

## Lab 11: Investigating browser history

### What You Need for this lab

- Install Virtualbox : <https://www.virtualbox.org/wiki/Downloads>
- Install Kali 2021.4. : <https://old.kali.org/kali-images/kali-2021.4/>
  - Notes: Suggest You configure the disk size of Kali VM 80G because the size of each leakage cases image is 30G+
- Image “cfreds\_2015\_data\_leakage\_pc.dd” from Lab 5

### Goals

- Understand the application layer of a computer system that generates evidence
- Understand the behavioral model of an application
- The approach to investigating browser history (evidence generated by an application)
- Familiar with important tools for browser investigations

### Step 1

- Set up loop device (a pseudo-**device** that makes a file accessible as a block **device**)

```
losetup --partscan --find --show --read-only cfreds_2015_data_leakage_pc.dd
```

```
mkdir /mnt/loopdev
```

```
mount -o ro,loop,offset=206848 cfreds_2015_data_leakage_pc.dd /mnt/loopdev
```

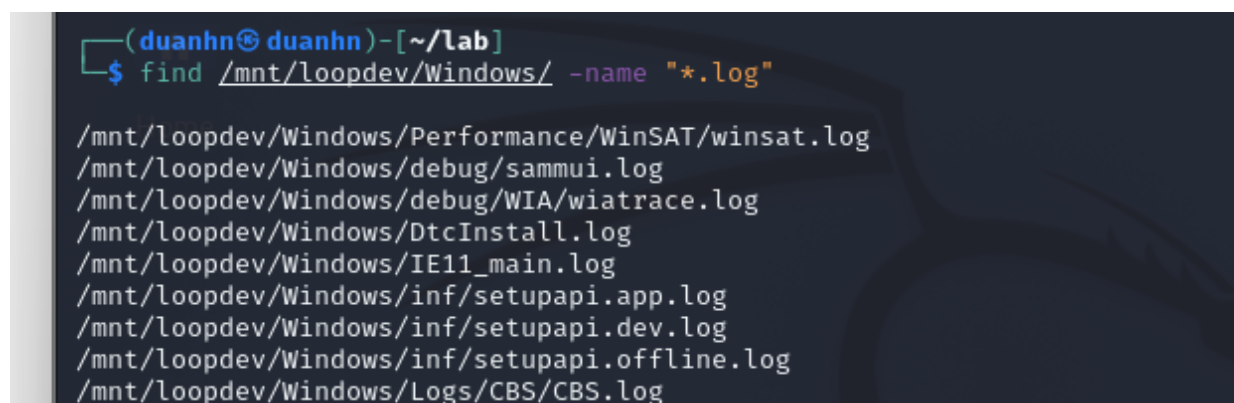


```
(duanhn@duanhn)-[~/Lab]
$ sudo losetup --partscan --find --show --read-only cfreds_2015_data_leakage_pc.dd

[sudo] password for duanhn:
/dev/loop0

(duanhn@duanhn)-[~/Lab]
$
```

- Check all versions of IE via .log



```
(duanhn@duanhn)-[~/Lab]
$ find /mnt/loopdev/Windows/ -name "*.log"

/mnt/loopdev/Windows/Performance/WinSAT/winsat.log
/mnt/loopdev/Windows/debug/sammui.log
/mnt/loopdev/Windows/debug/WIA/wiatrace.log
/mnt/loopdev/Windows/DtcInstall.log
/mnt/loopdev/Windows/IE11_main.log
/mnt/loopdev/Windows/inf/setupapi.app.log
/mnt/loopdev/Windows/inf/setupapi.dev.log
/mnt/loopdev/Windows/inf/setupapi.offline.log
/mnt/loopdev/Windows/Logs/CBS/CBS.log
```

- Exam IE logs

```
(duanhn@duanhn)~[~/Lab]
$ cat /mnt/loopdev/Windows/IE11 main.log | head

00:00.000: =====
00:00.000: Started: 2015/03/22 (Y/M/D) 11:12:32.577 (local)
00:00.000: Time Format in this log: MM:ss.mmm (minutes:seconds.milliseconds)
00:00.000: Command line: "C:\Users\informant\Desktop\Download\IE11-Windows6.1-x64-en-us.exe"
00:00.000: INFO: Setup installer for Internet Explorer: 11.0.9600.16428
00:00.000: INFO: Previous version of Internet Explorer: 8.0.7601.17514
00:00.015: INFO: Checking if iexplore.exe's current version is between 11.0.9600.0 ...
00:00.015: INFO: ... and 11.1.0.0 ...
00:00.015: INFO: Maximum version on which to run IEAK branding is: 11.1.0.0 ...
00:00.015: INFO: iexplore.exe version check success. Install can proceed.

(duanhn@duanhn)~[~/Lab]
```

- Can you find the version number?

Use Windows Registry hive shell (*hivexsh*)

- Install *hivexsh*

```
(duanhn@duanhn)~[~/Lab]
$ sudo apt-get install libhivex-bin
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  attr blt bluez-obexd cython3 dcmraw ettercap-common ettercap-graphical evolution-data-server-common fastjar
  figlet finger firebird3.0-common firebird3.0-common-doc flac fonts-font-awesome fonts-lyx fonts-roboto-slab
  freetds-common g++-11 gdal-data geoclue-2.0 gir1.2-atk-1.0 gir1.2-atspi-2.0 gir1.2-ayatanaappindicator3-0.1
  gir1.2-freedesktop gir1.2-gdkpixbuf-2.0 gir1.2-gstreamer-1.0 gir1.2-gtk-3.0 gir1.2-gtksource-3.0
  gir1.2-harfbuzz-0.0 gir1.2-javascriptcoregtk-4.0 gir1.2-nm-1.0 gir1.2-pango-1.0 gir1.2-soup-2.4 gir1.2-vte-2.91
  gir1.2-webkit2-4.0 gir1.2-wnck-3.0 gir1.2-xfconf-0 gnome-keyring gnome-keyring-pkcs11 graphviz hwloc
```

- Exam the version of IE using *hivexsh*

```
(duanhn@duanhn)~[~/Lab]
$ hivexsh

Welcome to hivexsh, the hivex interactive shell for examining
Windows Registry binary hive files.

Type: 'help' for help summary
      'quit' to quit the shell

> load SOFTWARE
hivexsh: failed to open hive file: SOFTWARE: No such file or directory

If you think this file is a valid Windows binary hive file (_not_
a regedit *.reg file) then please run this command again using the
hivexsh option '-d' and attach the complete output _and_ the hive file
which fails into a bug report at https://bugzilla.redhat.com/

> /mnt/loopdev/Windows/System32/config/SOFTWARE
hivexsh: you must load a hive file first using 'load hivefile'
> load /mnt/loopdev/Windows/System32/config/SOFTWARE
SOFTWARE\> cd Microsoft\Internet Explorer
SOFTWARE\Microsoft\Internet Explorer> lsval svcVersion
11.0.9600.17691
SOFTWARE\Microsoft\Internet Explorer> █
```

## Step 2.

Identify directory/file paths related to the web browser history

/mnt/loopdev/Users/informant/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat

C:\Users\<username>\AppData\Local\Microsoft\Windows\History\

C:\Users\<username>\AppData\Local\Microsoft\Windows\Temporary Internet Files\

/mnt/loopdev/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History

- Internet Explorer 11 History

```
(duanhn@duanhn)-[~/Lab]
$ find /mnt/loopdev/Users/informant/AppData/Local/Microsoft/Windows/WebCache

/mnt/loopdev/Users/informant/AppData/Local/Microsoft/Windows/WebCache
/mnt/loopdev/Users/informant/AppData/Local/Microsoft/Windows/WebCache/V01.chk
/mnt/loopdev/Users/informant/AppData/Local/Microsoft/Windows/WebCache/V01.log
/mnt/loopdev/Users/informant/AppData/Local/Microsoft/Windows/WebCache/V0100024.log
/mnt/loopdev/Users/informant/AppData/Local/Microsoft/Windows/WebCache/V0100025.log
/mnt/loopdev/Users/informant/AppData/Local/Microsoft/Windows/WebCache/V01res00001.jrs
/mnt/loopdev/Users/informant/AppData/Local/Microsoft/Windows/WebCache/V01res00002.jrs
/mnt/loopdev/Users/informant/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat

(duanhn@duanhn)-[~/Lab]
$
```

- Find Google Chrome Cache, Cookies, and History

```
(duanhn@duanhn)-[~/Lab]
$ ls -l /mnt/loopdev/Users/informant/AppData/Local/Google/Chrome/User\ Data/Default | grep -Ei "Cache|Cookies|History"

drwxrwxrwx 1 root root      0 Mar 22  2015 Application Cache
drwxrwxrwx 1 root root 98304 Mar 24  2015 Cache
-rwxrwxrwx 2 root root 14212730 Mar 22  2015 ChromeDWriteFontCache
-rwxrwxrwx 1 root root 137216 Mar 24  2015 Cookies
-rwxrwxrwx 2 root root 16384 Mar 24  2015 Cookies-journal
-rwxrwxrwx 2 root root 6144 Mar 24  2015 Extension Cookies
-rwxrwxrwx 2 root root 1544 Mar 24  2015 Extension Cookies-journal
drwxrwxrwx 1 root root      0 Mar 23  2015 GPUCache
-rwxrwxrwx 1 root root 135168 Mar 24  2015 History
-rwxrwxrwx 2 root root 16384 Mar 24  2015 History-journal
-rwxrwxrwx 2 root root 47175 Mar 24  2015 History Provider Cache
drwxrwxrwx 1 root root 4096 Mar 24  2015 Media Cache

(duanhn@duanhn)-[~/Lab]
$
```

What websites were the suspect accessing? (Timestamp, URL...)

- Get browser history files
- View these files

## Step 1.

Copy Three Browser History Files

Copy IE 11 History

```
(duanhn@duanhn)-[~/Lab]
$ ls -l webhistory
total 32832
-rwxr-xr-x 1 root root 33619968 Jun 29 16:16 WebCacheV01.dat

(duanhn@duanhn)-[~/Lab]
$
```

## Copy IE 8 History

```
(duanhn@duanhn)-[~/lab]
$ ls -l webhistory
total 33072
-rwxr-xr-x 1 root root 245760 Jun 29 16:18 index.dat
-rwxr-xr-x 1 root root 33619968 Jun 29 16:16 WebCacheV01.dat

(duanhn@duanhn)-[~/lab]
$ ls -l webhistory/index.dat
-rwxr-xr-x 1 root root 245760 Jun 29 16:18 webhistory/index.dat
```

## Copy Chrome History

```
(duanhn@duanhn)-[~/lab]
$ ls -l webhistory/History
-rwxr-xr-x 1 root root 135168 Jun 29 16:22 webhistory/History

(duanhn@duanhn)-[~/lab]
$
```

## Step 2.

View IE 11 History Using *libesedb*

Find the file type of *WebCacheV01.dat*

```
(duanhn@duanhn)-[~/lab]
$ file webhistory/WebCacheV01.dat
webhistory/WebCacheV01.dat: Extensible storage engine DataBase, version 0x620, checksum 0xe172001b, page size 32768, Windows version 6.1
```

- Install *libesedb*

```
(duanhn@duanhn)-[~/lab]
$ sudo apt-get install libesedb-utils -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
```

- Export *WebCacheV01.dat* to the folder *webhistory/IE11*

```
(duanhn@duanhn)-[~/lab]
$ sudo esedbexport webhistory/WebCacheV01.dat -t webhistory/IE11
esedbexport 20240627

Opening file.
Database type: MSIE WebCache.
Exporting table 1 (MSysObjects) out of 37.
Exporting table 2 (MSysObjectsShadow) out of 37.
Exporting table 3 (MSysUnicodeFixupVer2) out of 37.
Exporting table 4 (Containers) out of 37.
Exporting table 5 (Container_1) out of 37.
Exporting table 6 (Container_2) out of 37.
Exporting table 7 (Container_3) out of 37.
Exporting table 8 (Container_4) out of 37.
Exporting table 9 (Container_5) out of 37.
Exporting table 10 (Container_6) out of 37.
```

- Find the type of the file

```
(duanhn@duanhn)-[~/lab]
$ file webhistory/IE11.export/AppCache_1.21
webhistory/IE11.export/AppCache_1.21: ASCII text
(duanhn@duanhn)-[~/lab]
```

- Create three lines with three attributes

```
(duanhn@duanhn)-[~/lab]
$ echo -e "Frank manager 50000 \nAlex clerk 45000 \nEirc clerk 25000"
Frank manager 50000
Alex clerk 45000
Eirc clerk 25000
(duanhn@duanhn)-[~/lab]
```

- Select lines with the key word “manager”
- Select attributes 1 and 3

```
(duanhn@duanhn)-[~/lab]
$ echo -e "Frank manager 50000 \nAlex clerk 45000 \nEirc clerk 25000" | awk '/manager/ {print}'
Frank manager 50000

(duanhn@duanhn)-[~/lab]
$ echo -e "Frank manager 50000 \nAlex clerk 45000 \nEirc clerk 25000" | awk '/manager/ {print $1, $3}'
Frank 50000

(duanhn@duanhn)-[~/lab]
$ echo -e "Frank manager 50000 \nAlex clerk 45000 \nEirc clerk 25000" | awk '{print $1, $3}'
Frank 50000
Alex 45000
Eirc 25000

(duanhn@duanhn)-[~/lab]
$
```

- Show Row Number

```
echo -e "Frank manager 50000 \nAlex clerk 45000 \nEirc clerk 25000" | awk '{print NR, $1}'
```

```
(duanhn@duanhn)-[~/lab]
$ echo -e "Frank manager 50000 \nAlex clerk 45000 \nEirc clerk 25000" | awk '{print NR, $1}'
1 Frank
2 Alex
3 Eirc

(duanhn@duanhn)-[~/lab]
$
```

- Calculate sum

```
echo -e "Frank manager 50000 \nAlex clerk 45000 \nEirc clerk 25000" | awk '{sum += $3}; END {print sum}'
```

```
(duanhn@duanhn)-[~/lab]
$ echo -e "Frank manager 50000 \nAlex clerk 45000 \nEirc clerk 25000" | awk '{sum += $3}; END {print sum}'
120000
```

- Show field names

```
(duanhn@duanhn)-[~/lab]
$ cat webhistory/IE11.export/Container_1.4 | head -n 1
EntryId ContainerId CacheId UrlHash SecureDirectory FileSize Type Flags AccessCount SyncTime C
reationTime ExpiryTime ModifiedTime AccessedTime PostCheckTime SyncCount ExemptionDelta Url
Filename FileExtension RequestHeaders ResponseHeaders RedirectUrl Group ExtraData
```



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	EntryId	ContainerId	CacheId	UrlHash	SecureDirectory	FileSize	Type	Flags	AccessCount	SyncTime	CreationTime	ExpiryTime	ModifiedTime
2	24	1	0	1.03055020379310E+016	1	32088	69	1	1	1 Mar 23, 2015 18:12:08.194224700	Mar 23, 2015 18:12:08.084224600	Jan 01, 1601 00:00:00.000000000	Feb 27, 2015 00:47:45.000000000
3	49	1	0	8.05003838569575E+016	2	1150	69	1	1	1 Mar 23, 2015 20:45:22.349231400	Mar 23, 2015 20:45:22.308229100	Mar 24, 2015 01:05:50.308229100	Mar 20, 2015 14:36:39.000000000
4	50	1	0	8.05003869168228E+016	4	1150	69	1	1	1 Mar 23, 2015 20:56:32.953278700	Mar 23, 2015 20:56:32.953278700	Mar 24, 2015 18:56:15.953278700	Mar 20, 2015 14:36:39.000000000
5	58	1	0	6.03118138792257E+017	4	17	4161	0	1	1 Mar 23, 2015 15:15:56.842405500	Mar 25, 2015 15:15:56.842405500	Jan 01, 1601 00:00:00.000000000	Jan 01, 1601 00:00:00.000000000
6	21	1	0	9.5086571498908E+017	4	1327	65	0	1	1 Mar 23, 2015 17:28:55.700342200	Mar 23, 2015 17:28:55.690342100	Mar 30, 2015 17:28:54.690342100	Jan 01, 1601 00:00:00.000000000
7	53	1	0	9.82119349977706E+017	1	2550	69	1	1	1 Mar 23, 2015 14:47:06.132305500	Mar 25, 2015 14:47:06.116705500	Mar 24, 2016 14:47:06.116705500	May 25, 2012 05:50:00.000000000
8	40	1	0	1.01507051365704E+018	3	23223	65	2	2	2 Mar 23, 2015 20:34:08.844580200	Mar 23, 2015 20:34:08.782180100	Mar 19, 2016 23:36:29.782180100	Mar 19, 2015 23:51:21.000000000
9	46	1	0	1.01507051547304E+018	1	37098	65	2	2	2 Mar 23, 2015 20:34:09.750381800	Mar 23, 2015 20:34:09.734781800	Mar 20, 2016 00:35:46.734781800	Mar 19, 2015 23:51:21.000000000
10	39	1	0	1.01507051752252E+018	2	12780	65	3	2	2 Mar 23, 2015 20:34:08.735380000	Mar 23, 2015 20:34:08.704179900	Mar 23, 2015 21:04:08.704179900	Jan 01, 1601 00:00:00.000000000
11	44	1	0	1.01507051762795E+018	3	12771	65	3	2	2 Mar 23, 2015 20:34:09.719181800	Mar 23, 2015 20:34:09.703581700	Mar 23, 2015 21:04:09.703581700	Jan 01, 1601 00:00:00.000000000
12	42	1	0	1.02829495306628E+018	2	7595	65	1	2	2 Mar 23, 2015 20:34:09.641181800	Mar 23, 2015 20:34:09.406181100	Mar 24, 2015 20:34:09.406181100	Jan 01, 1601 00:00:00.000000000
13	45	1	0	1.12372193868294E+018	1	8522	65	2	2	2 Mar 23, 2015 20:34:09.734781800	Mar 23, 2015 20:34:09.719181800	Mar 17, 2016 23:02:56.719181800	Mar 16, 2015 21:38:46.000000000
14	43	1	0	1.12372193900529E+018	1	17836	65	0	2	2 Mar 23, 2015 20:34:09.672381700	Mar 23, 2015 20:34:09.672381700	Mar 10, 2016 13:39:25.672381700	Mar 10, 2015 20:51:43.000000000
15	30	1	0	1.12372193980654E+018	1	1619	65	0	1	1 Mar 23, 2015 20:04:18.921167800	Mar 23, 2015 20:04:18.858767700	Mar 17, 2016 23:03:02.858767700	Oct 24, 2014 21:49:35.000000000
16	32	1	0	1.12372193996051E+018	1	11156	65	0	1	1 Mar 23, 2015 20:04:18.921167800	Mar 23, 2015 20:04:18.889967700	Mar 17, 2016 23:03:01.889967700	Jul 23, 2013 19:36:21.000000000
17	31	1	0	1.12372194067089E+018	1	9005	65	0	1	1 Mar 23, 2015 20:04:18.921167800	Mar 23, 2015 20:04:18.858767700	Mar 17, 2016 23:03:02.858767700	Sep 17, 2013 00:02:19.000000000
18	35	1	0	1.12372194132048E+018	2	81351	65	0	1	1 Mar 23, 2015 20:04:54.079030200	Mar 23, 2015 20:04:53.938629900	Mar 16, 2016 01:26:55.938629900	Dec 11, 2014 00:49:41.000000000
19	34	1	0	1.64340097835678E+018	3	18719	65	0	1	1 Mar 23, 2015 20:04:19.248768400	Mar 23, 2015 20:04:19.139568200	Mar 09, 2016 01:03:24.139568200	Aug 21, 2014 18:08:10.000000000
20	33	1	0	1.64340097980202E+018	3	18218	65	0	1	1 Mar 23, 2015 20:04:19.233168400	Mar 23, 2015 20:04:19.139568200	Mar 17, 2016 23:03:01.139568200	Aug 21, 2014 18:06:58.000000000
21	11	1	0	1.67407236386841E+018	2	1102	65	1	11	11 Mar 22, 2015 15:48:45.537379300	Mar 22, 2015 15:48:45.537379300	Apr 22, 2015 15:48:45.537379300	Mar 16, 2015 05:30:18.000000000
22	8	1	0	1.67407236390956E+018	1	47346	65	3	11	11 Mar 22, 2015 15:48:45.412579100	Mar 22, 2015 15:48:45.412579100	Apr 22, 2015 15:48:45.412579100	Mar 16, 2015 05:30:12.000000000
23	9	1	0	1.67407236420281E+018	4	668	65	1	11	11 Mar 22, 2015 15:48:45.428179100	Mar 22, 2015 15:48:45.428179100	Apr 22, 2015 15:48:45.428179100	Mar 16, 2015 05:30:14.000000000
24	1	1	0	1.67407236431898E+018	2	5214	65	0	7	7 Mar 23, 2015 14:41:13.121405500	Mar 25, 2015 14:41:13.121405500	Jan 01, 1601 00:00:00.000000000	Jan 01, 1601 00:00:00.000000000
25	10	1	0	1.67407236437232E+018	3	162	65	1	11	11 Mar 22, 2015 15:48:45.521779200	Mar 22, 2015 15:48:45.521779200	Apr 22, 2015 15:48:45.521779200	Mar 16, 2015 05:30:18.000000000
26	36	1	0	1.67407236523197E+018	4	5208	65	0	1	1 Mar 23, 2015 20:26:59.199003100	Mar 23, 2015 20:26:59.199003100	Jan 01, 1601 00:00:00.000000000	Jan 01, 1601 00:00:00.000000000
27	6	1	0	1.67407236567095E+018	2	1380	65	2	11	11 Mar 22, 2015 15:48:45.287778800	Mar 22, 2015 15:48:45.287778800	Apr 22, 2015 15:48:45.287778800	Mar 16, 2015 05:30:12.000000000

- Separate fields with tab `\t` and show *ModifiedTime* and *URL*

```
awk '{print NR, $13, $18}' FS='\t' webhistory/IE11.export/Container_1.4 | head -n 5
```

```
(duanhn@duanhn)~[~/Lab]
$ awk '{print NR, $13, $18}' FS='\t' webhistory/IE11.export/Container_1.4 | head -n 5
1 ModifiedTime Url
2 Feb 27, 2015 00:47:45.000000000 https://technet.microsoft.com/favicon.ico
3 Mar 20, 2015 14:36:39.000000000 http://www.wired.com/wp-content/themes/Phoenix/assets/images/favicon.ico
4 Mar 20, 2015 14:36:39.000000000 http://www.wired.com/favicon.ico
5 Jan 01, 1601 00:00:00.000000000 https://license.piriform.com/verify/?p=ccpro&c=cc&cv=5.04.51516l=10336lk=CJ9T-J7C
U-SPNV-GWMB-WBEC&mk=YSNW-75UN-3WNW-QDJI-6UFT-T7TM-9AX9-8ZG8-USQZ
```

- Count the number records in the file

```
awk '{print NR, $13, $18}' FS='\t' webhistory/IE11.export/Container_1.4 | wc -l
```

```
(duanhn@duanhn)~[~/Lab]
$ awk '{print NR, $13, $18}' FS='\t' webhistory/IE11.export/Container_1.4 | wc -l
58
```

- Count the number records in all files start with the string “Container”

```
awk '{print NR, $13, $18}' FS='\t' webhistory/IE11.export/Container* | wc -l
```

```
(duanhn@duanhn)~[~/Lab]
$ awk '{print NR, $13, $18}' FS='\t' webhistory/IE11.export/Container* | wc -l
10248
```

### Step 3.

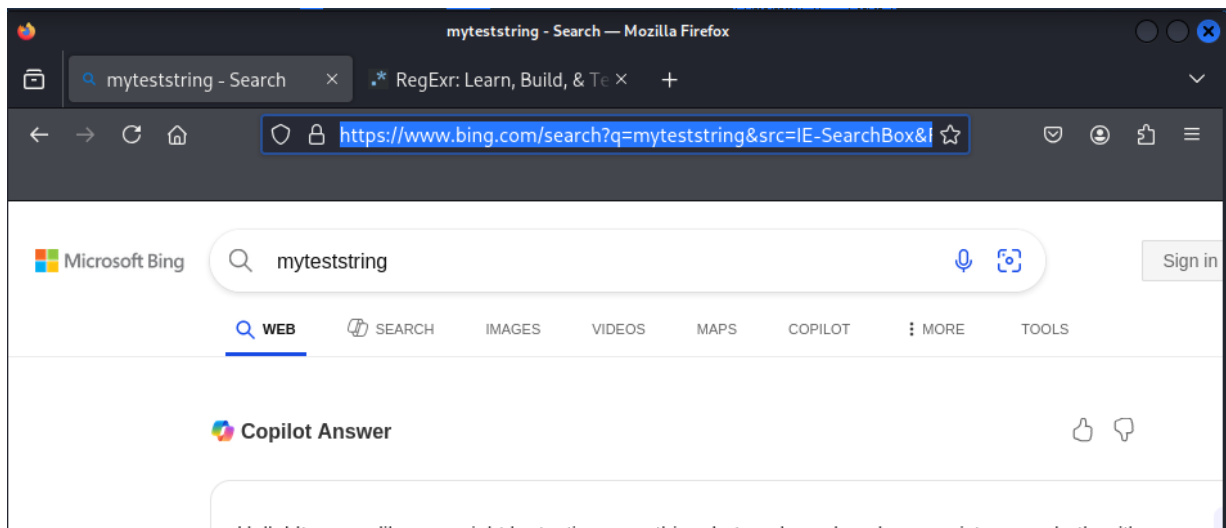
List all search keywords using web browsers. (Timestamp, URL, keyword...)

- IE browser

```
(duanhn@duanhn)~[~/Lab]
$ awk '{print NR, $13, $18}' FS='\t' webhistory/IE11.export/Container_1.4 | head -n 5
1 ModifiedTime Url
2 Feb 27, 2015 00:47:45.000000000 https://technet.microsoft.com/favicon.ico
3 Mar 20, 2015 14:36:39.000000000 http://www.wired.com/wp-content/themes/Phoenix/assets/images/favicon.ico
4 Mar 20, 2015 14:36:39.000000000 http://www.wired.com/favicon.ico
5 Jan 01, 1601 00:00:00.000000000 https://license.piriform.com/verify/?p=ccpro&c=cc&cv=5.04.51516l=10336lk=CJ9T-J7C
U-SPNV-GWMB-WBEC&mk=YSNW-75UN-3WNW-QDJI-6UFT-T7TM-9AX9-8ZG8-USQZ
```

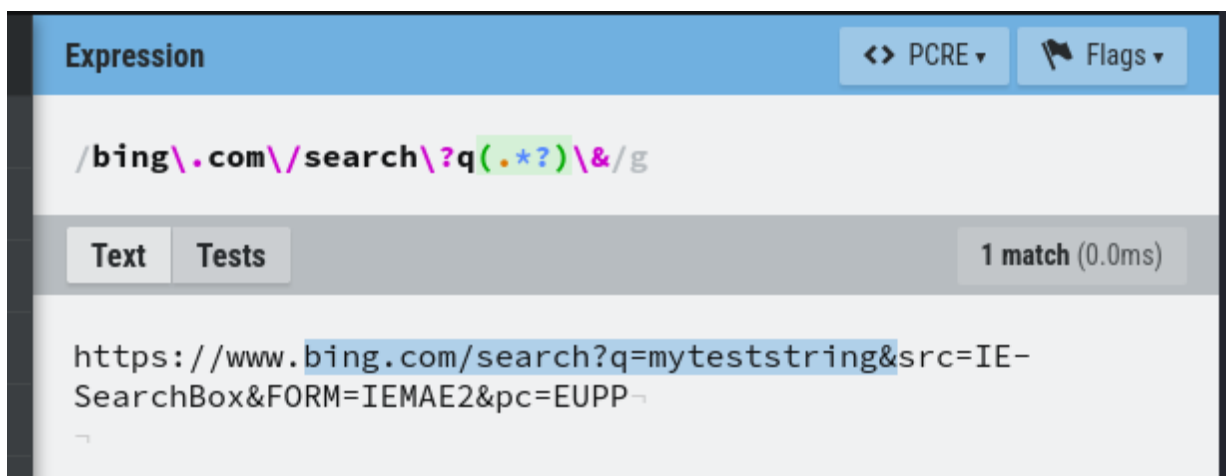
### Web Query String

<https://www.bing.com/search?q=myteststring&src=IE-SearchBox&FORM=IEMAE2&pc=EUPP>



- Regular expression for bing.com search

<https://regexr.com/>



**<http>Hello World</http>**

**<.+>: Greedy** will consume as much as possible

**<.+?>: lazy** will stop right after matching



- List IE 11 search keywords

```
(duanhn@duanhn)-[~/Lab]
$ awk '{print $34}' webhistory/IE11.export/Container* | grep -P "bing\.com\/search\?q=(.*?)\&" --color
informant@http://www.bing.com/search?q=Top+Stories&FORM=HDRSC1
informant@http://www.bing.com/search?q=external%20device%20and%20forensics&qs=n&form=QBRE&ppq=external%20device%20and%20forensics&sc=8-9&sp=-1&sk=6&cvid=c30c4b1f36114b1c9bc683838c69823a
informant@http://www.bing.com/search?q=anti-forensic+tools&qs=n&form=QLH&ppq=anti-forensic+tools&sc=8-13&sp=-1&sk=6&cvid=e799e715fa2244a5a7967675bdcca9d3
informant@http://www.bing.com/search?q=file+sharing+and+tethering&qs=n&form=QLH&ppq=file+sharing+and+tethering&sc=0-18&sp=-1&sk=6&cvid=171b77e4ffd54b2a92c4e97abf995fe1
informant@http://www.bing.com/search?q=DLP%20DRM&qs=n&form=QBRE&ppq=dlp%20drm&sc=8-7&sp=-1&sk=6&cvid=6e206ee8751e4ad89f882ed52daf3aea&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=0
informant@http://www.bing.com/search?q=what%20is%20windows%20system%20artifacts&qs=n&form=QBRE&ppq=what%20is%20windows%20system%20artifacts&sc=0-27&sp=-1&sk=6&cvid=1ef4ace146854d97acf263b53bf97b8c&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=4
informant@http://www.bing.com/search?q=Top+Stories&FORM=HDRSC1
informant@http://www.bing.com/search?q=external%20device%20and%20forensics&qs=n&form=QBRE&ppq=external%20device%20and%20forensics&sc=8-9&sp=-1&sk=6&cvid=c30c4b1f36114b1c9bc683838c69823a
informant@http://www.bing.com/search?q=external%20device%20and%20forensics&qs=n&form=QBRE&ppq=external%20device%20and%20forensics&sc=8-9&sp=-1&sk=6&cvid=c30c4b1f36114b1c9bc683838c69823a&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=9
informant@http://www.bing.com/search?q=Forensic+Email+Investigation&FORM=QSRE1&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=3
informant@http://www.bing.com/search?q=cd%20burning%20method&qs=n&form=QBRE&ppq=cd%20burning%20method&sc=8-2&sp=-1&sk=6&cvid=b7dbe6fb67424c578172ba57330a0894&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=7
```

**YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!**

Save the document with the filename "**YOUR NAME Lab 11.pdf**", replacing "YOUR NAME" with your real name.

Email the image to the instructor as an attachment to an e-mail message. Send it to: **xxx@fe.edu.vn** with a subject line of "**Lab 11 From YOUR NAME**", replacing "YOUR NAME" with your real name.