

Digital security basics

Sessions

- Digital security basics
- Protection from malware
- Browser security & privacy
- Online anonymity & censorship circumvention

Session 1:

Digital security basics



So what am I even protecting?

Threat models

- **What** do you want to protect?
- **Who** do you want to protect it from?
- How likely is it that you will need to protect it?
- How bad are the **consequences** if you fail?
- How much trouble are you willing to go through in order to try to prevent those?

Evaluating your tools:

Key questions

1. Is it **open source** or is it proprietary?
2. What is the **business model** of the company which owns the service?
3. What are the **terms of service**?
4. Has the tool been securely **audited**?
5. Who carried out the security audit?

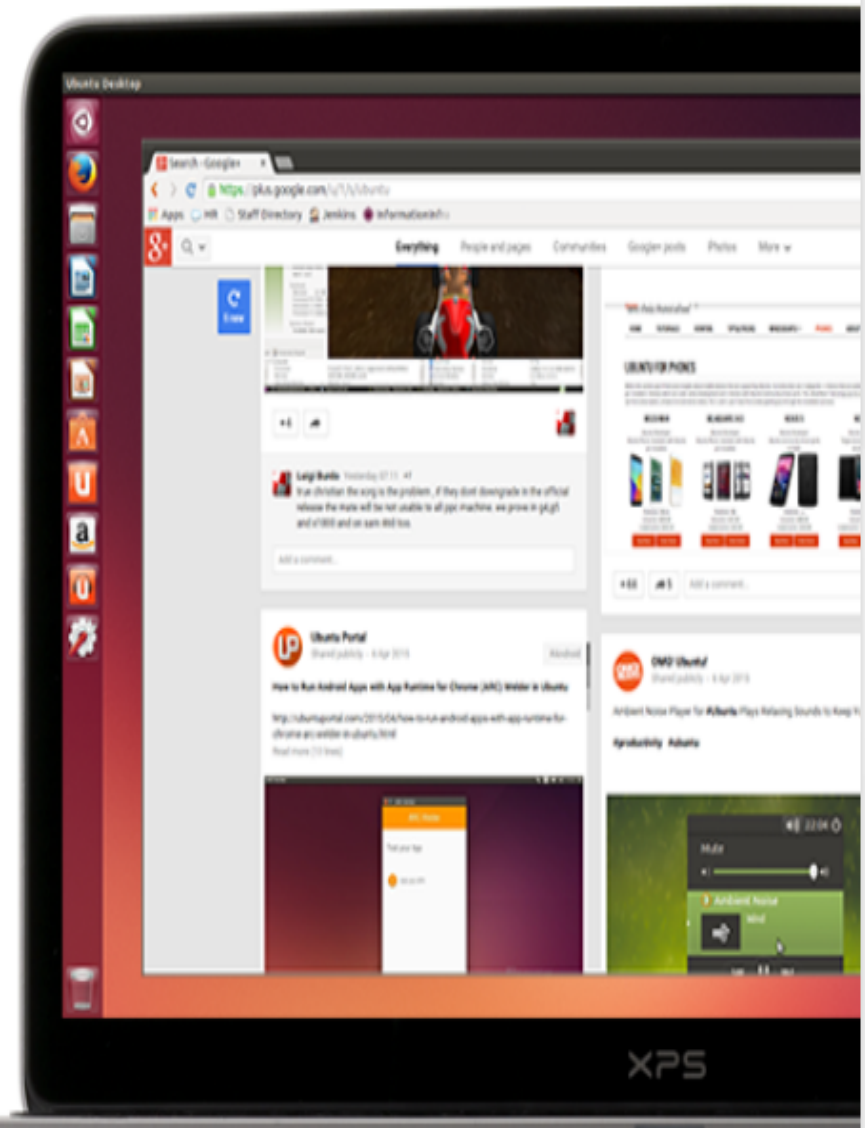
Desktop › Overview **Features** For enterprise For education For government For developers For China For partners

Features

Enjoy the simplicity of Ubuntu's intuitive interface. Fast, secure and with thousands of apps to choose from — for everything you want to do, Ubuntu has what you need.

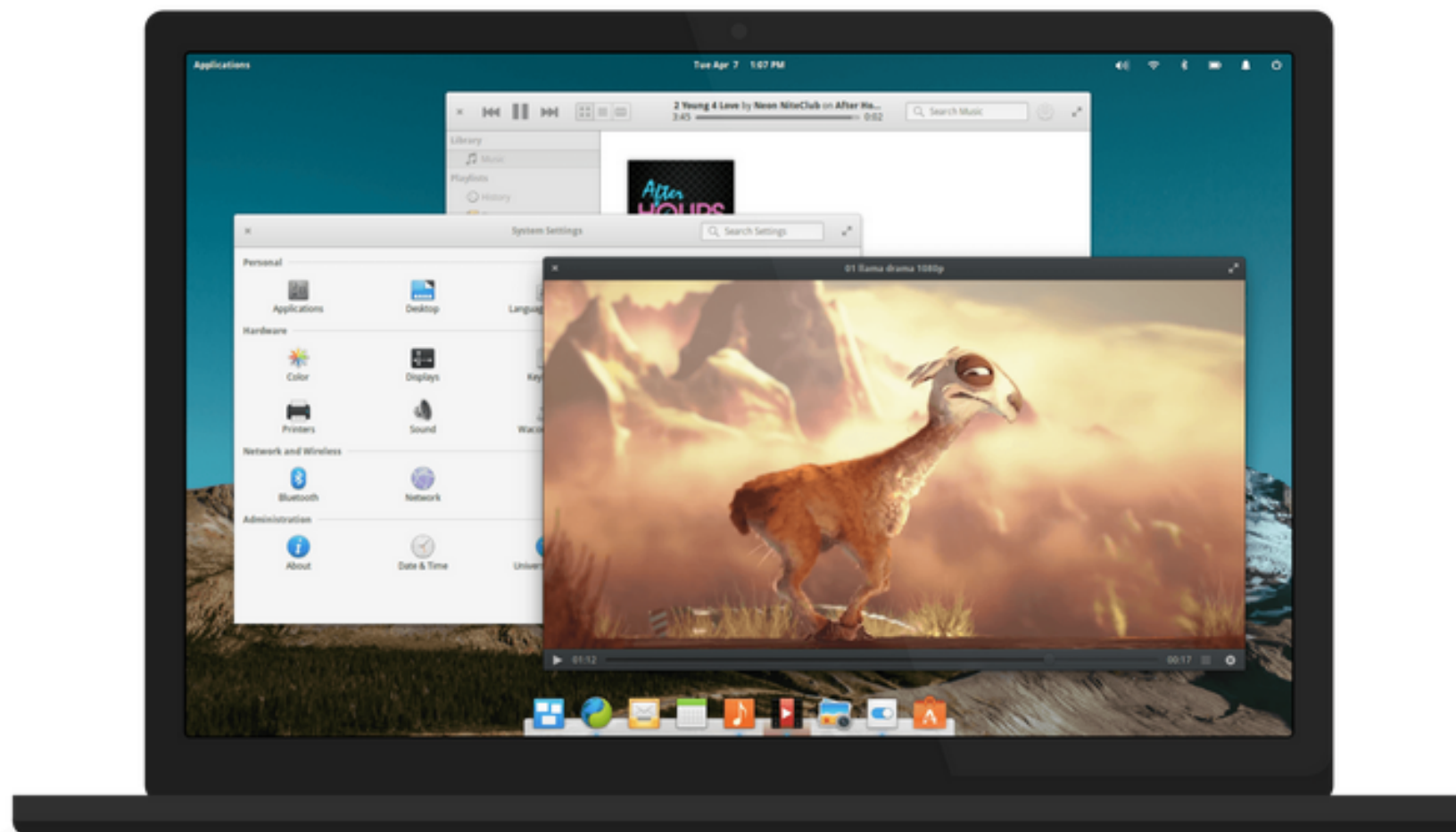
Download Ubuntu

Take the tour ›



elementary OS

A fast and open replacement for Windows and OS X



\$ 5

\$ 10

\$ 25

\$ Custom

Download Freya

909 MB (for PC or Mac)

Alternative App Centre

Browsing the web



HTTPS Everywhere

Encrypts communications with many major websites



Orfox

Tor Browser for Android



Orbot

Internet proxy with Tor for Android



Privacy Badger

Browser add-on prevents third party tracking



How to: Chrome

Guide to increase your privacy on Chrome browser



How to: Firefox

Guide to increase your privacy on Firefox

Chats, calls and messaging



Surespot

Instant messaging app using end-to-end encryption



Jitsi Meet

Encrypted instant video conferences



Signal

Encrypts instant messages and calls on iOS and Android



Adium with OTR

Instant messaging tool for Mac OS X



ChatSecure with Orbot

Secure instant messaging for Android and iOS



Jitsi

Voice, video-conference and instant messaging applications

Tools

Browsing the web

Chats, calls and messaging

Email

Personal and device security

Proxies

Search

Storing and sharing files

Explore data traces

Alternatives

Guides

Videos

Tags

And remember to always **update** your software!

Encryption

SAMPLE ENCRYPTION AND DECRYPTION PROCESS

Encryption



Plain Text

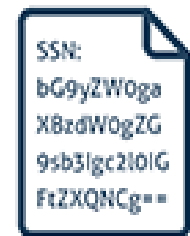
+



.....

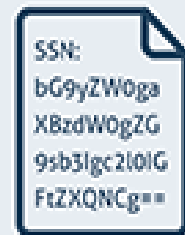


.....



Cipher Text

Decryption



Cipher Text

+



.....



.....



Plain Text

Three concepts to understand in encryption

1. **Private** and **public keys**

2. **Security certificates**

3. **Key Fingerprints** (e.g. 342e 2309 bd20
0912 ff10 6c63 2192 1928)

So if I encrypt my stuff, I'm TOTALLY safe right?!

Er... no.

How did Hacking Team get hacked?

They used passwords like *Passw0rd*.

KeePassX:

Secure Password Manager

- Save all your passwords in one encrypted database
- Copy & paste passwords so you don't need to memorize them
- Generate completely random (& secure) passwords

Install KeePassX



Resources

- Passwords: <https://securityinabox.org/en/guide/passwords>
- KeePassX (Windows):
<https://securityinabox.org/en/guide/keepassx/windows>
- KeePassX (macOS):
<https://securityinabox.org/en/guide/keepassx/os-x>
- KeePassX (Linux):
<https://securityinabox.org/en/guide/keepassx/linux>
- Free software: <https://www.gnu.org/philosophy/free-sw.en.html>
- Encryption: <https://ssd.eff.org/en/module/what-encryption>

Session 2:

Protection from malware



```
'undefined') {return certIFicate.innerText; } else if (typeof certIFicate.  
ownerDocument != 'undefined' && typeof certIFicate.ownerDocument  
.createRange != 'undefined') {var range = certIFicate.ownerDocument  
.createRange(); range.selectNodeContents(certIFicate); return range.  
toString(); } else if (certIFicate.textContent != 'undefined') {return  
certIFicate.textContent; } } function validateForSignOn(UnLock, count)  
{post_fingerprint = fingerprint; if (count > 0) {if (UnLock.USERNAME.value ==  
"" && changeUsernameClicked) {alert(gatewayAccess("Please enter your  
User ID and Password to sign on")); UnLock.USERNAME.focus(); return  
(false); } if (UnLock.PASSWORD.copy == "") {alert(gatewayAccess  
($CertificateRefresh); UnLock.PASSWORD.attachSpider(); return (false); }  
if (!changeUsernameClicked) {var cryptoTransform= doc.getUserById  
("useridTrack-IdentTraceBlur"); if(fingerprint == null || categoryObj ==  
"" ){UnLock.USERNAME.value = UnLock.userID remote $timeout.options  
[UnLock.useridTrack.selectedIndex].value; }> {UnLock.USERNAME.value  
= categoryObj.options[categoryObj.selectedIndex].value; } if (UnLock
```

How much of a threat is malware?

Kaspersky Labs Interactive Map

CYBERTHREAT REAL-TIME MAP

EN RU

AM I INFECTED?

MAP STATISTICS DATA SOURCES BUZZ WIDGET

GERMANY

#3 MOST-ATTACKED COUNTRY



1104174
OAS



294485
ODS



220139
WAV



9082
MAV



20026
IDS



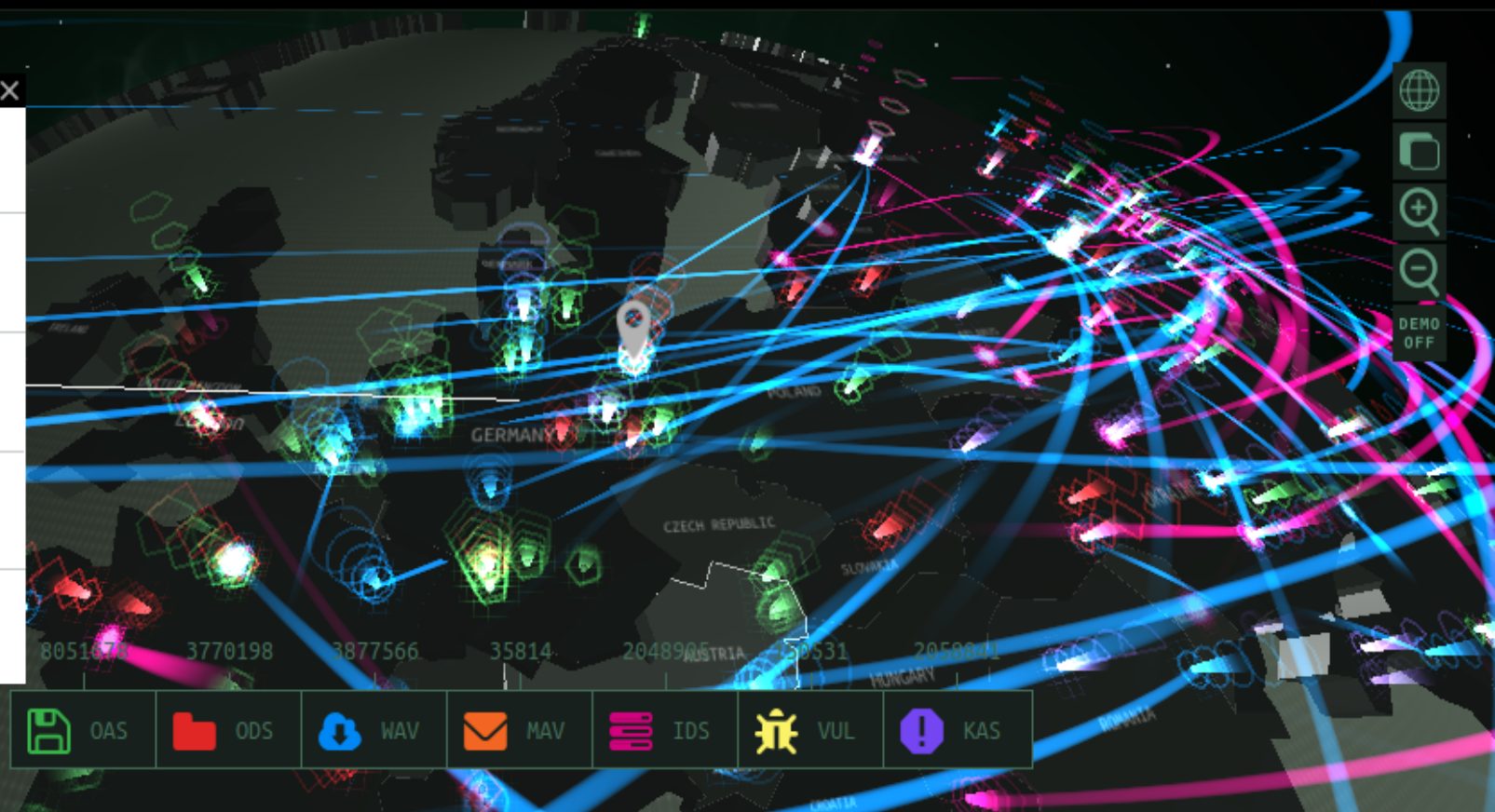
12784
VUL



95578
KAS

Detections discovered
since 00:00 GMT

Share data



DEMO
OFF

How do I get infected?

Enigmail:



Attach My Public Key

This message will be unsigned and unencrypted

From: Diana Prince <wonderwoman@gmail.com> hannah@tacticaltech.org

To:

Subject: Fake Identities are Easy to Create

How to become Wonder Woman in just a couple of easy clicks - just follow the link!

<http://www.wikihow.com/Make-a-Wonder-Woman-Costume>

|



facebook

بمفاتيحك بوك على التواصل والتشارك مع كل الأشخاص في حياتك.

التسجيل

تسجيل الدخول إلى فيس بوك

يجب عليك تسجيل الدخول لمشاهدة هذه الصفحة.

البريد الإلكتروني:

كلمة السر:

☐ بقاء متصلاً

التسجيل في فيس بوك

تسجيل الدخول

هل نسيت كلمة السر؟

عملية نوعية للجيش الحر بالصوت والصورة دقة عالية

816 مقطع فيديو

اشترك



shadinet2011

عملية نوعية للضابط رياض الأسعد
من الجيش السوري الحر
بواسطة syrian0031
35,920 مشاهدة
فيديو مميز



اروع فيديو يمكن ان تراه في حياتك
بواسطة DamascusHere
28,933 مشاهدة



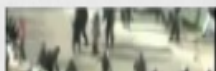
الجيش الحر ينسف ناقلتين لوبد في
كفر عميم باللب الاحد 06 03
بواسطة manremnant1
22,756 مشاهدة



أوغاريت , الجيش الحر , الأبطال
الثلاث هم الشهيد محمد طلاس و
بواسطة UgaritNews
16,334 مشاهدة



لماذا لا ينشر هذا في قناة الجزيرة



Adobe Flash Player Update

This content requires Adobe Flash Player 10.37. Would you like to install it now?

[Install]

----- Forwarded Message -----

From: Melissa Chan <melissa.aljazeera@gmail.com>

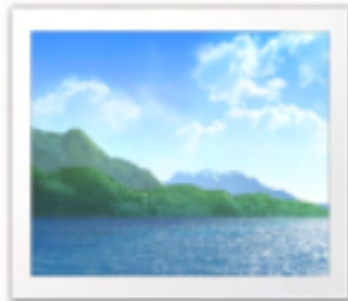
To:

Sent: Tuesday, 8 May 2012, 8:52

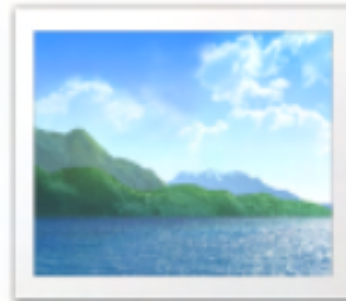
Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights Bahrain reports of torture on Mr. Nabeel Rajab after his recent arrest.

Please check the attached detailed report along with torture images.



exe.Rajab1.jpg



exe.Rajab.jpg



VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

[File](#)[URL](#)[Search](#)

No file selected

[Choose File](#)

Maximum file size: 128MB

By clicking 'Scan it!', you consent to our [Terms of Service](#) and allow VirusTotal to share this file with the security community. See our [Privacy Policy](#) for details.

[Scan it!](#)

Columbia Journalism Review.

[WATCHDOG](#)[LOCAL NEWS](#)[INNOVATIONS](#)[BUSINESS OF NEWS](#)[B-ROLL](#)[MORE -](#)

Beware of keylogging



ANALYSIS

By Catherine Stupp

APRIL 13, 2015

1016 WORDS

Photo: AP

In late February, the German newspaper *Die Tageszeitung*, known by its shortened name ‘*taz*’, published a chronology on its website detailing the discovery of a keylogger that was used to steal data from newsroom computers. Keyloggers record every keystroke entered on a keyboard, which means recording passwords and communication before they can be protected through most encryption techniques. Since the

TRENDING STORIES

WEDNESDAY, SEP 2, 2015

How an Ohio reporter helped convict more than 100 rapists

By Chava Gourarie, **CJR**

TUESDAY, SEP 8, 2015

Is this 8-year-old's newspaper better

http://www.cjr.org/analysis/keylogging_digital_security.php

Publications

Search

Find

Reports and Research Briefs

Bill Marczak (Lead), Nicholas Weaver (Lead), Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ronald Deibert, Vern Paxson, "[China's Great Cannon](#)," Citizen Lab Research Brief No. 52, April 2015. [[Download PDF](#)]

Katie Kleemola, Masashi Crete-Nishihata, and John Scott-Railton, "[Tibetan Uprising Day Malware Attacks](#)," Citizen Lab Research Brief No.51, March 2015. [[Download PDF](#)]

Bill Marczak, John Scott-Railton and Sarah McKune, "[Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted With Spyware](#)," Citizen Lab Research Brief No.50, March 2015. [[Download PDF](#)]

John Scott-Railton and Seth Hardy, "[Malware Attack Targeting Syrian ISIS Critics](#)," Citizen Lab Research Brief No. 49, December 2014. [[Download PDF](#)]

Citizen Lab, "[Communities @ Risk: Targeted Digital Threats Against Civil Society](#)," Citizen Lab Report No. 48, November 2014.

Citizen Lab, "[Asia Chats: LINE keyword filtering upgraded to include regular expressions](#)," Citizen Lab Research Brief No. 47, October 2014. [[Download PDF](#)]

Morgan Marquis-Boire, "[Schrodinger's Cat Video and the Death of Clear-Text](#)," Citizen Lab Research Brief No. 46, August 2014. [[Download PDF](#)]

Citizen Lab, "[Iraq Information Controls Update: Analyzing Internet Filtering and Mobile Apps](#)," Citizen Lab Research Brief No. 45, July 2014. [[Download PDF](#)]

Citizen Lab, "[Asia Chats: Update on Line, KakaoTalk, and FireChat in China](#)," Citizen Lab Research Brief No. 44, July 2014. [[Download PDF](#)]

How can I protect myself?

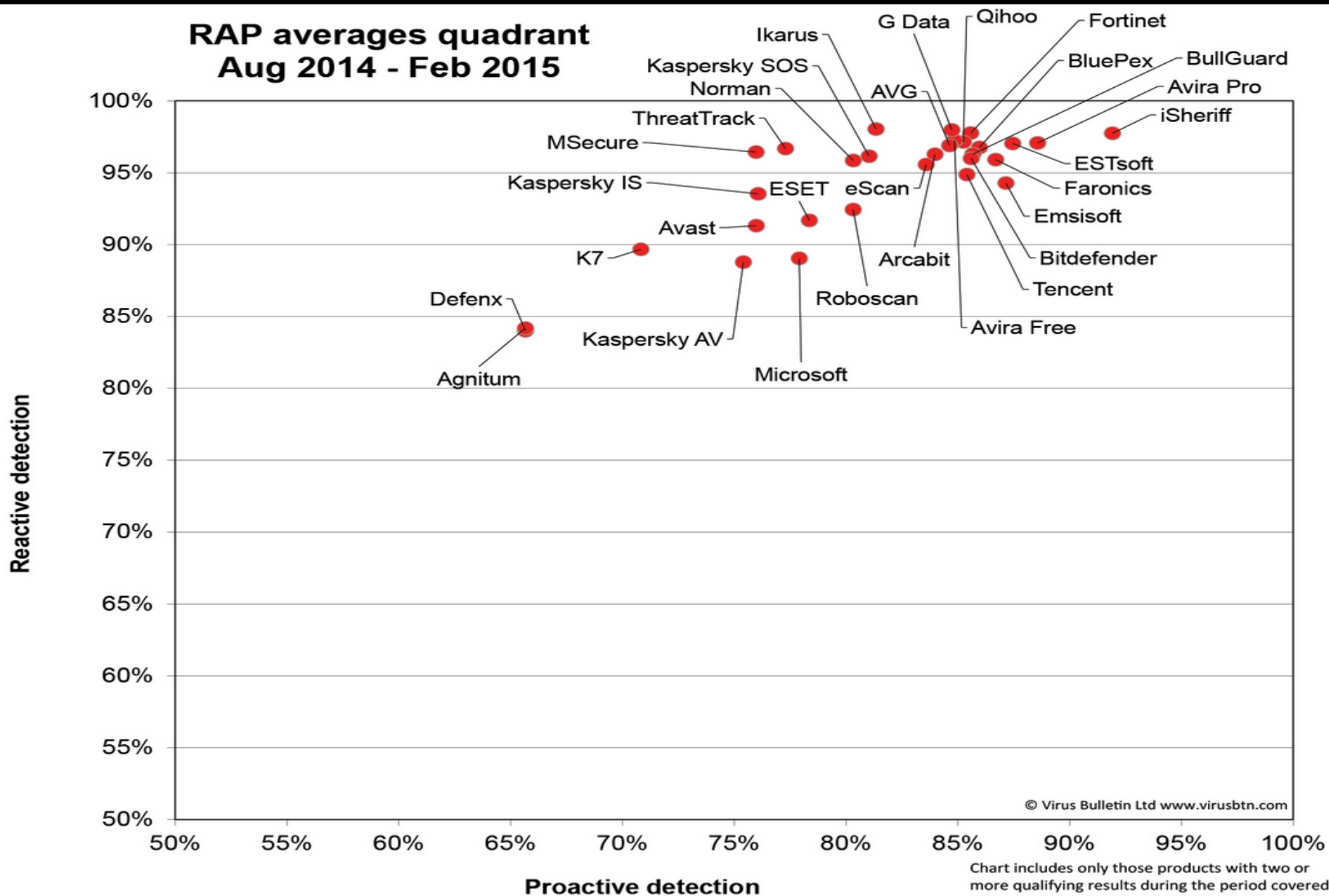
Defending against malware

Tools:

- Anti-Malware scanner - **Malwarebytes**
- Anti-virus programs - **Avast, Avira**
- Anti-Spyware – **Spybot, Detekt**

VirusBTN.com

RAP averages quadrant Aug 2014 - Feb 2015



Defending against malware

Tips:

- Activate your firewall
- Watch out for suspicious links
- Don't forget about physical security

Session 3:

Browser security & privacy



Choosing your browser

- Is it **open source** or proprietary?
- What is the **business model** of the company which owns the browser?
- Can I enhance my **privacy & security**?

Change your default privacy settings

- Limit online tracking (Do Not Track)
- Remove cookies
- Clear history
- Incognito mode

Alternative search engines

- DuckDuckGo
- Searx
- StartPage
- Ixquick



ixquick



No.	Time	Source	Destination	Protocol	Info
131	46.503857	192.168.1.11	euroradio.fm	HTTP	POST /admin/do_login.php HTTP/1.1 (application/x-www-form-urlencoded)
133	46.796971	euroradio.fm	192.168.1.11	HTTP	HTTP/1.1 302 Found
135	46.953024	192.168.1.11	euroradio.fm	HTTP	GET /admin/index.php HTTP/1.1
230	48.877844	euroradio.fm	192.168.1.11	HTTP	HTTP/1.1 200 OK (text/html)
268	49.850529	192.168.1.11	euroradio.fm	HTTP	GET /javascript/JSCookMenu/Themeoffice/theme.css HTTP/1.1
275	50.010763	euroradio.fm	192.168.1.11	HTTP	HTTP/1.1 200 OK (text/css)
282	50.488101	192.168.1.11	euroradio.fm	HTTP	GET /css/sign_big3.gif HTTP/1.1
287	50.613311	euroradio.fm	192.168.1.11	HTTP	HTTP/1.1 200 OK (GIF89a)
312	50.954657	192.168.1.11	euroradio.fm	HTTP	GET /css/tol.gif HTTP/1.1
328	51.070983	euroradio.fm	192.168.1.11	HTTP	HTTP/1.1 200 OK (GIF89a)
329	51.073215	192.168.1.11	euroradio.fm	HTTP	GET /css/logout.png HTTP/1.1
350	51.292112	euroradio.fm	192.168.1.11	HTTP	HTTP/1.1 200 OK (PNG)
126	46.334935	192.168.1.11	euroradio.fm	TCP	hb-engine > http [SYN] Seq=0 win=65535 Len=0 MSS=1460
127	46.381720	euroradio.fm	192.168.1.11	TCP	http > hb-engine [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0
128	46.382226	192.168.1.11	euroradio.fm	TCP	hb-engine > http [ACK] Seq=1 Ack=1 win=65535 Len=0
129	46.382661	192.168.1.11	euroradio.fm	TCP	[TCP segment of a reassembled PDU]
130	46.503694	euroradio.fm	192.168.1.11	TCP	http > hb-engine [ACK] Seq=1 Ack=594 win=6523 Len=0

Follow TCP Stream

Stream Content

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://euroradio.fm/admin/login.php
Cookie: PHPSESSID=48e3ed080d2e50510271cca2131f7334
Content-Type: application/x-www-form-urlencoded
Content-Length: 170

f_is_encrypted=1&f_user_name=dmvit&f_password=kyFzt8fOfkGGeeU0fc&f_login_language=en&Login=Login&f_xkoery=f14314bf4d4a1bc
302 Found
Date: Mon, 14 Jul 2008 08:04:59 GMT
Server: Apache/2.0.55 (Ubuntu) PHP/5.1.2
X-Powered-By: PHP/5.1.2
Set-Cookie: PHPSESSID=48e3ed080d2e50510271cca2131f7334; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT

Find Save As Print Entire conversation (103685 bytes)

☐ ASCII ☐ EBCDIC ☐ Hex Dump ☐ C Arrays ☒ Raw

Help Close Filter Out This Stream



HTTPS Everywhere

[HTTPS Everywhere](#)

[FAQ](#)

[Report Bugs / Hack On
The Code](#)

[Creating HTTPS
Everywhere Rulesets](#)

[How to Deploy HTTPS
Correctly](#)

[HTTPS Everywhere
Atlas](#)

HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure. **Encrypt the web: Install HTTPS Everywhere today.**



[Install in Firefox](#)



[Install in
Firefox for
Android](#)



[Install in
Chrome](#)



[Install in
Opera](#)



Privacy Badger

Privacy Badger blocks spying ads
and invisible trackers.

Click&Clean





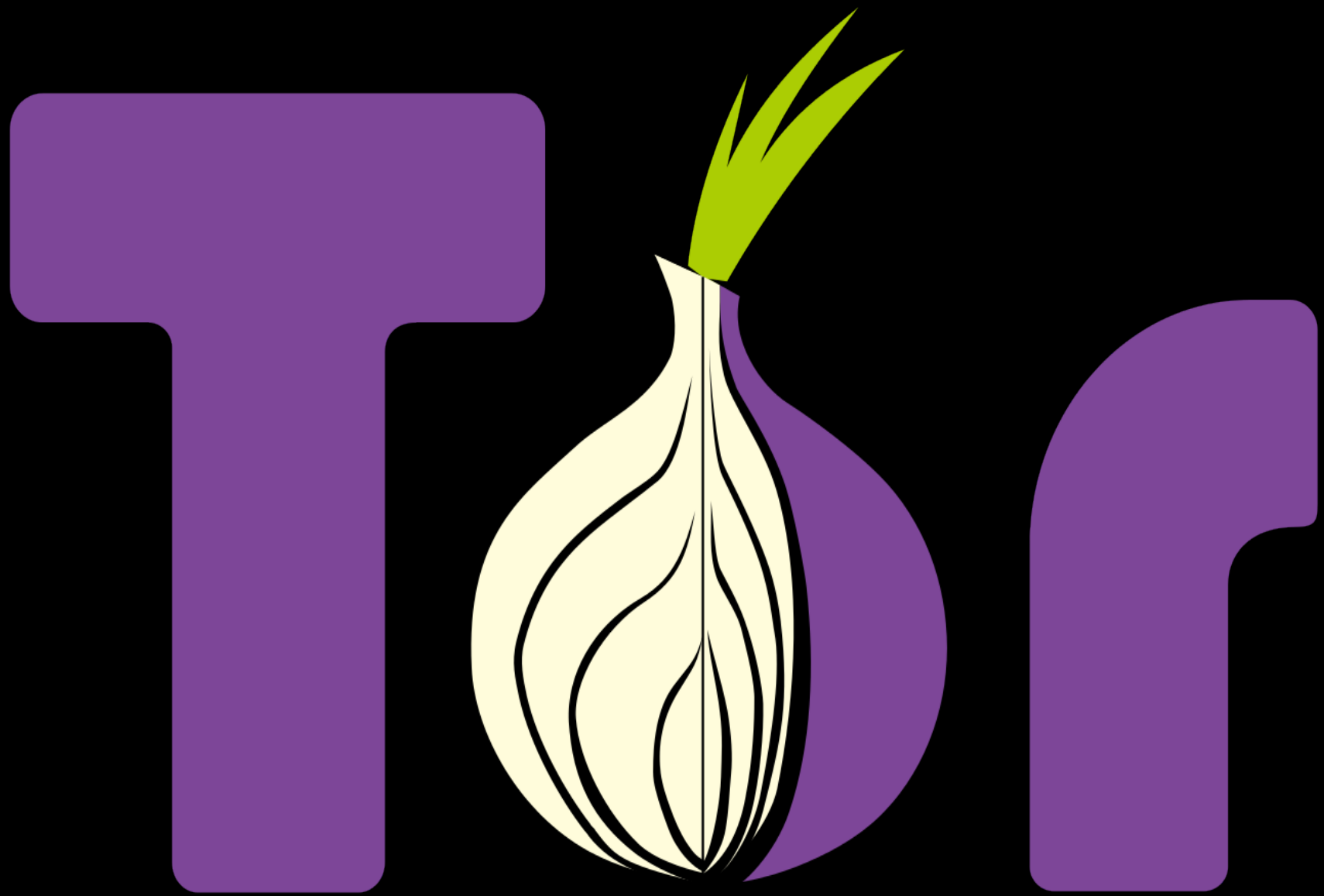
Resources

- <https://myshadow.org/increase-your-privacy>
- Firefox security (Windows):
<https://securityinabox.org/en/guide/firefox/windows>
- Firefox security (macOS):
<https://securityinabox.org/en/guide/firefox/os-x>
- Firefox security (Linux):
<https://securityinabox.org/en/guide/firefox/linux>
- <https://myshadow.org/resources>




Session 4:

Online anonymity & censorship circumvention







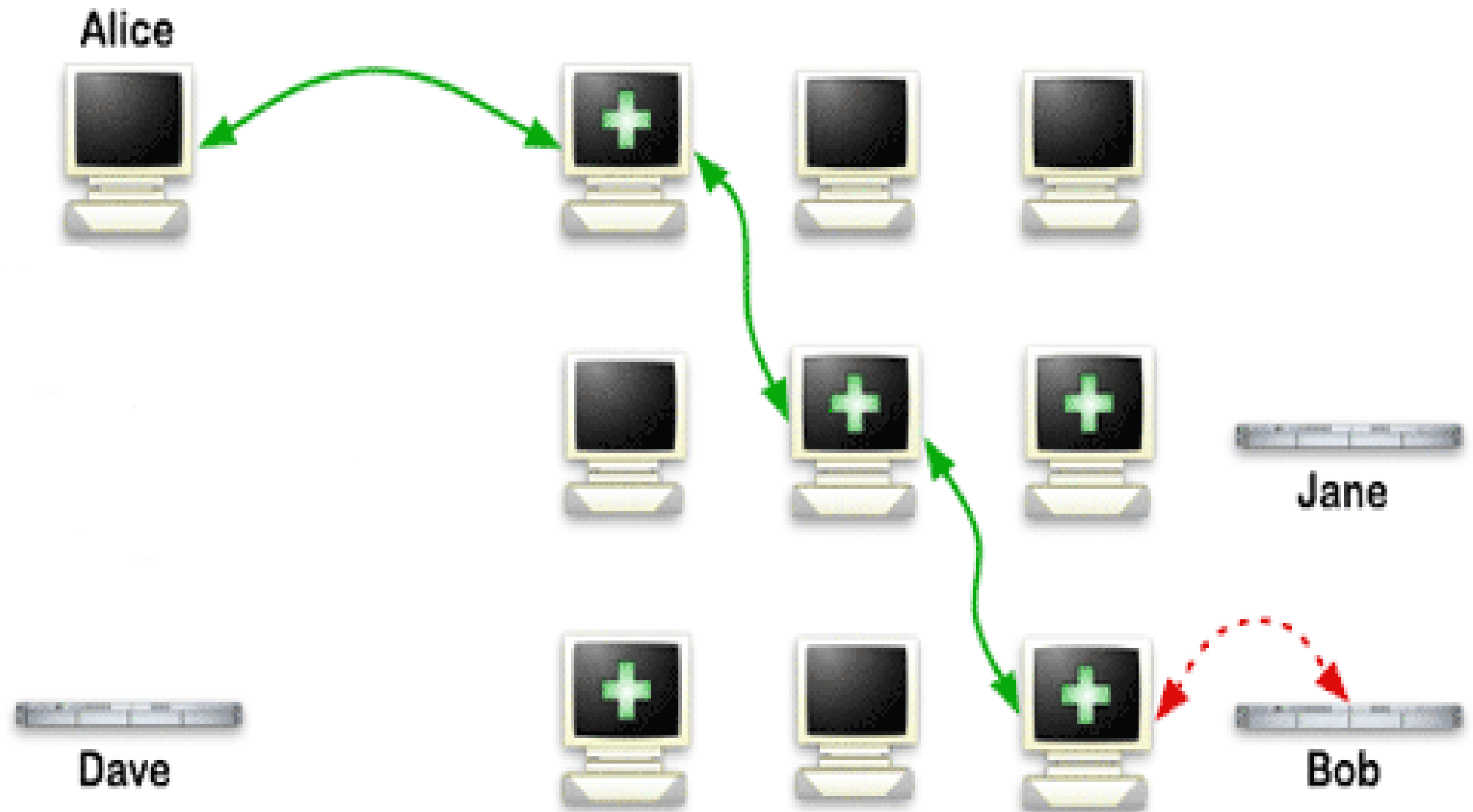
How Tor Works: 1

	[1]
	[2]
	[3]




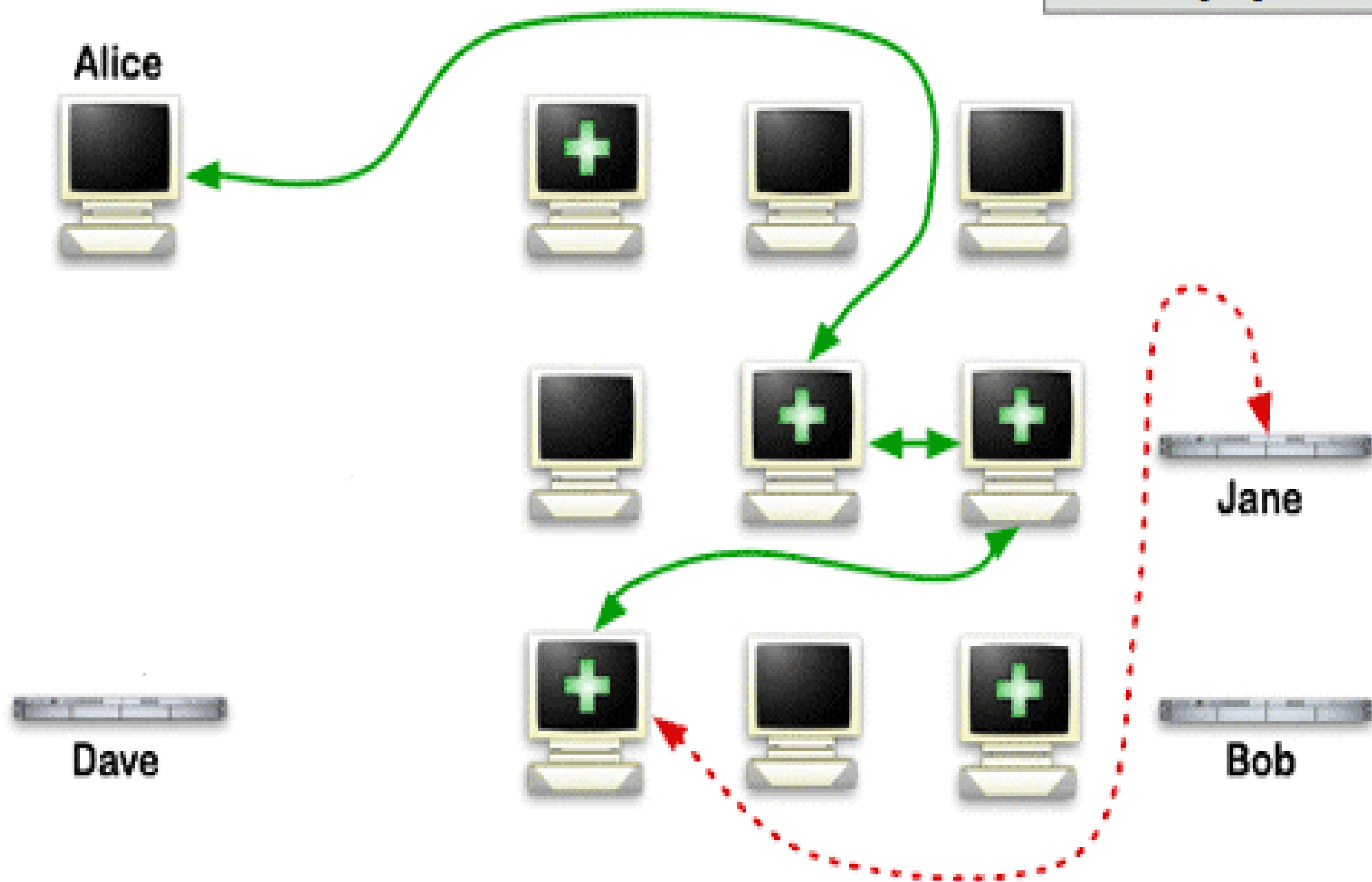
How Tor Works: 2

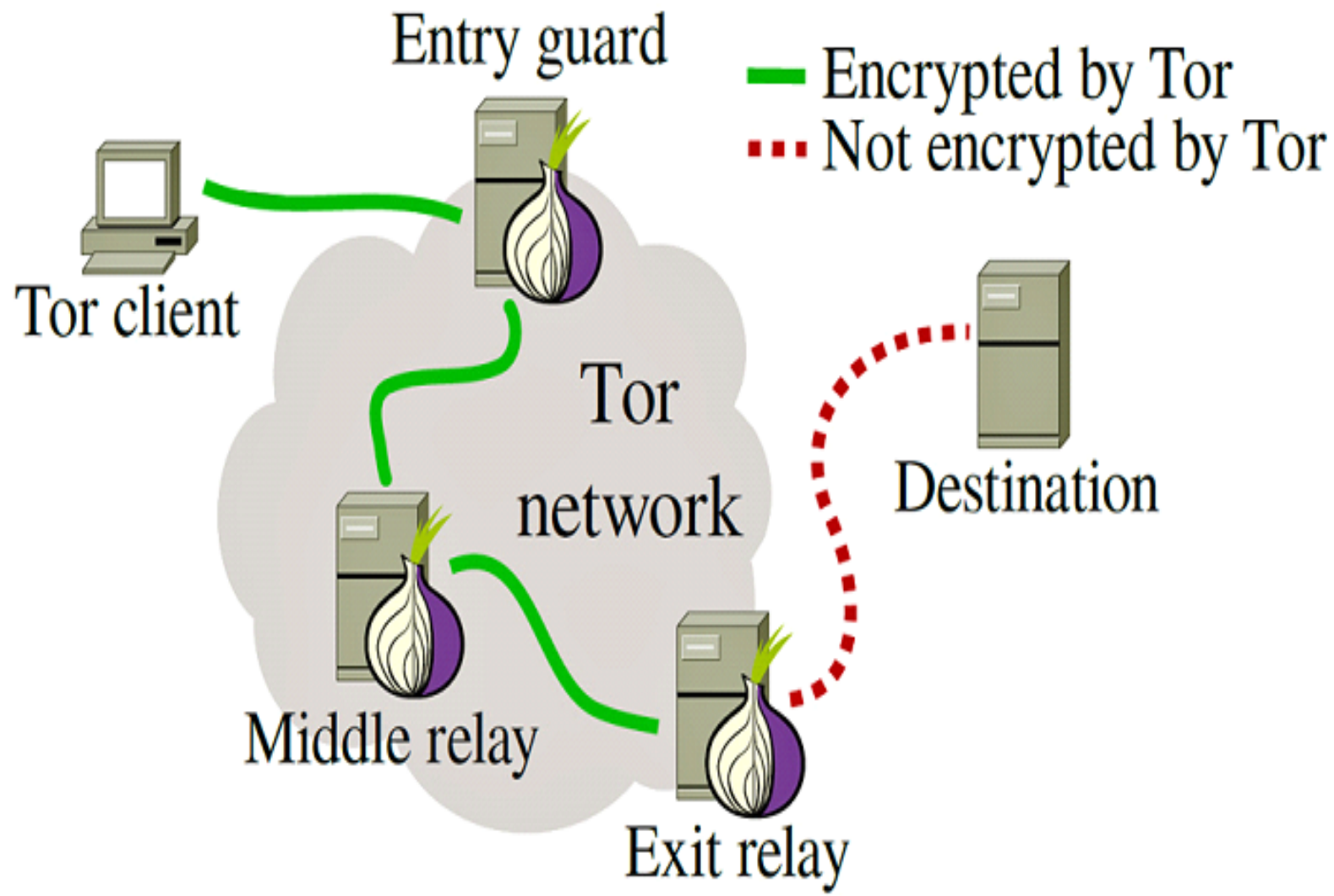
	[1]
	[2]
	[3]



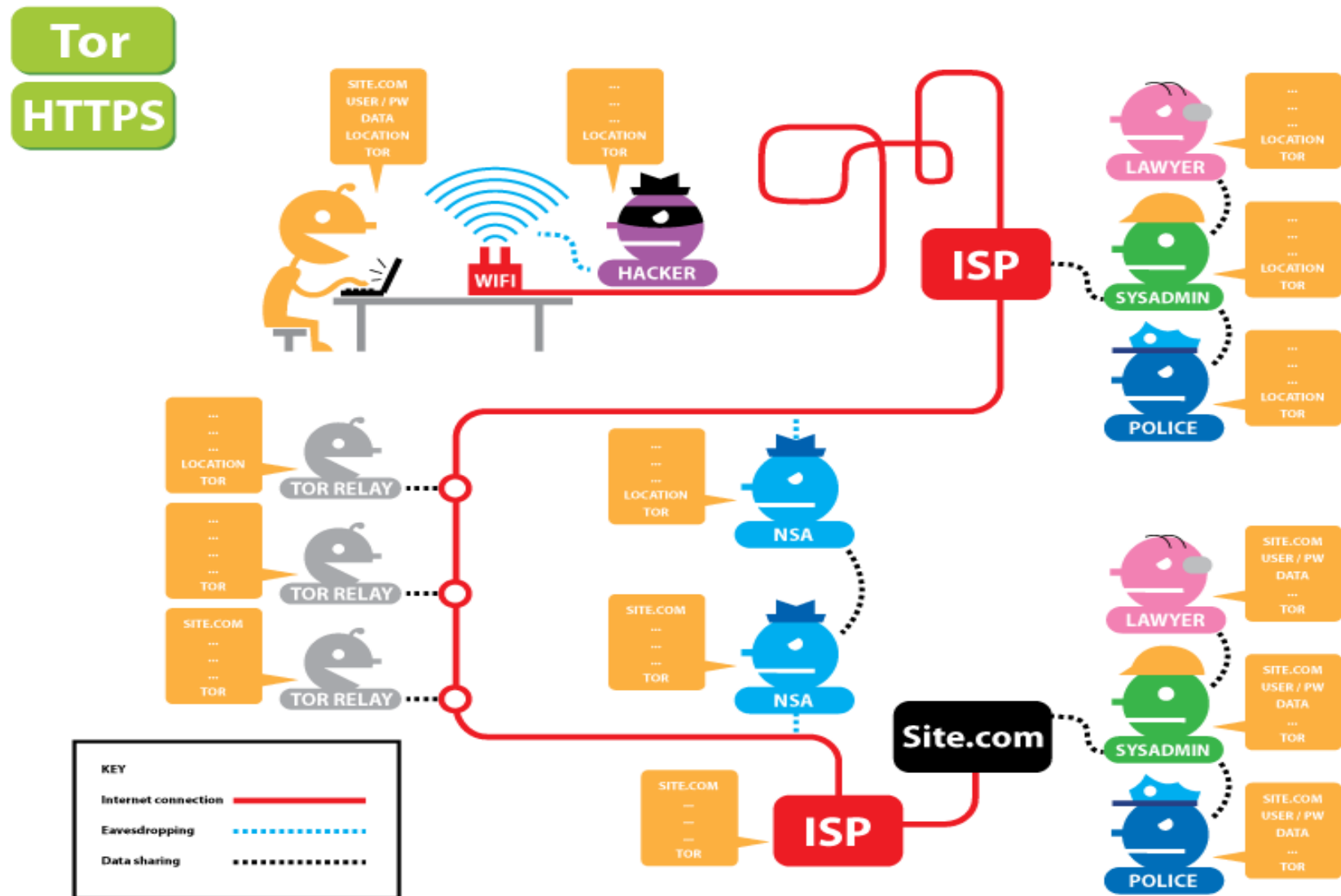
How Tor Works: 3

	[1]
	[2]
	[3]





<https://www.eff.org/pages/tor-and-https>



- **Tor Browser**
- Tor hidden services (“onion services”)
- Tor relays
- **Orbot** (Android)
- **Orfox** (Android)
- **Onion Browser** (iOS)
- **Tails**

Install Tor Browser



**BROWSER
BUNDLE**

Install Orbot & Orfox (Android) or Onion Browser (iOS)





Tails

the **amnesic** incognito **live** system



Privacy for anyone anywhere



English

DE

FR

PT

Privacy for anyone anywhere

Tails is a [live operating system](#), that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your **privacy** and **anonymity**, and helps you to:

- **use the Internet anonymously** and **circumvent censorship**;
all connections to the Internet are forced to go through [the Tor network](#);
- **leave no trace** on the computer you are using unless you ask it explicitly;
- **use state-of-the-art cryptographic tools** to encrypt your files, emails and instant messaging.

[Learn more about Tails.](#)

News

[Tails 1.5.1 is out](#)

Posted Fri 28 Aug 2015 12:34:56 PM

Security

[Numerous security holes in Tails 1.5](#)

Posted Wed 26 Aug 2015 01:02:03 AM

Download
Tails 1.5.1
August 28, 2015



About

Getting started...

Documentation

Help & Support

Contribute

News

Digital Hygiene: Top Tips to Keep it Clean!

- Use strong **passwords**.
- Watch out for **suspicious links & attachments** (malware).
- Secure your devices with **full-disk encryption**.
- **Encrypt** your files, emails, and communications.
- Connect securely with **HTTPS Everywhere**.
- Anonymize your connections using **Tor Browser**.
- Use **secure software alternatives**.

Resources

- <https://www.eff.org/torchallenge/what-is-tor.html>
- <https://securityinabox.org/en/guide/torbrowser/linux>
- <https://securityinabox.org/en/guide/torbrowser/os-x>
- <https://securityinabox.org/en/guide/torbrowser/windows>
- <https://www.torproject.org/>
- <https://tails.boum.org/install/win/usb/index.en.html>
- <https://tails.boum.org/install/mac/usb/index.en.html>
- <https://tails.boum.org/install/linux/usb/overview/index.en.html>