# Recovering Deleted and Damaged Files (4e)

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

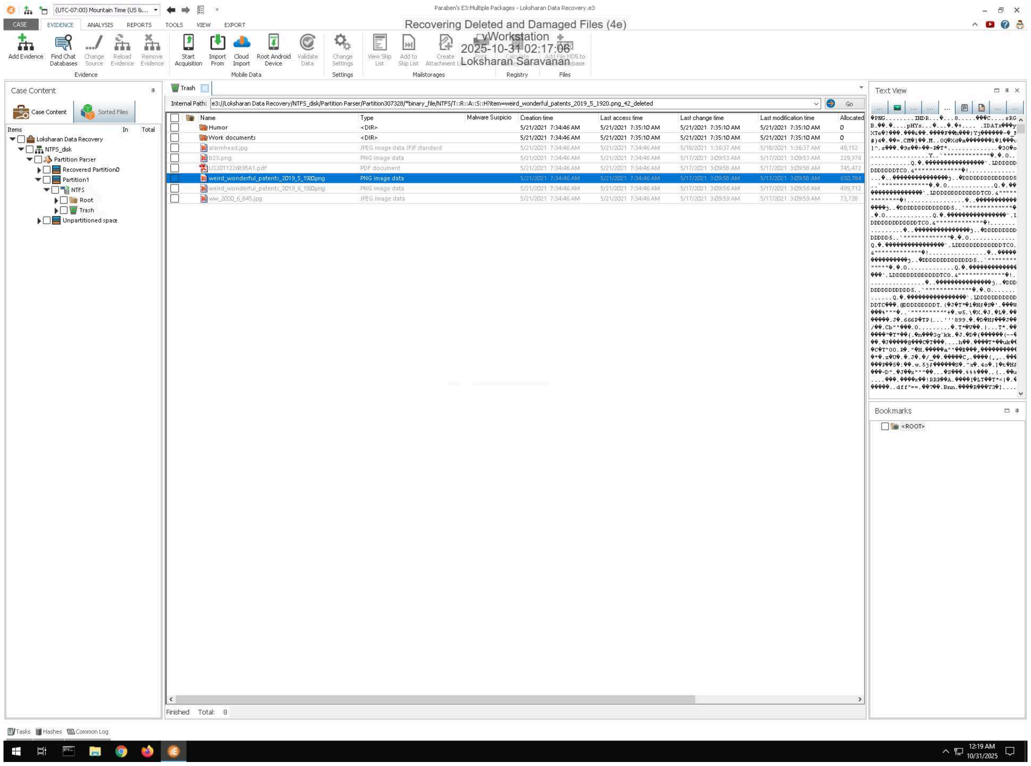
| | |
|---|---|
| Student:<br>Loksharan Saravanan | Email:<br>loksharan.soc@gmail.com |
| Time on Task:<br>5 hours, 43 minutes | Progress:<br>100% |

Report Generated: Thursday, November 20, 2025 at 1:13 AM

# Section 1: Hands-On Demonstration

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

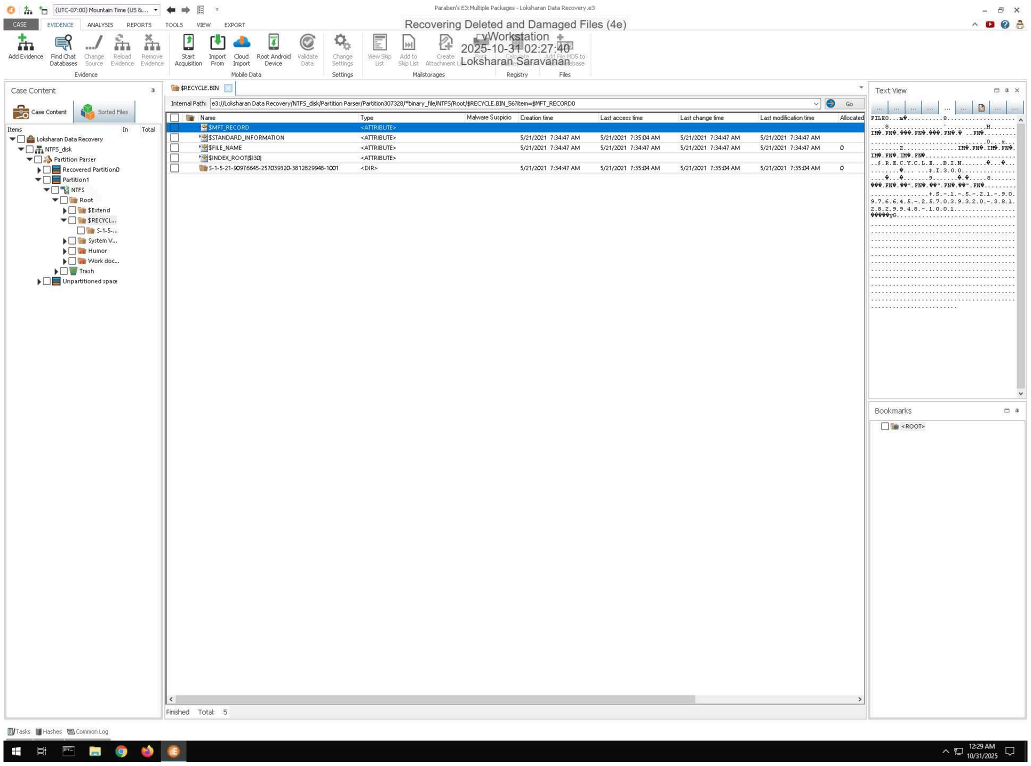
13. **Make a screen capture** showing the **list of recovered files and folders in the E3 Trash folder**.



Internal Path: e3://Loksharan Data Recovery/NTFS_disk/Partition Parser/Partition307328/*binary_file/NTFS/T::R::A::S::H?item=weird_wonderful_patents_2019_5_1920.png_42_deleted

| Name | Type | Malware Suspicio | Creation time | Last access time | Last change time | Last modification time | Allocated |
|---|---|---|---|---|---|---|---|
| Humor | <DIR> | | 5/21/2021 7:34:46 AM | 5/21/2021 7:35:10 AM | 5/21/2021 7:35:10 AM | 5/21/2021 7:35:10 AM | 0 |
| Work documents | <DIR> | | 5/21/2021 7:34:46 AM | 5/21/2021 7:35:10 AM | 5/21/2021 7:35:10 AM | 5/21/2021 7:35:10 AM | 0 |
| alarmhead.jpg | JPEG image data JFIF standard | | 5/21/2021 7:34:46 AM | 5/21/2021 7:34:46 AM | 5/18/2021 1:36:37 AM | 5/18/2021 1:36:37 AM | 49,152 |
| b23.png | PNG image data | | 5/21/2021 7:34:46 AM | 5/21/2021 7:34:46 AM | 5/17/2021 3:09:53 AM | 5/17/2021 3:09:53 AM | 229,376 |
| US2011226895A1.pdf | PDF document | | 5/21/2021 7:34:46 AM | 5/21/2021 7:34:46 AM | 5/17/2021 3:09:58 AM | 5/17/2021 3:09:58 AM | 745,472 |
| weird_wonderful_patents_2019_5_1920.png | PNG image data | | 5/21/2021 7:34:46 AM | 5/21/2021 7:34:46 AM | 5/17/2021 3:09:58 AM | 5/17/2021 3:09:58 AM | 630,784 |
| weird_wonderful_patents_2019_6_1920.png | PNG image data | | 5/21/2021 7:34:46 AM | 5/21/2021 7:34:46 AM | 5/17/2021 3:09:56 AM | 5/17/2021 3:09:56 AM | 499,712 |
| ww_2020_6_845.jpg | JPEG image data | | 5/21/2021 7:34:46 AM | 5/21/2021 7:34:46 AM | 5/17/2021 3:09:59 AM | 5/17/2021 3:09:59 AM | 73,728 |

20. **Make a screen capture** showing the **patent file in the File Viewer**.



Paraben's E3:Multiple Packages - Loksharan Data Recovery.e3

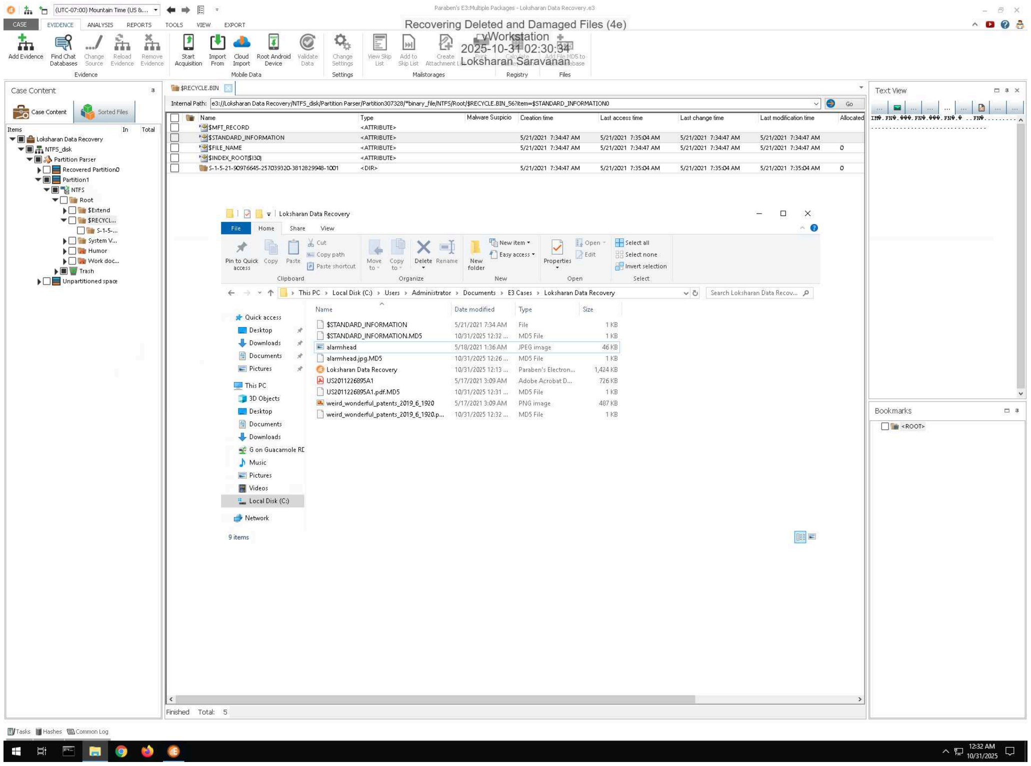
Recovering Deleted and Damaged Files (4e)
vWorkstation
2025-10-31 02:27:40
Loksharan Saravanan

Internal Path: e3://Loksharan Data Recovery/NTFS_disk/Partition Parser/Partition307328/*binary_file/NTFS/Root/$RECYCLE.BIN_56?item=$MFT_RECORD0

| Name | Type | Malware Suspicio | Creation time | Last access time | Last change time | Last modification time | Allocated |
|---|---|---|---|---|---|---|---|
| $MFT_RECORD | <ATTRIBUTE> | | | | | | |
| $STANDARD_INFORMATION | <ATTRIBUTE> | | 5/21/2021 7:34:47 AM | 5/21/2021 7:35:04 AM | 5/21/2021 7:34:47 AM | 5/21/2021 7:34:47 AM | |
| $FILE_NAME | <ATTRIBUTE> | | 5/21/2021 7:34:47 AM | 5/21/2021 7:34:47 AM | 5/21/2021 7:34:47 AM | 5/21/2021 7:34:47 AM | 0 |
| $INDEX_ROOT($I30) | <ATTRIBUTE> | | | | | | |
| S-1-5-21-90976645-257039320-3812829948-1001 | <DIR> | | 5/21/2021 7:34:47 AM | 5/21/2021 7:35:04 AM | 5/21/2021 7:35:04 AM | 5/21/2021 7:35:04 AM | 0 |

Finished Total: 5

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



Paraben's E3:Multiple Packages - Loksharan Data Recovery.e3

Recovering Deleted and Damaged Files (4e)
vWorkstation
2025-10-31 02:30:34
Loksharan Saravanan

Internal Path: e3://Loksharan Data Recovery/NTFS_disk/Partition Parser/Partition307328/*binary_file/NTFS/Root/$RECYCLE.BIN_56?item=$STANDARD_INFORMATION0

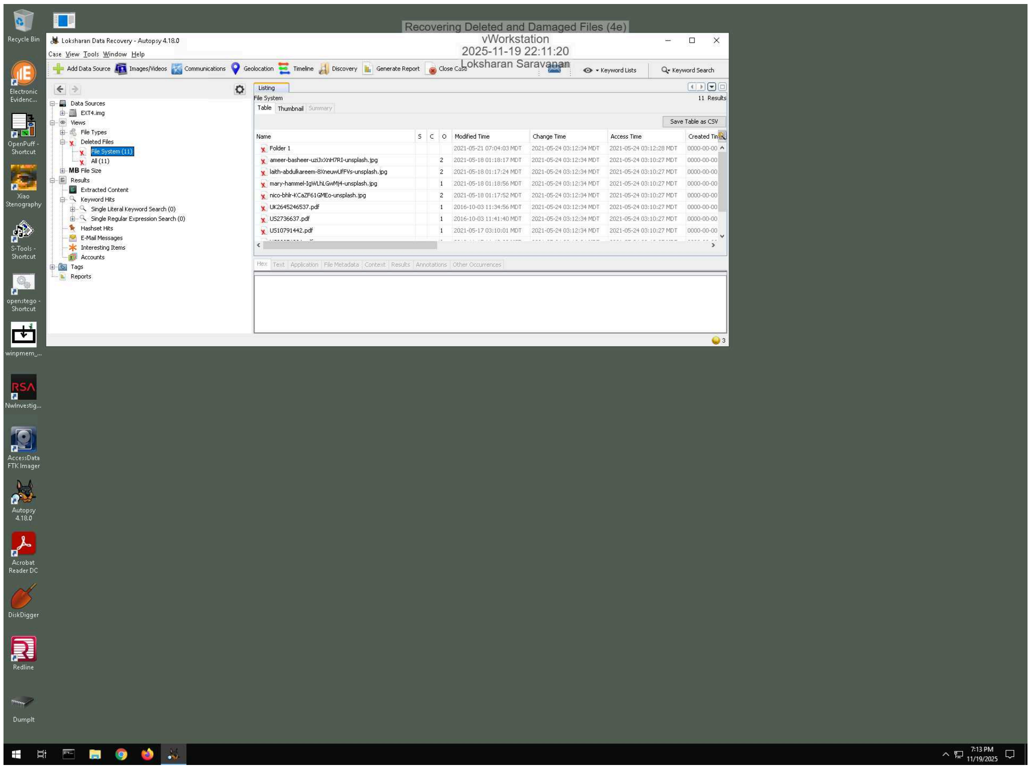
This PC > Local Disk (C:) > Users > Administrator > Documents > E3 Cases > Loksharan Data Recovery

| Name | Date modified | Type | Size |
|---|---|---|---|
| $STANDARD_INFORMATION | 5/21/2021 7:34 AM | File | 1 KB |
| $STANDARD_INFORMATION.MD5 | 10/31/2025 12:32 ... | MD5 File | 1 KB |
| alarmhead | 5/18/2021 1:36 AM | JPEG image | 46 KB |
| alarmhead.jpg.MD5 | 10/31/2025 12:26 ... | MD5 File | 1 KB |
| Loksharan Data Recovery | 10/31/2025 12:13 ... | Paraben's Electron... | 1,424 KB |
| US2011226895A1 | 5/17/2021 3:09 AM | Adobe Acrobat D... | 726 KB |
| US2011226895A1.pdf.MD5 | 10/31/2025 12:31 ... | MD5 File | 1 KB |
| weird_wonderful_patents_2019_6_1920 | 5/17/2021 3:09 AM | PNG image | 487 KB |
| weird_wonderful_patents_2019_6_1920.p... | 10/31/2025 12:32 ... | MD5 File | 1 KB |

9 items

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

14. **Make a screen capture** showing the **contents of the list of deleted files in Autopsy**.



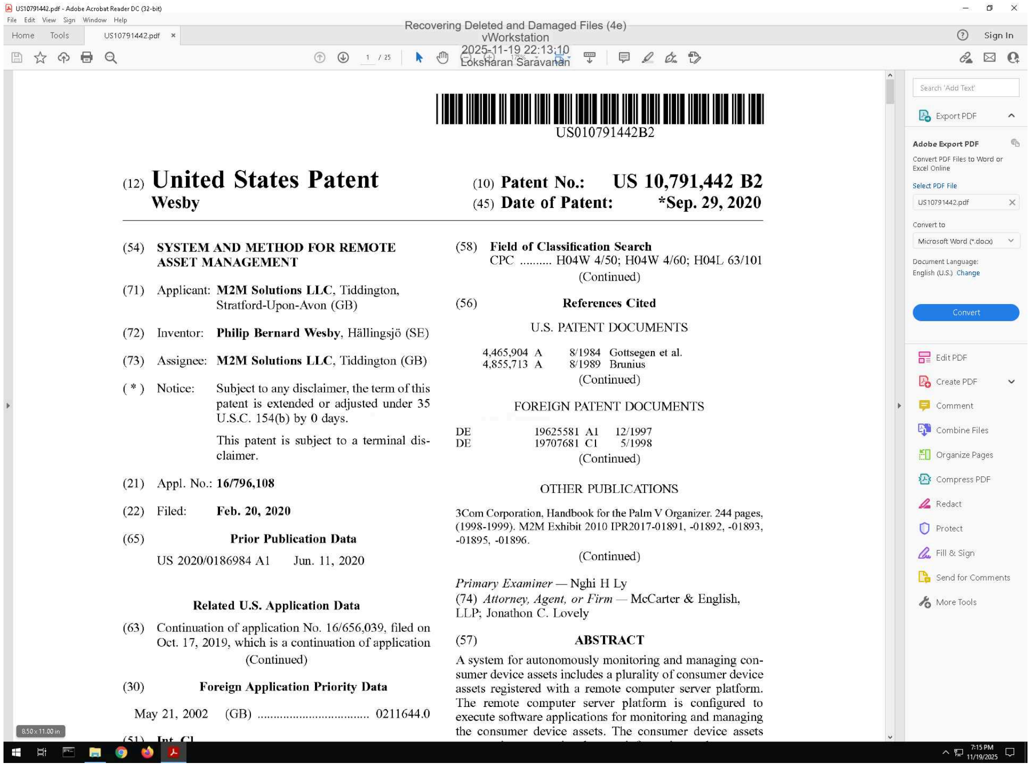
Recovering Deleted and Damaged Files (4e)
vWorkstation
2025-11-19 22:11:20
Loksharan Saravanan

Loksharan Data Recovery - Autopsy 4.18.0

File System — 11 Results

| Name | S | C | O | Modified Time | Change Time | Access Time | Created Ti |
|---|---|---|---|---|---|---|---|
| Folder 1 | | | | 2021-05-21 07:04:03 MDT | 2021-05-24 03:12:34 MDT | 2021-05-24 03:12:28 MDT | 0000-00-00 |
| ameer-basheer-uziJxXnH7RI-unsplash.jpg | | | 2 | 2021-05-18 01:18:17 MDT | 2021-05-24 03:12:34 MDT | 2021-05-24 03:10:27 MDT | 0000-00-00 |
| laith-abdulkareem-8XneuwUfFVs-unsplash.jpg | | | 2 | 2021-05-18 01:17:24 MDT | 2021-05-24 03:12:34 MDT | 2021-05-24 03:10:27 MDT | 0000-00-00 |
| mary-hammel-IgWLhLGwMj4-unsplash.jpg | | | 1 | 2021-05-18 01:18:56 MDT | 2021-05-24 03:12:34 MDT | 2021-05-24 03:10:27 MDT | 0000-00-00 |
| nico-bhlr-KCaZF61GMEo-unsplash.jpg | | | 2 | 2021-05-18 01:17:52 MDT | 2021-05-24 03:12:34 MDT | 2021-05-24 03:10:27 MDT | 0000-00-00 |
| UK2645246537.pdf | | | 1 | 2016-10-03 11:34:56 MDT | 2021-05-24 03:12:34 MDT | 2021-05-24 03:10:27 MDT | 0000-00-00 |
| US2736637.pdf | | | 1 | 2016-10-03 11:41:40 MDT | 2021-05-24 03:12:34 MDT | 2021-05-24 03:10:27 MDT | 0000-00-00 |
| US10791442.pdf | | | 1 | 2021-05-17 03:10:01 MDT | 2021-05-24 03:12:34 MDT | 2021-05-24 03:10:27 MDT | 0000-00-00 |

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



US010791442B2

(12) **United States Patent**
**Wesby**

(10) **Patent No.: US 10,791,442 B2**
(45) **Date of Patent: *Sep. 29, 2020**

(54) **SYSTEM AND METHOD FOR REMOTE ASSET MANAGEMENT**

(71) Applicant: **M2M Solutions LLC**, Tiddington, Stratford-Upon-Avon (GB)

(72) Inventor: **Philip Bernard Wesby**, Hällingsjö (SE)

(73) Assignee: **M2M Solutions LLC**, Tiddington (GB)

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

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/796,108**

(22) Filed: **Feb. 20, 2020**

(65) **Prior Publication Data**

US 2020/0186984 A1 Jun. 11, 2020

**Related U.S. Application Data**

(63) Continuation of application No. 16/656,039, filed on Oct. 17, 2019, which is a continuation of application
(Continued)

(30) **Foreign Application Priority Data**

May 21, 2002 (GB) .................................. 0211644.0

(51) Int. Cl.

(58) **Field of Classification Search**
CPC .......... H04W 4/50; H04W 4/60; H04L 63/101
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | |
|---|---|---|---|
| 4,465,904 | A | 8/1984 | Gottsegen et al. |
| 4,855,713 | A | 8/1989 | Brunius |

(Continued)

FOREIGN PATENT DOCUMENTS

| | | | |
|---|---|---|---|
| DE | 19625581 | A1 | 12/1997 |
| DE | 19707681 | C1 | 5/1998 |

(Continued)

OTHER PUBLICATIONS

3Com Corporation, Handbook for the Palm V Organizer. 244 pages, (1998-1999). M2M Exhibit 2010 IPR2017-01891, -01892, -01893, -01895, -01896.

(Continued)

*Primary Examiner* — Nghi H Ly
(74) *Attorney, Agent, or Firm* — McCarter & English, LLP; Jonathon C. Lovely

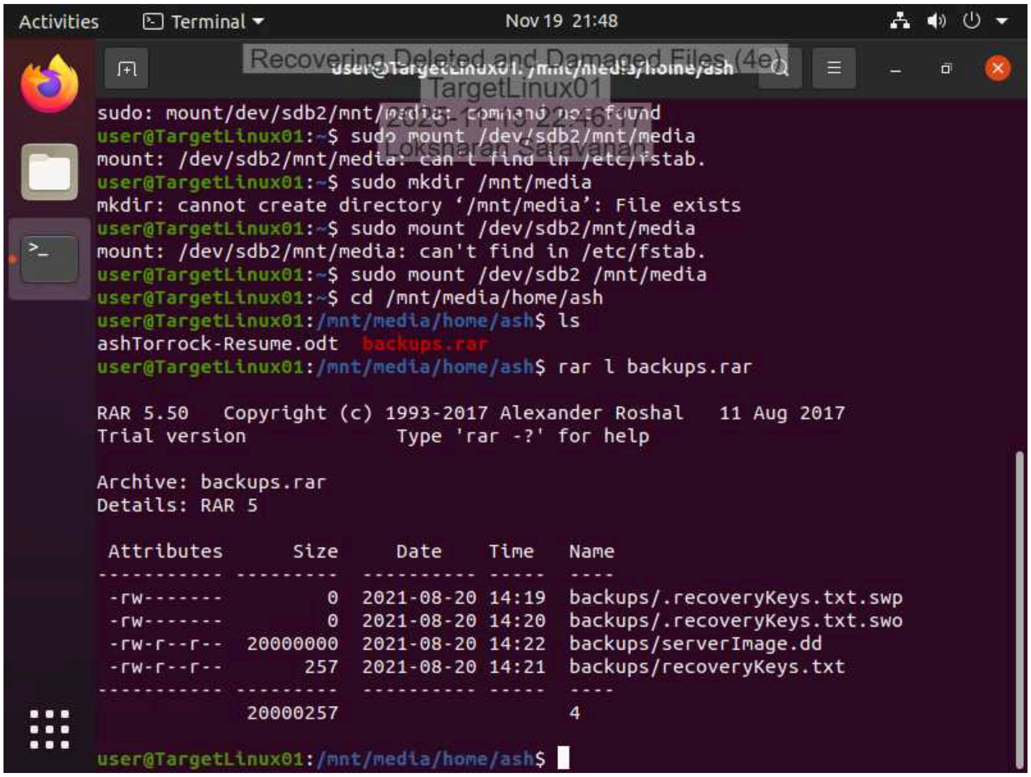
(57) **ABSTRACT**

A system for autonomously monitoring and managing consumer device assets includes a plurality of consumer device assets registered with a remote computer server platform. The remote computer server platform is configured to execute software applications for monitoring and managing the consumer device assets. The consumer device assets

# Section 2: Applied Learning

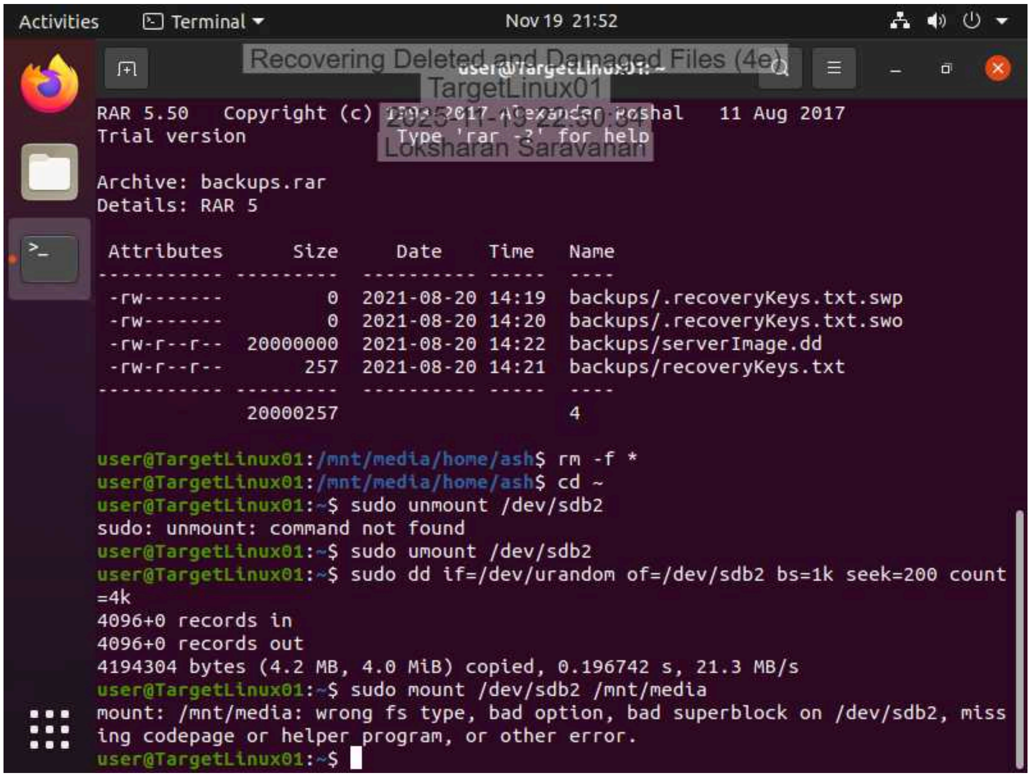
## Part 1: Recover Deleted Files in Linux with PhotoRec

9. **Make a screen capture** showing the **contents of the RAR archive in the /mnt/media/home/ash directory**.



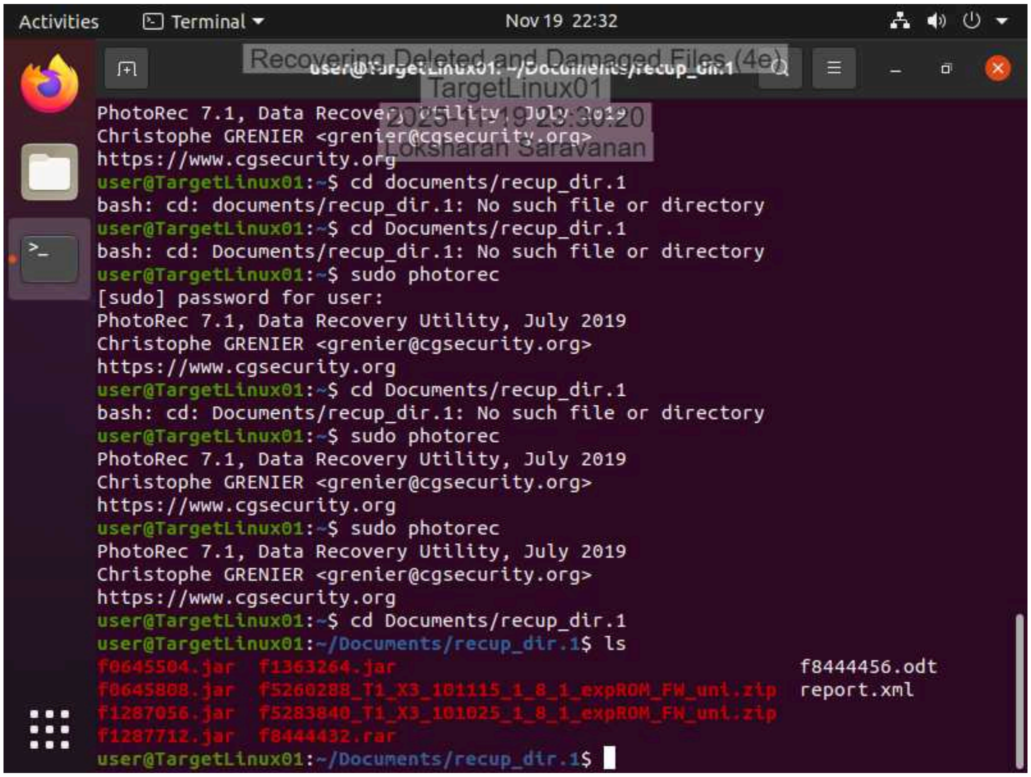
```
sudo: mount/dev/sdb2/mnt/media: command not found
user@TargetLinux01:~$ sudo mount /dev/sdb2/mnt/media
mount: /dev/sdb2/mnt/media: can't find in /etc/fstab.
user@TargetLinux01:~$ sudo mkdir /mnt/media
mkdir: cannot create directory '/mnt/media': File exists
user@TargetLinux01:~$ sudo mount /dev/sdb2/mnt/media
mount: /dev/sdb2/mnt/media: can't find in /etc/fstab.
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

user@TargetLinux01:/mnt/media/home/ash$
```

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



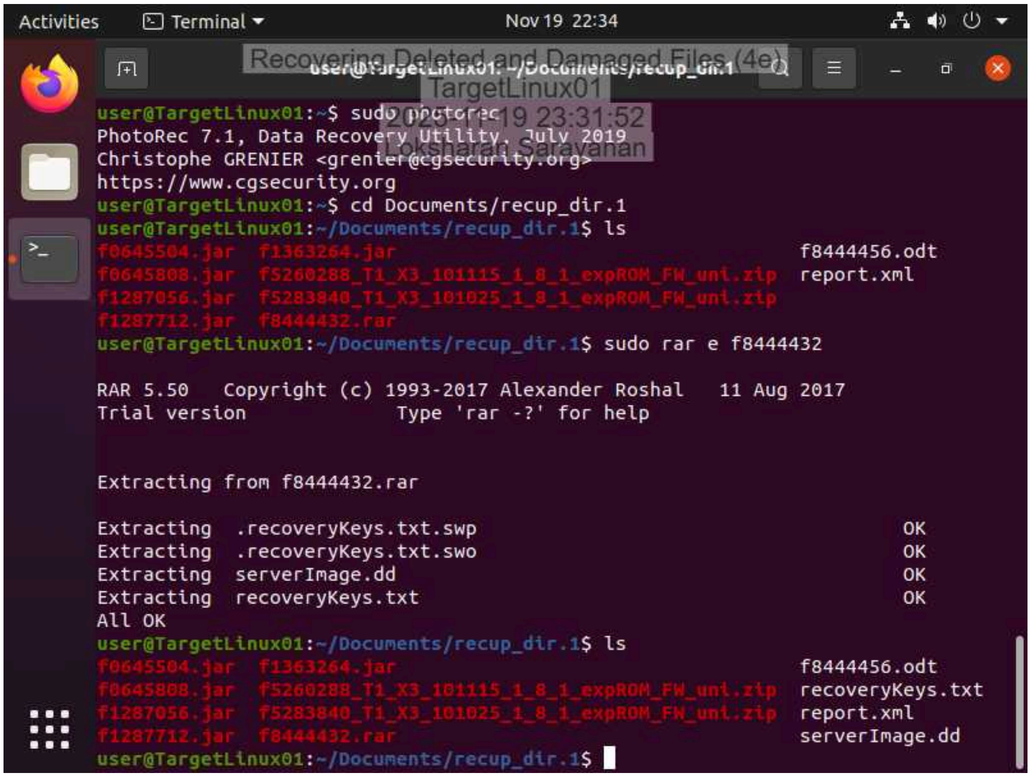
```
RAR 5.50   Copyright (c) 1993-2017 Alexander Roshal   11 Aug 2017
Trial version             Type 'rar -?' for help

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 unmount /dev/sdb2
sudo: unmount: 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, 0.196742 s, 21.3 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:~$ 
```

32. **Make a screen capture** showing the **compressed files recovered by 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
bash: cd: documents/recup_dir.1: No such file or directory
user@TargetLinux01:~$ cd Documents/recup_dir.1
bash: cd: Documents/recup_dir.1: No such file or directory
user@TargetLinux01:~$ sudo photorec
[sudo] password for user:
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
user@TargetLinux01:~$ cd Documents/recup_dir.1
bash: cd: Documents/recup_dir.1: No such file or directory
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
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$ 
```

35. **Make a screen capture** showing the **backup files recovered from the RAR archive**.

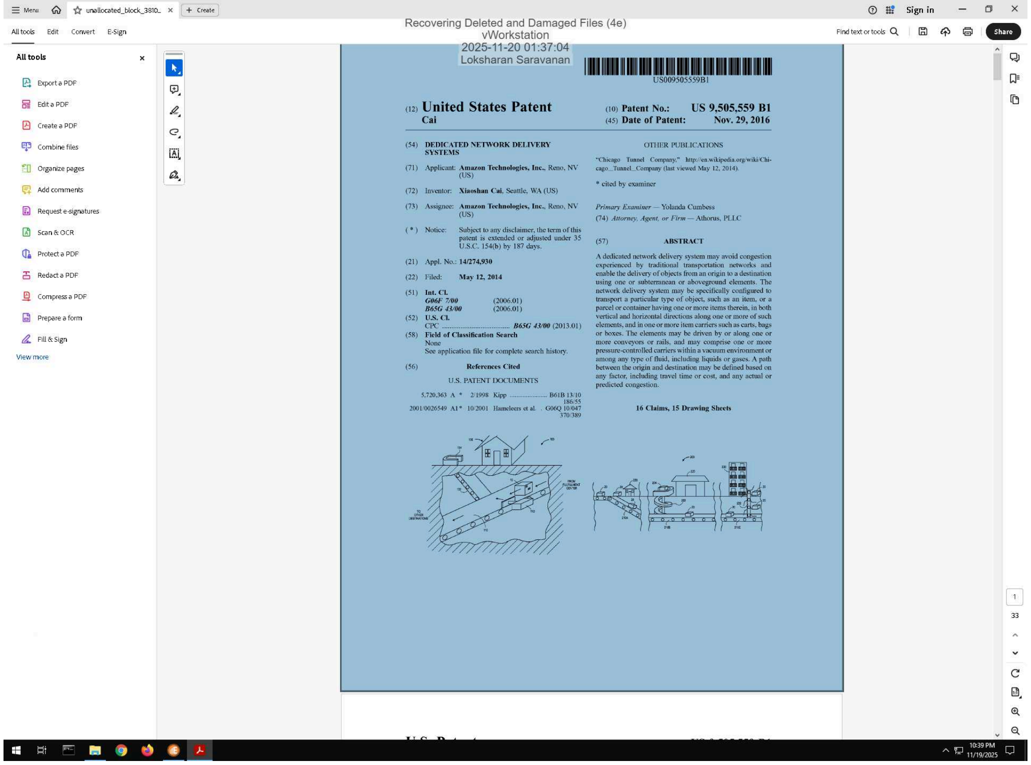

Activities
Terminal
Nov 19 22:34
user@TargetLinux01: ~/Documents/recup_dir.1
Recovering Deleted and Damaged Files (4e)
TargetLinux01
2025-11-19 23:31:52
Loksharan Saravanan

```
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 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$ ls
f0645504.jar  f1363264.jar                                    f8444456.odt
f0645808.jar  f5260288_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$ 
```

# 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**.



US009505559B1

(12) **United States Patent**
**Cai**

(10) **Patent No.: US 9,505,559 B1**
(45) **Date of Patent: Nov. 29, 2016**

(54) **DEDICATED NETWORK DELIVERY SYSTEMS**

(71) Applicant: **Amazon Technologies, Inc.**, Reno, NV (US)

(72) Inventor: **Xiaoshan Cai**, Seattle, WA (US)

(73) Assignee: **Amazon Technologies, Inc.**, Reno, NV (US)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 187 days.

(21) Appl. No.: **14/274,930**

(22) Filed: **May 12, 2014**

(51) **Int. Cl.**
***G06F 7/00*** (2006.01)
***B65G 43/00*** (2006.01)

(52) **U.S. Cl.**
CPC .................................... ***B65G 43/00*** (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,720,363 A * 2/1998 Kipp ........................ B61B 13/10
186/55
2001/0026549 A1* 10/2001 Hameleers et al. . G06Q 10/047
370/389

OTHER PUBLICATIONS

"Chicago Tunnel Company," http://en.wikipedia.org/wiki/Chicago_Tunnel_Company (last viewed May 12, 2014).

* cited by examiner

*Primary Examiner* — Yolanda Cumbess
(74) *Attorney, Agent, or Firm* — Athorus, PLLC

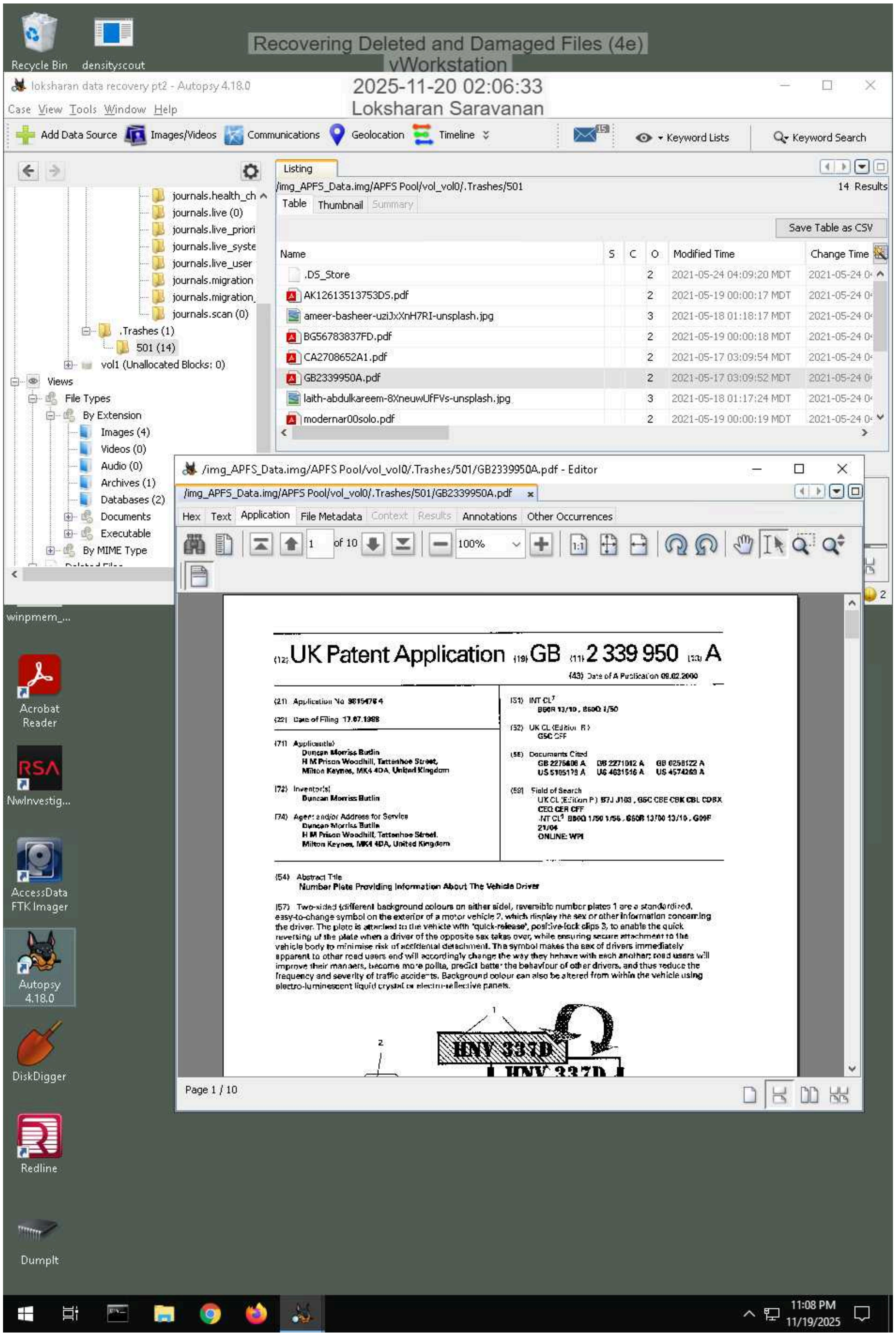
(57) **ABSTRACT**

A dedicated network delivery system may avoid congestion experienced by traditional transportation networks and enable the delivery of objects from an origin to a destination using one or subterranean or aboveground elements. The network delivery system may be specifically configured to transport a particular type of object, such as an item, or a parcel or container having one or more items therein, in both vertical and horizontal directions along one or more of such elements, and in one or more item carriers such as carts, bags or boxes. The elements may be driven by or along one or more conveyors or rails, and may comprise one or more pressure-controlled carriers within a vacuum environment or among any type of fluid, including liquids or gases. A path between the origin and destination may be defined based on any factor, including travel time or cost, and any actual or predicted congestion.

**16 Claims, 15 Drawing Sheets**

## Part 2: Recover Deleted Files from a APFS Drive Image

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



/img_APFS_Data.img/APFS Pool/vol_vol0/.Trashes/501 14 Results

| Name | S | C | O | Modified Time | Change Time |
|---|---|---|---|---|---|
| .DS_Store | | | 2 | 2021-05-24 04:09:20 MDT | 2021-05-24 0 |
| AK12613513753DS.pdf | | | 2 | 2021-05-19 00:00:17 MDT | 2021-05-24 0 |
| ameer-basheer-uziJxXnH7RI-unsplash.jpg | | | 3 | 2021-05-18 01:18:17 MDT | 2021-05-24 0 |
| BG56783837FD.pdf | | | 2 | 2021-05-19 00:00:18 MDT | 2021-05-24 0 |
| CA2708652A1.pdf | | | 2 | 2021-05-17 03:09:54 MDT | 2021-05-24 0 |
| GB2339950A.pdf | | | 2 | 2021-05-17 03:09:52 MDT | 2021-05-24 0 |
| laith-abdulkareem-8XneuwUfFVs-unsplash.jpg | | | 3 | 2021-05-18 01:17:24 MDT | 2021-05-24 0 |
| modernar00solo.pdf | | | 2 | 2021-05-19 00:00:19 MDT | 2021-05-24 0 |

/img_APFS_Data.img/APFS Pool/vol_vol0/.Trashes/501/GB2339950A.pdf - Editor

/img_APFS_Data.img/APFS Pool/vol_vol0/.Trashes/501/GB2339950A.pdf

(12) UK Patent Application (19) GB (11) 2 339 950 (13) A

(43) Date of A Publication 09.02.2000

(21) Application No 9815476 4

(22) Date of Filing 17.07.1998

(71) Applicant(s)
Duncan Morriss Butlin
H M Prison Woodhill, Tattenhoe Street,
Milton Keynes, MK4 4DA, United Kingdom

(72) Inventor(s)
Duncan Morriss Butlin

(74) Agent and/or Address for Service
Duncan Morriss Butlin
H M Prison Woodhill, Tattenhoe Street,
Milton Keynes, MK4 4DA, United Kingdom

(51) INT CL$^7$
B60R 13/10 , B60Q 1/50

(52) UK CL (Edition R)
G5C CFF

(56) Documents Cited
GB 2275806 A GB 2271012 A GB 0258122 A
US 5105179 A US 4631516 A US 4574269 A

(58) Field of Search
UK CL (Edition P) B7J J103 , G5C CBE CBK CBL CDBX CEQ CER CFF
INT CL$^6$ B60Q 1/50 1/56 , B60R 13/00 13/10 , G09F 21/04
ONLINE: WPI

(54) Abstract Title
Number Plate Providing Information About The Vehicle Driver

(57) Two-sided (different background colours on either side), reversible number plates 1 are a standardized, easy-to-change symbol on the exterior of a motor vehicle 2, which display the sex or other information concerning the driver. The plate is attached to the vehicle with 'quick-release', positive-lock clips 3, to enable the quick reversing of the plate when a driver of the opposite sex takes over, while ensuring secure attachment to the vehicle body to minimise risk of accidental detachment. The symbol makes the sex of drivers immediately apparent to other road users and will accordingly change the way they behave with each another; road users will improve their manners, become more polite, predict better the behaviour of other drivers, and thus reduce the frequency and severity of traffic accidents. Background colour can also be altered from within the vehicle using electro-luminescent liquid crystal or electro-reflective panels.