WINDOWS AND LINUX ARTIFACT DEEP DIVE

INFRASTRUCTURE AND SECURITY - FORENSICS INVESTIGATOR

DEPI GRADUATION PROJECT

REPORT THREE

COMPARATIVE FORENSICS

Prepared by:

Mohamed Rabia

Windows and Linux Artifact Deep Dive

Contents

About The Project

This work is part of the forensic investigation track within the **Digital Egypt Pioneers Initiative (DEPI)** and reflects a collaborative effort carried out with a professional, team-oriented approach.

The project aims to study and analyze digital evidence across both Windows and Linux operating systems.

This work represents our **graduation project** for the **DEPI Digital Forensics Track**, demonstrating our ability to apply real forensic methodologies, analyze system artifacts, and work effectively as a coordinated investigation team.

The work is organized into a structured four-week workflow, where each week focuses on a specific forensic domain.

The four-week structure of the project is as follows:

❖ **Week 1 – Windows Forensics**
Deep investigation of Windows volatile and non-volatile artifacts, including memory acquisition, registry analysis, jump lists, shellbags, and browser data.

❖ **Week 2 – Linux Forensics**
Forensic examination of a Linux environment, covering EXT4 filesystem analysis, log inspection, deleted history recovery, and RAM acquisition.

❖ **Week 3 – Comparative Forensics**
Cross-platform comparison of Windows and Linux artifacts, focusing on timestamp formats, user activity trails, evidence value, and tool compatibility.

❖ **Week 4 – Consolidated Reporting & Final Review**
Compilation of all findings into a unified forensic guide, including legal considerations and a complete professional analysis of both operating systems.

Week 3 Report: Comparative Forensics

1. Introduction

Digital forensics relies heavily on understanding how different operating systems record, store, and represent user activity.

Each platform, Windows, Linux, or macOS, maintains unique artifacts that reflect user behavior, system events, and application interactions. These differences affect how investigators extract evidence, interpret timestamp formats, handle encoding variations, and select compatible forensic tools.

During Week 3, the focus was on Comparative Forensics, emphasizing the systematic comparison of OS artifacts to understand their evidentiary value and the challenges they pose in an investigation. This week explored how user activity is traced across operating systems, how timestamps and encoding formats vary, and how forensic tools interact differently with each platform.

This report analyzes how different operating systems record and manage digital evidence. It focuses on three main areas:

1. the key differences in user activity artifacts such as browser history, command-line usage, system logs, execution traces, and file metadata;
2. variations in timestamp and encoding formats that affect timeline reconstruction;
3. The compatibility of major forensic tools when acquiring and analyzing artifacts across platforms.

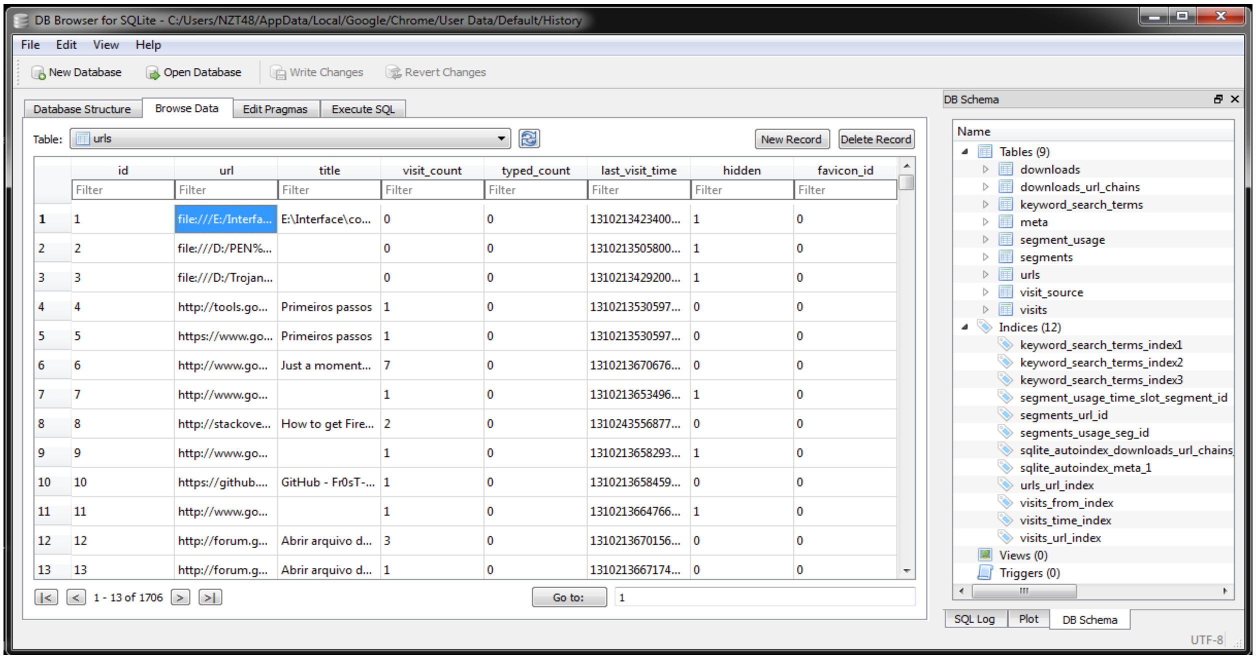
By comparing these factors, the report helps investigators select appropriate tools, anticipate OS-specific challenges, and accurately interpret evidence. It concludes with a presentation overview and an artifact comparison matrix summarizing findings across systems.

2. Identify Key Differences in User Activity Trails

1.2 Browser History Artifacts:

Windows

- **Path:** %USER%/AppData/Local/Google/Chrome/User Data/Default/History
- **Format:** SQLite database
- **Additional Artifacts:** Cookies, Cache, Login Data (SQLite)
- **Notes:** Windows often stores crash reports, session files, and Prefetch related to browser execution.



DB Browser for SQLite - C:/Users/NZT48/AppData/Local/Google/Chrome/User Data/Default/History

Table: urls

	id	url	title	visit_count	typed_count	last_visit_time	hidden	favicon_id
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	file:///E:/Interfa...	E:\Interface\co...	0	0	1310213423400...	1	0
2	2	file:///D:/PEN%...		0	0	1310213505800...	1	0
3	3	file:///D:/Trojan...		0	0	1310213429200...	1	0
4	4	http://tools.go...	Primeiros passos	1	0	1310213530597...	0	0
5	5	https://www.go...	Primeiros passos	1	0	1310213530597...	0	0
6	6	http://www.go...	Just a moment...	7	0	1310213670676...	0	0
7	7	http://www.go...		1	0	1310213653496...	1	0
8	8	http://stackove...	How to get Fire...	2	0	1310243556877...	0	0
9	9	http://www.go...		1	0	1310213658293...	1	0
10	10	https://github....	GitHub - Fr0sT-...	1	0	1310213658459...	0	0
11	11	http://www.go...		1	0	1310213664766...	1	0
12	12	http://forum.g...	Abrir arquivo d...	3	0	1310213670156...	0	0
13	13	http://forum.g...	Abrir arquivo d...	1	0	1310213667174...	0	0

|< < 1 - 13 of 1706 > >|

Go to: 1

DB Schema

Name
- Tables (9)
  - downloads
  - downloads_url_chains
  - keyword_search_terms
  - meta
  - segment_usage
  - segments
  - urls
  - visit_source
  - visits
- Indices (12)
  - keyword_search_terms_index1
  - keyword_search_terms_index2
  - keyword_search_terms_index3
  - segment_usage_time_slot_segment_id
  - segments_url_id
  - segments_usage_seg_id
  - sqlite_autoindex_downloads_url_chains
  - sqlite_autoindex_meta_1
  - urls_url_index
  - visits_from_index
  - visits_time_index
  - visits_url_index
- Views (0)
- Triggers (0)

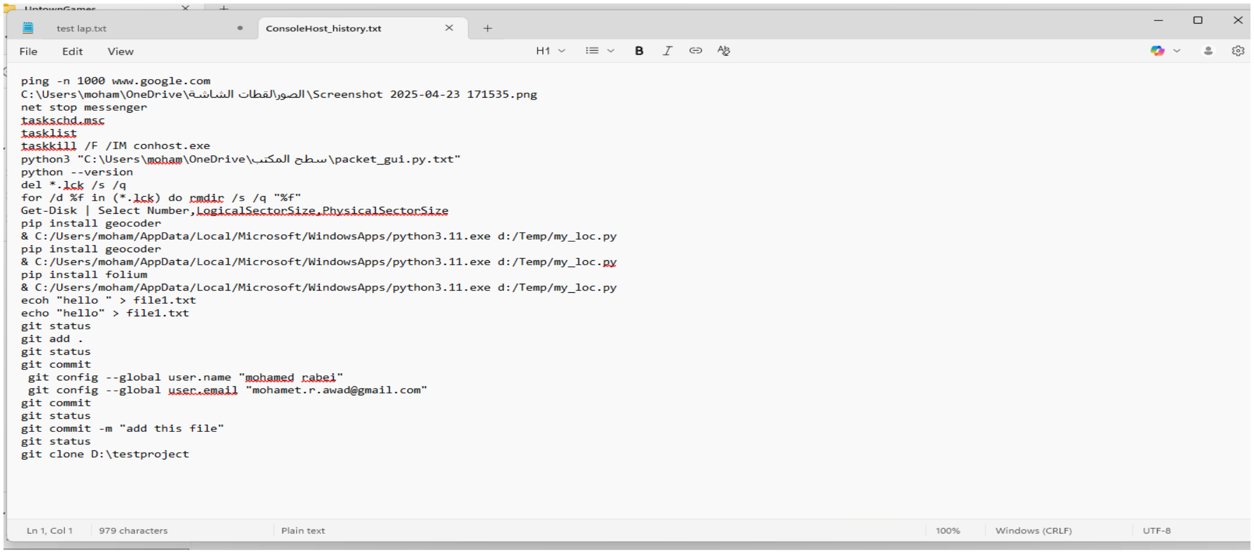
Linux

- **Path:** ~/.config/google-chrome/Default/History
- **Format:** SQLite
- **Notes:** Typically cleaner structure; fewer OS-level artifacts compared to Windows.

2.2 Shell / Command History

Windows

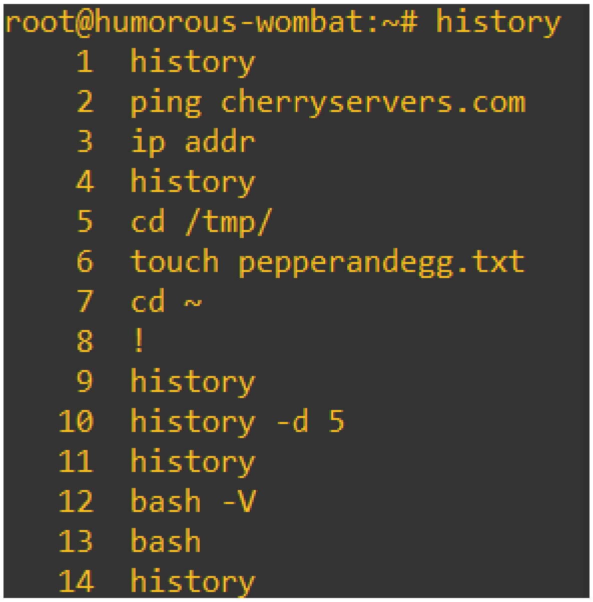
- **PowerShell History:**
  - Path: %APPDATA%/Microsoft/Windows/PowerShell/PSReadLine/ConsoleHost_history.txt
  - Format: UTF-8 text
- **CMD:** No persistent history by default.
- **Notes:** PowerShell history includes commands but not timestamps unless configured.



```
ping -n 1000 www.google.com
C:\Users\moham\OneDrive\الصور\لقطات الشاشة\Screenshot 2025-04-23 171535.png
net stop messenger
taskschd.msc
tasklist
taskkill /F /IM conhost.exe
python3 "C:\Users\moham\OneDrive\سطح المكتب\packet_gui.py.txt"
python --version
del *.lck /s /q
for /d %f in (*.lck) do rmdir /s /q "%f"
Get-Disk | Select Number,LogicalSectorSize,PhysicalSectorSize
pip install geocoder
& C:/Users/moham/AppData/Local/Microsoft/WindowsApps/python3.11.exe d:/Temp/my_loc.py
pip install geocoder
& C:/Users/moham/AppData/Local/Microsoft/WindowsApps/python3.11.exe d:/Temp/my_loc.py
pip install folium
& C:/Users/moham/AppData/Local/Microsoft/WindowsApps/python3.11.exe d:/Temp/my_loc.py
ecoh "hello " > file1.txt
echo "hello" > file1.txt
git status
git add .
git status
git commit
 git config --global user.name "mohamed rabei"
 git config --global user.email "mohamet.r.awad@gmail.com"
git commit
git status
git commit -m "add this file"
git status
git clone D:\testproject
```

Linux

- **Bash/Zsh History:**
  - ~/.bash_history
  - ~/.zsh_history
- **Format: plain text**; may include timestamps if HISTTIMEFORMAT is enabled.

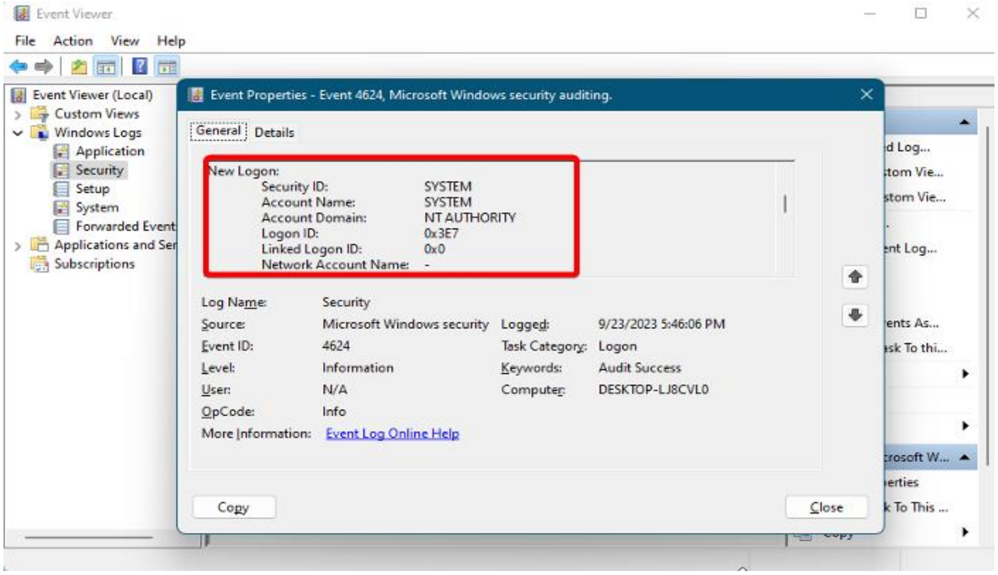


```
root@humorous-wombat:~# history
    1  history
    2  ping cherryservers.com
    3  ip addr
    4  history
    5  cd /tmp/
    6  touch pepperandegg.txt
    7  cd ~
    8  !
    9  history
   10  history -d 5
   11  history
   12  bash -V
   13  bash
   14  history
```

3.2 System Logs and Authentication Records

Windows

- **Windows Event Logs:**
  - Path: C:/Windows/System32/winevt/Logs/*.evtx
  - Format: EVTX (binary)
  - Categories: Security, System, Application
- **Notes:** Extremely detailed (logon types, privileges, services, auditing).

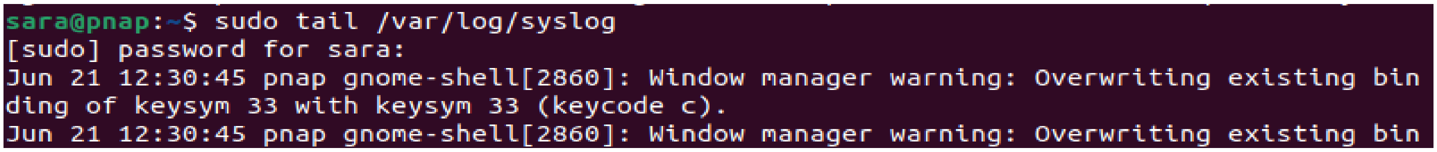


```
New Logon:
        Security ID:            SYSTEM
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:               0x3E7
        Linked Logon ID:        0x0
        Network Account Name:   -
```

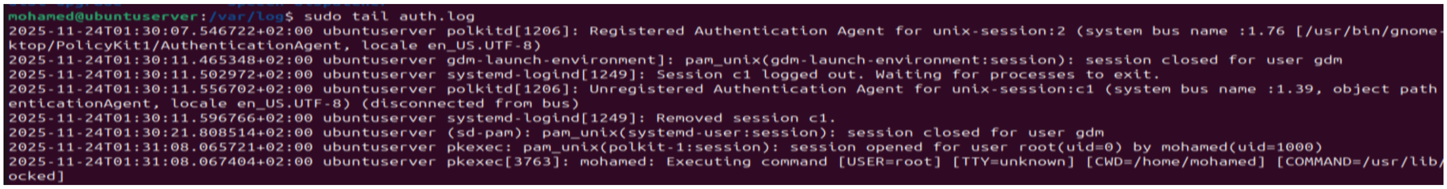
```
Log Name:          Security
Source:            Microsoft Windows security    Logged:         9/23/2023 5:46:06 PM
Event ID:          4624                          Task Category:  Logon
Level:             Information                   Keywords:       Audit Success
User:              N/A                           Computer:       DESKTOP-LJ8CVL0
OpCode:            Info
More Information:  Event Log Online Help
```

Linux

- **Syslog-based logs:**
  - /var/log/auth.log
  - /var/log/syslog
- **Systemd journal:**
  - Binary logs accessed via journalct



```
sara@pnap:~$ sudo tail /var/log/syslog
[sudo] password for sara:
Jun 21 12:30:45 pnap gnome-shell[2860]: Window manager warning: Overwriting existing bin
ding of keysym 33 with keysym 33 (keycode c).
Jun 21 12:30:45 pnap gnome-shell[2860]: Window manager warning: Overwriting existing bin
```

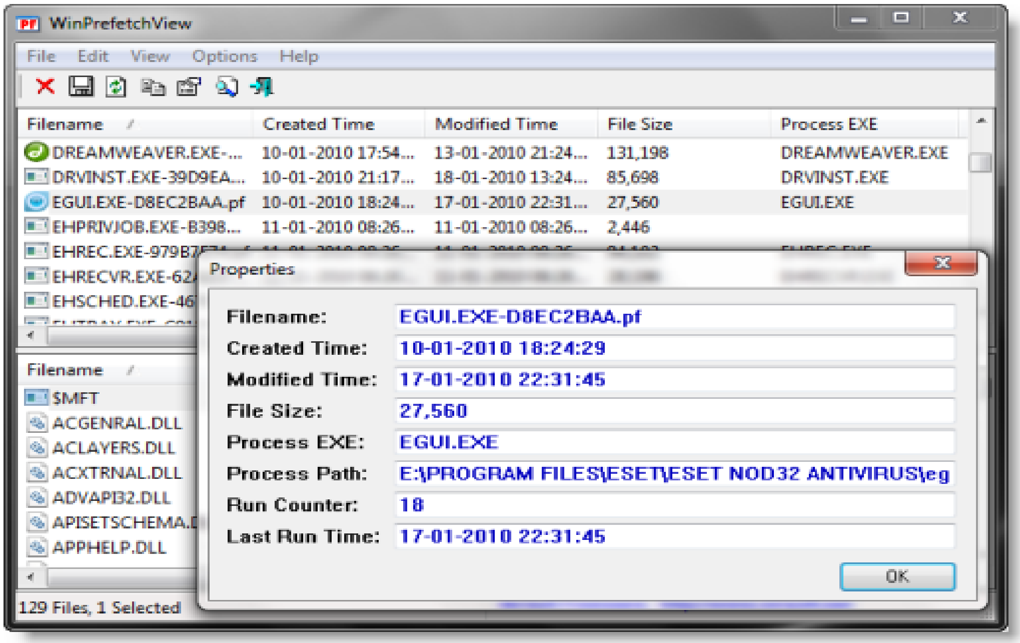


```
mohamed@ubuntuserver:/var/log$ sudo tail auth.log
2025-11-24T01:30:07.546722+02:00 ubuntuserver polkitd[1206]: Registered Authentication Agent for unix-session:2 (system bus name :1.76 [/usr/bin/gnome-
ktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
2025-11-24T01:30:11.465348+02:00 ubuntuserver gdm-launch-environment]: pam_unix(gdm-launch-environment:session): session closed for user gdm
2025-11-24T01:30:11.502972+02:00 ubuntuserver systemd-logind[1249]: Session c1 logged out. Waiting for processes to exit.
2025-11-24T01:30:11.556702+02:00 ubuntuserver polkitd[1206]: Unregistered Authentication Agent for unix-session:c1 (system bus name :1.39, object path
enticationAgent, locale en_US.UTF-8) (disconnected from bus)
2025-11-24T01:30:11.596766+02:00 ubuntuserver systemd-logind[1249]: Removed session c1.
2025-11-24T01:30:21.808514+02:00 ubuntuserver (sd-pam): pam_unix(systemd-user:session): session closed for user gdm
2025-11-24T01:31:08.065721+02:00 ubuntuserver pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by mohamed(uid=1000)
2025-11-24T01:31:08.067404+02:00 ubuntuserver pkexec[3763]: mohamed: Executing command [USER=root] [TTY=unknown] [CWD=/home/mohamed] [COMMAND=/usr/lib/
ocked]
```

4.2 Execution Artifacts

Windows

- **Prefetch:**
  - Path: `C:/Windows/Prefetch/*.pf`
  - Shows program execution count + last run time.



WinPrefetchView

Filename	Created Time	Modified Time	File Size	Process EXE
DREAMWEAVER.EXE-...	10-01-2010 17:54...	13-01-2010 21:24...	131,198	DREAMWEAVER.EXE
DRVINST.EXE-39D9EA...	10-01-2010 21:17...	18-01-2010 13:24...	85,698	DRVINST.EXE
EGUI.EXE-D8EC2BAA.pf	10-01-2010 18:24...	17-01-2010 22:31...	27,560	EGUI.EXE
EHPRIVJOB.EXE-B398...	11-01-2010 08:26...	11-01-2010 08:26...	2,446	
EHREC.EXE-979B7				
EHRECVR.EXE-62				
EHSCHED.EXE-46				

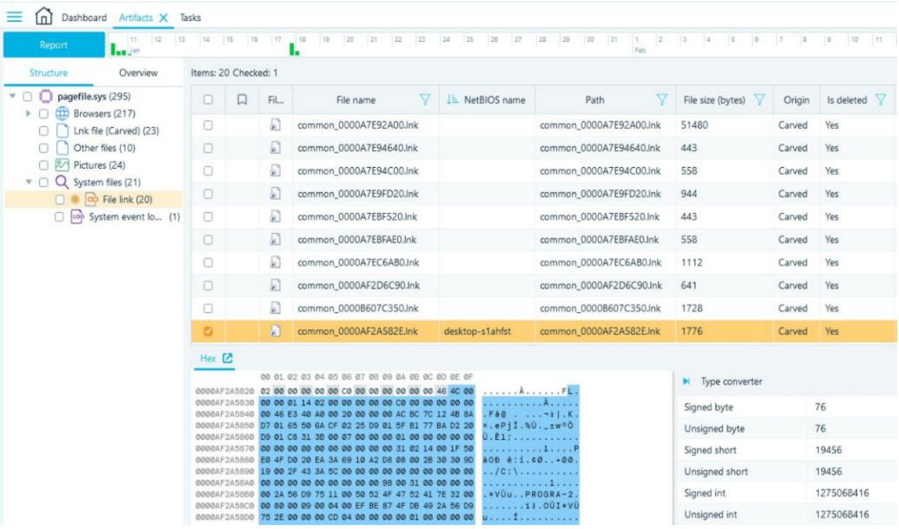
Filename
$MFT
ACGENRAL.DLL
ACLAYERS.DLL
ACXTRNAL.DLL
ADVAPI32.DLL
APISETSCHEMA.D
APPHELP.DLL

129 Files, 1 Selected

Properties

Filename:	EGUI.EXE-D8EC2BAA.pf
Created Time:	10-01-2010 18:24:29
Modified Time:	17-01-2010 22:31:45
File Size:	27,560
Process EXE:	EGUI.EXE
Process Path:	E:\PROGRAM FILES\ESET\ESET NOD32 ANTIVIRUS\eg
Run Counter:	18
Last Run Time:	17-01-2010 22:31:45

- **LNK (Shortcut Files):**
  - Contain paths, timestamps, and working directory.



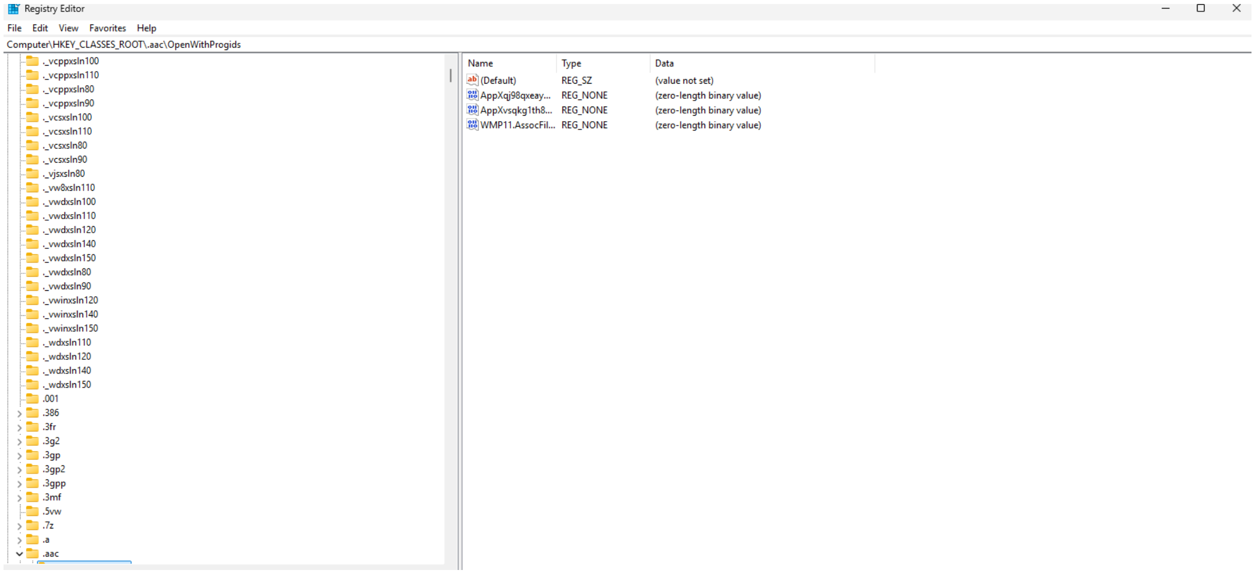
Items: 20 Checked: 1

		Fil...	File name	NetBIOS name	Path	File size (bytes)	Origin	Is deleted
□			common_0000A7E92A00.lnk		common_0000A7E92A00.lnk	51480	Carved	Yes
□			common_0000A7E94640.lnk		common_0000A7E94640.lnk	443	Carved	Yes
□			common_0000A7E94C00.lnk		common_0000A7E94C00.lnk	558	Carved	Yes
□			common_0000A7E9FD20.lnk		common_0000A7E9FD20.lnk	944	Carved	Yes
□			common_0000A7EBF520.lnk		common_0000A7EBF520.lnk	443	Carved	Yes
□			common_0000A7EBFAE0.lnk		common_0000A7EBFAE0.lnk	558	Carved	Yes
□			common_0000A7EC6AB0.lnk		common_0000A7EC6AB0.lnk	1112	Carved	Yes
□			common_0000AF2D6C90.lnk		common_0000AF2D6C90.lnk	641	Carved	Yes
□			common_0000B607C350.lnk		common_0000B607C350.lnk	1728	Carved	Yes
☑			common_0000AF2A582E.lnk	desktop-s1ahfst	common_0000AF2A582E.lnk	1776	Carved	Yes

```
            00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0000AF2A5820 02 00 00 00 00 00 C0 00 00 00 00 00 00 46 4C 00  .......À......FL.
0000AF2A5830 00 00 01 14 02 00 00 00 00 00 C0 00 00 00 00 00  ...........À.....
0000AF2A5840 00 46 E3 40 A0 00 20 00 00 00 AC BC 7C 12 4B 8A  .Fã@ . ...¬¼|.K.
0000AF2A5850 D7 01 65 50 6A CF 02 25 D9 01 5F B1 77 BA D2 20  ×.ePjÏ.%Ù._±wºÒ
0000AF2A5860 D9 01 C8 31 3B 00 07 00 00 00 01 00 00 00 00 00  Ù.È1;...........
0000AF2A5870 00 00 00 00 00 00 00 00 00 00 31 02 14 00 1F 50  ..........1....P
0000AF2A5880 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D  àOÐ ê:i.¢Ø..+00.
0000AF2A5890 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 00 00  ../C:\..........
0000AF2A58A0 00 00 00 00 00 00 00 00 00 98 00 31 00 00 00 00  ...........1....
0000AF2A58B0 00 2A 56 D9 75 11 00 50 52 4F 47 52 41 7E 32 00  .*VÙu..PROGRA~2.
0000AF2A58C0 00 80 00 09 00 04 00 EF BE 87 4F DB 49 2A 56 D9  .......ï¾.OÛI*VÙ
0000AF2A58D0 75 2E 00 00 00 CD 04 00 00 00 00 01 00 00 00 00  u....Í..........
```

Signed byte	76
Unsigned byte	76
Signed short	19456
Unsigned short	19456
Signed int	1275068416
Unsigned int	1275068416

- **Registry Keys:**
  - Run, UserAssist, RecentDocs, etc.



Computer\HKEY_CLASSES_ROOT\.aac\OpenWithProgids

```
._vcppxsln100
._vcppxsln110
._vcppxsln80
._vcppxsln90
._vcsxsln100
._vcsxsln110
._vcsxsln80
._vcsxsln90
._vjsxsln80
._vw8xsln110
._vwdxsln100
._vwdxsln110
._vwdxsln120
._vwdxsln140
._vwdxsln150
._vwdxsln80
._vwdxsln90
._vwinxsln120
._vwinxsln140
._vwinxsln150
._wdxsln110
._wdxsln120
._wdxsln140
._wdxsln150
.001
.386
.3fr
.3g2
.3gp
.3gp2
.3gpp
.3mf
.5vw
.7z
.a
.aac
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
AppXqj98qxeay...	REG_NONE	(zero-length binary value)
AppXvsqkg1th8...	REG_NONE	(zero-length binary value)
WMP11.AssocFil...	REG_NONE	(zero-length binary value)

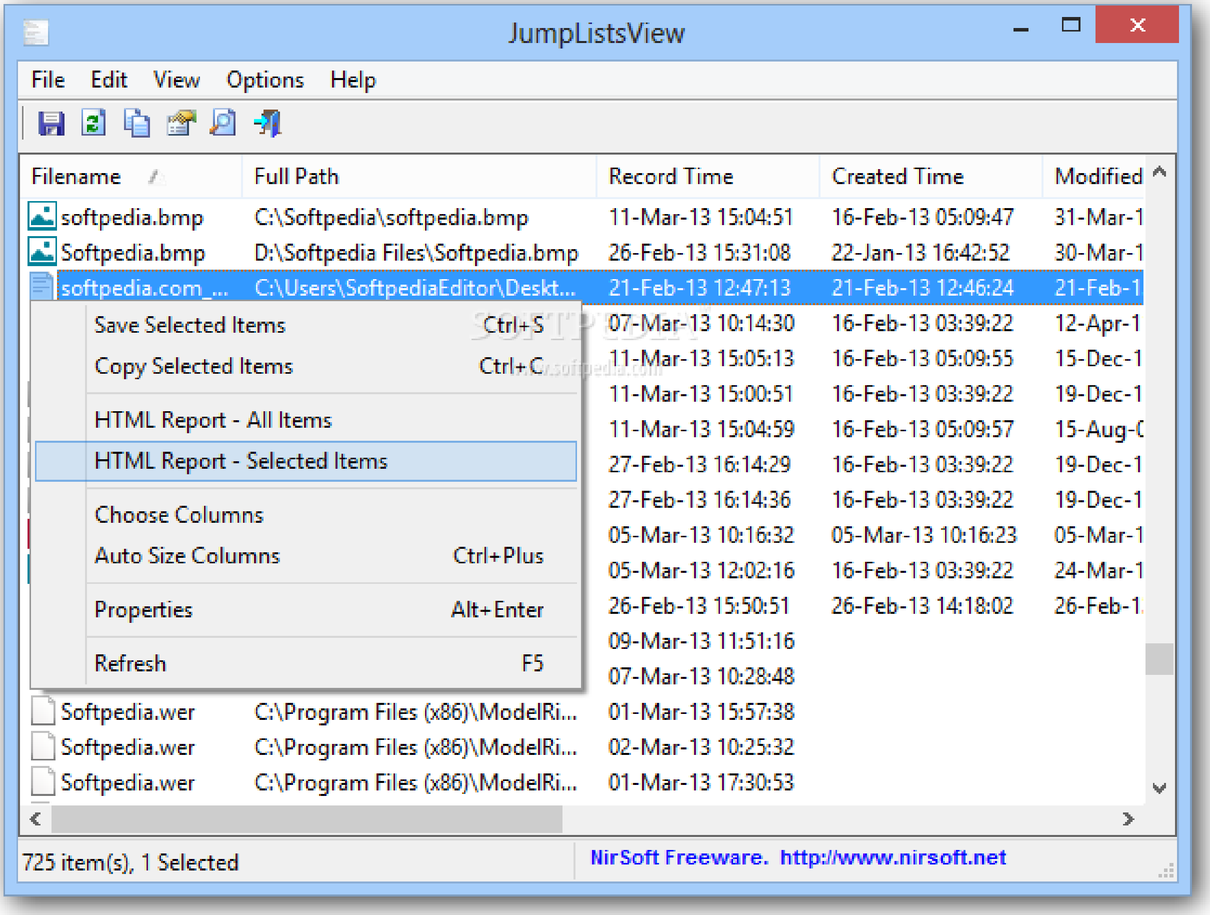
Linux

- No Prefetch equivalent.
- Execution tracked via: .bash_history , /var/log/auth.log
- File timestamps (inode changes)

5.2 File Interaction & Metadata

Windows

- NTFS provides rich timestamps (MFT: $STANDARD_INFORMATION and $FILE_NAME)
- Jump Lists (AutomaticDestinations-ms)


JumpListsView
File
Edit
View
Options
Help
Save Selected Items Ctrl+S
Copy Selected Items Ctrl+C
HTML Report - All Items
HTML Report - Selected Items
Choose Columns
Auto Size Columns Ctrl+Plus
Properties Alt+Enter
Refresh F5

Filename	Full Path	Record Time	Created Time	Modified
softpedia.bmp	C:\Softpedia\softpedia.bmp	11-Mar-13 15:04:51	16-Feb-13 05:09:47	31-Mar-1
Softpedia.bmp	D:\Softpedia Files\Softpedia.bmp	26-Feb-13 15:31:08	22-Jan-13 16:42:52	30-Mar-1
softpedia.com_...	C:\Users\SoftpediaEditor\Deskt...	21-Feb-13 12:47:13	21-Feb-13 12:46:24	21-Feb-1
		07-Mar-13 10:14:30	16-Feb-13 03:39:22	12-Apr-1
		11-Mar-13 15:05:13	16-Feb-13 05:09:55	15-Dec-1
		11-Mar-13 15:00:51	16-Feb-13 03:39:22	19-Dec-1
		11-Mar-13 15:04:59	16-Feb-13 05:09:57	15-Aug-(
		27-Feb-13 16:14:29	16-Feb-13 03:39:22	19-Dec-1
		27-Feb-13 16:14:36	16-Feb-13 03:39:22	19-Dec-1
		05-Mar-13 10:16:32	05-Mar-13 10:16:23	05-Mar-1
		05-Mar-13 12:02:16	16-Feb-13 03:39:22	24-Mar-1
		26-Feb-13 15:50:51	26-Feb-13 14:18:02	26-Feb-1.
		09-Mar-13 11:51:16		
		07-Mar-13 10:28:48		
Softpedia.wer	C:\Program Files (x86)\ModelRi...	01-Mar-13 15:57:38		
Softpedia.wer	C:\Program Files (x86)\ModelRi...	02-Mar-13 10:25:32		
Softpedia.wer	C:\Program Files (x86)\ModelRi...	01-Mar-13 17:30:53		

725 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

Linux

- EXT4: atime, mtime, ctime
- No Jump Lists equivalent

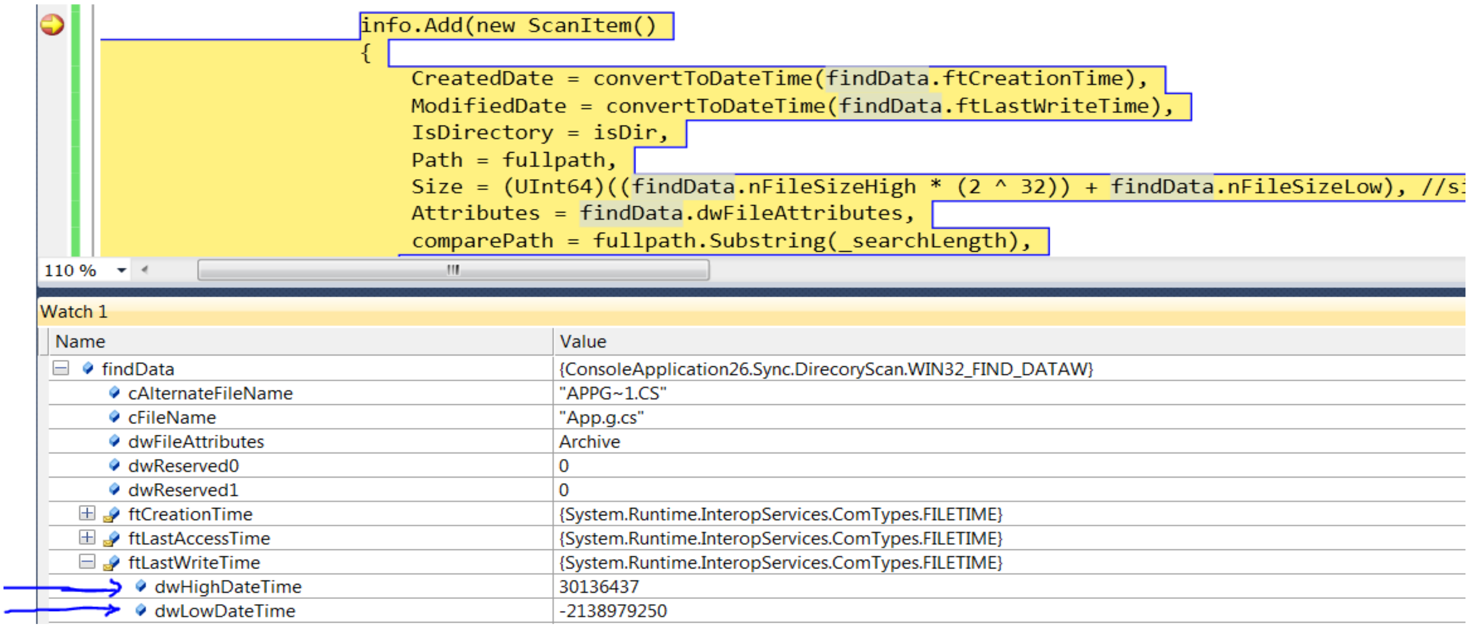
3. Analyze Encoding and Timestamp Formats Across Platforms

1.3 Timestamp Formats Across Operating Systems

Windows Timestamp Formats

1. FILETIME

- **Definition:** 64-bit value representing the number of 100-nanosecond intervals since **January 1, 1601 (UTC)**.
- **Used In:** NTFS, Prefetch, LNK files, Registry keys, MFT ($STANDARD_INFORMATION), Jump Lists, Event Logs.
- **Characteristics:**
  - Very high precision
  - Requires conversion tools to read
  - Often stored in binary structures

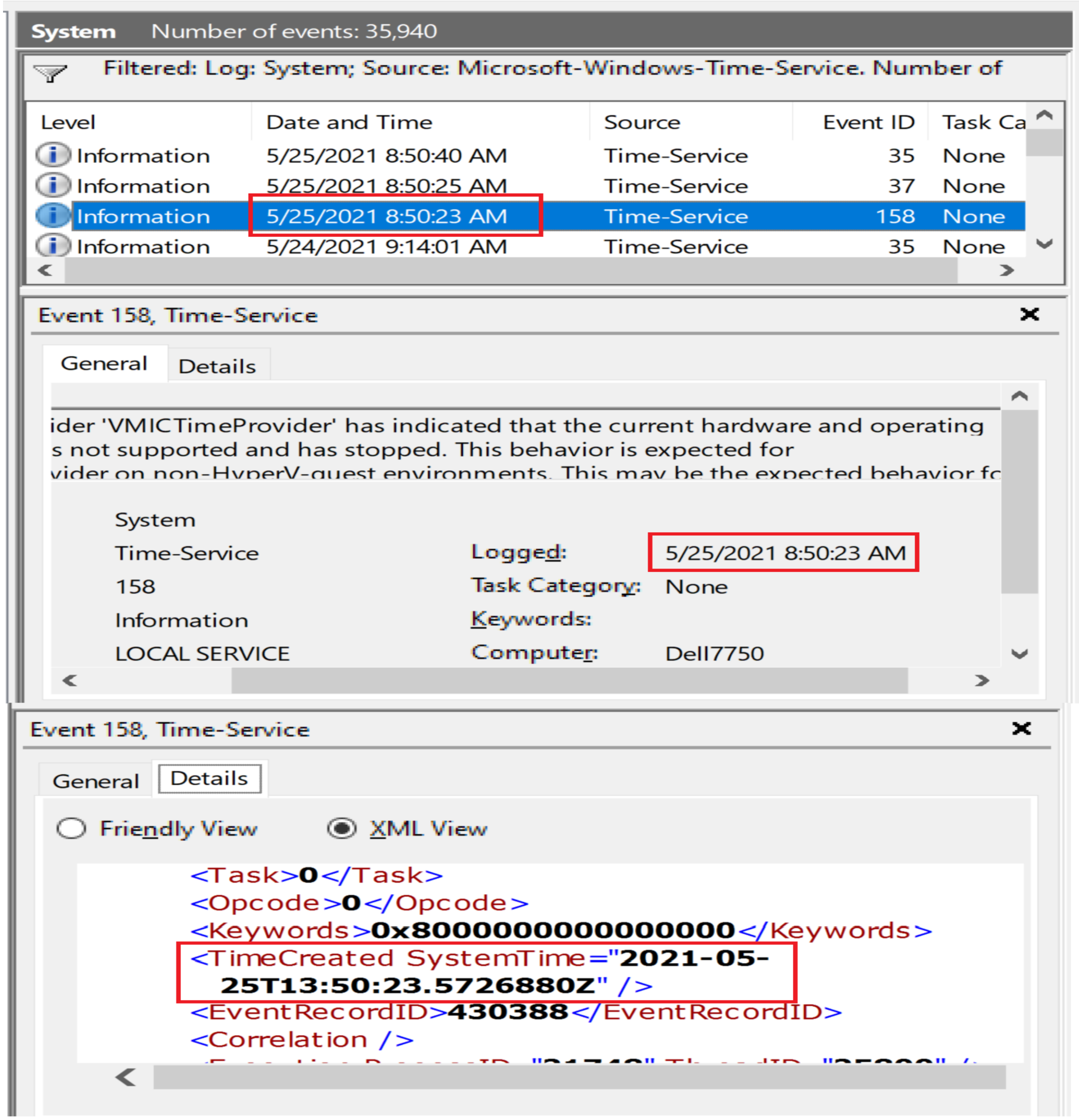


```
info.Add(new ScanItem()
{
    CreatedDate = convertToDateTime(findData.ftCreationTime),
    ModifiedDate = convertToDateTime(findData.ftLastWriteTime),
    IsDirectory = isDir,
    Path = fullpath,
    Size = (UInt64)((findData.nFileSizeHigh * (2 ^ 32)) + findData.nFileSizeLow), //s
    Attributes = findData.dwFileAttributes,
    comparePath = fullpath.Substring(_searchLength),
```

Name	Value
findData	{ConsoleApplication26.Sync.DirecoryScan.WIN32_FIND_DATAW}
cAlternateFileName	"APPG~1.CS"
cFileName	"App.g.cs"
dwFileAttributes	Archive
dwReserved0	0
dwReserved1	0
ftCreationTime	{System.Runtime.InteropServices.ComTypes.FILETIME}
ftLastAccessTime	{System.Runtime.InteropServices.ComTypes.FILETIME}
ftLastWriteTime	{System.Runtime.InteropServices.ComTypes.FILETIME}
dwHighDateTime	30136437
dwLowDateTime	-2138979250

Windows Event Logs Timestamp

- **Format:** ISO-like
- Example: 2025-02-10T18:32:55.1234567Z
- Includes timezone, making correlation easier.



System Number of events: 35,940

Filtered: Log: System; Source: Microsoft-Windows-Time-Service. Number of

Level	Date and Time	Source	Event ID	Task Ca
Information	5/25/2021 8:50:40 AM	Time-Service	35	None
Information	5/25/2021 8:50:25 AM	Time-Service	37	None
Information	5/25/2021 8:50:23 AM	Time-Service	158	None
Information	5/24/2021 9:14:01 AM	Time-Service	35	None

Event 158, Time-Service

ider 'VMICTimeProvider' has indicated that the current hardware and operating
s not supported and has stopped. This behavior is expected for
vider on non-HyperV-guest environments. This may be the expected behavior fc

System			
Time-Service	Logged:	5/25/2021 8:50:23 AM
158	Task Category:	None
Information	Keywords:	
LOCAL SERVICE	Computer:	Dell7750

Event 158, Time-Service

○ Friendly View ● XML View

```
<Task>0</Task>
<Opcode>0</Opcode>
<Keywords>0x8000000000000000</Keywords>
<TimeCreated SystemTime="2021-05-
  25T13:50:23.5726880Z" />
<EventRecordID>430388</EventRecordID>
<Correlation />
```

Linux Timestamp Formats

1. UNIX Epoch (Seconds or Milliseconds)

- Counts seconds (or ms) since **January 1, 1970 (UTC)**.
- Used in:
  - Log files (/var/log/auth.log, syslog)
  - EXT4 filesystem metadata
  - Browser history (Chrome/Firefox)

2. EXT4 Inode Timestamps

- **atime** → Last access
- **mtime** → Last modification
- **ctime** → Metadata change
- **crtime** (creation time) available in newer EXT4 versions
- Precision often in **nanoseconds**

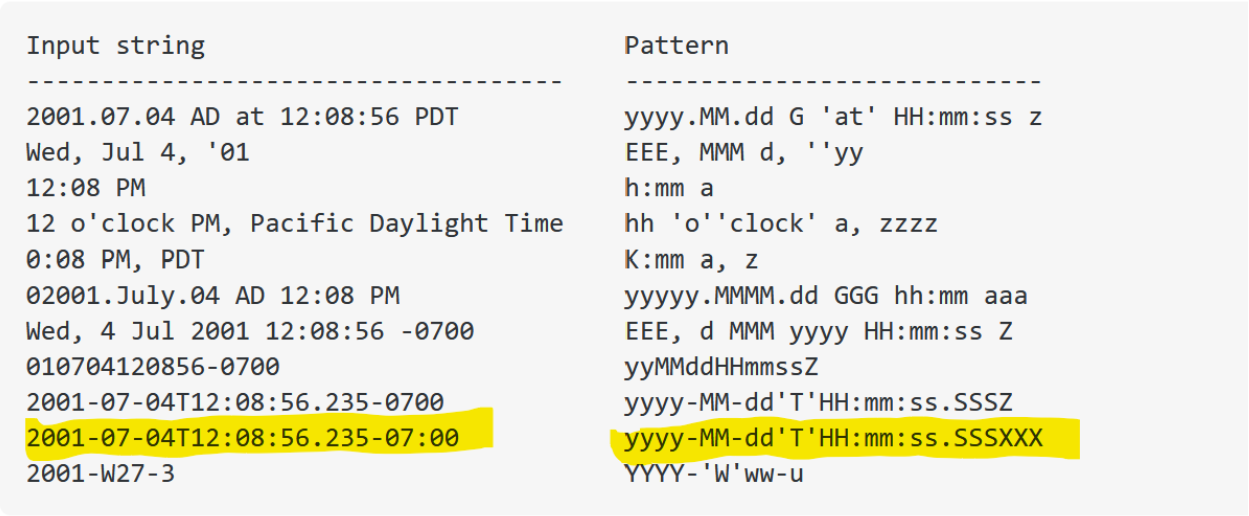
2.3 Timestamp Formats Used by Applications

1. Browser Timestamps (Chrome & Firefox)

- Stored in SQLite databases.
- Common formats:
  - UNIX Epoch (seconds)
  - UNIX Epoch (milliseconds)
  - Chrome WebKit timestamp: microseconds since **1601** (similar to FILETIME)

2. Application Logs

- Many cross-platform apps use **ISO8601** for consistency.
- Example:
  2025-11-23T17:20:02Z

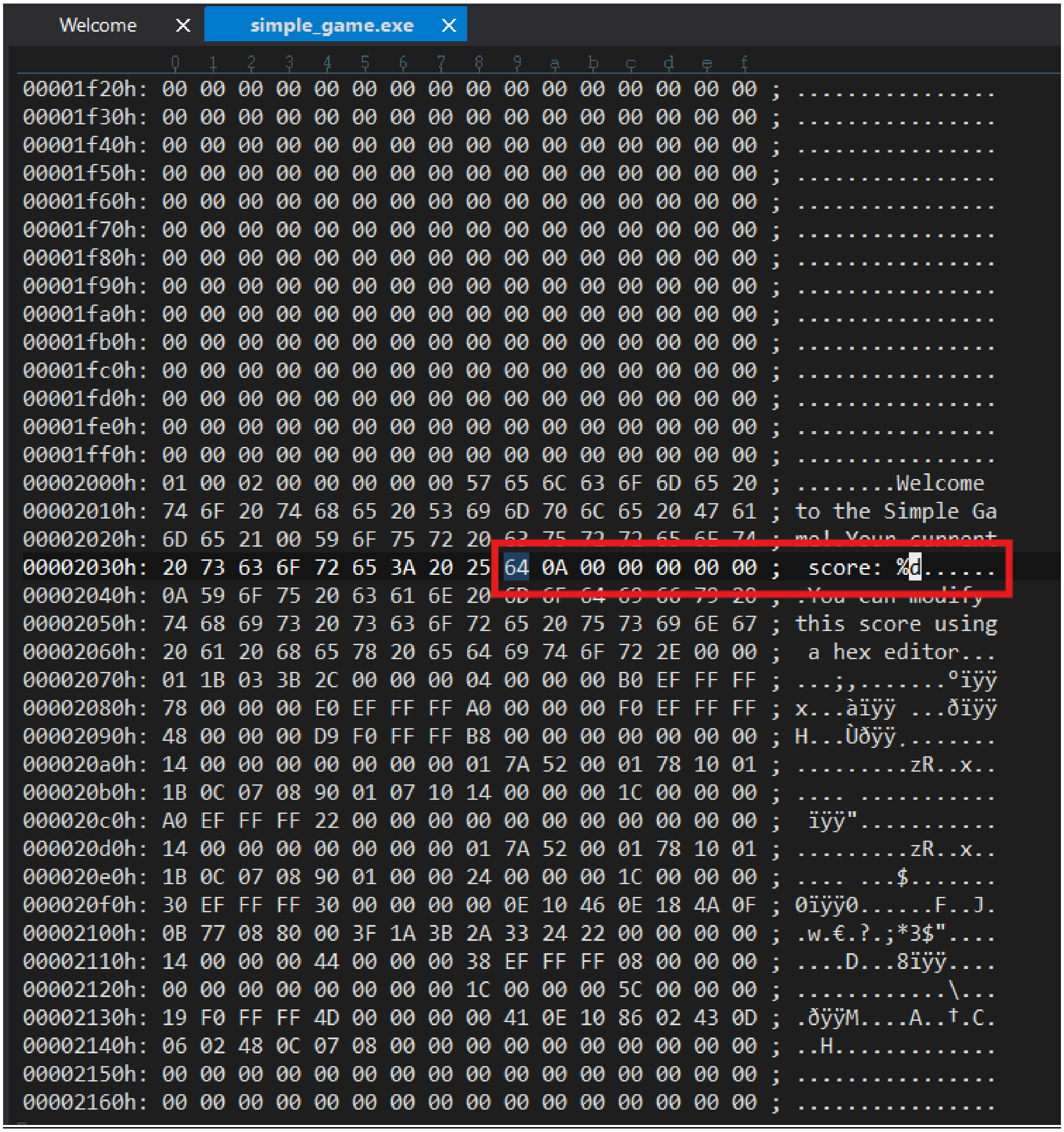


```
Input string                            Pattern
------------------------------------    ----------------------------
2001.07.04 AD at 12:08:56 PDT           yyyy.MM.dd G 'at' HH:mm:ss z
Wed, Jul 4, '01                         EEE, MMM d, ''yy
12:08 PM                                h:mm a
12 o'clock PM, Pacific Daylight Time    hh 'o''clock' a, zzzz
0:08 PM, PDT                            K:mm a, z
02001.July.04 AD 12:08 PM               yyyyy.MMMM.dd GGG hh:mm aaa
Wed, 4 Jul 2001 12:08:56 -0700          EEE, d MMM yyyy HH:mm:ss Z
010704120856-0700                       yyMMddHHmmssZ
2001-07-04T12:08:56.235-0700            yyyy-MM-dd'T'HH:mm:ss.SSSZ
2001-07-04T12:08:56.235-07:00           yyyy-MM-dd'T'HH:mm:ss.SSSXXX
2001-W27-3                              YYYY-'W'ww-u
```

3.3 Encoding Formats Across OS

Windows Encoding

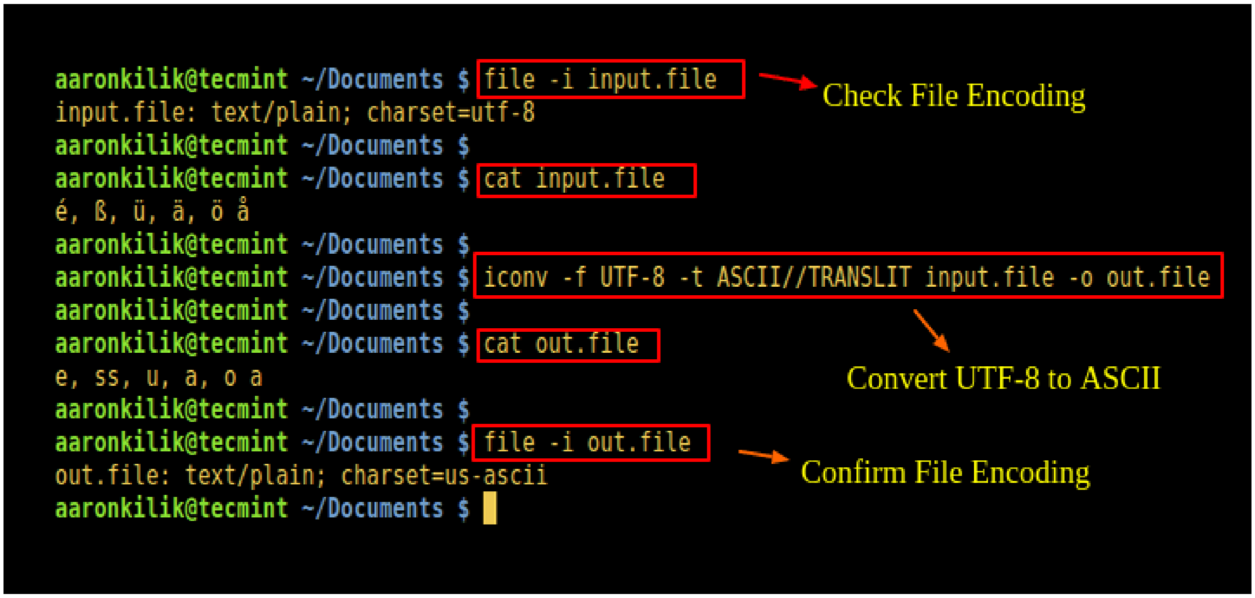
- Many system artifacts use **UTF-16LE** (Registry exports, some log files).
- Binary logs (EVTX, prefetch, LNK) require compatible parsers.



```
            0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00001f20h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00001f30h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00001f40h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00001f50h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00001f60h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00001f70h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00001f80h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00001f90h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00001fa0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00001fb0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00001fc0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00001fd0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00001fe0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00001ff0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00002000h: 01 00 02 00 00 00 00 00 57 65 6C 63 6F 6D 65 20 ; ........Welcome
00002010h: 74 6F 20 74 68 65 20 53 69 6D 70 6C 65 20 47 61 ; to the Simple Ga
00002020h: 6D 65 21 00 59 6F 75 72 20 63 75 72 72 65 6E 74 ; me!.Your current
00002030h: 20 73 63 6F 72 65 3A 20 25 64 0A 00 00 00 00 00 ;  score: %d......
00002040h: 0A 59 6F 75 20 63 61 6E 20 6D 6F 64 69 66 79 20 ; .You can modify
00002050h: 74 68 69 73 20 73 63 6F 72 65 20 75 73 69 6E 67 ; this score using
00002060h: 20 61 20 68 65 78 20 65 64 69 74 6F 72 2E 00 00 ;  a hex editor...
00002070h: 01 1B 03 3B 2C 00 00 00 04 00 00 00 B0 EF FF FF ; ...;,.......°ïÿÿ
00002080h: 78 00 00 00 E0 EF FF FF A0 00 00 00 F0 EF FF FF ; x...àïÿÿ ...ðïÿÿ
00002090h: 48 00 00 00 D9 F0 FF FF B8 00 00 00 00 00 00 00 ; H...Ùðÿÿ¸.......
000020a0h: 14 00 00 00 00 00 00 00 01 7A 52 00 01 78 10 01 ; .........zR..x..
000020b0h: 1B 0C 07 08 90 01 07 10 14 00 00 00 1C 00 00 00 ; .... ...........
000020c0h: A0 EF FF FF 22 00 00 00 00 00 00 00 00 00 00 00 ;  ïÿÿ"...........
000020d0h: 14 00 00 00 00 00 00 00 01 7A 52 00 01 78 10 01 ; .........zR..x..
000020e0h: 1B 0C 07 08 90 01 00 00 24 00 00 00 1C 00 00 00 ; .... ...$.......
000020f0h: 30 EF FF FF 30 00 00 00 00 0E 10 46 0E 18 4A 0F ; 0ïÿÿ0......F..J.
00002100h: 0B 77 08 80 00 3F 1A 3B 2A 33 24 22 00 00 00 00 ; .w.€.?.;*3$"....
00002110h: 14 00 00 00 44 00 00 00 38 EF FF FF 08 00 00 00 ; ....D...8ïÿÿ....
00002120h: 00 00 00 00 00 00 00 00 1C 00 00 00 5C 00 00 00 ; ............\...
00002130h: 19 F0 FF FF 4D 00 00 00 00 41 0E 10 86 02 43 0D ; .ðÿÿM....A..†.C.
00002140h: 06 02 48 0C 07 08 00 00 00 00 00 00 00 00 00 00 ; ..H.............
00002150h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00002160h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
```

Linux Encoding

- Almost all logs use **UTF-8**.
- Shell histories are plain text, often ASCII/UTF-8.



```
aaronkilik@tecmint ~/Documents $ file -i input.file
input.file: text/plain; charset=utf-8
aaronkilik@tecmint ~/Documents $
aaronkilik@tecmint ~/Documents $ cat input.file
é, ß, ü, ä, ö å
aaronkilik@tecmint ~/Documents $
aaronkilik@tecmint ~/Documents $ iconv -f UTF-8 -t ASCII//TRANSLIT input.file -o out.file
aaronkilik@tecmint ~/Documents $
aaronkilik@tecmint ~/Documents $ cat out.file
e, ss, u, a, o a
aaronkilik@tecmint ~/Documents $
aaronkilik@tecmint ~/Documents $ file -i out.file
out.file: text/plain; charset=us-ascii
aaronkilik@tecmint ~/Documents $ 
```

Check File Encoding

Convert UTF-8 to ASCII

Confirm File Encoding

4.3 Common Challenges with Timestamp Analysis

1. **Timezone Differences**
   - Logs may be stored in UTC while user activity is interpreted in local time.
2. **Daylight Savings Adjustments**
   - May cause hour offsets during timeline creation.
3. **Different Epochs**
   - Windows (1601) vs Unix (1970) vs older HFS+ (1904).
4. **Mixed Precision**
   - Seconds, milliseconds, microseconds, nanoseconds.
5. **Cross-platform correlation**
   - Requires converting all timestamps into a unified format.

4. Evaluate Forensic Tool Compatibility

1.4 Autopsy / Sleuth Kit (TSK)

Supported OS Artifacts:

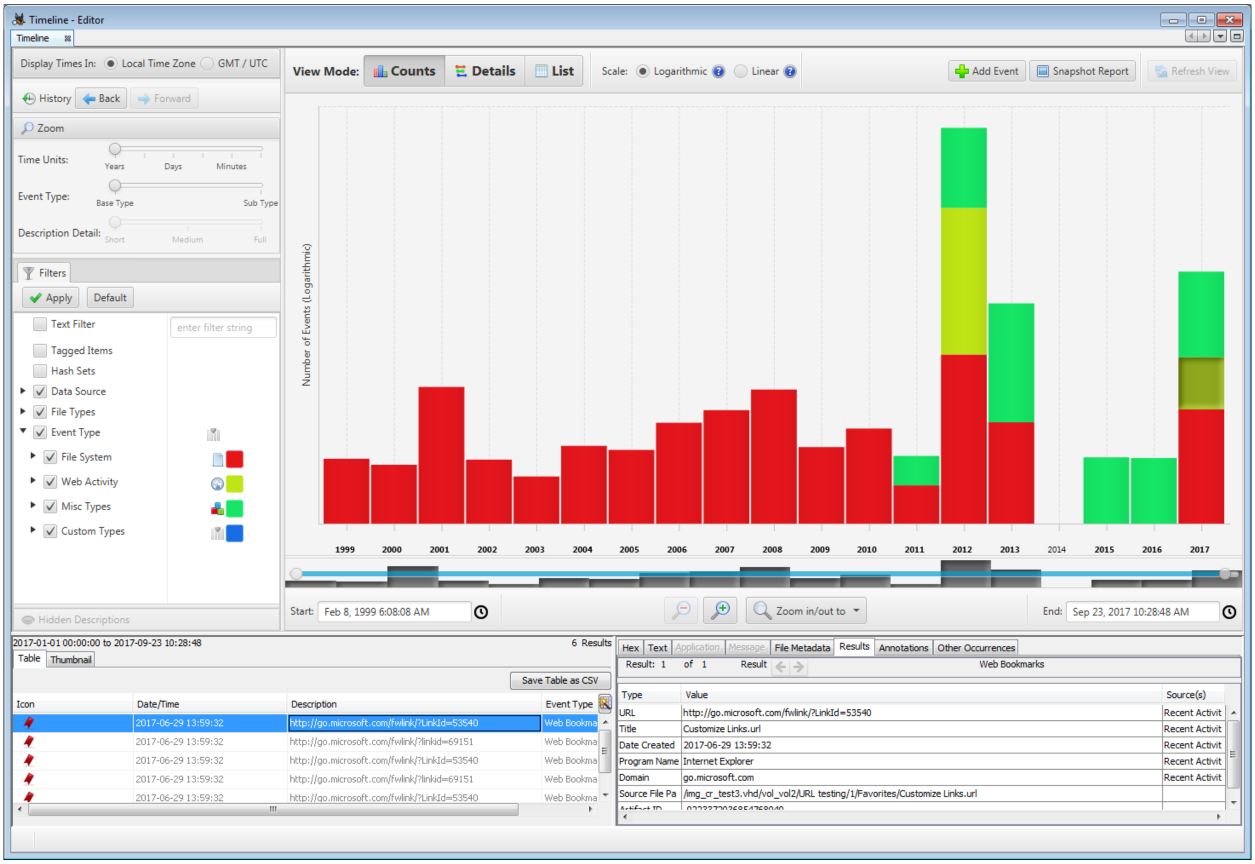
- Windows: NTFS, FAT, exFAT
- Linux: EXT3/EXT4
- macOS: HFS+ (good), APFS (partial support depending on version)

Strengths:

- Strong disk analysis capabilities
- Timeline feature integrates MFT + logs + browser history
- Artifact categorization (Web history, Recent files, Executables)

Limitations:

- Limited APFS support
- Cannot parse EVTX natively (needs plugins)
- Prefetch parsing may require external modules



Display Times In: ● Local Time Zone ○ GMT / UTC

View Mode: **Counts** Details List

Scale: ● Logarithmic ○ Linear

☐ Text Filter [enter filter string]
☐ Tagged Items
☐ Hash Sets
☑ Data Source
☑ File Types
☑ Event Type
☑ File System 🟥
☑ Web Activity 🟨
☑ Misc Types 🟩
☑ Custom Types 🟦

Start: Feb 8, 1999 6:08:08 AM

End: Sep 23, 2017 10:28:48 AM

2017-01-01 00:00:00 to 2017-09-23 10:28:48 — 6 Results

Table | Thumbnail

Icon	Date/Time	Description	Event Type
	2017-06-29 13:59:32	http://go.microsoft.com/fwlink/?LinkId=53540	Web Bookma
	2017-06-29 13:59:32	http://go.microsoft.com/fwlink/?linkid=69151	Web Bookma
	2017-06-29 13:59:32	http://go.microsoft.com/fwlink/?LinkId=53540	Web Bookma
	2017-06-29 13:59:32	http://go.microsoft.com/fwlink/?linkid=69151	Web Bookma
	2017-06-29 13:59:32	http://go.microsoft.com/fwlink/?LinkId=53540	Web Bookma

Hex | Text | Application | Message | File Metadata | Results | Annotations | Other Occurrences

Result: 1 of 1 Result — Web Bookmarks

Type	Value	Source(s)
URL	http://go.microsoft.com/fwlink/?LinkId=53540	Recent Activit
Title	Customize Links.url	Recent Activit
Date Created	2017-06-29 13:59:32	Recent Activit
Program Name	Internet Explorer	Recent Activit
Domain	go.microsoft.com	Recent Activit
Source File Pa	/img_cr_test3.vhd/vol_vol2/URL testing/1/Favorites/Customize Links.url	
Artifact ID	-9223372036854768040	

2.4 FTK Imager

Supported OS Artifacts:

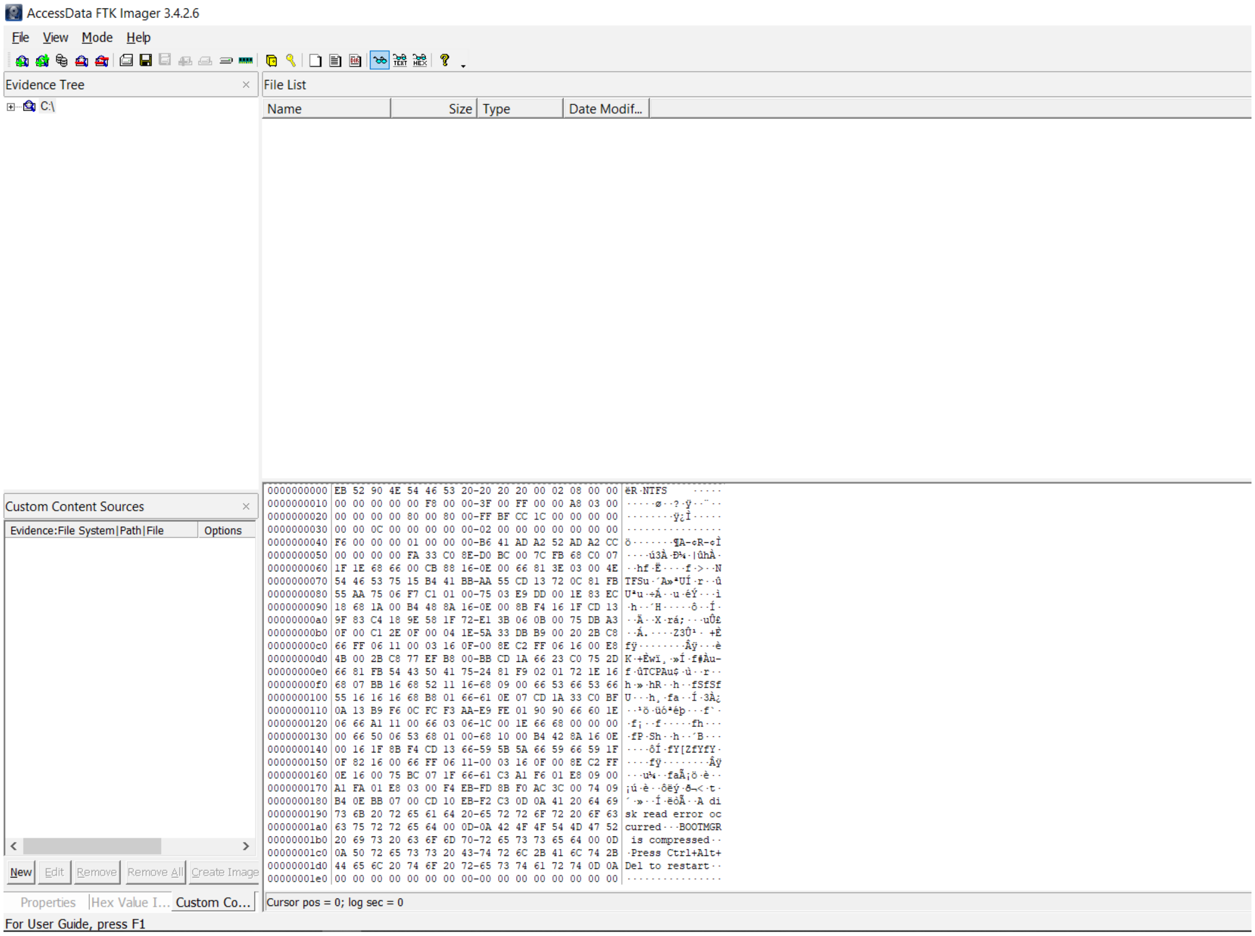
- Excellent Windows support
- Can mount Linux/macOS images but limited deep parsing

Strengths:

- Ideal for creating forensic images (E01, RAW)
- Allows previewing NTFS metadata
- Very stable and widely accepted in industry

Limitations:

- Not a full analysis suite
- Weak support for EXT4 metadata
- Cannot parse APFS detailed artifacts



```
0000000000 EB 52 90 4E 54 46 53 20-20 20 20 00 02 08 00 00 ëR·NTFS    ·····
0000000010 00 00 00 00 00 F8 00 00-3F 00 FF 00 00 A8 03 00 ·····ø··?·ÿ··¨··
0000000020 00 00 00 00 80 00 80 00-FF BF CC 1C 00 00 00 00 ········ÿ¿Ì·····
0000000030 00 00 0C 00 00 00 00 00-02 00 00 00 00 00 00 00 ················
0000000040 F6 00 00 00 01 00 00 00-B6 41 AD A2 52 AD A2 CC ö·······¶A-¢R-¢Ì
0000000050 00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB 68 C0 07 ····ú3À·Ð¼·|ûhÀ·
0000000060 1F 1E 68 66 00 CB 88 16-0E 00 66 81 3E 03 00 4E ··hf·Ë····f·>··N
0000000070 54 46 53 75 15 B4 41 BB-AA 55 CD 13 72 0C 81 FB TFSu·´A»ªUÍ·r··û
0000000080 55 AA 75 06 F7 C1 01 00-75 03 E9 DD 00 1E 83 EC Uªu·÷Á··u·éÝ···ì
0000000090 18 68 1A 00 B4 48 8A 16-0E 00 8B F4 16 1F CD 13 ·h··´H·····ô··Í·
00000000a0 9F 83 C4 18 9E 58 1F 72-E1 3B 06 0B 00 75 DB A3 ··Ä··X·rá;···uÛ£
00000000b0 0F 00 C1 2E 0F 00 04 1E-5A 33 DB B9 00 20 2B C8 ··Á.····Z3Û¹· +È
00000000c0 66 FF 06 11 00 03 16 0F-00 8E C2 FF 06 16 00 E8 fÿ········Âÿ···è
00000000d0 4B 00 2B C8 77 EF B8 00-BB CD 1A 66 23 C0 75 2D K·+Èwï¸·»Í·f#Àu-
00000000e0 66 81 FB 54 43 50 41 75-24 81 F9 02 01 72 1E 16 f·ûTCPAu$·ù··r··
00000000f0 68 07 BB 16 68 52 11 16-68 09 00 66 53 66 53 66 h·»·hR··h··fSfSf
0000000100 55 16 16 16 68 B8 01 66-61 0E 07 CD 1A 33 C0 BF U···h¸·fa··Í·3À¿
0000000110 0A 13 B9 F6 0C FC F3 AA-E9 FE 01 90 90 66 60 1E ··¹ö·üóªéþ···f`·
0000000120 06 66 A1 11 00 66 03 06-1C 00 1E 66 68 00 00 00 ·f¡··f·····fh···
0000000130 00 66 50 06 53 68 01 00-68 10 00 B4 42 8A 16 0E ·fP·Sh··h··´B···
0000000140 00 16 1F 8B F4 CD 13 66-59 5B 5A 66 59 66 59 1F ····ôÍ·fY[ZfYfY·
0000000150 0F 82 16 00 66 FF 06 11-00 03 16 0F 00 8E C2 FF ····fÿ········Âÿ
0000000160 0E 16 00 75 BC 07 1F 66-61 C3 A1 F6 01 E8 09 00 ···u¼··faÃ¡ö·è··
0000000170 A1 FA 01 E8 03 00 F4 EB-FD 8B F0 AC 3C 00 74 09 ¡ú·è··ôëý·ð¬<·t·
0000000180 B4 0E BB 07 00 CD 10 EB-F2 C3 0D 0A 41 20 64 69 ´·»··Í·ëòÃ··A di
0000000190 73 6B 20 72 65 61 64 20-65 72 72 6F 72 20 6F 63 sk read error oc
00000001a0 63 75 72 72 65 64 00 0D-0A 42 4F 4F 54 4D 47 52 curred···BOOTMGR
00000001b0 20 69 73 20 63 6F 6D 70-72 65 73 73 65 64 00 0D  is compressed··
00000001c0 0A 50 72 65 73 73 20 43-74 72 6C 2B 41 6C 74 2B ·Press Ctrl+Alt+
00000001d0 44 65 6C 20 74 6F 20 72-65 73 74 61 72 74 0D 0A Del to restart··
00000001e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
```

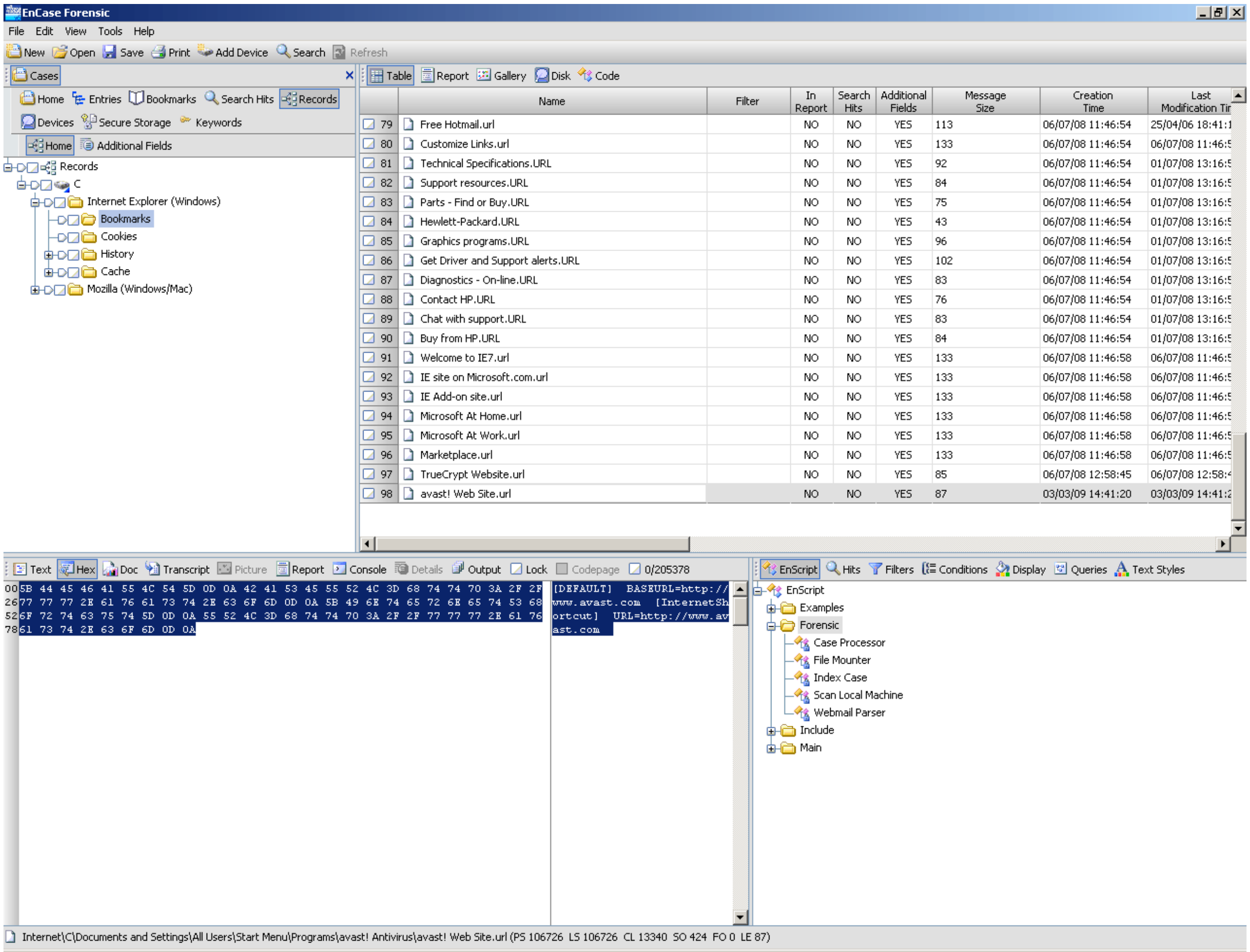
Cursor pos = 0; log sec = 0

For User Guide, press F1

3.4 EnCase (Commercial)

Supported OS Artifacts:

- Broad su


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases
Home Entries Bookmarks Search Hits Records
Devices Secure Storage Keywords
Home Additional Fields
Records
C
Internet Explorer (Windows)
Bookmarks
Cookies
History
Cache
Mozilla (Windows/Mac)
Table Report Gallery Disk Code
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/205378
EnScript Hits Filters Conditions Display Queries Text Styles
EnScript
Examples
Forensic
Case Processor
File Mounter
Index Case
Scan Local Machine
Webmail Parser
Include
Main

	Name	Filter	In Report	Search Hits	Additional Fields	Message Size	Creation Time	Last Modification Tir
79	Free Hotmail.url		NO	NO	YES	113	06/07/08 11:46:54	25/04/06 18:41:1
80	Customize Links.url		NO	NO	YES	133	06/07/08 11:46:54	06/07/08 11:46:5
81	Technical Specifications.URL		NO	NO	YES	92	06/07/08 11:46:54	01/07/08 13:16:5
82	Support resources.URL		NO	NO	YES	84	06/07/08 11:46:54	01/07/08 13:16:5
83	Parts - Find or Buy.URL		NO	NO	YES	75	06/07/08 11:46:54	01/07/08 13:16:5
84	Hewlett-Packard.URL		NO	NO	YES	43	06/07/08 11:46:54	01/07/08 13:16:5
85	Graphics programs.URL		NO	NO	YES	96	06/07/08 11:46:54	01/07/08 13:16:5
86	Get Driver and Support alerts.URL		NO	NO	YES	102	06/07/08 11:46:54	01/07/08 13:16:5
87	Diagnostics - On-line.URL		NO	NO	YES	83	06/07/08 11:46:54	01/07/08 13:16:5
88	Contact HP.URL		NO	NO	YES	76	06/07/08 11:46:54	01/07/08 13:16:5
89	Chat with support.URL		NO	NO	YES	83	06/07/08 11:46:54	01/07/08 13:16:5
90	Buy from HP.URL		NO	NO	YES	84	06/07/08 11:46:54	01/07/08 13:16:5
91	Welcome to IE7.url		NO	NO	YES	133	06/07/08 11:46:58	06/07/08 11:46:5
92	IE site on Microsoft.com.url		NO	NO	YES	133	06/07/08 11:46:58	06/07/08 11:46:5
93	IE Add-on site.url		NO	NO	YES	133	06/07/08 11:46:58	06/07/08 11:46:5
94	Microsoft At Home.url		NO	NO	YES	133	06/07/08 11:46:58	06/07/08 11:46:5
95	Microsoft At Work.url		NO	NO	YES	133	06/07/08 11:46:58	06/07/08 11:46:5
96	Marketplace.url		NO	NO	YES	133	06/07/08 11:46:58	06/07/08 11:46:5
97	TrueCrypt Website.url		NO	NO	YES	85	06/07/08 12:58:45	06/07/08 12:58:4
98	avast! Web Site.url		NO	NO	YES	87	03/03/09 14:41:20	03/03/09 14:41:2

```
005B 44 45 46 41 55 4C 54 5D 0D 0A 42 41 53 45 55 52 4C 3D 68 74 74 70 3A 2F 2F   [DEFAULT]  BASEURL=http://
2677 77 77 2E 61 76 61 73 74 2E 63 6F 6D 0D 0A 5B 49 6E 74 65 72 6E 65 74 53 68   www.avast.com  [InternetSh
526F 72 74 63 75 74 5D 0D 0A 55 52 4C 3D 68 74 74 70 3A 2F 2F 77 77 77 2E 61 76   ortcut]  URL=http://www.av
7861 73 74 2E 63 6F 6D 0D 0A                                                       ast.com
```

Internet\C\Documents and Settings\All Users\Start Menu\Programs\avast! Antivirus\avast! Web Site.url (PS 106726 LS 106726 CL 13340 SO 424 FO 0 LE 87)