Recovering Deleted and Damaged Files (4e)

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

Student:	Email:
Karan Atul Vora	kxv230021@utdallas.edu

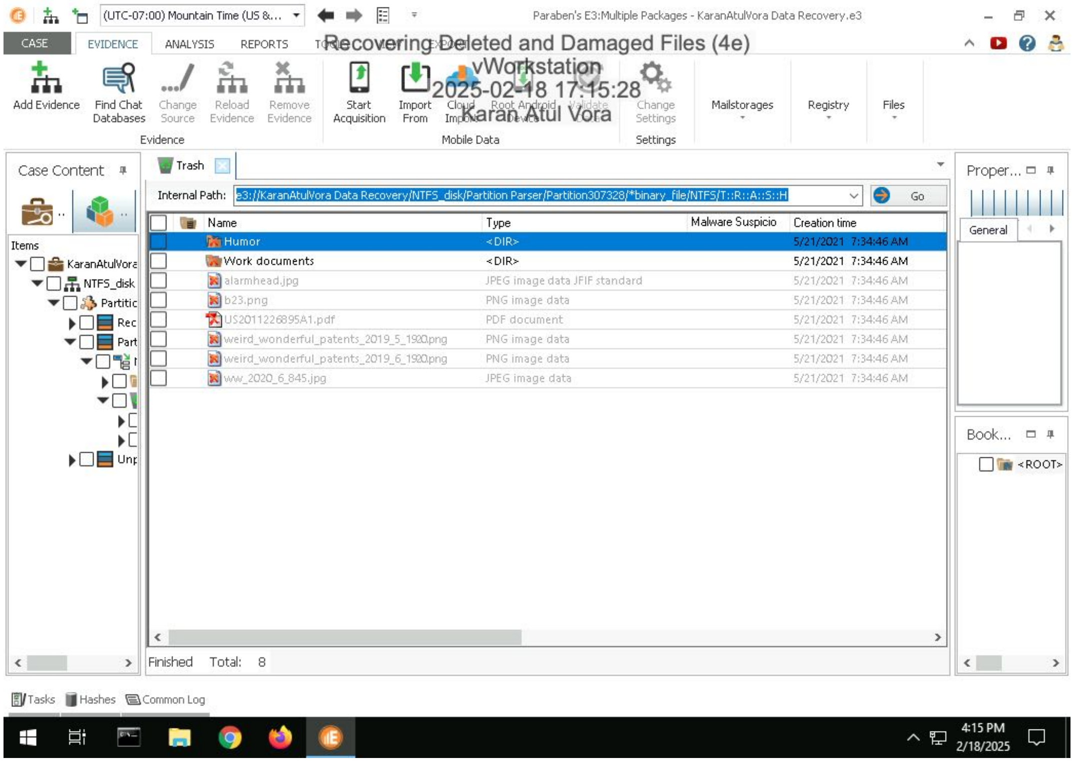
Time on Task:	Progress:
1 hour, 44 minutes	100%

Report Generated: Monday, February 24, 2025 at 4:31 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**.

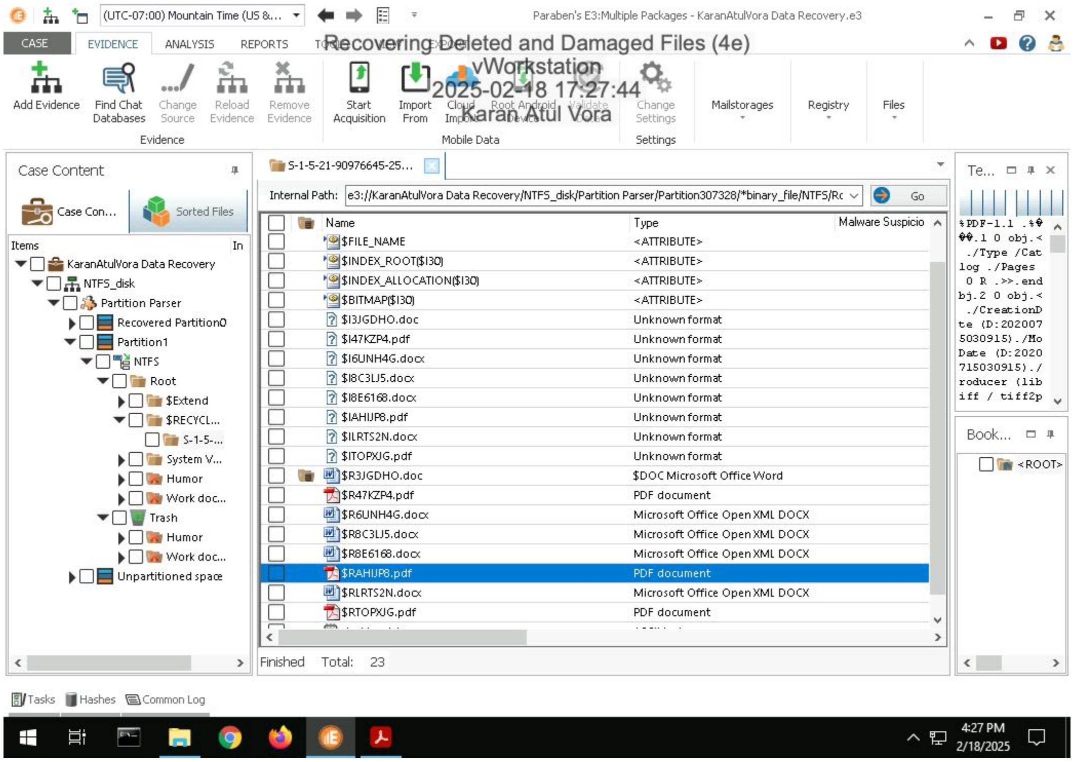


Internal Path: e3://KaranAtulVora Data Recovery/NTFS_disk/Partition Parser/Partition307328/*binary_file/NTFS/T::R::A::S::H

Name	Type	Malware Suspicio	Creation time
Humor	<DIR>		5/21/2021 7:34:46 AM
Work documents	<DIR>		5/21/2021 7:34:46 AM
alarmhead.jpg	JPEG image data JFIF standard		5/21/2021 7:34:46 AM
b23.png	PNG image data		5/21/2021 7:34:46 AM
US2011226895A1.pdf	PDF document		5/21/2021 7:34:46 AM
weird_wonderful_patents_2019_5_1920.png	PNG image data		5/21/2021 7:34:46 AM
weird_wonderful_patents_2019_6_1920.png	PNG image data		5/21/2021 7:34:46 AM
ww_2020_6_845.jpg	JPEG image data		5/21/2021 7:34:46 AM

Finished Total: 8

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



Recovering Deleted and Damaged Files (4e)
vWorkstation
2025-02-18 17:27:44
Karan Atul Vora

Items
- KaranAtulVora Data Recovery
  - NTFS_disk
    - Partition Parser
      - Recovered Partition0
      - Partition1
        - NTFS
          - Root
            - $Extend
            - $RECYCL...
              - S-1-5-...
            - System V...
            - Humor
            - Work doc...
          - Trash
            - Humor
            - Work doc...
      - Unpartitioned space

S-1-5-21-90976645-25...

Internal Path: e3://KaranAtulVora Data Recovery/NTFS_disk/Partition Parser/Partition307328/*binary_file/NTFS/Rc

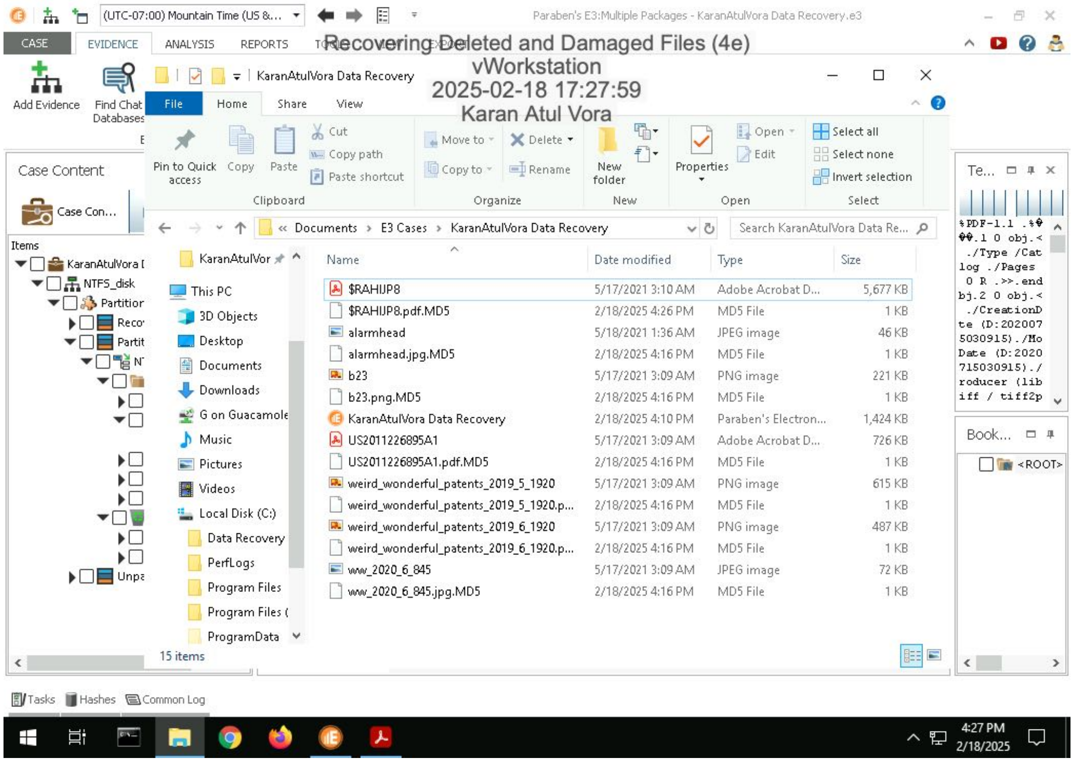
Name	Type	Malware Suspicio
$FILE_NAME	<ATTRIBUTE>	
$INDEX_ROOT($I30)	<ATTRIBUTE>	
$INDEX_ALLOCATION($I30)	<ATTRIBUTE>	
$BITMAP($I30)	<ATTRIBUTE>	
$I3JGDHO.doc	Unknown format	
$I47KZP4.pdf	Unknown format	
$I6UNH4G.docx	Unknown format	
$I8C3LJ5.docx	Unknown format	
$I8E6168.docx	Unknown format	
$IAHIJP8.pdf	Unknown format	
$ILRTS2N.docx	Unknown format	
$ITOPXJG.pdf	Unknown format	
$R3JGDHO.doc	$DOC Microsoft Office Word	
$R47KZP4.pdf	PDF document	
$R6UNH4G.docx	Microsoft Office Open XML DOCX	
$R8C3LJ5.docx	Microsoft Office Open XML DOCX	
$R8E6168.docx	Microsoft Office Open XML DOCX	
$RAHIJP8.pdf	PDF document	
$RLRTS2N.docx	Microsoft Office Open XML DOCX	
$RTOPXJG.pdf	PDF document	

Finished Total: 23

```
%PDF-1.1 .%@
@@.1 0 obj.<
./Type /Cat
log ./Pages
 0 R .>>.end
bj.2 0 obj.<
./CreationD
te (D:202007
5030915)./Mo
Date (D:2020
715030915)./
roducer (lib
iff / tiff2p
```

Book...
<ROOT>

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



Recovering Deleted and Damaged Files (4e)
vWorkstation
2025-02-18 17:27:59
Karan Atul Vora

« Documents › E3 Cases › KaranAtulVora Data Recovery

Search KaranAtulVora Data Re...

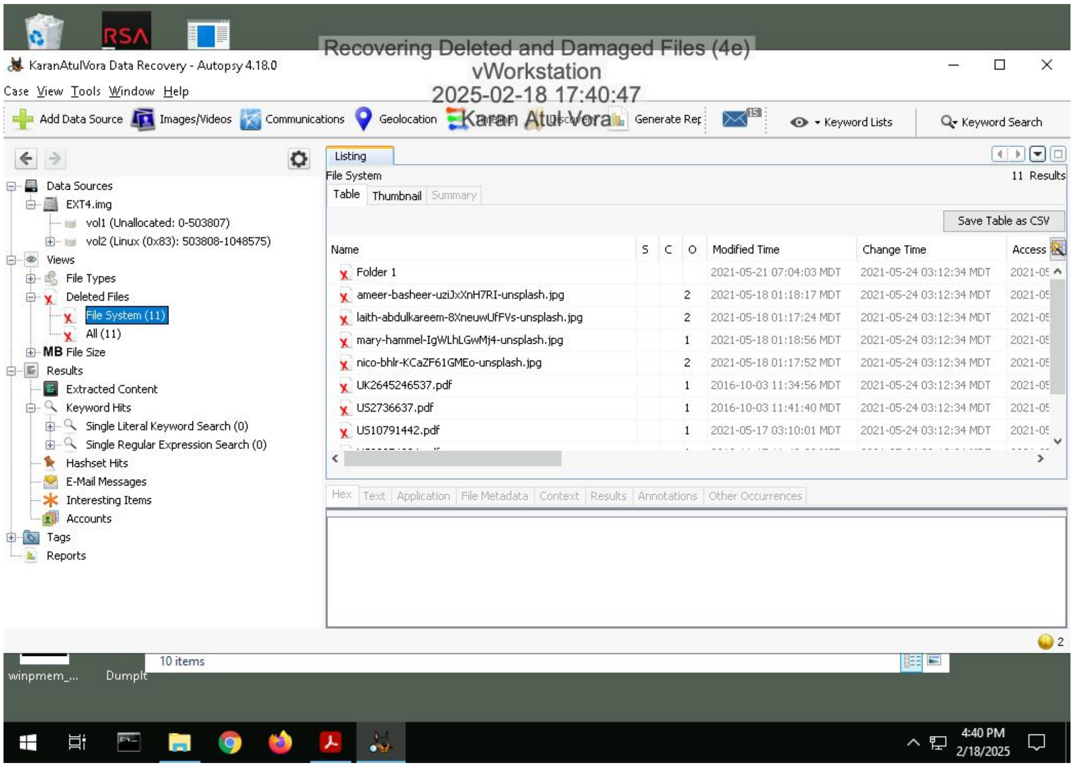
- KaranAtulVor
- This PC
- 3D Objects
- Desktop
- Documents
- Downloads
- G on Guacamole
- Music
- Pictures
- Videos
- Local Disk (C:)
- Data Recovery
- PerfLogs
- Program Files
- Program Files (
- ProgramData

Name	Date modified	Type	Size
$RAHIJP8	5/17/2021 3:10 AM	Adobe Acrobat D...	5,677 KB
$RAHIJP8.pdf.MD5	2/18/2025 4:26 PM	MD5 File	1 KB
alarmhead	5/18/2021 1:36 AM	JPEG image	46 KB
alarmhead.jpg.MD5	2/18/2025 4:16 PM	MD5 File	1 KB
b23	5/17/2021 3:09 AM	PNG image	221 KB
b23.png.MD5	2/18/2025 4:16 PM	MD5 File	1 KB
KaranAtulVora Data Recovery	2/18/2025 4:10 PM	Paraben's Electron...	1,424 KB
US2011226895A1	5/17/2021 3:09 AM	Adobe Acrobat D...	726 KB
US2011226895A1.pdf.MD5	2/18/2025 4:16 PM	MD5 File	1 KB
weird_wonderful_patents_2019_5_1920	5/17/2021 3:09 AM	PNG image	615 KB
weird_wonderful_patents_2019_5_1920.p...	2/18/2025 4:16 PM	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...	2/18/2025 4:16 PM	MD5 File	1 KB
ww_2020_6_845	5/17/2021 3:09 AM	JPEG image	72 KB
ww_2020_6_845.jpg.MD5	2/18/2025 4:16 PM	MD5 File	1 KB

15 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**.

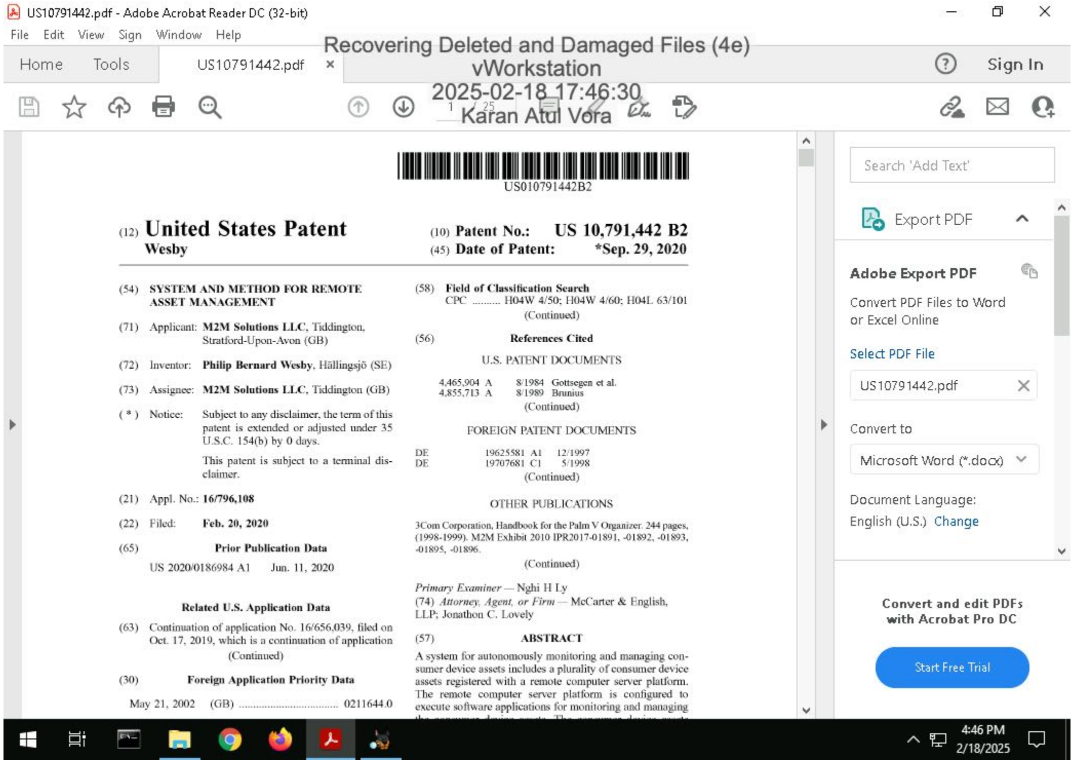


Recovering Deleted and Damaged Files (4e)
vWorkstation
2025-02-18 17:40:47
Karan Atul Vora

File System — 11 Results

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

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

(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

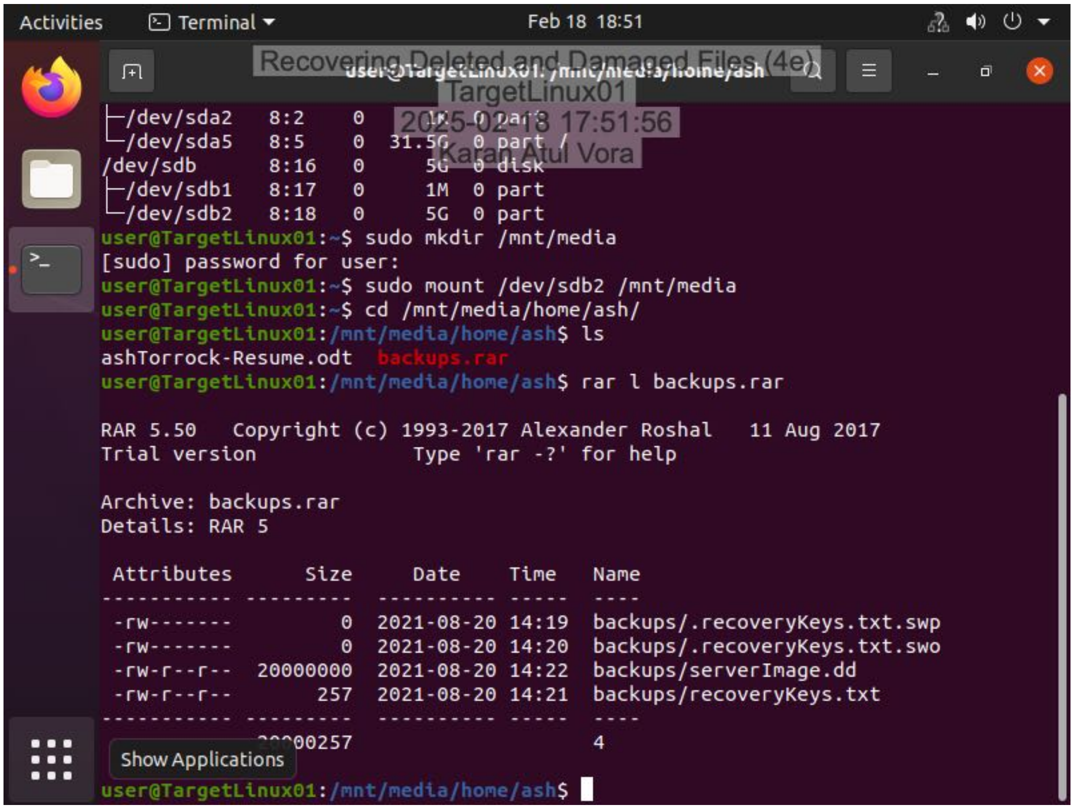
(57) **ABSTRACT**

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

Section 2: Applied Learning

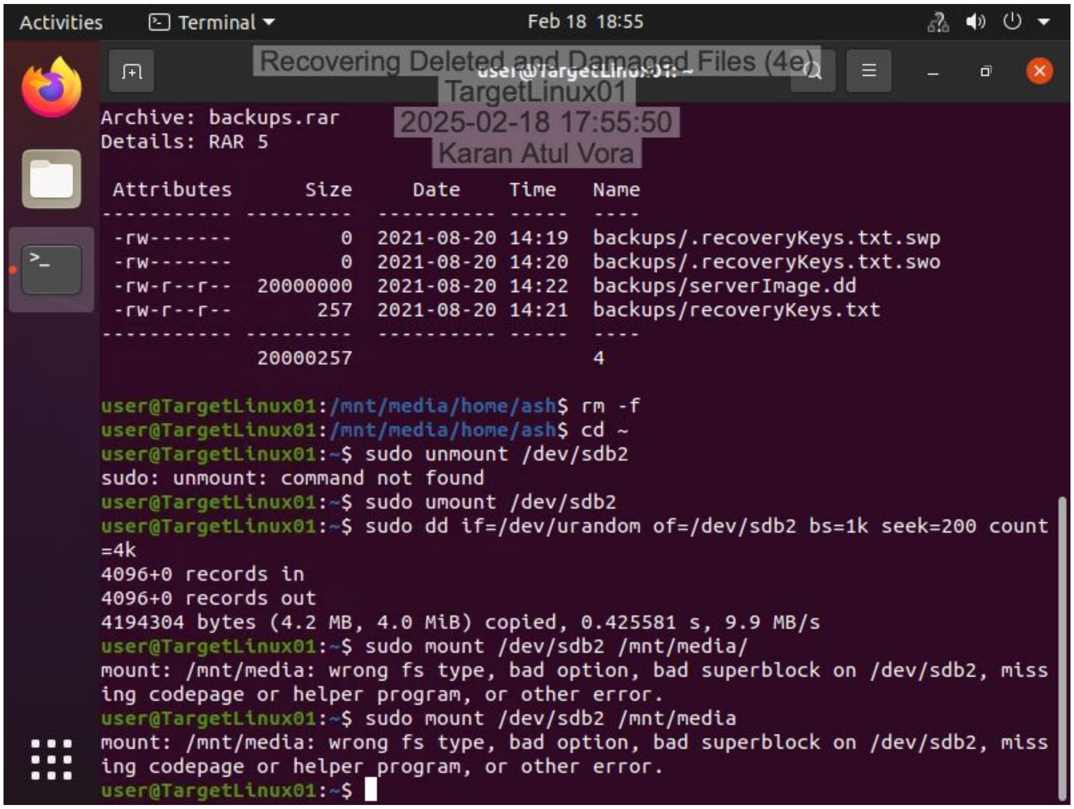
Part 1: Recover Deleted Files in Linux with PhotoRec

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



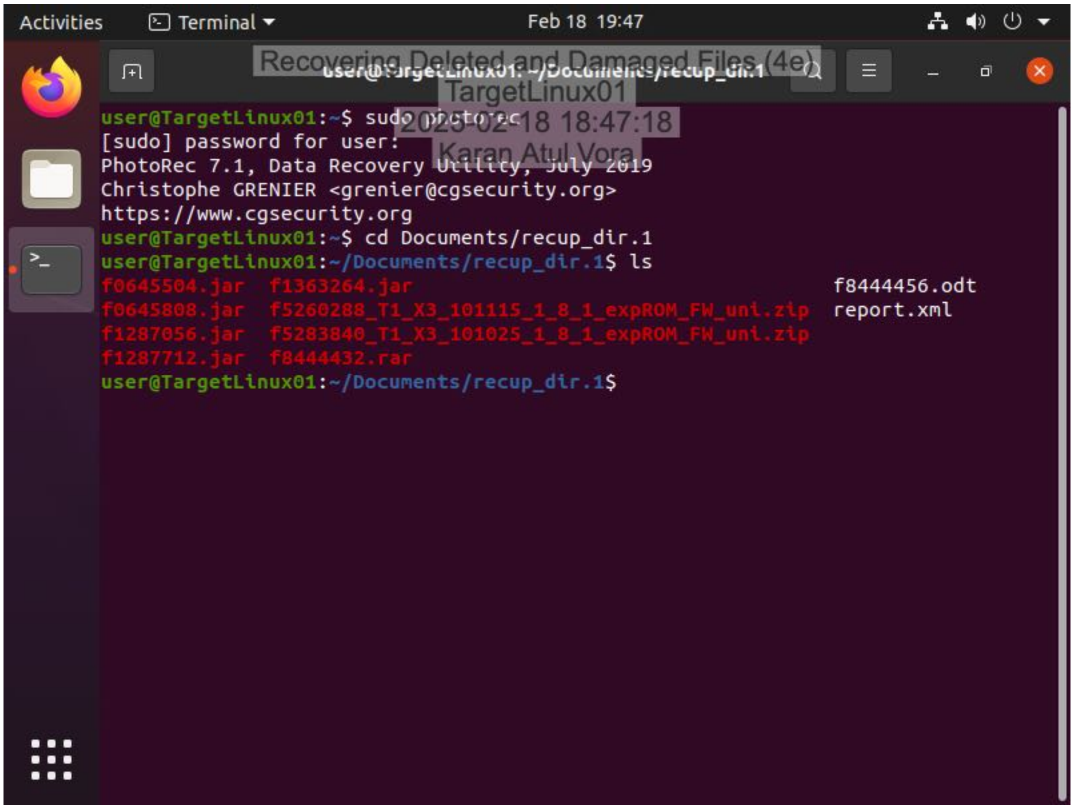
```
├─/dev/sda2   8:2    0     1K  0 part
└─/dev/sda5   8:5    0  31.5G  0 part /
/dev/sdb      8:16   0     5G  0 disk
├─/dev/sdb1   8:17   0     1M  0 part
└─/dev/sdb2   8:18   0     5G  0 part
user@TargetLinux01:~$ sudo mkdir /mnt/media
[sudo] password for user:
user@TargetLinux01:~$ sudo mount /dev/sdb2 /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

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

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



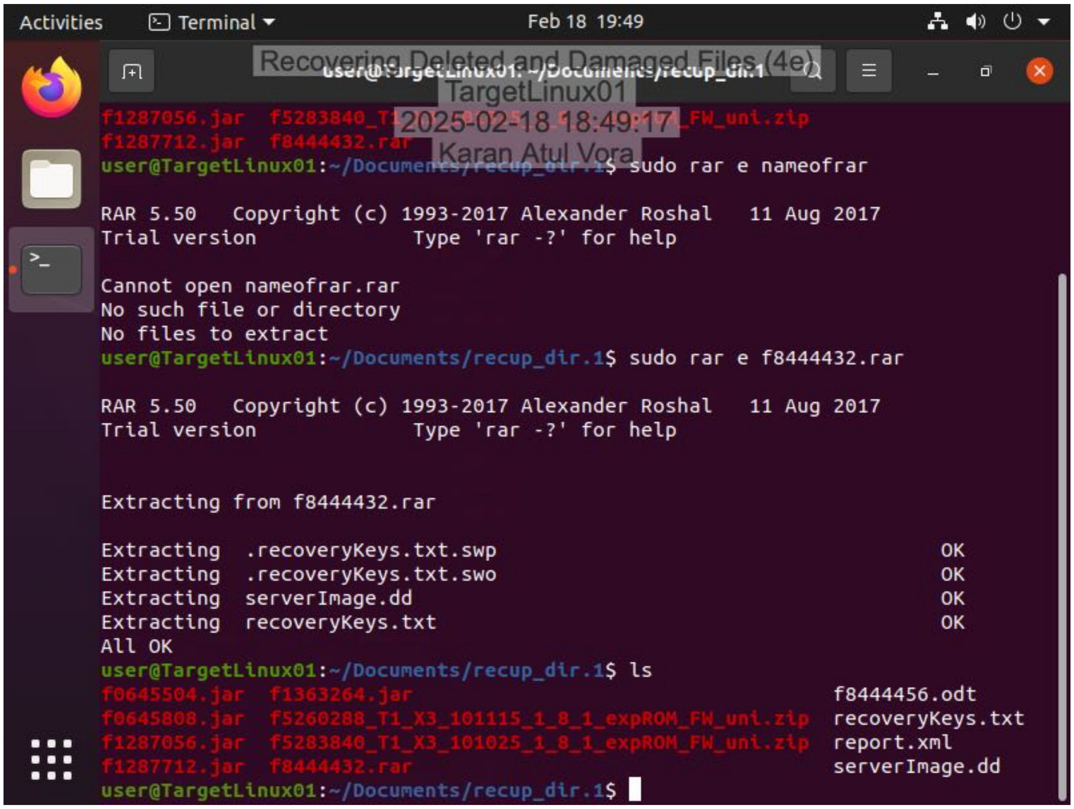
```
Archive: backups.rar
Details: RAR 5

 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, 0.425581 s, 9.9 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.
user@TargetLinux01:~$ 
```

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


Activities
Terminal
Feb 18 19:47
user@TargetLinux01: ~/Documents/recup_dir.1
Recovering Deleted and Damaged Files (4e)
TargetLinux01
2025-02-18 18:47:18
Karan Atul Vora

```
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
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**.

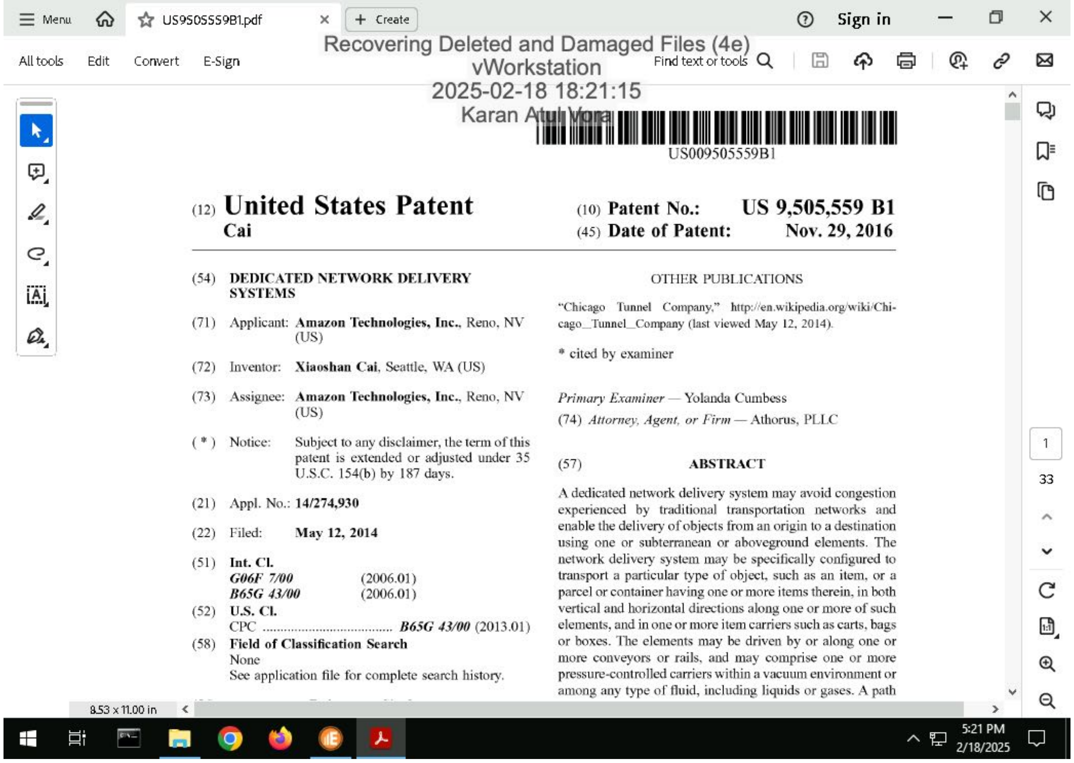

Activities
Terminal
Feb 18 19:49
user@TargetLinux01: ~/Documents/recup_dir.1
Recovering Deleted and Damaged Files (4e)
TargetLinux01
2025-02-18 18:49:17
Karan Atul Vora

```
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 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 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  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.

OTHER PUBLICATIONS

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

* cited by examiner

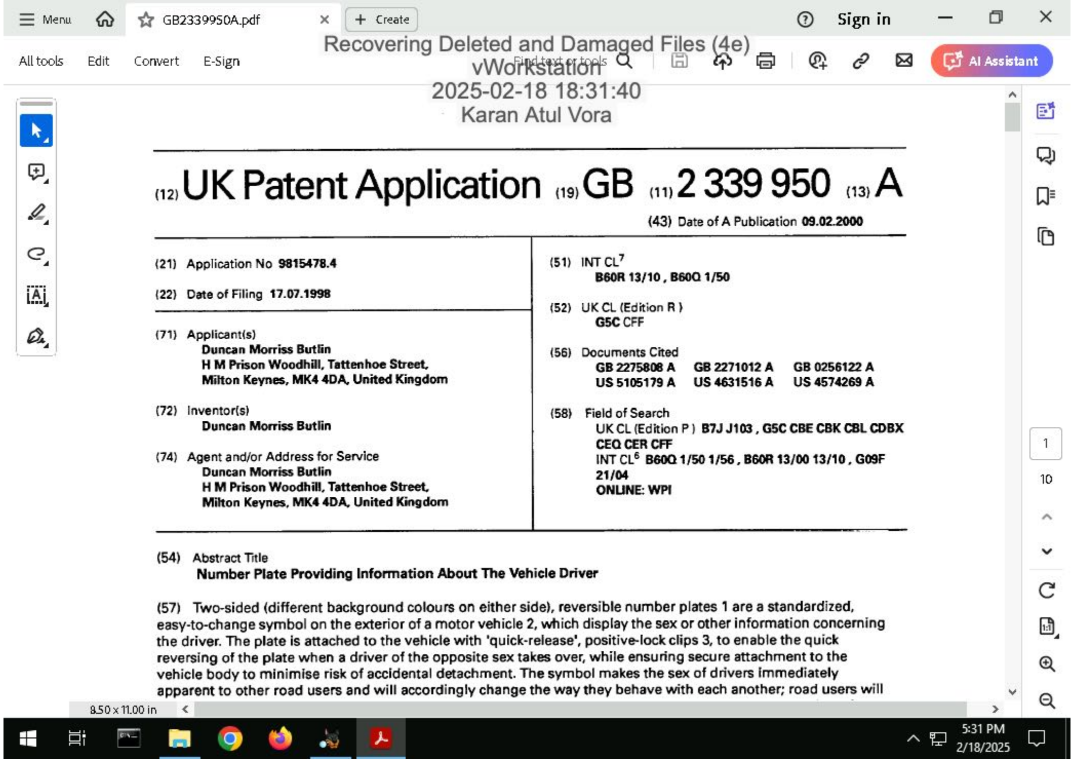
Primary Examiner — Yolanda Cumbess
(74) *Attorney, Agent, or Firm* — Athorus, PLLC

(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

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**.



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

(43) Date of A Publication **09.02.2000**

(21) Application No **9815478.4**

(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 2275808 A	**GB 2271012 A**	**GB 0256122 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