# Supporting Privacy and Freedom of Expression Worldwide

## (and Helping Your Research, Too!)

Ian Goldberg

Cryptography, Security, and Privacy (CrySP) Research Group
University of Waterloo

1 April 2024

UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS
DAVID R. CHERITON SCHOOL
OF COMPUTER SCIENCE

CrySP

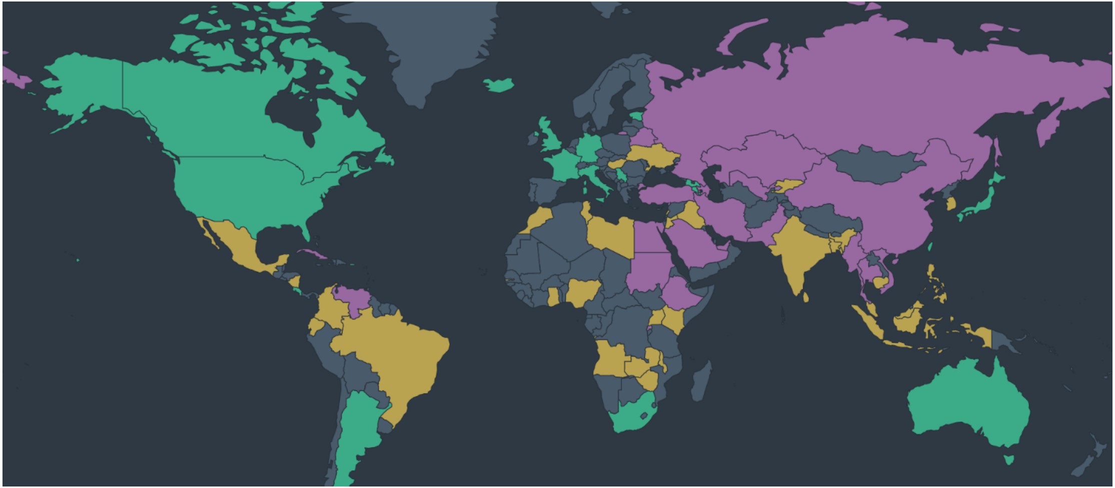
# Privacy

# Privacy

July 27, 1970 / 50 cents
Newsweek
IS PRIVACY DEAD?
FILE No 235149577-5203
buehnergarth

https://www.theamericanconservative.com/newsweek-ponders-privacy-in-1970/

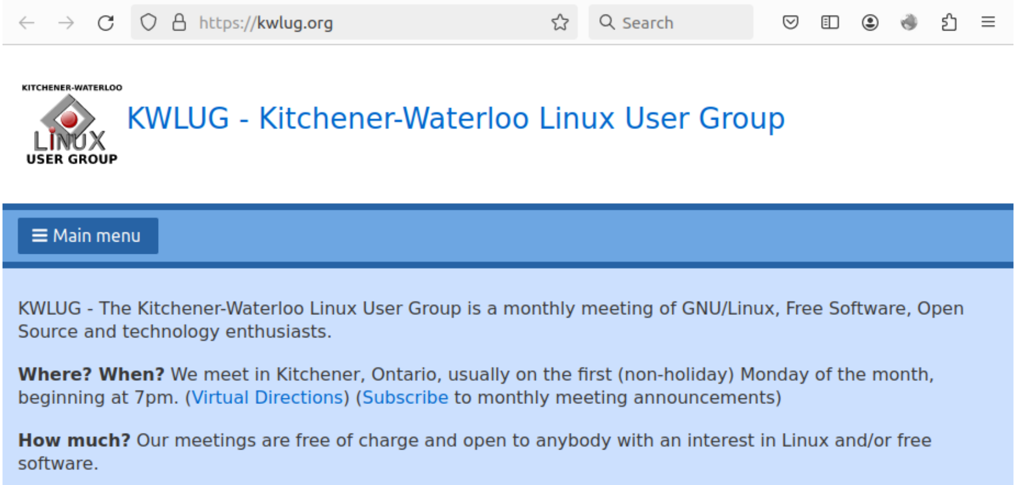
# Privacy



https://freedomhouse.org/explore-the-map?type=fotn&year=2023

# Protecting the data

# Protecting the data



KWLUG - Kitchener-Waterloo Linux User Group

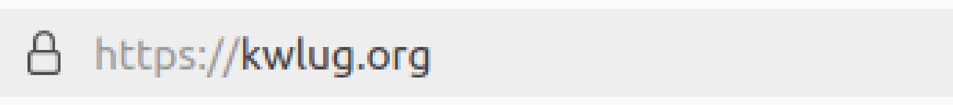
KWLUG - The Kitchener-Waterloo Linux User Group is a monthly meeting of GNU/Linux, Free Software, Open Source and technology enthusiasts.

**Where? When?** We meet in Kitchener, Ontario, usually on the first (non-holiday) Monday of the month, beginning at 7pm. (Virtual Directions) (Subscribe to monthly meeting announcements)

**How much?** Our meetings are free of charge and open to anybody with an interest in Linux and/or free software.

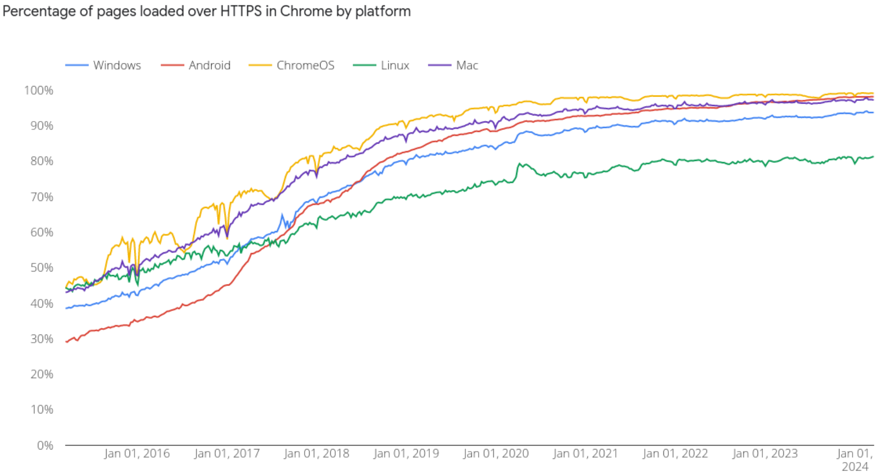
https://kwlug.org/

# Protecting the data



https://kwlug.org

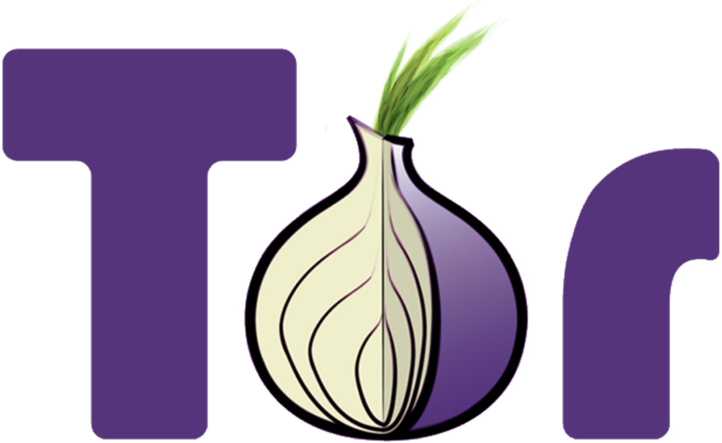
# Protecting the data



https://transparencyreport.google.com/https/overview?hl=en

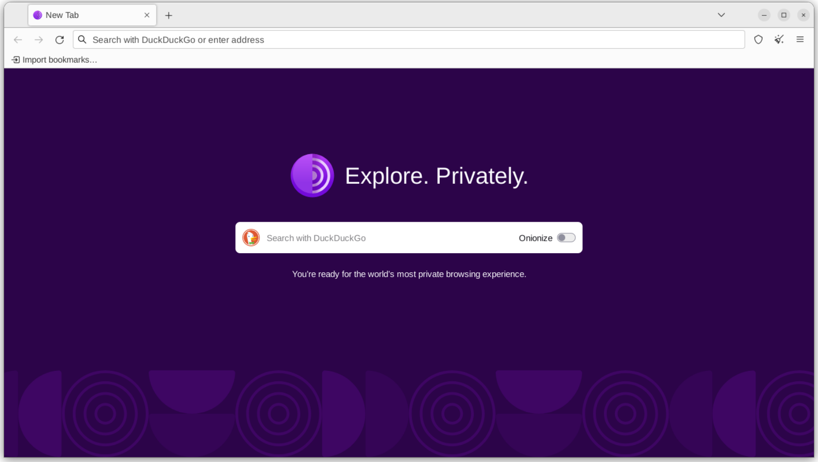
# Protecting the metadata

# Protecting the metadata



https://commons.wikimedia.org/wiki/File:Tor_project_logo_hq.png

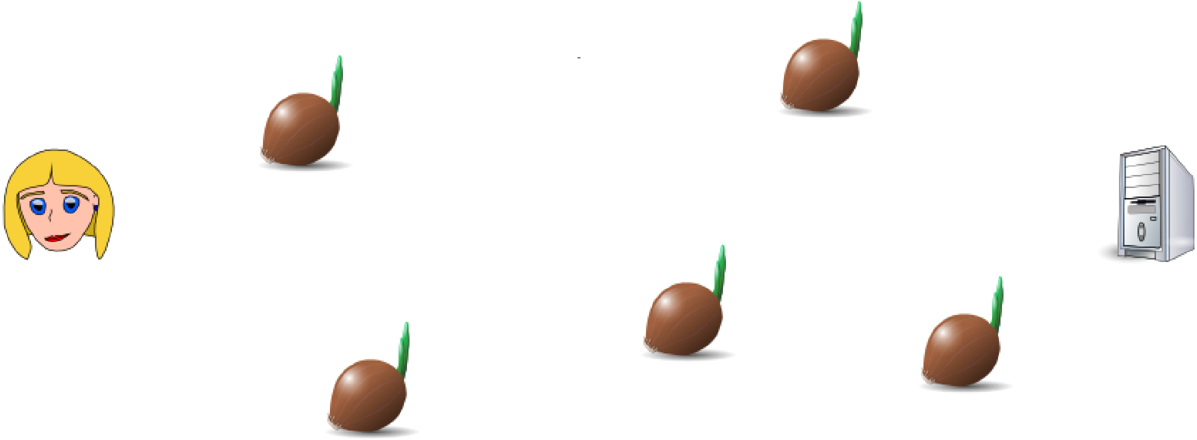
# Protecting the metadata



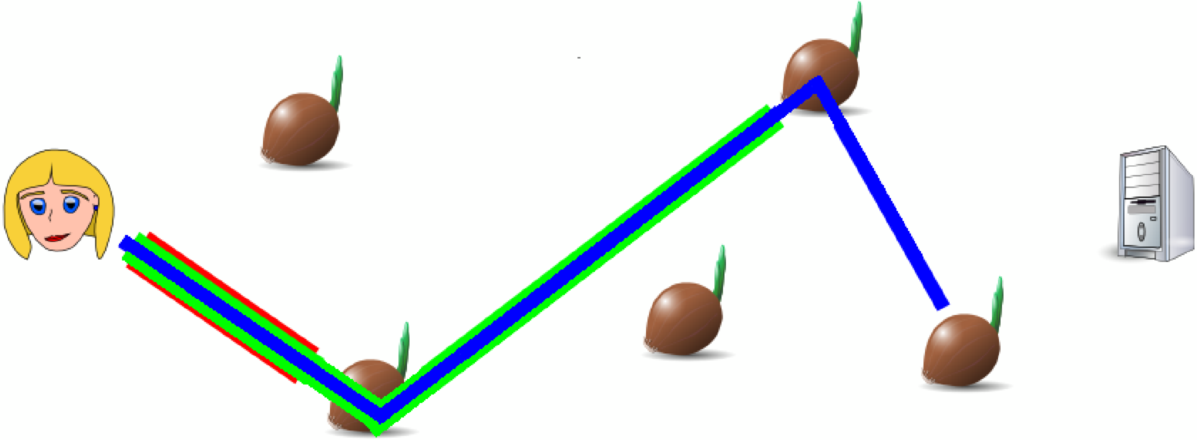
New Tab
Search with DuckDuckGo or enter address
Import bookmarks…
Explore. Privately.
Search with DuckDuckGo
Onionize
You're ready for the world's most private browsing experience.

# Tor circuits

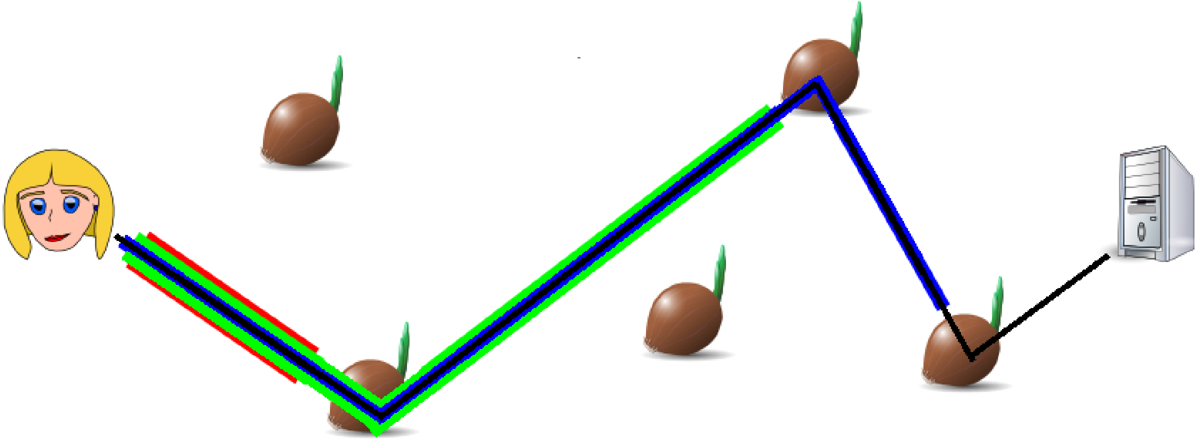
# Tor circuits



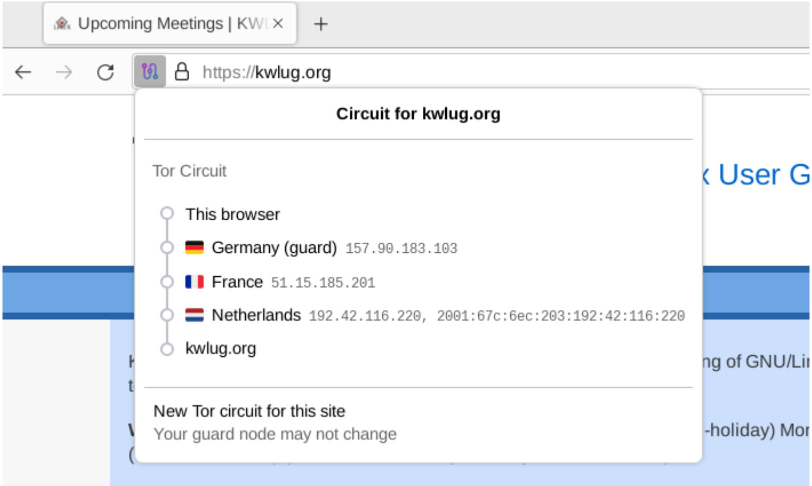
# Tor circuits



# Tor circuits



# Tor circuits



**Circuit for kwlug.org**

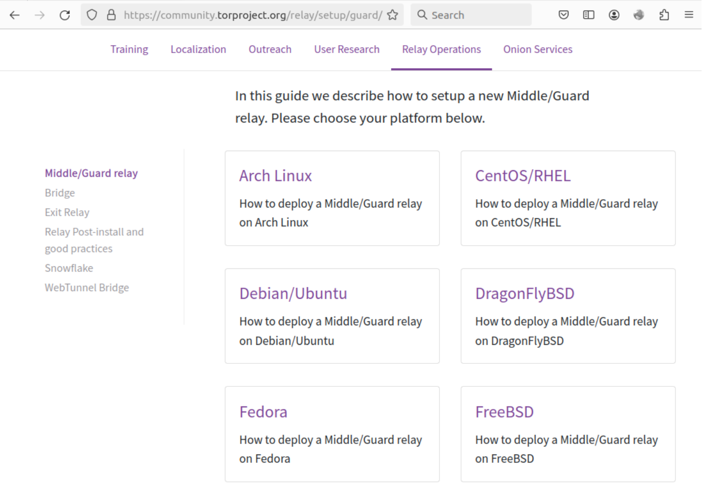
Tor Circuit

- This browser
- Germany (guard) 157.90.183.103
- France 51.15.185.201
- Netherlands 192.42.116.220, 2001:67c:6ec:203:192:42:116:220
- kwlug.org

New Tor circuit for this site
Your guard node may not change

# Running a Tor node

# Running a Tor node



In this guide we describe how to setup a new Middle/Guard relay. Please choose your platform below.

**Arch Linux**
How to deploy a Middle/Guard relay on Arch Linux

**CentOS/RHEL**
How to deploy a Middle/Guard relay on CentOS/RHEL

**Debian/Ubuntu**
How to deploy a Middle/Guard relay on Debian/Ubuntu

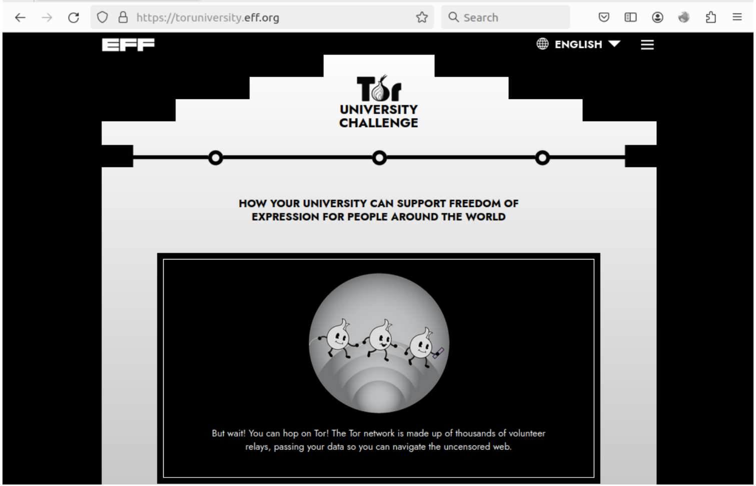
**DragonFlyBSD**
How to deploy a Middle/Guard relay on DragonFlyBSD

**Fedora**
How to deploy a Middle/Guard relay on Fedora

**FreeBSD**
How to deploy a Middle/Guard relay on FreeBSD

https://community.torproject.org/relay/setup/guard/

# Running a Tor node

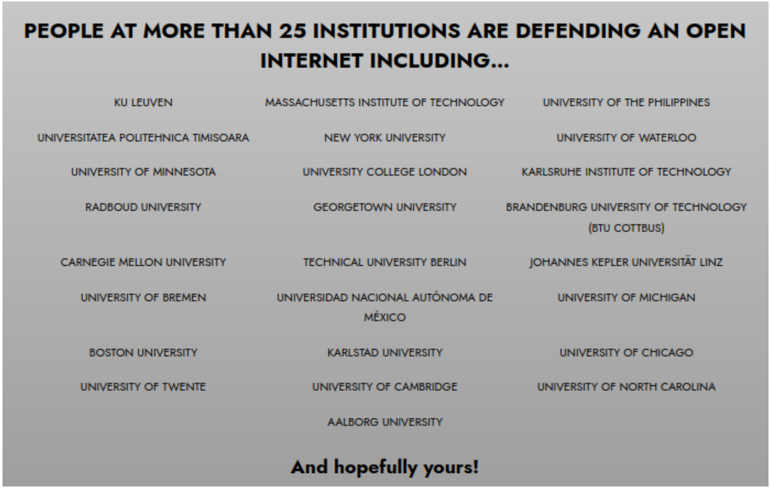


HOW YOUR UNIVERSITY CAN SUPPORT FREEDOM OF EXPRESSION FOR PEOPLE AROUND THE WORLD

But wait! You can hop on Tor! The Tor network is made up of thousands of volunteer relays, passing your data so you can navigate the uncensored web.

https://toruniversity.eff.org/

# Running a Tor node



## PEOPLE AT MORE THAN 25 INSTITUTIONS ARE DEFENDING AN OPEN INTERNET INCLUDING...

KU LEUVEN

UNIVERSITATEA POLITEHNICA TIMISOARA

UNIVERSITY OF MINNESOTA

RADBOUD UNIVERSITY

CARNEGIE MELLON UNIVERSITY

UNIVERSITY OF BREMEN

BOSTON UNIVERSITY

UNIVERSITY OF TWENTE

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

NEW YORK UNIVERSITY

UNIVERSITY COLLEGE LONDON

GEORGETOWN UNIVERSITY

TECHNICAL UNIVERSITY BERLIN

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

KARLSTAD UNIVERSITY

UNIVERSITY OF CAMBRIDGE

AALBORG UNIVERSITY

UNIVERSITY OF THE PHILIPPINES

UNIVERSITY OF WATERLOO

KARLSRUHE INSTITUTE OF TECHNOLOGY

BRANDENBURG UNIVERSITY OF TECHNOLOGY (BTU COTTBUS)

JOHANNES KEPLER UNIVERSITÄT LINZ

UNIVERSITY OF MICHIGAN

UNIVERSITY OF CHICAGO

UNIVERSITY OF NORTH CAROLINA

**And hopefully yours!**

https://toruniversity.eff.org/

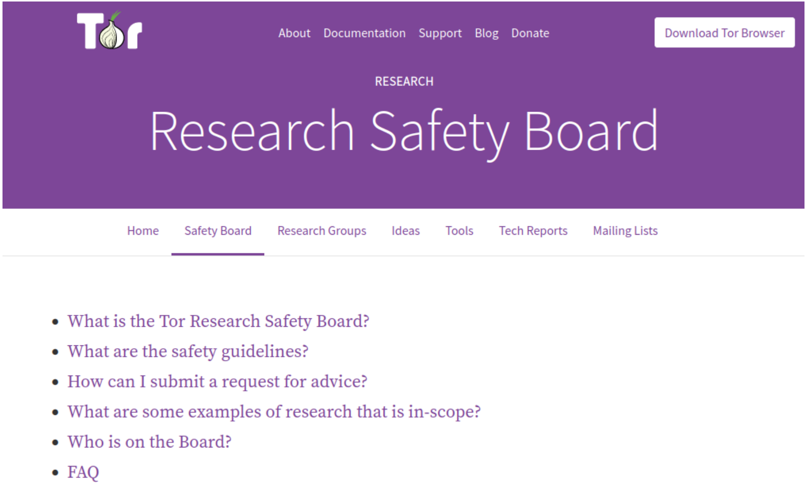
# Benefits

# Benefits

Benefits for running Tor nodes at universities include (see https://toruniversity.eff.org/ for more):

- Supporting privacy and freedom of expression worldwide
- Getting students involved in civil society
  - Tor Project, EFF, Citizen Lab, etc.
- Research
  - If you research the Tor network, you should contribute to it
  - Having direct access to the Tor network

# Benefits



RESEARCH

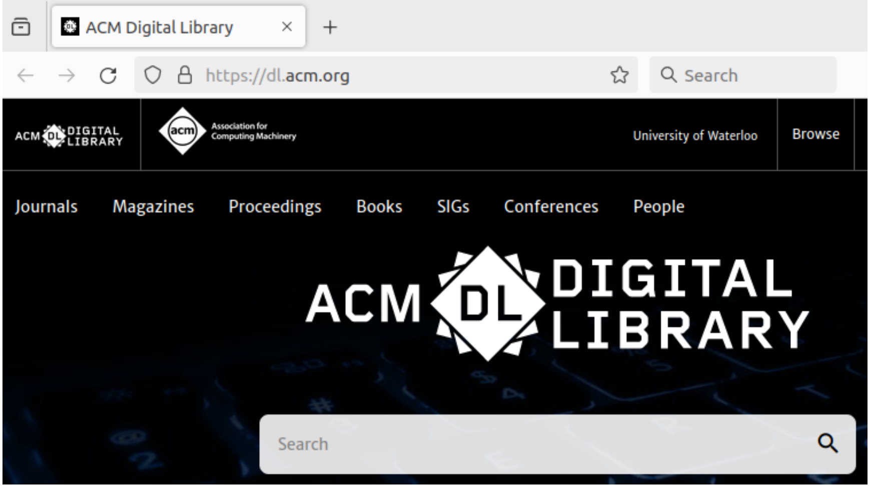
## Research Safety Board

- What is the Tor Research Safety Board?
- What are the safety guidelines?
- How can I submit a request for advice?
- What are some examples of research that is in-scope?
- Who is on the Board?
- FAQ

https://research.torproject.org/safetyboard/

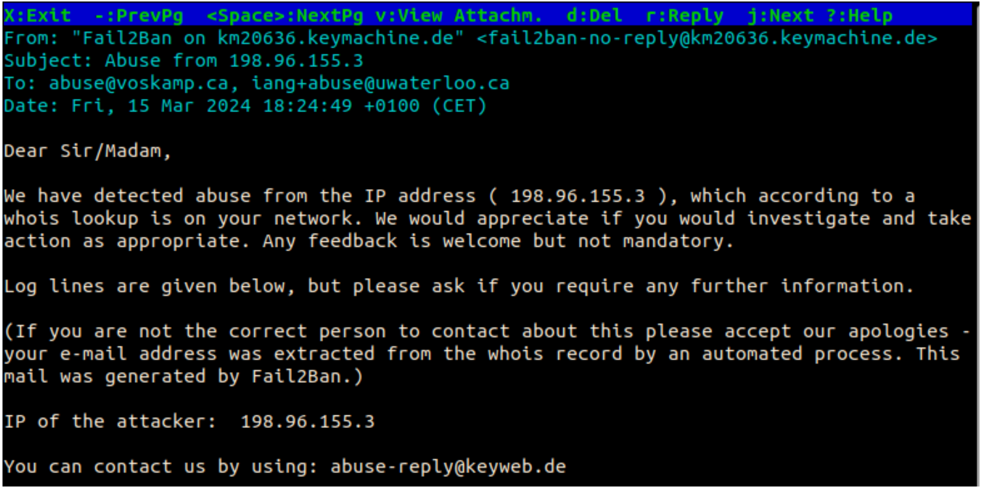
# Challenges

# Challenges



https://dl.acm.org

# Challenges



```
X:Exit  -:PrevPg  <Space>:NextPg v:View Attachm.  d:Del  r:Reply  j:Next ?:Help
From: "Fail2Ban on km20636.keymachine.de" <fail2ban-no-reply@km20636.keymachine.de>
Subject: Abuse from 198.96.155.3
To: abuse@voskamp.ca, iang+abuse@uwaterloo.ca
Date: Fri, 15 Mar 2024 18:24:49 +0100 (CET)

Dear Sir/Madam,

We have detected abuse from the IP address ( 198.96.155.3 ), which according to a
whois lookup is on your network. We would appreciate if you would investigate and take
action as appropriate. Any feedback is welcome but not mandatory.

Log lines are given below, but please ask if you require any further information.

(If you are not the correct person to contact about this please accept our apologies -
your e-mail address was extracted from the whois record by an automated process. This
mail was generated by Fail2Ban.)

IP of the attacker:  198.96.155.3

You can contact us by using: abuse-reply@keyweb.de
```

# Technical

# Technical

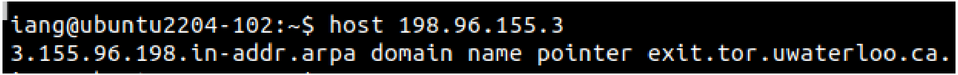
- Machine and network
  - Machine can be pretty much anything
  - Your favourite Linux distro
  - IP address not in a site-licensed space
  - Minimally 1 Mbps networking, but 10–100 Mbps is more reasonable

# Technical

- DNS
  - Use your own DNS recursive resolver, not a public one like 8.8.8.8 or 1.1.1.1

# Technical

- Reverse DNS



```
iang@ubuntu2204-102:~$ host 198.96.155.3
3.155.96.198.in-addr.arpa domain name pointer exit.tor.uwaterloo.ca.
```

# Technical

- SWIP
  - You can set a custom Abuse contact in whois using SWIP, for a range of addresses as small as 3 bits (/29, or 8 addresses)
  - You really should do this, so that you get the Fail2Ban reports, and importantly, your upstream provider *doesn't*.

# Technical

- Exit policy
  - Decide what protocols (technically, ports) you do and do not want exiting your node.
  - Minimally allow ports 80 and 443.
  - There is a standard Tor "Reduced Exit Policy" that's a good place to start.
  - If individual server operators don't want connections from your Tor exit node, then can ask you to add their IP addresses to the deny list in your exit policy.

# Takeaways

- Tor is used by millions of people around the world every day to protect their privacy online
- By running a Tor node (especially an exit node), you can help promote privacy and freedom of expression around the world
- Added benefits if you do research on Tor and related topics