

# Privacy Assignment - 2

Submitted by : Prashanthi Kanniappan Murthy

1) Discussing the two scenarios of tracking here:

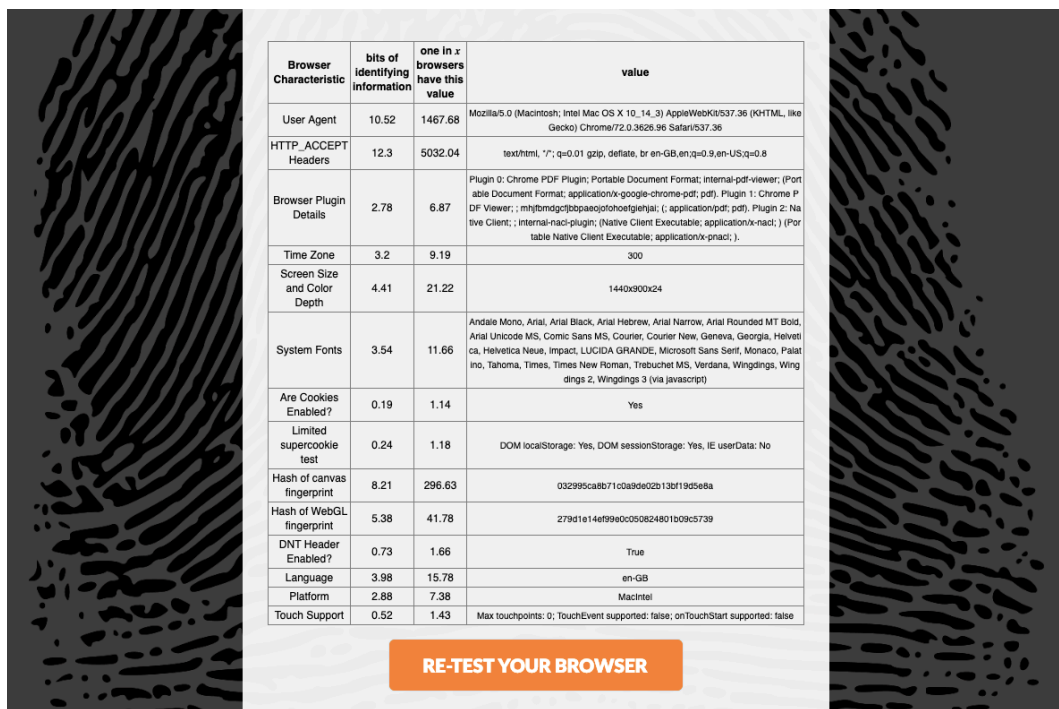
- a) Using third party cookies: When my iframe is included in multiple websites and I track based on third party cookies, every time a response is sent back to my domain, all the cookies from websites that are hit with my iframe are sent back. During this process, I get a clear picture of what my targeted client does - all the websites he visited, his interests, his current situation etc.
- b) Using Canvas fingerprinting: When I use this technique to track my user, I get his machine's unique hashcode based on the graphics and other entities used to create the uniqueness.

Case (b) doesn't give you a detailed picture of your targeted user. If the user visits multiple sites, canvas fingerprinting will give the same uniqueness irrespective of the sites he visited, whereas third party cookies give a in-depth view of his interests and situations. Therefore, canvas fingerprinting does not eliminate the need for third-party cookies.

2) **Panopticlick**



FIG1: PANOPTICCLICK FROM DESKTOP BROWSER.



**FIG2: DETAILED ENTROPY BITS FROM BROWSER**

How well are you protected against non-consensual Web tracking? After analyzing your browser and add-ons, the answer is ...

No. You are not protected against tracking on the Web. We suggest **installing extra protections**. Privacy Badger isn't available for your browser / OS, but **Disconnect** may work for you.

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

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticlick does not measure all forms of tracking and protection.

Your browser fingerprint **appears to be unique** among the 140,909 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.1 bits of identifying information**.

FIG3: PANOPTICCLICK FROM MOBILE CHROME BROWSER

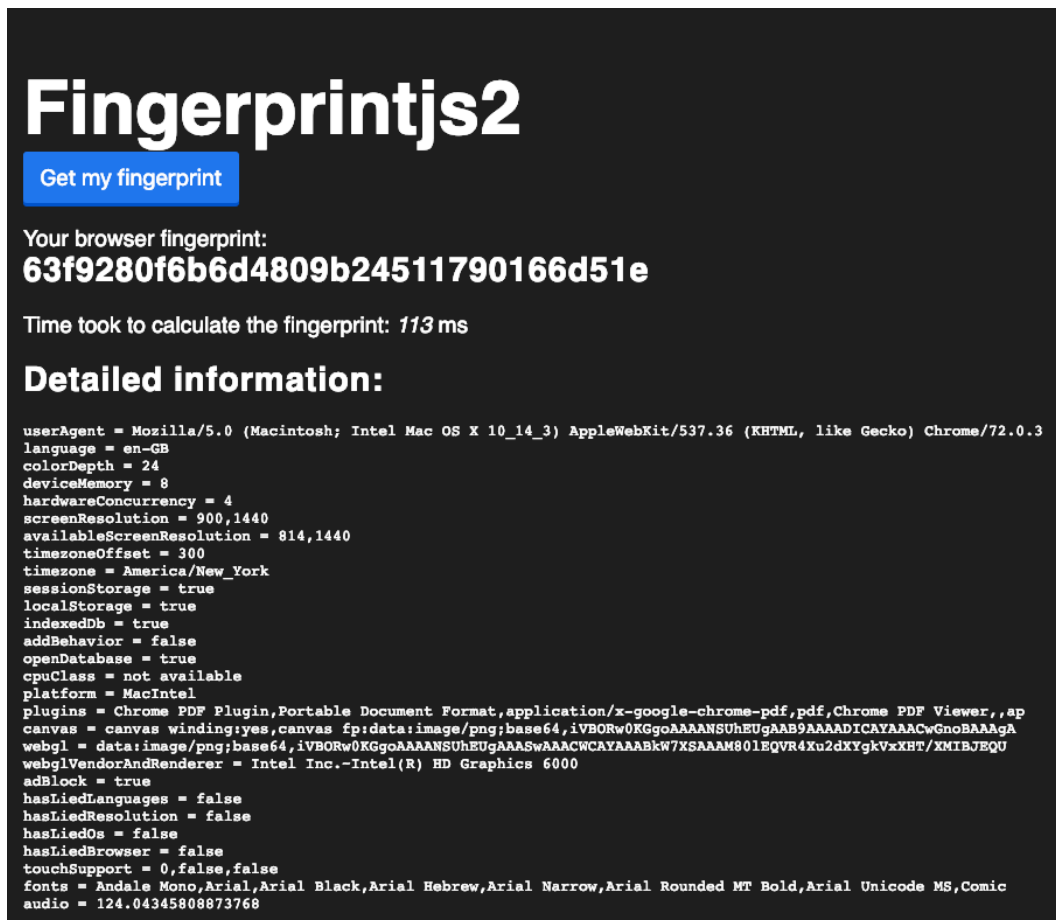
Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	11.68	3276.95	Mozilla/5.0 (Linux; Android 9; ONEPLUS A5000) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Mobile Safari/537.36
HTTP_ACCEPT Headers	12.3	5032.46	text/html, */*; q=0.01 gzip, deflate, br en-GB,en;q=0.9,en-US;q=0.8
Browser Plugin Details	0.87	1.82	undefined
Time Zone	3.2	9.19	300
Screen Size and Color Depth	7.28	155.7	412x732x24
System Fonts	3.91	15.08	Arial, Courier, Courier New, Georgia, Helvetica, Monaco, Palatino, Tahoma, Times, Times New Roman, Verdana, Wingdings 2, Wingdings 3 (via javascript)
Are Cookies Enabled?	0.19	1.14	Yes
Limited supercookie test	0.24	1.18	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	6.83	114.0	59c8024adea9c76bb21545de5fb7c966
Hash of WebGL fingerprint	5.84	57.37	4022cea05438948fc62758501af3c454
DNT Header Enabled?	1.34	2.52	False
Language	3.98	15.78	en-GB
Platform	3.96	15.6	Linux armv8l
Touch Support	3.92	15.1	Max touchpoints: 5; TouchEvent supported: true; onTouchStart supported: true

**FIG4: ENTROPY BIT DETAILS FROM MOBILE CHROME BROWSER.**

Major differences noted are:

- 1) My desktop Chrome browser is guarded with Adblock Plus, Ghostery and Privacy Badger whereas my Chrome browser in mobile doesn't have any of these tools. Still I get the same number of bit entropy in both cases.
- 2) Browser plugin details vary greatly, when my mobile chrome didn't have any extensions and was undefined. in desktop I was uniquely identifiable as 1 in 7, whereas in mobile I was uniquely identifiable as 1 in 2 (half the users didn't have any extensions for protection in mobile chrome version)
- 3) Hash of Canvas Fingerprinting: Browser uniqueness was 1 in 300, whereas mobile uniqueness was 1 in 115, which is a huge difference. Just by using a desktop one can decrease their Canvas fingerprinting by a huge margin
- 4) Regarding the Do Not Track Header enabled bit calculation, mobile browser have 1 in 2.5 set to False (my mobile version doesn't have any protection ), whereas desktop browser have 1 in 1.67 set to True. (Half more than half have their DNT enabled ! )
- 5) Major bit for identifying an individual comes from the User Agent and HTTP\_ACCEPT Headers in both versions of mobile browser and desktop browser (Chrome both)

## Fingerprintjs:



**Fingerprintjs2**

Get my fingerprint

Your browser fingerprint:  
**63f9280f6b6d4809b24511790166d51e**

Time took to calculate the fingerprint: 113 ms

**Detailed information:**

```
userAgent = Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3
language = en-GB
colorDepth = 24
deviceMemory = 8
hardwareConcurrency = 4
screenResolution = 900,1440
availableScreenResolution = 814,1440
timezoneOffset = 300
timezone = America/New_York
sessionStorage = true
localStorage = true
indexedDb = true
addBehavior = false
openDatabase = true
cpuClass = not available
platform = MacIntel
plugins = Chrome PDF Plugin,Portable Document Format,application/x-google-chrome-pdf,pdf,Chrome PDF Viewer,,ap
canvas = canvas winding:yes,canvas fp:data:image/png;base64,iVBORw0KGgoAAAANSUHEugAAB9AAAAADICAYAAACwGnoBAAAgA
webgl = data:image/png;base64,iVBORw0KGgoAAAANSUHEugAAASwAAACWCAYAAABkw7XSAAAM801EQVR4Xu2dXYgkVxxHT/XMIBJEQU
webglVendorAndRenderer = Intel Inc.-Intel(R) HD Graphics 6000
adBlock = true
hasLiedLanguages = false
hasLiedResolution = false
hasLiedOs = false
hasLiedBrowser = false
touchSupport = 0,false,false
fonts = Andale Mono,Arial,Arial Black,Arial Hebrew,Arial Narrow,Arial Rounded MT Bold,Arial Unicode MS,Comic
audio = 124.04345808873768
```

**FIG5: FINGERPRINTJS FOR CHROME FROM DESKTOP**

Major differences noticed:

- 1) Time taken is larger in a mobile version than the laptop version for Chrome browser.
- 2) The Plugins are different in both cases
- 3) WebGL Vendor and Renderer are perfectly captured that helps in Canvas fingerprinting.

Your browser fingerprint:

**9e360a6ea8421e43b069aa4786ac2199**

Time took to calculate the fingerprint: 279 ms

### Detailed information:

```
userAgent = Mozilla/5.0 (Linux; Android 9; ONEPLUS
language = en-GB
colorDepth = 24
deviceMemory = 4
hardwareConcurrency = 8
screenResolution = 732,412
availableScreenResolution = 732,412
timezoneOffset = 300
timezone = America/New_York
sessionStorage = true
localStorage = true
indexedDb = true
addBehavior = false
openDatabase = true
cpuClass = not available
platform = Linux armv8l
plugins =
canvas = canvas winding:yes,canvas fp:data:image/p
webgl = data:image/png;base64,iVBORw0KGgoAAAANSUHE
webglVendorAndRenderer = Qualcomm~Adreno (TM) 540
adBlock = false
hasLiedLanguages = false
hasLiedResolution = false
hasLiedOs = false
hasLiedBrowser = false
touchSupport = 5,true,true
fonts = Arial,Courier,Courier New,Georgia,Helvetic
audio = 124.08072291687131
```

FIG6: FINGERPRINTJS FOR MOBILE CHROME BROWSER

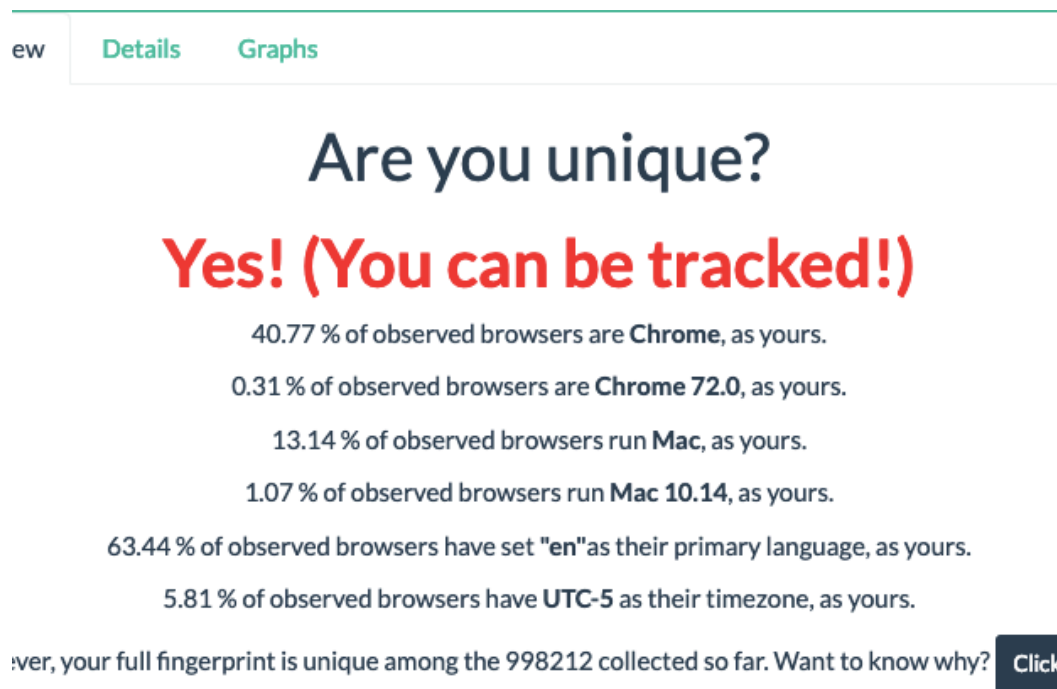


FIG7: AMIUNIQUE RESULTS FROM CHROME ON MAC DESKTOP

Major differences :

- 1) Most of the differences are again in the hardware configurations.
- 2) A clear picture of how Canvas Fingerprinting occurs is given in this case, as compared with panopticlick or fingerprintjs

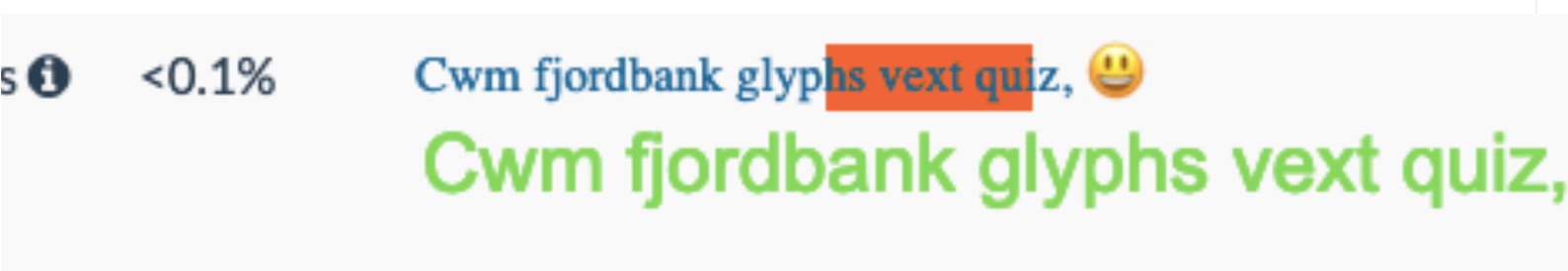


FIG8 : CLEAR EXAMPLE OF CANVAS FINGERPRINTING



Am I Unique?



Overview

Details

Graphs

# Are you unique?

## Yes! (You can be tracked!)

40.77 % of observed browsers are **Chrome**, as yours.

2.19 % of observed browsers are **Chrome 71.0**, as yours.

7.41 % of observed browsers run **Android**, as yours.

0.58 % of observed browsers run **Android Unknown**, as yours.

63.44 % of observed browsers have set "**en**" as their primary language, as yours.

5.81 % of observed browsers have **UTC-5** as their timezone, as yours.

However, your full fingerprint is unique among the 998222 collected so far. Want to know why?

[Click here](#)

FIG9: AMIUNIQUE RESULTS FROM MOBILE CHROME RUNNING ON ANDROID



### 3) Ghostery (mobile and desktop):

#### MOBILE BROWSER:

Site visited	No of Trackers found	No of Trackers Blocked
cnn.com	30	18
alibaba.com	0	0
espn.com	15	8

Table 1 : Mobile Browser overall view of Trackers

Site Visited	Advertising	Site Analytics	Customer Interaction	Social Media	Essential	Audio/ Video Player	Adult Advertising	Comments
Total	1760/1760	638/638	0/284	0/100	0/64	0/60	23/23	0/10
cnn	14/14	4/4	0/2	0	0	0	0	0/1
alibaba	0	0	0	0	0	0	0	0
espn	5/5	3/3	0	0	0	0	0	0/1

Table2:Detailed view of the different trackers Ghostery checks against and each site trackers that are blocked by default

#### DESKTOP PLUGIN:

Site visited	No of Trackers found	No of Trackers Blocked
cnn.com	29	22
alibaba.com	1	1
espn.com	9	8

Table 1 : Desktop Plugin overall view of Trackers

Site Visited	Advertising	Site Analytics	Customer Interaction	Social Media	Essential	Audio/ Video Player	Adult Advertising	Comments
Total	1760/1760	638/638	0/284	0/100	0/64	0/60	23/23	0/10
cnn	11/13	3/3	0/2	0	0/2		0	0/1
alibaba	1/1	0	0	0	0	0	0	0
espn	3/3	2/2	0	1/2	0	0	0	0

Table2:Detailed view of the different trackers Ghostery checks against and each site trackers that are blocked by default in desktop plugin version

### General Takeaways :

- 1) Majority of Tracking is done by Advertisers.
- 2) After Advertising, its for Site Analytics followed by Social Media.
- 3) There isn't much difference in tracking between mobile vs desktop, seems to be the same amount across devices.

### 4) Trackers:

reddit.com	usatoday.com	bankofamerica.com
aaxads.com	1rx.io	agkn.com
aaxdetect.com	254a.com	bac-assets.com
amazon-adsystem.com	2mdn.net	bankofamerica.com
doubleclick.net	33across.com	coremetrics.com
google.com	360yield.com	demdex.net
googletagmanager.com	3lift.com	doubleclick.net
googletagservices.com	abtasty.com	omtrdc.net
redd.it	acuityplatform.com	tiqcdn.com
reddit.com	acxiomapac.com	
redditmedia.com	addthis.com	
redditstatic.com	adform.net	
rlcdn.com	adgrx.com	
	adnxs.com	
	adroll.com	
	ads-twitter.com	
	adsafeprotected.com	
	adsrvr.org	
	adsymptotic.com	
	adtechus.com	
	advertising.com	
	agkn.com	
	amazon-adsystem.com	
	bidswitch.net	
	bing.com	
	bluekai.com	

reddit.com	usatoday.com	bankofamerica.com
	bounceexchange.com	
	brealtime.com	
	bttrack.com	
	casalemedia.com	
	chartbeat.com	
	chartbeat.net	
	clarium.io	
	clickagy.com	
	cloudflare.com	
	cloudfront.net	
	clrstm.com	
	colossusssp.com	
	connexity.net	
	contextweb.com	
	createjs.com	
	creative-serving.com	
	criteo.com	
	criteo.net	
	crwdcntrl.net	
	ctnsnet.com	
	demdex.net	
	digitaloceanspaces.com	
	digitru.st	
	districtm.io	
	dotomi.com	
	doubleclick.net	
	emxdgt.com	
	eqads.com	
	everesttech.net	
	exelator.com	

reddit.com	usatoday.com	bankofamerica.com
	exposebox.com	
	eyeota.net	
	eyereturn.com	
	facebook.com	
	facebook.net	
	fastly.net	
	fastly.net	
	gannett-cdn.com	
	gannett.com	
	gannettdigital.com	
	gcion.com	
	google.com	
	googleadservices.com	
	googleapis.com	
	googlesyndication.com	
	googletagservices.com	
	gssprt.jp	
	gstatic.com	
	iasds01.com	
	ib-ibi.com	
	indexww.com	
	insightexpressai.com	
	ipredictive.com	
	krxd.net	
	liadm.com	
	lijit.com	
	mathtag.com	
	media.net	
	media6degrees.com	
	mfadsrvr.com	

reddit.com	usatoday.com	bankofamerica.com
	ml314.com	
	moatads.com	
	mobileadtrading.com	
	mookie1.com	
	mxptint.net	
	netmng.com	
	newrelic.com	
	npttech.com	
	nr-data.net	
	omnitagjs.com	
	openx.net	
	owneriq.net	
	placed.com	
	polarcdn-pentos.com	
	polarcdn-terrax.com	
	polarcdn.com	
	polyfill.io	
	powerlinks.com	
	pswec.com	
	pubmatic.com	
	quantserve.com	
	reson8.com	
	rfihub.com	
	rkdms.com	
	rlcdn.com	
	rubiconproject.com	
	scorecardresearch.com	
	scroll.com	
	semasio.net	
	serverbid.com	

reddit.com	usatoday.com	bankofamerica.com
	simpli.fi	
	sitescout.com	
	smartadserver.com	
	sonobi.com	
	spotxchange.com	
	stickyadstv.com	
	storygize.net	
	summerhamster.com	
	survata.com	
	t.co	
	taboola.com	
	tapad.com	
	thrtle.com	
	tiqcdn.com	
	turn.com	
	twitter.com	
	urbanairship.com	
	usatoday.com	
	w55c.net	
	yahoo.com	
	youtube.com	

Trackers across sites :

usatoday & reddit	reddit & bankofamerica	usatoday & bankofamerica
amazon-adsystem.com	agkn.com	doubleclick.net
doubleclick.net	demdex.net	
google.com	doubleclick.net	
googletagservices.com	tiqcdn.com	
rlcdn.com		

Connectivity Graph generated :



**CONNECTIVITY GRAPH BETWEEN DIFFERENT SITES**

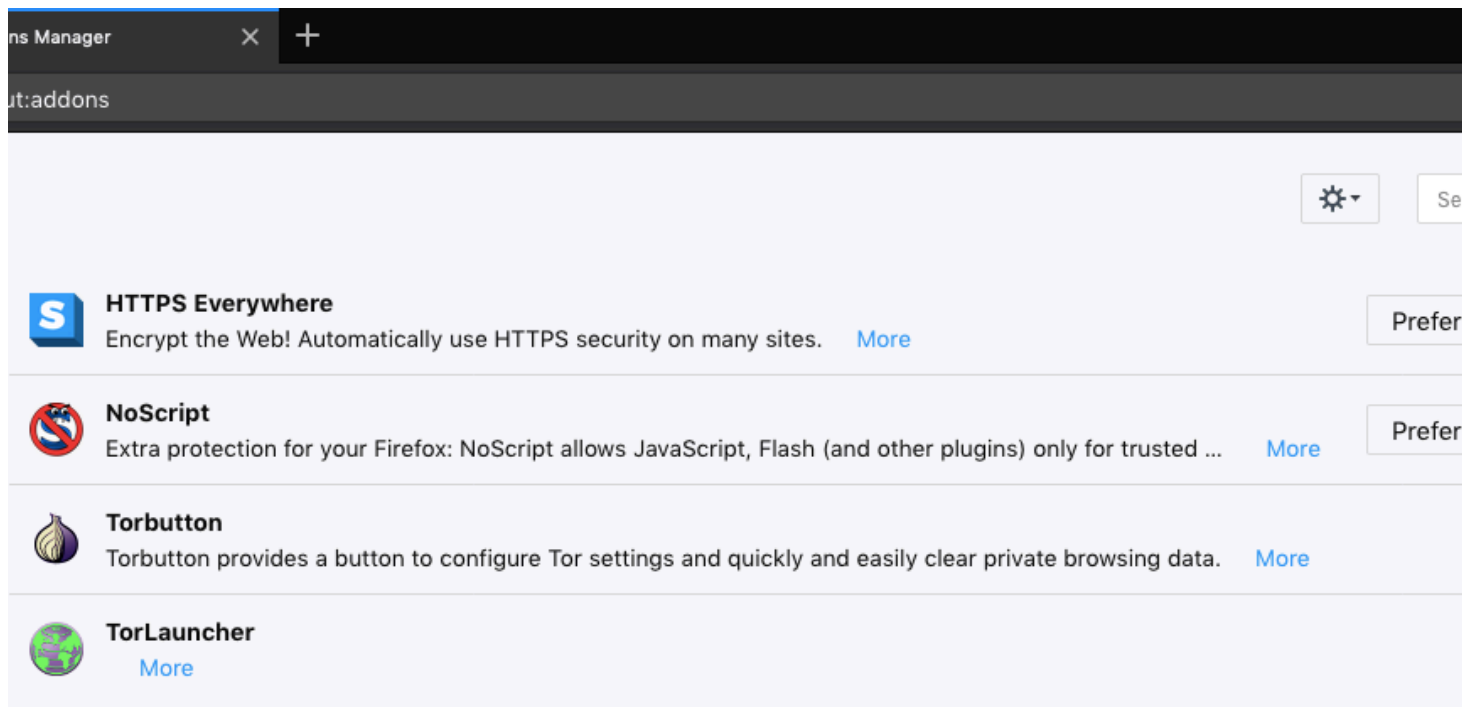


## 5) Tor Browser:

Default Search Engine : DuckDuckGo

List of extensions available by default:

- a. HTTPS Everywhere
- b. NoScript
- c. Torbutton
- d. TorLauncher



## DEFAULT PLUGINS IN TOR

Time to load for various sites and security options :

Site	Standard (in secs)	Safer (in secs)	Safest (in secs)
amazon.com	3.798	5.428	2.907
bbc.com	10.215	3.911	7.044
espn.com	5.529	9.804	2.517

6) Hidden Service that was attempted to hit:

<http://3g2upl4pq6kufc4m.onion/> - DuckDuckGo Search Engine

Commands executed to get the data dump and the unique IP addresses:

```
tcpdump -i en0 -s 0 -B 524288 -w ~/Desktop/testsDumps/  
ddgDataCapture.pcap
```

```
tshark -r ddgDataCapture.pcap -T fields -e ip.src -e ip.dst | tr "\t"  
"\n" | sort | uniq
```

All the unique addresses found :

	Nickname (Tor Relays)	Country associated	Platform
10.154.27.248			
216.58.217.161			
224.0.0.251			
51.38.112.240	ServbrStuttgart	Germany	Tor 0.3.4.9 on Linux
52.114.32.7			

Technically, all the .onion websites will never leave the Tor Network and all the IP addresses should be Tor Relays. But from the list, the name mapping for only one Relay Node could be found, as a source I can only see my guard node, which is captured by Wireshark.

7) List of Tor Relays : (Data as extracted on 14 Feb 2019 17:10 )

a. Top 5 countries hosting Tor Relays

Country Code	Country Name	Count of nodes hosted ( x/6573)
DE	Germany	1340
US	United States	1043
FR	France	874
NL	The Netherlands	441
CA	Canada	268

b. Top 5 bandwidth-contributing relays:

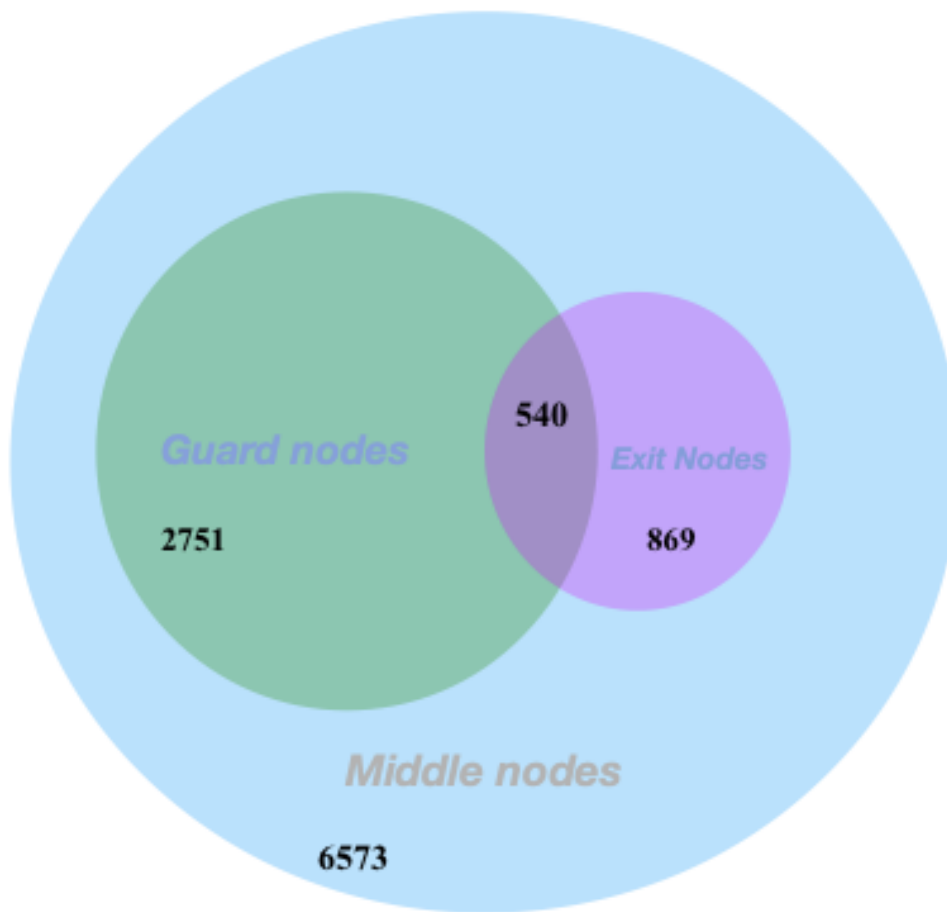
Router Name	Country Code	Consensus Bandwidth (Kb/sec)
IPredator	LR	368000
PrivacyRepublic0001	FR	157000
ExitNinja	DE	153000
PIAnycexit	US	141000
hyacinthinus	NL	131000

c. Bandwidth distribution of each node :

Here middle nodes are considered to be all the nodes (universal)

Type of Node	No of Nodes	Cumulative Bandwidth (Kb/s)
Middle Nodes ( universal )	6573	1,95,40,203
Guard Nodes ( Flag - Guard == 1 )	2751	1,68,80,742
Exit Nodes ( Flag - Exit == 1 )	869	58,93,892
Guard & Exit Nodes ( Flag - Guard == 1 && Flag - Exit == 1 )	540	53,55,285

Venn diagram for the node distribution:



VENN DIAGRAM FOR THE NODE DISTRIBUTION

8)

Below notations are followed for this question :

M : Malicious relays

NM : Non Malicious relays

'c' : Probability of Tor relay being malicious.

Table of different permutations of the Tor circuit:

S. No	Guard	Middle	Exit	Source Anonymity	Destination Anonymity
1	M	NM	NM	Known	Unknown
2	NM	M	NM	Unknown	Unknown
3	NM	NM	M	Unknown	Known
4	M	M	NM	Known	Unknown
5	M	NM	M	Known	Known
6	NM	M	M	Unknown	Known
7	M	M	M	Known	Known
8	NM	NM	NM	Unknown	Unknown

Probability of compromising a circuit in the original condition = Case where exit & guard are both malicious =  $c^2$  (without Selective DoS)

When the circuit is compromised, we have two cases where it could be compromised and still the circuit is up and stable.

Case 1 : when the exit and guard are both under control of the malicious middle node (Case 7)  
=  $c^2$

Case 2 : when all nodes are non malicious  
=  $(1 - c)^3$

Compromised probability =  $c^2$

Total probability. =  $\frac{c^2}{c^2 + (1 - c)^3}$

Comparing with the original probability :

$$\frac{c^2}{c^2 + (1 - c)^3} > c^2$$