

## Forensic Analysis Notes:

### Case Information:

Case: Analyzing Firefox Browser History

Analyst: Julius Niyonzima

Professor: Dr. Chris Lamb

Email: [jnbfg@umkc.edu](mailto:jnbfg@umkc.edu)

Id	File name	Hash(None)	Notes
1	Disk image	Zipped windows image	Suspicious browser activity

### Tools and Environment

Kali Linux v2025.2

```
(tempuser@kali)-[~/Downloads]
$ lsb_release -a
No LSB modules are available.
Distributor ID: Kali
Description:    Kali GNU/Linux Rolling
Release:       2025.2
Codename:      kali-rolling
```

mount v2.41.1 to attach filesystem like(USB, partition, hard drive, and ISO image) to existing directory structure

```
/mnt/ewf/ewf1 on /mnt/ntfs type fuseblk (ro,relatime,user_id=0,group_id=0,allow_other,blksize=4096)
(root@kali)-[/home/kali/scheduled_task]
# mount --version
mount from util-linux 2.41.1 (libmount 2.41.1: selinux, smack, btrfs, verity, namespaces, idmapping, fd-based-mount, statmount, statx, assert, debug)
```

Ewfmount : Mount expert witness format (ewf) as a raw disk for analysis

```
(root@kali)-[/home/kali/scheduled_task]
# ewfmount -V
ewfmount 20140816

Copyright (C) 2006-2021, Joachim Metz.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
Report bugs to <joachim.metz@gmail.com>.
```

/mnt/hgfs/: created a shard folder to allow the virtual machine to access the folder on my external SanDisk driver

```
(root@kali)-[/home/kali/scheduled_task]
# ls -lah /mnt/hgfs/
total 21K
dr-xr-xr-x 1 root root 4.1K Sep 27 23:09 .
drwxr-xr-x 5 root root 4.0K Sep 27 21:05 ..
drwxrwxrwx 1 root root 0 Sep 27 19:17 BackUps
drwxrwxrwx 1 root root 12K Sep 27 19:20 certificates
```

```
(root@kali)-[/home/kali/scheduled_task]
# mount | grep hgfs
vmhgfs-fuse on /mnt/hgfs type fuse.vmhgfs-fuse (rw,nosuid,nodev,relatime,user_id=0,group_id=0,allow_other)

(root@kali)-[/home/kali/scheduled_task]
```

Grep v3.11

```
(tempuser@kali)-[~/Downloads]
$ grep -V
grep (GNU grep) 3.11
Copyright (C) 2023 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>.
>.
```

Cat:

```
(root@kali)-[/home/kali/scheduled_tasks]
# cat --version
cat (GNU coreutils) 9.7
Packaged by Debian (9.7-3)
Copyright (C) 2025 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Written by Torbjörn Granlund and Richard M. Stallman.
```

cp v9.7 for copying files and directories

```
(root@kali)-[/mnt/ntfs]
# cp --version
cp (GNU coreutils) 9.7
Packaged by Debian (9.7-3)
Copyright (C) 2025 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

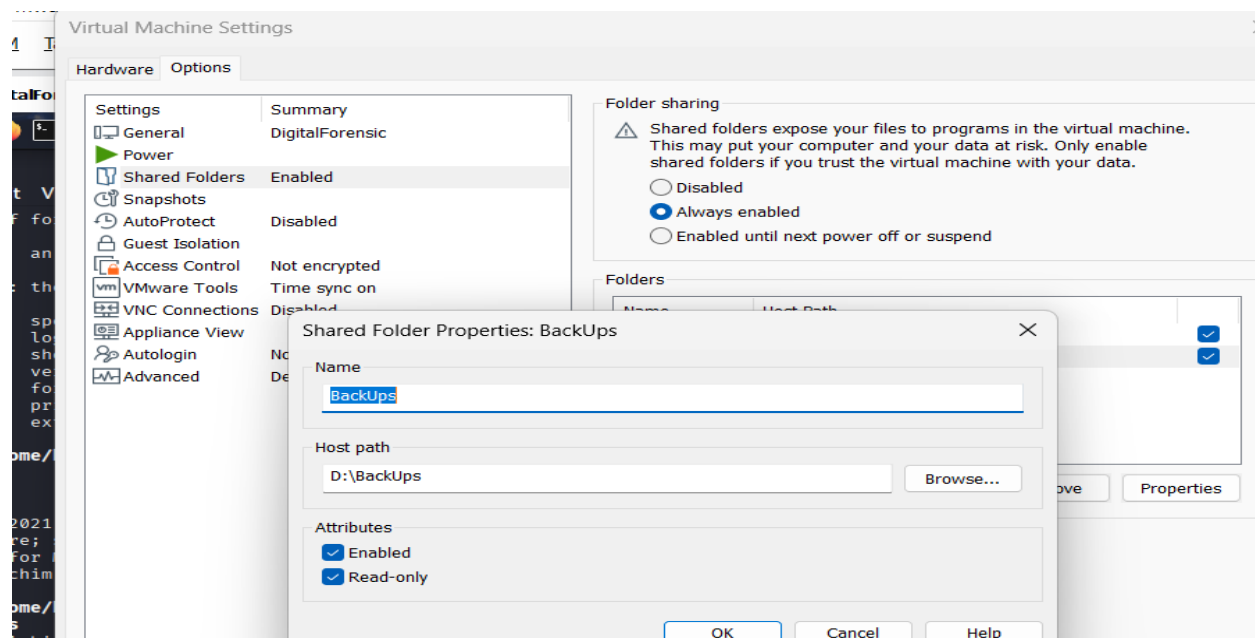
Written by Torbjörn Granlund, David MacKenzie, and Jim Meyering.
```

SQLite3 v3.46.1 that stores structured data for interaction with applications

```
(kali@kali)-[/mnt/ntfs]
$ sqlite3 --version
3.46.1 2024-08-13 09:16:08 c9c2ab54ba1f5f46360f1b4f35d849cd3f080e6fc2b6c60e91b16c63f69aalt1 (64-bit)

(kali@kali)-[/mnt/ntfs]
```

Step 1: Created a shared folder to allow the virtual machine (VM) to access the **backup** folder located at `*D:\holders*` on the external drive. This folder contains the disk image.



Step 2: Mount manually to allow vm to share the shared folder

```
[sudo] password for kali:
(root@kali)-[/home/kali]
# vmhgfs-fuse .host:/ /mnt/hgfs -o allow_other
```

copied from chatGPT

#### Fix on Kali

Try remounting manually:

```
bash
sudo vmhgfs-fuse .host:/ /mnt/hgfs -o allow_other
```

Analysis Steps :

Step3 : Created the directory where the image should be mounted and used the **ewfmount** command to mount the image

Command:

```
(root@kali)-[~]
# mkdir /mnt/ewf/
```

Result: Directory was created

Status: Worked

Step4 : Mount the image to directory created

Command

```
mkd11: cannot create directory /mnt/ewf/: File exists
(root@kali)-[/home/kali]
# ewfmount /mnt/hgfs/BackUps/CS436/CS436_Windows11_PWNED.E01 /mnt/ewf/
ewfmount 20140816
```

**Result:** The entire image was mounted in the /mnt/ewf/ directory

**Status:** worked

Step 5: List the characteristics of the mounted drive

```
(root@kali)-[/home/kali]
# fdisk -l /mnt/ewf/ewf1
Disk /mnt/ewf/ewf1: 70 GiB, 75161927680 bytes, 146800640 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 530B465D-65A0-41F3-9A2F-D76BBD90DE2C

Device            Start      End  Sectors  Size Type
/mnt/ewf/ewf1p1    2048      206847    204800   100M EFI System
/mnt/ewf/ewf1p2    206848    239615     32768    16M Microsoft reserved
/mnt/ewf/ewf1p3    239616   145481727 145242112 69.3G Microsoft basic data
/mnt/ewf/ewf1p4   145481728 146796543    1314816   642M Windows recovery environment
```

**Result:** Partitions captured were listed, with the sector starting at **239616**

**Status:** Worked

**Step 5:** Mount the NTFS partitions

Command:

```
(root@kali)-[/home/kali]
# mount -t ntfs-3g -o ro,loop,offset=122683392,show_sys_files,streams_interface=windows /mnt/ewf/ewf1 /mnt/ntfs
```

**Result:** The disk image was mounted as read-only at /mnt/ntfs

**Status:** Worked

**Step 6:** listed all contents from the disk image mounted at /mnt/ntfs

```

(kali@kali)-[/mnt/ntfs]
# ls -la
total 1757044
drwxrwxrwx 1 root root      4096 Jul 19 20:11 .
drwxr-xr-x 5 root root      4096 Sep 27 23:35 ..
-rwxrwxrwx 1 root root      2560 Jul 19 07:32 '$AttrDef'
-rwxrwxrwx 1 root root         0 Jul 19 07:32 '$BadClus'
-rwxrwxrwx 1 root root 2269408 Jul 19 07:32 '$Bitmap'
-rwxrwxrwx 1 root root      8192 Jul 19 07:32 '$Boot'
drwxrwxrwx 1 root root         0 Jul 19 07:32 '$Extend'
-rwxrwxrwx 1 root root 67108864 Jul 19 07:32 '$LogFile'
-rwxrwxrwx 1 root root 236453888 Jul 19 07:32 '$MFT'
-rwxrwxrwx 1 root root      4096 Jul 19 07:32 '$MFTMirr'
drwxrwxrwx 1 root root         0 Jul 19 10:39 '$Recycle.Bin'
-rwxrwxrwx 1 root root         0 Jul 19 07:32 '$Secure'
-rwxrwxrwx 1 root root    131072 Jul 19 07:32 '$UpCase'
-rwxrwxrwx 1 root root         0 Jul 19 07:32 '$Volume'
lrwxrwxrwx 2 root root      15 Jul 19 06:42 'Documents and Settings' → /mnt/ntfs/Users
-rwxrwxrwx 2 root root    12288 Jul 19 19:50 DumpStack.log.tmp
drwxrwxrwx 1 root root         0 Jul 19 05:13 inetpub
drwxrwxrwx 1 root root         0 Jul 19 05:41 OneDriveTemp
-rwxrwxrwx 1 root root 1476395008 Jul 19 19:50 pagefile.sys
drwxrwxrwx 1 root root         0 Apr  1 2024 PerfLogs
drwxrwxrwx 1 root root      4096 Jul 19 10:42 ProgramData
drwxrwxrwx 1 root root      4096 Jul 19 20:10 'Program Files'
drwxrwxrwx 1 root root      4096 Jul 19 10:42 'Program Files (x86)'
drwxrwxrwx 1 root root         0 Jul 19 05:01 Recovery
-rwxrwxrwx 1 root root 16777216 Jul 19 19:50 swapfile.sys
drwxrwxrwx 1 root root      4096 Jul 19 05:29 'System Volume Information'
drwxrwxrwx 1 root root      4096 Jul 19 10:40 Users
drwxrwxrwx 1 root root    16384 Jul 19 05:42 Windows
drwxrwxrwx 1 root root         0 Jul 19 07:38 Windows.old

```

**Step 7:** Created a directory to hold all Firefox artifacts collected from partitions

```

(kali@kali)-[/mnt/ntfs]
$ mkdir /home/kali/Firefox_artifacts
(kali@kali)-[/mnt/ntfs]

```

**Step 8:** 1 Traverse to the Firefox user profile on the system using the NTFS file system. This will provide information about bookmarks, cookies, history, extensions, and other user-related activities in the browser

```
(root@kali)-[/]
# cd /mnt/ntfs/Users/cs436/AppData/Roaming/Mozilla/Firefox/Profiles/94mc0c08.default-release

(root@kali)-[/mnt/ntfs/Mozilla/Firefox/Profiles/94mc0c08.default-release]
# ls
addons.json                                extension-store                             security_state
addonStartup.json.lz4                     favicons.sqlite                           sessionCheckpoints.json
AlternateServices.bin                     favicons.sqlite-shm                       sessionstore-backups
bookmarkbackups                           favicons.sqlite-wal                       sessionstore.jsonlz4
bounce-tracking-protection.sqlite         formhistory.sqlite                        settings
broadcast-listeners.json                  gmp-gmpopenh264                          shield-preference-experiments.json
cert9.db                                  gmp-widevinecdm                          SiteSecurityServiceState.bin
compatibility.ini                          handlers.json                             storage
containers.json                           key4.db                                  storage.sqlite
content-prefs.sqlite                      minidumps                                suggest.sqlite
cookies.sqlite                            parent.lock                               suggest.sqlite-shm
cookies.sqlite-shm                        permissions.sqlite                        suggest.sqlite-wal
cookies.sqlite-wal                        pkcs11.txt                               targeting.snapshot.json
crashes                                   places.sqlite                             times.json
datareporting                             places.sqlite-shm                        webappsstore.sqlite
domain_to_categories.sqlite               places.sqlite-wal                        webappsstore.sqlite-shm
domain_to_categories.sqlite-journal       prefs.js                                webappsstore.sqlite-wal
ExperimentStoreData.json                  protections.sqlite                       xulstore.json
extension-preferences.json                 saved-telemetry-pings
extensions.json                           search.json.mozlz4
```

Step 8: Accessing the Firefox places.sqlite database, which stores the user's browsing history and other activity.

Command: `table` to access visits counts, history, timestamps, and bookmark.

```
(root@kali)-[/mnt/ntfs/Mozilla/Firefox/Profiles/94mc0c08.default-release]
# cp -r places.sqlite /home/kali/Firefox_artifacts

(root@kali)-[/mnt/ntfs/Mozilla/Firefox/Profiles/94mc0c08.default-release]
# cd /home/kali/Firefox_artifacts

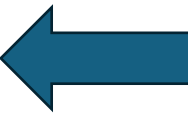
(root@kali)-[/home/kali/Firefox_artifacts]
# sqlite3 places.sqlite
SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> .tables
moz_anno_attributes      moz_meta
moz_annos                moz_newtab_story_click
moz_bookmarks            moz_newtab_story_impression
moz_bookmarks_deleted   moz_origins
moz_historyvisits        moz_places
moz_historyvisits_extra  moz_places_extra
moz_inpuhistory          moz_places_metadata
moz_items_annos          moz_places_metadata_search_queries
moz_keywords             moz_previews_tombstones
sqlite> 
```

Step 9: Retrieve everything from the database.

```

moz_places_metadata_search_queries
moz_keywords
moz_previews_tombstones
sqlite> SELECT * FROM moz_places
... > ;
1|https://support.mozilla.org/products/firefox||gro.allizom.troppus.|0|0|0|137||YdX3YiHcydsG|1|47358327123126||||1|0|1|
2|https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-browser&utm_medium=default-bookmarks&utm_campaign=customize||gro.allizom.troppus.|0|0|0|137||IM-cmSAXM7cX|1|47359956450016||||1|0|1|
3|https://www.mozilla.org/contribute/||gro.allizom.www.|0|0|0|137||2LNHYC4AKPM|1|47357364218428||||2|0|1|
4|https://www.mozilla.org/about/||gro.allizom.www.|0|0|0|137||R184PsowrOX3|1|47357608426557||||2|0|1|
5|http://192.168.17.196/Directory listing for /|691.71.861.291.|1|0|1|1950|1752965540736000|w_96dd6lhaMx|0|125510908127155||||3|0|1|
6|http://192.168.17.196/1.exe|1.exe|691.71.861.291.|0|0|0|0|1752965543274000|m9KifokjWtbL|0|125510180464706||||3|0|1|
7|https://dotnet.microsoft.com/en-us/download/dotnet/9.0|Download .NET 9.0 (Linux, macOS, and Windows) | .NET|moc.tfosorcim.tentod.|1|0|0|100|1752969794668000|P5Pv7tBIXmY6|0|47358809481181|.NET 9.0 downloads for Linux, macOS, and Windows. .NET is a free, cross-platform, open-source developer platform for building many different types of applications.|https://dotnet.microsoft.com/blob-assets/images/dotnet-icons/square.png||4|0|1|
8|https://dotnet.microsoft.com/en-us/download/dotnet/thank-you/sdk-9.0.303-windows-x64-installer|Download .NET 9.0 SDK (v9.0.303) - Windows x64 Installer|moc.tfosorcim.tentod.|1|0|0|100|1752969810705000|KSfUQUKvdeOn|0|47360487949388||https://dotnet.microsoft.com/blob-assets/images/dotnet-icons/square.png||4|0|1|
9|https://builds.dotnet.microsoft.com/dotnet/Sdk/9.0.303/dotnet-sdk-9.0.303-win-x64.exe|dotnet-sdk-9.0.303-win-x64.exe|moc.tfosorcim.tentod.sdliub.|0|0|0|0|1752969811583000|TD8UNOMphhR7|0|47359848746365||||5|0|1|

```



The database contains a link to an executable

**Step 10:** Retrieve the timestamp for the last visit.

Command

```

CREATE INDEX moz_places_originidindex ON moz_places (origin_id);
CREATE INDEX moz_places_altfrecencyindex ON moz_places (alt_frecency);
sqlite> SELECT DATETIME(last_visit_date/1000000, 'unixepoch') FROM moz_places WHERE id=6
... > ;
1|2025-07-19 22:52:23
sqlite>

```

**Result:** As shown in the screenshot, the browser appears to have last been used on 19<sup>th</sup> /07/2025 at 10:52 PM.

Status: worked

**Findings:**

The latest visit appears to have occurred on 19/07/2025 at 10:52 PM. Upon analyzing the URL's user interactions, a suspicious IP was found linking to an executable, which could potentially be malware or related to other malicious activity. This executable warrants a thorough investigation for possible compromise, unauthorized access, or misuse.

## Conclusion

The presence of executable links and a suspicious IP address indicates potentially malicious activity. The web browser was last accessed on 19th July 2025 at 10:52 PM. Further analysis of downloads, cookies, and the WebAppStore SQLite database is recommended, along with scanning system logs for potential threats.