Kevin Gallagher

PhD Candidate

New York University
Tandon School of Engineering

My Recent Work

Peeling the Onion's User Experience Layer: Examining Naturalistic Use of the Tor Browser

Kevin Gallagher

New York University

Sameer Patil

Indiana University Bloomington

Brendan Dolan-Gavitt

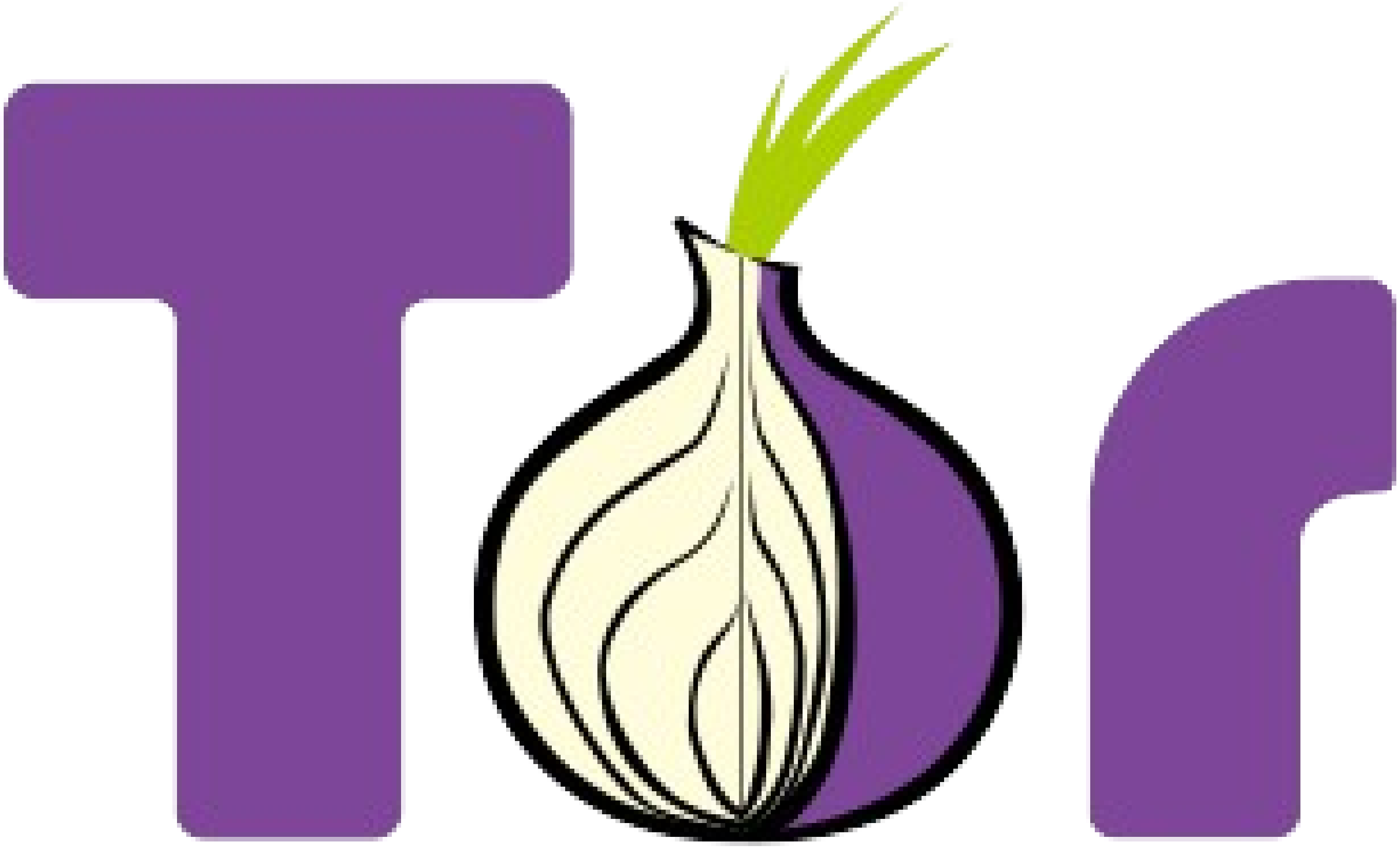
New York University

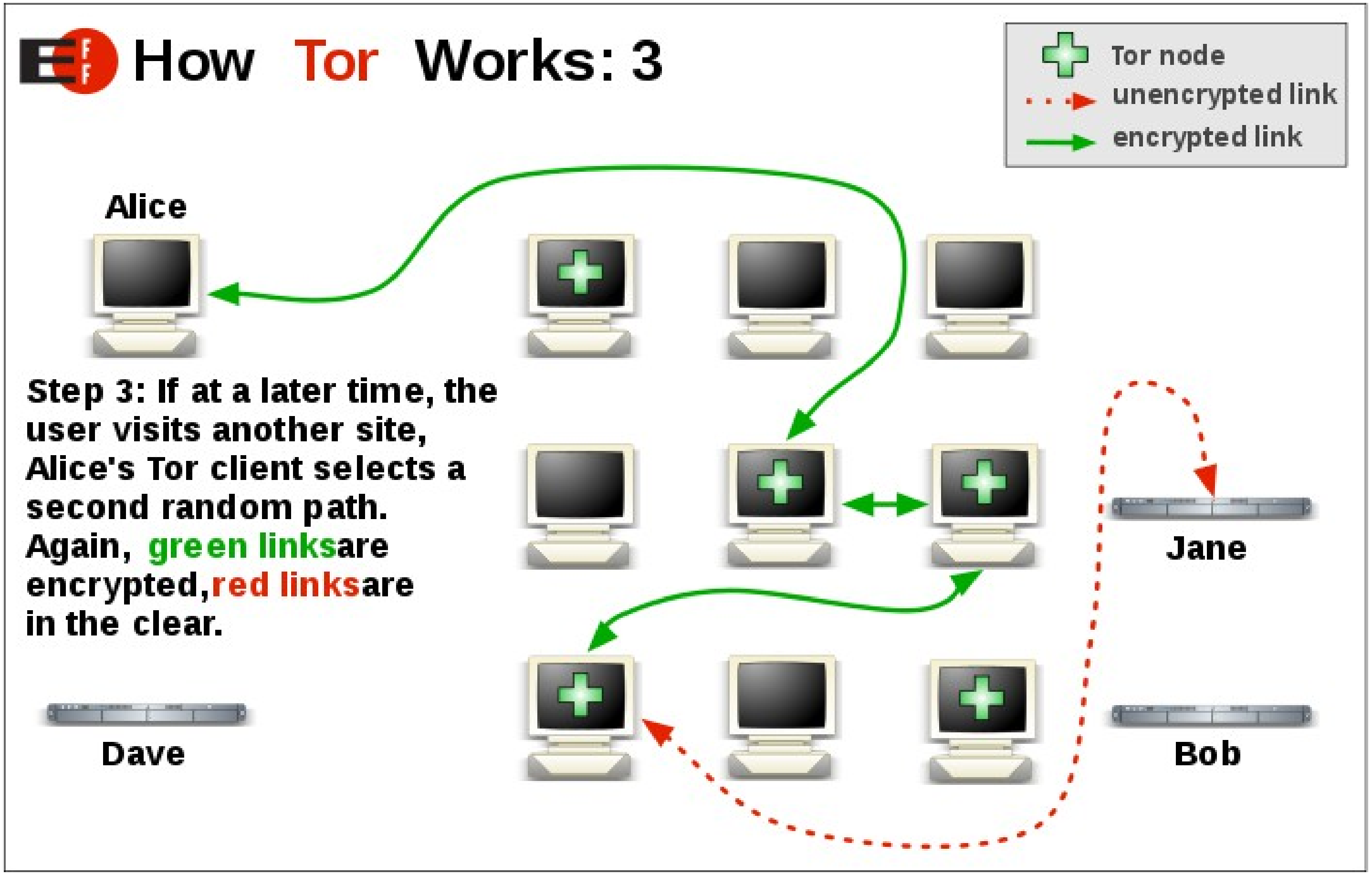
Damon McCoy

New York University

Nasir Memon

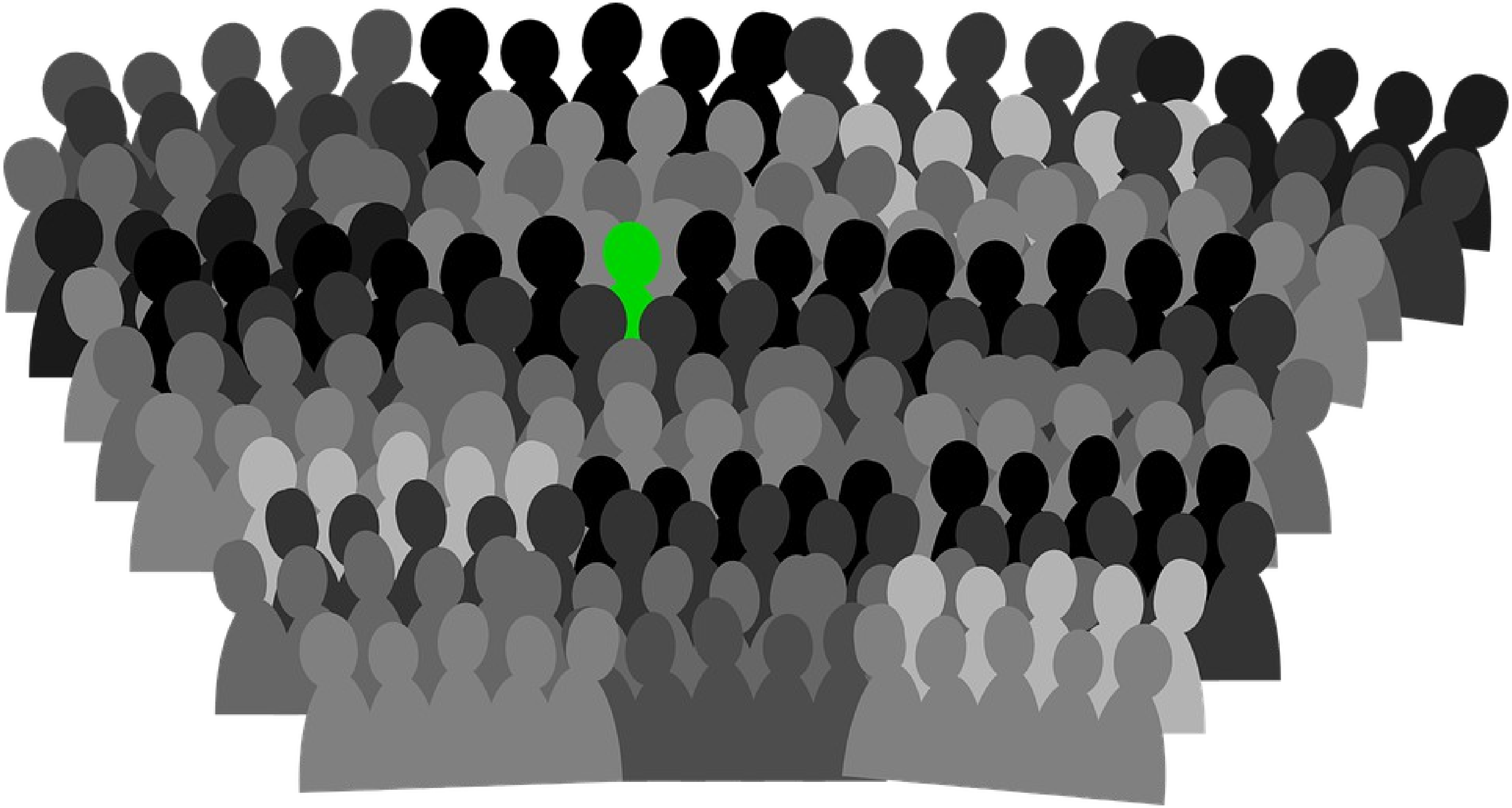
New York University

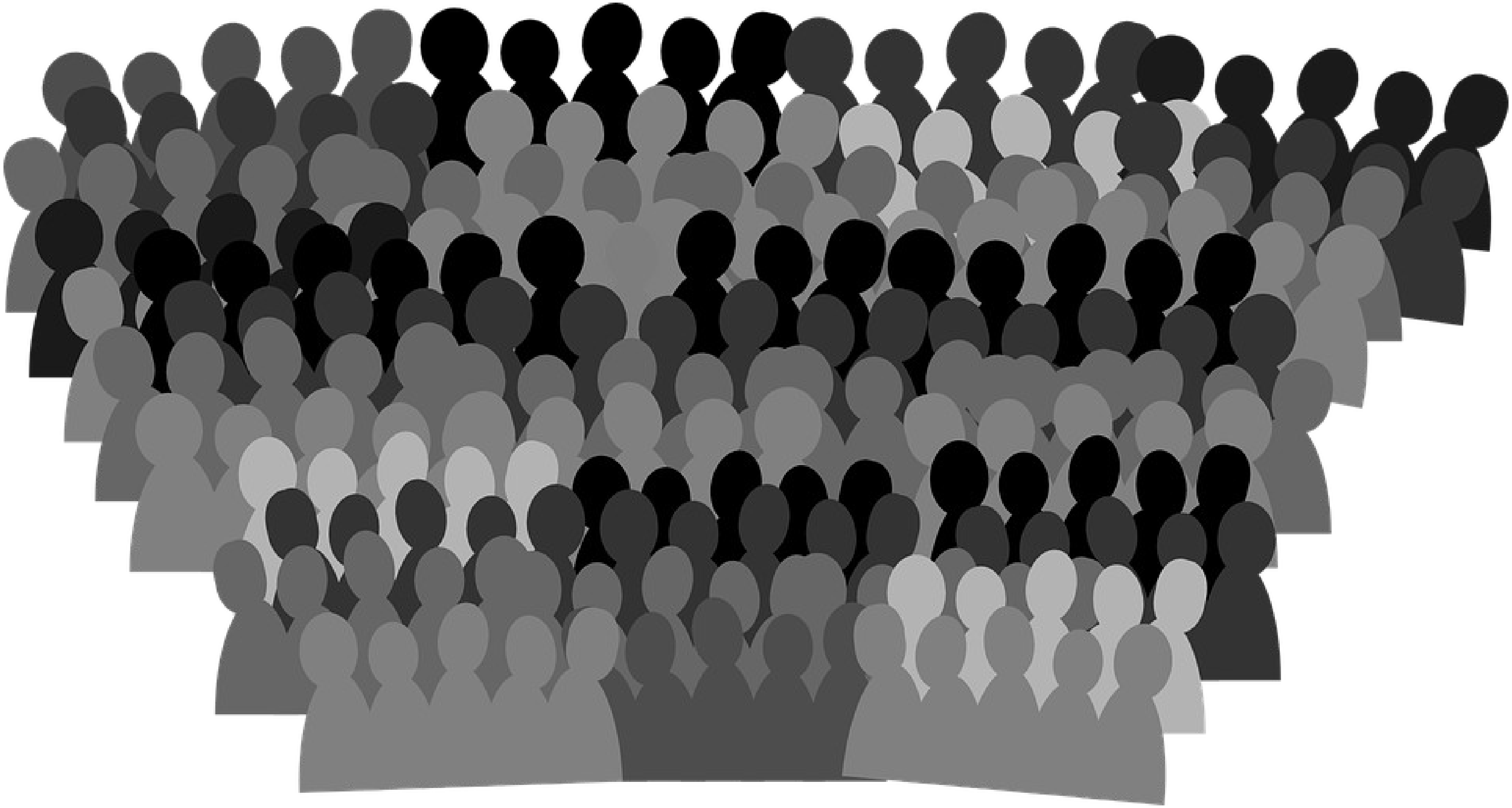


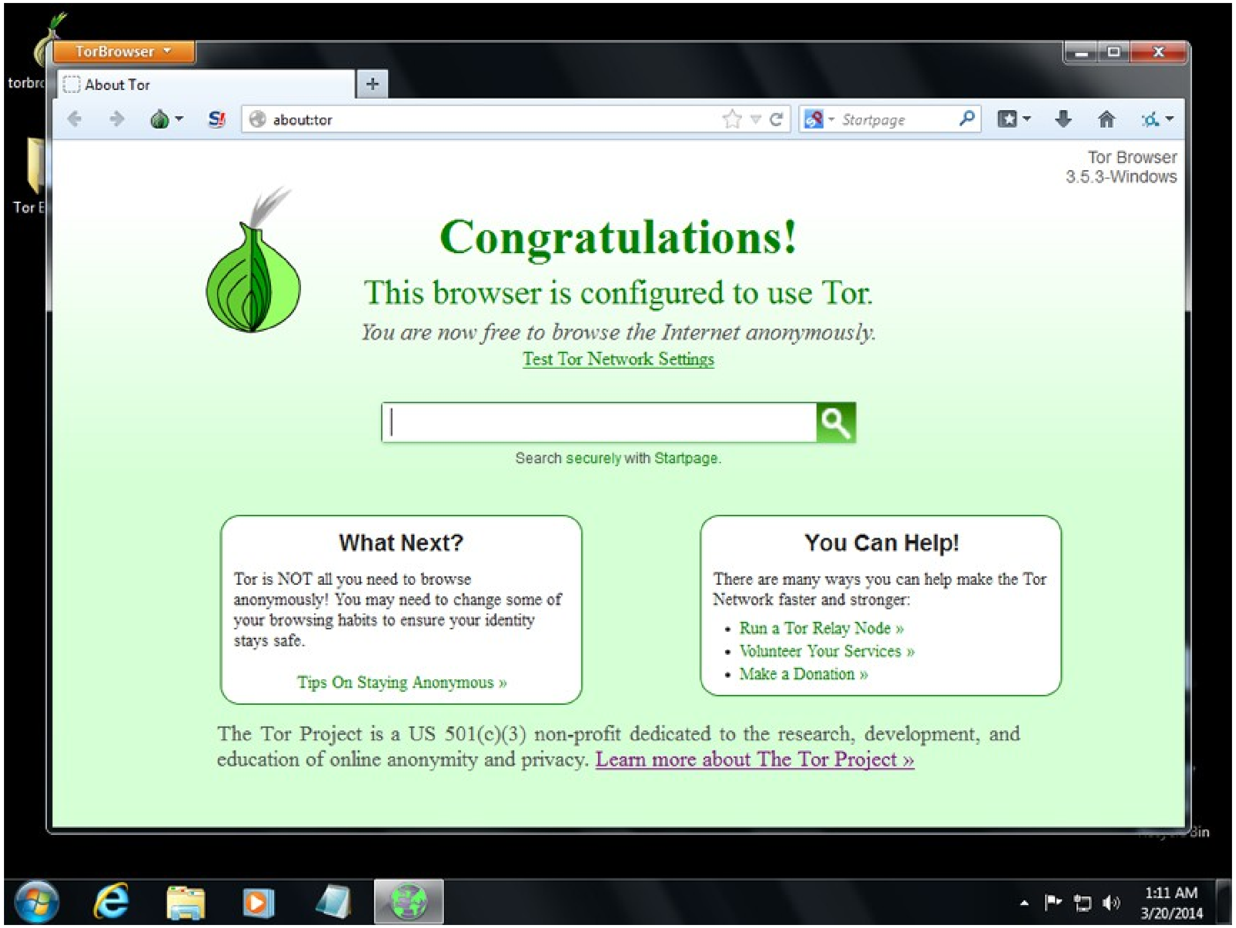


How Tor Works: 3

Step 3: If at a later time, the user visits another site, Alice's Tor client selects a second random path. Again, green linksare encrypted,red linksare in the clear.







Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Startpage.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

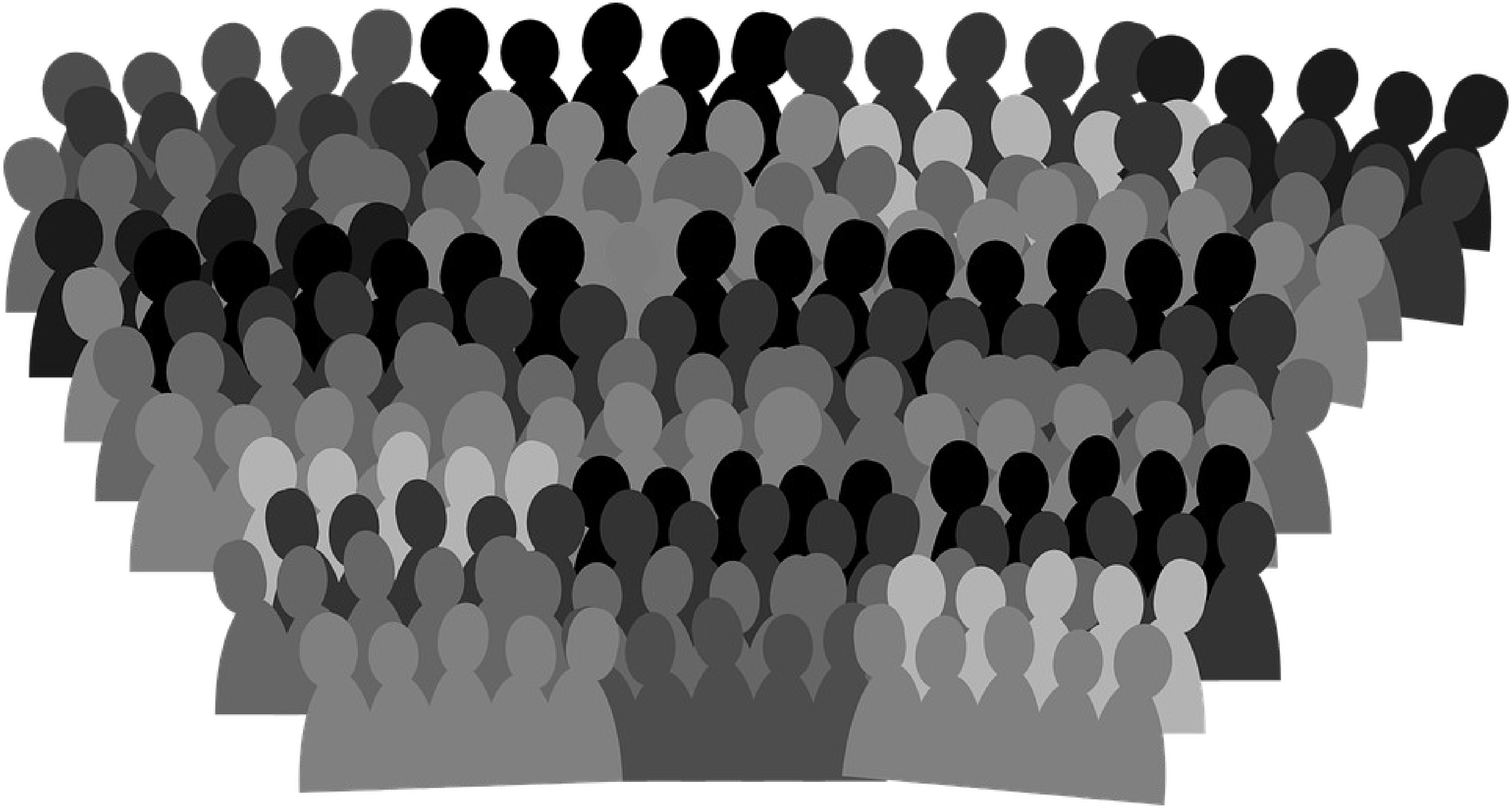
You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

How do users experience everyday naturalistic Web browsing when using the Tor Browser?



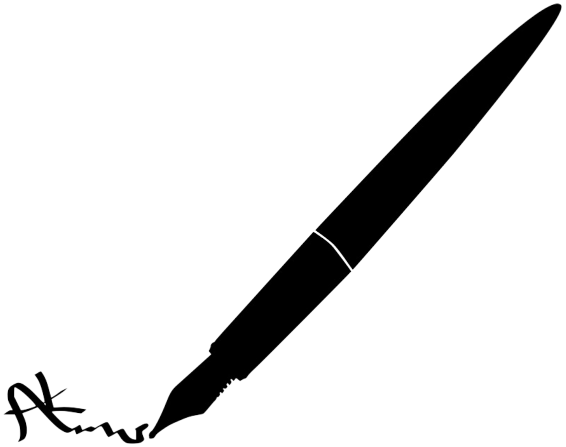
Naturalistic Tor Browser Use

Privacy for Participants

Granular Data

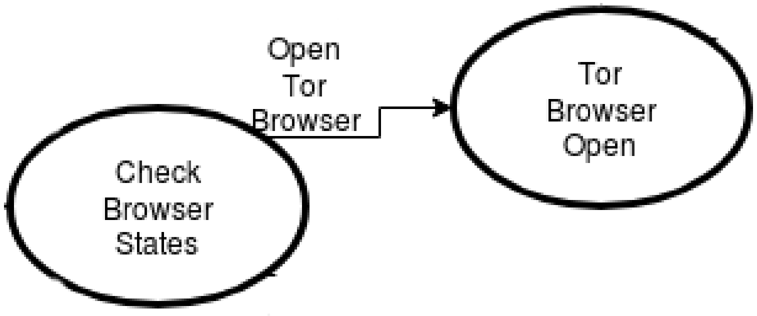
Questionnaires

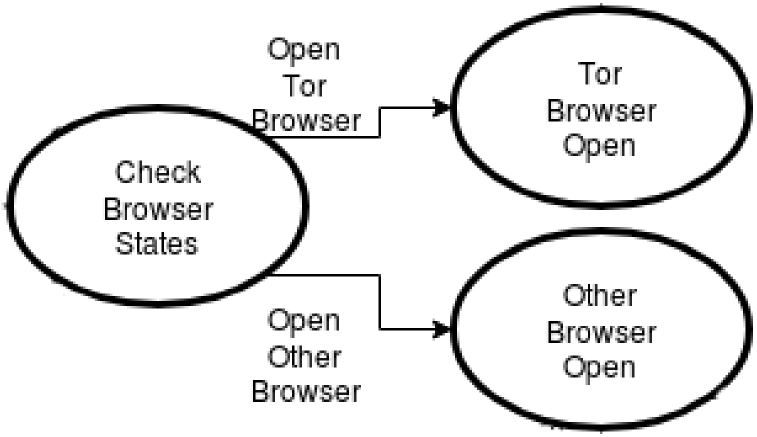
Interview

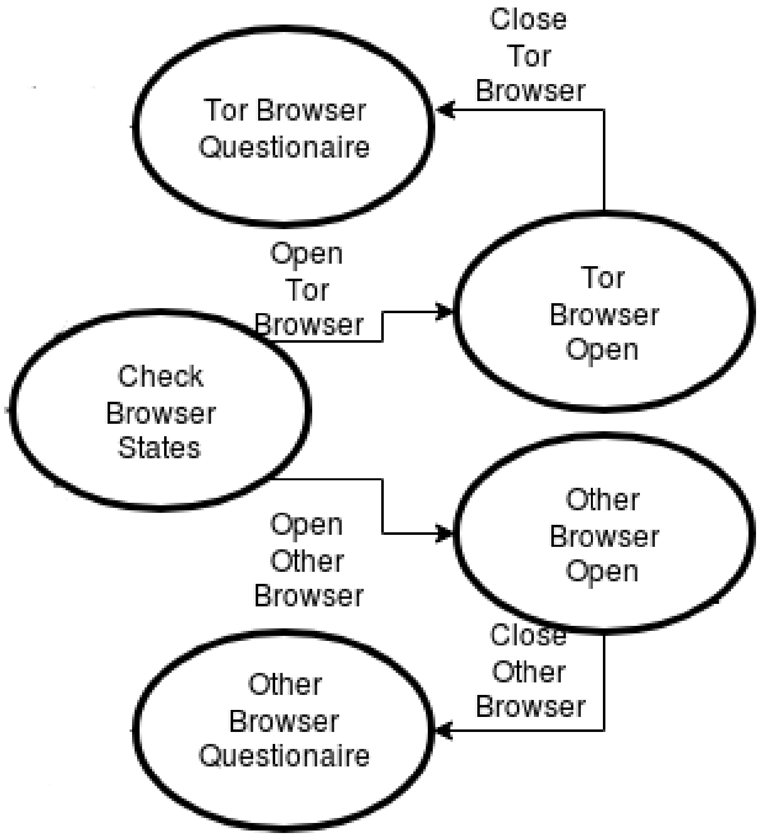


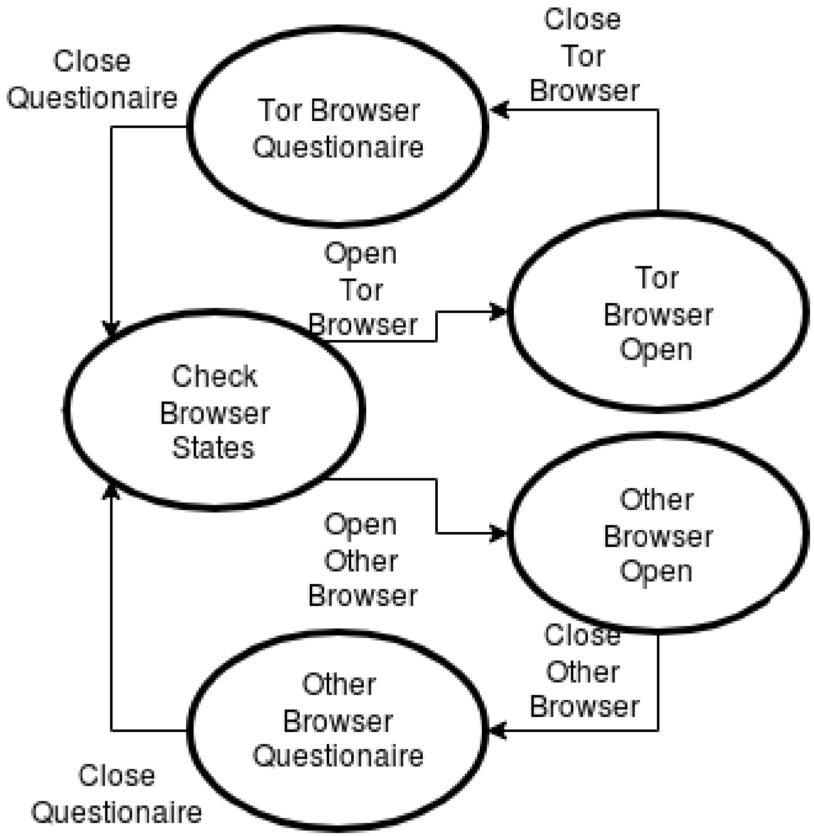
Write-up

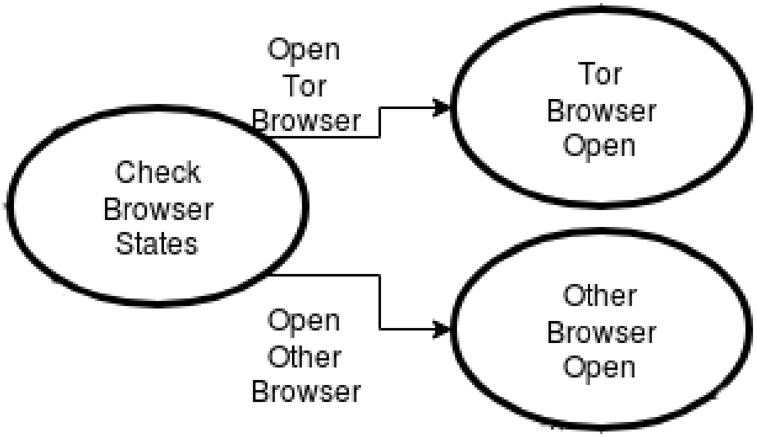
Check Browser States

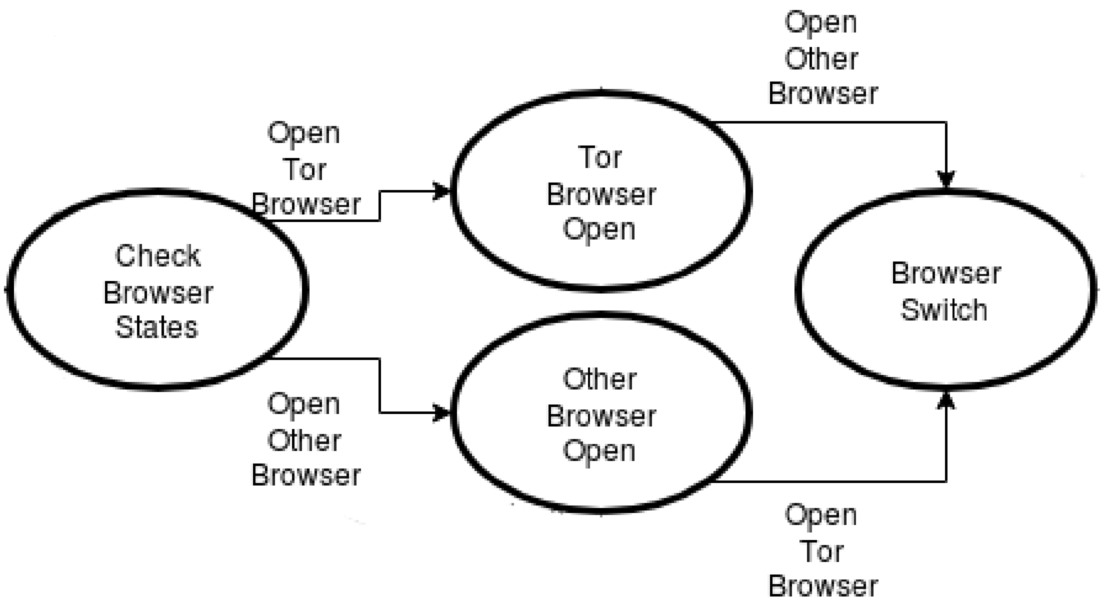

Open
Tor
Browser
Check
Browser
States
Tor
Browser
Open

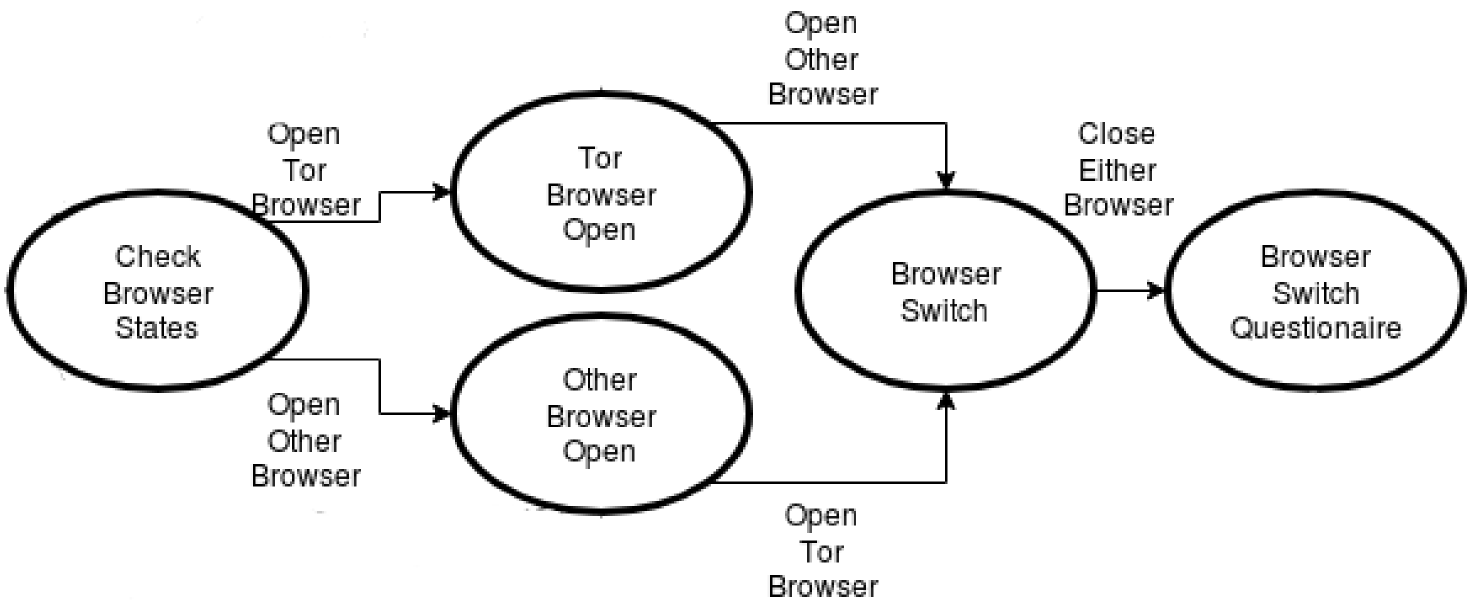

Open
Tor
Browser
Tor
Browser
Open
Check
Browser
States
Other
Browser
Open
Open
Other
Browser

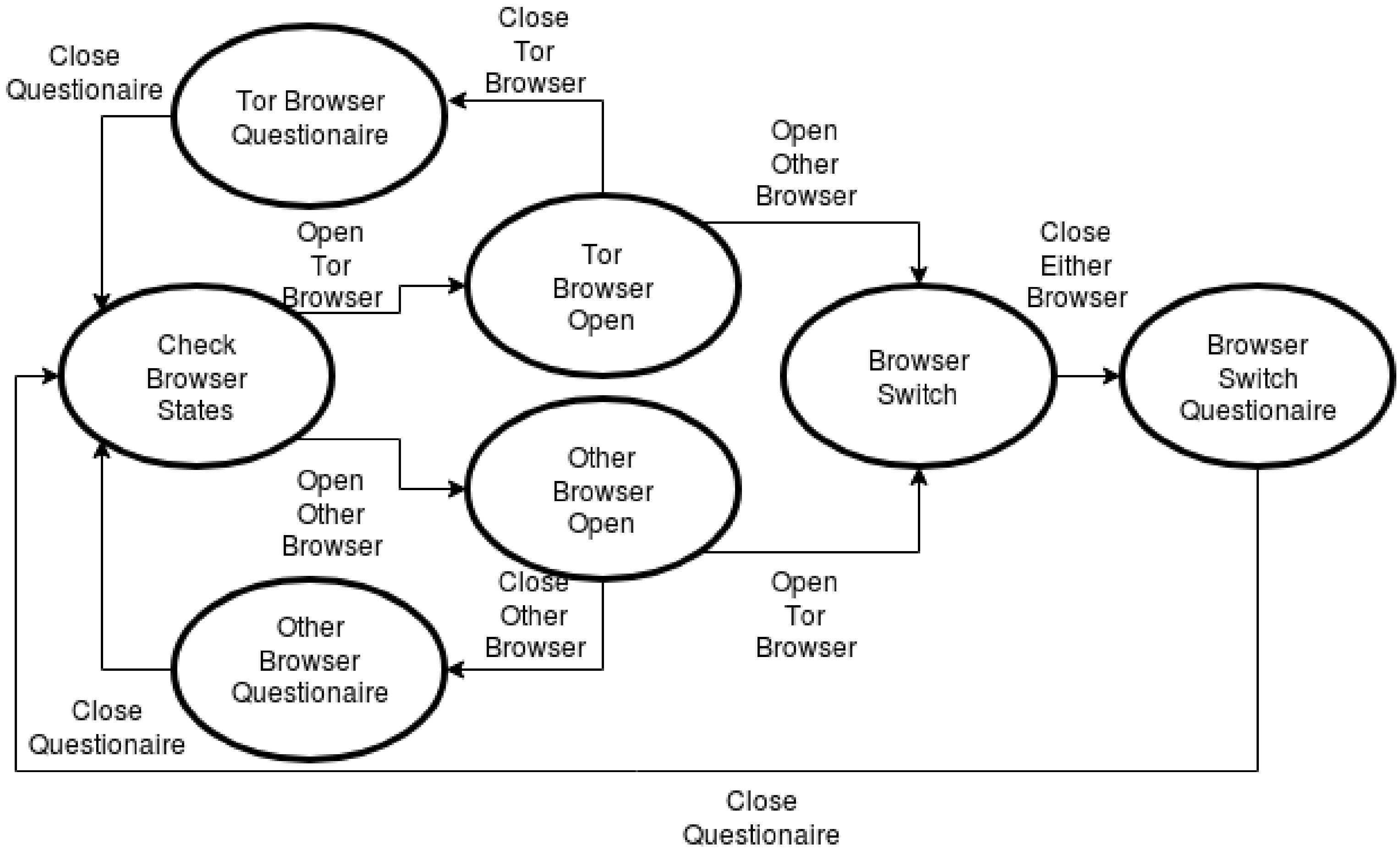

Close Tor Browser
Tor Browser Questionaire
Open Tor Browser
Tor Browser Open
Check Browser States
Other Browser Open
Open Other Browser
Close Other Browser
Other Browser Questionaire

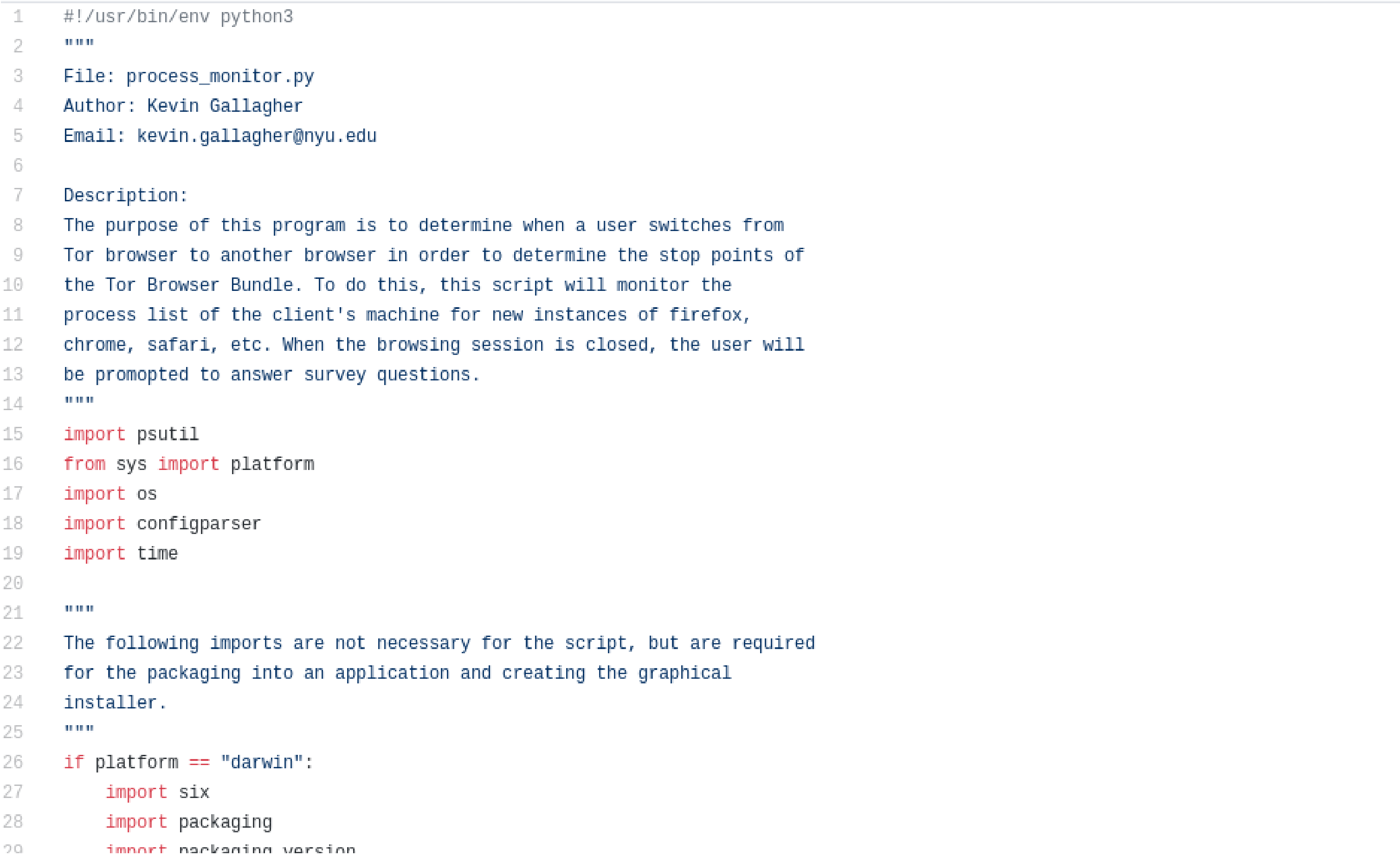

Close
Questionaire
Tor Browser
Questionaire
Close
Tor
Browser
Open
Tor
Browser
Tor
Browser
Open
Check
Browser
States
Other
Browser
Open
Open
Other
Browser
Close
Other
Browser
Other
Browser
Questionaire
Close
Questionaire


Open
Tor
Browser
Check
Browser
States
Tor
Browser
Open
Open
Other
Browser
Other
Browser
Open


Open
Other
Browser
Open
Tor
Browser
Tor
Browser
Open
Check
Browser
States
Browser
Switch
Other
Browser
Open
Open
Other
Browser
Open
Tor
Browser


Open Other Browser
Open Tor Browser
Close Either Browser
Check Browser States
Tor Browser Open
Browser Switch
Browser Switch Questionaire
Other Browser Open
Open Other Browser
Open Tor Browser


Close
Questionaire
Tor Browser
Questionaire
Close
Tor
Browser
Open
Other
Browser
Open
Tor
Browser
Tor
Browser
Open
Close
Either
Browser
Check
Browser
States
Browser
Switch
Browser
Switch
Questionaire
Other
Browser
Open
Open
Other
Browser
Close
Other
Browser
Open
Tor
Browser
Other
Browser
Questionaire
Close
Questionaire
Close
Questionaire



```python
#!/usr/bin/env python3
"""
File: process_monitor.py
Author: Kevin Gallagher
Email: kevin.gallagher@nyu.edu

Description:
The purpose of this program is to determine when a user switches from
Tor browser to another browser in order to determine the stop points of
the Tor Browser Bundle. To do this, this script will monitor the
process list of the client's machine for new instances of firefox,
chrome, safari, etc. When the browsing session is closed, the user will
be promopted to answer survey questions.
"""
import psutil
from sys import platform
import os
import configparser
import time

"""
The following imports are not necessary for the script, but are required
for the packaging into an application and creating the graphical
installer.
"""
if platform == "darwin":
    import six
    import packaging
    import packaging.version
```

Code available at https://github.com/kcg295/TorUsabilityBrowserSensor/

19 participants

20 years old on average

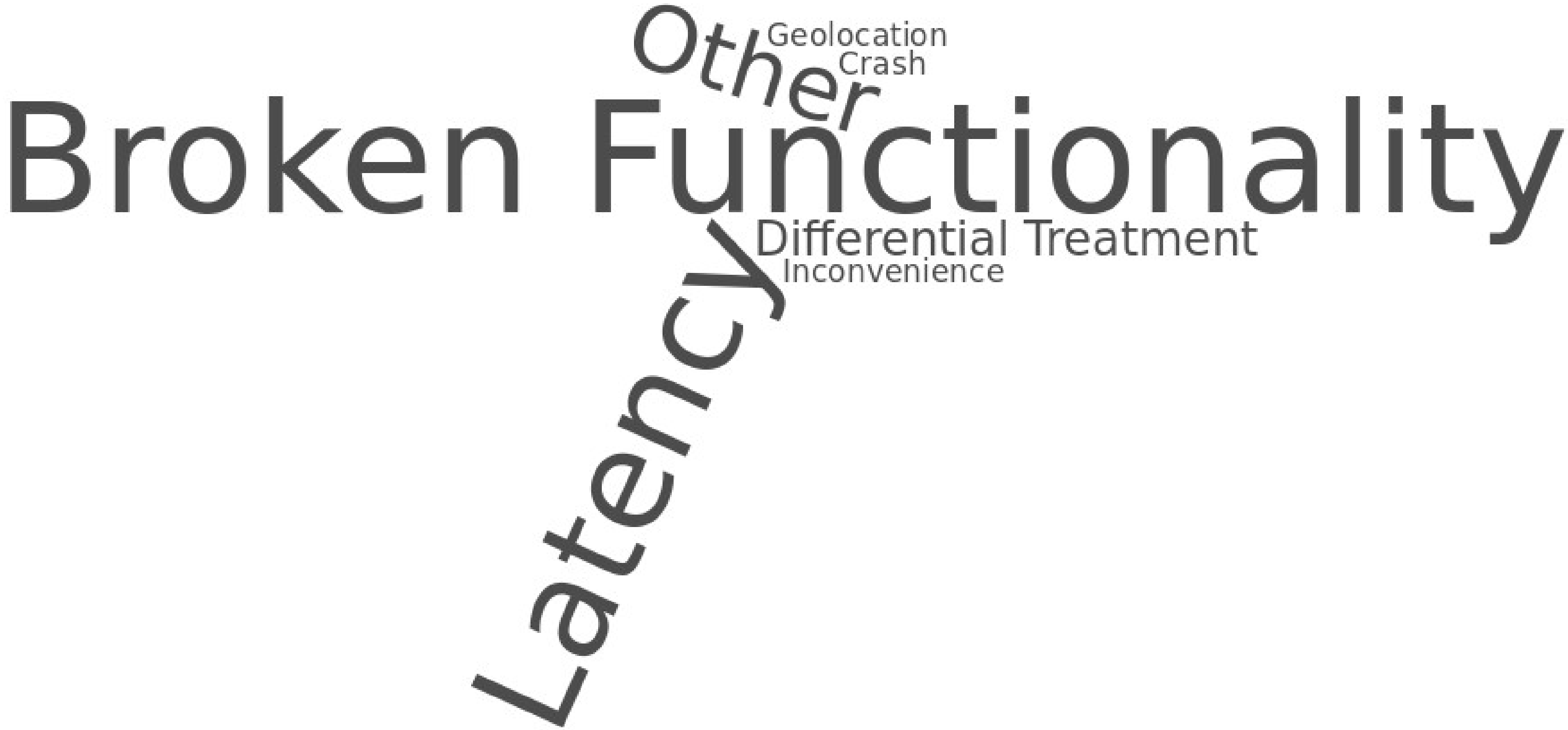
3 used Tor before

121 questionnaires

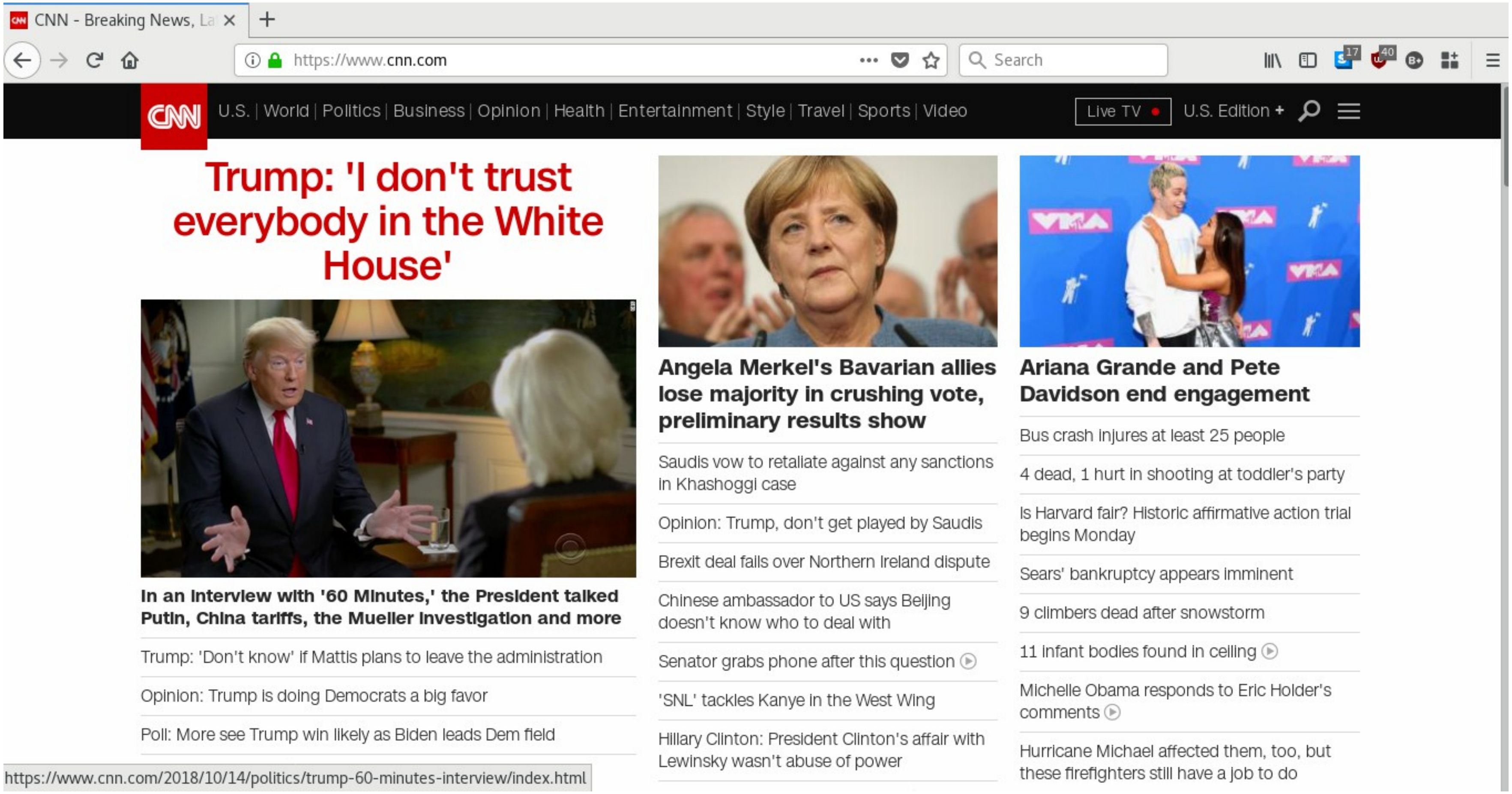
11 interviews

19 write-ups

Findings


Other
Geolocation
Crash
Broken Functionality
Differential Treatment
Inconvenience
Latency

The Bad


CNN - Breaking News, La
https://www.cnn.com
Search
CNN
U.S. | World | Politics | Business | Opinion | Health | Entertainment | Style | Travel | Sports | Video
Live TV
U.S. Edition +

Trump: 'I don't trust everybody in the White House'

In an interview with '60 Minutes,' the President talked Putin, China tariffs, the Mueller investigation and more

Trump: 'Don't know' if Mattis plans to leave the administration

Opinion: Trump is doing Democrats a big favor

Poll: More see Trump win likely as Biden leads Dem field

Angela Merkel's Bavarian allies lose majority in crushing vote, preliminary results show

Saudis vow to retaliate against any sanctions in Khashoggi case

Opinion: Trump, don't get played by Saudis

Brexit deal fails over Northern Ireland dispute

Chinese ambassador to US says Beijing doesn't know who to deal with

Senator grabs phone after this question

'SNL' tackles Kanye in the West Wing

Hillary Clinton: President Clinton's affair with Lewinsky wasn't abuse of power

Ariana Grande and Pete Davidson end engagement

Bus crash injures at least 25 people

4 dead, 1 hurt in shooting at toddler's party

Is Harvard fair? Historic affirmative action trial begins Monday

Sears' bankruptcy appears imminent

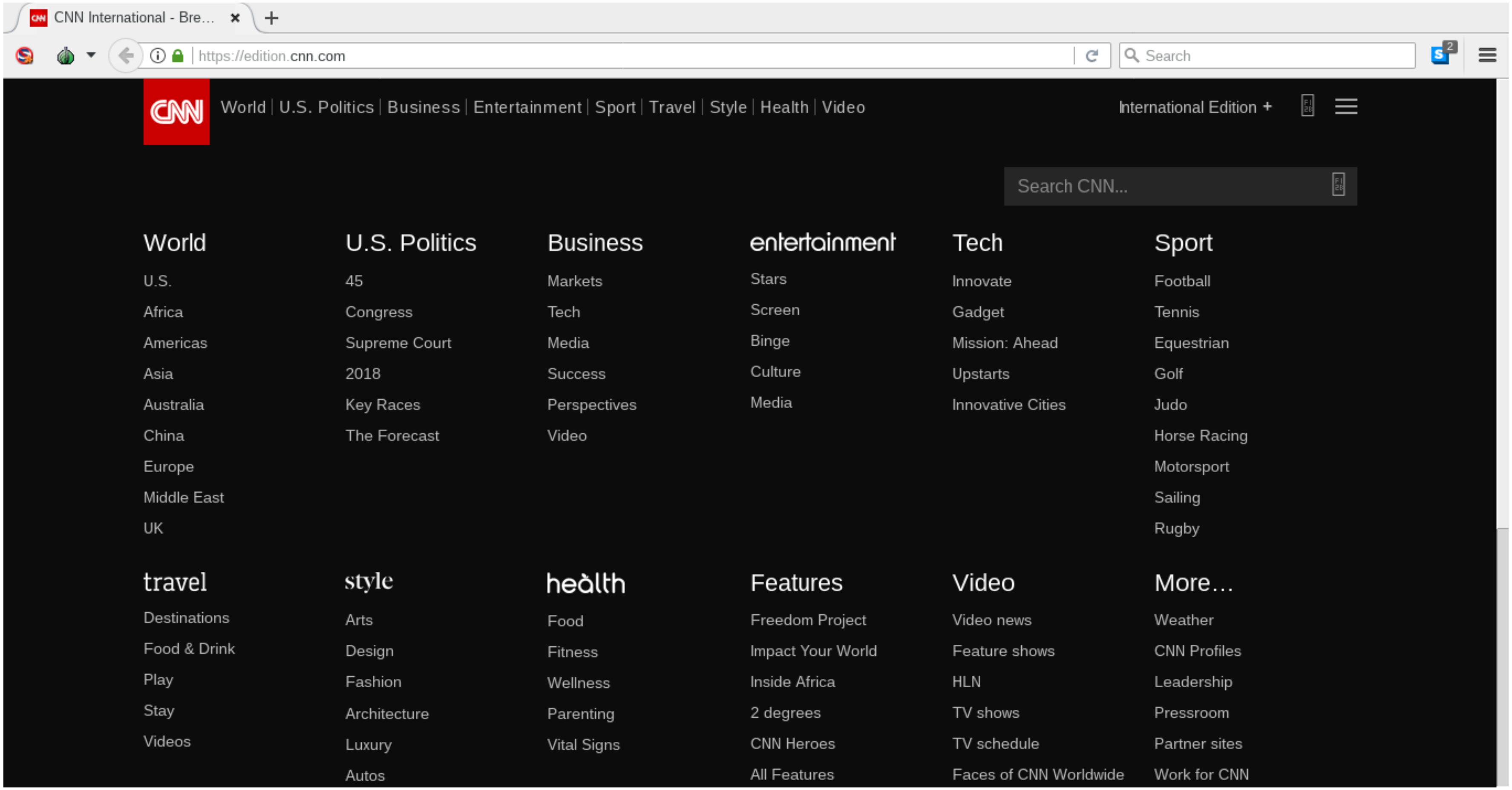
9 climbers dead after snowstorm

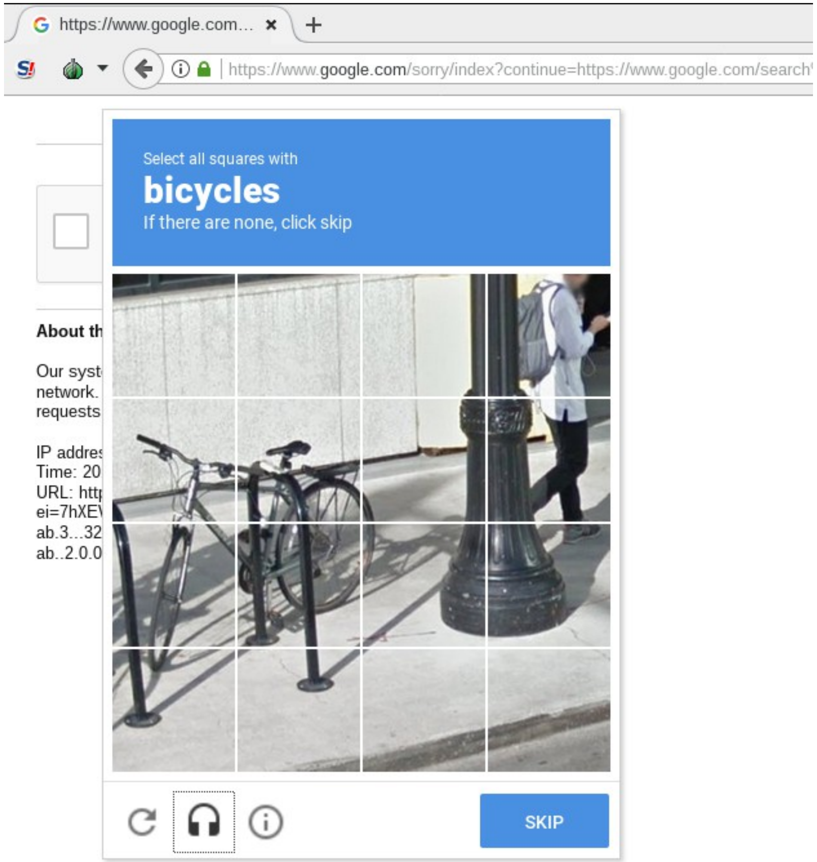
11 infant bodies found in ceiling

Michelle Obama responds to Eric Holder's comments

Hurricane Michael affected them, too, but these firefighters still have a job to do

https://www.cnn.com/2018/10/14/politics/trump-60-minutes-interview/index.html


CNN International - Bre…
https://edition.cnn.com
Search
CNN
World | U.S. Politics | Business | Entertainment | Sport | Travel | Style | Health | Video
International Edition +
Search CNN...
World
U.S.
Africa
Americas
Asia
Australia
China
Europe
Middle East
UK
U.S. Politics
45
Congress
Supreme Court
2018
Key Races
The Forecast
Business
Markets
Tech
Media
Success
Perspectives
Video
entertainment
Stars
Screen
Binge
Culture
Media
Tech
Innovate
Gadget
Mission: Ahead
Upstarts
Innovative Cities
Sport
Football
Tennis
Equestrian
Golf
Judo
Horse Racing
Motorsport
Sailing
Rugby
travel
Destinations
Food & Drink
Play
Stay
Videos
style
Arts
Design
Fashion
Architecture
Luxury
Autos
health
Food
Fitness
Wellness
Parenting
Vital Signs
Features
Freedom Project
Impact Your World
Inside Africa
2 degrees
CNN Heroes
All Features
Video
Video news
Feature shows
HLN
TV shows
TV schedule
Faces of CNN Worldwide
More…
Weather
CNN Profiles
Leadership
Pressroom
Partner sites
Work for CNN



https://www.google.com/sorry/index?continue=https://www.google.com/search'

Select all squares with

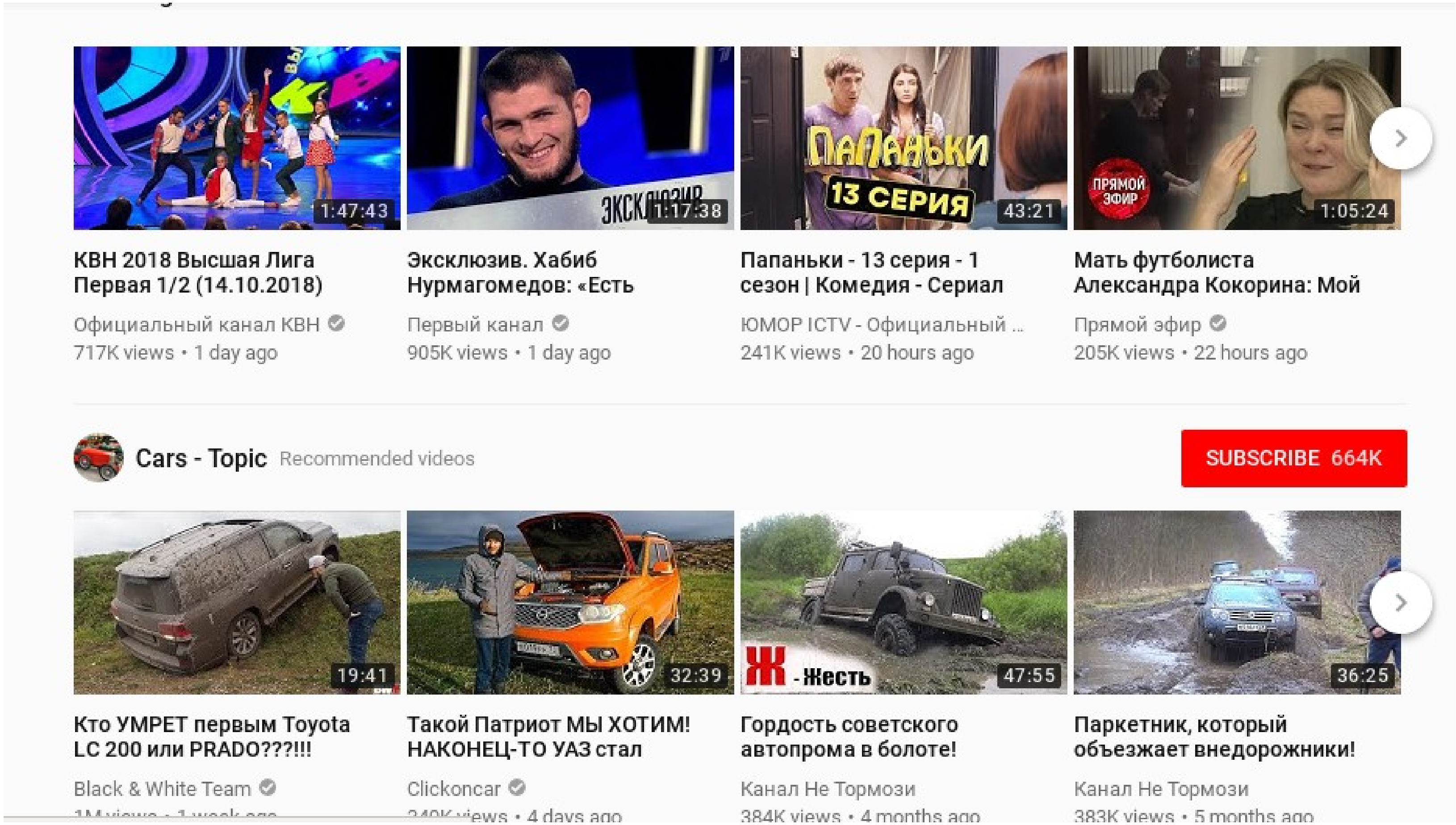
bicycles

If there are none, click skip

About th

Our syst
network.
requests

IP addres
Time: 20
URL: http
ei=7hXE\
ab.3...32
ab..2.0.0



КВН 2018 Высшая Лига Первая 1/2 (14.10.2018)
Официальный канал КВН
717K views • 1 day ago

Эксклюзив. Хабиб Нурмагомедов: «Есть
Первый канал
905K views • 1 day ago

Папаньки - 13 серия - 1 сезон | Комедия - Сериал
ЮМОР ICTV - Официальный ...
241K views • 20 hours ago

Мать футболиста Александра Кокорина: Мой
Прямой эфир
205K views • 22 hours ago

Cars - Topic Recommended videos

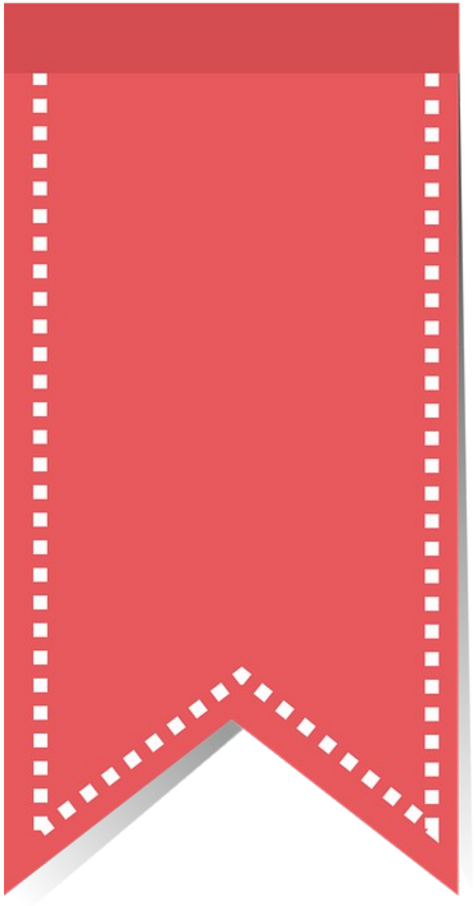
SUBSCRIBE 664K

Кто УМРЕТ первым Toyota LC 200 или PRADO???!!!
Black & White Team
1M views • 1 week ago

Такой Патриот МЫ ХОТИМ! НАКОНЕЦ-ТО УАЗ стал
Clickoncar
240K views • 4 days ago

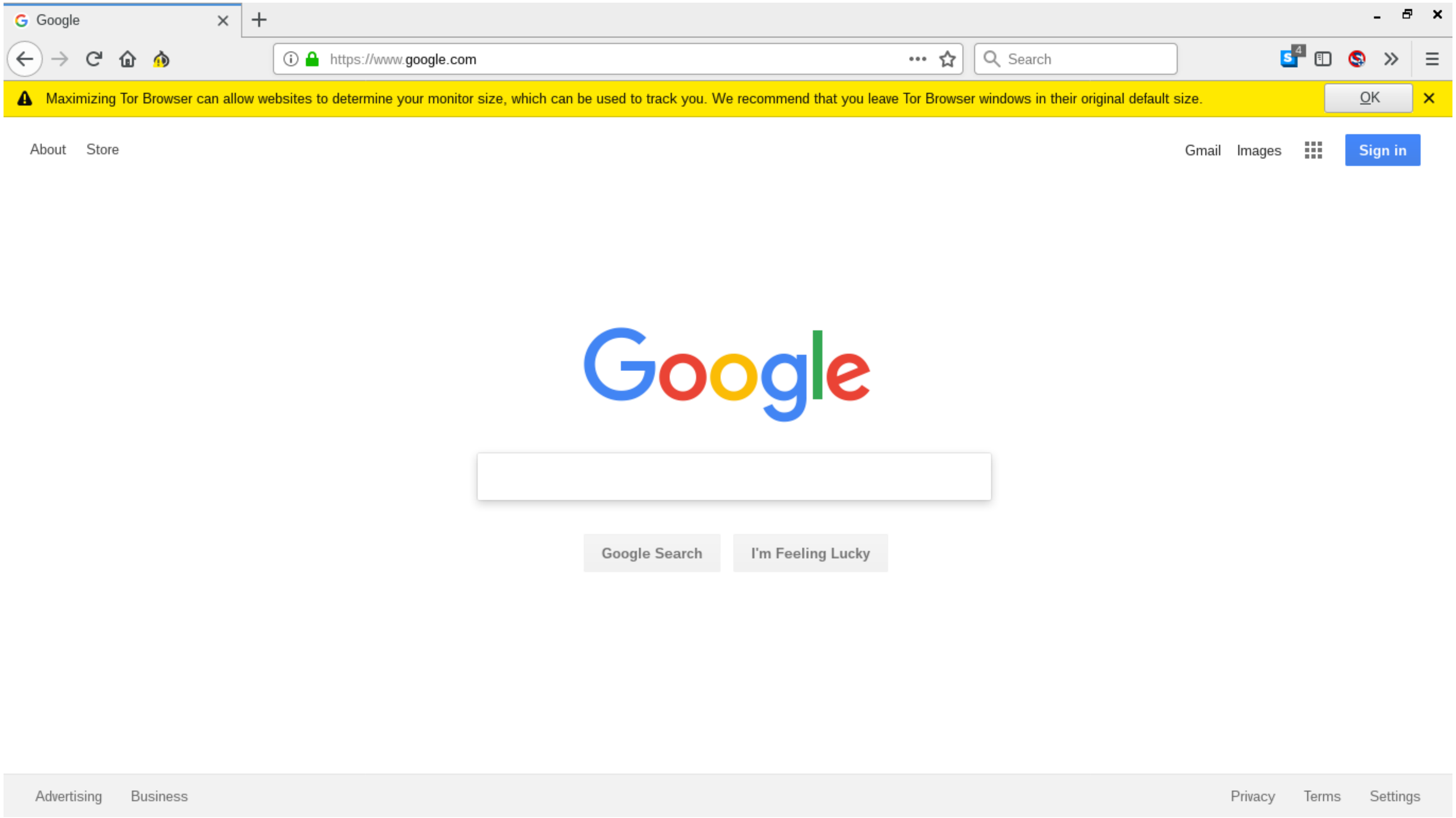
Гордость советского автопрома в болоте!
Канал Не Тормози
384K views • 4 months ago

Паркетник, который объезжает внедорожники!
Канал Не Тормози
383K views • 5 months ago

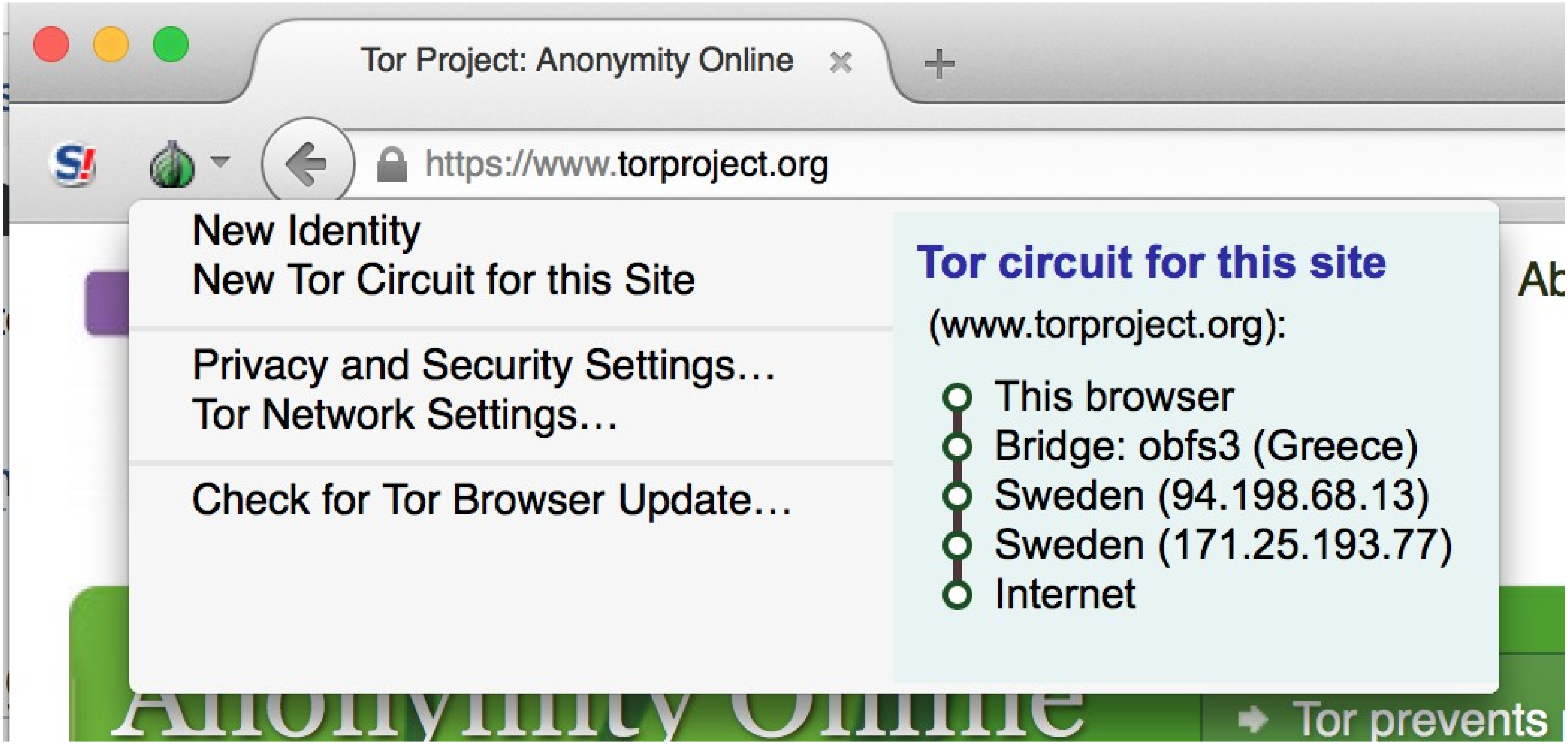


86120834
PASSWORD
08342056

The Good



Maximizing Tor Browser can allow websites to determine your monitor size, which can be used to track you. We recommend that you leave Tor Browser windows in their original default size.



Tor Project: Anonymity Online
https://www.torproject.org
New Identity
New Tor Circuit for this Site
Privacy and Security Settings…
Tor Network Settings…
Check for Tor Browser Update…
Ab
Anonymity Online
Tor prevents

Tor circuit for this site

(www.torproject.org):

- This browser
- Bridge: obfs3 (Greece)
- Sweden (94.198.68.13)
- Sweden (171.25.193.77)
- Internet

Implications

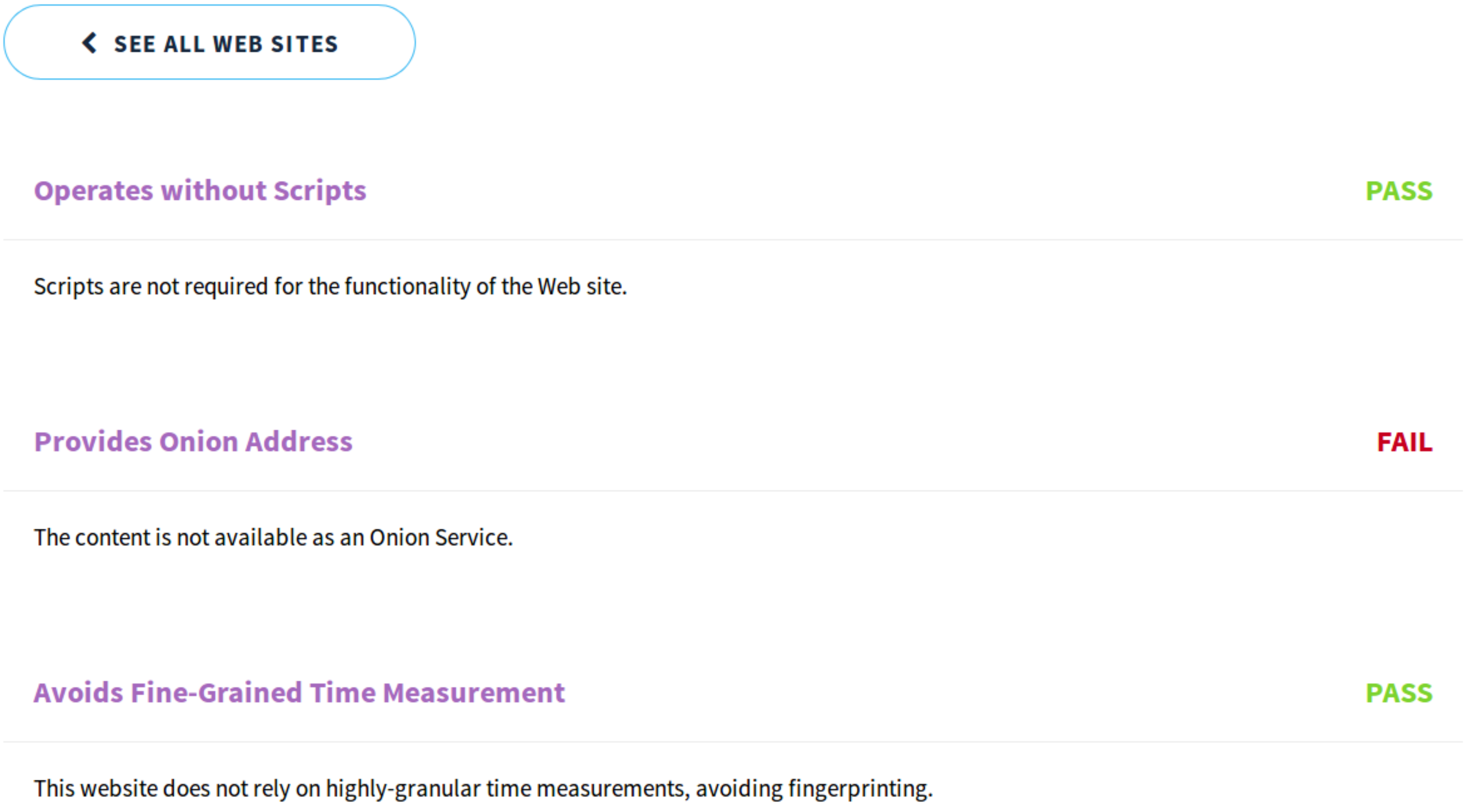
ISP

Coffee Shop Hacker

Select **Your** Adversary

Government Agency

Snooping Family



Operates without Scripts PASS

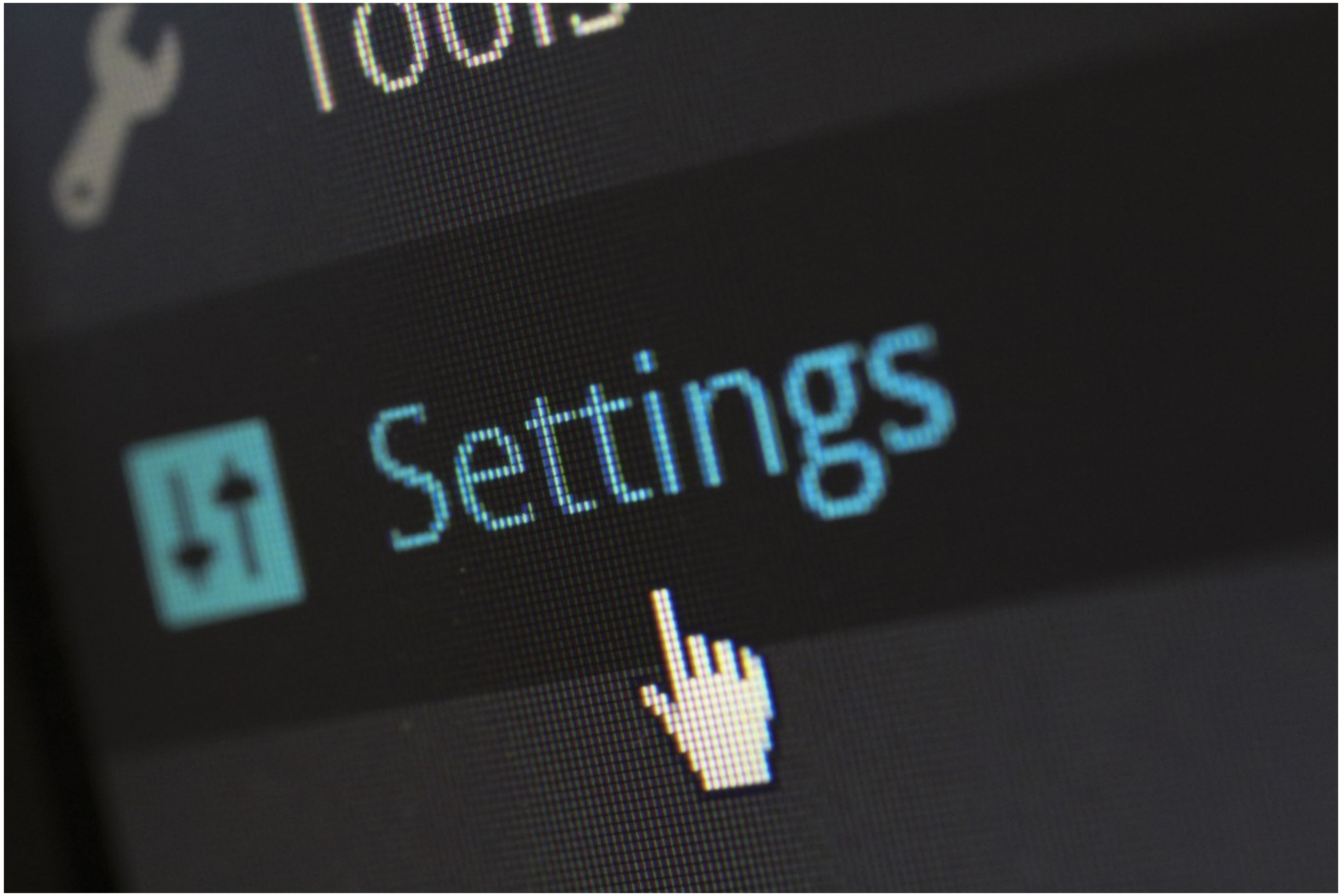
Scripts are not required for the functionality of the Web site.

Provides Onion Address FAIL

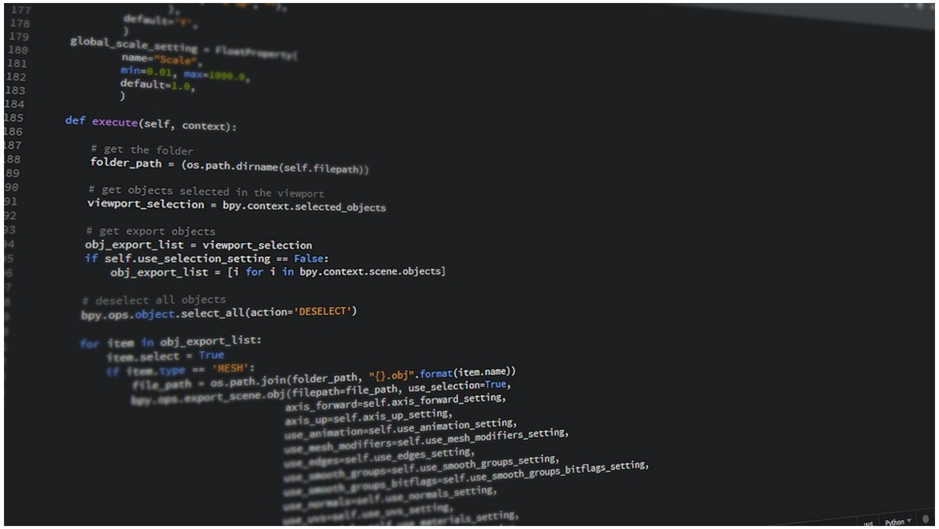
The content is not available as an Onion Service.

Avoids Fine-Grained Time Measurement PASS

This website does not rely on highly-granular time measurements, avoiding fingerprinting.


Tools
Settings

Limitations

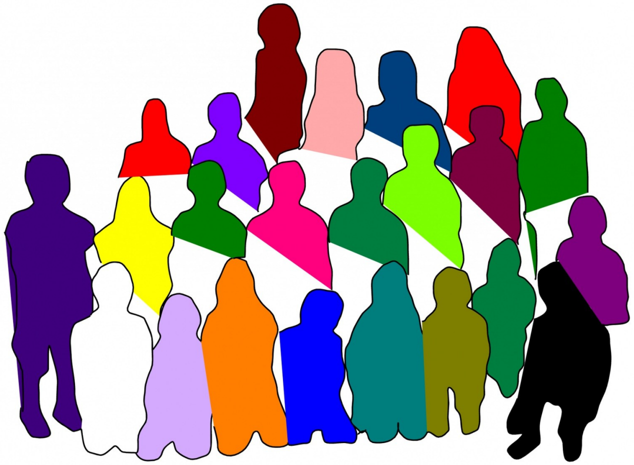


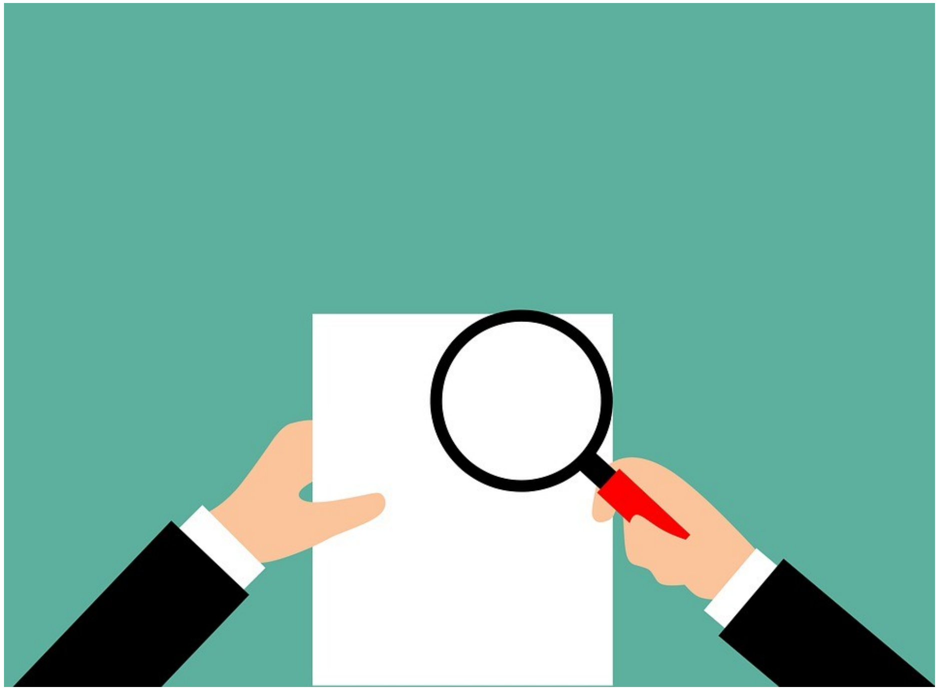
```
            ),
        default='Y',
        )
    global_scale_setting = FloatProperty(
        name="Scale",
        min=0.01, max=1000.0,
        default=1.0,
        )

def execute(self, context):

    # get the folder
    folder_path = (os.path.dirname(self.filepath))

    # get objects selected in the viewport
    viewport_selection = bpy.context.selected_objects

    # get export objects
    obj_export_list = viewport_selection
    if self.use_selection_setting == False:
        obj_export_list = [i for i in bpy.context.scene.objects]

    # deselect all objects
    bpy.ops.object.select_all(action='DESELECT')

    for item in obj_export_list:
        item.select = True
        if item.type == 'MESH':
            file_path = os.path.join(folder_path, "{}.obj".format(item.name))
            bpy.ops.export_scene.obj(filepath=file_path, use_selection=True,
                                    axis_forward=self.axis_forward_setting,
                                    axis_up=self.axis_up_setting,
                                    use_animation=self.use_animation_setting,
                                    use_mesh_modifiers=self.use_mesh_modifiers_setting,
                                    use_edges=self.use_edges_setting,
                                    use_smooth_groups=self.use_smooth_groups_setting,
                                    use_smooth_groups_bitflags=self.use_smooth_groups_bitflags_setting,
                                    use_normals=self.use_normals_setting,
                                    use_uvs=self.use_uvs_setting,
                                    use_materials=self.use_materials_setting,
```

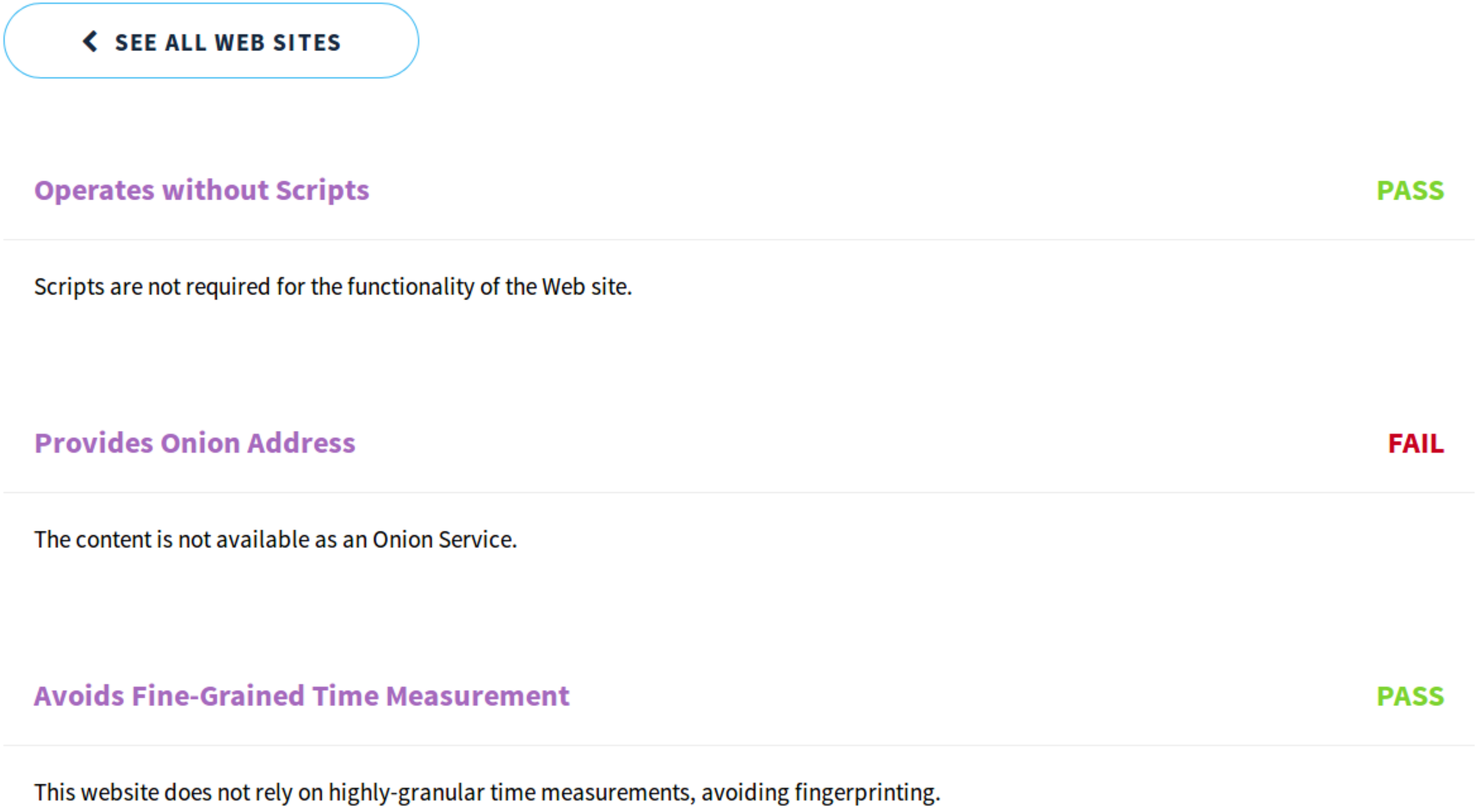
Sample Limitations

Script Limitations

Future Work







Operates without Scripts PASS

Scripts are not required for the functionality of the Web site.

Provides Onion Address FAIL

The content is not available as an Onion Service.

Avoids Fine-Grained Time Measurement PASS

This website does not rely on highly-granular time measurements, avoiding fingerprinting.

In summary...

Naturalistic Tor UX issues

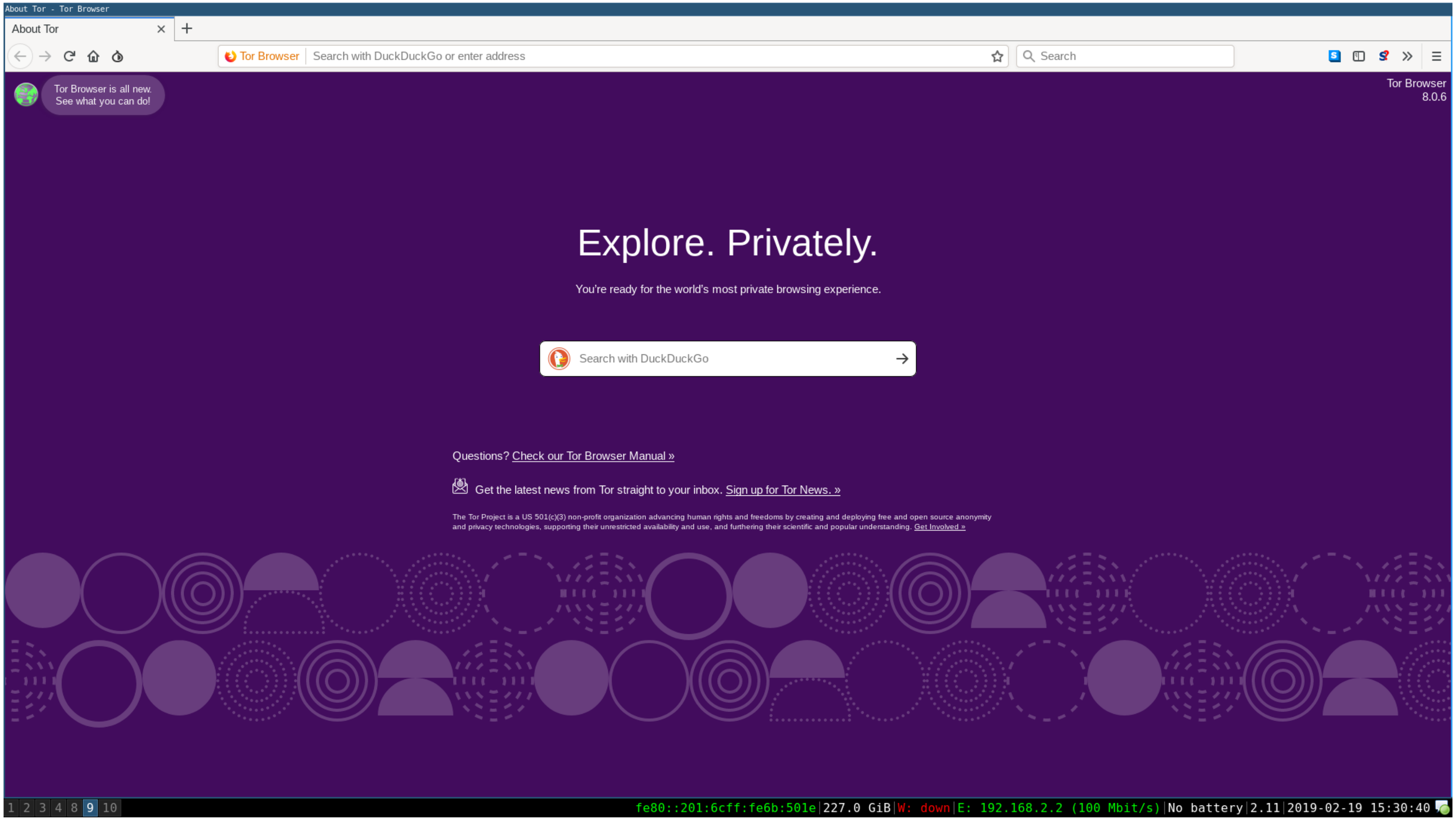
Frequent UX hurdles

Recommendations drawn from the data

kevin.gallagher@nyu.edu

Code at https://github.com/kcg295/TorUsabilityBrowserSensor/

Current State of Tor UX



Explore. Privately.

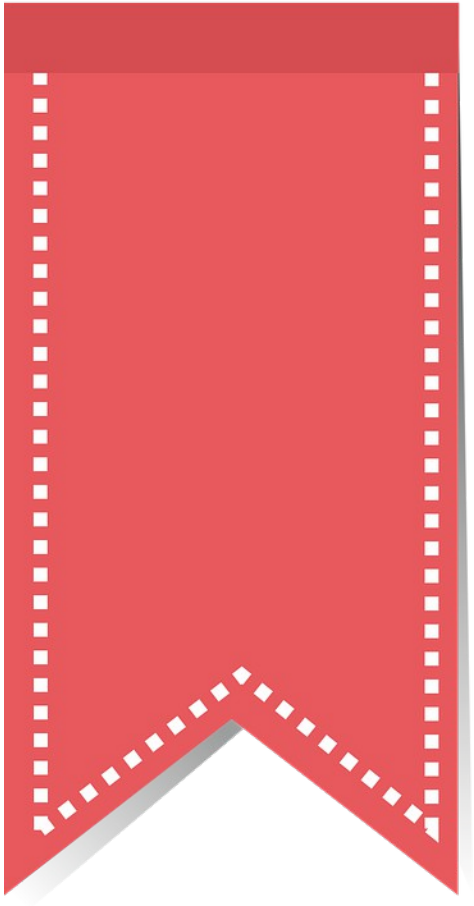
You're ready for the world's most private browsing experience.

Questions? Check our Tor Browser Manual »

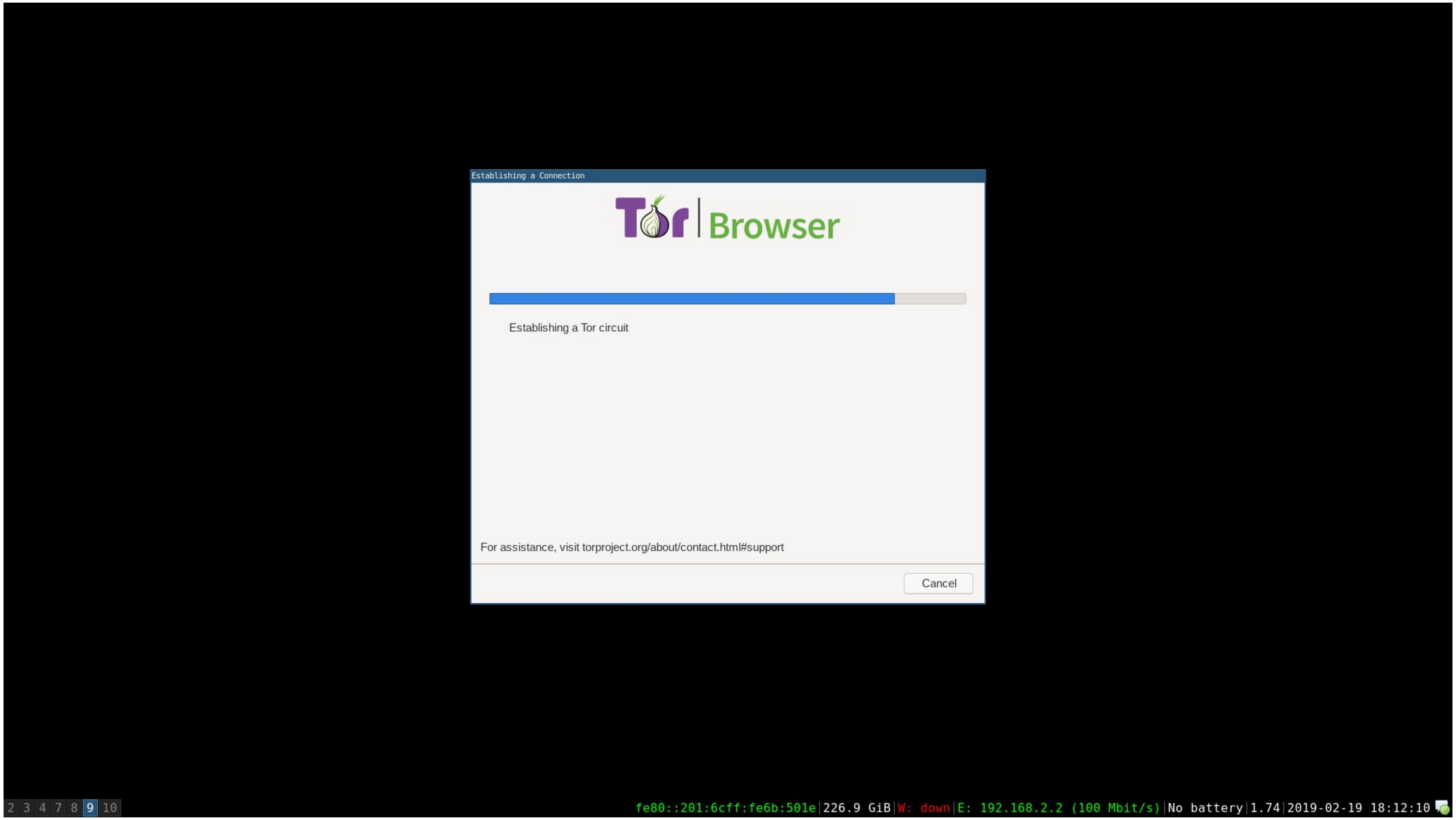
Get the latest news from Tor straight to your inbox. Sign up for Tor News. »

The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Get Involved »

```
1 2 3 4 8 9 10                fe80::201:6cff:fe6b:501e|227.0 GiB|W: down|E: 192.168.2.2 (100 Mbit/s)|No battery|2.11|2019-02-19 15:30:40
```



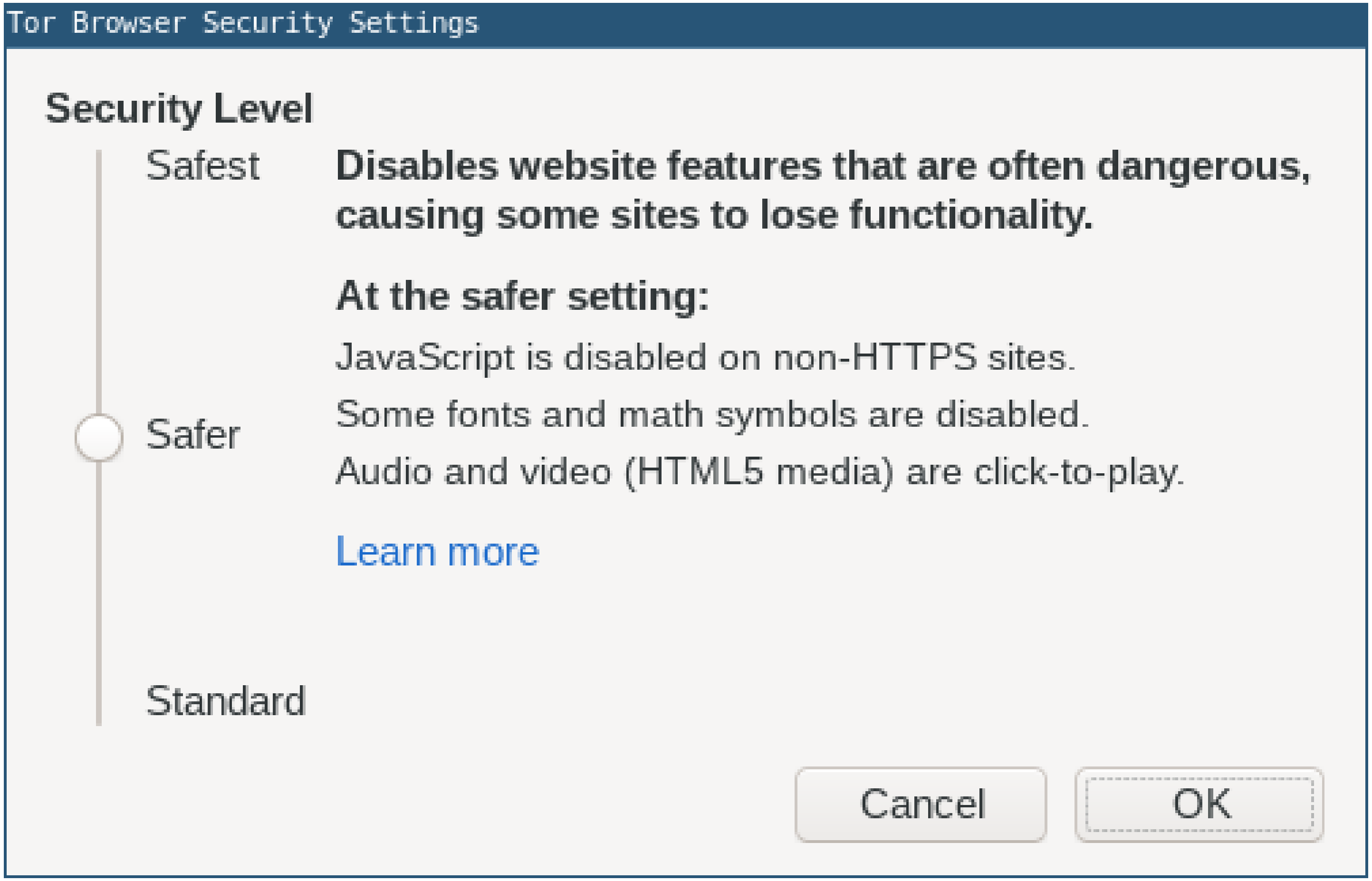
8 6 1 2 0 8 3 4
P A S S W O R D
0 8 3 4 2 0 5 6



Establishing a Tor circuit

For assistance, visit torproject.org/about/contact.html#support

```
fe80::201:6cff:fe6b:501e|226.9 GiB|W: down|E: 192.168.2.2 (100 Mbit/s)|No battery|1.74|2019-02-19 18:12:10
```



Tor Browser Security Settings

Security Level

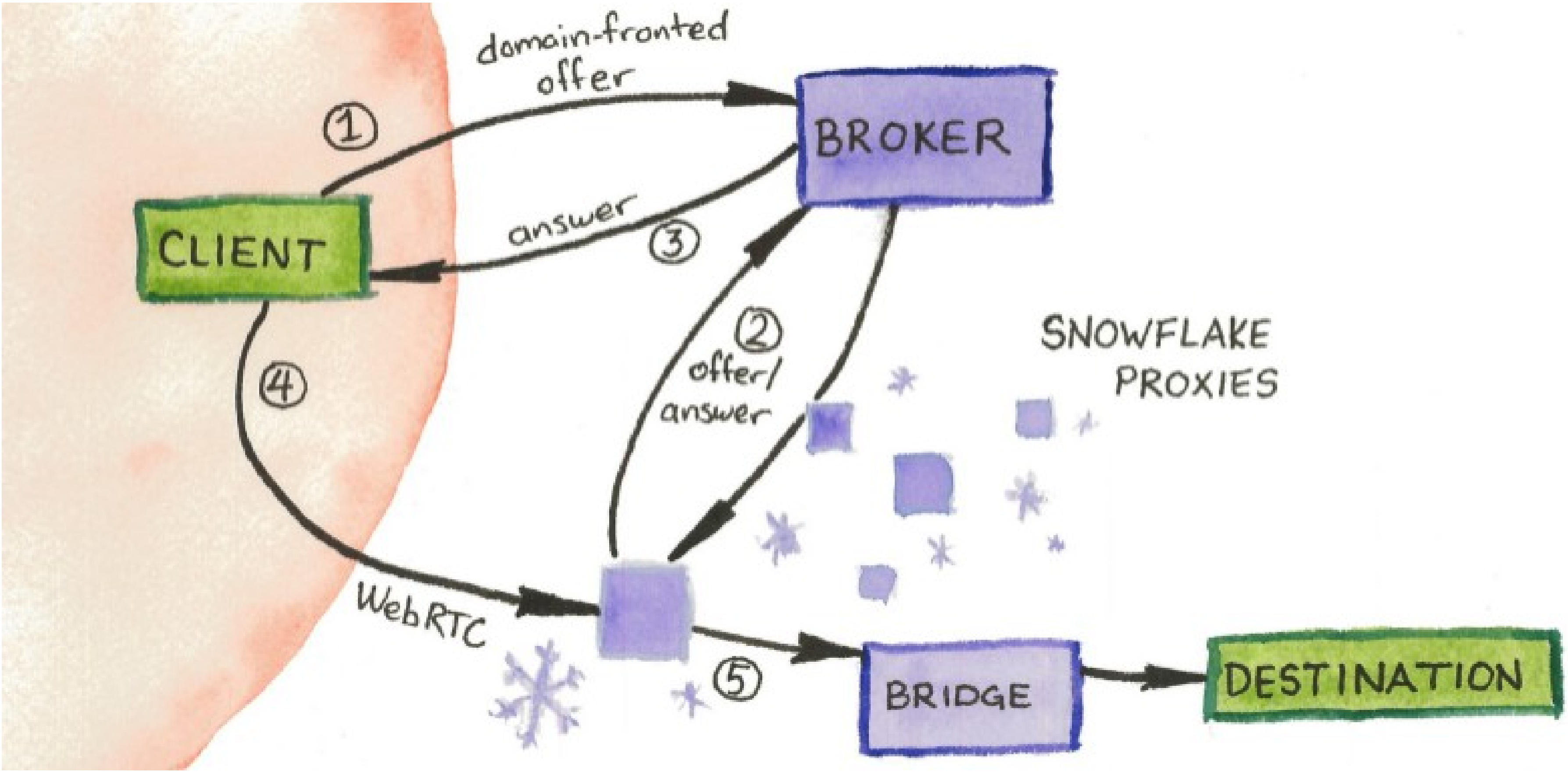
Disables website features that are often dangerous, causing some sites to lose functionality.

At the safer setting:

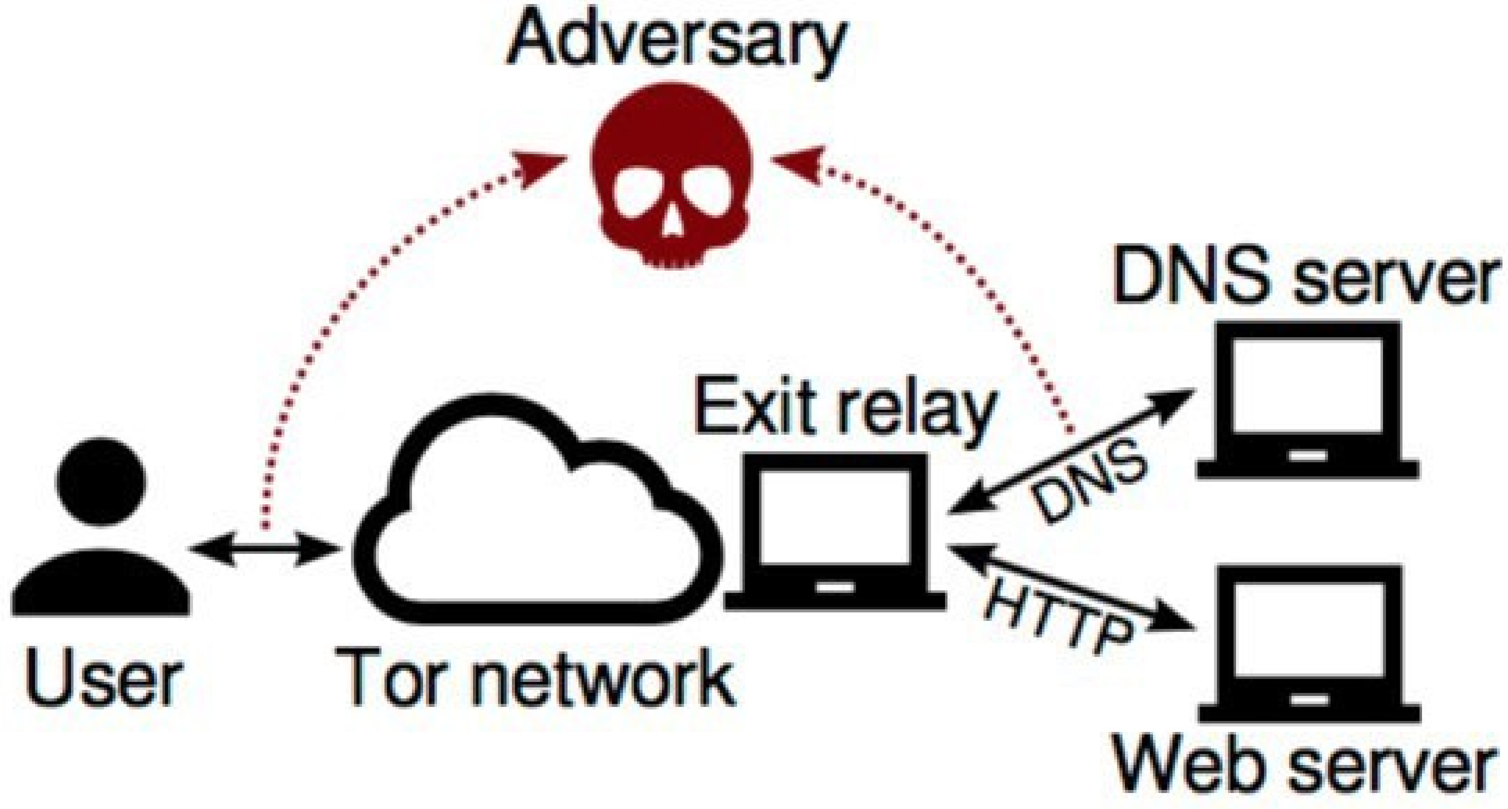
JavaScript is disabled on non-HTTPS sites.

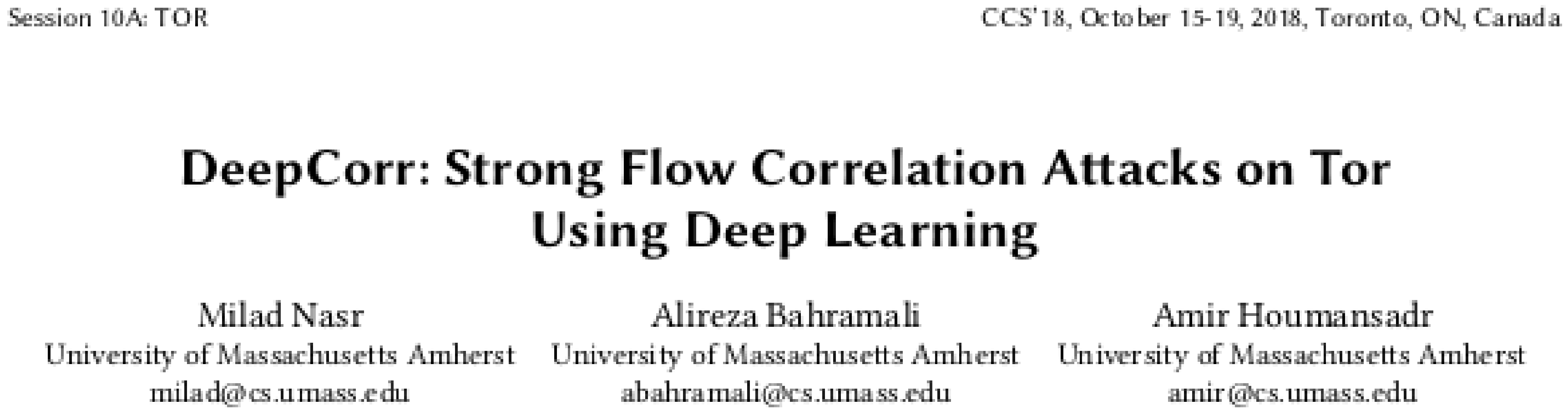
Some fonts and math symbols are disabled.

Audio and video (HTML5 media) are click-to-play.


domain-fronted offer
①
BROKER
CLIENT
answer
③
②
offer/answer
④
SNOWFLAKE PROXIES
WebRTC
⑤
BRIDGE
DESTINATION

State of Traffic Analysis Attacks


Adversary
DNS server
Exit relay
DNS
User
Tor network
HTTP
Web server



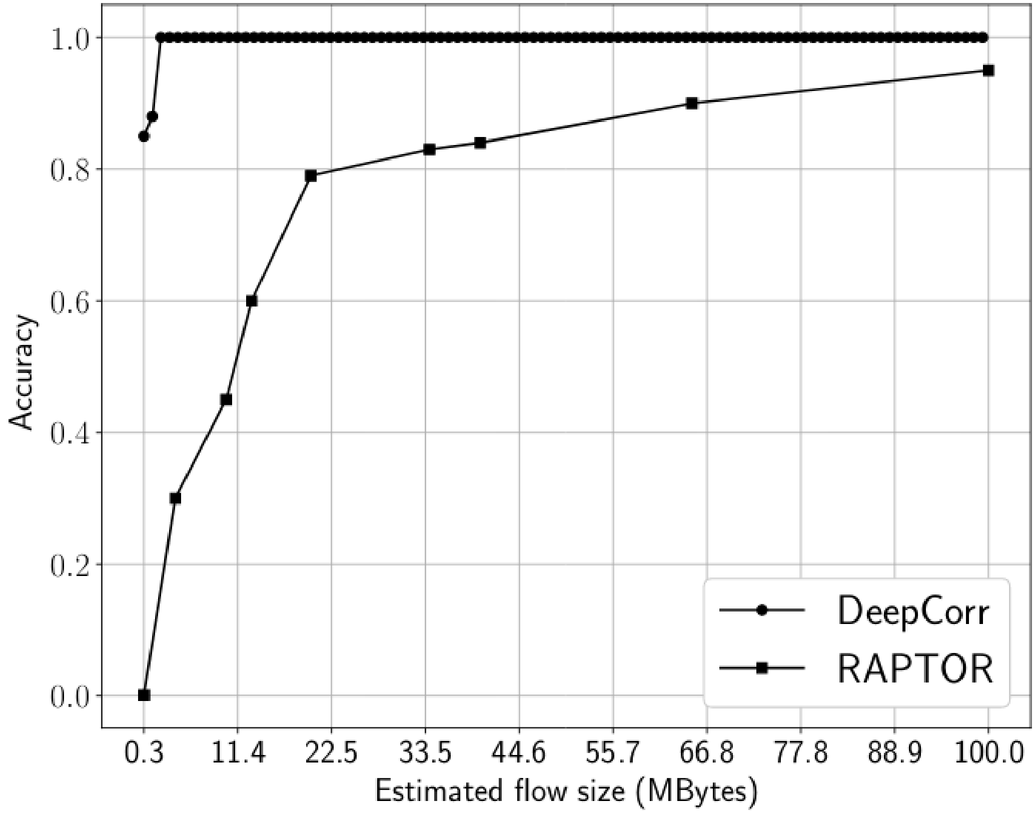
Session 10A: TOR CCS'18, October 15-19, 2018, Toronto, ON, Canada

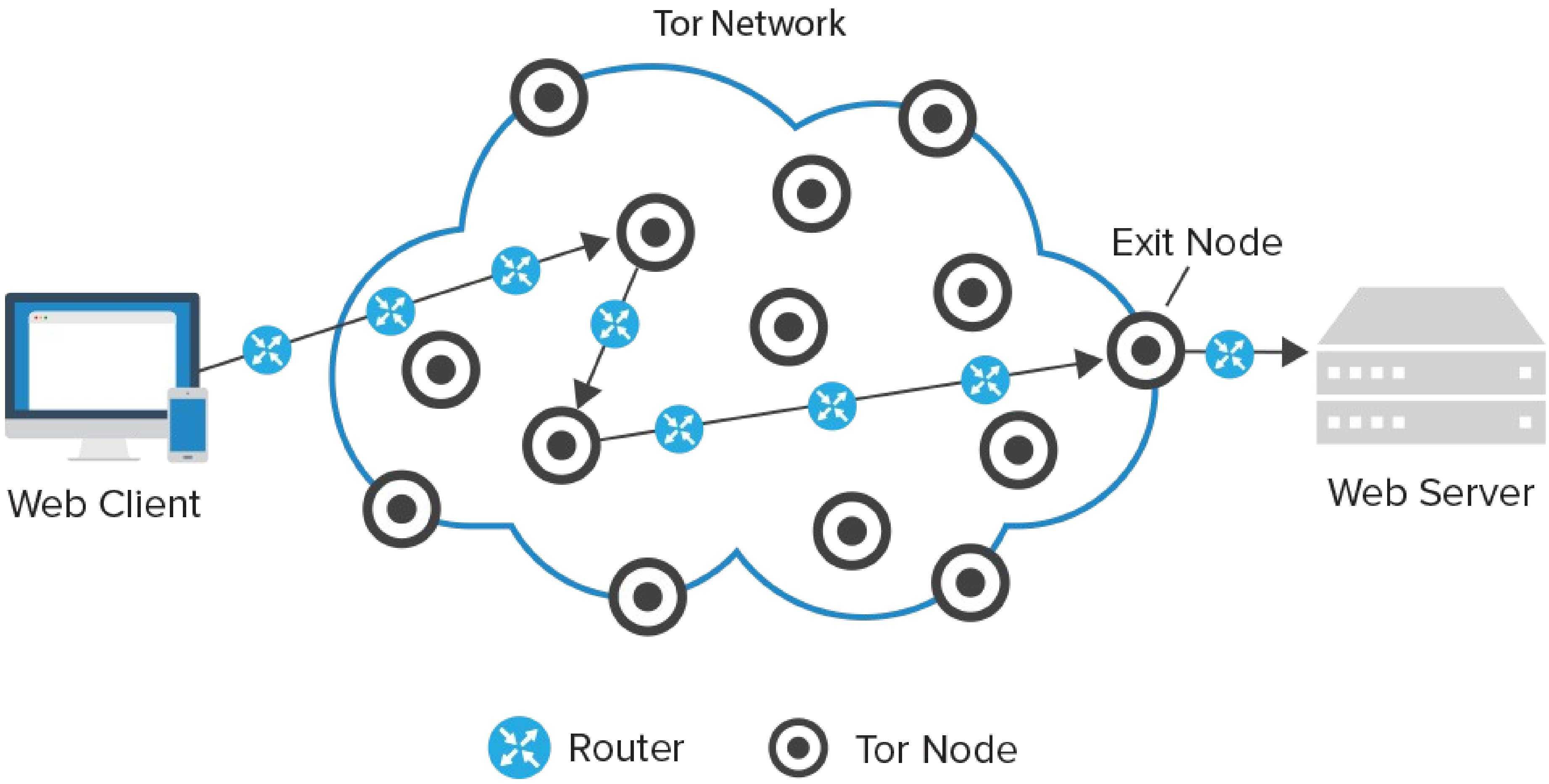
DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning

Milad Nasr
University of Massachusetts Amherst
milad@cs.umass.edu

Alireza Bahramali
University of Massachusetts Amherst
abahramali@cs.umass.edu

Amir Houmansadr
University of Massachusetts Amherst
amir@cs.umass.edu


1.0
0.8
0.6
0.4
0.2
0.0
Accuracy
0.3
11.4
22.5
33.5
44.6
55.7
66.8
77.8
88.9
100.0
Estimated flow size (MBytes)
DeepCorr
RAPTOR


Tor Network
Exit Node
Web Client
Web Server
Router
Tor Node

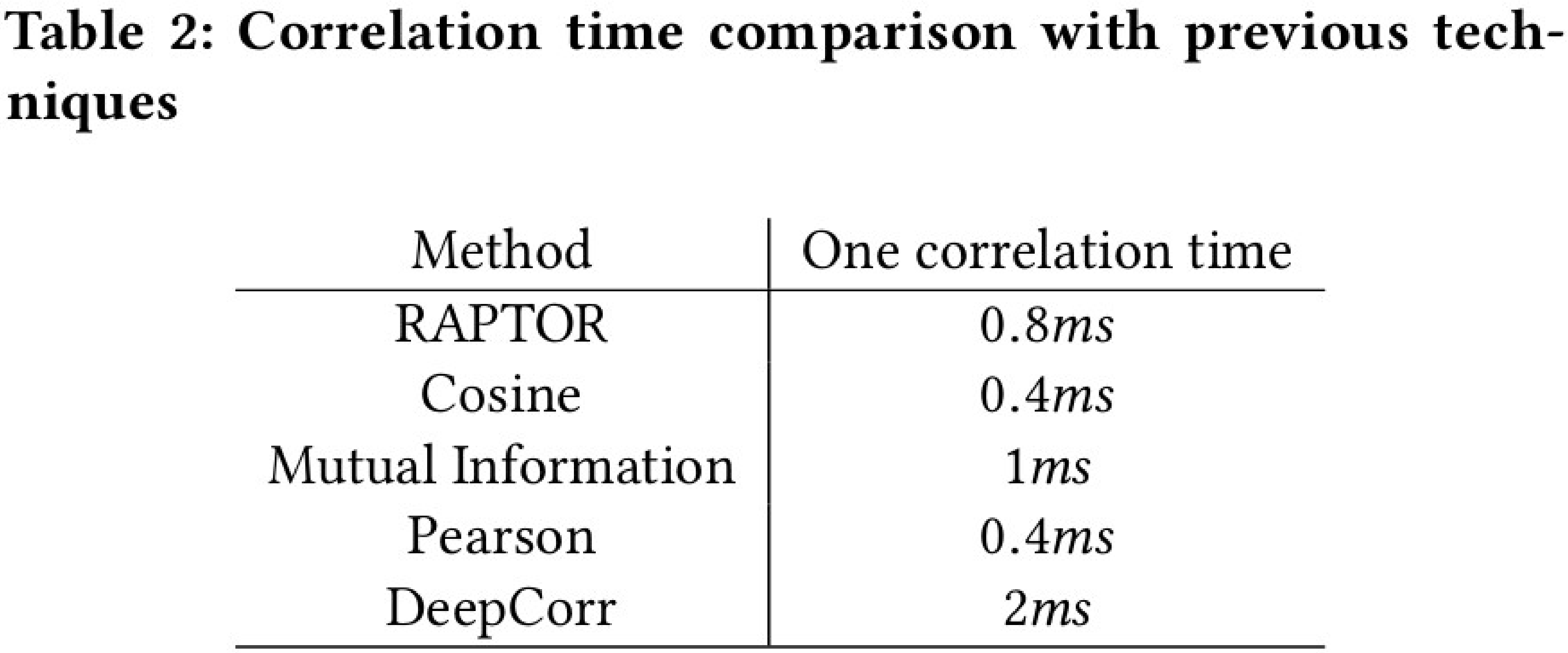
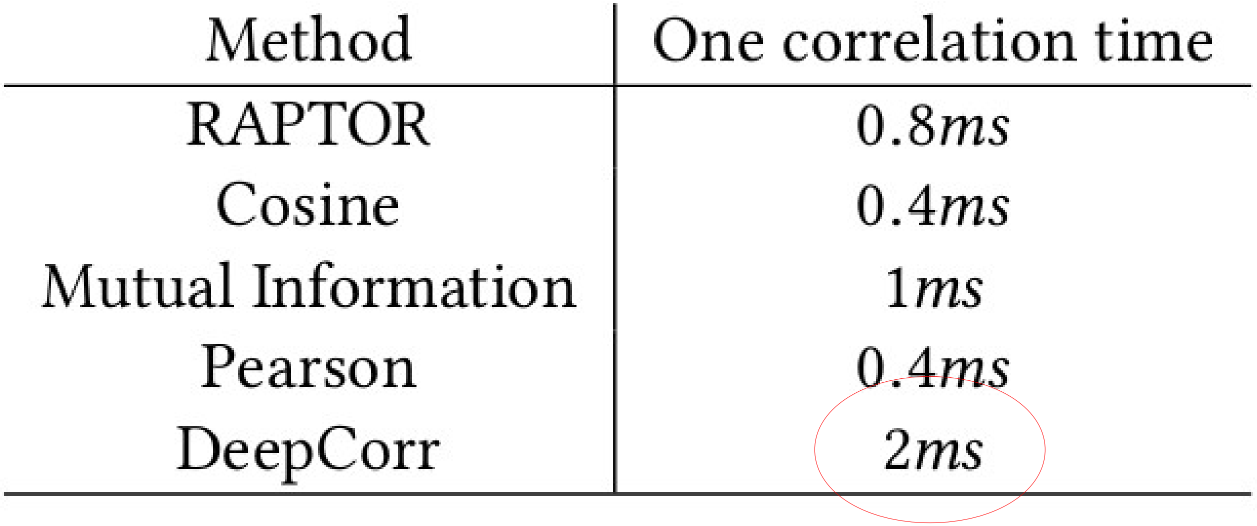


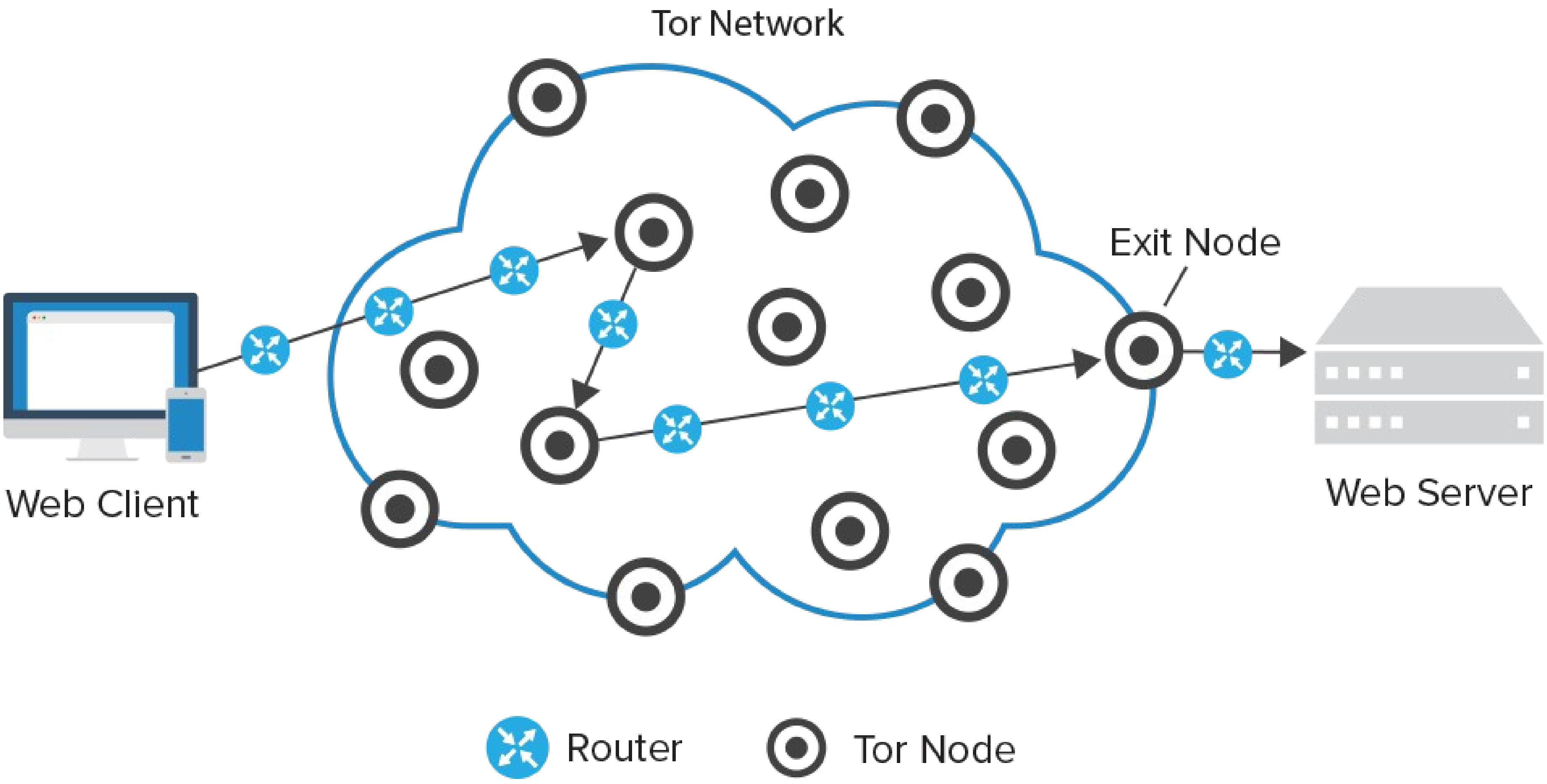
Table 2: Correlation time comparison with previous techniques

Method	One correlation time
RAPTOR	$0.8ms$
Cosine	$0.4ms$
Mutual Information	$1ms$
Pearson	$0.4ms$
DeepCorr	$2ms$

Table 2: Correlation time comparison with previous techniques



Method	One correlation time
RAPTOR	0.8*ms*
Cosine	0.4*ms*
Mutual Information	1*ms*
Pearson	0.4*ms*
DeepCorr	2*ms*


Tor Network
Exit Node
Web Client
Web Server
Router
Tor Node

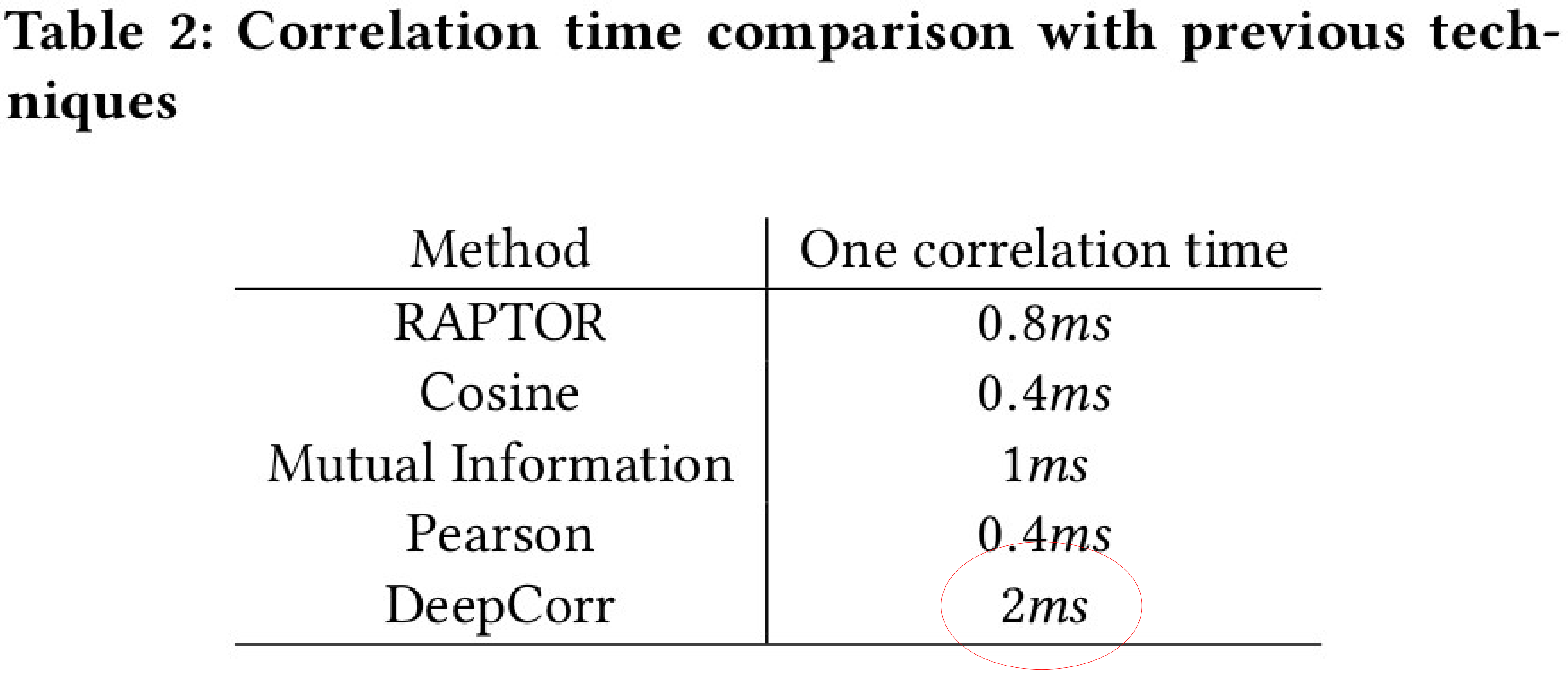
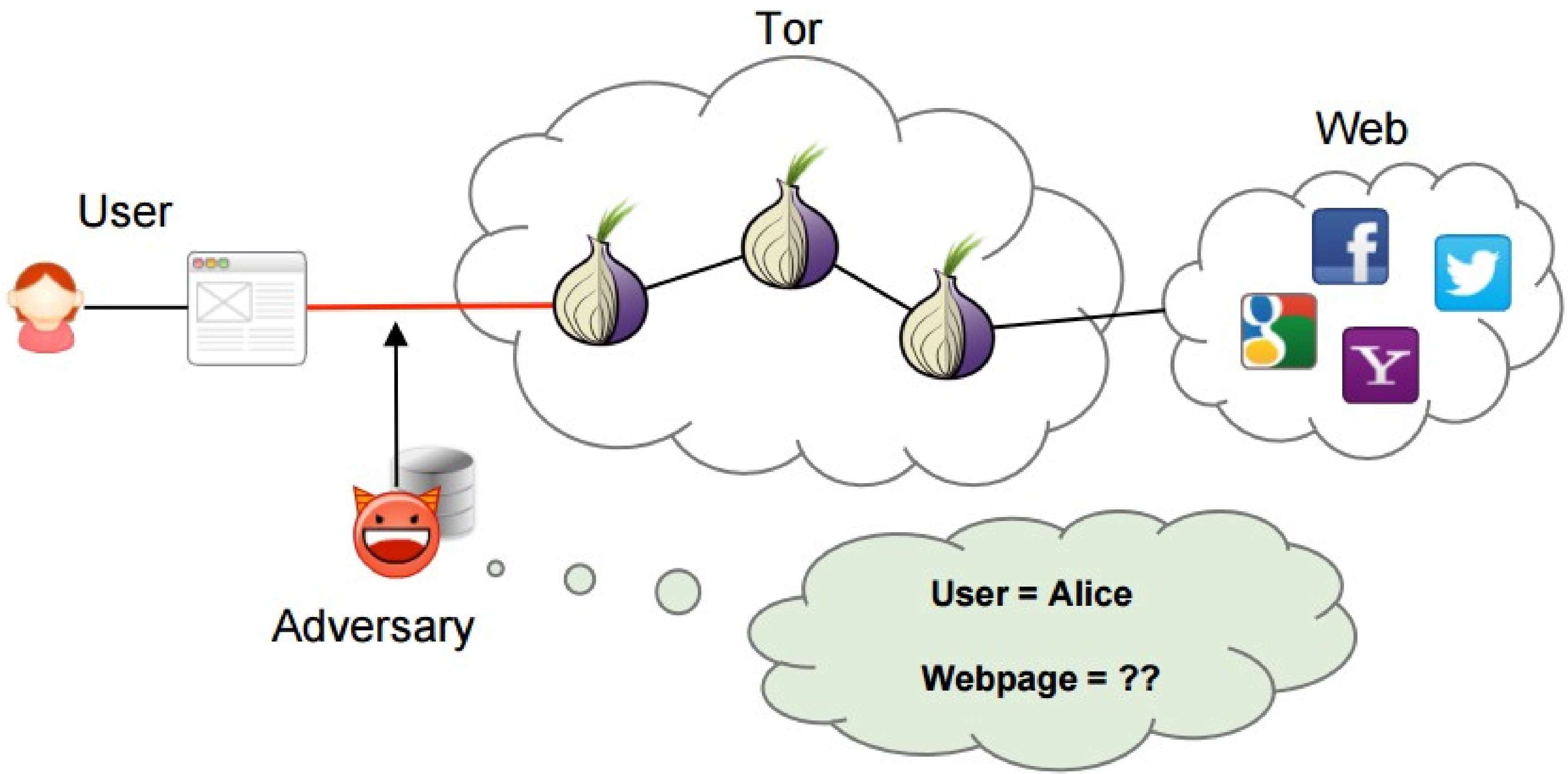


Table 2: Correlation time comparison with previous techniques

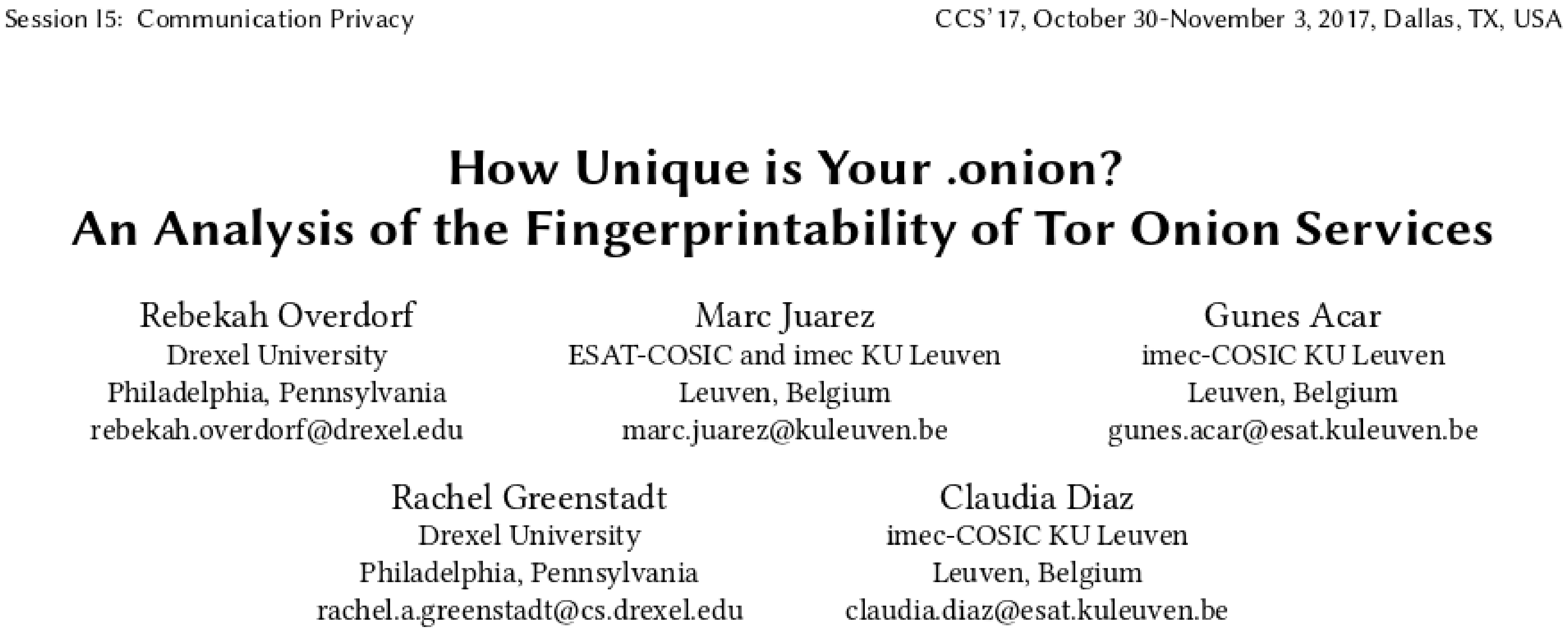
Method	One correlation time
RAPTOR	$0.8ms$
Cosine	$0.4ms$
Mutual Information	$1ms$
Pearson	$0.4ms$
DeepCorr	$2ms$

- Good for targeted attacks
- Bad for dragnet surveillance
- Works in practical lab settings, unknown in practice



User = Alice

Webpage = ??



How Unique is Your .onion? An Analysis of the Fingerprintability of Tor Onion Services

Rebekah Overdorf
Drexel University
Philadelphia, Pennsylvania
rebekah.overdorf@drexel.edu

Marc Juarez
ESAT-COSIC and imec KU Leuven
Leuven, Belgium
marc.juarez@kuleuven.be

Gunes Acar
imec-COSIC KU Leuven
Leuven, Belgium
gunes.acar@esat.kuleuven.be

Rachel Greenstadt
Drexel University
Philadelphia, Pennsylvania
rachel.a.greenstadt@cs.drexel.edu

Claudia Diaz
imec-COSIC KU Leuven
Leuven, Belgium
claudia.diaz@esat.kuleuven.be

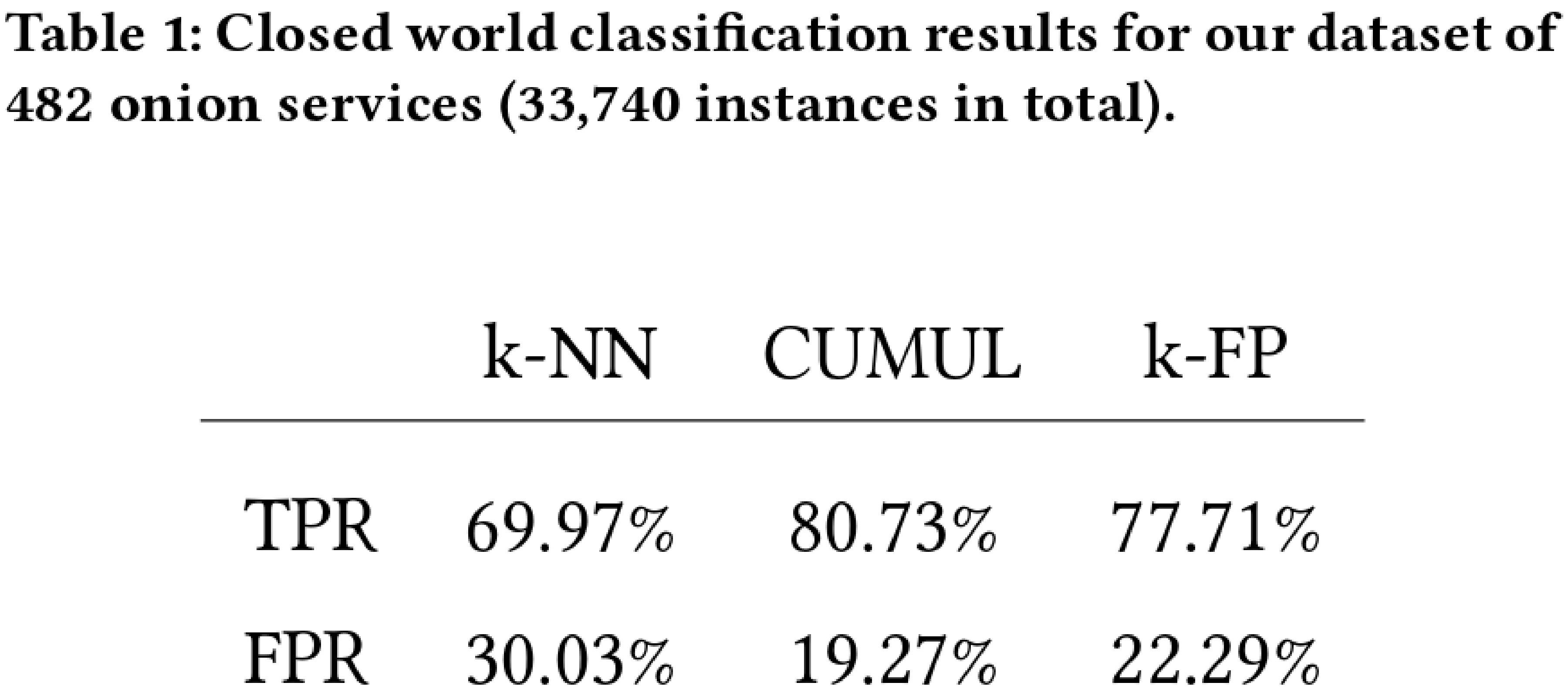


Table 1: Closed world classification results for our dataset of 482 onion services (33,740 instances in total).

	k-NN	CUMUL	k-FP
TPR	69.97%	80.73%	77.71%
FPR	30.03%	19.27%	22.29%

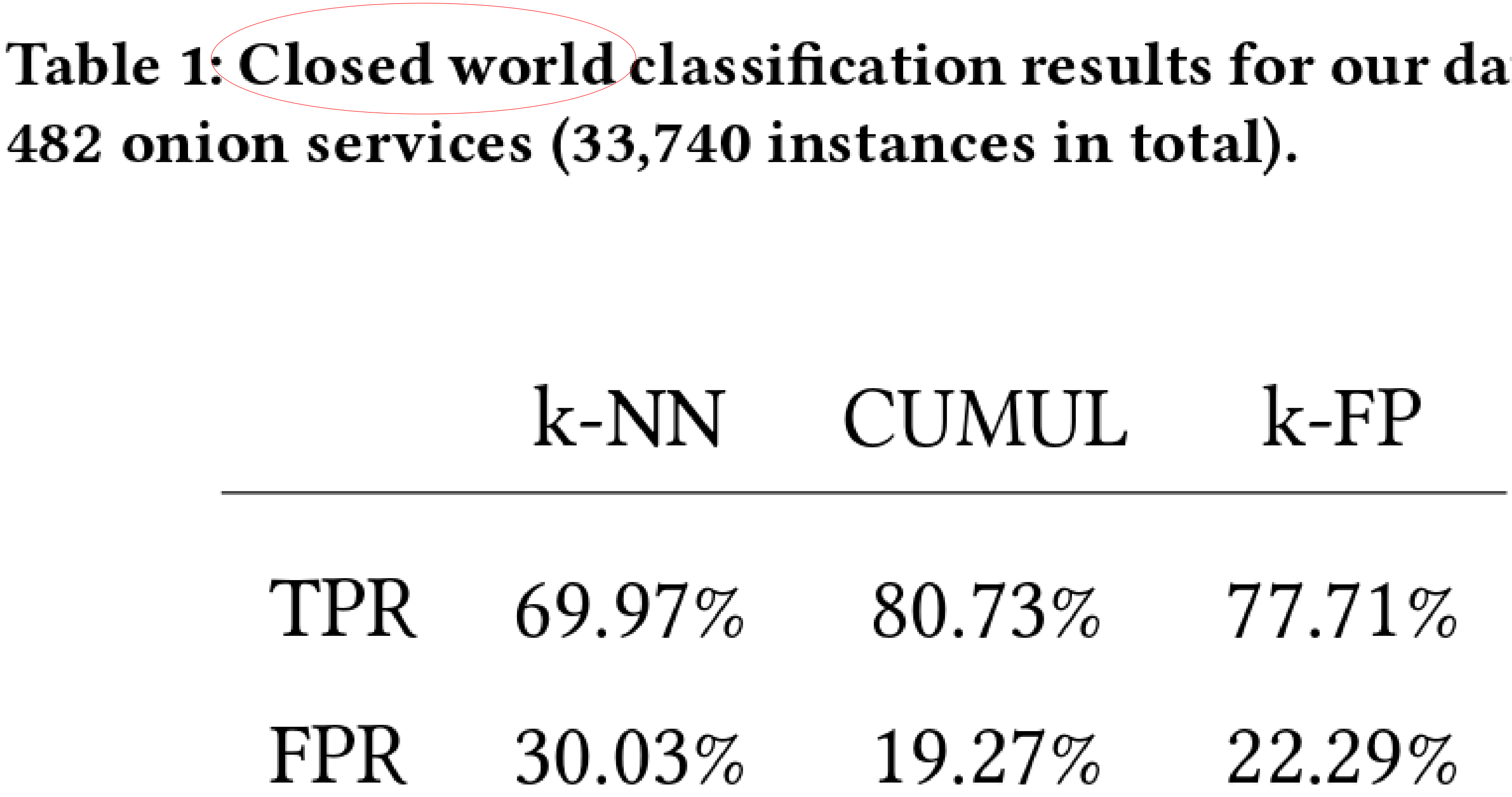
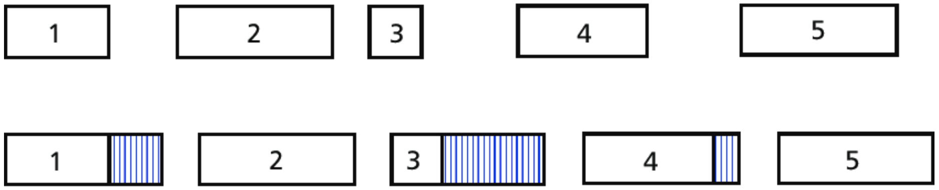
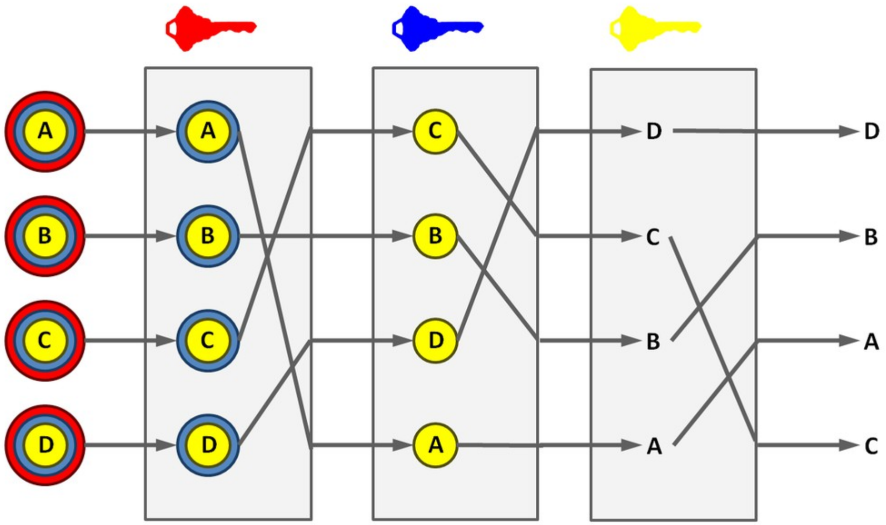


Table 1: Closed world classification results for our dataset of 482 onion services (33,740 instances in total).

	k-NN	CUMUL	k-FP
TPR	69.97%	80.73%	77.71%
FPR	30.03%	19.27%	22.29%

- Good for targeted attacks
- OK-ish for dragnet surveillance
- Works in practical lab settings, unknown in practice


1
2
3
4
5
1
2
3
4
5


A
B
C
D
A
B
C
D
C
B
D
A
D
C
B
A
D
B
A
C