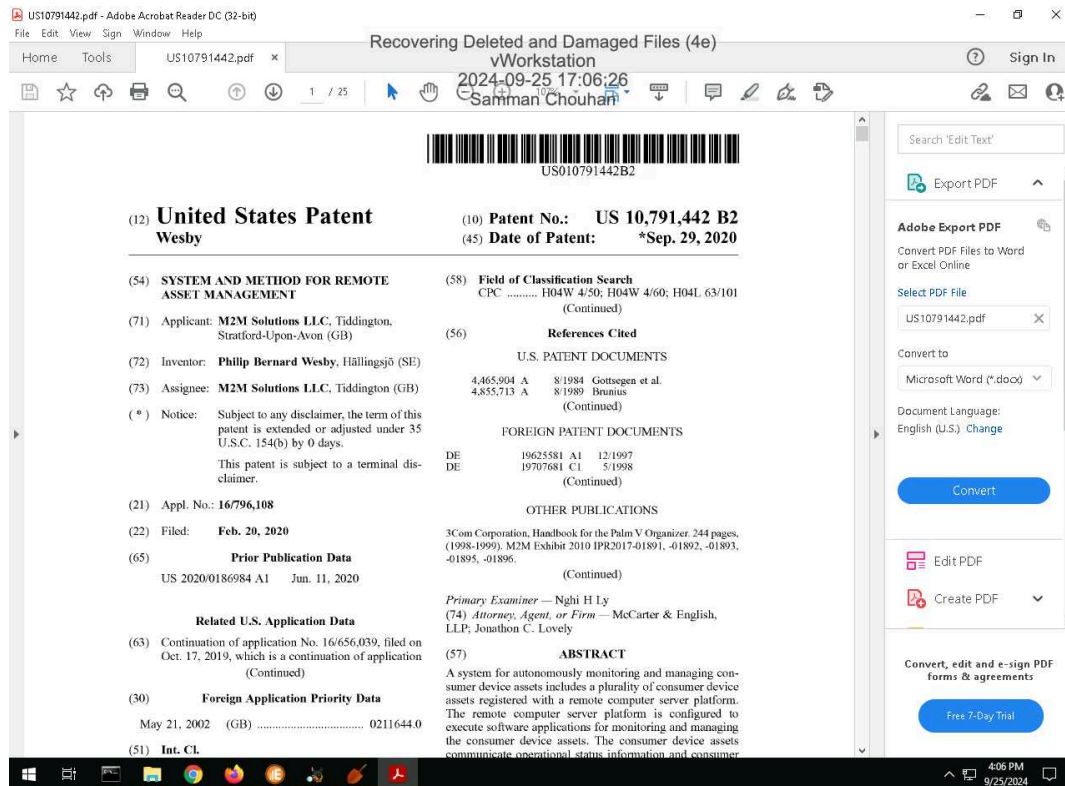
## Section 2: Applied Learning

### 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.



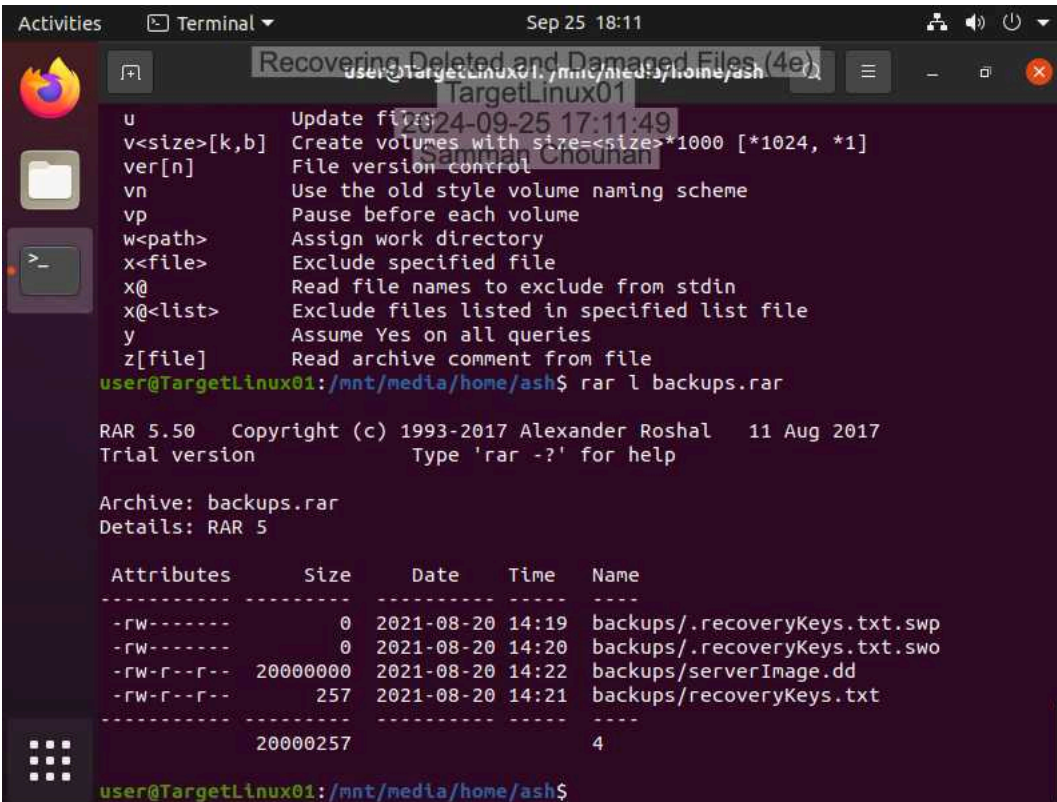
## Part 2: Recover Deleted Files in Linux with PhotoRec



## 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 titled "Recovering Deleted and Damaged Files (4e)" with the user "user@TargetLinux01" and the directory "/mnt/media/home/ash". The terminal displays the output of the command `rar l backups.rar`. The output shows the RAR version (5.50), copyright information, and a list of files in the archive. The files are:

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

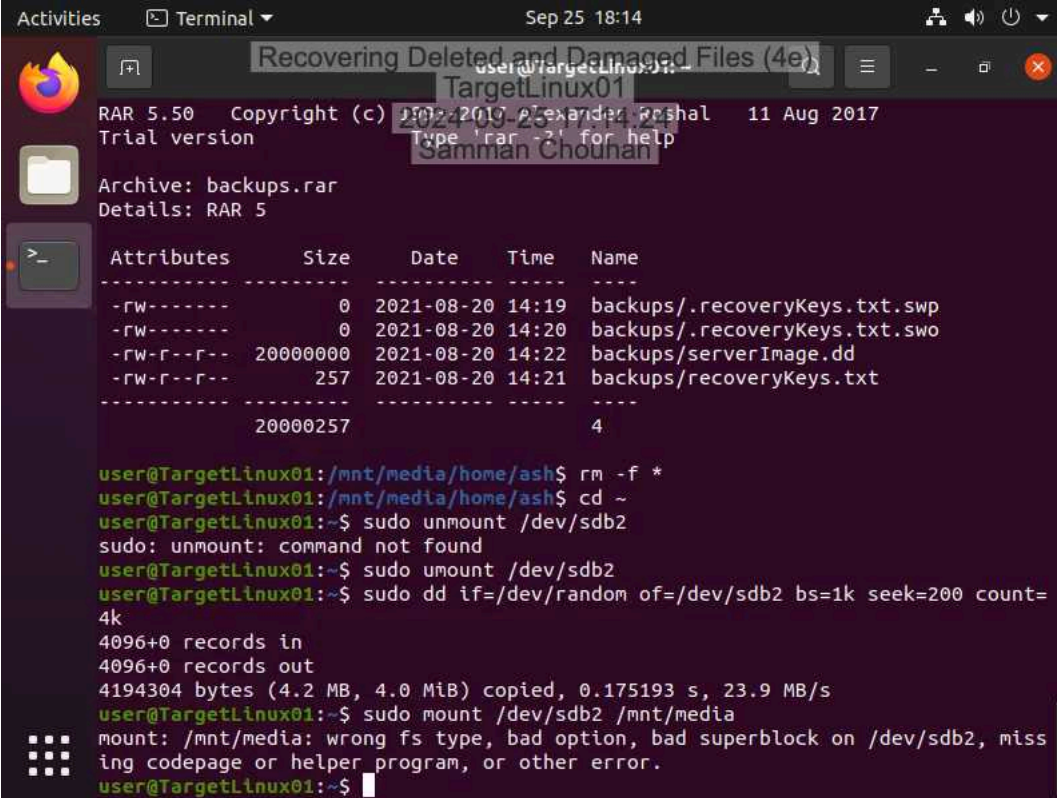
The terminal prompt is `user@TargetLinux01:/mnt/media/home/ash$`.



## 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 extracted a RAR file named 'backups.rar' which contains several files. The user then attempts to unmount `/dev/sdb2` using `sudo unmount`, which fails with the error 'command not found'. They then attempt to mount `/dev/sdb2` using `sudo mount`, which fails with the error 'wrong fs type, bad option, bad superblock on /dev/sdb2, missing codepage or helper program, or other error.'

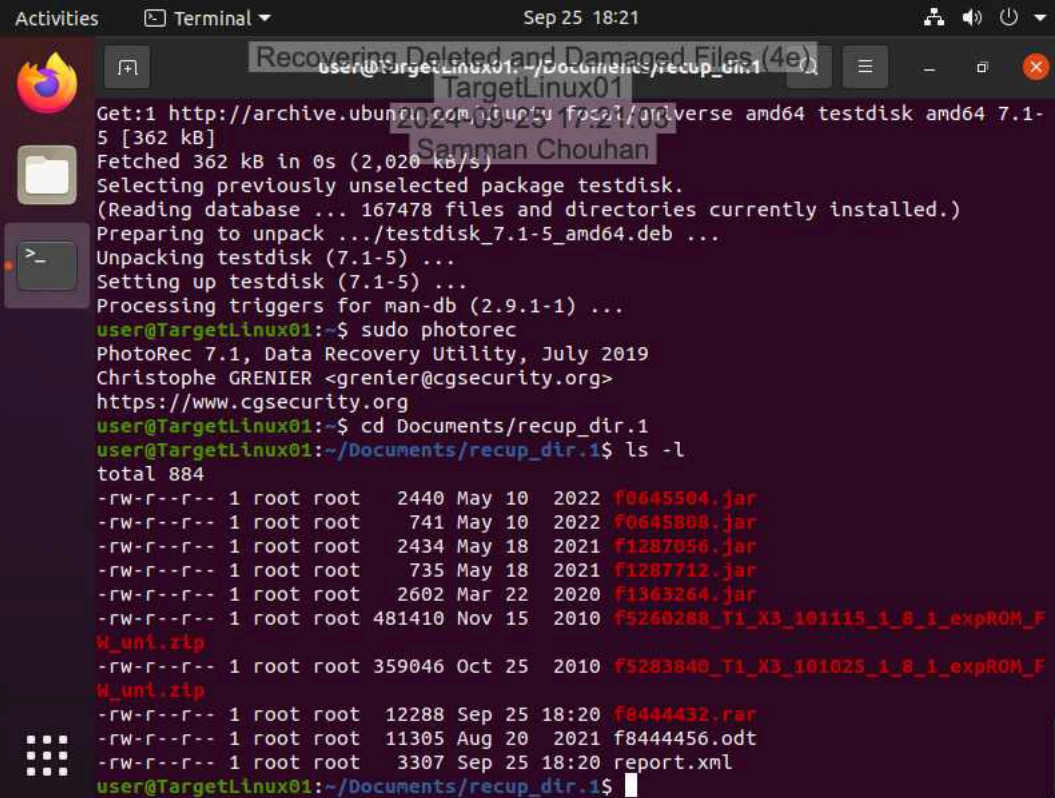
```
user@TargetLinux01:~$ rm -f *
user@TargetLinux01:~$ cd ~
user@TargetLinux01:~$ sudo unmount /dev/sdb2
sudo: unmount: command not found
user@TargetLinux01:~$ sudo umount /dev/sdb2
user@TargetLinux01:~$ sudo dd if=/dev/random of=/dev/sdb2 bs=1k seek=200 count=4k
4096+0 records in
4096+0 records out
4194304 bytes (4.2 MB, 4.0 MiB) copied, 0.175193 s, 23.9 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:~$
```

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

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

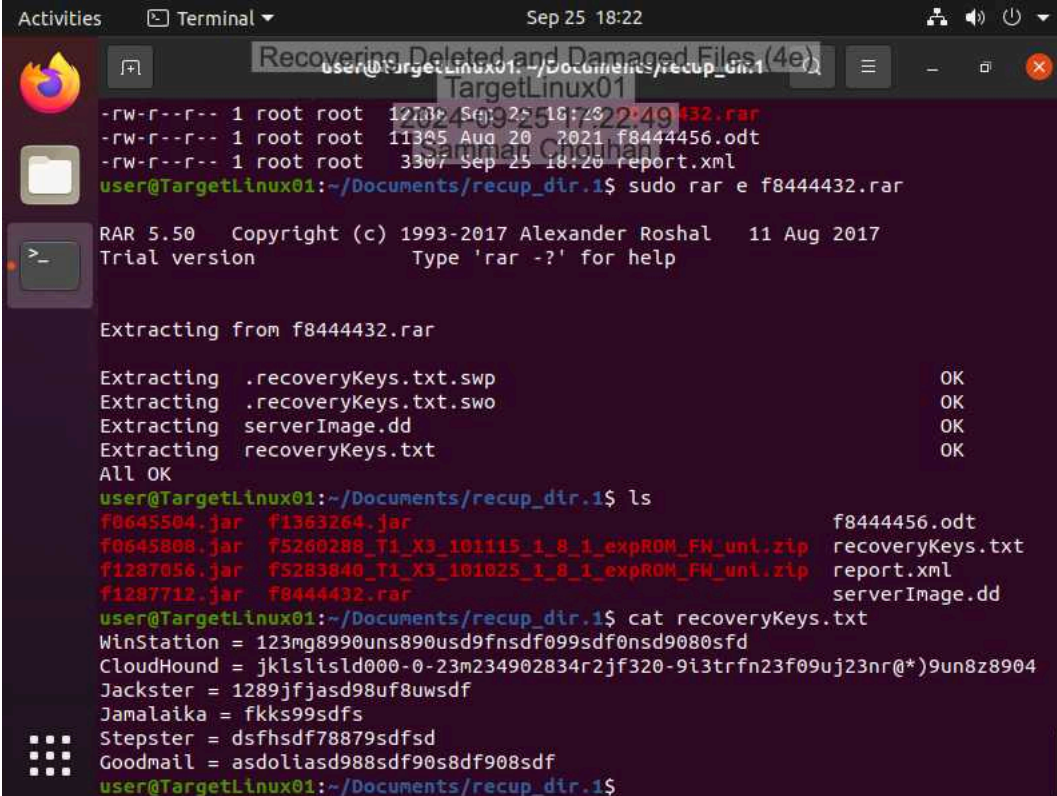


```
user@TargetLinux01:~/Documents/recup_dir.1$ sudo apt-get install testdisk
Get:1 http://archive.ubuntu.com/ubuntu focal/universe amd64 testdisk amd64 7.1-5 [362 kB]
Fetched 362 kB in 0s (2,020 kB/s)
Selecting previously unselected package testdisk.
(Reading database ... 167478 files and directories 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 -l
total 884
-rw-r--r-- 1 root root 2440 May 10 2022 f0645504.jar
-rw-r--r-- 1 root root 741 May 10 2022 f0645808.jar
-rw-r--r-- 1 root root 2434 May 18 2021 f1287056.jar
-rw-r--r-- 1 root root 735 May 18 2021 f1287712.jar
-rw-r--r-- 1 root root 2602 Mar 22 2020 f1363264.jar
-rw-r--r-- 1 root root 481410 Nov 15 2010 f5260288_T1_X3_101115_1_8_1_expROM_F
W_uni.zip
-rw-r--r-- 1 root root 359046 Oct 25 2010 f5283840_T1_X3_101025_1_8_1_expROM_F
W_uni.zip
-rw-r--r-- 1 root root 12288 Sep 25 18:20 f8444432.rar
-rw-r--r-- 1 root root 11305 Aug 20 2021 f8444456.odt
-rw-r--r-- 1 root root 3307 Sep 25 18:20 report.xml
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 titled "Recovering Deleted and Damaged Files (4e)" with the command prompt "user@TargetLinux01:~/Documents/recup\_dir.1". The terminal displays the following commands and output:

```
user@TargetLinux01:~/Documents/recup_dir.1$ ls -l
-rw-r--r-- 1 root root 12100 Sep 25 18:20 f8444432.rar
-rw-r--r-- 1 root root 11305 Aug 20 2021 f8444456.odt
-rw-r--r-- 1 root root 3307 Sep 25 18:20 report.xml
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

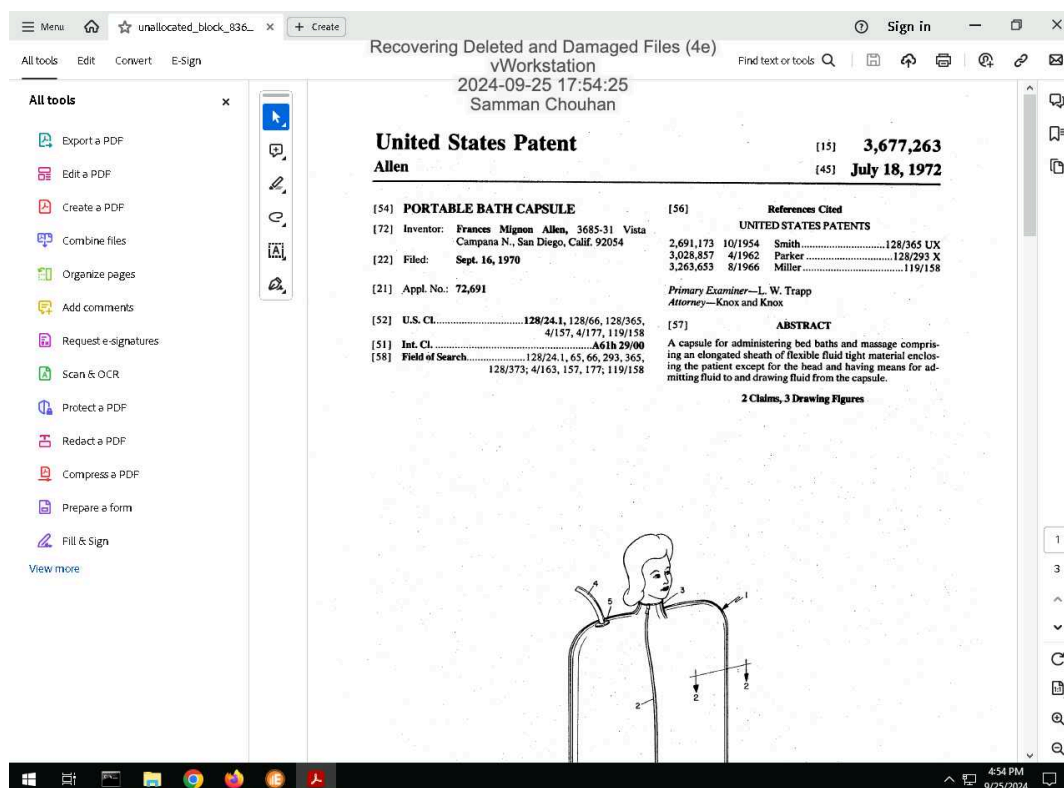
Extracting from f8444432.rar

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 f5280288_T1_X3_101115_1_8_1_expROM_FW_uni.zip recoveryKeys.txt
f1287056.jar f5283840_T1_X3_101025_1_8_1_expROM_FW_uni.zip report.xml
f1287712.jar f8444432.rar serverImage.dd
user@TargetLinux01:~/Documents/recup_dir.1$ cat recoveryKeys.txt
WinStation = 123mg8990uns890usd9fnsdf099sdf0nsd9080sfd
CloudHound = jklslisld000-0-23m234902834r2jf320-9i3trfn23f09uj23nr(*)9un8z8904
Jackster = 1289jffjasd98uf8uwsdf
Jamalaika = fkks99sdfs
Stepster = dsfhdsf78879sdfs
Goodmail = asdoliasd988sdf90s8df908sdf
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.



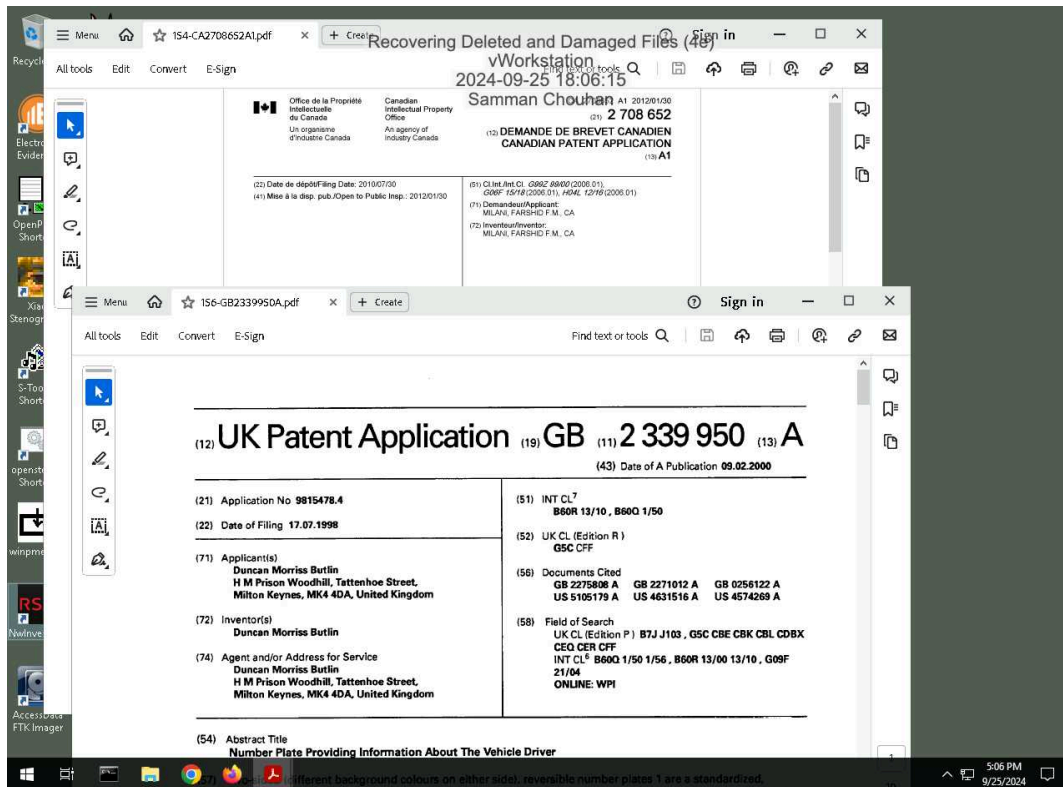
the file was recovered from paraben's e3 under unallocated space items on unallocated block 36

### 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.



i found 2 files in the APFS drive , one for UK and another for canada