Forensic Analysis of Browsers

-SHREY DHUNGANA

- SYED ALI QASIM

Goal of the project

- Forensic analysis of the browsing data of following browsers on Ubutnu, Windows 7 and Mac OSX.
- Firefox, Google Chrome, Internet Explorer and Safari.
- Analysis of the private browsing data on volatile memory and hard drive.
- Retrieval of artifacts from the “private browsing” mode.
- Retrieval of deleted normal browsing data.
- Conclusion based on the privacy of browsers.

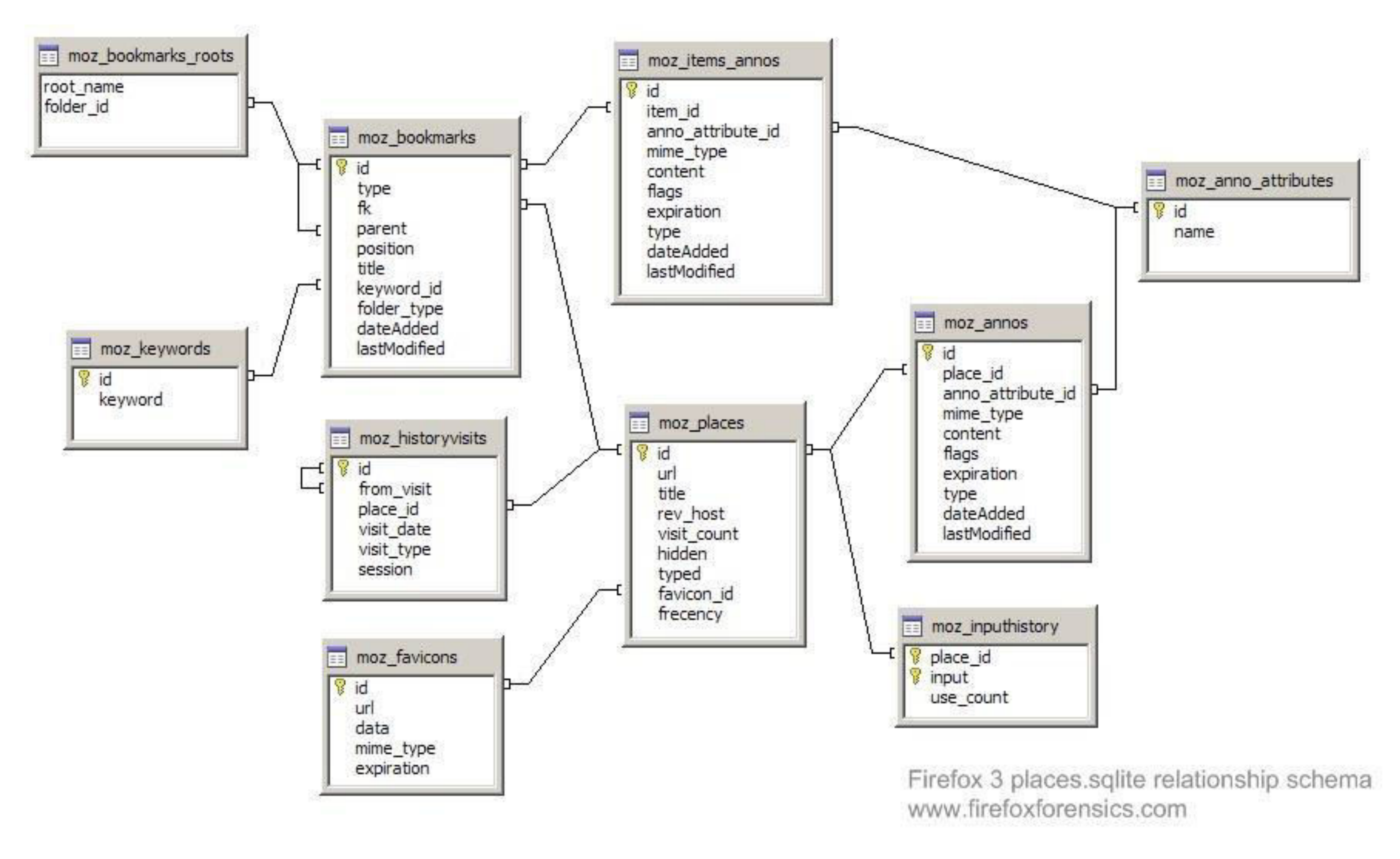
Contents

Part One : **Forensic Analysis of deleted browsing.** **Privacy – Browser Fingerprinting** **-Shrey Dhungana**	**Pages :** **5 -13** **14-6**
Part Two: Retrieval of Artifacts from Private Browsing. -Syed Ali Qasim	17 -30
Conclusion and Related Work	31-33

Introduction

- Web browsers use the **SQLite Database** to store the browsing data.
- This database structure has user history, passwords, searches, extensions, plugins, user preferences etc.
- Forensic Analysis of this database gives the complete browsing data of a user.
- Threat model – Local or Web Attacker.
- We assume an attacker/forensic analyst accesses a machine after the user has left the machine.
- Two scenarios : User can delete the browsing history or use the "private" or " incognito mode".
- Retrieval of the artifacts for Firefox, Chrome, Edge browsing sessions.

Firefox Database Structure



moz_bookmarks_roots
- root_name
- folder_id

moz_bookmarks
- id
- type
- fk
- parent
- position
- title
- keyword_id
- folder_type
- dateAdded
- lastModified

moz_keywords
- id
- keyword

moz_items_annos
- id
- item_id
- anno_attribute_id
- mime_type
- content
- flags
- expiration
- type
- dateAdded
- lastModified

moz_anno_attributes
- id
- name

moz_historyvisits
- id
- from_visit
- place_id
- visit_date
- visit_type
- session

moz_places
- id
- url
- title
- rev_host
- visit_count
- hidden
- typed
- favicon_id
- frecency

moz_annos
- id
- place_id
- anno_attribute_id
- mime_type
- content
- flags
- expiration
- type
- dateAdded
- lastModified

moz_favicons
- id
- url
- data
- mime_type
- expiration

moz_inputhistory
- place_id
- input
- use_count

Firefox 3 places.sqlite relationship schema
www.firefoxforensics.com

Implementation : Firefox

Files	Data Stored
places.sqlite	Bookmarks, history, download list
key3.db and logins.json	Password Manager, Saved Passwords
permissions.sqlite,content-prefs.sqlite	Site-specific preferences
search.json.mozlz4	Search engines
persdict.dat	Personal dictionary
formhistory.sqlite	Autocomplete history
cookie.sqlite	Cookies
prefs.js	Customized changes
Cert8.db	Security Setting and SSL certificates
webappsstore.sqlite, chromeappsstore.sqlite	Dom Storage
secmod.db	Security device settings

Implementation : Firefox

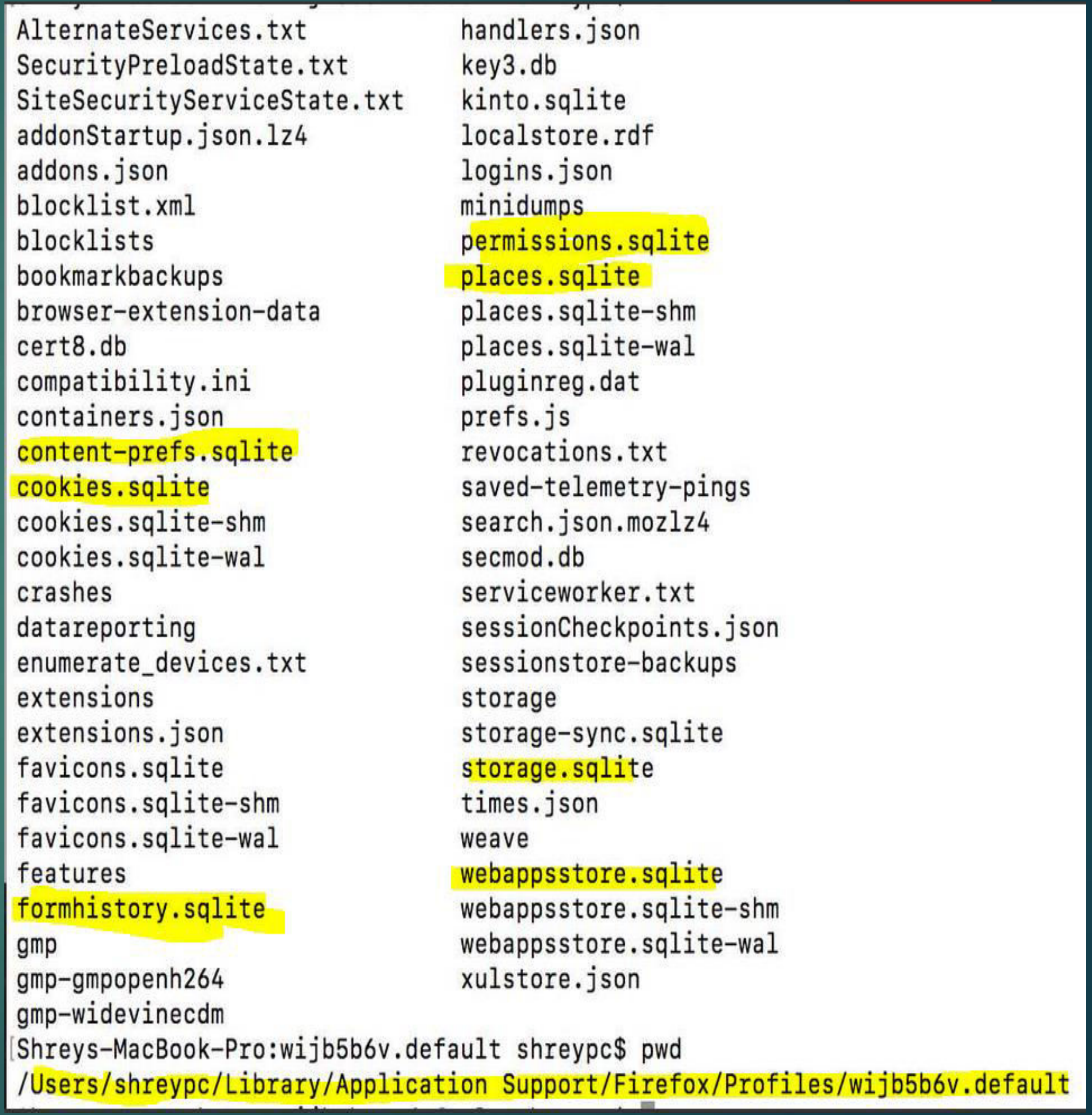
- We used OS, Ubuntu 16.04 and Windows 7 machines.
- Firefox supports multiple user profiles.
- Firefox(including 3 other browsers) do not update history file in private mode and delete other data on exit.
- Not all data is deleted.

62.0.3202.94

- In MacOS Sierra, Firefox database is found ~/Library/ApplicationSupport/Firefox/Profiles/somename.default/places.sqlite
- In Windows C:\Users\csadmin\AppData\Local\Temp\BCLTMP\firefox\places.sqlite
- In Ubuntu : /home/<user>/.mozilla/firefox/<profile folder>/places.sqlite

Implementation

- We use SQLite DB Browser to analyze the browsing data.
- In our test, we assume the local attacker gains the access after user deletes the history.
- We use file recovery software Disk Drill in macOS and Recuva in Windows 10.
- Attacker/Analyst can take the copy the database files.
- In case web attackers get access, they can not view live sessions because of lock but can steal database files.

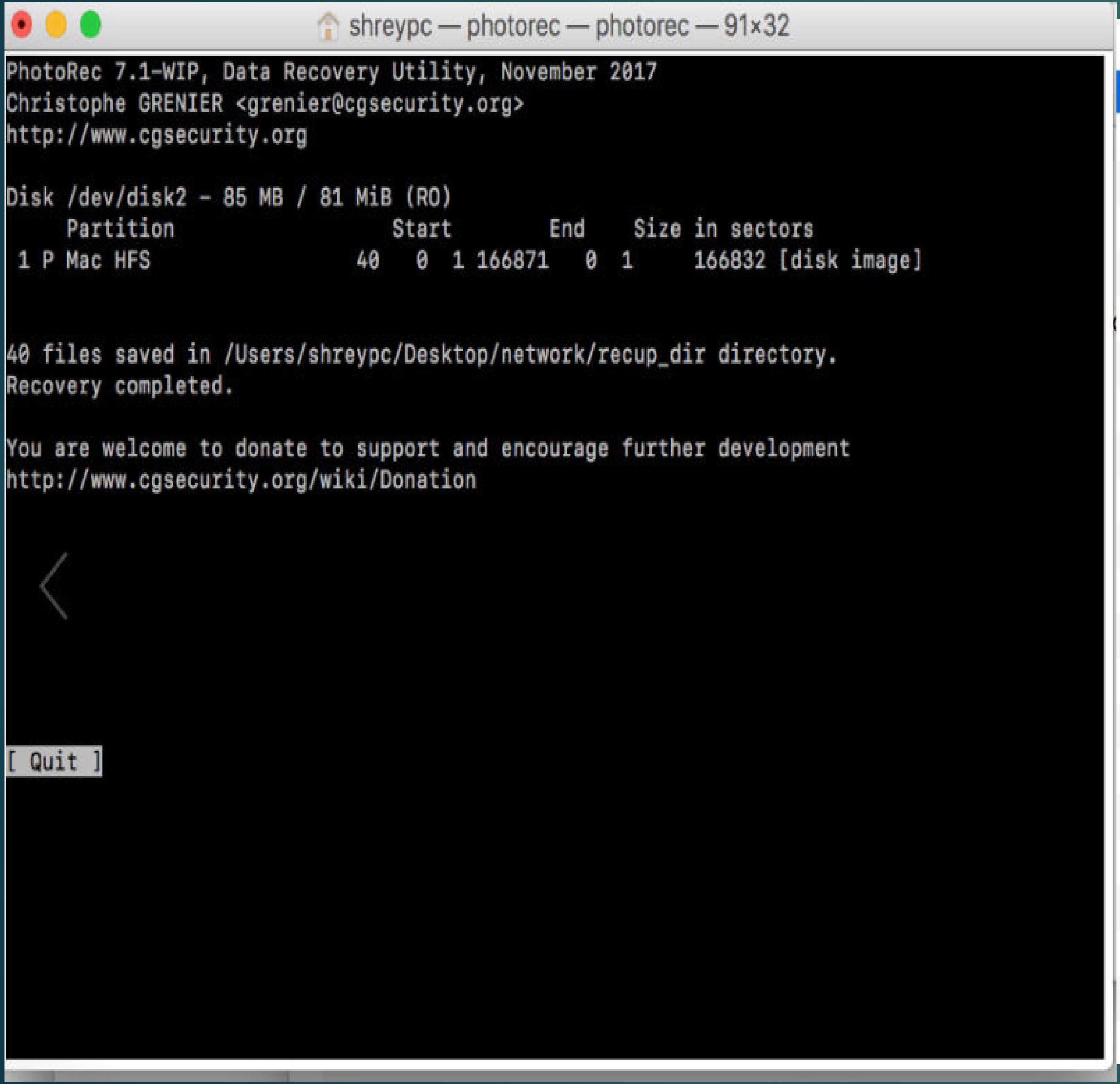


```
AlternateServices.txt           handlers.json
SecurityPreloadState.txt        key3.db
SiteSecurityServiceState.txt    kinto.sqlite
addonStartup.json.lz4           localstore.rdf
addons.json                     logins.json
blocklist.xml                   minidumps
blocklists                      permissions.sqlite
bookmarkbackups                 places.sqlite
browser-extension-data          places.sqlite-shm
cert8.db                        places.sqlite-wal
compatibility.ini               pluginreg.dat
containers.json                 prefs.js
content-prefs.sqlite            revocations.txt
cookies.sqlite                  saved-telemetry-pings
cookies.sqlite-shm              search.json.mozlz4
cookies.sqlite-wal              secmod.db
crashes                         serviceworker.txt
datareporting                   sessionCheckpoints.json
enumerate_devices.txt           sessionstore-backups
extensions                      storage
extensions.json                 storage-sync.sqlite
favicons.sqlite                 storage.sqlite
favicons.sqlite-shm             times.json
favicons.sqlite-wal             weave
features                        webappsstore.sqlite
formhistory.sqlite              webappsstore.sqlite-shm
gmp                             webappsstore.sqlite-wal
gmp-gmpopenh264                 xulstore.json
gmp-widevinecdm
[Shreys-MacBook-Pro:wijb5b6v.default shreypc$ pwd
/Users/shreypc/Library/Application Support/Firefox/Profiles/wijb5b6v.default
```

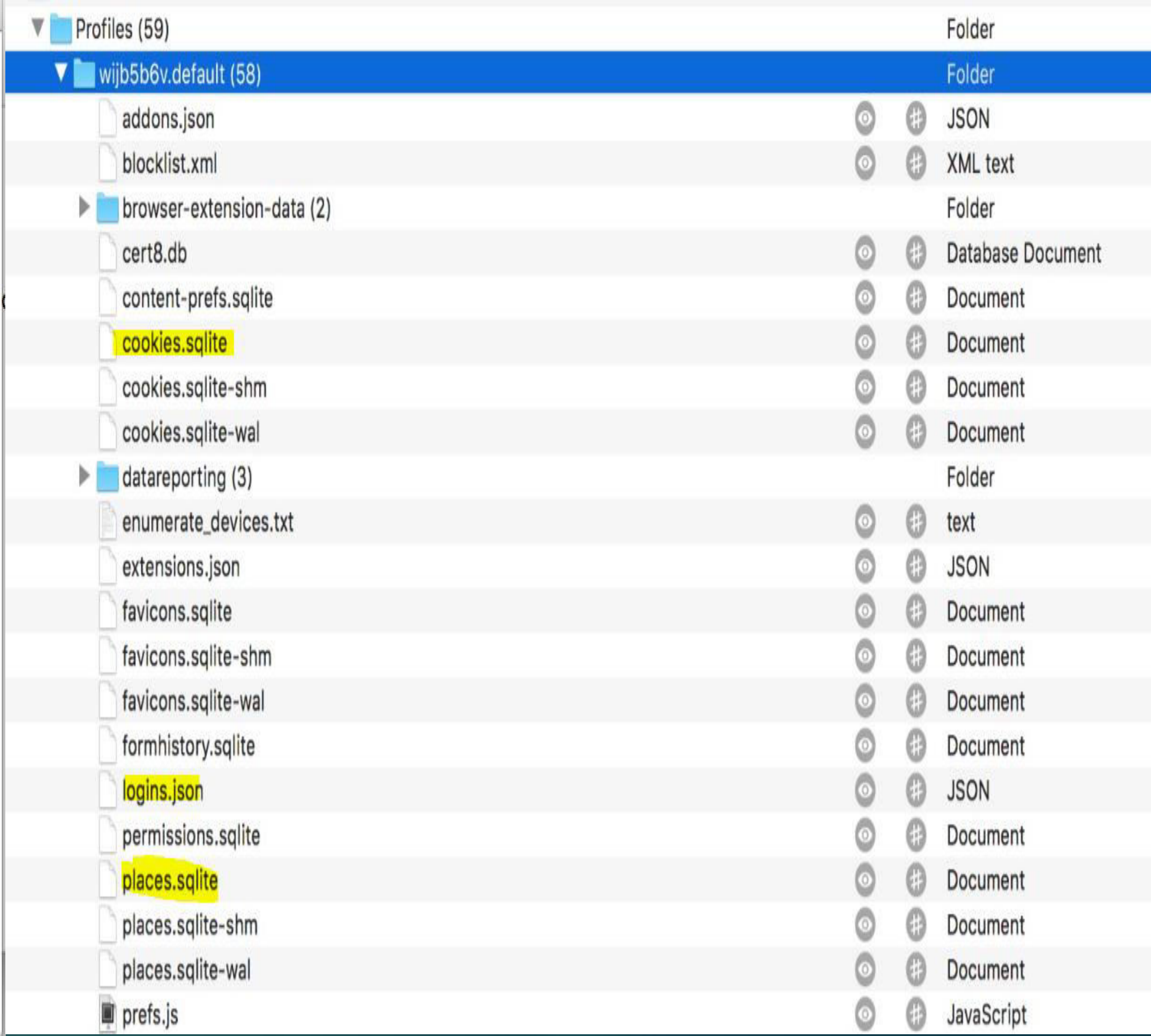
Implementation : Firefox

- Step 1 : Delete all the history, cookies and all the data from the browsing session.
- Step 2 : Run the photorec or disk drill recovery software.
- Step 4 : Recovered the .sqlite files.
- Step 5 : places.sqlite file is of interest.
- Step 6 : Open the places.sqlite file in SQLite DB .
- Step 7 : Able to search for searches, history, and browsing data.
- Step 8 : Time in NSDate format , converted to accurate time

Firefox : Data Recovery

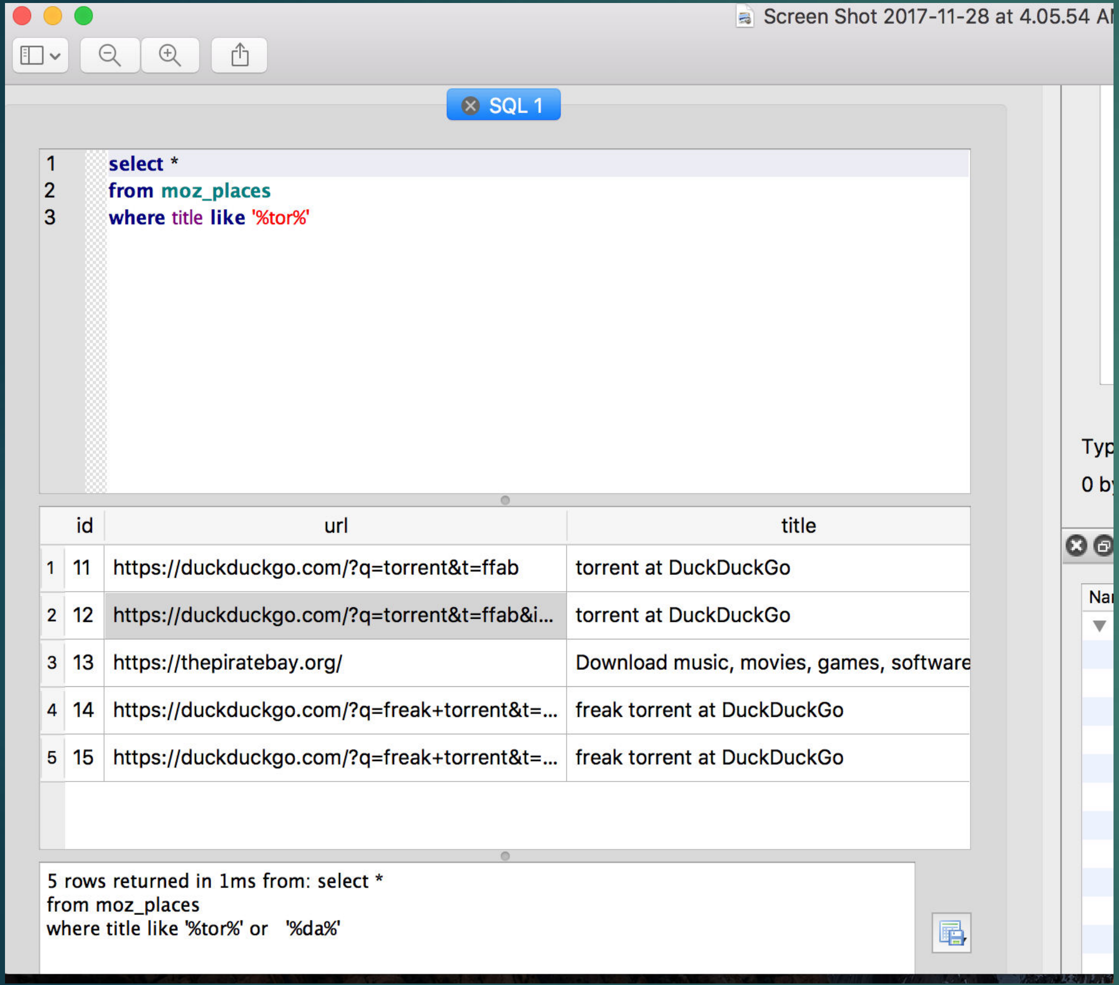


```
PhotoRec 7.1-WIP, Data Recovery Utility, November 2017
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/disk2 - 85 MB / 81 MiB (RO)
     Partition                  Start        End    Size in sectors
 1 P Mac HFS                   40   0  1 166871   0  1     166832 [disk image]


40 files saved in /Users/shreypc/Desktop/network/recup_dir directory.
Recovery completed.

You are welcome to donate to support and encourage further development
http://www.cgsecurity.org/wiki/Donation







[ Quit ]
```



▼ Profiles (59)	Folder
▼ wijb5b6v.default (58)	Folder
addons.json	JSON
blocklist.xml	XML text
▶ browser-extension-data (2)	Folder
cert8.db	Database Document
content-prefs.sqlite	Document
cookies.sqlite	Document
cookies.sqlite-shm	Document
cookies.sqlite-wal	Document
▶ datareporting (3)	Folder
enumerate_devices.txt	text
extensions.json	JSON
favicons.sqlite	Document
favicons.sqlite-shm	Document
favicons.sqlite-wal	Document
formhistory.sqlite	Document
logins.json	JSON
permissions.sqlite	Document
places.sqlite	Document
places.sqlite-shm	Document
places.sqlite-wal	Document
prefs.js	JavaScript

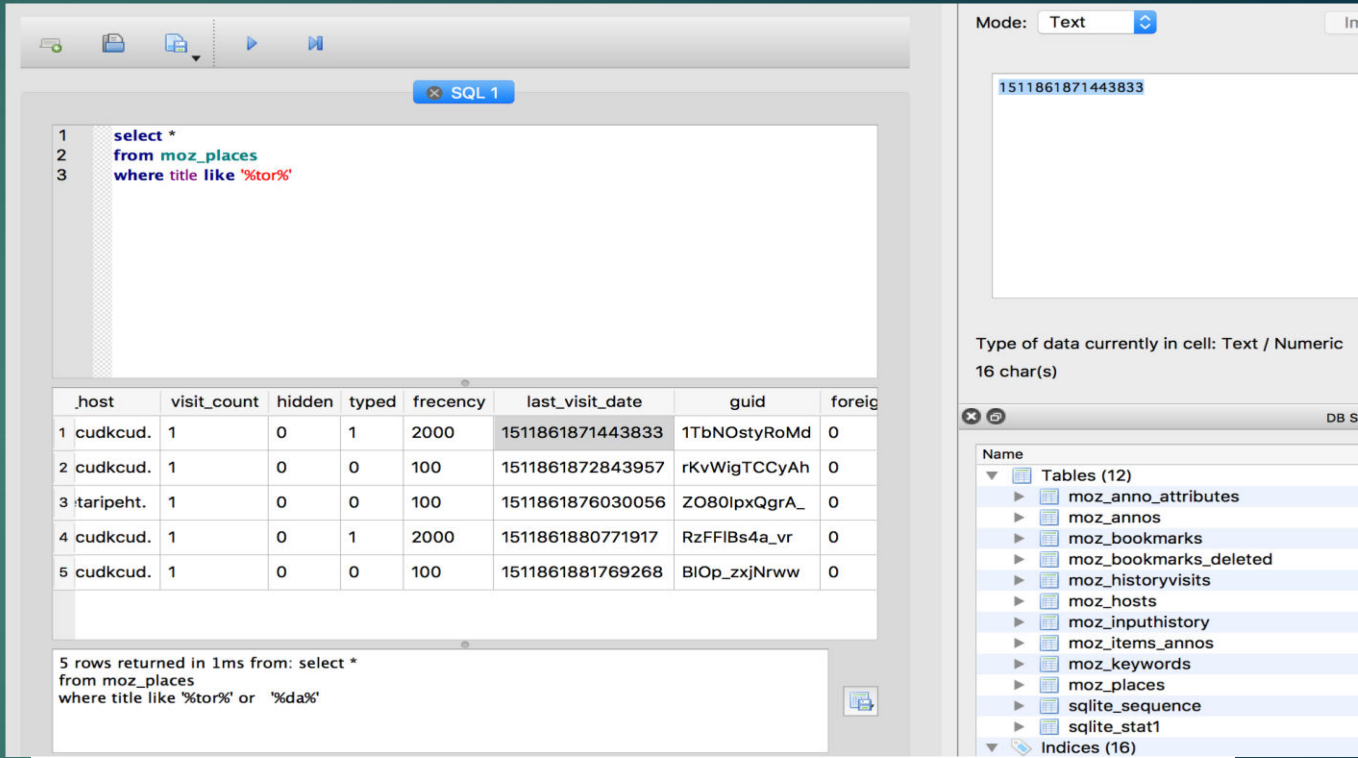
Firefox : Information Retrieval



```
select *
from moz_places
where title like '%tor%'
```

	id	url	title
1	11	https://duckduckgo.com/?q=torrent&t=ffab	torrent at DuckDuckGo
2	12	https://duckduckgo.com/?q=torrent&t=ffab&i...	torrent at DuckDuckGo
3	13	https://thepiratebay.org/	Download music, movies, games, software
4	14	https://duckduckgo.com/?q=freak+torrent&t=...	freak torrent at DuckDuckGo
5	15	https://duckduckgo.com/?q=freak+torrent&t=...	freak torrent at DuckDuckGo

```
5 rows returned in 1ms from: select *
from moz_places
where title like '%tor%' or   '%da%'
```



```
select *
from moz_places
where title like '%tor%'
```

	host	visit_count	hidden	typed	frecency	last_visit_date	guid	foreig
1	cudkcud.	1	0	1	2000	1511861871443833	1TbNOstyRoMd	0
2	cudkcud.	1	0	0	100	1511861872843957	rKvWigTCCyAh	0
3	taripeht.	1	0	0	100	1511861876030056	ZO80IpxQgrA_	0
4	cudkcud.	1	0	1	2000	1511861880771917	RzFFIBs4a_vr	0
5	cudkcud.	1	0	0	100	1511861881769268	BIOp_zxjNrww	0

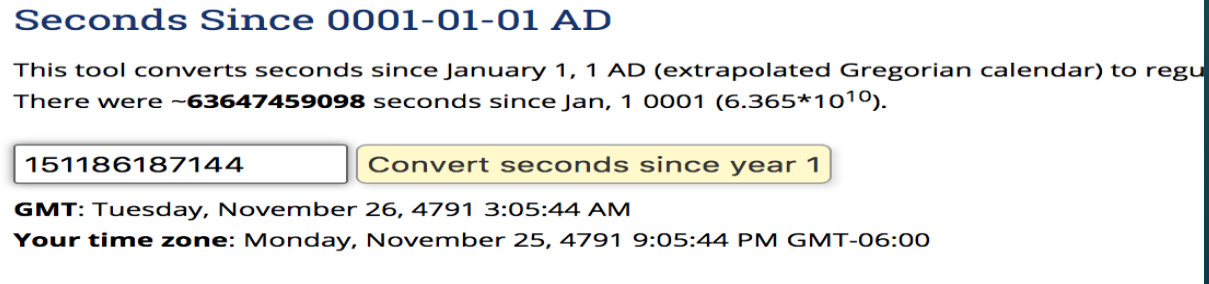
```
5 rows returned in 1ms from: select *
from moz_places
where title like '%tor%' or   '%da%'
```

Mode: Text

1511861871443833

Type of data currently in cell: Text / Numeric
16 char(s)

- Tables (12)
  - moz_anno_attributes
  - moz_annos
  - moz_bookmarks
  - moz_bookmarks_deleted
  - moz_historyvisits
  - moz_hosts
  - moz_inputhistory
  - moz_items_annos
  - moz_keywords
  - moz_places
  - sqlite_sequence
  - sqlite_stat1
- Indices (16)



Seconds Since 0001-01-01 AD

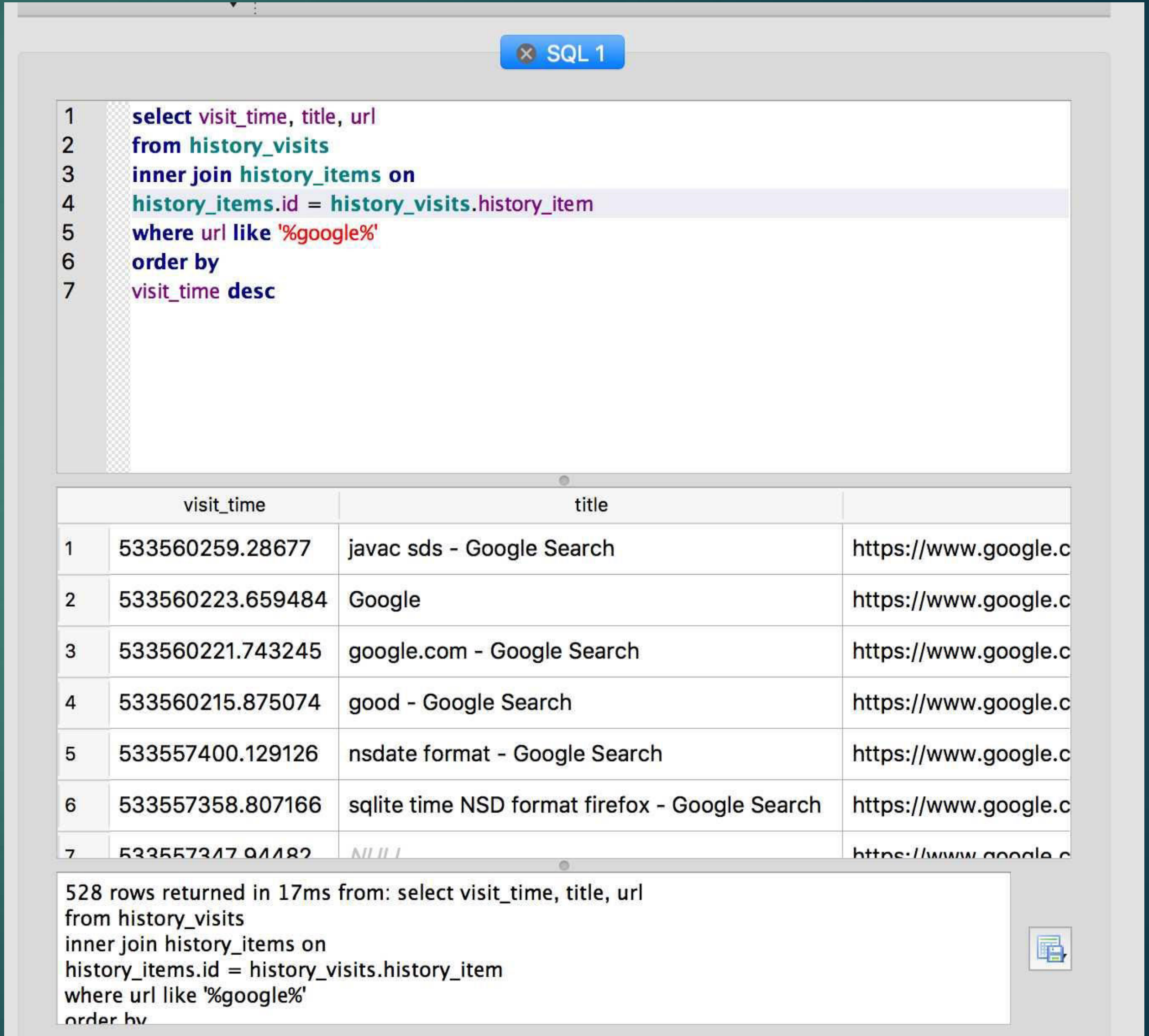
This tool converts seconds since January 1, 1 AD (extrapolated Gregorian calendar) to regu
There were ~**63647459098** seconds since Jan, 1 0001 (6.365*10^{10}).

151186187144 | Convert seconds since year 1

GMT: Tuesday, November 26, 4791 3:05:44 AM
Your time zone: Monday, November 25, 4791 9:05:44 PM GMT-06:00

Safari : Browsing Data Retrieval

- Followed the previous steps.
- Using the appropriate queries
- Browsing data with the time in descending order for google.com
- Able to retrieve a user’s browsing data after history and cache deletion.



```
select visit_time, title, url
from history_visits
inner join history_items on
history_items.id = history_visits.history_item
where url like '%google%'
order by
visit_time desc
```

	visit_time	title	
1	533560259.28677	javac sds - Google Search	https://www.google.c
2	533560223.659484	Google	https://www.google.c
3	533560221.743245	google.com - Google Search	https://www.google.c
4	533560215.875074	good - Google Search	https://www.google.c
5	533557400.129126	nsdate format - Google Search	https://www.google.c
6	533557358.807166	sqlite time NSD format firefox - Google Search	https://www.google.c
7	533557347.94482	NULL	https://www.google.c

```
528 rows returned in 17ms from: select visit_time, title, url
from history_visits
inner join history_items on
history_items.id = history_visits.history_item
where url like '%google%'
order by
```

Findings

Firefox

- Able to extract the deleted Firefox history in Ubuntu, Mac OS, and Windows 10.
- Versions of Firefox used : 57.0, 56.02.
- Complete browsing detail of a user with queries and time.
- For private browsing memory capture was used.

Safari

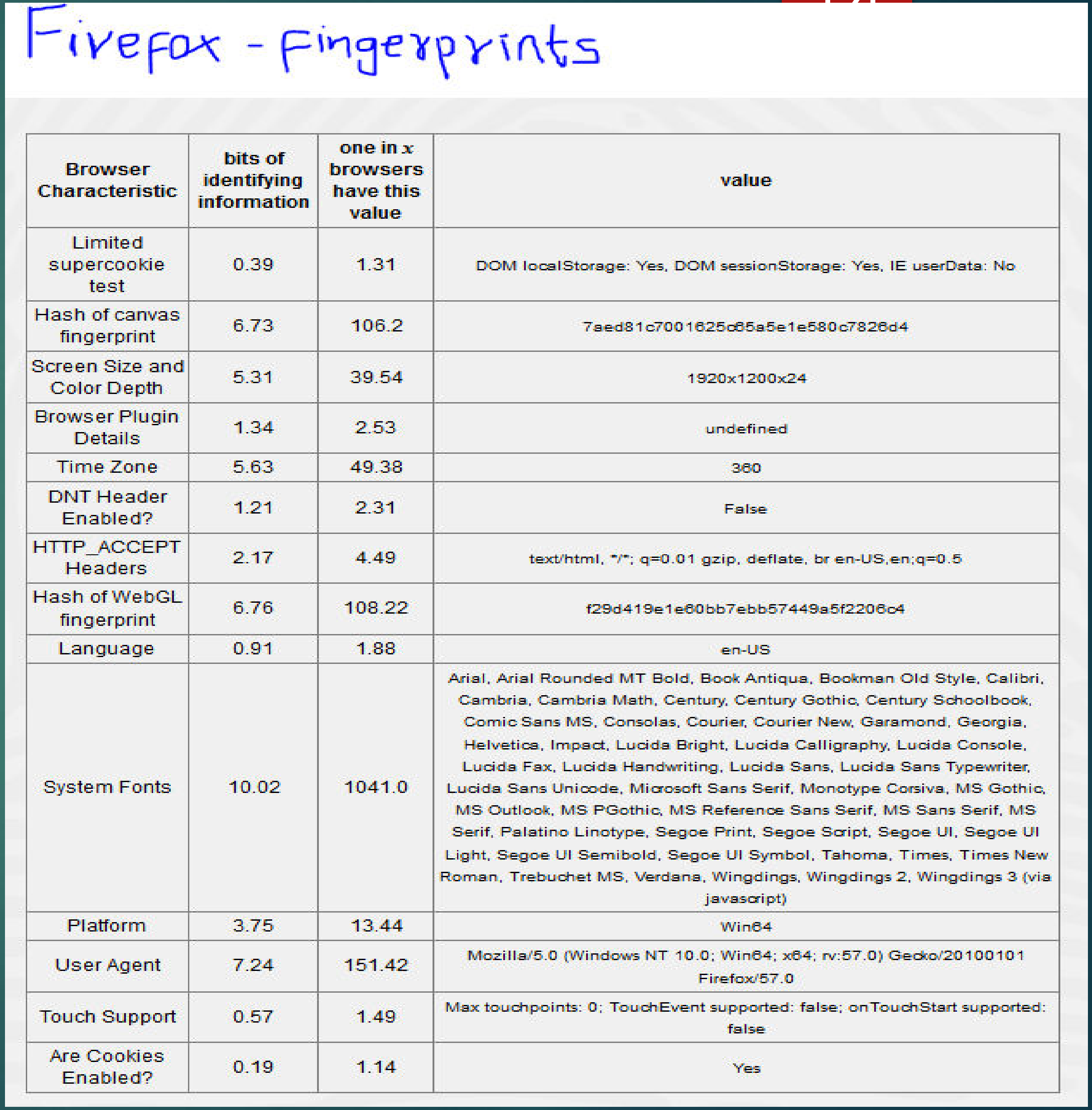
- Database found in : ~/Library/Safari/History.db
- Deleted browsing data and applied recovery
- Able to extract data with queries
- Similar structure with different keys.
- Private browsing does not save data to the disk.

Browser Fingerprints

- A website can link a user in normal mode to private mode based on

  identifying bits of canvas fingerprint, plugins, HTTP_ACCEPT, System Fonts, Time Zone etc.

- Browser Fingerprinting allows websites to passively gather data
- Panopticlick study showed on around 1 million visits, 83.6 % browsers had unique fingerprint, for Flash and Java enabled, 94.2 %.
- Cookies not needed.

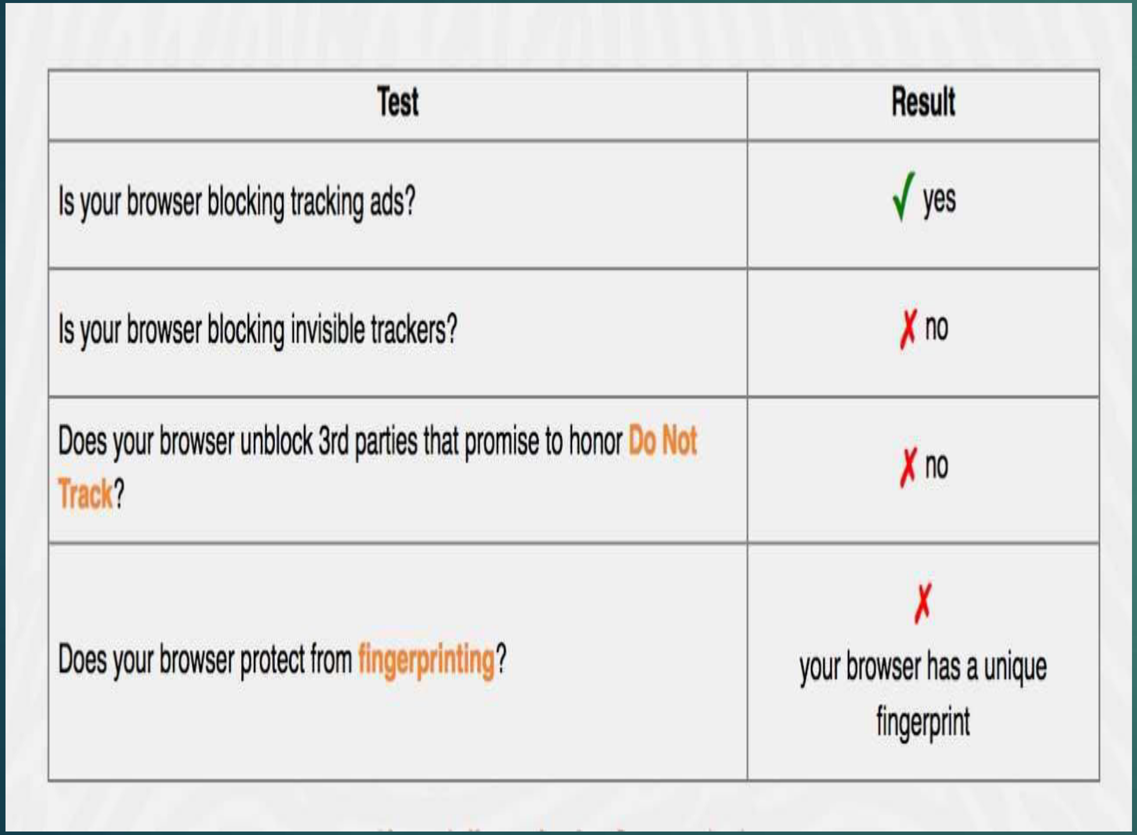


Firefox - Fingerprints

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
Limited supercookie test	0.39	1.31	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	6.73	106.2	7aed81c7001625c65a5e1e580c7826d4
Screen Size and Color Depth	5.31	39.54	1920x1200x24
Browser Plugin Details	1.34	2.53	undefined
Time Zone	5.63	49.38	360
DNT Header Enabled?	1.21	2.31	False
HTTP_ACCEPT Headers	2.17	4.49	text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.5
Hash of WebGL fingerprint	6.76	108.22	f29d419e1e60bb7ebb57449a5f2206c4
Language	0.91	1.88	en-US
System Fonts	10.02	1041.0	Arial, Arial Rounded MT Bold, Book Antiqua, Bookman Old Style, Calibri, Cambria, Cambria Math, Century, Century Gothic, Century Schoolbook, Comic Sans MS, Consolas, Courier, Courier New, Garamond, Georgia, Helvetica, Impact, Lucida Bright, Lucida Calligraphy, Lucida Console, Lucida Fax, Lucida Handwriting, Lucida Sans, Lucida Sans Typewriter, Lucida Sans Unicode, Microsoft Sans Serif, Monotype Corsiva, MS Gothic, MS Outlook, MS PGothic, MS Reference Sans Serif, MS Sans Serif, MS Serif, Palatino Linotype, Segoe Print, Segoe Script, Segoe UI, Segoe UI Light, Segoe UI Semibold, Segoe UI Symbol, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings, Wingdings 2, Wingdings 3 (via javascript)
Platform	3.75	13.44	Win64
User Agent	7.24	151.42	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0
Touch Support	0.57	1.49	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.19	1.14	Yes

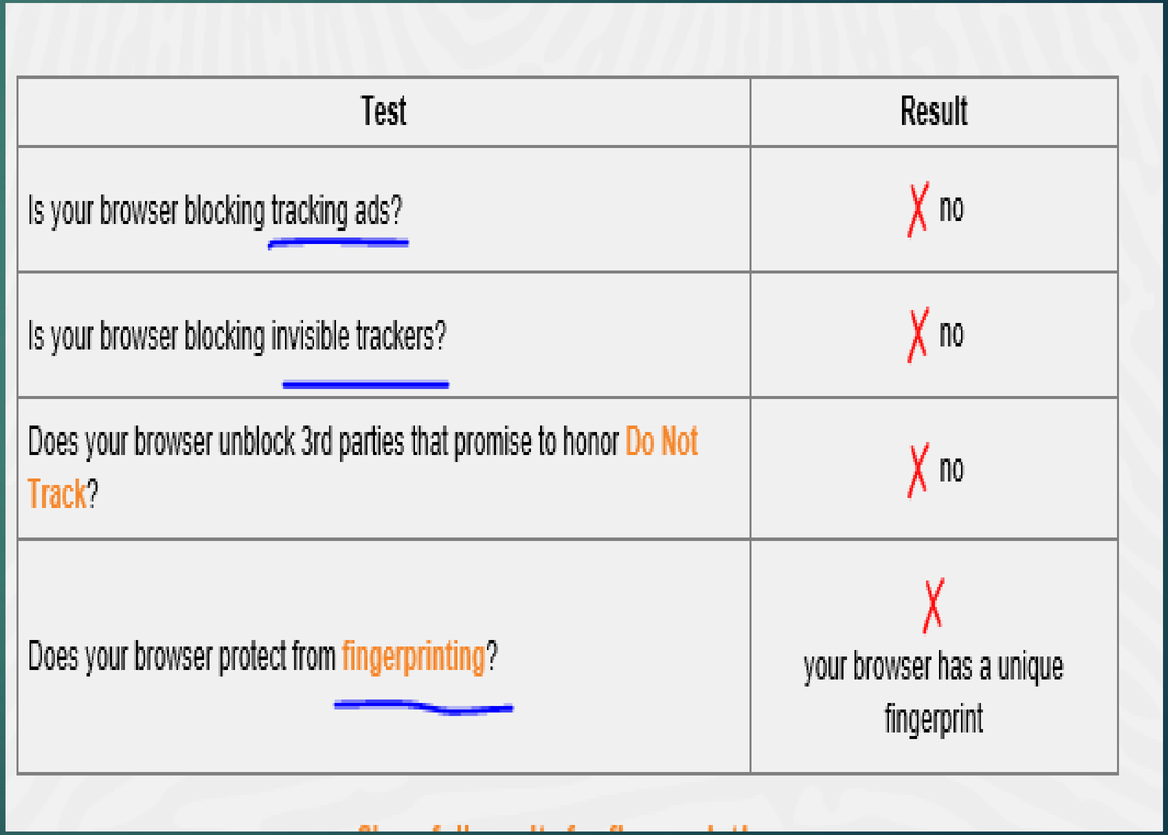
Fingerprint Comparison

Safari 11.01



Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✗ no
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Microsoft Edge 40.15063.674.0

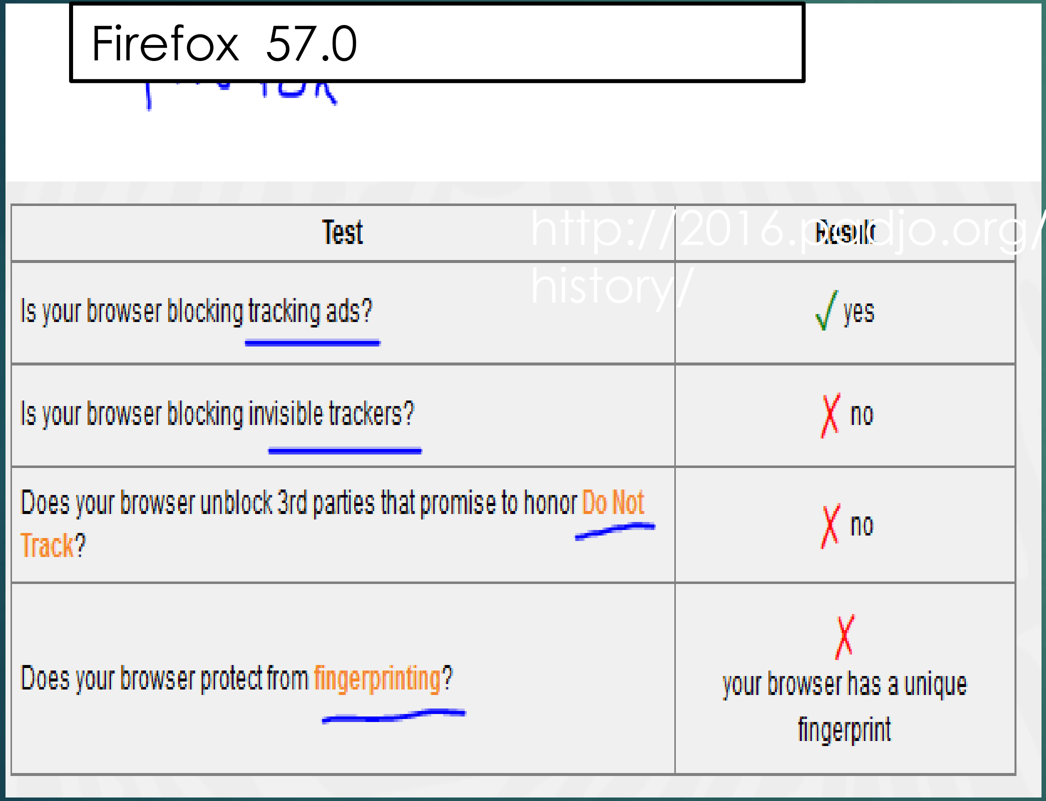


Test	Result
Is your browser blocking tracking ads?	✗ no
Is your browser blocking invisible trackers?	✗ no
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Fingerprint Comparison

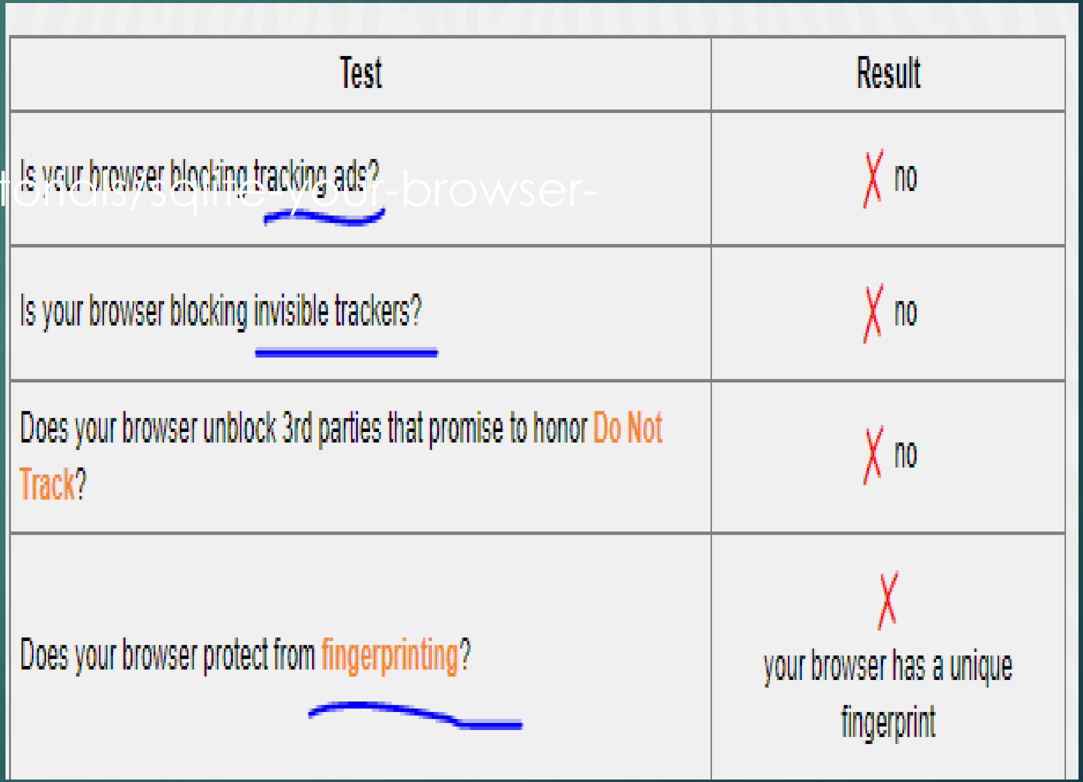
http://2016.padjo.org/tutorials/sqlite-your-browser-history/

Firefox 57.0



Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✗ no
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Chrome 62.0.3202.94



Test	Result
Is your browser blocking tracking ads?	✗ no
Is your browser blocking invisible trackers?	✗ no
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Part Two : Forensic analysis of private browsing mode

MICROSOFT EDGE	V(25.10586.672.0)
GOOGLE CHROME	V(62.0.3202.94)
MOZILLA FIREFOX	V(57.0)

TOOLS USED:

FDK IMAGER

WHATCHANGED.EXE

VOLATILITY

STRINGS

RECUVA

WINHEX

SYSTEM:

WINDOWS 7

2 GB RAM   60 GB STORAGE

Experiment:

- For each web browser:
- Opened the private browsing and visited the following website:
- www.mirror.co.uk
- www.uno.edu
- www.livescore.com
- Searched for the following terms on google:
- Black Friday
- Football
- Winter
- Logged into privateer place resident portal
- https://portal.campushousing.com/UNO-Privateer-Place/Default.aspx?Params=L9ezxPcQnQuRGKTzF%2b4sxeNblvAA%2b26c&_ga=2.189002987.1937925296.1511825121-710119258.1511825121

- Stopped the private browsing and captured the RAM and pagefile using FTK Imager
- Used whatchanged.exe to find the changes made in the filesystem by private browsing
- Tried to recover any deleted data.
- Analyzed the RAM using volatility and strings to find network connections, html code, usernames, passwords, images etc. related to private browsing

Microsoft Edge

- According to Microsoft:
- “When you use InPrivate tabs or windows, your browsing data (like your history, temporary internet files, and cookies) isn't saved on your PC once you're done.”

- Findings:
- Unlike other browsers edge stores the private browsing data on filesystem and deletes it after the session.
- Using whatchanged.exe I found the changed made on file system and recovered the deleted files

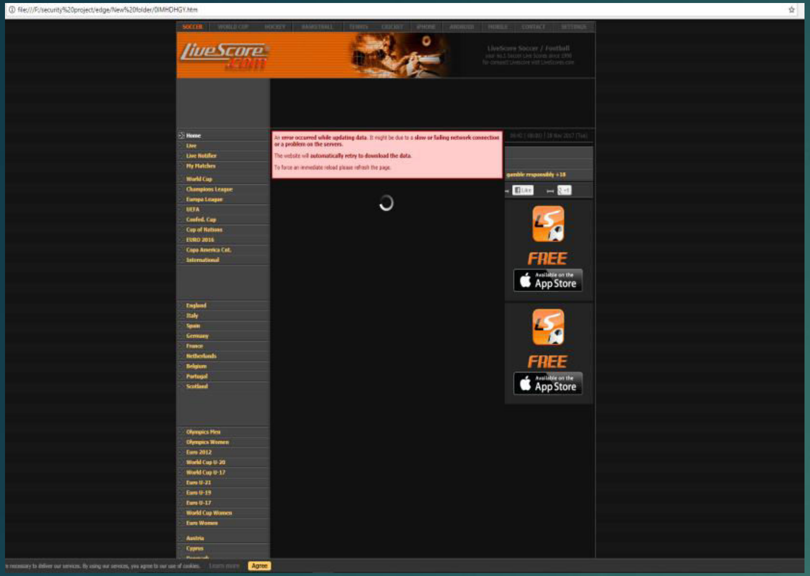
Edge store the files in

C:\Users\(username)\AppData\Local\Packages\Microsoft.MicrosoftEdge_(profile)\AC\#!001\MicrosoftEdge\Cache
C:\Users\(username)\AppData\Local\Packages\Microsoft.MicrosoftEdge_(profile)\AC\#!002\MicrosoftEdge\Cache

In my case:
C:\Users\test\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\Cache
C:\Users\test\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!002\MicrosoftEdge\Cache

- Recuva recovered around 700 files including html,JavaScript and images.

Some of the recovered artifacts:



file:///F:/security%20project/edge/New%20folder/0IMHDHGY.htm

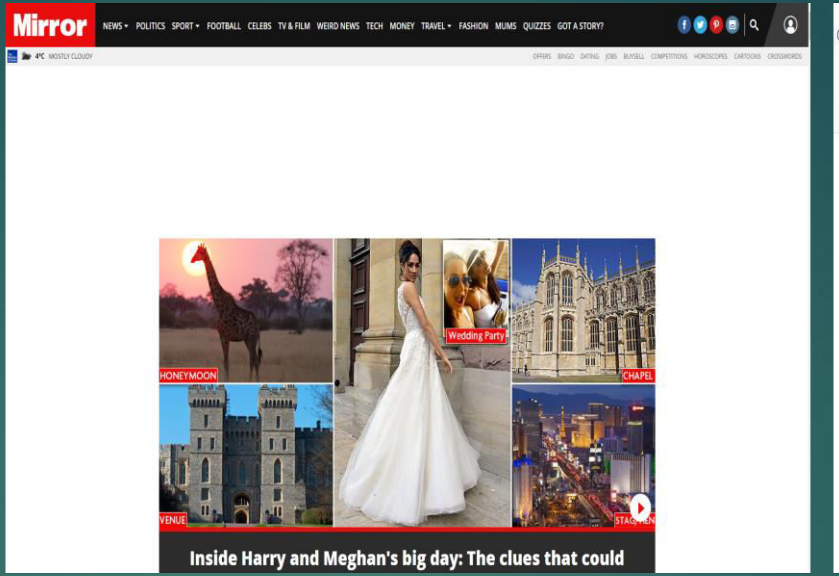
An error occurred while updating data. It might be due to a slow or failing network connection or a problem on the servers.

The website will automatically retry to download the data.

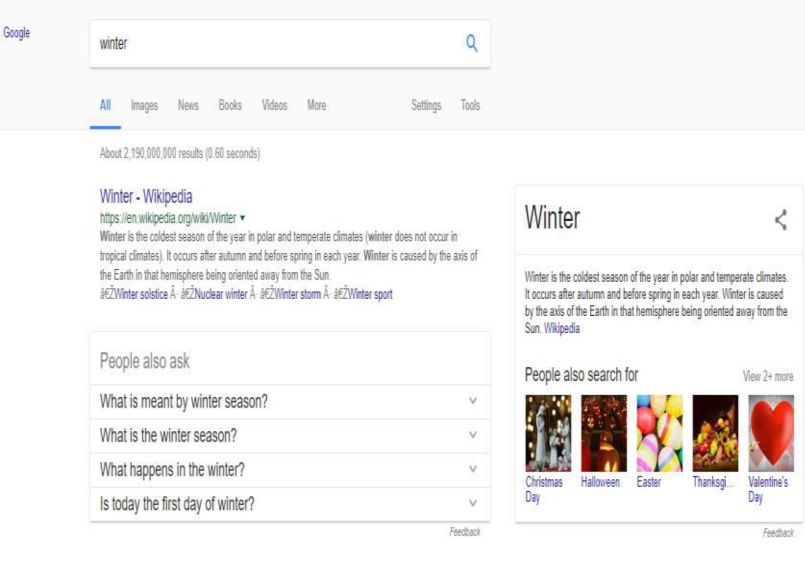
To force an immediate reload please refresh the page.

gamble responsibly +18

...necessary to deliver our services. By using our services, you agree to our use of cookies. Learn more Agree



Inside Harry and Meghan's big day: The clues that could



winter

About 2,190,000,000 results (0.60 seconds)

Winter - Wikipedia
https://en.wikipedia.org/wiki/Winter ▾
Winter is the coldest season of the year in polar and temperate climates (winter does not occur in tropical climates). It occurs after autumn and before spring in each year. Winter is caused by the axis of the Earth in that hemisphere being oriented away from the Sun.
â€ŽWinter solstice Â· â€ŽNuclear winter Â· â€ŽWinter storm Â· â€ŽWinter sport

People also ask
What is meant by winter season?
What is the winter season?
What happens in the winter?
Is today the first day of winter?

Winter

Winter is the coldest season of the year in polar and temperate climates. It occurs after autumn and before spring in each year. Winter is caused by the axis of the Earth in that hemisphere being oriented away from the Sun. Wikipedia

People also search for

UNO Scholarships Portal

Finding and applying for scholarships, grants and loans can be a daunting task. Visit our all new Scholarships Portal and discover the opportunities that are available.

RAM

- I was unable to find connection between the host and visited websites. Most of the ips found during ram analysis were related to akami, amazon and other third party servers and content distributors. But the strings analysis of RAM showed the get request to all the websites visited during private session

Google Chrome:

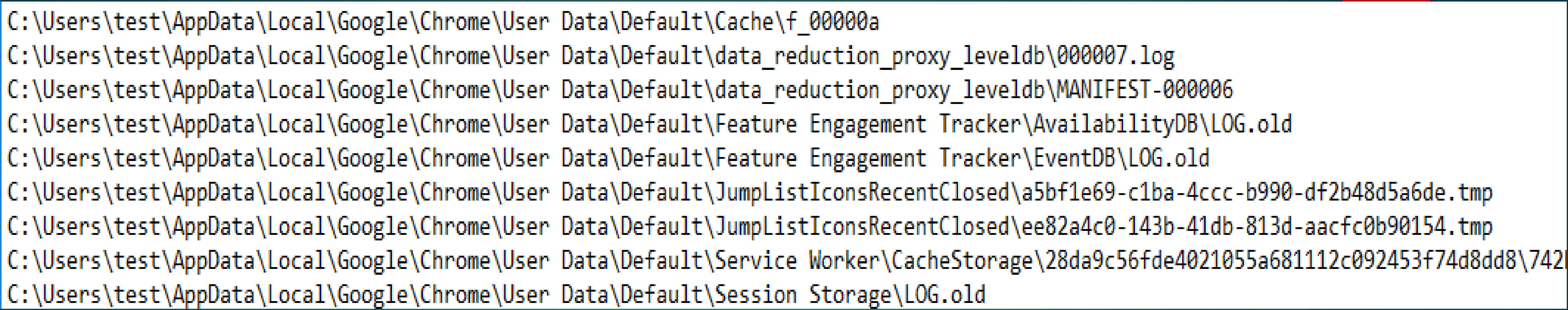
“Chrome doesn't save your browsing history or information entered in forms. Cookies and site data are remembered while you're browsing, but deleted when you close Incognito mode.”

- When you use incognito window google Chorme store the data on RAM.
- Findings:

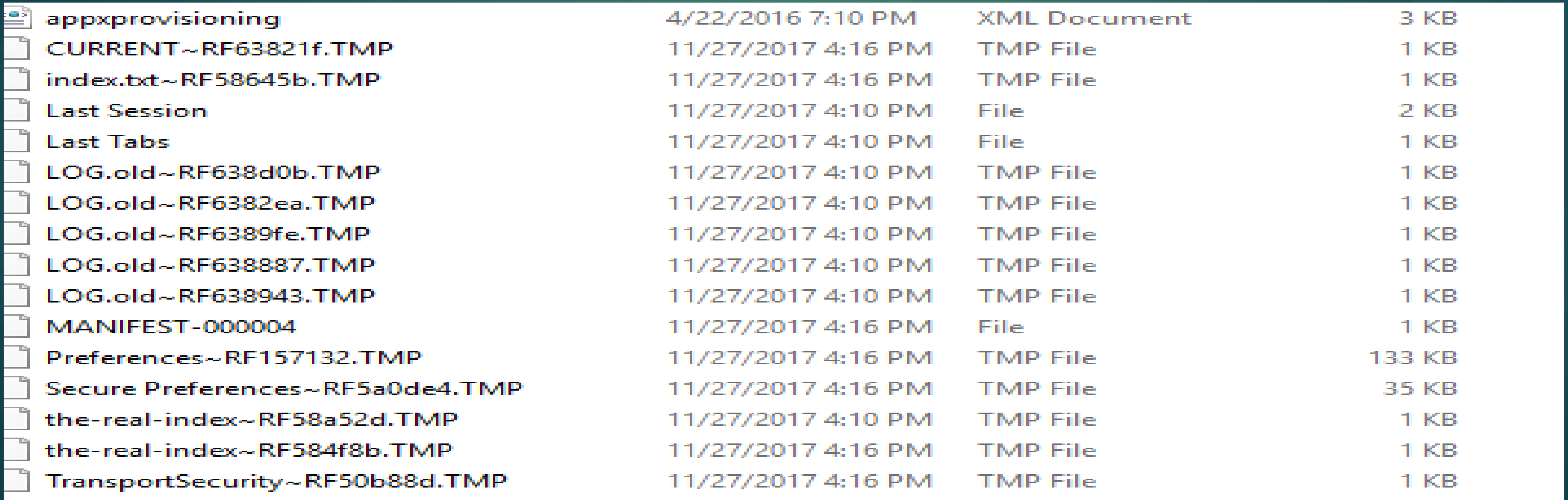
There was some changes in the file system in

C:\Users\test\AppData\Local\Google\Chrome\User Data\Default\

But my recovery software was unable to recover those files



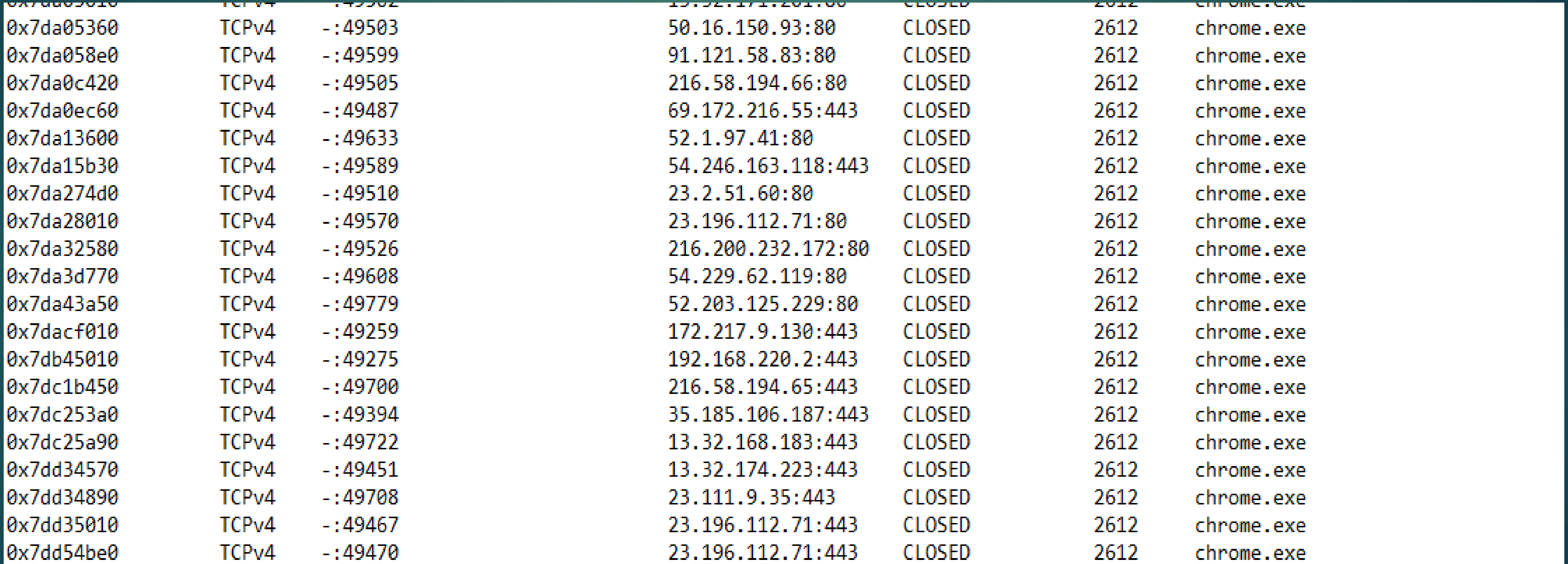
```
C:\Users\test\AppData\Local\Google\Chrome\User Data\Default\Cache\f_00000a
C:\Users\test\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000007.log
C:\Users\test\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000006
C:\Users\test\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old
C:\Users\test\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old
C:\Users\test\AppData\Local\Google\Chrome\User Data\Default\JumpListIconsRecentClosed\a5bf1e69-c1ba-4ccc-b990-df2b48d5a6de.tmp
C:\Users\test\AppData\Local\Google\Chrome\User Data\Default\JumpListIconsRecentClosed\ee82a4c0-143b-41db-813d-aacfc0b90154.tmp
C:\Users\test\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\28da9c56fde4021055a681112c092453f74d8dd8\742
C:\Users\test\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old
```



```
appxprovisioning                      4/22/2016 7:10 PM     XML Document        3 KB
CURRENT~RF63821f.TMP                  11/27/2017 4:16 PM    TMP File            1 KB
index.txt~RF58645b.TMP                11/27/2017 4:16 PM    TMP File            1 KB
Last Session                          11/27/2017 4:10 PM    File                2 KB
Last Tabs                             11/27/2017 4:10 PM    File                1 KB
LOG.old~RF638d0b.TMP                  11/27/2017 4:10 PM    TMP File            1 KB
LOG.old~RF6382ea.TMP                  11/27/2017 4:10 PM    TMP File            1 KB
LOG.old~RF6389fe.TMP                  11/27/2017 4:10 PM    TMP File            1 KB
LOG.old~RF638887.TMP                  11/27/2017 4:10 PM    TMP File            1 KB
LOG.old~RF638943.TMP                  11/27/2017 4:10 PM    TMP File            1 KB
MANIFEST-000004                       11/27/2017 4:16 PM    File                1 KB
Preferences~RF157132.TMP              11/27/2017 4:16 PM    TMP File          133 KB
Secure Preferences~RF5a0de4.TMP       11/27/2017 4:16 PM    TMP File           35 KB
the-real-index~RF58a52d.TMP           11/27/2017 4:10 PM    TMP File            1 KB
the-real-index~RF584f8b.TMP           11/27/2017 4:16 PM    TMP File            1 KB
TransportSecurity~RF50b88d.TMP        11/27/2017 4:16 PM    TMP File            1 KB
```

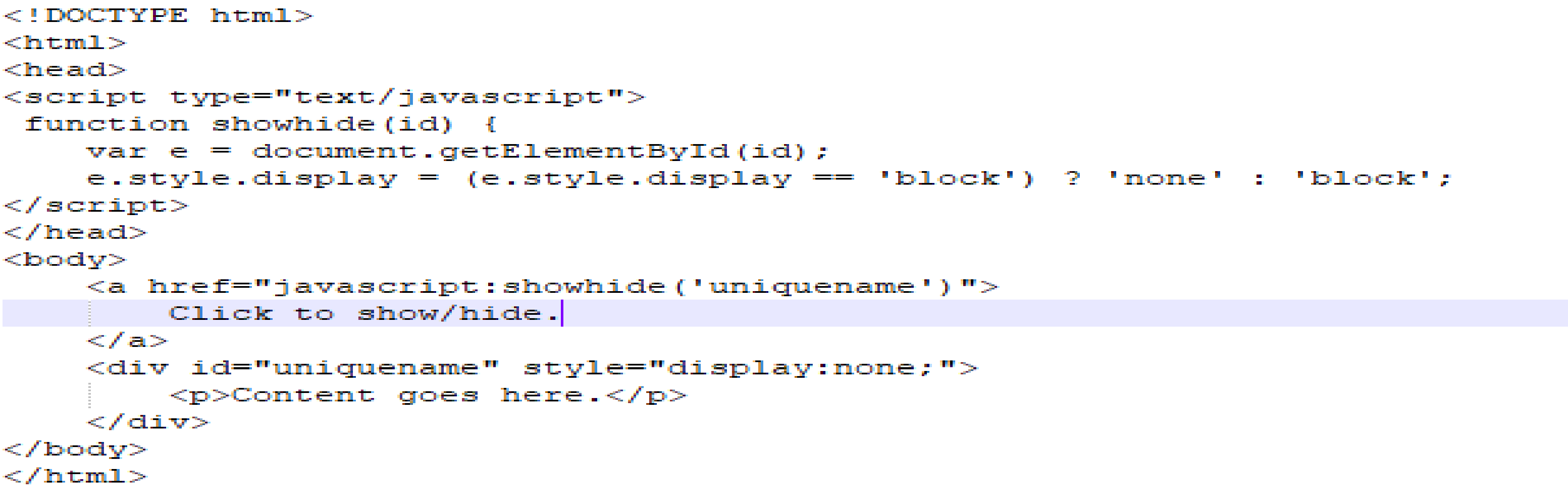
RAM

- My goal was to find the network connections made by the host and figure out the webpages visited. So I used volatility to analyze the network information. So I used netscan commands to scan for tcp connections.



```
0x7da05360         TCPv4    -:49503                             50.16.150.93:80     CLOSED           2612     chrome.exe
0x7da058e0         TCPv4    -:49599                             91.121.58.83:80     CLOSED           2612     chrome.exe
0x7da0c420         TCPv4    -:49505                             216.58.194.66:80    CLOSED           2612     chrome.exe
0x7da0ec60         TCPv4    -:49487                             69.172.216.55:443   CLOSED           2612     chrome.exe
0x7da13600         TCPv4    -:49633                             52.1.97.41:80       CLOSED           2612     chrome.exe
0x7da15b30         TCPv4    -:49589                             54.246.163.118:443  CLOSED           2612     chrome.exe
0x7da274d0         TCPv4    -:49510                             23.2.51.60:80       CLOSED           2612     chrome.exe
0x7da28010         TCPv4    -:49570                             23.196.112.71:80    CLOSED           2612     chrome.exe
0x7da32580         TCPv4    -:49526                             216.200.232.172:80  CLOSED           2612     chrome.exe
0x7da3d770         TCPv4    -:49608                             54.229.62.119:80    CLOSED           2612     chrome.exe
0x7da43a50         TCPv4    -:49779                             52.203.125.229:80   CLOSED           2612     chrome.exe
0x7dacf010         TCPv4    -:49259                             172.217.9.130:443   CLOSED           2612     chrome.exe
0x7db45010         TCPv4    -:49275                             192.168.220.2:443   CLOSED           2612     chrome.exe
0x7dc1b450         TCPv4    -:49700                             216.58.194.65:443   CLOSED           2612     chrome.exe
0x7dc253a0         TCPv4    -:49394                             35.185.106.187:443  CLOSED           2612     chrome.exe
0x7dc25a90         TCPv4    -:49722                             13.32.168.183:443   CLOSED           2612     chrome.exe
0x7dd34570         TCPv4    -:49451                             13.32.174.223:443   CLOSED           2612     chrome.exe
0x7dd34890         TCPv4    -:49708                             23.111.9.35:443     CLOSED           2612     chrome.exe
0x7dd35010         TCPv4    -:49467                             23.196.112.71:443   CLOSED           2612     chrome.exe
0x7dd54be0         TCPv4    -:49470                             23.196.112.71:443   CLOSED           2612     chrome.exe
```

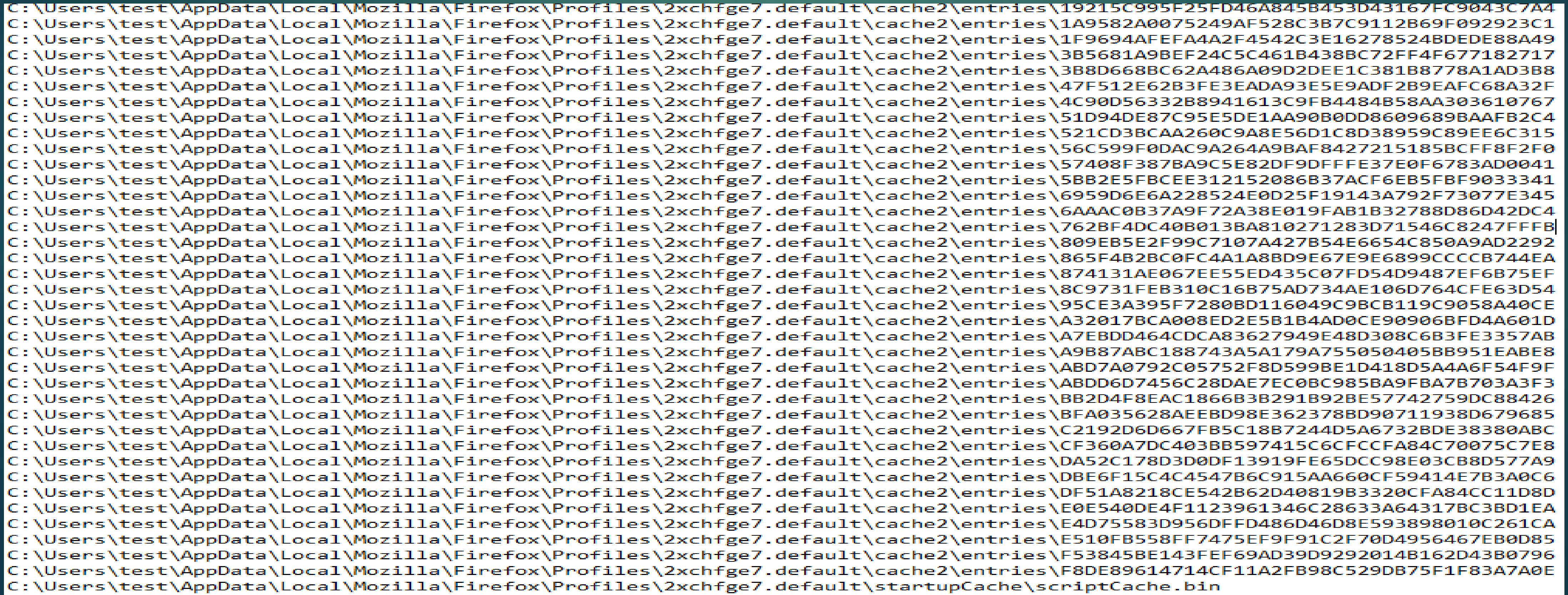
- But almost all the connections found were to third party servers and content provides like akami.
- There was one tcp connection with www.google.com 216.58.194.65:80
- Then I used strings tool to find the readable strings present in the ram and was able to see the http request made to websites in experiment.
- I also found large amount of html code which can be used to reconstruct the webpages.



```
<!DOCTYPE html>
<html>
<head>
<script type="text/javascript">
 function showhide(id) {
    var e = document.getElementById(id);
    e.style.display = (e.style.display == 'block') ? 'none' : 'block';
</script>
</head>
<body>
    <a href="javascript:showhide('uniquename')">
        Click to show/hide.
    </a>
    <div id="uniquename" style="display:none;">
        <p>Content goes here.</p>
    </div>
</body>
</html>
```

Mozilla Firefox

- Similar to chrome, Firefox also don't save visited pages, cookies, searches and temporary files during the private browsing and most of the data is stored on RAM.
- Findings:
- The whatchanged.exe showed that filesystem was changed after the private browsing session and some files in the cache2\entries were deleted after the session and I am unable to recover these.



```
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\19215C995F25FD46A845B453D43167FC9043C7A4
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\1A9582A0075249AF528C3B7C9112B69F092923C1
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\1F9694AFEFA4A2F4542C3E16278524BDEDE88A49
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\3B5681A9BEF24C5C461B438BC72FF4F677182717
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\3B8D668BC62A486A09D2DEE1C381B8778A1AD3B8
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\47F512E62B3FE3EADA93E5E9ADF2B9EAFC68A32F
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\4C90D56332B8941613C9FB4484B58AA303610767
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\51D94DE87C95E5DE1AA90B0DD8609689BAAFB2C4
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\521CD3BCAA260C9A8E56D1C8D38959C89EE6C315
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\56C599F0DAC9A264A9BAF8427215185BCFF8F2F0
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\57408F387BA9C5E82DF9DFFFE37E0F6783AD0041
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\5BB2E5FBCEE312152086B37ACF6EB5FBF9033341
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\6959D6E6A228524E0D25F19143A792F73077E345
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\6AAAC0B37A9F72A38E019FAB1B32788D86D42DC4
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\762BF4DC40B013BA810271283D71546C8247FFFB
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\809EB5E2F99C7107A427B54E6654C850A9AD2292
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\865F4B2BC0FC4A1A8BD9E67E9E6899CCCCB744EA
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\874131AE067EE55ED435C07FD54D9487EF6B75EF
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\8C9731FEB310C16B75AD734AE106D764CFE63D54
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\95CE3A395F7280BD116049C9BCB119C9058A40CE
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\A32017BCA008ED2E5B1B4AD0CE90906BFD4A601D
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\A7EBDD464CDCA83627949E48D308C6B3FE3357AB
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\A9B87ABC188743A5A179A755050405BB951EABE8
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\ABD7A0792C05752F8D599BE1D418D5A4A6F54F9F
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\ABDD6D7456C28DAE7EC0BC985BA9FBA7B703A3F3
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\BB2D4F8EAC1866B3B291B92BE57742759DC88426
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\BFA035628AEEBD98E362378BD90711938D679685
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\C2192D6D667FB5C18B7244D5A6732BDE38380ABC
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\CF360A7DC403BB597415C6CFCCFA84C70075C7E8
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\DA52C178D3D0DF13919FE65DCC98E03CB8D577A9
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\DBE6F15C4C4547B6C915AA660CF59414E7B3A0C6
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\DF51A8218CE542B62D40819B3320CFA84CC11D8D
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\E0E540DE4F1123961346C28633A64317BC3BD1EA
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\E4D75583D956DFFD486D46D8E593898010C261CA
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\E510FB558FF7475EF9F91C2F70D4956467EB0D85
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\F53845BE143FEF69AD39D9292014B162D43B0796
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\cache2\entries\F8DE89614714CF11A2FB98C529DB75F1F83A7A0E
C:\Users\test\AppData\Local\Mozilla\Firefox\Profiles\2xchfge7.default\startupCache\scriptCache.bin
```

RAM:

- The RAM analysis of Firefox were similar to chrome and edge and most of the tcp connection were to third party servers and content provides.

- String results showed the get requests to websites and html code.

- A separate experiment was run to test the known DNS caching threat.
- The vulnerability is caused due to the operating system caching all the DNS queries sent by a web browser. We confirm that this vulnerability still persist in latest versions of all browsers. The queries made during the private sessions are also not removed/deleted and anyone on the system can see this.

Conclusions

- Deleting Browsing history does not remove the track of web browsing.
- Private Browsing does not save the data to the hard drive but memory analysis can help to retrieve it.
- In Microsoft Edge private browsing data is saved to hard drive and deleted it. So, retrieval is possible.
- DNS cache after private browsing is still visible in all four major browsers.
- A website can track a user using browser fingerprinting which can not be prevented by private browsing.
- Tor browser or Tor extension for Firefox are examples that provide relatively anonymous browsing.

Related Works:

1. Aggarwal, Gaurav, Elie Bursztein, Collin Jackson, and Dan Boneh. An Analysis of Private Browsing Modes in Modern Browsers." Proceedings of the 19th USENIX Security Symposium, Wardman Park Marriott Hotel, Washington, D.C. 11-13 Aug. 2013. Web. 8

2. In Private Browsing." Microsoft Windows. Microsoft, 10 Dec. 2013. Web. 10 Dec. 2013. <http://windows.microsoft.com/en-us/internet-explorer/products/ie-9/features/in-private>.

3. Ohana, Donny, and Narasimha Shashidhar. "Do Private and Portable Web Browsers Leave Incriminating Evidence? A Forensic Analysis of Residual Artifacts from Private and PortableWeb Browsing Sessions." IEEE CS Security and Privacy Workshops (SPW),The Westin St. Francis, San Francisco, CA. 23-24 May 2013. Web. 9 Dec. 2013.

4. Said, Huwida, Noora Al Mutawa, Ibtesam Al Awadhi, and Mario Guimaraes. "Forensic Analysis of Private Browsing Artifacts." 7th International Conference on Innovations in Information Technology, Abu Dhabi, United Arab Emirates. 25-27 Apr. 2011.

5. Verdi, Michael et al.Private Browsing." Mozilla Support. Mozilla Foundation, 29 Mar. 2013. Web. 10 Dec. 2013.

Related work:

- What Private Browsing Leaves Behind John Filleau, Milda Zizyte Electrical and Computer Engineering, Carnegie Mellon University Pittsburgh, Pennsylvania, USA jfilleau@cmu.edu milda@cmu.edu

- On the Privacy of Private Browsing – A Forensic Approach Kiavash Satvat, Matthew Forshaw, Feng Hao, Ehsan Toreini School of Computing Science Newcastle University

- Forensic Analysis of Private Browsing Artifacts Huwida Said, Noora Al Mutawa, Ibtesam Al Awadhi and Mario Guimaraes College of Information Technology Zayed University, Dubai United Arab Emirates {Huwida.said, M80000952, M80000938, Mario.guimaraes}@zu.ac.ae