MissionName

BritishBot

History Background

Claire and Ethan are at the library, looking for the librarian who might have information about the code snippets. Claire asks a bot in the library for information.

Technical High-Level Overview

An obfuscated code is provided to the player. The goal of this challenge is to carry out all the necessary activities to analyse the evidence and get the malicious URL provided by Britishbot.

Short Description

You´re going to analyse a Windows evidence provided by the BOT. Your goal is to find a malicious URL, the whole URL, including the ending.

Mission Description

You´re going to analyse a Windows evidence provided by the BOT. This time, the bot has prepared an special challenge for you based on a malicious domain. Your goal is to find a malicious URL, the whole URL, including the ending.

Location

LONDON | BRITISH LIBRARY

Tools

- dumpzilla https://github.com/Busindre/dumpzilla
- ewf-tools
- OpenOffice: apt-get update && apt-get -y install libreoffice
- git clone https://github.com/log2timeline/plaso.git

Questions

Which is the hostname of the evidence provided?

- DESKTOP-4LBNI7L

The file you used to solve the challenge, which type of file was?

- GZIP

Items

1. Check browsers installed.
2. Check History on Firefox browser.
3. Check cached files on Firefox browser.

Write Up

Install EWF tools and mount the forensic image provided:

- sudo apt install ewf-tools
- sudo mkdir /mnt/forensic_image
- sudo ewfmount IMAGE.E01 /mnt/forensic_image/
- sudo mkdir /home/kali/mountpoint
- fdisk -l /mnt/forensic_image/ewf1

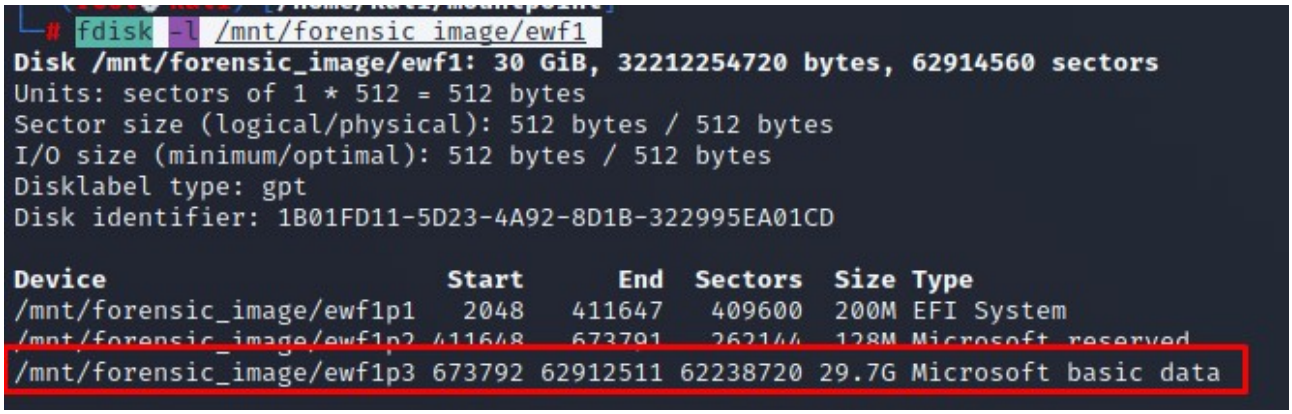


Figure 1

Above image, shows offset to mount the necessary partition on Linux, finally launch the following command:

- mount /mnt/forensic_image/**ewf1** /home/kali/mountpoint -o ro,loop,show_sys_files,streams_interace=windows,offset=$((**673792***512))

```
┌──(root💀kali)-[/home/kali/mountpoint]
└─# ls -l
total 1241508
-rwxrwxrwx 1 root root       2560 Jul 19 23:28 '$AttrDef'
-rwxrwxrwx 1 root root          0 Jul 19 23:28 '$BadClus'
-rwxrwxrwx 1 root root     972480 Jul 19 23:28 '$Bitmap'
-rwxrwxrwx 1 root root       8192 Jul 19 23:28 '$Boot'
drwxrwxrwx 1 root root          0 Jul 19 23:28 '$Extend'
-rwxrwxrwx 1 root root   43515904 Jul 19 23:28 '$LogFile'
-rwxrwxrwx 1 root root       4096 Jul 19 23:28 '$MFTMirr'
drwxrwxrwx 1 root root          0 Jul 19 13:35 '$Recycle.Bin'
---------- 1 root root          0 Jul 19 23:28 '$Secure'
-rwxrwxrwx 1 root root     131072 Jul 19 23:28 '$UpCase'
-rwxrwxrwx 1 root root          0 Jul 19 23:28 '$Volume'
drwxrwxrwx 1 root root       4096 Jul 19 15:57 '$WINDOWS.~BT'
drwxrwxrwx 1 root root          0 Jul 19 15:43 '$WinREAgent'
lrwxrwxrwx 2 root root         27 Jul 19 13:34 'Documents and Settings' → /home/kali/mountpoint/Users
-rwxrwxrwx 1 root root 1209847808 Jul 19 16:19  pagefile.sys
drwxrwxrwx 1 root root          0 Mar 19  2019  PerfLogs
drwxrwxrwx 1 root root       4096 Jul 19 13:44  ProgramData
drwxrwxrwx 1 root root       4096 Jul 19 15:52 'Program Files'
drwxrwxrwx 1 root root       4096 Jul 19 13:44 'Program Files (x86)'
drwxrwxrwx 1 root root          0 Jul 19 22:34  Recovery
-rwxrwxrwx 1 root root   16777216 Jul 19 13:37  swapfile.sys
drwxrwxrwx 1 root root       4096 Jul 19 13:41 'System Volume Information'
drwxrwxrwx 1 root root       4096 Jul 19 13:35  Users
drwxrwxrwx 1 root root      16384 Jul 19 15:57  Windows
```

Figure 2

Check users on the image mounted:

```
┌──(root💀kali)-[/home/kali/mountpoint/Users]
└─# tree -L 1
.
├── All Users → /home/kali/mountpoint/ProgramData
├── britishbot
├── Default
├── Default User → /home/kali/mountpoint/Users/Default
├── desktop.ini
└── Public
```

Figure 3

Check all browsers installed:

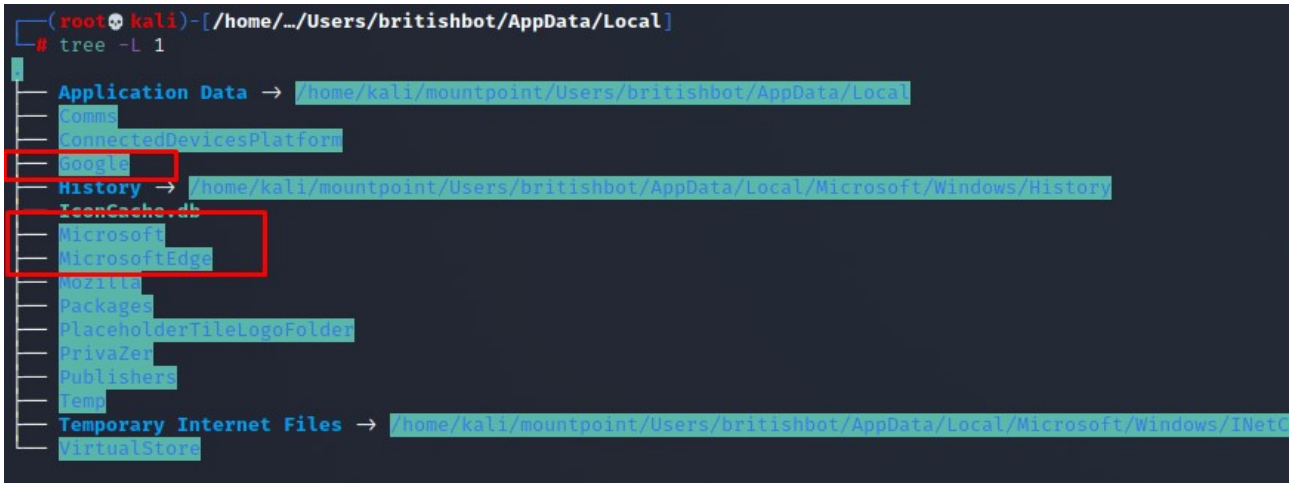


Figure 4

Player must find a malicious domain. Player could make a timeline, as we are talking about domains, we should only make timelines related to browsing.

webhist	binary_cookies, chrome_cache, chrome_preferences, esedb/msie_webcache, firefox_cache, java_idx, msiecf, opera_global, opera_typed_history, plist/safari_history, sqlite/chrome_8_history, sqlite/chrome_17_cookies, sqlite/chrome_27_history, sqlite/chrome_66_cookies, sqlite/chrome_autofill, sqlite/chrome_extension_activity, sqlite/firefox_cookies, sqlite/firefox_downloads, sqlite/firefox_history, sqlite/safari_historydb

- log2timeline --parsers="webhist" --status_view window /home/recon/Desktop/08_BritishBot/hard/evidence/image.E01

After launching timeline, it´s essential to select the good partition:

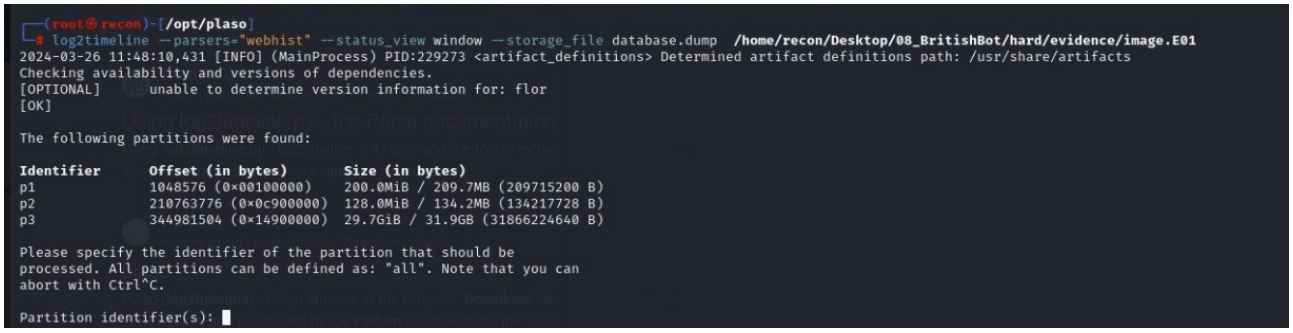


Figure 5

Finally plaso is working:

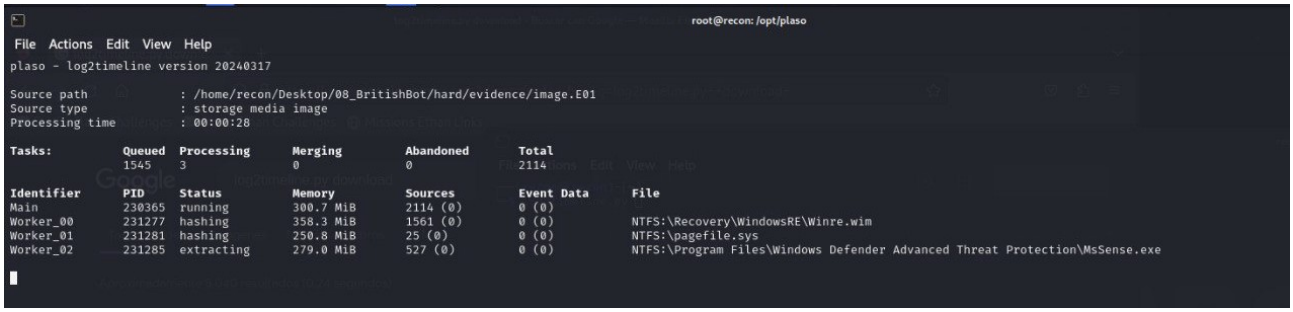


Figure 6

Once timeline, finishes, we should check events located, launching:

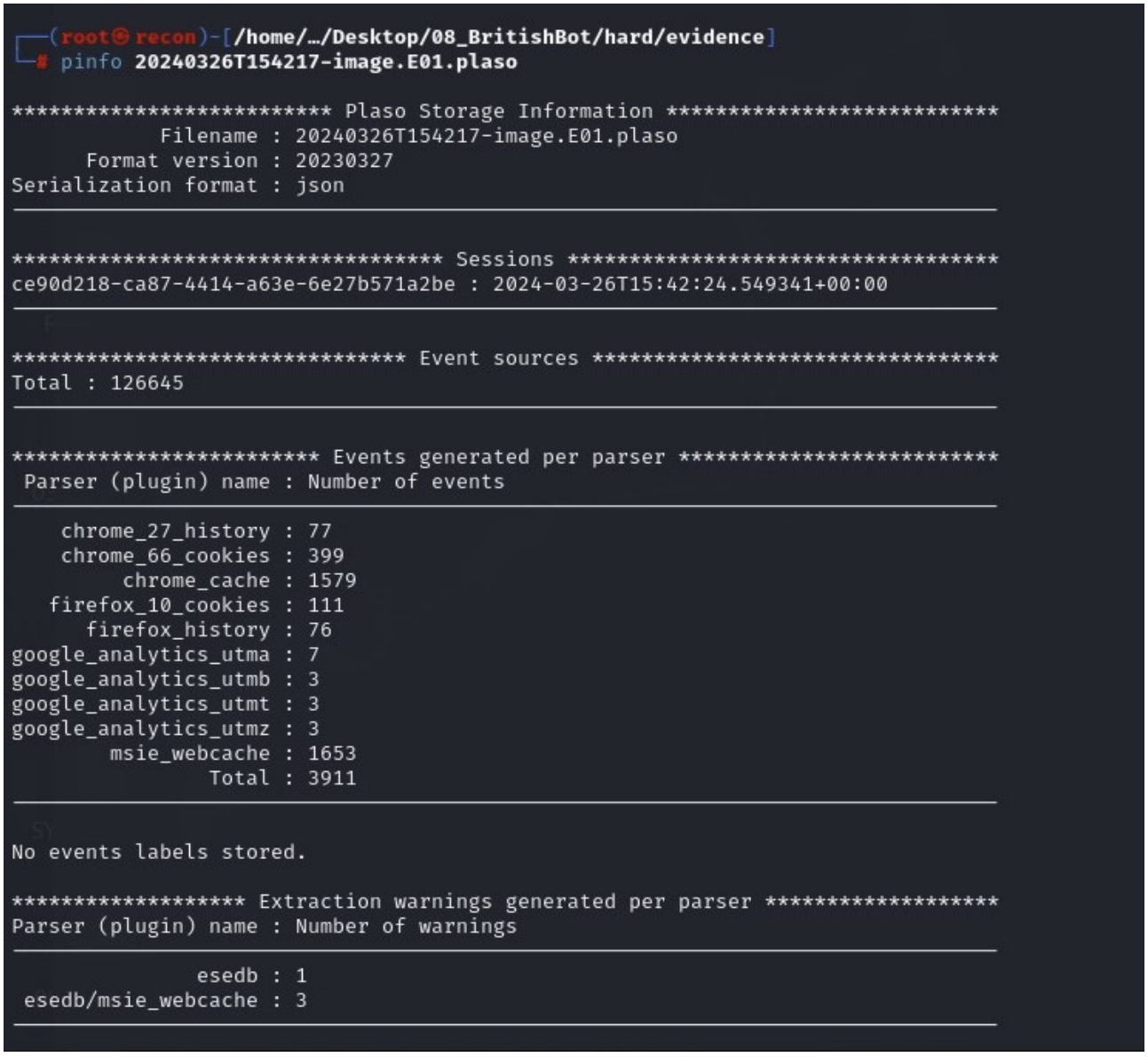


Figure 7

Next step would to extract information from database.dump:

- psort.py database.dump --output_time_zone "UTC" -o L2tcsv -w super-timeline.csv

```
┌──(root💀kali)-[/home/kali]
└─# psort.py database.dump --output_time_zone "UTC" -o L2tcsv -w super-timeline.csv
```

Figure 8

```
plaso - psort version 20201007

Storage file            : database.dump
Processing time         : 00:00:01

Events:         Filtered        In time slice   Duplicates      MACB grouped    Total
                0               0               0               1188            3627

Identifier              PID     Status          Memory          Events          Tags    Reports
Main                    4166    exporting       89.5 MiB        3627 (203)      0 (0)   0 (0)
```

Figure 9

Open the CSV file generated (super-timeline.csv), using Open office:

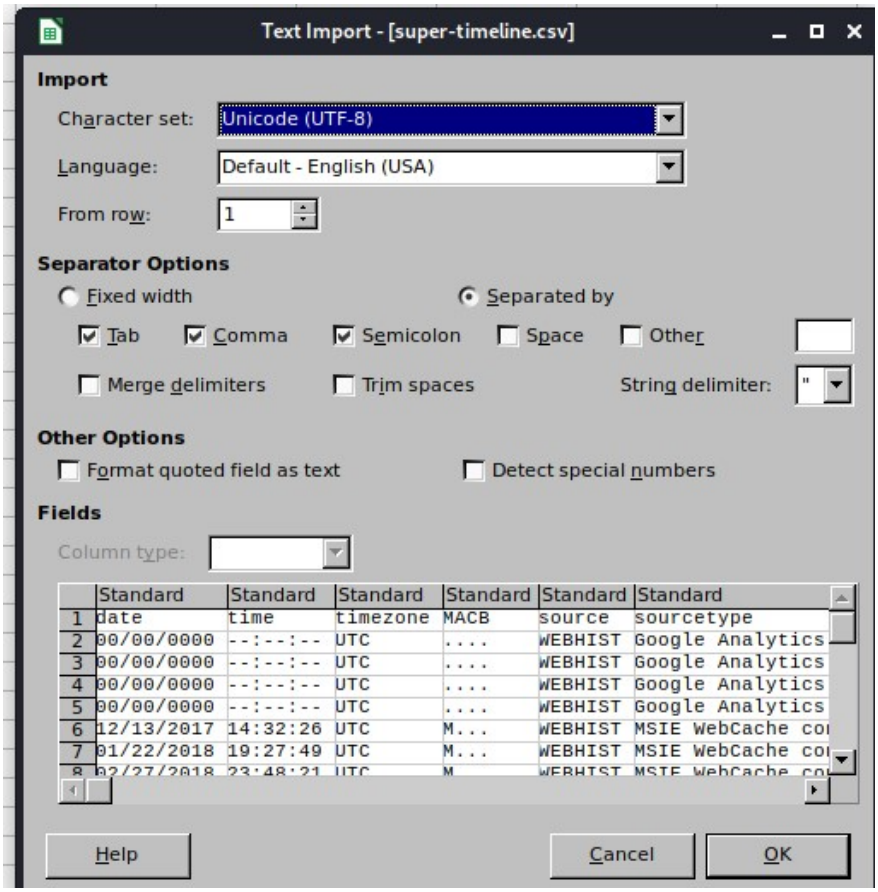


Figure 10

Filter **sourcetype** column:

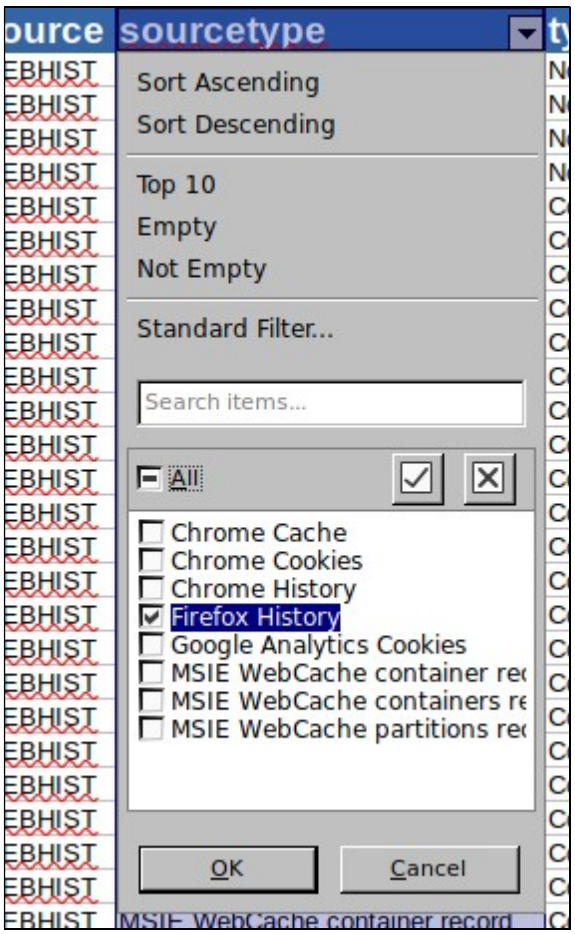
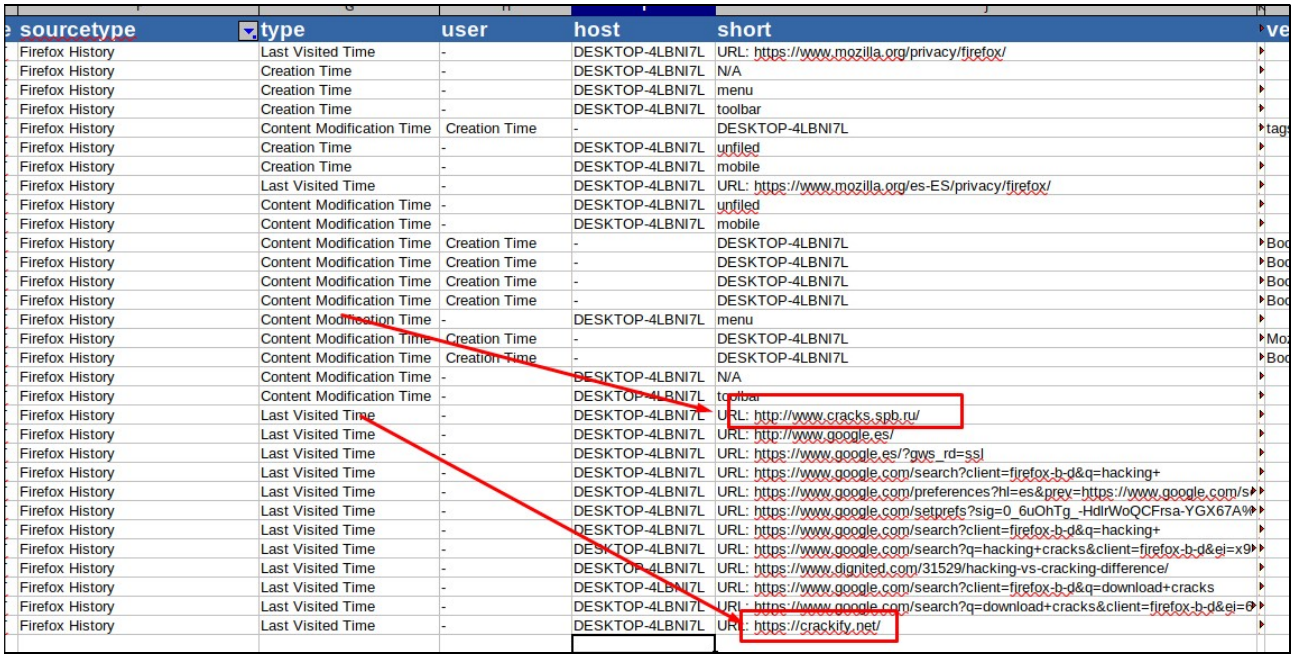


Figure 11



sourcetype	type	user	host	short	ve
Firefox History	Last Visited Time	-	DESKTOP-4LBNI7L	URL: https://www.mozilla.org/privacy/firefox/	
Firefox History	Creation Time	-	DESKTOP-4LBNI7L	N/A	
Firefox History	Creation Time	-	DESKTOP-4LBNI7L	menu	
Firefox History	Creation Time	-	DESKTOP-4LBNI7L	toolbar	
Firefox History	Content Modification Time	Creation Time	-	DESKTOP-4LBNI7L	tag
Firefox History	Creation Time	-	DESKTOP-4LBNI7L	unfiled	
Firefox History	Creation Time	-	DESKTOP-4LBNI7L	mobile	
Firefox History	Last Visited Time	-	DESKTOP-4LBNI7L	URL: https://www.mozilla.org/es-ES/privacy/firefox/	
Firefox History	Content Modification Time	-	DESKTOP-4LBNI7L	unfiled	
Firefox History	Content Modification Time	-	DESKTOP-4LBNI7L	mobile	
Firefox History	Content Modification Time	Creation Time	-	DESKTOP-4LBNI7L	Boo
Firefox History	Content Modification Time	Creation Time	-	DESKTOP-4LBNI7L	Boo
Firefox History	Content Modification Time	Creation Time	-	DESKTOP-4LBNI7L	Boo
Firefox History	Content Modification Time	Creation Time	-	DESKTOP-4LBNI7L	Boo
Firefox History	Content Modification Time	-	DESKTOP-4LBNI7L	menu	
Firefox History	Content Modification Time	Creation Time	-	DESKTOP-4LBNI7L	Moz
Firefox History	Content Modification Time	Creation Time	-	DESKTOP-4LBNI7L	Boo
Firefox History	Content Modification Time	-	DESKTOP-4LBNI7L	N/A	
Firefox History	Content Modification Time	-	DESKTOP-4LBNI7L	toolbar	
Firefox History	Last Visited Time	-	DESKTOP-4LBNI7L	URL: http://www.cracks.spb.ru/	
Firefox History	Last Visited Time	-	DESKTOP-4LBNI7L	URL: http://www.google.es/	
Firefox History	Last Visited Time	-	DESKTOP-4LBNI7L	URL: https://www.google.es/?gws_rd=ssl	
Firefox History	Last Visited Time	-	DESKTOP-4LBNI7L	URL: https://www.google.com/search?client=firefox-b-d&q=hacking+	
Firefox History	Last Visited Time	-	DESKTOP-4LBNI7L	URL: https://www.google.com/preferences?hl=es&prev=https://www.google.com/s	
Firefox History	Last Visited Time	-	DESKTOP-4LBNI7L	URL: https://www.google.com/setprefs?sig=0_6uOhTg_-HdlrWoQCFrsa-YGX67A%3	
Firefox History	Last Visited Time	-	DESKTOP-4LBNI7L	URL: https://www.google.com/search?client=firefox-b-d&q=hacking+	
Firefox History	Last Visited Time	-	DESKTOP-4LBNI7L	URL: https://www.google.com/search?q=hacking+cracks&client=firefox-b-d&ei=x9	
Firefox History	Last Visited Time	-	DESKTOP-4LBNI7L	URL: https://www.dignited.com/31529/hacking-vs-cracking-difference/	
Firefox History	Last Visited Time	-	DESKTOP-4LBNI7L	URL: https://www.google.com/search?client=firefox-b-d&q=download+cracks	
Firefox History	Last Visited Time	-	DESKTOP-4LBNI7L	URL: https://www.google.com/search?q=download+cracks&client=firefox-b-d&ei=6	
Firefox History	Last Visited Time	-	DESKTOP-4LBNI7L	URL: https://crackify.net/	

Figure 12

Below image shows potential malicious domains, based on Cracking Software. Next step would to download a tool to get more info about Firefox History:

- git clone https://github.com/Busindre/dumpzilla.git
- cd dumpzilla
- python3 dumpzilla.py /home/kali/mountpoint/Users/britishbot/AppData/Roaming/Mozilla/Firefox/Profiles/dl5b4622.default-release

Total information:

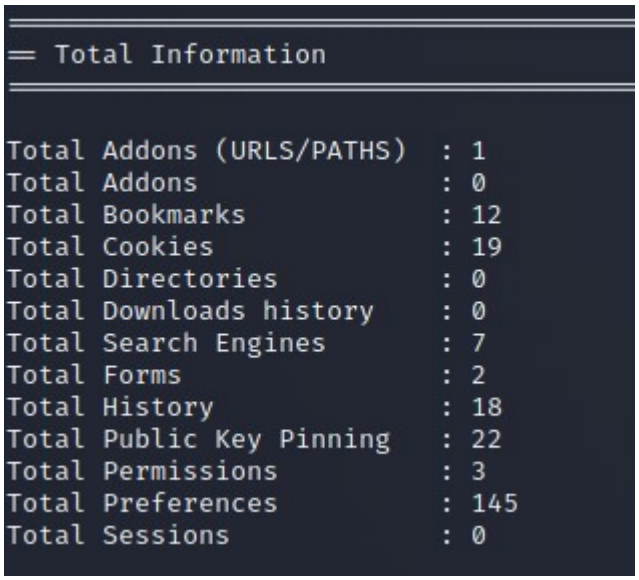


Figure 13

- python3 dumpzilla.py /home/kali/mountpoint/Users/britishbot/AppData/Roaming/Mozilla/Firefox/Profiles/dl5b4622.default-release –Downloads

To get Downloads:

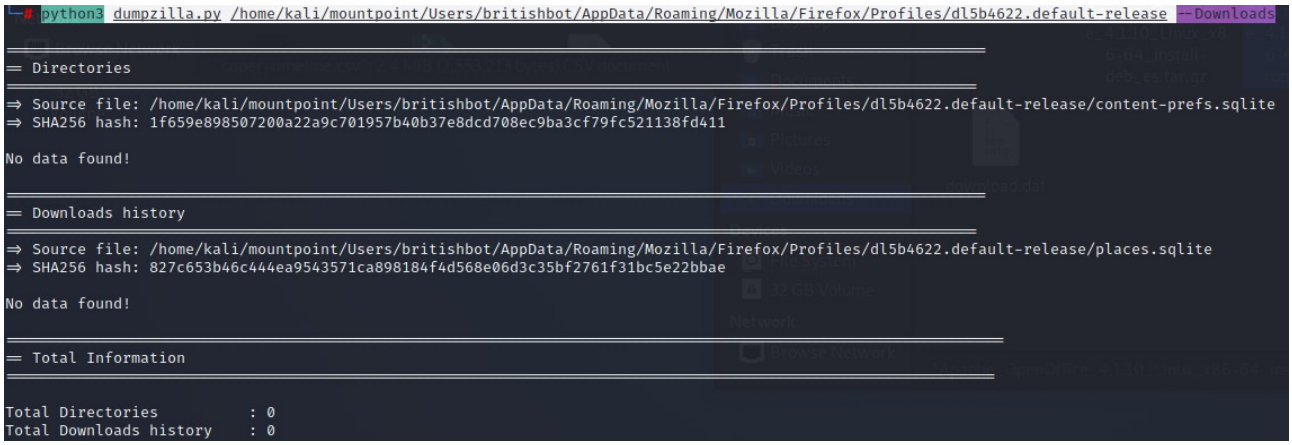


Figure 14

In this point we have to investigate cached files:

- /home/kali/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/dl5b4622.default-release/cache2/entries

Install zutils :

- apt-get install zutils

We need to extract domains from cached files, in order to identified malicious domain:

- zgrep -Eor '(http|https)://[^/"]+' /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/dl5b4622.default-release/cache2/entries/ | sort | uniq -c | sort -n

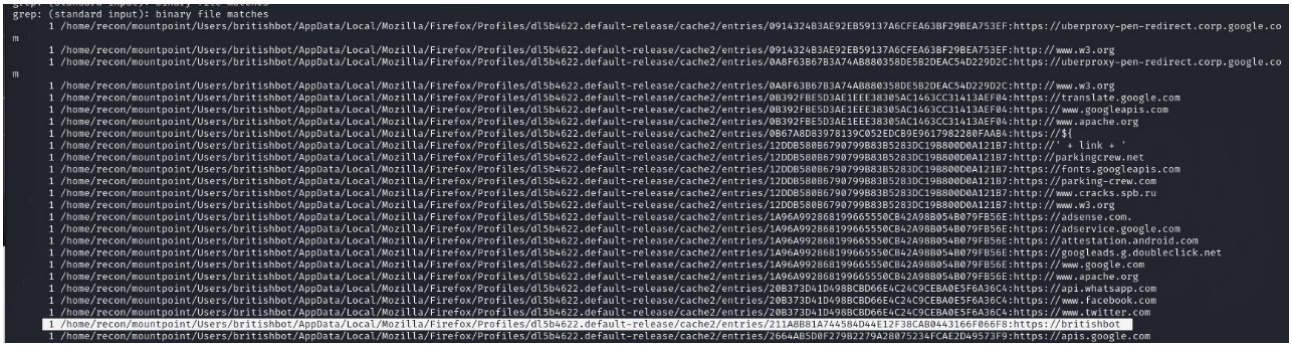


Figure 15

Above image, shows a big clue related to the name of this challenge: **https://britishbot.com**

Finally, launch Zgrep command to extract the content:

```
zgrep "britishbot" 211A8B81A744584D44E12F38CAB0443166F066F8
```

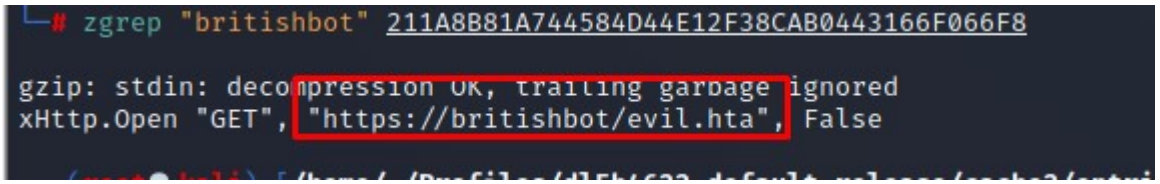


Figure 16

The malicious URL is: https://britishbot/evil.hta

Flag Information

flag{https://britishbot/evil.hta }