Remaining Anonymous

Osman Surkatty
surkatty.org / @surkatty

Full Disclosure

- I’m a person, not representing a company.
- Information here is for educational purposes.
- What you do with it, is your problem.

Overview

- What?
- Why?
- How?
- Tools

Plausible Deniability

Surfing anonymously

Anonymity

Why?

- Political harassment
- Threats to livelihood
- and...

Tinfoil

How?

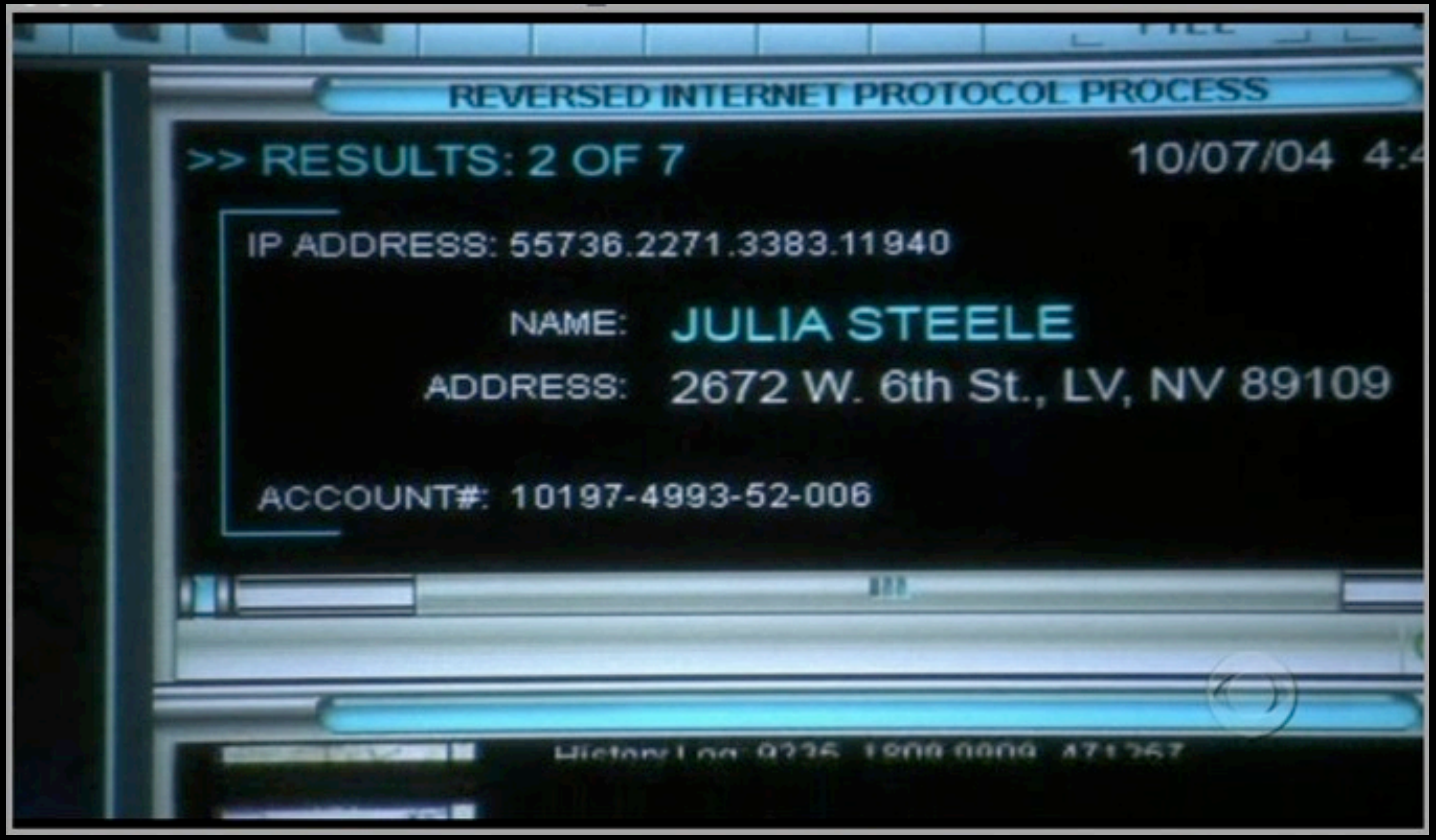
- Wiretapping / Dragnet surveillance
- Forensic analysis
- Online tracking
- Metadata

Dragnet

- Syrian government
- US government and commercial cooperation
- OSINT Monitoring

Forensic Analysis

- 9/11 <- tinfoil
- Encryption? Or fauxscription
- COFEE



REVERSED INTERNET PROTOCOL PROCESS

>> RESULTS: 2 OF 7 10/07/04 4:4

IP ADDRESS: 55736.2271.3383.11940

NAME: JULIA STEELE

ADDRESS: 2672 W. 6th St., LV, NV 89109

ACCOUNT#: 10197-4993-52-006

History Log 9235 1800 0909 471267

COFEE

(Computer Online Forensics Evidence Extractor)

- Description: Easily capture important "live" computer evidence at the scene of in cybercrime investigations, without special forensics expertise.
- "Microsoft has been pouring free COFEE to law enforcement since at least mid-2007." - The Register
- "...a job that previously took 3 hours, now can be done in 20 minutes with COFEE" - Wikipedia
- Remains available today on Wikileaks and Torrent sites

COFEE

(Computer Online Forensics Evidence Extractor)

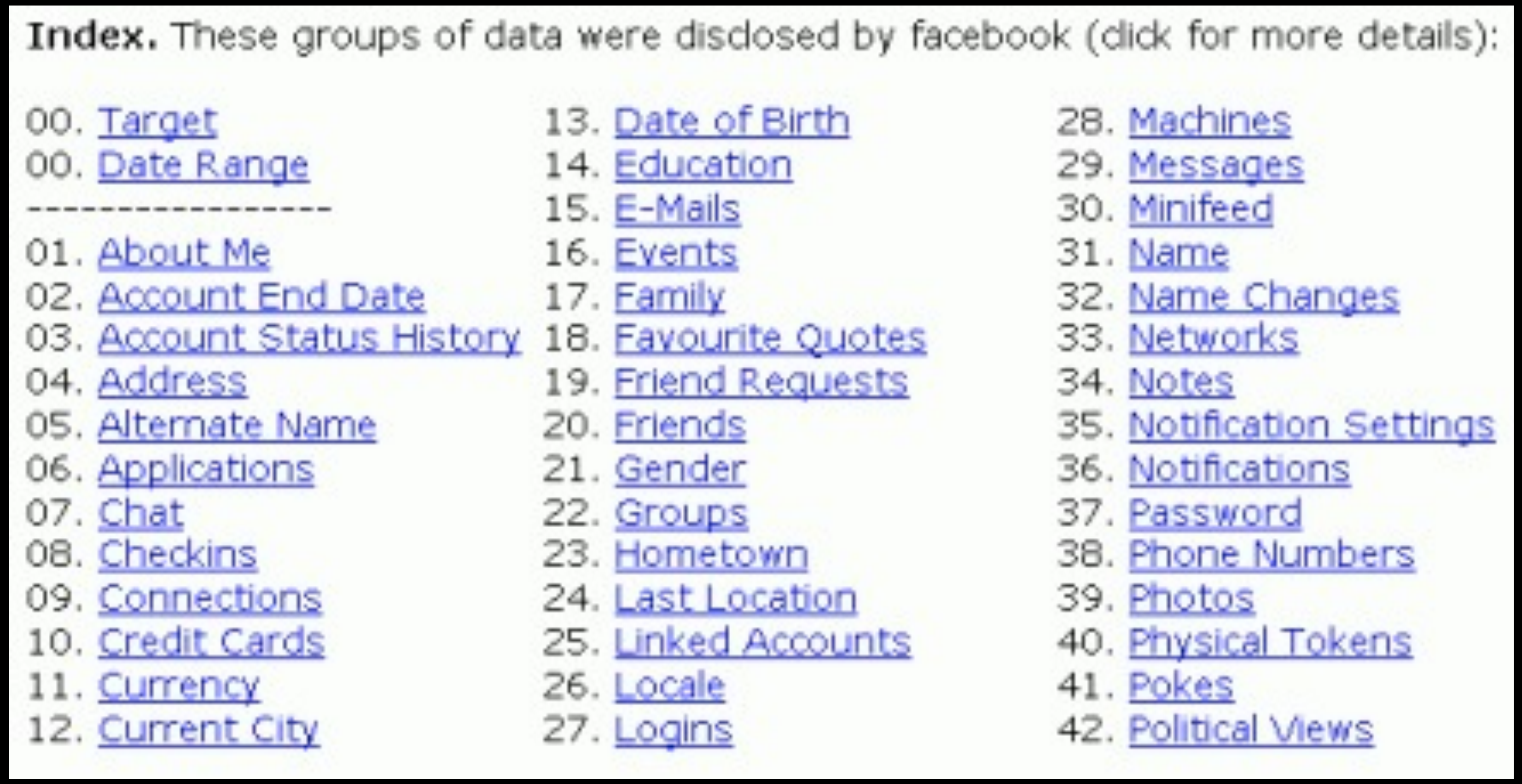
- Tools in COFEE:
  - netstat.exe
  - tasklist.exe
  - ipconfig.exe
  - whoami.exe
  - ...and about ~~1337~~ 146 other programs

Online Tracking

- Data brokers
- Tracking / Super cookies
- Misc tracking

Online Tracking

- Data brokers
  - Over 234 known data brokers; Only half allow opting-out
  - Facebook (a CIA program), biggest of them all



Index. These groups of data were disclosed by facebook (click for more details):

00. Target
00. Date Range
----
01. About Me
02. Account End Date
03. Account Status History
04. Address
05. Alternate Name
06. Applications
07. Chat
08. Checkins
09. Connections
10. Credit Cards
11. Currency
12. Current City
13. Date of Birth
14. Education
15. E-Mails
16. Events
17. Family
18. Favourite Quotes
19. Friend Requests
20. Friends
21. Gender
22. Groups
23. Hometown
24. Last Location
25. Linked Accounts
26. Locale
27. Logins
28. Machines
29. Messages
30. Minifeed
31. Name
32. Name Changes
33. Networks
34. Notes
35. Notification Settings
36. Notifications
37. Password
38. Phone Numbers
39. Photos
40. Physical Tokens
41. Pokes
42. Political Views

Online Tracking

- Cookies:
  - Tracking cookies (Google Analytics, KissMetrics)
  - Flash cookies (KissMetrics/DoubleClick)
  - Super cookies (KissMetrics/QuantCast/ClearSpring)

Online Tracking

- Misc tracking:
  - Browser attributes
  - Toolbars
  - IP Address
  - Metadata
  - and more

Demo!

- How unique are you? http://panopticlick.eff.org/
- Cookie?

How to track someone

- Put a tap on their connection
- Analyze their devices or identities
- Buy it
- Actively put beacons on them

How to defend yourself (tools)

Risk assessment

Risk assessment

- Who?
- What?
- When?
- Why?
- How?

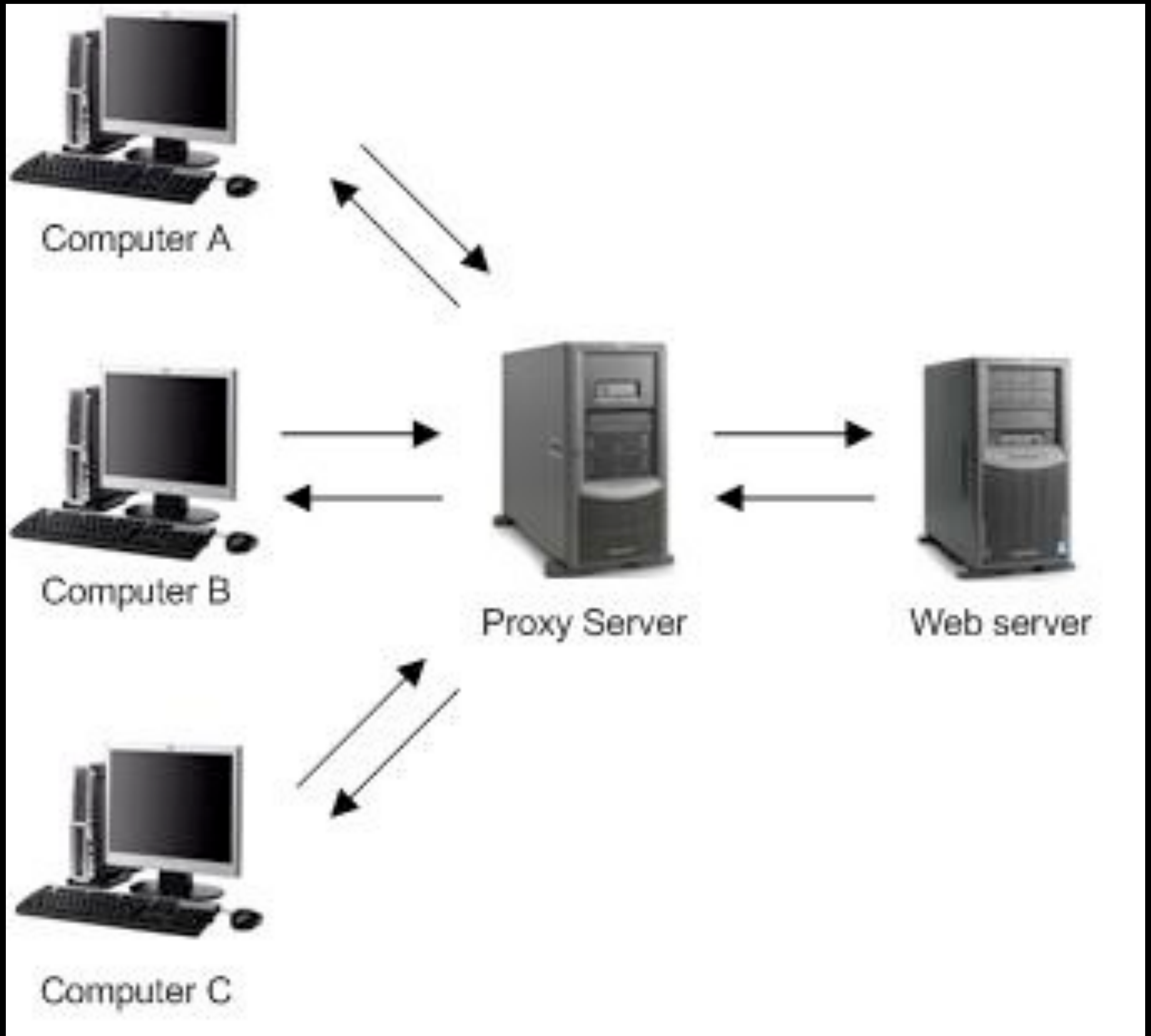
Dragnet

- ~~You’re fucked~~ Try harder
- Obfuscate and/or bypass

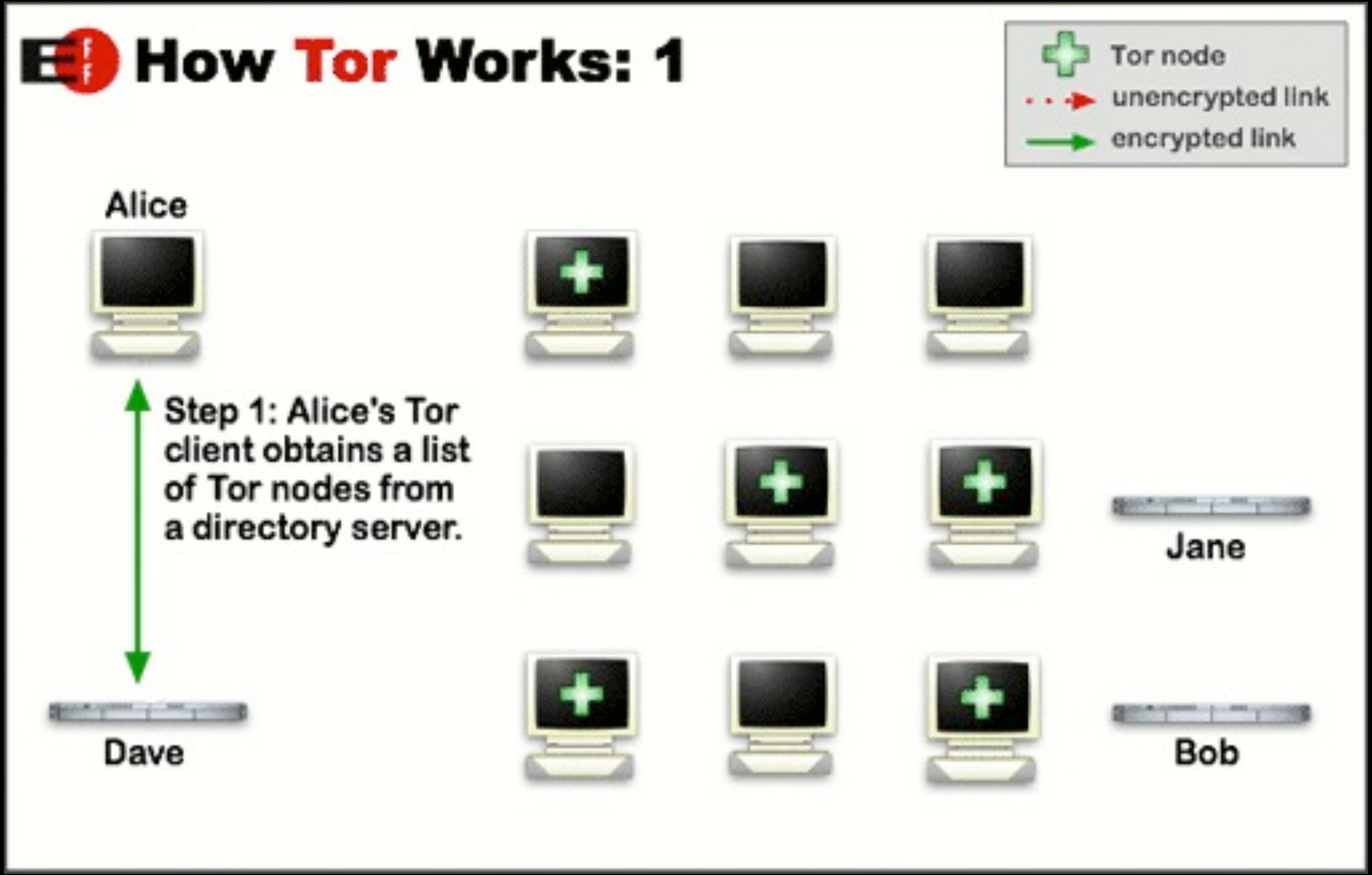
Dragnet

- Proxies: Tor
- Encryption: SSH, SSL, PGP/GPG, OTR

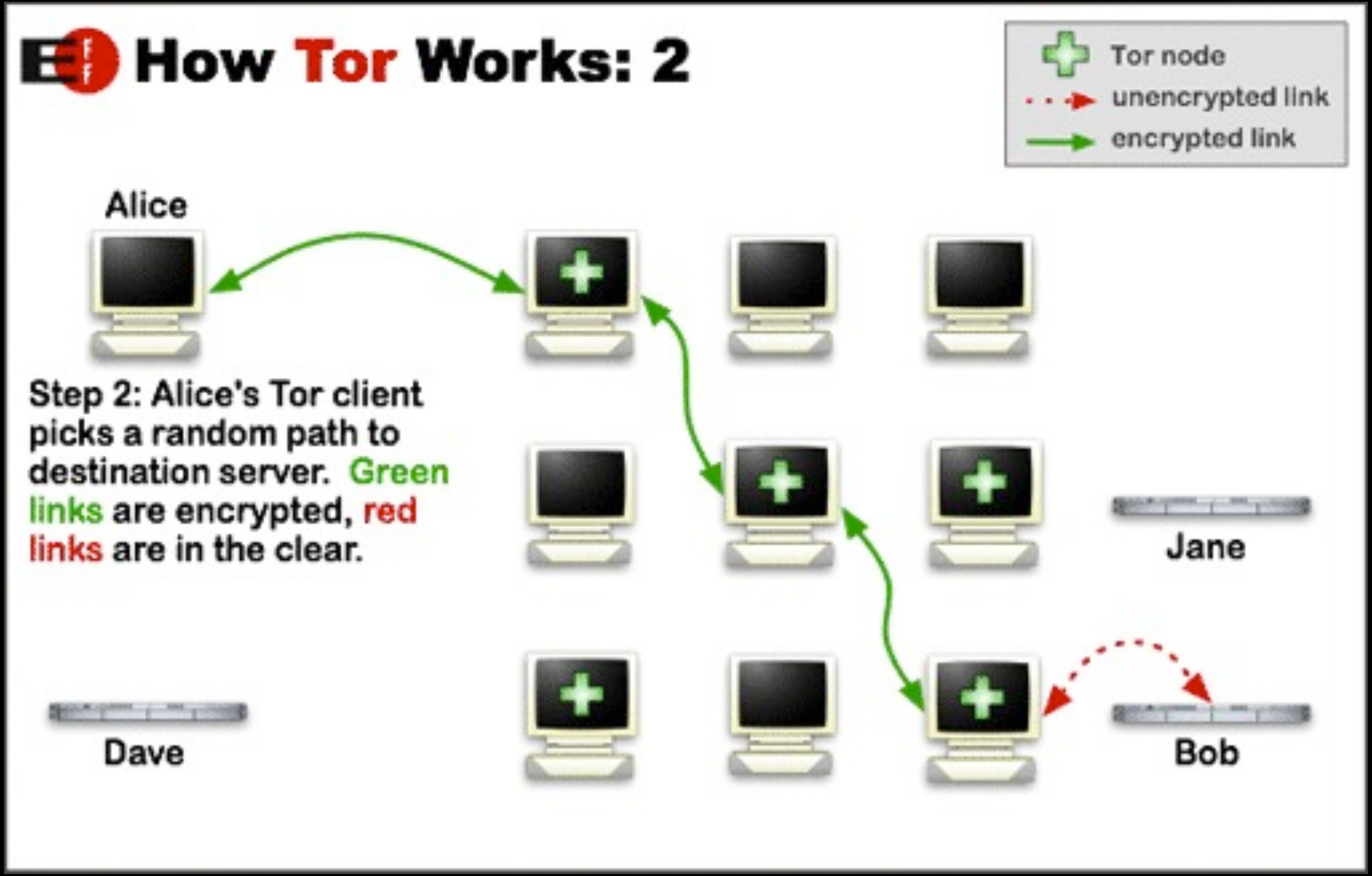
Proxies 101



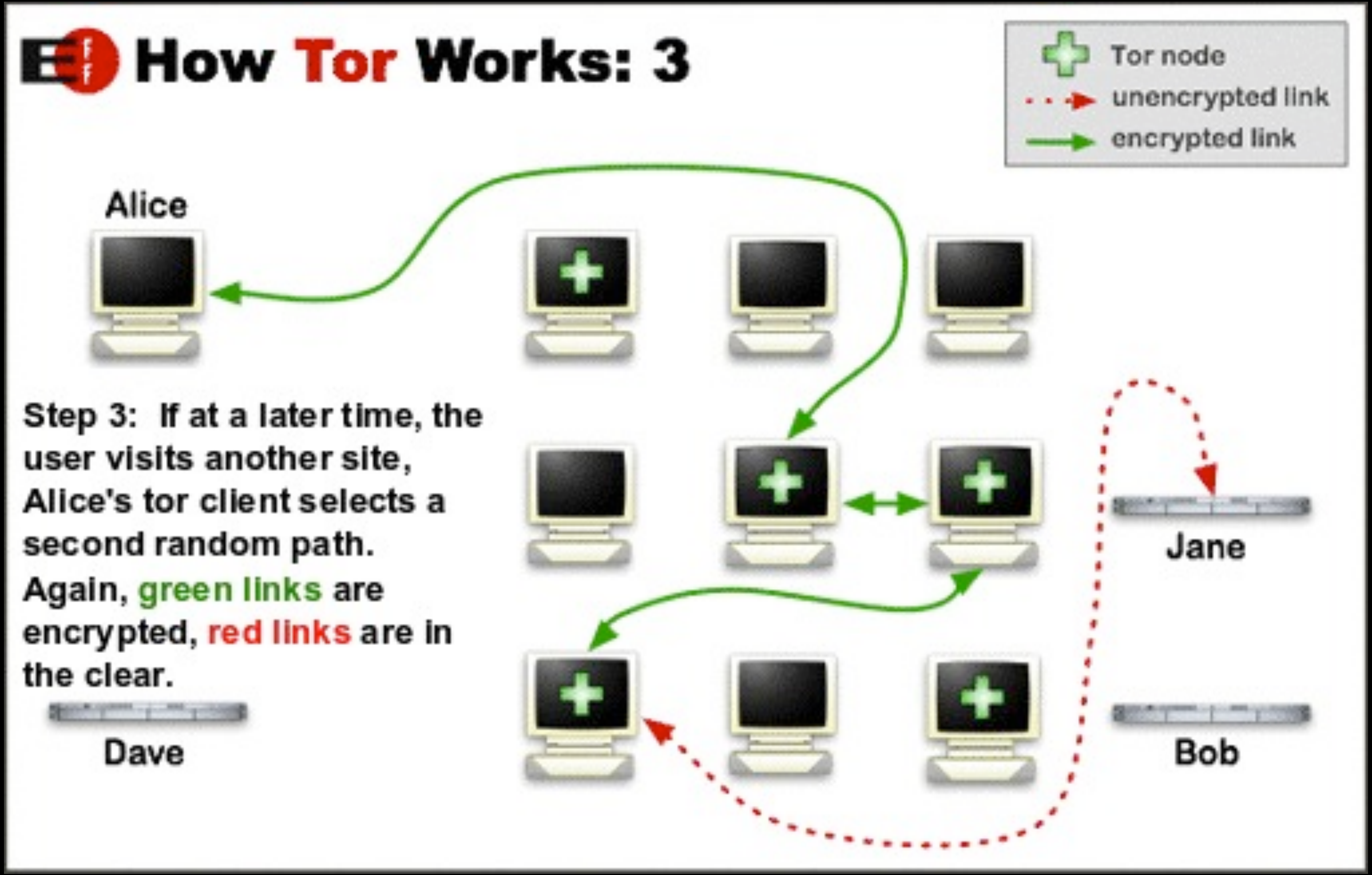
Tor


EFF
How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob

Tor


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Tor



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 links are encrypted, red links are in the clear.

Tor Demo!

- Goal: Install the Tor Browser Bundle from:
  - https://torproject.org/download/

OTR

(Off-the-record)

- OTR allows you to have private conversations over instant messaging.
  - Not to be confused with Google Talk's OTR!
- It provides encryption, authentication, deniability, and forward secrecy for *some* chat clients

So, now we’re safe right?

- Nope.
  - Tor security patches
  - HideMyAss reveals ass
  - OTR, Audium, and Pidgin audit by EFF

Anti-Forensics

- !obfuscate && !bypass
- erase! (and do so properly)

Step 1: ???

Step 1: You're fucked.

Example scenario

- Purchased laptop from BestBuy
- Formatted HD
- Installed fresh copy of Windows
- Installed office program
- Linked printer, webcam, and other peripherals
- Password protected it!

Nope, still fucked.

Purchasing

- BestBuy:
  - Security camera
  - Credit card transaction
  - Warranty information
  - Rewards program

Formatting

- Fresh copy of windows:
  - Left traces from not wiping
  - Entered name into Windows
  - Registered Windows
  - Inherit security flaws with Windows (Sorry MS!)

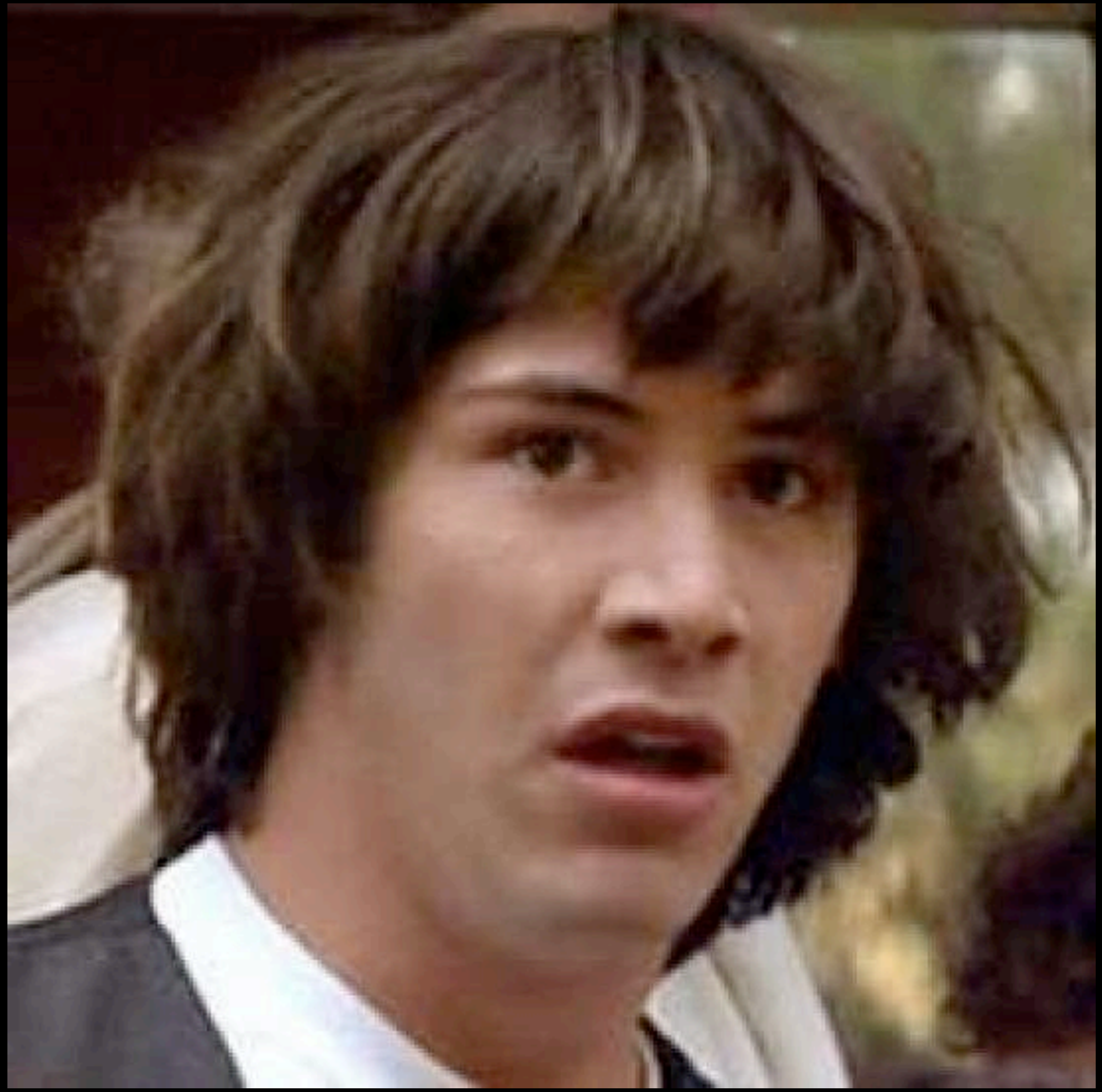
Programs & Peripherals

- Installed Office
- Installed web browser
- Installed printer

Password protected

- Hash dump
- Password reuse

So how do I protect myself?



Anti-Forensics

- “Anti-forensics is more than technology. It is an approach to criminal hacking that can be summed up like this: Make it hard for them to find you and impossible for them to prove they found you.” - The Rise of Anti-Forensics, by Scott Berinato

Anti-Forensics

- Covering/obfuscating your tracks.
- Wiping your tracks (Thermite or overwriting)

Encryption

- Anti-forensics second biggest hope = Encryption
- Encryption was the best thing we had going.
- Well, until recently: Court rulings and border searches.

Data Brokers

Data Brokers

- Manually opt-out (don’t laugh too hard)
- Tools:
  - NoScript
  - AdBlock Plus
  - Disconnect

Browser

- Many choices, near infinite ways to configure
- Suggestion: Firefox
- Main config items: privacy-mode, cookies, cache, history, certificate authorities, and addons.
- ....or Tor Browser Bundle

Browser Demo!

- Goal: Tighten up the privacy within your browser

So, now we're safe right?

- Nope
  - LEO and court subpeonas
  - Password reuse
  - Supercookies
  - Leaky/Insecure plugins

Communicate anonymously?

Anonymous/Secure Communication

- Real-time
  - OTR / IM
  - IRC
- Relayed
  - Temporary email
  - Anonymous remailers

Demo Time!

- Find a temporary email provider
- Send an email to osman@surkatty.org

...so now I’m secure right?

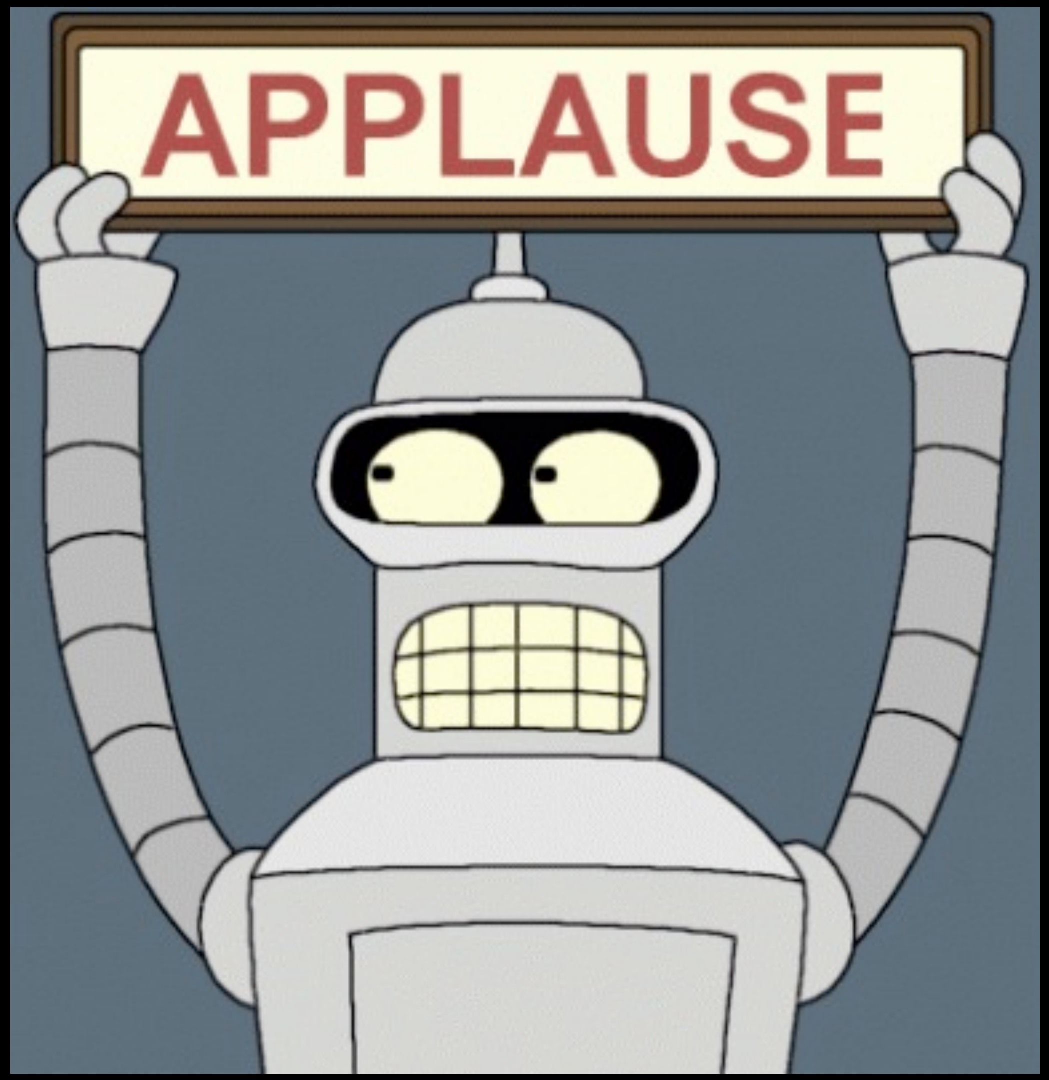
Anonymous/Secure Communication

- Real-time
  - OTR / IM = Broken protocols, security bugs, logs
  - IRC = IP, logs
- Relayed
  - Temporary email = Monitored, one-way, logs
  - Anonymous remailers = Monitored, one-way, logs

Will I <u>ever</u> be anonymous?

Short answer: No

Thanks!



- Questions? Email osman@surkatty.org

Questions?