

Digital Evidence Analysis Report – drive2.E01

1. Overview

This digital forensic analysis was conducted on the disk image drive2.E01. The investigation involved:

- File system examination with FTK Imager
- Extraction of a raw image via ewfexport
- File recovery using Foremost
- Timeline construction based on FTK file metadata

2. Tools Used

FTK Imager	File system analysis, metadata export
ewfexport	Convert .E01 to .raw disk image
Foremost	Data carving (file recovery)
Excel	Timeline organization from FTK export

The .E01 image was successfully exported to raw format using:

- ewfexport drive2.E01
 - Output: drive2_raw.raw (996 MiB)
 - Export started: May 07, 2025 – 20:42:41
 - MD5 hash: 19328072609a68e60b67bad0b7c5f018

Screenshot:

```
[X]-[user@parrot]~[~/Desktop]
$ewfexport drive2.E01
ewfexport 20140813 Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
Information for export required, please provide the necessary input
Export to format (raw, files, ewf, smart, ftk, encase1, encase2, encase3, encase4, encase5, encase6, encase7, encase7-v2, linen5, linen6, linen7, ewfx) [raw]:
Target path and filename without extension or - for stdout: drive2_raw
Evidence segment file size in bytes (0 is unlimited) (0 B <= value <= 7.9 EiB) [0 B]:
Start export at offset (0 <= value <= 1044905984) [0]:
Number of bytes to export (0 <= value <= 1044905984) [1044905984]:

Export started at: May 07, 2025 20:42:41 and paste this URL in it:
This could take a while.
http://localhost:8080/autopsy
Status: at 43%.
Progress: exported 436 MiB (457179136 bytes) of total 996 MiB (1044905984 bytes).
Progress: completion in 5 second(s) with 110 MiB/s (116100664 bytes/second). Sector: 811
End time: Wed May 07 20:43:05 2025
Status: at 79%.
Progress: exported 787 MiB (826081280 bytes) of total 996 MiB (1044905984 bytes).
Progress: completion in 2 second(s) with 99 MiB/s (104490598 bytes/second).
Progress: 1044905984 bytes in 10 second(s) with 99 MiB/s (104490598 bytes/second).
Export completed at: May 07, 2025 20:42:51
Written: 996 MiB (1044905984 bytes) in 10 second(s) with 99 MiB/s (104490598 bytes/second).
MD5 hash calculated over data: 19328072609a68e60b67bad0b7c5f018
ewfexport: SUCCESS
```

4. File Carving with Foremost

Foremost was used to analyze and carve files from the raw disk image:

- `foremost -i drive2_raw.raw -o foremost_output`

Recovered Directories:

- `/dll/`
- `/exe/`
- `/png/`

 Audit Log: `foremost_output/audit.txt`

Screenshot:

```
[user@parrot]~[~/Desktop]
$foremost -i drive2_raw.raw -o foremost_output
Processing: drive2_raw.raw
*****
[user@parrot]~[~/Desktop]
$ls foremost_output data: 19328072609a68e60b67bad0b7c5f018
audit.txt: dll exe png
```

5. FTK File System Analysis

Using FTK Imager:

- Found system files in Windows\system32 (DLLs, XMLs, logs)
- No winevt\Logs present
- Observed .FileSlack artifacts and unallocated space

Screenshots:

Evidence Tree

- drive2.E01
 - NONAME [ext4]
 - [root]
 - \$RECYCLE.BIN
 - bin
 - boot
 - dev
 - Documents and Settings
 - etc
 - home
 - lost+found
 - sys
 - System Volume Information
 - tmp
 - Users
 - Admin
 - All Users
 - Default
 - Default Users
 - Public
 - usr
 - var
 - Windows
 - system32
 - [unallocated space]

File List

Name	Size	Type	Date Modified
ncryptui.dll	60,928 (60 KB)	Regular File	7/14/2009 1:16:04 AM
ncsi.dll	152,064 (149 KB)	Regular File	7/14/2009 1:16:04 AM
ndadmin.exe	75,264 (74 KB)	Regular File	7/14/2009 1:14:28 AM
ndadmin.exe.FileSlack	2,560 (3 KB)	File Slack	
nddeapi.dll	8,192 (8 KB)	Regular File	7/14/2009 1:16:04 AM
ndfapi.dll	200,192 (196 KB)	Regular File	7/14/2009 1:16:04 AM
ndfctw.dll	29,696 (29 KB)	Regular File	7/14/2009 1:16:04 AM
ndfctw.dll.FileSlack	3,072 (3 KB)	File Slack	
NdfEventView.xml	565 (1 KB)	Regular File	6/10/2009 9:18:30 PM
ndfhcdiscvery.dll	94,720 (93 KB)	Regular File	7/14/2009 1:16:04 AM
ndiscapCfg.dll	41,984 (41 KB)	Regular File	7/14/2009 1:16:04 AM
ndish.dll	71,168 (70 KB)	Regular File	7/14/2009 1:16:04 AM
ndproxystub.dll	12,288 (12 KB)	Regular File	7/14/2009 1:16:04 AM
ndptsp.tsp	50,688 (50 KB)	Regular File	7/14/2009 1:14:12 AM

Custom Content Sources

Evidence:File System[Path]... Options

New Edit Remove Remove All

Properties | Hex Value... Custom C...

Listed: 14 Selected: 0 drive2.E01/NONAME [ext4]/[root]/Windows/system32

Evidence Tree

- drive2.E01
 - NONAME [ext4]
 - [root]
 - \$RECYCLE.BIN
 - bin
 - boot
 - dev
 - Documents and Settings
 - etc
 - home
 - lost+found
 - sys
 - System Volume Information
 - tmp
 - Users
 - Admin
 - All Users
 - Default
 - Default Users
 - Public
 - usr
 - var
 - Windows
 - system32
 - [unallocated space]

File List

Name	Size	Type	Date Modified
004099	75,628,544 (73,856 KB)	Unallocated Space	
022564	41,799,680 (40,820 KB)	Unallocated Space	
033088	104,857,600 (102,400 KB)	Unallocated Space	
058688	28,053,504 (27,396 KB)	Unallocated Space	
069633	104,857,600 (102,400 KB)	Unallocated Space	
095233	12,582,912 (12,288 KB)	Unallocated Space	
098369	104,857,600 (102,400 KB)	Unallocated Space	
123969	104,857,600 (102,400 KB)	Unallocated Space	
149569	58,458,112 (57,088 KB)	Unallocated Space	
163905	104,857,600 (102,400 KB)	Unallocated Space	
189505	104,857,600 (102,400 KB)	Unallocated Space	
215105	58,458,112 (57,088 KB)	Unallocated Space	
229441	104,857,600 (102,400 KB)	Unallocated Space	
255041	258,048 (252 KB)	Unallocated Space	

Custom Content Sources

Evidence:File System[Path]... Options

New Edit Remove Remove All

Properties | Hex Value... Custom C...

Listed: 14 Selected: 0 drive2.E01/NONAME [ext4]/[root]/Windows/system32

The screenshot shows a forensic tool interface with a file list and a hex dump. The file list on the right shows files like system32, DPINST.LOG, DtcInstall.log, Enterprise.xml, msdfmap.ini, msdfmap.ini.FileSlack, PPRO.log, PPRO.log.FileSlack, setupact.log, setuperr.log, Starter.xml, system.ini, and TSSysprep.log. The hex dump at the bottom shows a list of files and their sizes, including system32, DPINST.LOG, DtcInstall.log, Enterprise.xml, msdfmap.ini, msdfmap.ini.FileSlack, PPRO.log, PPRO.log.FileSlack, setupact.log, setuperr.log, Starter.xml, system.ini, and TSSysprep.log.

- system32: DLLs and slack files
- Unallocated space segments
- Root and log files under Windows

6. Timeline of Activity

Using the exported fileListings.csv:

- Files last modified around July 2009 to October 2015
- setupact.log, PPRO.log, and Starter.xml show system activity logs
- Sorted timeline captured in spreadsheet form

Column 1	Filename	Full Path	Modified
0	[unallocated space]	NONAME [ext4]\[unallocated space]\	
18	149569	NONAME [ext4]\[unallocated space]\149569	
17	123969	NONAME [ext4]\[unallocated space]\123969	
16	98369	NONAME [ext4]\[unallocated space]\098369	
15	95233	NONAME [ext4]\[unallocated space]\095233	

14	69633	NONAME [ext4]\[unallocated space]\069633	
13	58688	NONAME [ext4]\[unallocated space]\058688	
12	33088	NONAME [ext4]\[unallocated space]\033088	
11	22564	NONAME [ext4]\[unallocated space]\022564	
19	163905	NONAME [ext4]\[unallocated space]\163905	
10	4099	NONAME [ext4]\[unallocated space]\004099	
22	229441	NONAME [ext4]\[unallocated space]\229441	
23	255041	NONAME [ext4]\[unallocated space]\255041	
6	boot record	NONAME [ext4]\boot record	
5	inode table	NONAME [ext4]\inode table	
4	inode bitmap	NONAME [ext4]\inode bitmap	
3	block bitmap	NONAME [ext4]\block bitmap	
2	group descriptor table	NONAME [ext4]\group descriptor table	
1	superblock	NONAME [ext4]\superblock	
21	215105	NONAME [ext4]\[unallocated space]\215105	
20	189505	NONAME [ext4]\[unallocated space]\189505	
66	ndptsp.tsp	NONAME [ext4]\[root]\Windows\system32\ndptsp.tsp	2009-Jul-14 01:14:12 UTC
57	ndadmin.exe	NONAME [ext4]\[root]\Windows\system32\ndadmin.exe	2009-Jul-14 01:14:28 UTC
65	ndproxystub.dll	NONAME [ext4]\[root]\Windows\system32\ndproxystub.dll	2009-Jul-14 01:16:04 UTC
64	ndishc.dll	NONAME [ext4]\[root]\Windows\system32\ndishc.dll	2009-Jul-14 01:16:04 UTC

63	ndiscapCfg.dll	NONAME [ext4]\[root]\Windows\system32\ndiscapCfg.dll	2009-Jul-14 01:16:04 UTC
62	ndfhcdiscovery.dll	NONAME [ext4]\[root]\Windows\system32\ndfhcdiscovery.dll	2009-Jul-14 01:16:04 UTC
60	ndfetw.dll	NONAME [ext4]\[root]\Windows\system32\ndfetw.dll	2009-Jul-14 01:16:04 UTC
59	ndfapi.dll	NONAME [ext4]\[root]\Windows\system32\ndfapi.dll	2009-Jul-14 01:16:04 UTC
58	nddeapi.dll	NONAME [ext4]\[root]\Windows\system32\nddeapi.dll	2009-Jul-14 01:16:04 UTC
56	ncsi.dll	NONAME [ext4]\[root]\Windows\system32\ncsi.dll	2009-Jul-14 01:16:04 UTC
55	ncryptui.dll	NONAME [ext4]\[root]\Windows\system32\ncryptui.dll	2009-Jul-14 01:16:04 UTC
50	setuperr.log	NONAME [ext4]\[root]\Windows\setuperr.log	2009-Jul-14 04:39:10 UTC
46	Enterprise.xml	NONAME [ext4]\[root]\Windows\Enterprise.xml	2009-Jun-10 21:14:32 UTC
51	Starter.xml	NONAME [ext4]\[root]\Windows\Starter.xml	2009-Jun-10 21:14:46 UTC
61	NdfEventView.xml	NONAME [ext4]\[root]\Windows\system32\NdfEventView.xml	2009-Jun-10 21:18:30 UTC
47	msdfmap.ini	NONAME [ext4]\[root]\Windows\msdfmap.ini	2009-Jun-10 21:19:28 UTC
52	system.ini	NONAME [ext4]\[root]\Windows\system.ini	2009-Jun-10 21:46:30 UTC
45	DtcInstall.log	NONAME [ext4]\[root]\Windows\DtcInstall.log	2011-Nov-23 16:13:36 UTC
53	TSSysprep.log	NONAME [ext4]\[root]\Windows\TSSysprep.log	2011-Nov-23 16:14:44 UTC
44	DPINST.LOG	NONAME [ext4]\[root]\Windows\DPINST.LOG	2012-Jan-19 19:21:10 UTC

48	PFR0.log	NONAME [ext4]\[root]\Windows\PFR0.log	2015-Aug-14 03:10:16 UTC
49	setupact.log	NONAME [ext4]\[root]\Windows\setupact.log	2015-Oct-07 15:50:40 UTC
31	\$RECYCLE.BIN	NONAME [ext4]\[root]\\$RECYCLE.BIN\	2015-Oct-07 16:26:24 UTC
26	Boot	NONAME [ext4]\[root]\Boot\	2015-Oct-07 16:26:36 UTC
33	System Volume Information	NONAME [ext4]\[root]\System Volume Information\	2015-Oct-07 16:26:46 UTC
28	Documents and Settings	NONAME [ext4]\[root]\Documents and Settings\	2015-Oct-07 16:27:16 UTC
25	bin	NONAME [ext4]\[root]\bin\	2015-Oct-07 16:30:36 UTC
27	dev	NONAME [ext4]\[root]\dev\	2015-Oct-07 16:30:40 UTC
29	etc	NONAME [ext4]\[root]\etc\	2015-Oct-07 16:30:44 UTC
30	home	NONAME [ext4]\[root]\home\	2015-Oct-07 16:30:50 UTC
36	usr	NONAME [ext4]\[root]\usr\	2015-Oct-07 16:31:00 UTC
34	tmp	NONAME [ext4]\[root]\tmp\	2015-Oct-07 16:31:04 UTC
37	var	NONAME [ext4]\[root]\var\	2015-Oct-07 16:31:14 UTC
32	sys	NONAME [ext4]\[root]\sys\	2015-Oct-07 16:31:18 UTC
24	lost+found	NONAME [ext4]\[root]\lost+found\	2015-Oct-07 16:40:36 UTC
8	bad blocks	NONAME [ext4]\bad blocks	2015-Oct-07 16:40:36 UTC
9	journal	NONAME [ext4]\journal	2015-Oct-07 16:40:36 UTC
38	Windows	NONAME [ext4]\[root]\Windows\	2015-Oct-07 16:43:30 UTC
40	All Users	NONAME [ext4]\[root]\Users\All Users\	2015-Oct-07 16:44:18 UTC
41	Default	NONAME [ext4]\[root]\Users\Default\	2015-Oct-07 16:44:26

			UTC
42	Default Users	NONAME [ext4]\[root]\Users\Default Users\	2015-Oct-07 16:44:30 UTC
43	Public	NONAME [ext4]\[root]\Users\Public\	2015-Oct-07 16:44:36 UTC
35	Users	NONAME [ext4]\[root]\Users\	2015-Oct-07 16:44:42 UTC
39	Admin	NONAME [ext4]\[root]\Users\Admin\	2015-Oct-07 16:44:42 UTC
54	system32	NONAME [ext4]\[root]\Windows\system32\	2015-Oct-07 16:47:38 UTC
7	[root]	NONAME [ext4]\[root]\	2015-Oct-07 16:59:40 UTC

7. Key Findings

- No user-specific files found in typical locations (Documents, Desktop)
- Files recovered through carving include executables and images
- System artifacts and log timestamps suggest a setup or recovery partition
- File slack and unallocated space may contain remnants of deleted data

8. Conclusion

drive2.E01 appears to be a limited Windows volume with minimal user interaction and notable system configuration logs. Despite the absence of typical event logs, the timeline and recovered artifacts provide insight into operational activity. Data carving recovered executable and image files, demonstrating the value of analyzing unallocated disk space.