Browser forensics: Adblocker extensions

Willem Rens (UvA MSc SNE student)

Supervisor: Johannes de Vries (Fox-IT)

Why traditional browser forensics may not work

- Cleared
  - Cookies
  - Cache
  - History

Sometimes recoverable, Jeon et al(2012). Modern SSD’s make it impossible.

Why traditional browser forensics may not work

- Cleared
  - Cookies
  - Cache
  - History

  Sometimes recoverable, Jeon et al(2012). Modern SSD's make it impossible.

- Private browsing
  - Incognito (Chrome)
  - InPrivate (Ie&edge)
  - Private browsing (Firefox)

Why traditional browser forensics may not work

- Cleared
  - Cookies
  - Cache
  - History

  Sometimes recoverable, Jeon et al(2012). Modern SSD's make it impossible.

- Private browsing
  - Incognito (Chrome)
  - InPrivate (Ie&edge)
  - Private browsing (Firefox)

Claims to maintain complete user privacy by not storing traces of web browsing sessions. Flowers et al. (2016) studied the validity of this claim. IE11 still left traces, Chrome and Firefox did not.

Adblocker extension usage estimates

Usage estimates vary widely

Adblocker extension usage estimates

Usage estimates vary widely

- 20% ? (Metadata analysis within a large European ISP, 2015, Metwalley, et al.)

Adblocker extension usage estimates

Usage estimates vary widely

- 20% ? (Metadata analysis within a large European ISP, 2015, Metwalley, et al.)
- 62% ? (Undergraduate business students, 2011, Sandvig, et al.)

Adblocker extension usage estimates

Usage estimates vary widely

- 20% ? (Metadata analysis within a large European ISP, 2015, Metwalley, et al.)
- 62% ? (Undergraduate business students, 2011, Sandvig, et al.)

41% increase year by year(Adobe and Pagefair, 2015)

Research questions

- RQ1 - What artifacts are stored by the tested ad-blocking extensions during *normal* and *private* browsing?

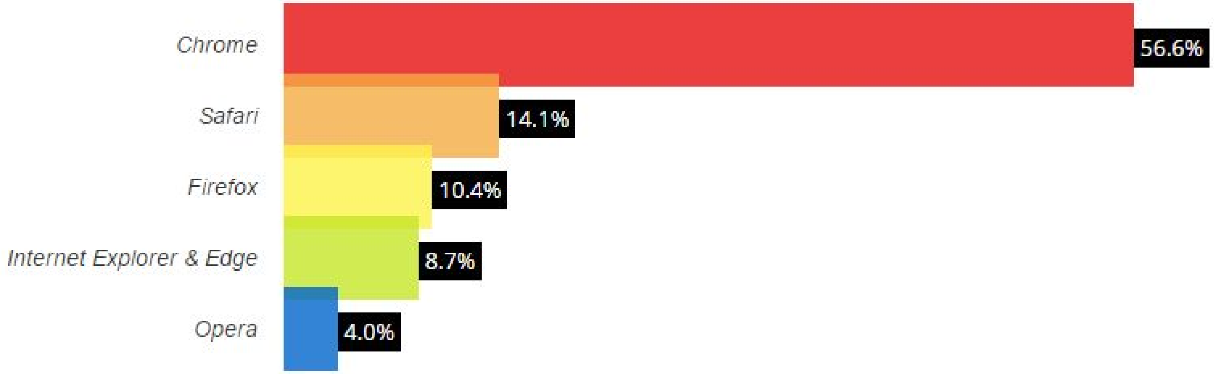
Research questions

- RQ1 - What artifacts are stored the tested ad-blocking extensions during *normal* and *private* browsing?

- RQ2 - If artifacts are found, what is their usefulness in browser forensics?

Tested browsers & their most popular Adblocker extension.

Browser	Adblocker extension
Mozilla Firefox 46.0	Adblock Plus 2.8.2
Google Chrome/55.0.2883.87	AdBlock 3.8.4
Internet Explorer 11	Adblock Plus 1.6
Microsoft Edge/14.14393	AdBlock 1.9.0.0



AdBlock & Adblock Plus are **not** related.

Source most popular adblocking extensions = amount of downloads and reviews as stated by respective webstore. Other adblocking extensions have significant smaller market shares < 10%.

Approach

- Automated sample gathering.
  - *Control* Sample.
  - *Adblock* Sample.
  - *Private* browsing sample.
  - Browsing session entails the visitation of top 50 NL websites as per alexa.com.
  - Python + selenium + save timestamps on url request.
  - Chrome & Firefox have the concept of user profiles, create a new one and extract the user data directory.
  - Ie & Edge more difficult to automate due to limited control with selenium, such as for adding an extension and it does not have the concept of user profiles.

Approach

- Automated sample gathering.
  - *Control* Sample.
  - *Adblock* Sample.
  - *Private* browsing sample.
  - Browsing session entails the visitation of top 50 NL websites as per alexa.com.
  - Python + selenium + save timestamps on url request.
  - Chrome & Firefox have the concept of user profiles, create a new one and extract the user data directory.
  - Ie & Edge more difficult to automate due to limited control with selenium, such as for adding an extension and it does not have the concept of user profiles.
- OSForensics (trialware)
  - Also used by Flowers et al. (2016).
  - Snapshots of the file system, compare them pre and after sample gathering.

Approach

- Automated sample gathering.
  - *Control* Sample.
  - *Adblock* Sample.
  - *Private* browsing sample.
  - Browsing session entails the visitation of top 50 NL websites as per alexa.com.
  - Python + selenium + save timestamps on url request.
  - Chrome & Firefox have the concept of user profiles, create a new one and extract the user data directory.
  - Ie & Edge more difficult to automate due to limited control with selenium, such as for adding an extension and it does not have the concept of user profiles.
- OSForensics (trialware)
  - Also used by Flowers et al. (2016).
  - Snapshots of the file system, compare them pre and after sample gathering.
- W10 Home 64-bit.

Approach

- Automated sample gathering.
  - *Control* Sample.
  - *Adblock* Sample.
  - *Private* browsing sample.
  - Browsing session entails the visitation of top 50 NL websites as per alexa.com.
  - Python + selenium + save timestamps on url request.
  - Chrome & Firefox have the concept of user profiles, create a new one and extract the user data directory.
  - Ie & Edge more difficult to automate due to limited control with selenium, such as for adding an extension and it does not have the concept of user profiles.
- OSForensics (trialware)
  - Also used by Flowers et al. (2016).
  - Snapshots of the file system, compare them pre and after sample gathering.
- W10 Home 64-bit.
- Research indicates 80% of software is used in its default setting, Wills et al. (2016) confirms this for the use of Adblock Plus.

Approach

- Automated sample gathering.
  - *Control* Sample.
  - *Adblock* Sample.
  - *Private* browsing sample.
  - Browsing session entails the visitation of top 50 NL websites as per alexa.com.
  - Python + selenium + save timestamps on url request.
  - Chrome & Firefox have the concept of user profiles, create a new one and extract the user data directory.
  - Ie & Edge more difficult to automate due to limited control with selenium, such as for adding an extension and it does not have the concept of user profiles.
- OSForensics (trialware)
  - Also used by Flowers et al. (2016).
  - Snapshots of the file system, compare them pre and after sample gathering.
- W10 Home 64-bit.
- Research indicates 80% of software is used in its default setting, Wills et al. (2016) confirms this for the use of Adblock Plus.

But first explore the mechanisms used by ad blocking extensions and study its source code.

Adblocker mechanics

- Filter lists
    - By far most popular is EasyList
    - Whitelist filters overrule

Adblocker mechanics

- Filter lists
  - By far most popular is EasyList
  - Whitelist filters overrule

- Blocking requests
  - Extensions can register **content policies**, they get called whenever the browser needs to load something.
  - If there is a filter hit do not request the resource.

Adblocker mechanics

- Filter lists
  - By far most popular is EasyList
  - Whitelist filters overrule

- Blocking requests
  - Extensions can register **content policies**, they get called whenever the browser needs to load something.
  - If there is a filter hit do not request the resource.

- Hiding elements
  - Some elements can not be blocked otherwise page won't load.
  - Update **user style sheet** (overrides other styling) with styling > **display: none !important**

AdBlock Plus 3.8.4 - Firefox

```
addUserCSS(subject, selectors.map(
  selector => selector + "{display: none !important;}"
).join("\n"));
```

AdBlock Plus 3.8.4 - Firefox

```
addUserCSS(subject, selectors.map(
  selector => selector + "{display: none !important;}"
).join("\n"));

if (!isPrivate(subject))
  port.emit("addHits", filters);
```

Extensions storing capabilities

- **SessionStorage** - stores data for one session (data is lost when the browser tab is closed).

Extensions storing capabilities

- **SessionStorage** - stores data for one session (data is lost when the browser tab is closed).

- **LocalStorage** - stores data with no expiration date.

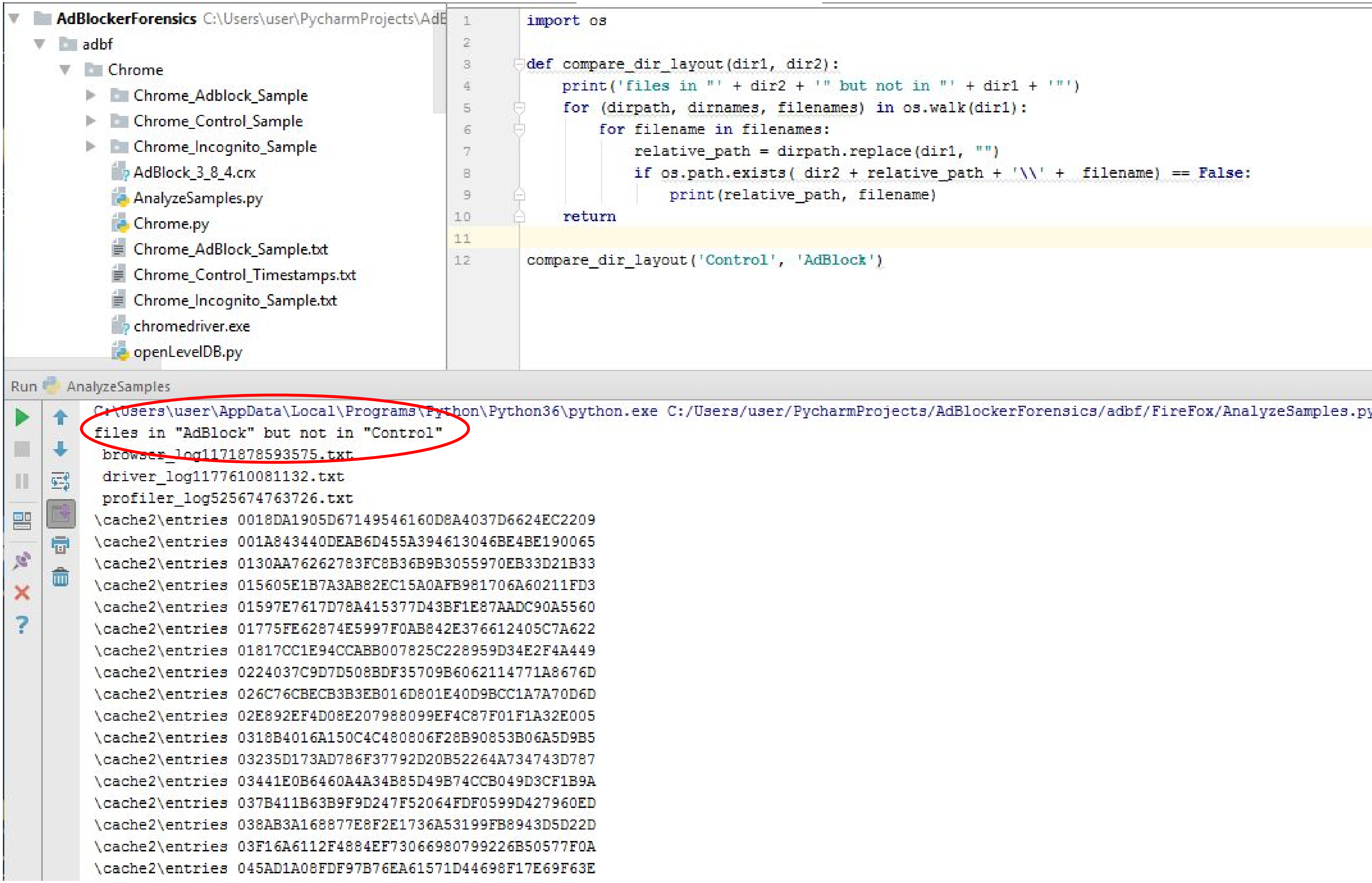
Extensions storing capabilities

- **SessionStorage** - stores data for one session (data is lost when the browser tab is closed).

- **LocalStorage** - stores data with no expiration date.

This concept is used in all the tested browsers.

Comparing samples



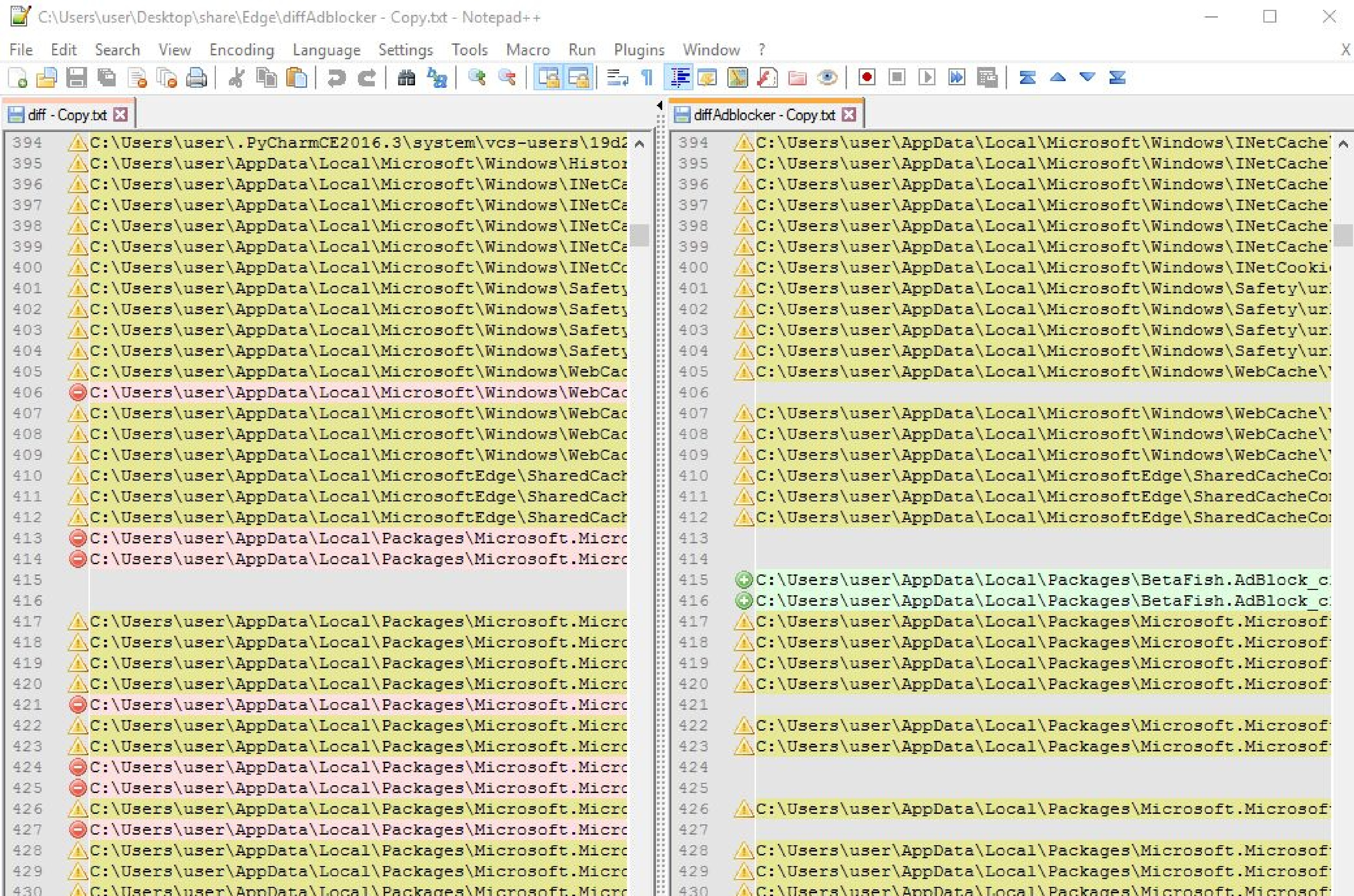
```python
import os

def compare_dir_layout(dir1, dir2):
    print('files in "' + dir2 + '" but not in "' + dir1 + '"')
    for (dirpath, dirnames, filenames) in os.walk(dir1):
        for filename in filenames:
            relative_path = dirpath.replace(dir1, "")
            if os.path.exists( dir2 + relative_path + '\\' +  filename) == False:
                print(relative_path, filename)
    return

compare_dir_layout('Control', 'AdBlock')
```

```
C:\Users\user\AppData\Local\Programs\Python\Python36\python.exe C:/Users/user/PycharmProjects/AdBlockerForensics/adbf/FireFox/AnalyzeSamples.py
files in "AdBlock" but not in "Control"
 browser_log1171878593575.txt
 driver_log1177610081132.txt
 profiler_log525674763726.txt
\cache2\entries 0018DA1905D67149546160D8A4037D6624EC2209
\cache2\entries 001A843440DEAB6D455A394613046BE4BE190065
\cache2\entries 0130AA76262783FC8B36B9B3055970EB33D21B33
\cache2\entries 015605E1B7A3AB82EC15A0AFB981706A60211FD3
\cache2\entries 01597E7617D78A415377D43BF1E87AADC90A5560
\cache2\entries 01775FE62874E5997F0AB842E376612405C7A622
\cache2\entries 01817CC1E94CCABB007825C228959D34E2F4A449
\cache2\entries 0224037C9D7D508BDF35709B6062114771A8676D
\cache2\entries 026C76CBECB3B3EB016D801E40D9BCC1A7A70D6D
\cache2\entries 02E892EF4D08E207988099EF4C87F01F1A32E005
\cache2\entries 0318B4016A150C4C480806F28B90853B06A5D9B5
\cache2\entries 03235D173AD786F37792D20B52264A734743D787
\cache2\entries 03441E0B6460A4A34B85D49B74CCB049D3CF1B9A
\cache2\entries 037B411B63B9F9D247F52064FDF0599D427960ED
\cache2\entries 038AB3A168877E8F2E1736A53199FB8943D5D22D
\cache2\entries 03F16A6112F4884EF73066980799226B50577F0A
\cache2\entries 045AD1A08FDF97B76EA61571D44698F17E69F63E
```

Comparing file change differences of samples.



diff - Copy.txt

```
⚠C:\Users\user\.PyCharmCE2016.3\system\vcs-users\19d2
⚠C:\Users\user\AppData\Local\Microsoft\Windows\Histor
⚠C:\Users\user\AppData\Local\Microsoft\Windows\INetCa
⚠C:\Users\user\AppData\Local\Microsoft\Windows\INetCa
⚠C:\Users\user\AppData\Local\Microsoft\Windows\INetCa
⚠C:\Users\user\AppData\Local\Microsoft\Windows\INetCa
⚠C:\Users\user\AppData\Local\Microsoft\Windows\INetCo
⚠C:\Users\user\AppData\Local\Microsoft\Windows\Safety
⚠C:\Users\user\AppData\Local\Microsoft\Windows\Safety
⚠C:\Users\user\AppData\Local\Microsoft\Windows\Safety
⚠C:\Users\user\AppData\Local\Microsoft\Windows\Safety
⚠C:\Users\user\AppData\Local\Microsoft\Windows\WebCac
⊖C:\Users\user\AppData\Local\Microsoft\Windows\WebCac
⚠C:\Users\user\AppData\Local\Microsoft\Windows\WebCac
⚠C:\Users\user\AppData\Local\Microsoft\Windows\WebCac
⚠C:\Users\user\AppData\Local\Microsoft\Windows\WebCac
⚠C:\Users\user\AppData\Local\MicrosoftEdge\SharedCach
⚠C:\Users\user\AppData\Local\MicrosoftEdge\SharedCach
⚠C:\Users\user\AppData\Local\MicrosoftEdge\SharedCach
⊖C:\Users\user\AppData\Local\Packages\Microsoft.Micro
⊖C:\Users\user\AppData\Local\Packages\Microsoft.Micro


⚠C:\Users\user\AppData\Local\Packages\Microsoft.Micro
⚠C:\Users\user\AppData\Local\Packages\Microsoft.Micro
⚠C:\Users\user\AppData\Local\Packages\Microsoft.Micro
⚠C:\Users\user\AppData\Local\Packages\Microsoft.Micro
⊖C:\Users\user\AppData\Local\Packages\Microsoft.Micro
⚠C:\Users\user\AppData\Local\Packages\Microsoft.Micro
⚠C:\Users\user\AppData\Local\Packages\Microsoft.Micro
⊖C:\Users\user\AppData\Local\Packages\Microsoft.Micro
⊖C:\Users\user\AppData\Local\Packages\Microsoft.Micro
⚠C:\Users\user\AppData\Local\Packages\Microsoft.Micro
⊖C:\Users\user\AppData\Local\Packages\Microsoft.Micro
⚠C:\Users\user\AppData\Local\Packages\Microsoft.Micro
⚠C:\Users\user\AppData\Local\Packages\Microsoft.Micro
⚠C:\Users\user\AppData\Local\Packages\Microsoft.Micro
```

diffAdblocker - Copy.txt

```
⚠C:\Users\user\AppData\Local\Microsoft\Windows\INetCache
⚠C:\Users\user\AppData\Local\Microsoft\Windows\INetCache
⚠C:\Users\user\AppData\Local\Microsoft\Windows\INetCache
⚠C:\Users\user\AppData\Local\Microsoft\Windows\INetCache
⚠C:\Users\user\AppData\Local\Microsoft\Windows\INetCache
⚠C:\Users\user\AppData\Local\Microsoft\Windows\INetCache
⚠C:\Users\user\AppData\Local\Microsoft\Windows\INetCooki
⚠C:\Users\user\AppData\Local\Microsoft\Windows\Safety\ur
⚠C:\Users\user\AppData\Local\Microsoft\Windows\Safety\ur
⚠C:\Users\user\AppData\Local\Microsoft\Windows\Safety\ur
⚠C:\Users\user\AppData\Local\Microsoft\Windows\Safety\ur
⚠C:\Users\user\AppData\Local\Microsoft\Windows\WebCache\

⚠C:\Users\user\AppData\Local\Microsoft\Windows\WebCache\
⚠C:\Users\user\AppData\Local\Microsoft\Windows\WebCache\
⚠C:\Users\user\AppData\Local\Microsoft\Windows\WebCache\
⚠C:\Users\user\AppData\Local\MicrosoftEdge\SharedCacheCo
⚠C:\Users\user\AppData\Local\MicrosoftEdge\SharedCacheCo
⚠C:\Users\user\AppData\Local\MicrosoftEdge\SharedCacheCo


⊕C:\Users\user\AppData\Local\Packages\BetaFish.AdBlock_c
⊕C:\Users\user\AppData\Local\Packages\BetaFish.AdBlock_c
⚠C:\Users\user\AppData\Local\Packages\Microsoft.Microsof
⚠C:\Users\user\AppData\Local\Packages\Microsoft.Microsof
⚠C:\Users\user\AppData\Local\Packages\Microsoft.Microsof
⚠C:\Users\user\AppData\Local\Packages\Microsoft.Microsof

⚠C:\Users\user\AppData\Local\Packages\Microsoft.Microsof
⚠C:\Users\user\AppData\Local\Packages\Microsoft.Microsof


⚠C:\Users\user\AppData\Local\Packages\Microsoft.Microsof

⚠C:\Users\user\AppData\Local\Packages\Microsoft.Microsof
⚠C:\Users\user\AppData\Local\Packages\Microsoft.Microsof
⚠C:\Users\user\AppData\Local\Packages\Microsoft.Microsof
```

Results Google Chrome/55.0.2883.87 + AdBlock

Chrome local storage for extensions -> LevelDB (key-value store written by Google)

Key	Value (contents)
blockage_stats	Epoch installation time
file:pattern.ini	Filter list + subscription
next_ping_time	Sends user data to https://ping.getadblock.com/stats/ on given epoch time
pref:blocked_total	Total amount of filter hits since installation
pref:currentVersion	Version number
pref:notificationdata	Stats about the subscriptions, including when to check for updates.
pref:settings	Some settings
pref:total_pings	Total amount of pings
userid	Unique user ID

Results Google Chrome/55.0.2883.87 + AdBlock

Chrome local storage for extensions -> LevelDB (key-value store written by Google)

Key	Value (contents)
blockage_stats	Epoch installation time
file:pattern.ini	Filter list + subsciption
next_ping_time	Sends user data to https://ping.getadblock.com/stats/ on given epoch time
pref:blocked_total	Total amount of filter hits since installation
pref:currentVersion	Version number
pref:notificationdata	Stats about the subscriptions, including when to check for updates.
pref:settings	Some settings
pref:total_pings	Total amount of pings
userid	Unique user ID

Results Microsoft Edge/14.14393 + AdBlock 1.9.0.0

Edge local storage for extensions -> .dat

Key	**Value (contents)**
Blockage_stats	Epoch time first filter hit+ total amount of filter hits since installation, split between 'total' and 'malware_total'.
Filter_lists	Pointing to filter lists location.
Last_subscriptions_check	Epoch time last time filters were updated
Next_ping_time	Sends user data to https://ping.getadblock.com/stats/ on given epoch time
Settings	Settings
Total_pings	Total amount of pings
Userid	Unique user ID

Results Microsoft Edge/14.14393 + AdBlock 1.9.0.0

Edge local storage for extensions -> .dat

Key	**Value (contents)**
Blockage_stats	Epoch time first filter hit+ total amount of filter hits since installation, split between 'total' and 'malware_total’.
Filter_lists	Pointing to filter lists location.
Last_subscriptions_check	Epoch time last time filters were updated
Next_ping_time	Sends user data to https://ping.getadblock.com/stats/ on given epoch time
Settings	Settings
Total_pings	Total amount of pings
Userid	Unique user ID

Results Internet Explorer 11 + Adblock Plus 1.6

Patterns.ini -> filter list subscription + filters

Settings.ini -> settings other than default

prefs.json -> notificationdata

Results Internet Explorer 11 + Adblock Plus 1.6

Patterns.ini -> filter list subscription + filters

Settings.ini -> settings other than default

prefs.json -> notificationdata

Results Mozilla Firefox 46.0 + Adblock Plus 2.8.2

Loc	Content
/adblockplus/patterns.ini	**Filter hits including a hitCounter and lastHit parameter** + filterList
/adblockplus/patterns-backup1.ini	If patterns.ini is full patterns-backup.ini is created with a number incrementing from 1.
AdBlock\extensions\{d10d0bf8-f5b5-c8b4-a8b2-2b9879e08c5d}/	AdBlock application files
prefs.js	Ablock Plus settings that are different than default are added here

Location is relative to the data directory of the Firefox profile.

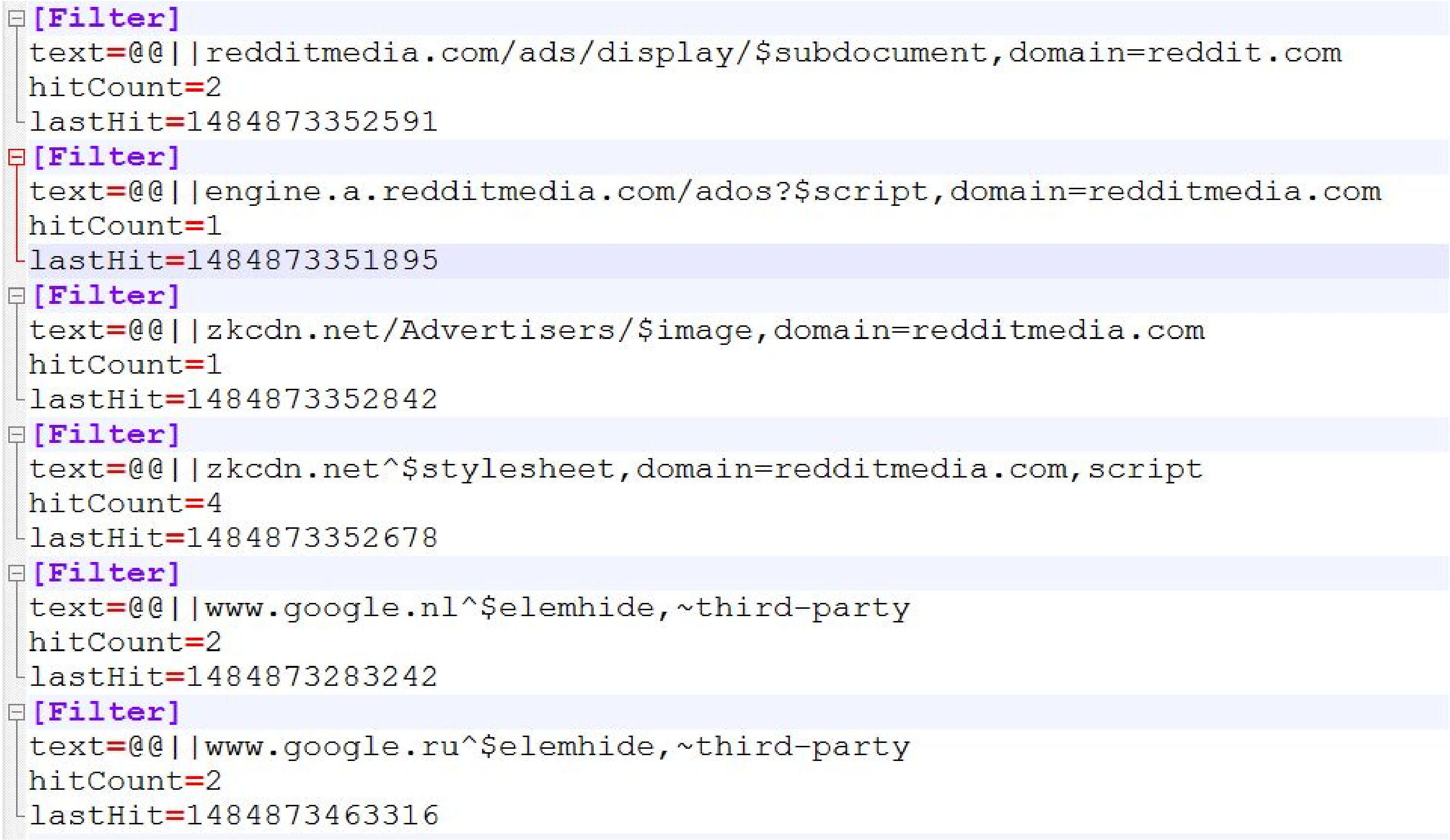
Results Mozilla Firefox 46.0 + Adblock Plus 2.8.2

Loc	
/adblockplus/patterns.ini	**hits including a ounter and lastHit rameter** + filterList
/adbloc atterns-backup	patterns.ini is full patterns-backup.ini is created with a number incrementing from 1.
10 a 8	AdBlock application files
prefs	Ablock Plus settings that are different than default are added here

Location is relativ directory of the Firefox profile.

Patterns.ini

- Filter
- hitCount (amount of times this filter is activated)
- Last time this filter is activated in epoch time



```
[Filter]
text=@@||redditmedia.com/ads/display/$subdocument,domain=reddit.com
hitCount=2
lastHit=1484873352591
[Filter]
text=@@||engine.a.redditmedia.com/ados?$script,domain=redditmedia.com
hitCount=1
lastHit=1484873351895
[Filter]
text=@@||zkcdn.net/Advertisers/$image,domain=redditmedia.com
hitCount=1
lastHit=1484873352842
[Filter]
text=@@||zkcdn.net^$stylesheet,domain=redditmedia.com,script
hitCount=4
lastHit=1484873352678
[Filter]
text=@@||www.google.nl^$elemhide,~third-party
hitCount=2
lastHit=1484873283242
[Filter]
text=@@||www.google.ru^$elemhide,~third-party
hitCount=2
lastHit=1484873463316
```

PoC - test on top 500 sites per https://moz.com/top500

- Bigger sample (top 500 websites per https://moz.com/top500).

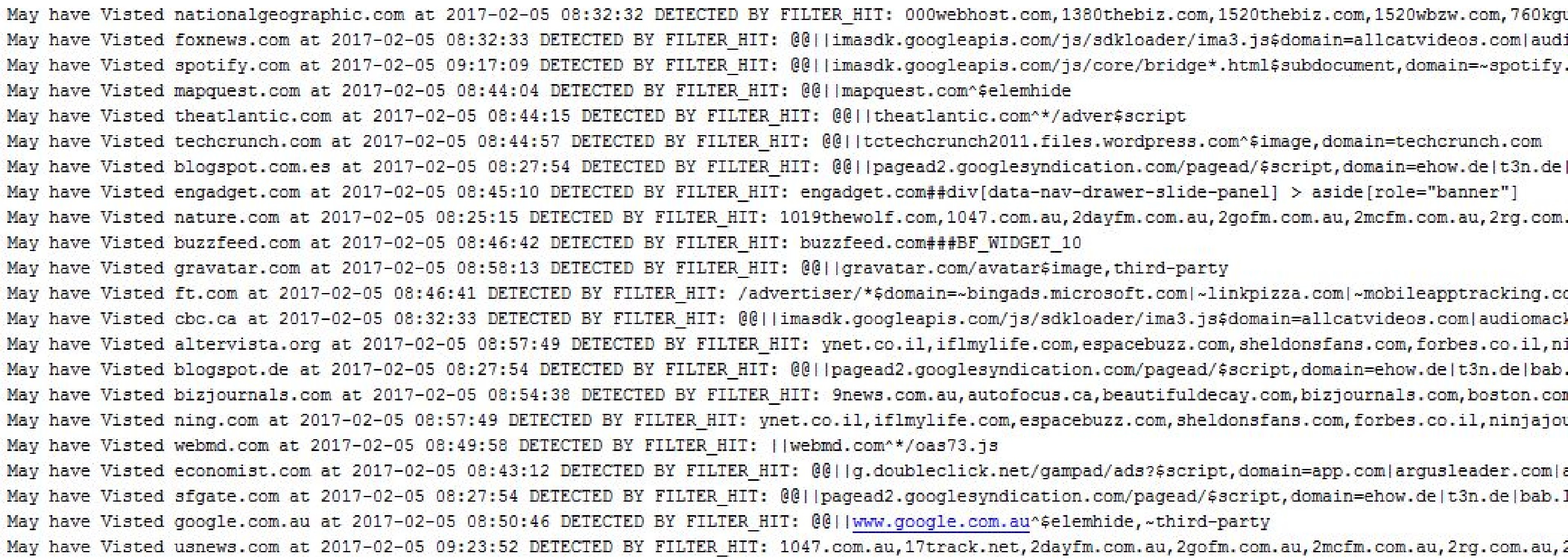
PoC - test on top 500 sites per https://moz.com/top500

- Bigger sample (top 500 websites per https://moz.com/top500).
- Use Firefox options to clear history / cookies / caches.

PoC - test on top 500 sites per https://moz.com/top500

- Bigger sample (top 500 websites per https://moz.com/top500).
- Use Firefox options to clear history / cookies / caches.

143 / 500 site visits left traces by filter hits.



```
May have Visted nationalgeographic.com at 2017-02-05 08:32:32 DETECTED BY FILTER_HIT: 000webhost.com,1380thebiz.com,1520thebiz.com,1520wbzw.com,760kgu
May have Visted foxnews.com at 2017-02-05 08:32:33 DETECTED BY FILTER_HIT: @@||imasdk.googleapis.com/js/sdkloader/ima3.js$domain=allcatvideos.com|audi
May have Visted spotify.com at 2017-02-05 09:17:09 DETECTED BY FILTER_HIT: @@||imasdk.googleapis.com/js/core/bridge*.html$subdocument,domain=~spotify.
May have Visted mapquest.com at 2017-02-05 08:44:04 DETECTED BY FILTER_HIT: @@||mapquest.com^$elemhide
May have Visted theatlantic.com at 2017-02-05 08:44:15 DETECTED BY FILTER_HIT: @@||theatlantic.com^*/adver$script
May have Visted techcrunch.com at 2017-02-05 08:44:57 DETECTED BY FILTER_HIT: @@||tctechcrunch2011.files.wordpress.com^$image,domain=techcrunch.com
May have Visted blogspot.com.es at 2017-02-05 08:27:54 DETECTED BY FILTER_HIT: @@||pagead2.googlesyndication.com/pagead/$script,domain=ehow.de|t3n.de|
May have Visted engadget.com at 2017-02-05 08:45:10 DETECTED BY FILTER_HIT: engadget.com##div[data-nav-drawer-slide-panel] > aside[role="banner"]
May have Visted nature.com at 2017-02-05 08:25:15 DETECTED BY FILTER_HIT: 1019thewolf.com,1047.com.au,2dayfm.com.au,2gofm.com.au,2mcfm.com.au,2rg.com.
May have Visted buzzfeed.com at 2017-02-05 08:46:42 DETECTED BY FILTER_HIT: buzzfeed.com###BF_WIDGET_10
May have Visted gravatar.com at 2017-02-05 08:58:13 DETECTED BY FILTER_HIT: @@||gravatar.com/avatar$image,third-party
May have Visted ft.com at 2017-02-05 08:46:41 DETECTED BY FILTER_HIT: /advertiser/*$domain=~bingads.microsoft.com|~linkpizza.com|~mobileapptracking.co
May have Visted cbc.ca at 2017-02-05 08:32:33 DETECTED BY FILTER_HIT: @@||imasdk.googleapis.com/js/sdkloader/ima3.js$domain=allcatvideos.com|audiomack
May have Visted altervista.org at 2017-02-05 08:57:49 DETECTED BY FILTER_HIT: ynet.co.il,iflmylife.com,espacebuzz.com,sheldonsfans.com,forbes.co.il,ni
May have Visted blogspot.de at 2017-02-05 08:27:54 DETECTED BY FILTER_HIT: @@||pagead2.googlesyndication.com/pagead/$script,domain=ehow.de|t3n.de|bab.
May have Visted bizjournals.com at 2017-02-05 08:54:38 DETECTED BY FILTER_HIT: 9news.com.au,autofocus.ca,beautifuldecay.com,bizjournals.com,boston.com
May have Visted ning.com at 2017-02-05 08:57:49 DETECTED BY FILTER_HIT: ynet.co.il,iflmylife.com,espacebuzz.com,sheldonsfans.com,forbes.co.il,ninjajou
May have Visted webmd.com at 2017-02-05 08:49:58 DETECTED BY FILTER_HIT: ||webmd.com^*/oas73.js
May have Visted economist.com at 2017-02-05 08:43:12 DETECTED BY FILTER_HIT: @@||g.doubleclick.net/gampad/ads?$script,domain=app.com|argusleader.com|a
May have Visted sfgate.com at 2017-02-05 08:27:54 DETECTED BY FILTER_HIT: @@||pagead2.googlesyndication.com/pagead/$script,domain=ehow.de|t3n.de|bab.l
May have Visted google.com.au at 2017-02-05 08:50:46 DETECTED BY FILTER_HIT: @@||www.google.com.au^$elemhide,~third-party
May have Visted usnews.com at 2017-02-05 09:23:52 DETECTED BY FILTER_HIT: 1047.com.au,17track.net,2dayfm.com.au,2gofm.com.au,2mcfm.com.au,2rg.com.au,2
```

Conclusion

RQ1: What artifacts are stored by the tested ad-blocking extensions during normal and private browsing?

Mode	**AdBlock + Chrome&Edge**	**Adblock Plus + Ie**	**Adblock Plus FireFox**
Normal	Settings, filterlist, total amount of filterHits	Settings, filterlists	Settings, filterlists, **filter hits.**
Private	Settings, filterlist, total amount of filterHits	Settings, filterlists	Settings, filterlists

Conclusion

RQ2: If artifacts are found, what is their usefulness in browser forensics?

- Total hitcount since installation -> useless.

Conclusion

RQ2: If artifacts are found, what is their usefulness in browser forensics?

- Total hitcount since installation -> useless.

- Filter hits -> useful.
- 143 / 500 traces in filter hits leading to last time visited.
- Firefox market share -> 10.4%.
- Estimated usage of Adblock Plus -> 20%.

0.104*0.2*(143/500) = Minimum of **~ 0.6%**

Future work

- Improve PoC by parsing the filter hits in such a way that domains can be classified as in:
    - definitely visited
    - maybe visited

Future work

- Improve PoC by parsing the filter hits in such a way that domains can be classified as in:
    - definitely visited
    - maybe visited

- Other adblocking extensions have a much smaller market share. So might not be interesting to test them. Use Windows tool Process Explorer instead of OSforensics.

?