
STUDY AND ANALYSIS OF ORWEB (AND ORFOX) ANONYMIZER(S) ON ANDROID DEVICES

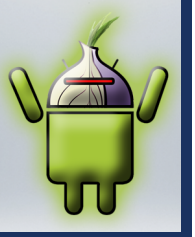
CLAUDIA MEDA & MATTIA EPIFANI

DFRWSEU 2016

LAUSANNE, 31 MARCH 2016

ORBOT

[HTTPS://GUARDIANPROJECT.INFO/APPS/ORBOT/](https://guardianproject.info/apps/orbot/)



What is Orbot?

- Open source software for Internet traffic encryption through computers around the world
- Configured to transparently proxy all of Internet traffic through **Tor** (The Onion Router)
- Choice which specific apps can be use through Tor
- Private internet connection
- Private web surfing
- Private chat messaging
- Privacy on Twitter

ORWEB

HTTPS://GUARDIANPROJECT.INFO/APPS/ORWEB/

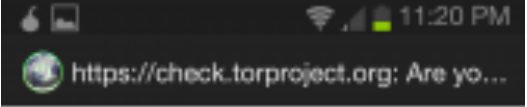


What is Orweb?

- Current default browser for Orbot on Android → evades tracking and censorship by bouncing encrypted traffic several times through computers around the world.
- Based on Orbot



“When a communication arrives from Tor, you can never know where or whom it’s from”



Congratulations. Your browser is configured to use Tor.

Please refer to the [Tor website](#) for further information about using Tor safely. You are now free to browse the Internet anonymously.

Your IP address appears to be: 204.124.83.131

This page is also available in the following languages:

- [العربية](#) [Arabic](#) [Burmese](#) [Cebuano](#) [Deutsch](#) [Dutch](#) [English](#) [Español](#) [Estonian](#) [فارسی](#) [Farsi](#) [Français](#) [Italiano](#) [日本語](#) [Nihongo](#) [Português](#) [Portuguese](#) [Русский](#) [Russian](#) [Türkçe](#) [Turkish](#) [Українська](#) [Ukrainian](#)

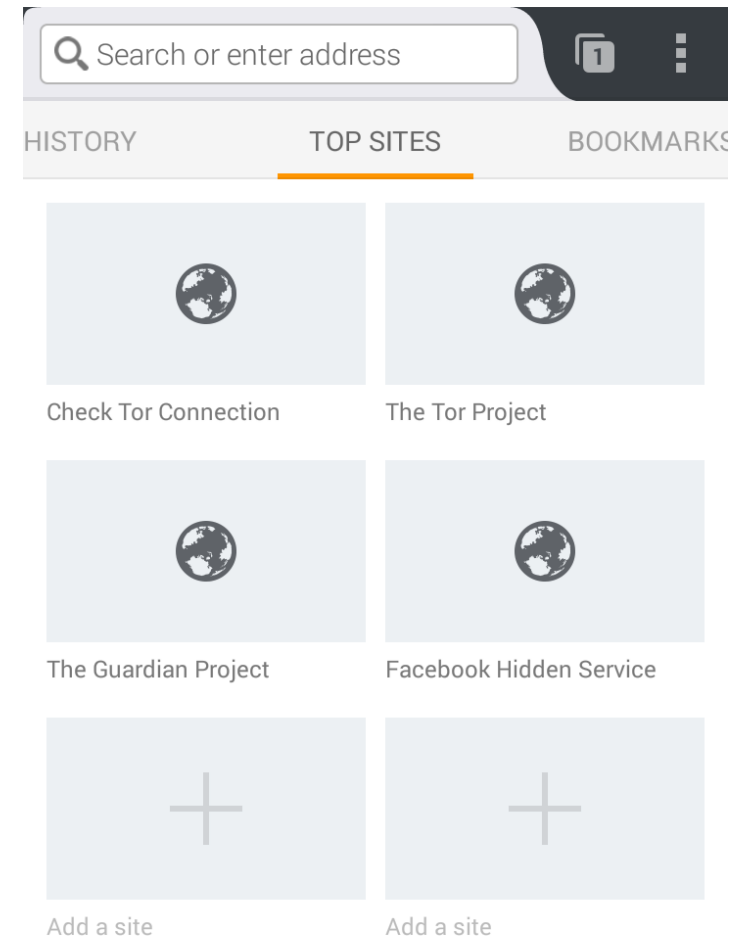
ORFOX

[HTTPS://GUARDIANPROJECT.INFO/2015/06/30/ORFOX-ASPIRING-TO-BRING-TOR-BROWSER-TO-ANDROID/](https://guardianproject.info/2015/06/30/orfox-aspiring-to-bring-tor-browser-to-android/)



What is Orfox?

- New browser for Android → BETA release available on Google Play for public testing only
- Built from the same source code as Tor Browser (which is built upon Firefox)
- Required Orbot app to connect to the Tor network
- It allows users to bookmark sites



<https://t.me/learningnets>

ANALYSIS METHODOLOGY – PART I



ENVIRONMENT

Samsung Galaxy S5 with
Android 5.0

Rooting with KingoRoot

INSTALLATION

Orbot download, install and
execution

Orweb download, install
and execution

Orfox download, install and
execution

DEVICE PHYSICAL ACQUISITION

SYSTEM FOLDER
PACKAGES.LIST

INSTALLED APPS INFORMATION (PACKAGE NAME, UID, APP PATH)



- Package name **org.torproject.android**
UserID **10076**
App path **/data/data/org.torproject.android**
- Package name **info.guardianproject.browser**
UserID **10077**
App path **/data/data/info.guardianproject.browser**
- Package name **info.guardianproject.orfox**
UserID **10078**
App path **/data/data/info.guardianproject.orfox**

ORBOT

ORWEB

ORFOX

SYSTEM FOLDER PACKAGES.XML

LIST OF PERMISSIONS AND PACKAGES/APPLICATIONS



```
<package name="org.torproject.android" userId="10076" version="15012310" ut="151b5c6d5a5"
it="151b5c6d5a5" ft="151b5c6cf20" flags="540228" dt="151b5c6db57" dm="2"
nativeLibraryRootRequiresIsa="true" nativeLibraryDir="/data/app/org.torproject.android-1/lib/arm"
nativeLibraryRootDir="/data/app/org.torproject.android-1/lib"
nativeLibraryPath="/data/app/org.torproject.android-1/lib" codePath="/data/app/org.torproject.android-1"
primaryCpuAbi="armeabi-v7a" installer="com.android.vending">
```

```
<perms>
```

```
<item name="android.permission.RECEIVE_BOOT_COMPLETED"/>
```

```
<item name="org.torproject.android.MANAGE_TOR"/>
```

Attribute	Description	Timestamp
UT	Timestamp in hex format of last update	Fri, 18 Dec 2015 – 15:48:05
IT	Timestamp in hex format of fist time installation	Fri, 18 Dec 2015 – 15:48:05

```
</package>
```

SYSTEM FOLDER
PACKAGE-USAGE.LIST
APP LAST EXECUTIONTIME (EPOCH)



Application	Timestamp
org.torproject.android	1451345825.267
info.guardianproject.browser	1450459648.348
info.guardianproject.orfox	1452006535.657

SYSTEM FOLDER
POWERMANAGER
POWER (AND APPS) USAGE STATISTICS



info.guardianproject.browser

time	power	totalpower
Filter	Filter	Filter
1450455938456	0.0	0.0
1450457755107	0.0	0.0
1450460984733	0.0	0.0
1451385746078	0.653686011023...	0.653686011023...

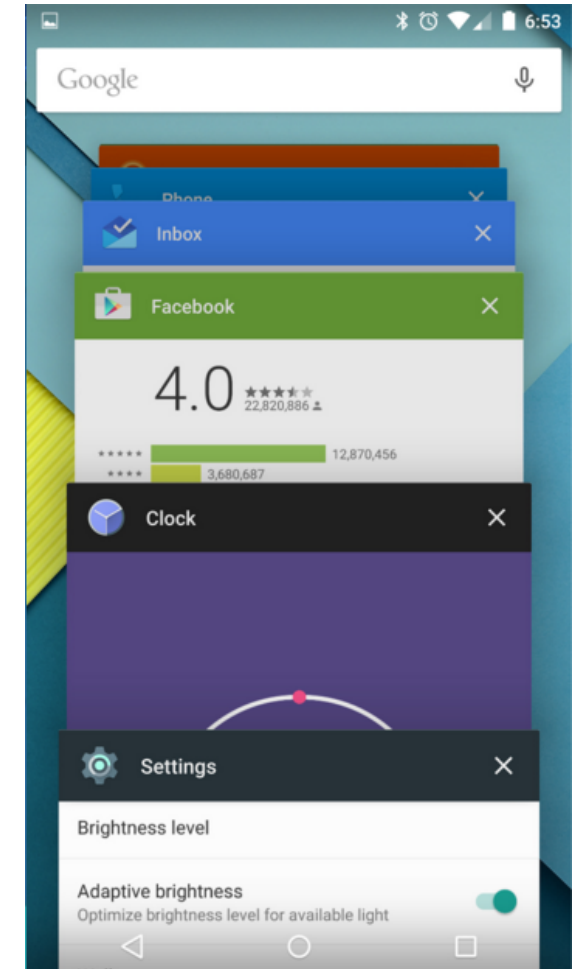
usage_time
Filter
0
0
0
10710

SYSTEM FOLDER \\RECENT_TASKS RECENT ACTIVITIES LOGS (XML FORMAT)



```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<task task_id="13" real_activity="info.guardianproject.browser/.Browser"
affinity="info.guardianproject.browser" root_has_reset="true"
auto_remove_recents="false" asked_compat_mode="false" user_id="0"
effective_uid="10077" task_type="0" first_active_time="1451385683082"
last_active_time="1451385798766" last_time_moved="1451385798756"
never_relinquish_identity="true" task_description_color="ff212121"
task_affiliation_color="-14606047" task_affiliation="13" prev_affiliation="-1"
next_affiliation="-1" calling_uid="10077"
calling_package="info.guardianproject.browser" multiwindow_style="0"
is_private_mode="false">
<intent action="android.intent.action.MAIN"
component="info.guardianproject.browser/.Browser" flags="10200000">
<categories category="android.intent.category.LAUNCHER" />
</intent>
</task>
```

<https://t.me/learningnets>



SYSTEM FOLDER

\USAGESTATS\WEEKLY - \USAGESTATS\MONTHLY -
\USAGESTATS\YEARLY
USAGE STATISTICS



```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
```

```
<usagestats version="1" endTime="2381450658">
```

...

```
<packages>
```

```
<package lastTimeActive="1454766326" package="org.torproject.android"  
timeActive="193858" lastEvent="2" />
```

```
<package lastTimeActive="1456652361" package="info.guardianproject.browser"  
timeActive="3519627" lastEvent="2" />
```

...

```
</packages>
```

```
</usagestats>
```

DATA FOLDER

\COM.ANDROID.VENDING\DATABASES\LOCALAPPSTATE.DB

APPLICATION INFORMATION AND UPDATES



- Package Name
- Delivery Data Timestamp
- First Download Timestamp

package_name	delivery_data_timestamp_ms	first_download_ms
tv.peel.smartremote	1451338441276	1451338442217
stericson.busybox	1450446629183	1450446629822
org.torproject.android	1450453680050	1450453680778
info.guardianproject.browser	1450454309701	1450454310364

- Account
- Title
- Last Notified Version
- Last Update Timestamp

account	title	last_notified...	last_update_timestamp_...
orbotforensics@gmail.com	Peel Smart Remote	86120	1451338461971
mattia.epifani@realitynet.it	BusyBox	186	0
orbotforensics@gmail.com	Orbot: Proxy with Tor	15012310	0
orbotforensics@gmail.com	Naviga in Privato	7010	0

<https://t.me/learningnets>

DATA FOLDER

\COM.SEC.ANDROID.APP.LAUNCHER\DATABASES\LAUNCHER.DB

APPLICATION DESKTOP SHORTCUTS (POSITION, ICON, INTENT, ETC.)



- Screen position
- Intent

cellX	cellY	spanX	spanY	title	intent
1	3	1	1	Orweb	#Intent;action=android.intent.action.MAIN;category=android.intent.category.LAUNCHER;launchFlags=0x10000000;package=info.guardianproject.browser;component=info.guardianproject.browser/.Browser;end
3	2	1	1	Orbot	#Intent;action=android.intent.action.MAIN;category=android.intent.category.LAUNCHER;launchFlags=0x10000000;package=org.torproject.android;component=org.torproject.android/.OrbotMainActivity;end

- Icon Package
- Icon Resource
- Icon

iconPackage	iconResource	icon
info.guardianproject.browser	info.guardianproject.browser:drawable/ic_launcher	
org.torproject.android	org.torproject.android:drawable/ic_launcher	

<https://t.me/learningnets>

DATA FOLDER

\COM.SAMSUNG.ANDROID.SM\DATABASES\LOWPOWERCONTEXT-
SYSTEM-DB

SAMSUNG SMART MANAGER



Package name

Start Time

End Time

id	package_name	start_time	start_time_string	end_time	end_time_string	uploaded	created_at	modified_at
74	org.torproject.android	1450454093829	2015/12/18 16:54:53	1450454157367	2015/12/18 16:55:57	<null>	1450459124000	1450459124000
76	info.guardianproject.browser	1450454335077	2015/12/18 16:58:55	1450454758257	2015/12/18 17:05:58	<null>	1450459124000	1450459124000
78	info.guardianproject.browser	1450454812155	2015/12/18 17:06:52	1450454910645	2015/12/18 17:08:30	<null>	1450459124000	1450459124000
87	info.guardianproject.browser	1450457718584	2015/12/18 17:55:18	1450458131244	2015/12/18 18:02:11	<null>	1450459124000	1450459124000
88	info.guardianproject.browser	1450458133410	2015/12/18 18:02:13	1450458134810	2015/12/18 18:02:14	<null>	1450459124000	1450459124000
89	info.guardianproject.browser	1450458136523	2015/12/18 18:02:16	1450458137820	2015/12/18 18:02:17	<null>	1450459124000	1450459124000
90	info.guardianproject.browser	1450458143235	2015/12/18 18:02:23	1450458146889	2015/12/18 18:02:26	<null>	1450459124000	1450459124000
91	info.guardianproject.browser	1450458397807	2015/12/18 18:06:37	1450459089757	2015/12/18 18:18:09	<null>	1450459124000	1450459124000
92	info.guardianproject.browser	1450459100118	2015/12/18 18:18:20	1450459101350	2015/12/18 18:18:21	<null>	1450459124000	1450459124000
93	info.guardianproject.browser	1450459102819	2015/12/18 18:18:22	1450459104457	2015/12/18 18:18:24	<null>	1450459124000	1450459124000
94	info.guardianproject.browser	1450459106692	2015/12/18 18:18:26	1450459107923	2015/12/18 18:18:27	<null>	1450459124000	1450459124000
96	org.torproject.android	1450459466971	2015/12/18 18:24:26	1450459483405	2015/12/18 18:24:43	<null>	1450461534000	1450461534000
97	org.torproject.android	1450459535906	2015/12/18 18:25:35	1450459649363	2015/12/18 18:27:29	<null>	1450461534000	1450461534000

SYSTEM AND DATA FOLDER OTHER FILES



- `\system\batterystats-checkin.bin`
- `\system\AppOps.XML`
- `\system\procstats\state-YYYY-MM-DD-HH-MM-SS.bin`
- `\data\com.android.vending\databases\library.db`
- `\data\com.android.vending\databases\package_verification.db`
- `\data\com.google.android.partnersetup\shared_prefs\ApplicationHidingPreferences.xml`
- `\data\com.samsung.android.sm\databases\sm.db`
- `\data\com.google.android.googlequicksearchbox\databases\icingcorpora.db`

ANALYSIS METHODOLOGY – PART 2



BROWSING WITH ORWEB

1

Visited sites

genoacfc.it

thehiddenwiki.org

rso4hutlefirefqp.onion

torlinkbgs6aabns.onion

xfnwyig7olypdq5r.onion

dfrws.org

luccacomicsandgames.com

starwars.com

DEVICE PHYSICAL ACQUISITION

2

ORWEB APPLICATION FOLDER
\\DATA\\INFO.GUARDIANPROJECT.BROWSER\\APP_WEBVIEW\\COOKIES
COOKIES DATABASE



host_key
rso4hutlefirefqp.onion
xfnwyig7olypdq5r.onion
.flickr.com
.flickr.com
adv.luccacomicsandgames.com
adv.luccacomicsandgames.com
adv.luccacomicsandgames.com
adv.luccacomicsandgames.com
adv.luccacomicsandgames.com

SQLite DB
Temporarily store website Cookies

Information not
immediately deleted

Information about
previously visited sites

Unallocated space
inside DB file and
Cookies-journal

ORWEB APPLICATION FOLDER \DATA\INFO.GUARDIANPROJECT.BROWSER\CACHE\ORG.CHROMIUM.ANDROID_WEBVIEW CACHE FOLDER



Specific structure of cache element

Header

30 5C 72 A7 1B 6D FB FC 05 00 00 00

URL

Encoded content (i.e. JPG file)

HTTP response with DATE and TIME

```

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 30 5C 72 A7 1B 6D FB FC 05 00 00 00 4A 00 00 00 0\r$.mũü....J...
00000010 E7 8F E1 36 00 00 00 00 68 74 74 70 3A 2F 2F 67 ç.á6....http://g
00000020 70 2D 63 6F enoacfc.it/wp-co
00000030 79 2F 6C 75 nent/gallery/lu
00000040 6E 6F 50 72 glio-2015/TanoPr
00000050 31 38 2E 6A ess_Srl_140618.j
00000060 00 01 01 01 pgÿÿÿà..JFIF....
00000070 45 41 54 4F .`. . .ÿp.;CREATO
00000080 31 2E 30 20 R: gd-jpeg v1.0
00000090 50 45 47 20 (using IJG JPEG
000000A0 79 20 3D 20 v62), quality =
000000B0 02 02 03 03 90.ÿÿ.C.....

00007960 20 32 30 30 *...HTTP/1.1 200
00007970 4C 65 6E 67 OK.Content-Leng
00007980 74 68 3A 20 33 30 39 32 36 00 45 54 61 67 3A 20 th: 30926.ETag:
00007990 22 37 38 63 65 2D 35 32 33 63 64 61 33 35 34 62 "78ce-523cda354b
000079A0 38 62 38 22 00 44 61 74 65 3A 20 46 72 69 2C 20 8b8".Date: Fri,
000079B0 31 38 20 44 65 63 20 32 30 31 35 20 31 36 3A 30 18 Dec 2015 16:0
000079C0 38 3A 32 39 20 47 4D 54 00 4C 61 73 74 2D 4D 6F 8:29 GMT.Last-Mo
000079D0 64 69 66 69 65 64 3A 20 54 68 75 2C 20 30 35 20 dified: Thu, 05
000079E0 4E 6F 76 20 32 30 31 35 20 31 36 3A 32 39 3A 35 Nov 2015 16:29:5
000079F0 39 20 47 4D 54 00 53 65 72 76 65 72 3A 20 41 70 9 GMT.Server: Ap
00007A00 61 63 68 65 2F 32 2E 34 2E 31 30 00 41 63 63 65 ache/2.4.10.Acce
00007A10 70 74 2D 52 61 6E 67 65 73 3A 20 62 79 74 65 73 pt-Ranges: bytes
00007A20 00 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 69 .Content-Type: i
00007A30 6D 61 67 65 2F 6A 70 65 67 00 00 09 00 00 00 mage/jpeg.....
00007A40 31 32 37 2E 30 2E 30 2E 31 00 00 00 B6 1F 00 00 127.0.0.1...
  
```



ANALYSIS METHODOLOGY – PART 3



1
**BROWSING
WITH ORFOX**

Visited sites
thehiddenwiki.org
3g2upl4pq6kufc4m.onion
wikitjerrta4qgz4.onion
easycoinsayj7p5l.onion
torbox3uiot6wchz.onion
bodybuilding.com
genoacfc.it
volleyball.org
atpworldtour.com

<https://t.me/learningnets>

2
**ADDED
GENOACFC.IT TO
BOOKMARKS**

3
**DEVICE PHYSICAL
ACQUISITION**

ORFOX APPLICATION FOLDER

`\DATA\INFO.GUARDIANPROJECT.ORFOX\FILE\MOZILLA\<ID>.DEFAULT`



STORE TEMPORARY FILE
DURING BROWSER ACTIVITY

Browser.db-wal

Tabs.db

Tabs.db-wal

Tabs.db:
• current Tabbed sites
Tabs.db-wal:
• previously Tabbed sites

```
root@klte:/data/data/info.guardianproject.orfox/files/mozilla/9wks9tiv.default # ls -la
-rw----- u0_a78 u0_a78 0 2016-01-15 17:10 .parentlock
drwx----- u0_a78 u0_a78 2016-01-05 16:00 HTTPSEverywhereUserRules
-rw----- u0_a78 u0_a78 208 2016-01-15 17:37 SiteSecurityServiceState.txt
-rw----- u0_a78 u0_a78 154384 2016-01-15 17:11 blocklist.xml
-rw-rw---- u0_a78 u0_a78 4096 2016-01-05 16:00 browser.db
-rw----- u0_a78 u0_a78 32768 2016-01-15 17:37 browser.db-shm
-rw----- u0_a78 u0_a78 2315472 2016-01-15 17:37 browser.db-wal
-rw----- u0_a78 u0_a78 218 2016-01-15 17:10 compatibility.ini
-rw----- u0_a78 u0_a78 131072 2016-01-05 16:00 cookies.sqlite
-rw----- u0_a78 u0_a78 32768 2016-01-15 17:10 cookies.sqlite-shm
-rw----- u0_a78 u0_a78 0 2016-01-15 17:10 cookies.sqlite-wal
drwx----- u0_a78 u0_a78 2016-01-15 17:10 extensions
-rw----- u0_a78 u0_a78 193 2016-01-15 17:10 extensions.ini
-rw----- u0_a78 u0_a78 3687 2016-01-15 17:10 extensions.json
-rw----- u0_a78 u0_a78 0 2016-01-05 16:00 extensions.sqlite
-rw----- u0_a78 u0_a78 196608 2016-01-05 16:00 formhistory.sqlite
drwx----- u0_a78 u0_a78 2016-01-05 16:01 gmp
drwx----- u0_a78 u0_a78 2016-01-05 16:01 gmp-gmopenh264
-rw-rw---- u0_a78 u0_a78 73728 2016-01-15 17:37 health.db
-rw----- u0_a78 u0_a78 41552 2016-01-15 17:37 health.db-journal
lrwxrwxrwx u0_a78 u0_a78 2016-01-15 17:10 lock -> 127.0.0.1:+15172
-rw-rw---- u0_a78 u0_a78 37 2016-01-15 17:11 prefs.js
-rw-rw---- u0_a78 u0_a78 80 2016-01-15 17:09 profile_info_cache.json
-rw-rw---- u0_a78 u0_a78 2016-01-15 17:32 readercache
-rw-rw---- u0_a78 u0_a78 96 2016-01-15 17:10 revocations.txt
-rw-rw---- u0_a78 u0_a78 2016-01-05 16:01 safebrowsing
-rw-rw---- u0_a78 u0_a78 97 2016-01-05 16:00 search.json
-rw-rw---- u0_a78 u0_a78 41 2016-01-15 17:07 sessionstore.bak
-rw-rw---- u0_a78 u0_a78 41 2016-01-15 17:37 sessionstore.js
-rw-rw---- u0_a78 u0_a78 2 2016-01-15 17:09 snippets.json
-rw-rw---- u0_a78 u0_a78 2016-01-15 17:13 startupCache
-rw-rw---- u0_a78 u0_a78 42 2016-01-05 16:00 suggestedsites.json
-rw-rw---- u0_a78 u0_a78 40960 2016-01-15 17:36 tabs.db
-rw----- u0_a78 u0_a78 32768 2016-01-15 17:37 tabs.db-shm
-rw----- u0_a78 u0_a78 420272 2016-01-15 17:37 tabs.db-wal
-rw----- u0_a78 u0_a78 27 2016-01-05 16:00 times.json
-rw-rw---- u0_a78 u0_a78 98304 2016-01-05 16:02 webappsstore.sqlite
-rw----- u0_a78 u0_a78 32768 2016-01-15 17:10 webappsstore.sqlite-shm
-rw----- u0_a78 u0_a78 0 2016-01-15 17:10 webappsstore.sqlite-wal
```

http

ORFOX APPLICATION FOLDER

\\DATA\INFO.GUARDIANPROJECT.ORFOX\FILE\MOZILLA\<ID>.DEFAULT



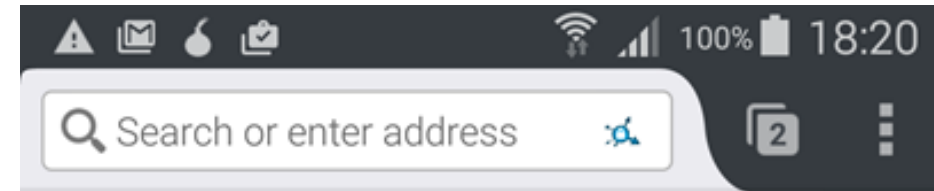
BROWSER.DB-WAL

Bookmarks

Reading List

Top Sites (only if added by user)

Visited websites URLs



```
Cyber Certifications | Researchhttps://www.sans.org/€
encyclopediahttps://en.m.wikipedia.org/wiki/Genoa€
ehhttp://genoacfc.it/€ R W M RF „ Y_zrmCHvT69md
e ý R N!, R N!,cGduvBu09b7k\ 3M % Firefox Marl
```

```
7 % SANS Information Security Training |
RF% ·ý RF% ·ö8A_ecdfx198u| JW % Genoa - Wikipedia, the free
RF!FL RF!FIAuvNDEwNYVzKa I3 % Genoa Cfc â€” Official Websit
-c % Firefox: Supporthttps://support.mozilla.org/products/mobil
etplacehttps://marketplace.firefox.com/ p R N!, R N!,YfTwi-1dgoLxj KS
```

https://t.me/learningnets

ANALYSIS METHODOLOGY – PART 4



UNINSTALL

Orbot uninstall

Orweb uninstall

Orfox uninstall

DEVICE PHYSICAL ACQUISITION

RESIDUAL TRACES AFTER UNINSTALL



- `\system\powerManager`
- `\system\usagestats\monthly` - `\usagestats\weekly` - `\usagestats\yearly`
- `\data\com.android.vending\databases\localappstate.db`
- `\data\com.android.vending\databases\library.db`
- `\data\com.android.vending\databases\package_verification.db`
- `\data\com.google.android.googlequicksearchbox\databases\icingcorpora.db`
- `\data\com.google.android.partnersetup\shared_prefs\ApplicationHidingPreferences.xml`
- `\data\com.samsung.android.sm\databases\lowpowercontext-system-db`
- `\data\com.samsung.android.sm\databases\sm.db`

PROPOSED INVESTIGATION METHODOLOGY



\SYSTEM

- PACKAGES.LIST
- PACKAGE-
USAGE.LIST
- POWERMANAGER
- RECENT_TASKS
- USAGESTATS

\DATA

- LOCALAPPSTATE.DB
- LAUNCHER.DB
- LOWPOWERCONTEX
T-SYSTEM-DB

\INFO.GUARDIANP PROJECT.BROWSER

- \COOKIES
- \CACHE
 - STRING HEADER
SEARCH
[30 5C 72 A7 1B 6D FB
FC 05 00 00 00]

\INFO.GUARDIANP ROJECT.ORFOX

- BROWSER.DB-
WAL
- TABS.DB
- TABS.DB-WAL

Q&A?

Claudia Meda



- PhD student in Science and Technology for Electronic and Telecommunications Engineering
University of Genoa, Italy



claudia22.meda@gmail.com



[@KlodiaMaida](https://twitter.com/KlodiaMaida)



<https://it.linkedin.com/in/claudia-meda-3142046b>

Mattia Epifani



- Digital Forensics Analyst
- CEO @ REALITY NET – System Solutions – Genoa, Italy
- GCFA, GMOB, GNFA, GREM
- CEH, CHFI, CCE, CIFI, ECCE, AME, ACE, MPSC



mattia.epifani@realitynet.it



[@mattiaep](https://twitter.com/mattiaep)



<http://www.linkedin.com/in/mattiaepifani>



<http://www.realitynet.it>



<http://blog.digital-forensics.it>

<https://t.me/learningnets>