Cybersecurity
Privacy and Open Source Intelligent (OSINT)

Kasun De Zoysa

Department of Communication and Media Technologies
University of Colombo School of Computing
University of Colombo
Sri Lanka

Threats to Privacy

Legal

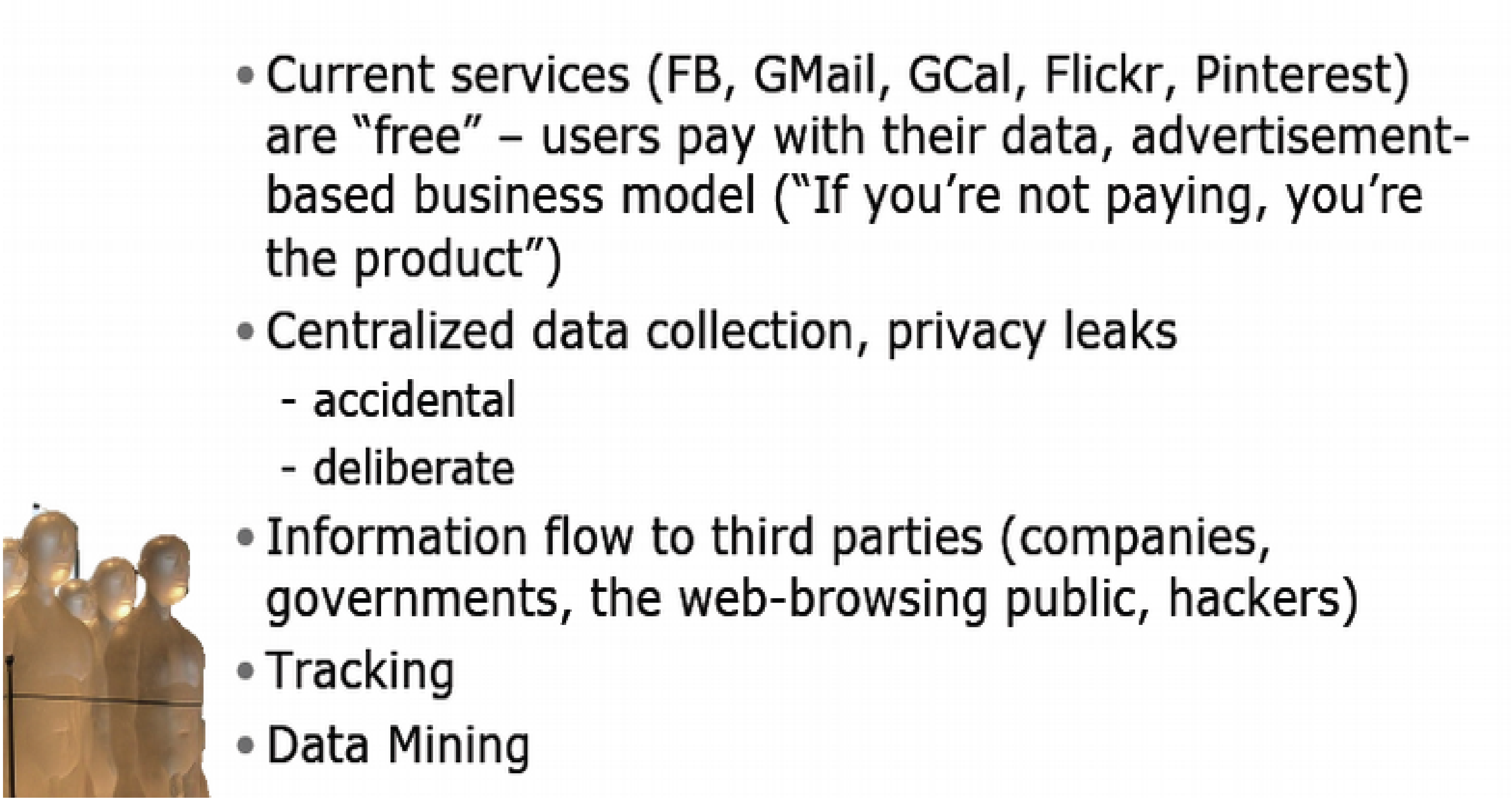
- Company/employer access to data and ‘personal’ communications
- Local (and remote) logging of communication
- Personal info sent to online service providers,
- merchants or other users
- Cookies
- Web intelligence gathering

Illegal

- Eavesdropping/Interception
- Man-in-the-middle
- Keylogging

Image courtesy of: Tech Tips.com

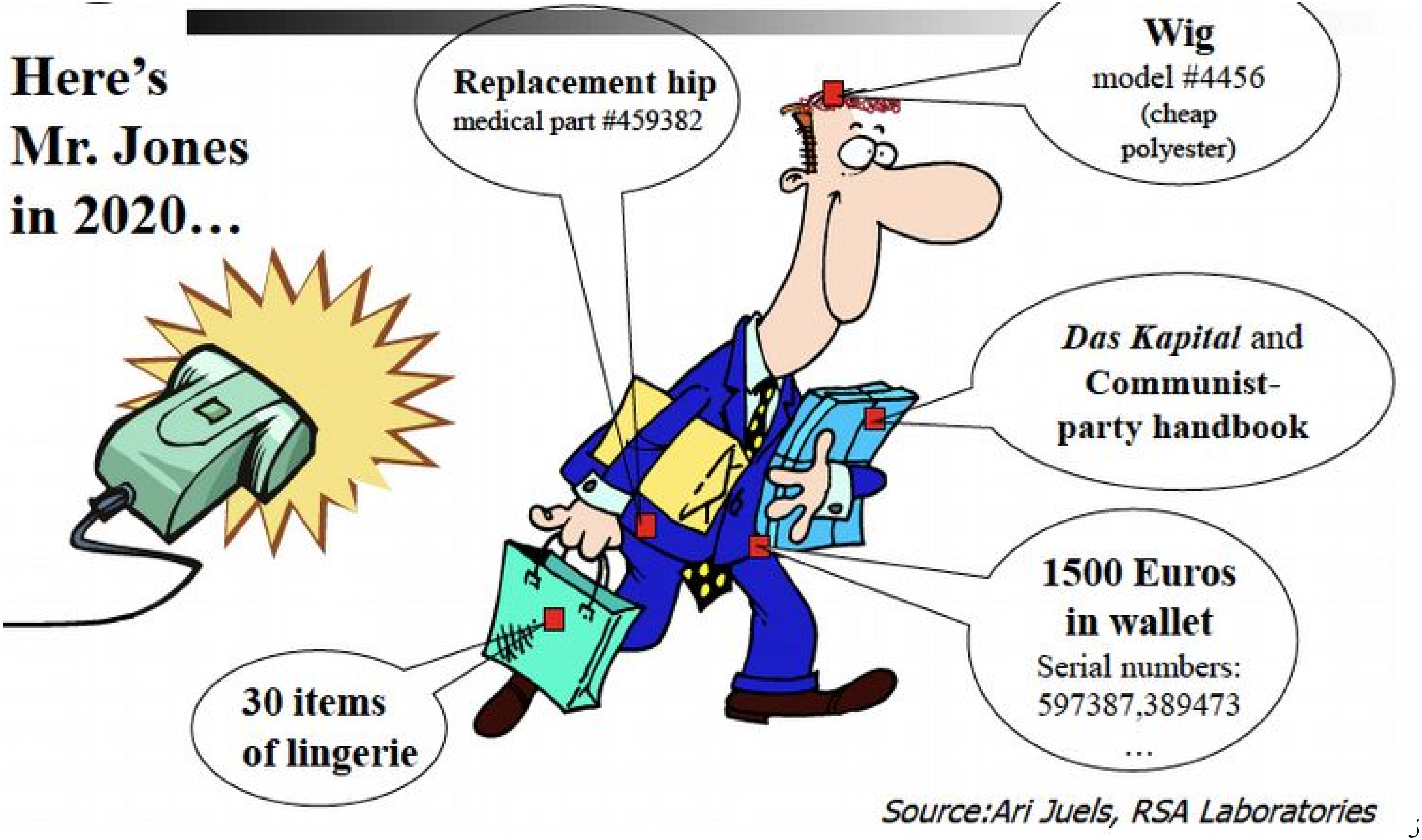
Online Privacy Problematic



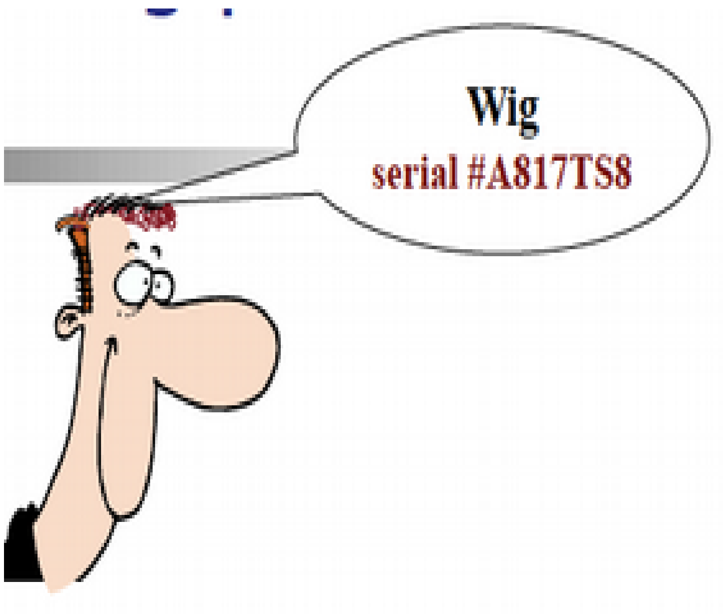
- Current services (FB, GMail, GCal, Flickr, Pinterest) are “free” – users pay with their data, advertisement-based business model (“If you’re not paying, you’re the product”)
- Centralized data collection, privacy leaks
  - accidental
  - deliberate
- Information flow to third parties (companies, governments, the web-browsing public, hackers)
- Tracking
- Data Mining

- Once leaked, the data cannot be revoked
- Potential audience exceeds expectations, copying easy
- Not known who has what information
- Pieces of information that are harmless, taken together can be identifying or damaging

The RFID Consumer Privacy Problem


Here's Mr. Jones in 2020…
Replacement hip medical part #459382
Wig model #4456 (cheap polyester)
Das Kapital and Communist-party handbook
1500 Euros in wallet Serial numbers: 597387,389473 …
30 items of lingerie

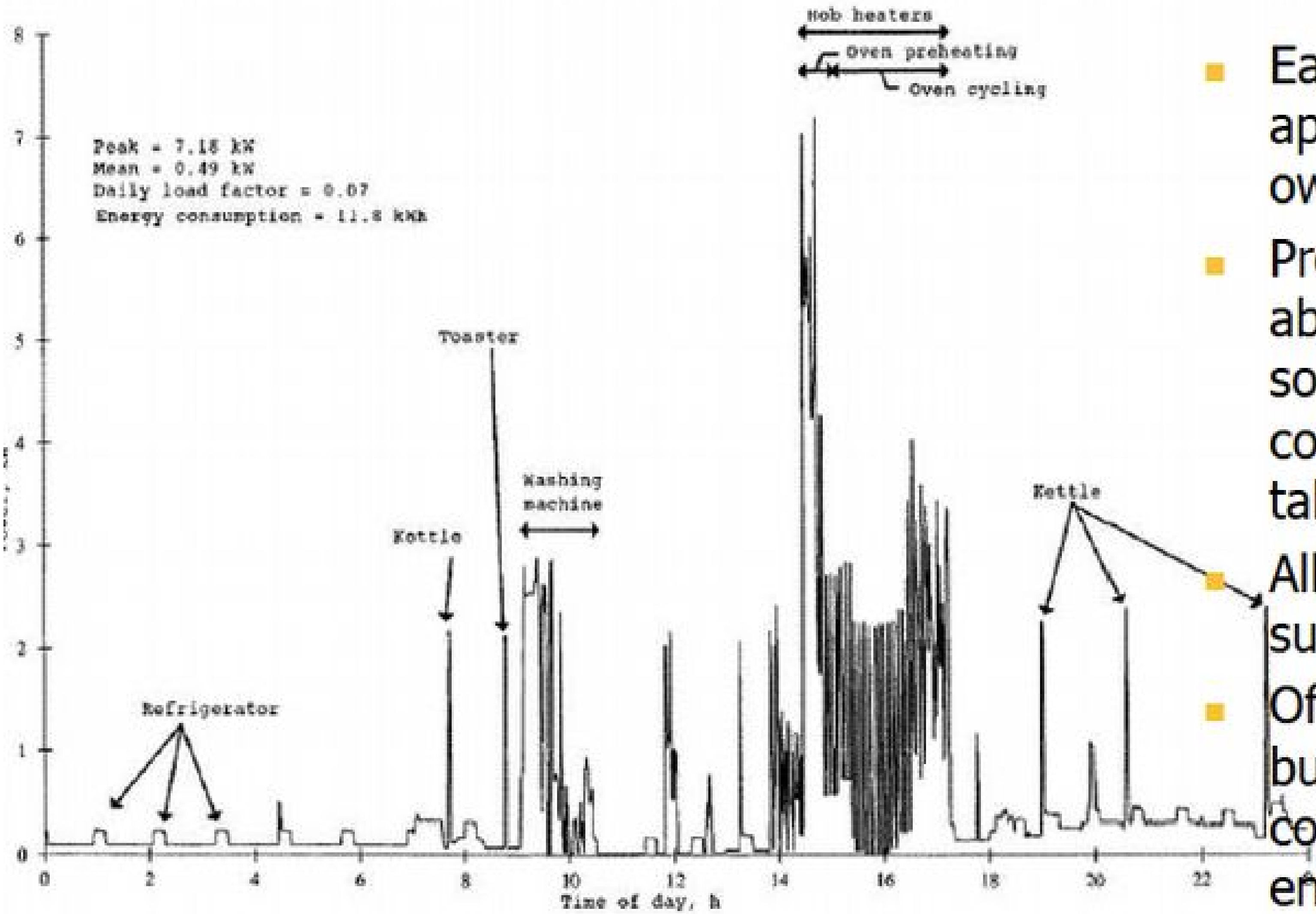
Source:Ari Juels, RSA Laboratories



Tracking Problem

- Mr. Jones pays with a credit card; his RFID tags now linked to his identity
- Mr. Jones attends a political rally; law enforcement scans his RFID tags
- Mr. Jones wins Turing Award; physically tracked by paparazzi via RFID

Smart Metering – Privacy Risk



- Each electrical appliance has its own fingerprint
- Provides information about when someone is at home, cooks, watches TV, takes a shower, etc.
- Allows real-time surveillance
- Of interest for burglars, insurance companies, law enforcement,…

Source: Smart Metering & Privacy, Elias Leake Quinn, 2009

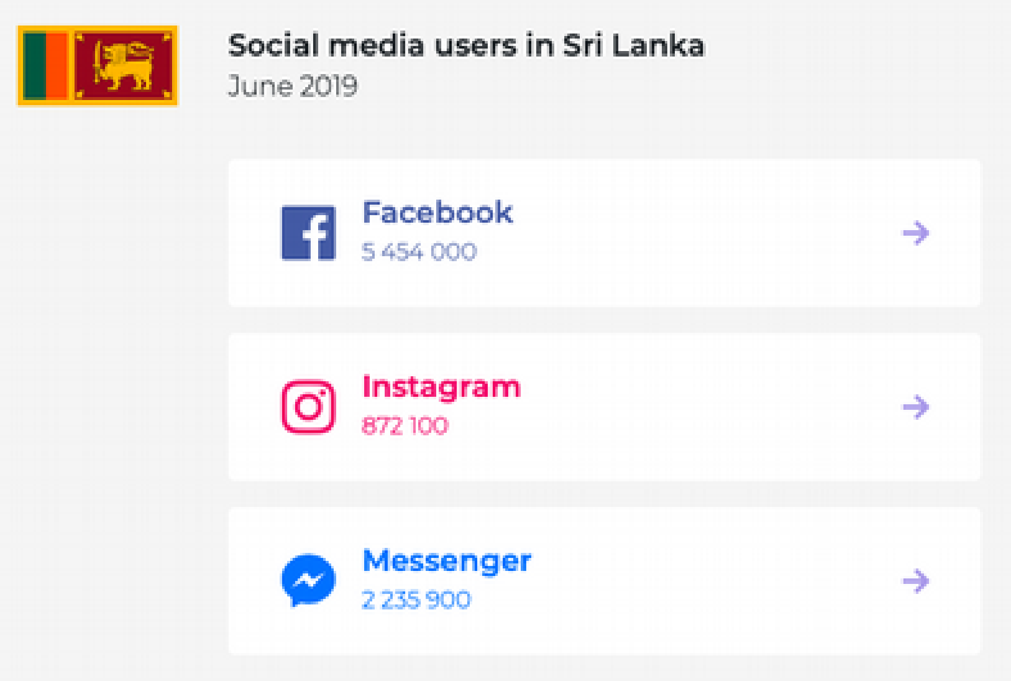
Privacy Risk by Social Networks

- Intimate personal details about social contacts, personal life, etc.
- The Internet never forgets completely....
- Not only accessible by ”friends”

Social Network Analysis/Profiling by:

- Employers
- Schools/Universities
- Tax authorities
- Law Enforcement
- Insurances
- Hackers

Facebook Statistics (https://napoleoncat.com/stats/)

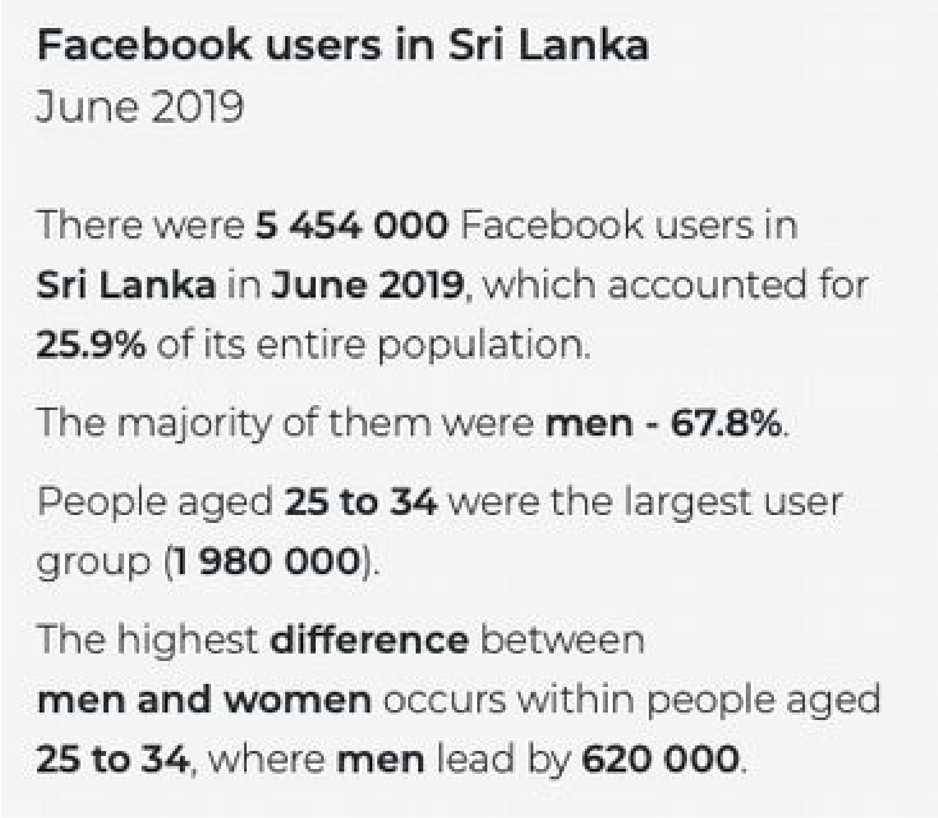


Social media users in Sri Lanka
June 2019

Facebook
5 454 000

Instagram
872 100

Messenger
2 235 900



Facebook users in Sri Lanka
June 2019

There were **5 454 000** Facebook users in **Sri Lanka** in **June 2019**, which accounted for **25.9%** of its entire population.

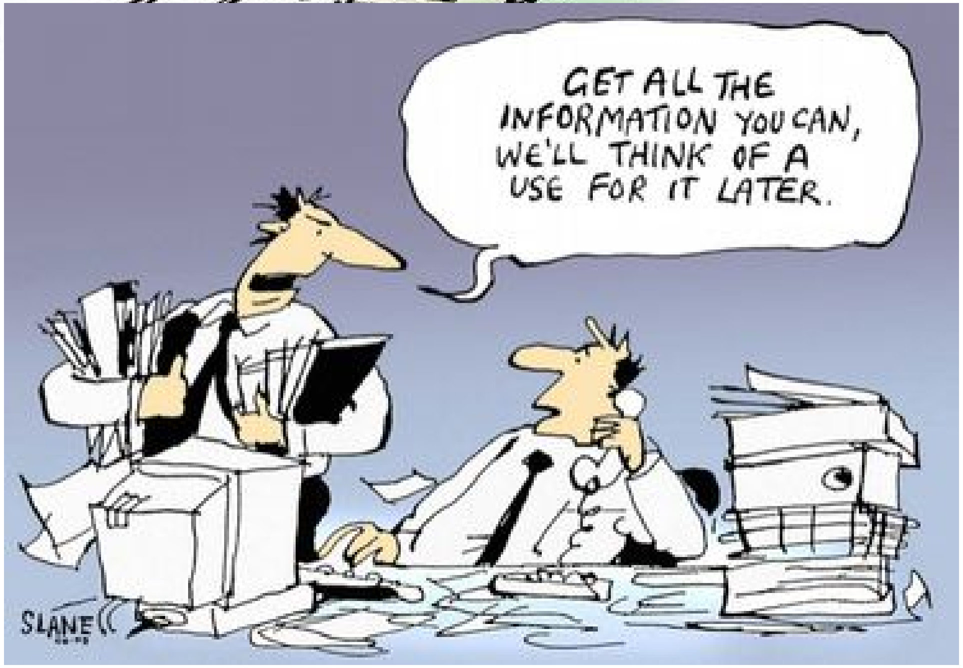
The majority of them were **men - 67.8%**.

People aged **25 to 34** were the largest user group (**1 980 000**).

The highest **difference** between **men and women** occurs within people aged **25 to 34**, where **men** lead by **620 000**.

NAME...
AGE... GENDER...
HEIGHT... WEIGHT...
SSN... NET WORTH...
MARITAL STATUS...
PET PEEVES...
WORST FEARS...
SEXUAL FANTASIES...
MEDICAL HISTORY...
TYPE TYPE TYPE ENTER ENTER ENTER
OF COURSE I EXPECT ALL OF THIS TO REMAIN STRICTLY PRIVATE!
Social Net-Working

MIKE KEEFE THE DENVER POST 5·26·10


GET ALL THE INFORMATION YOU CAN, WE'LL THINK OF A USE FOR IT LATER.
SLANE

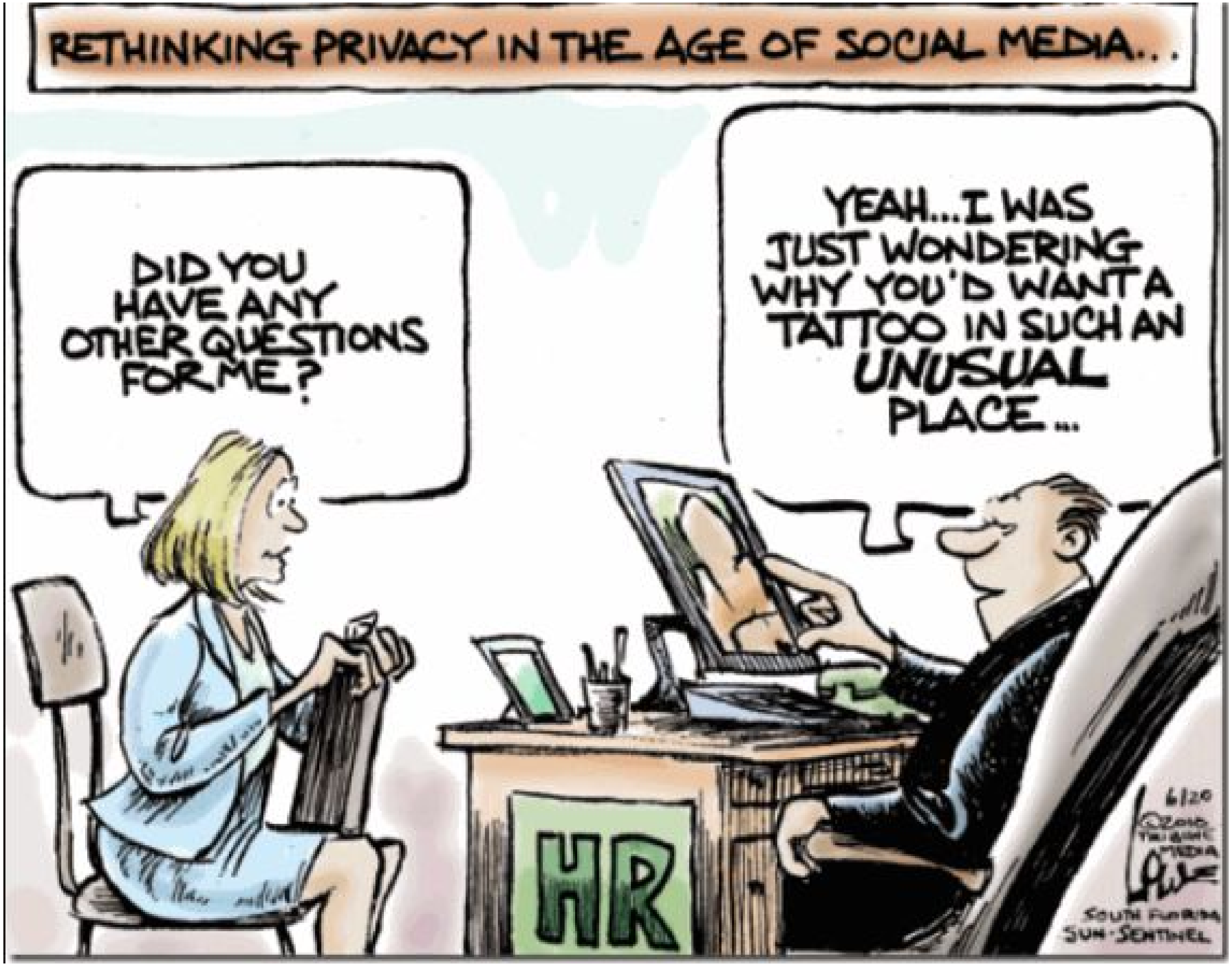
Sharing a Selfie

© MARK ANDERSON, WWW.ANDERTOONS.COM
HEY, STOP AND TAKE A SELFIE HERE AND SHARE IT WITH US!
ANDERSON

"It's cheaper than a security cam."

Privacy

facebook
facebook
facebook
Privacy
Policy


RETHINKING PRIVACY IN THE AGE OF SOCIAL MEDIA...
DID YOU HAVE ANY OTHER QUESTIONS FOR ME?
YEAH...I WAS JUST WONDERING WHY YOU'D WANT A TATTOO IN SUCH AN *UNUSUAL* PLACE...
HR
6/20
©2010 TRIBUNE MEDIA
SOUTH FLORIDA SUN-SENTINEL

Location based Systems

- Provide service based on current position
- Typically use GPS
- Store location data
- Not always trusted

People deliberately give their location:

- cinemas / shows
- friend's places
- work
- travels

Still people want (and have the right to) choose when to give away private information

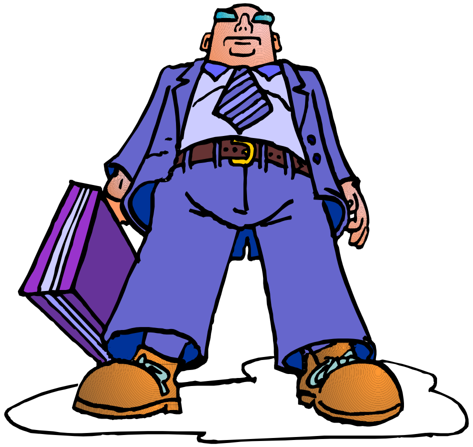
(Possible) Sensitive places:

- Political parties
- Hospital
- Strip clubs

Location based Systems

TAKE THESE AND KEEP THE LOCATION APP ON - THE BOSS SAID HE MIGHT NEED TO KNOW WHERE WE ARE.
SLANE.co.nz
SLANE CARTOONS

PET



Privacy Enhancement Tool (PET) is a generic term for computer tools, applications and mechanisms which allow online users to protect the privacy of their personally identifiable information.

PETs are often integrated with, or used in conjunction with, online services or applications

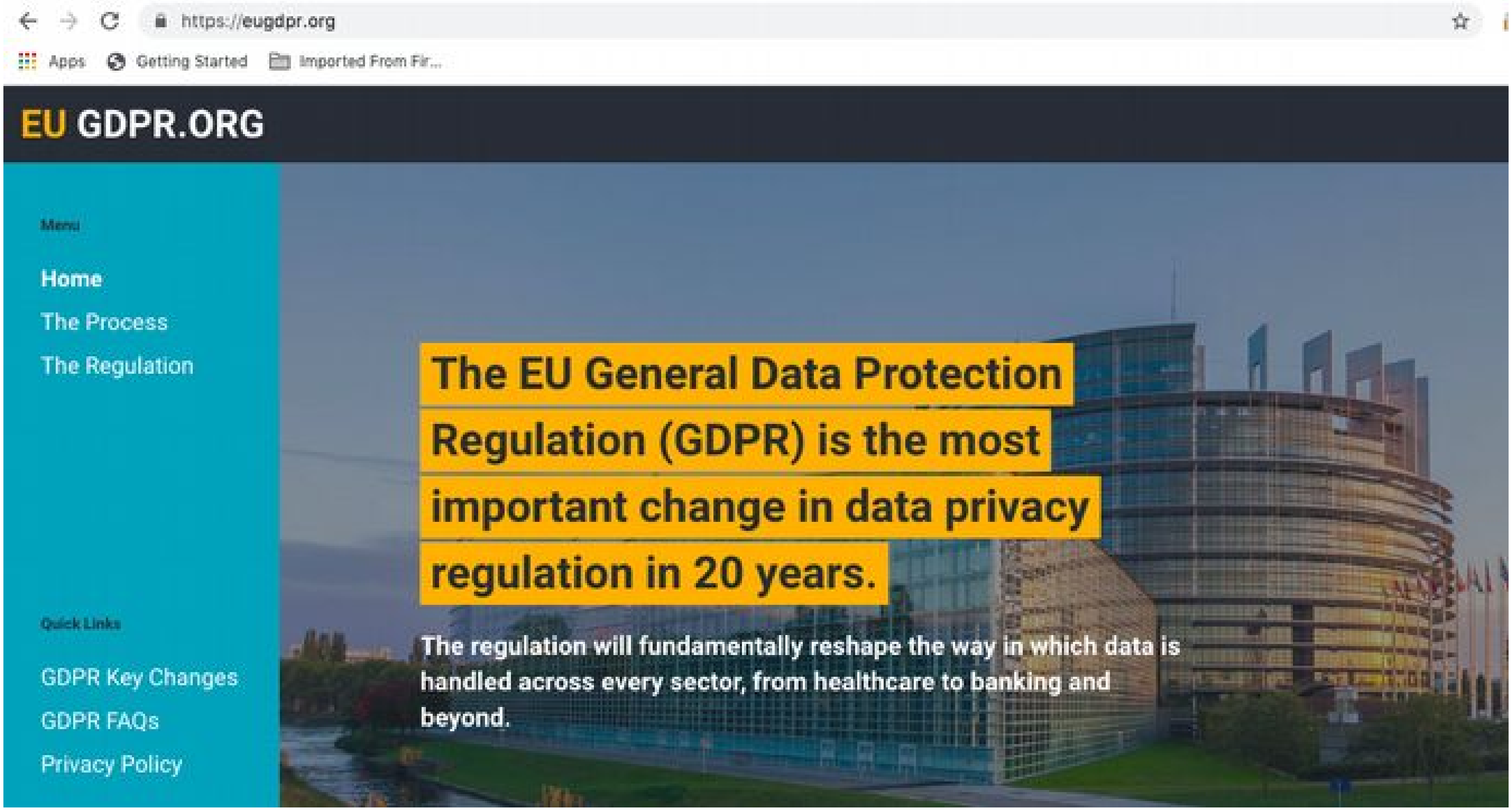
- e.g. email, Web,…

PETs Overview

The main objectives of PETs are one or more of the following:

- increase control over the personal data sent to, and used by, online service providers, merchants or other online users
- minimize the personal data collected and used by service providers and merchants choose the degree of anonymity
  - e.g. by using pseudonyms

General Data Protection Regulation



The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years.

The regulation will fundamentally reshape the way in which data is handled across every sector, from healthcare to banking and beyond.

Example PET Applications

- Encryption on local storage
- Encryption on transmitted data
- Anonymous browsing
  - cookies
- Anonymous email
- Onion routing (Tor)

- **Prevent unauthorized access to local data**
  - Complete disk encryption
    - e.g. TrueCrypt,VeraCrypt,Bitlocker,LUKS

- **Encryption data for transmission**
  - secure email

    S/MIME, PGP
  - VPN tunnels

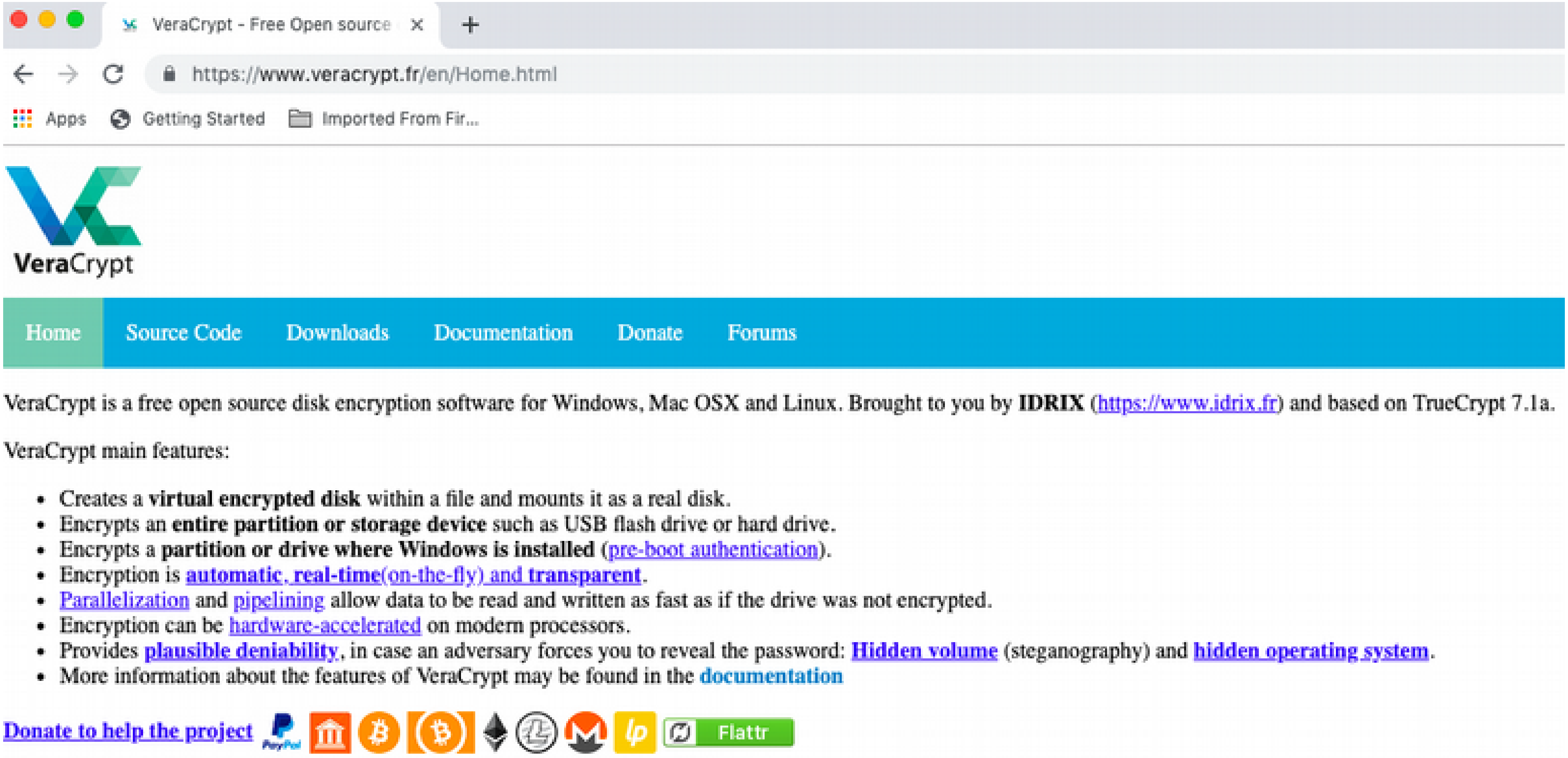
    IPSec, SSL/TLS
  - Secure Web connections

    HTTPS (TLS)

TrueCrypt 7.1a

- Free open-source disk encryption software
- Creates a virtual encrypted disk within a file and mounts it as a real disk.
- Encrypts an entire partition or storage device such as USB flash drive or hard drive.
- Encryption is automatic, real-time (on-the-fly) and transparent.
- Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted.
- Encryption can be hardware-accelerated on modern processors.

VeraCrypt



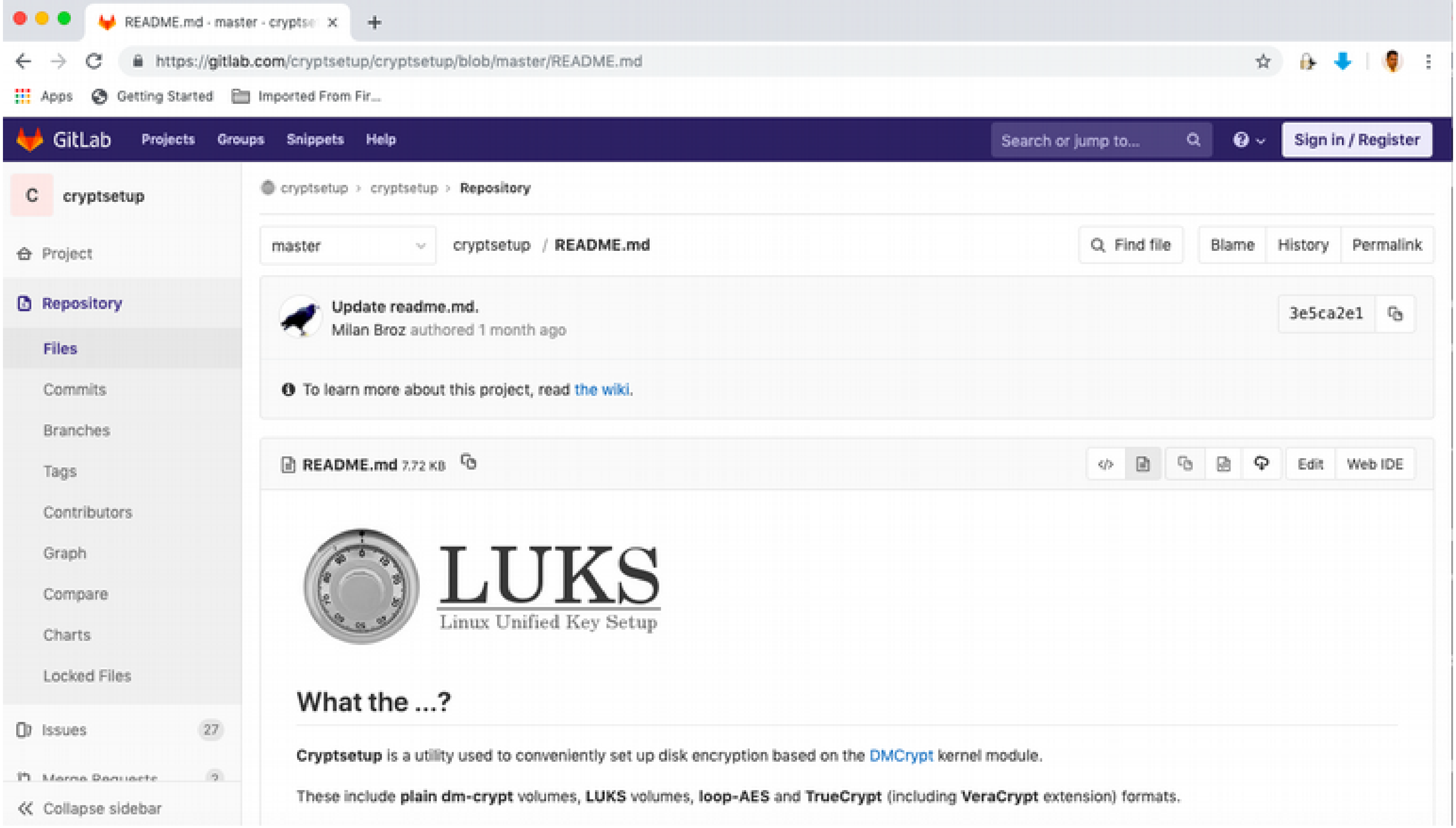
VeraCrypt is a free open source disk encryption software for Windows, Mac OSX and Linux. Brought to you by **IDRIX** (https://www.idrix.fr) and based on TrueCrypt 7.1a.

VeraCrypt main features:

- Creates a **virtual encrypted disk** within a file and mounts it as a real disk.
- Encrypts an **entire partition or storage device** such as USB flash drive or hard drive.
- Encrypts a **partition or drive where Windows is installed** (pre-boot authentication).
- Encryption is **automatic, real-time**(on-the-fly) **and transparent**.
- Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted.
- Encryption can be hardware-accelerated on modern processors.
- Provides **plausible deniability**, in case an adversary forces you to reveal the password: **Hidden volume** (steganography) and **hidden operating system**.
- More information about the features of VeraCrypt may be found in the **documentation**

Donate to help the project

LUKS



Update readme.md.
Milan Broz authored 1 month ago

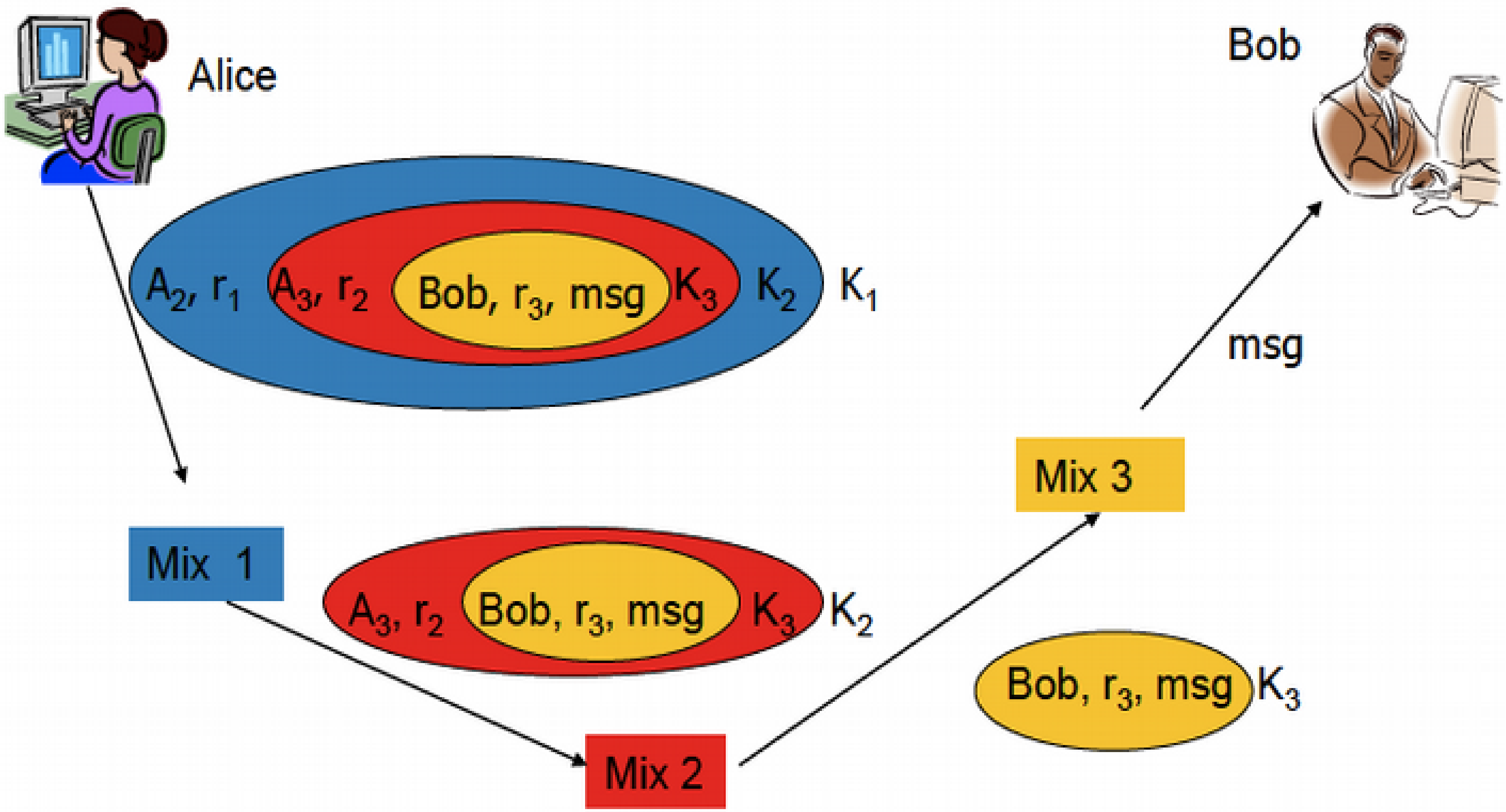
To learn more about this project, read the wiki.

What the ...?

Cryptsetup is a utility used to conveniently set up disk encryption based on the DMCrypt kernel module.

These include **plain dm-crypt** volumes, **LUKS** volumes, **loop-AES** and **TrueCrypt** (including **VeraCrypt** extension) formats.

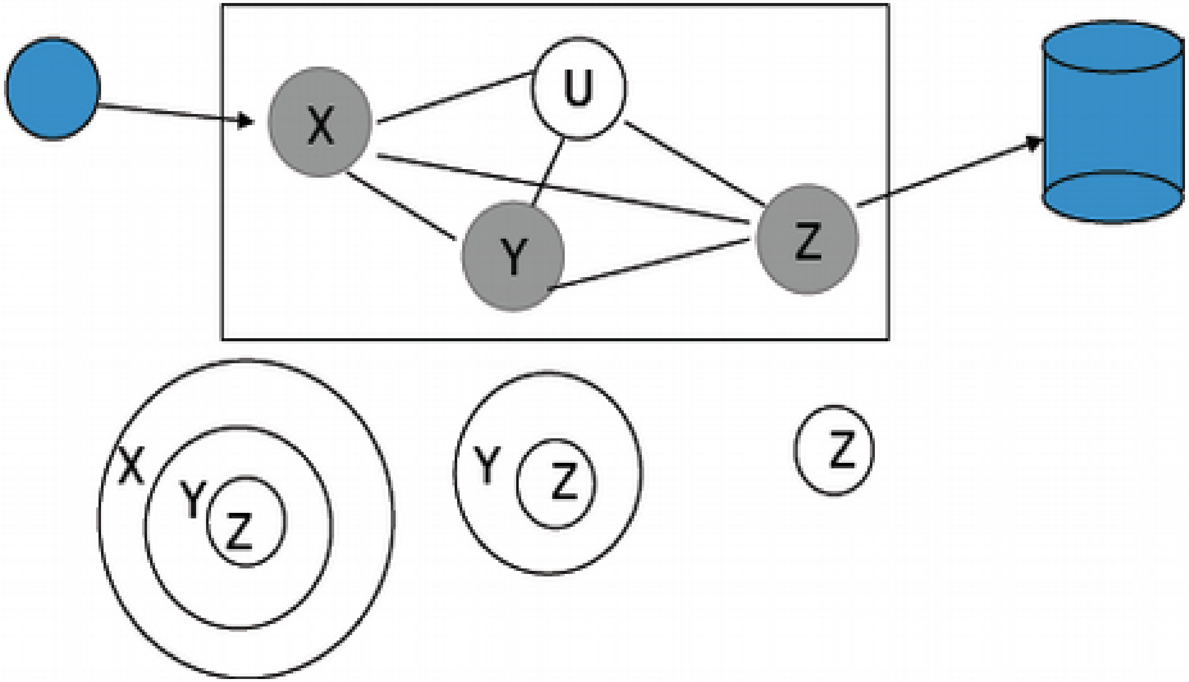
Mix-nets (Chaum, 1981)


Alice
Bob
A_2, r_1 A_3, r_2 Bob, r_3, msg K_3 K_2 K_1
Mix 1
A_3, r_2 Bob, r_3, msg K_3 K_2
Mix 2
Mix 3
Bob, r_3, msg K_3
msg

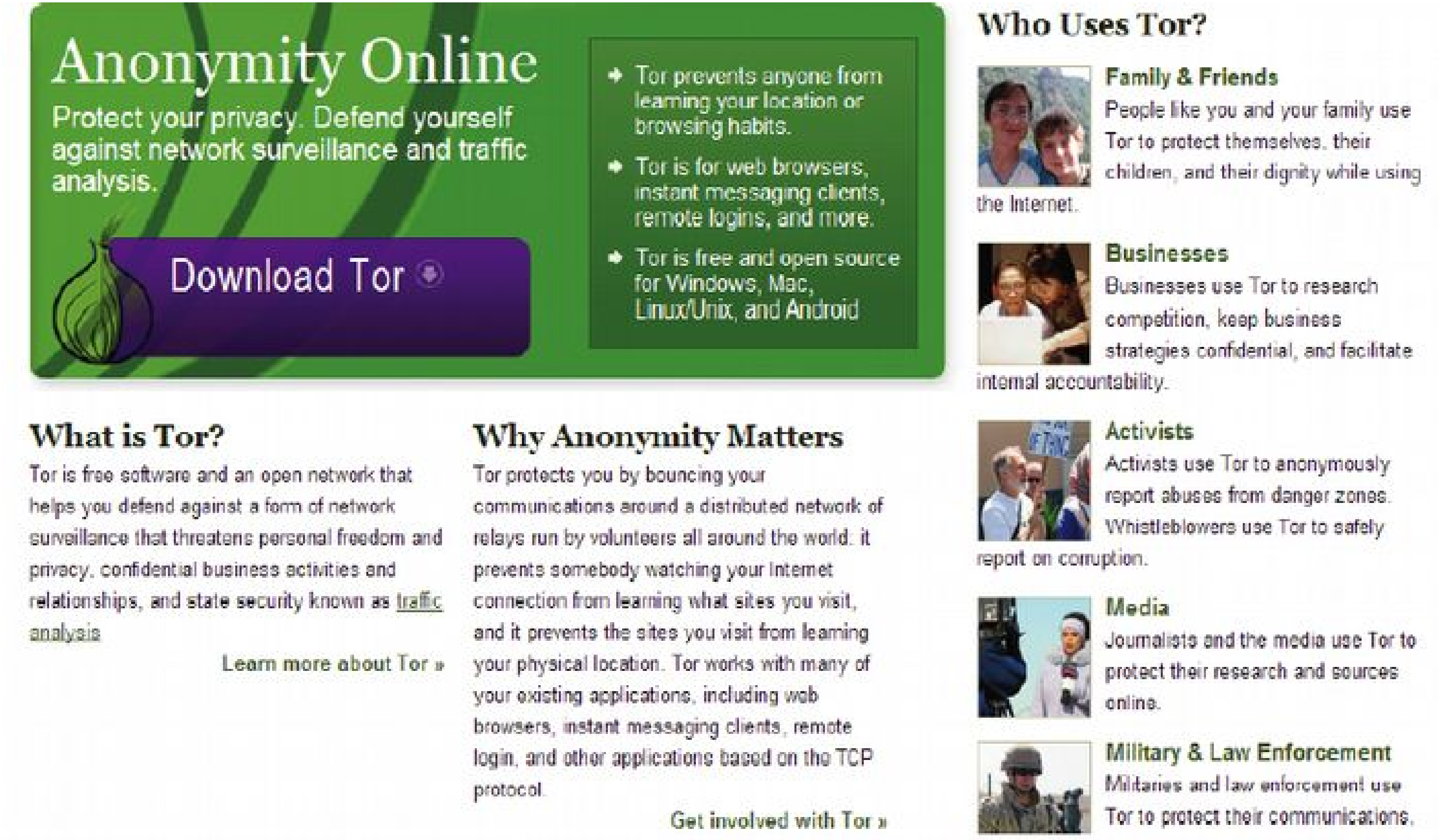
K_i: public key of Mix_i, r_i: random number, A_i: address of Mix_i

Onion Routing

- Onion = Object with layers of public key encryption to produce anonymous bi-directional virtual circuit between communication partners and to distribute symmetric keys
- Initiator's proxy constructs "forward onion" which encapsulates a route to the responder
- (Faster) symmetric encryption for data communication via the circuit



Tor : www.torproject.org



Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

Download Tor

- Tor prevents anyone from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, remote logins, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

What is Tor?

Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis

Learn more about Tor »

Why Anonymity Matters

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location. Tor works with many of your existing applications, including web browsers, instant messaging clients, remote login, and other applications based on the TCP protocol.

Get involved with Tor »

Who Uses Tor?

Family & Friends
People like you and your family use Tor to protect themselves, their children, and their dignity while using the Internet.

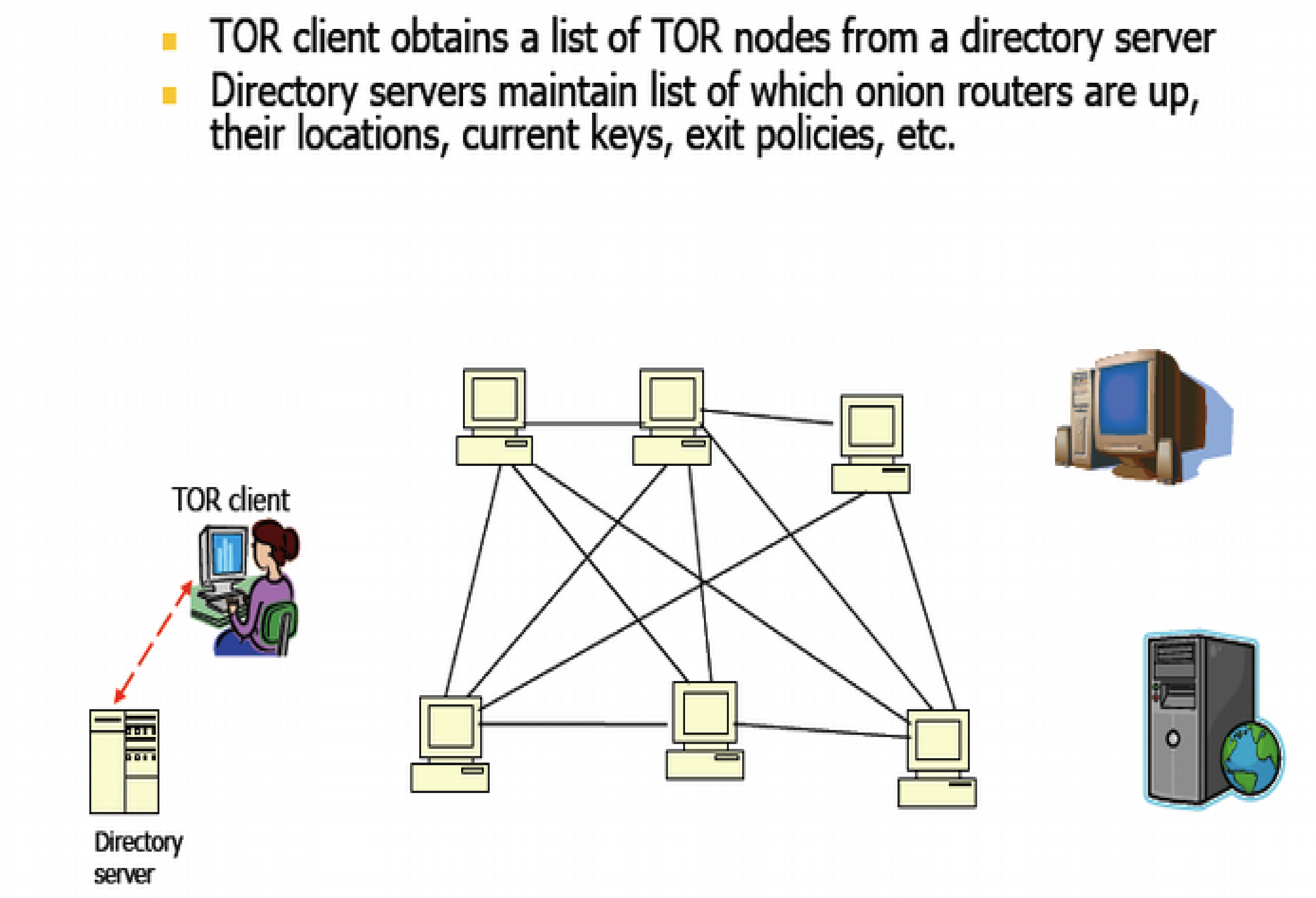
Businesses
Businesses use Tor to research competition, keep business strategies confidential, and facilitate internal accountability.

Activists
Activists use Tor to anonymously report abuses from danger zones. Whistleblowers use Tor to safely report on corruption.

Media
Journalists and the media use Tor to protect their research and sources online.

Military & Law Enforcement
Militaries and law enforcement use Tor to protect their communications.

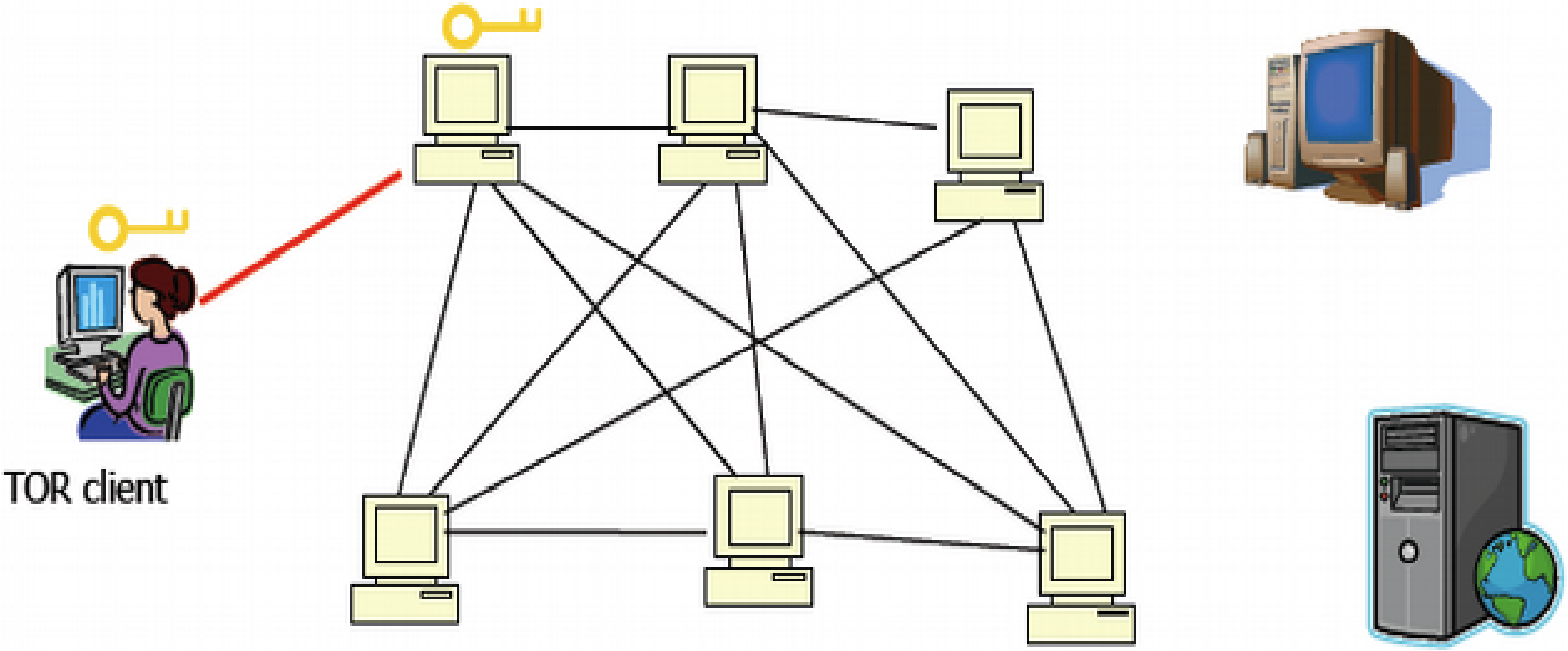
First Step



- TOR client obtains a list of TOR nodes from a directory server
- Directory servers maintain list of which onion routers are up, their locations, current keys, exit policies, etc.

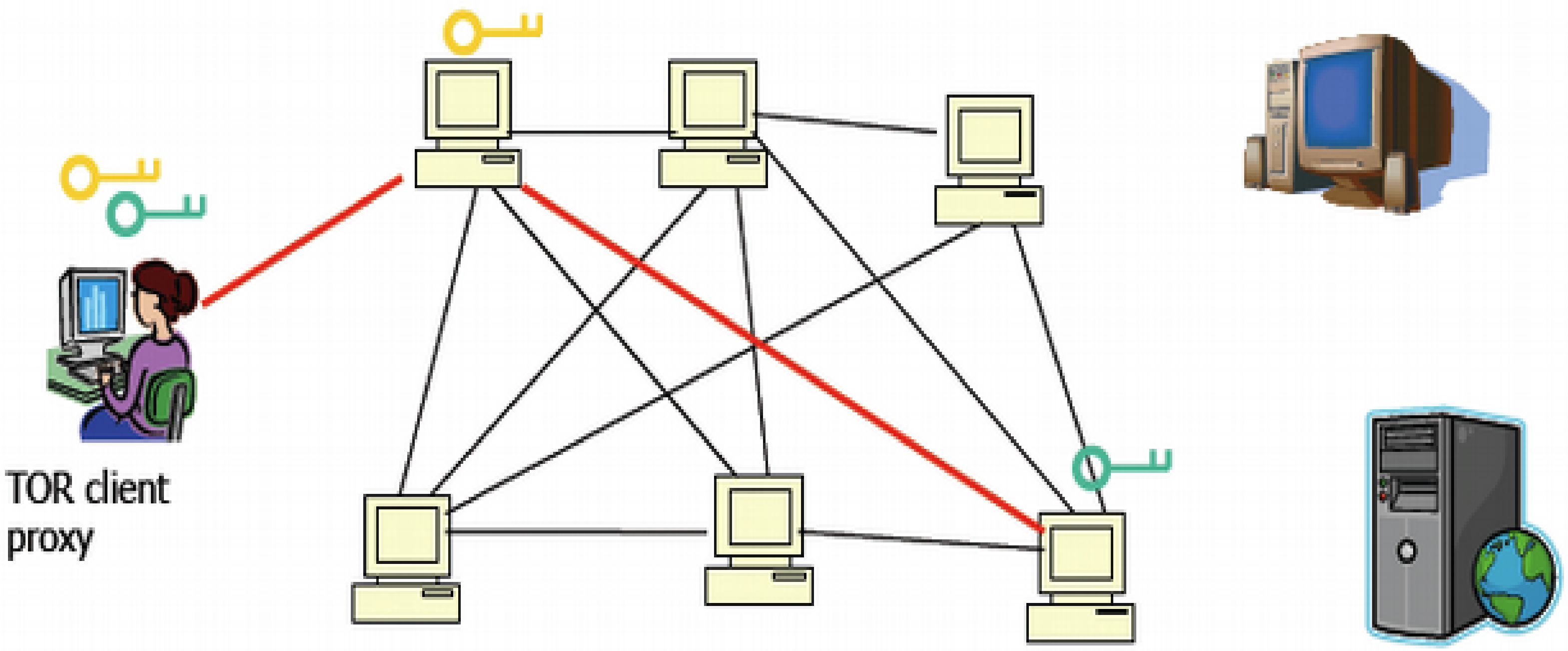
Tor Circuit Setup

- Client proxy establishes key + circuit with Onion Router 1

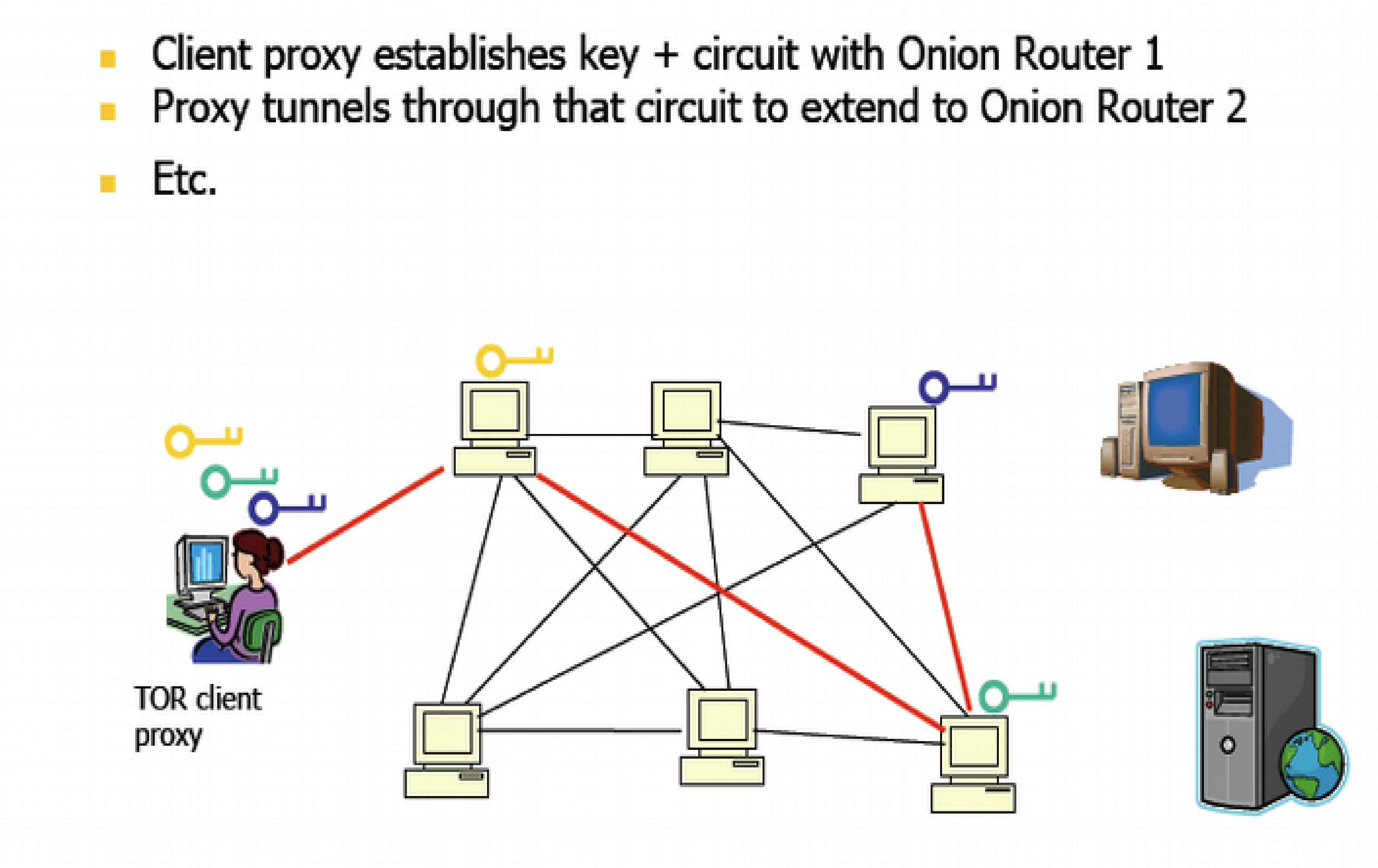


Tor Circuit Setup

- Client proxy establishes key + circuit with Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2

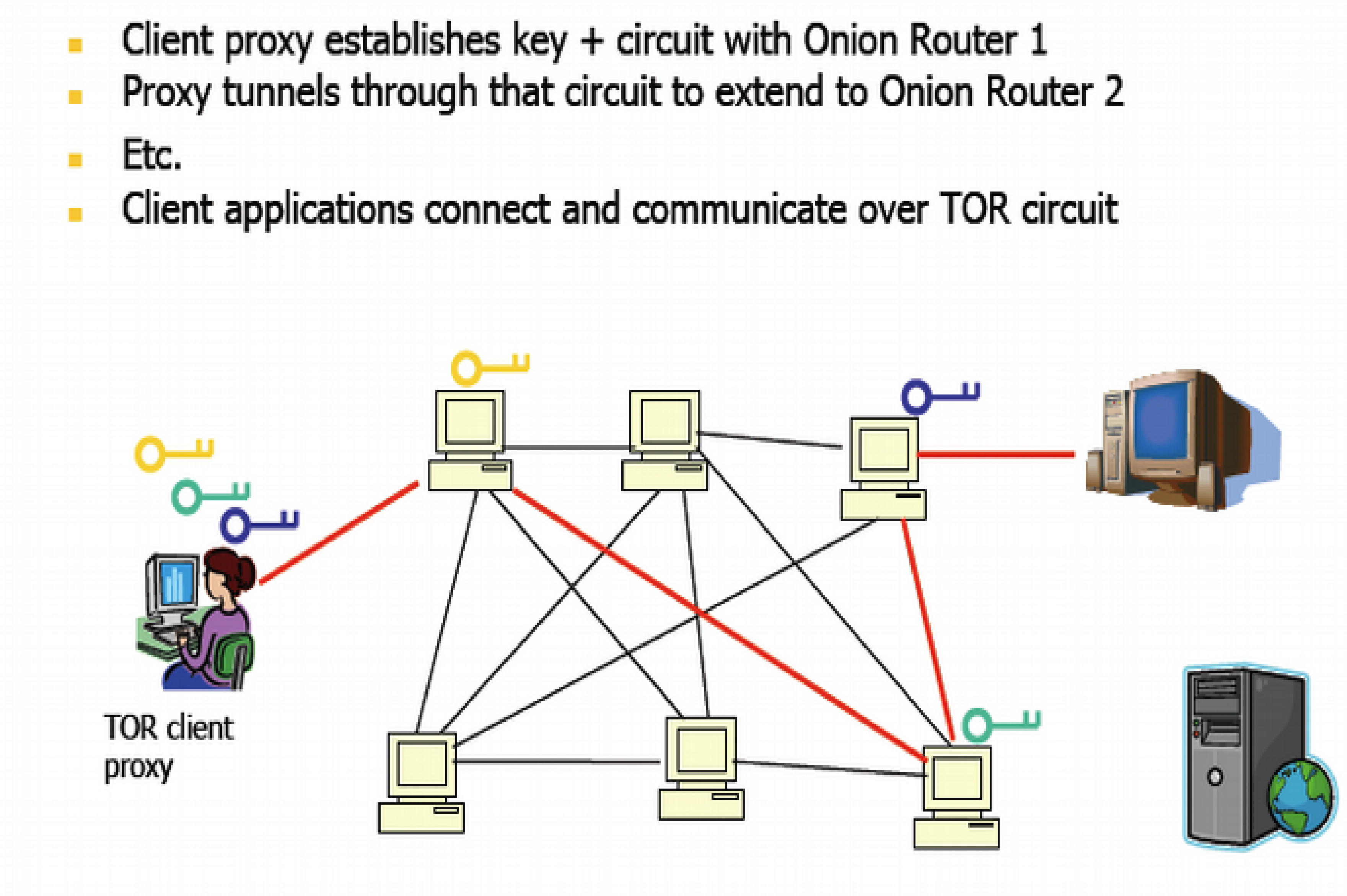


Tor Circuit Setup



- Client proxy establishes key + circuit with Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2
- Etc.

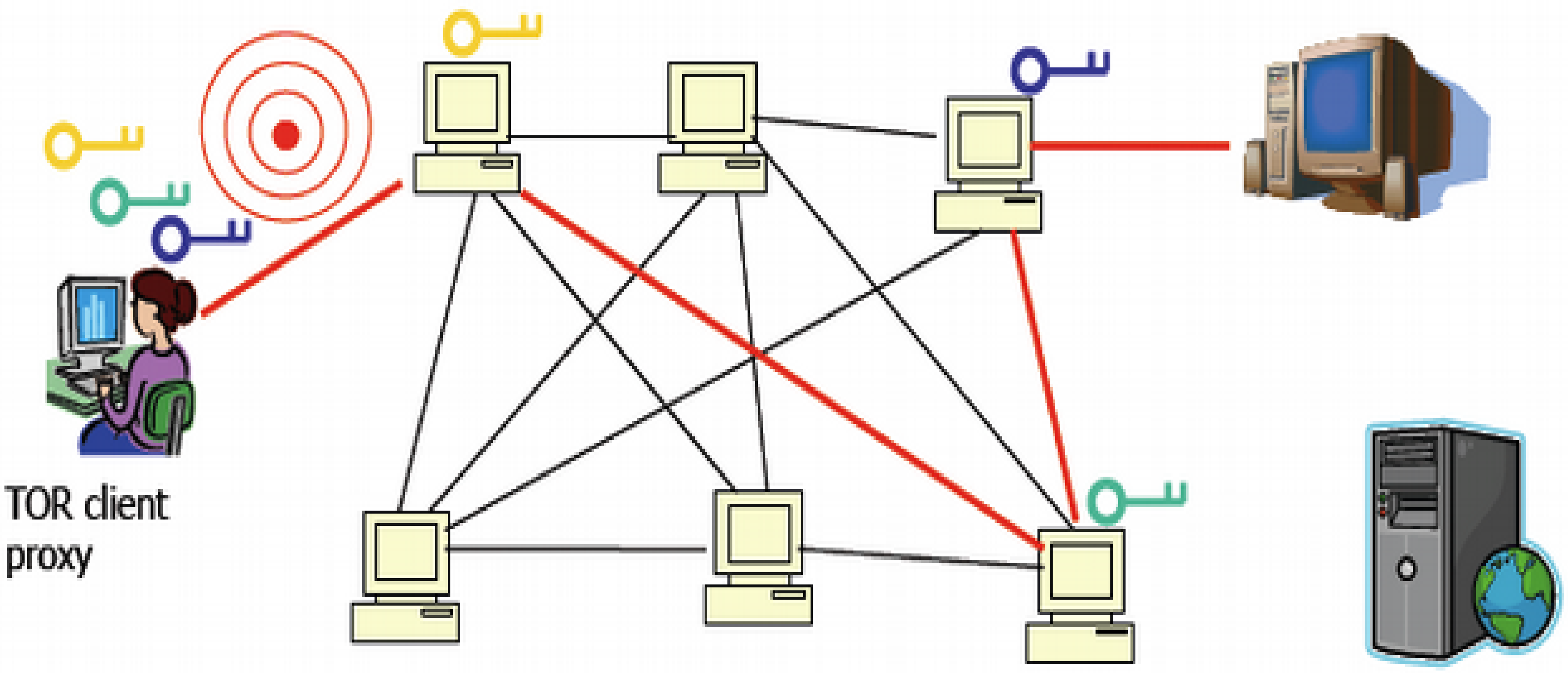
Tor Circuit Setup



- Client proxy establishes key + circuit with Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2
- Etc.
- Client applications connect and communicate over TOR circuit

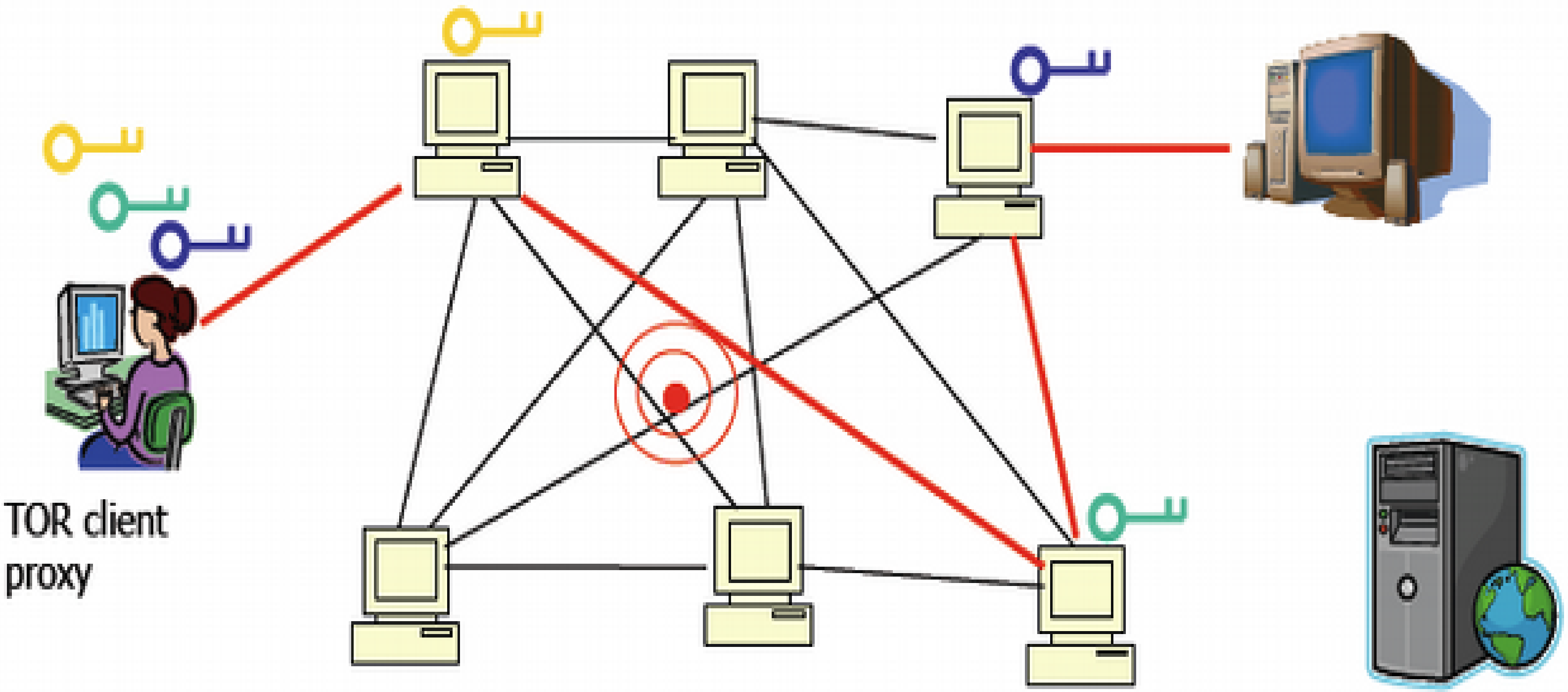
Tor Circuit Setup

- Client proxy establishes key + circuit with Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2
- Etc.
- Client applications connect and communicate over TOR circuit

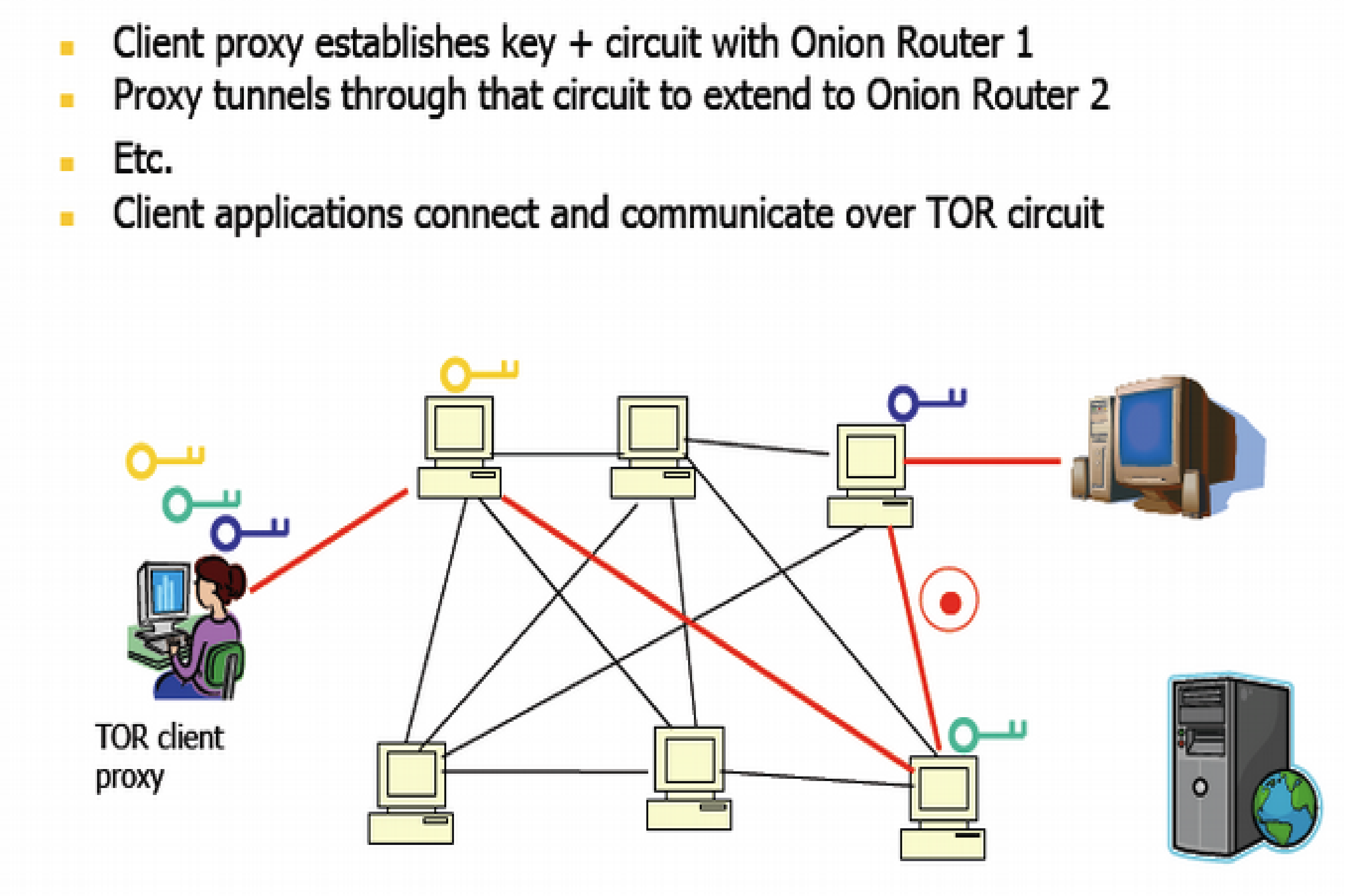


Tor Circuit Setup

- Client proxy establishes key + circuit with Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2
- Etc.
- Client applications connect and communicate over TOR circuit

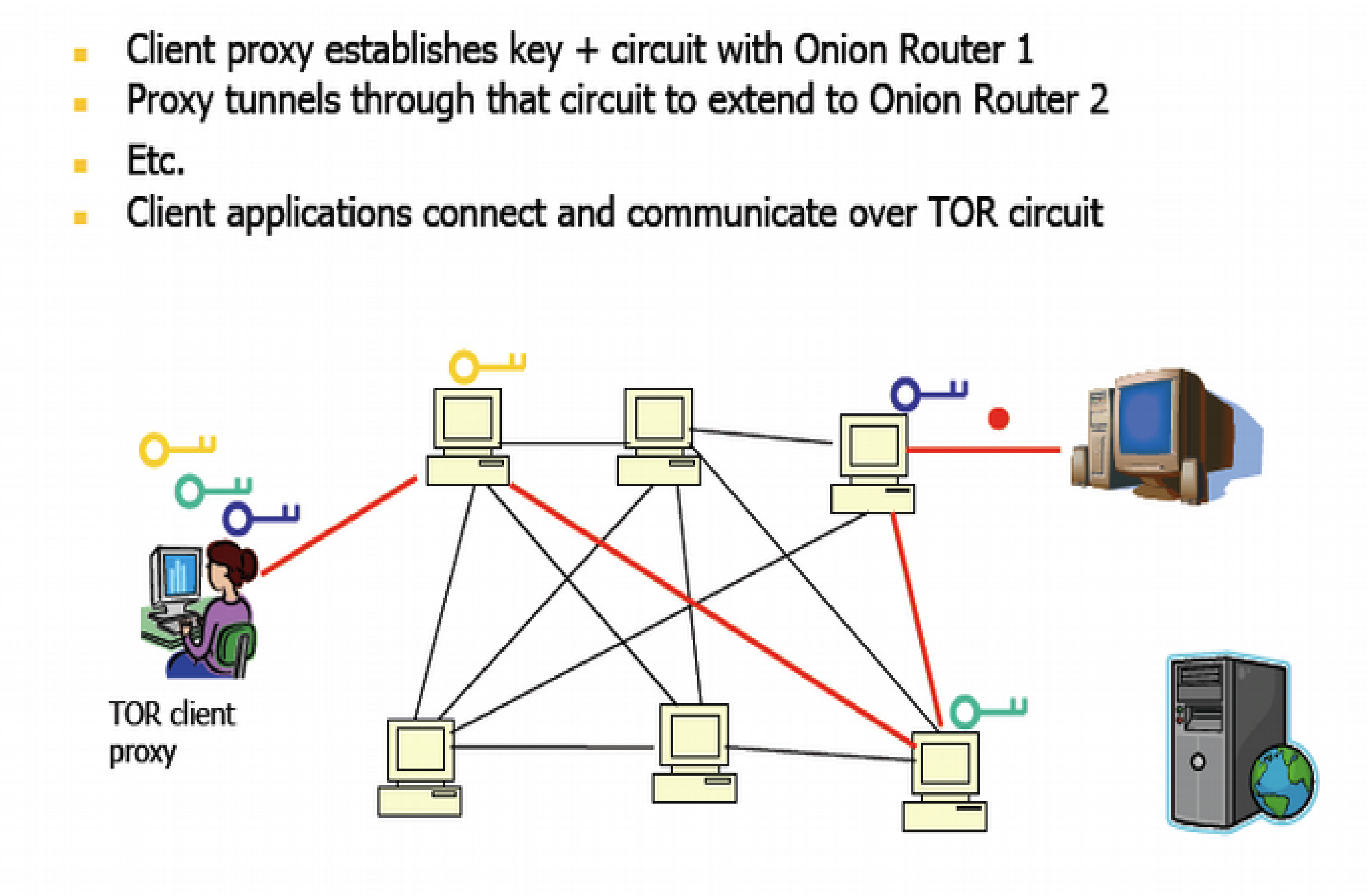


Tor Circuit Setup

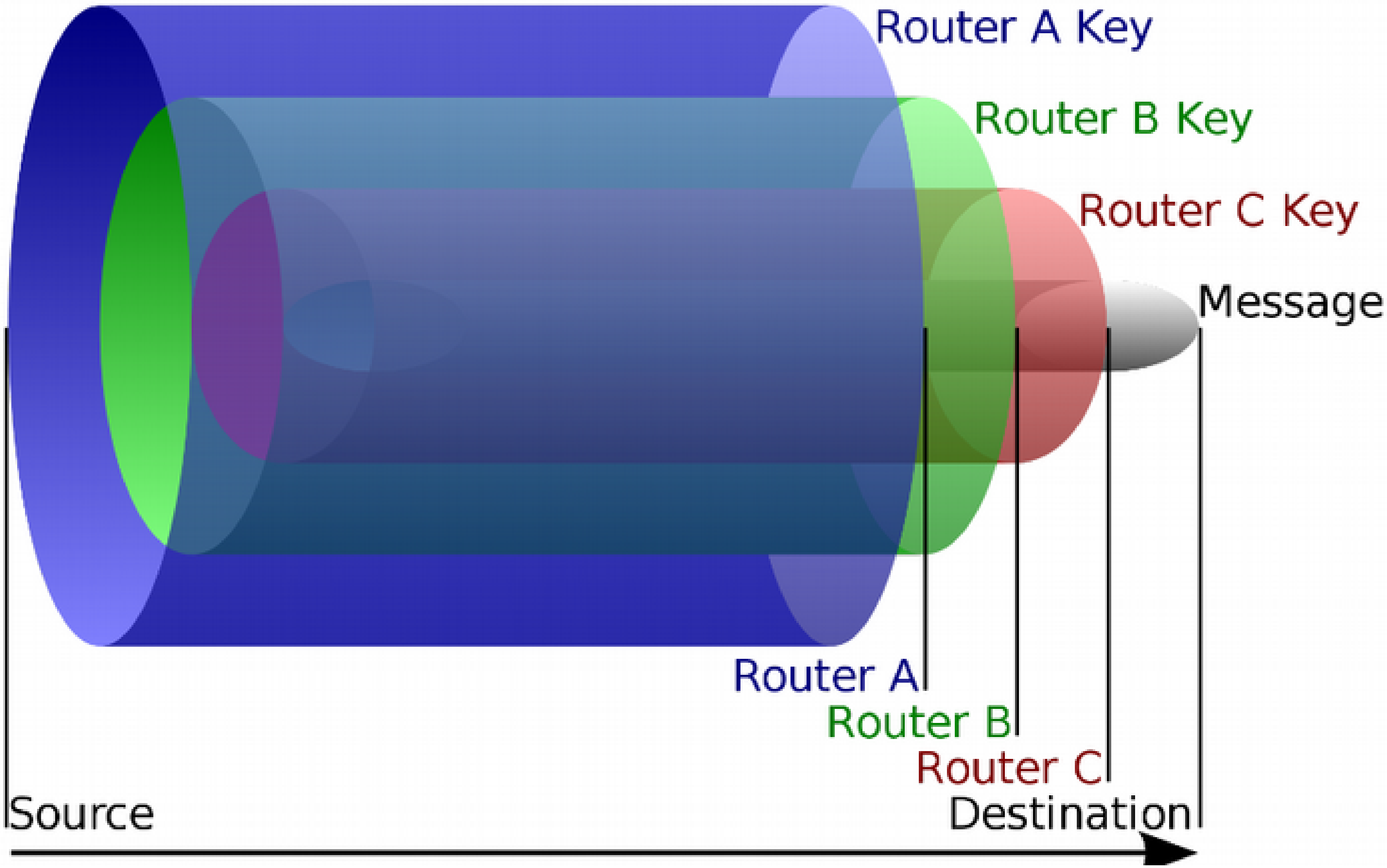


- Client proxy establishes key + circuit with Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2
- Etc.
- Client applications connect and communicate over TOR circuit

Tor Circuit Setup



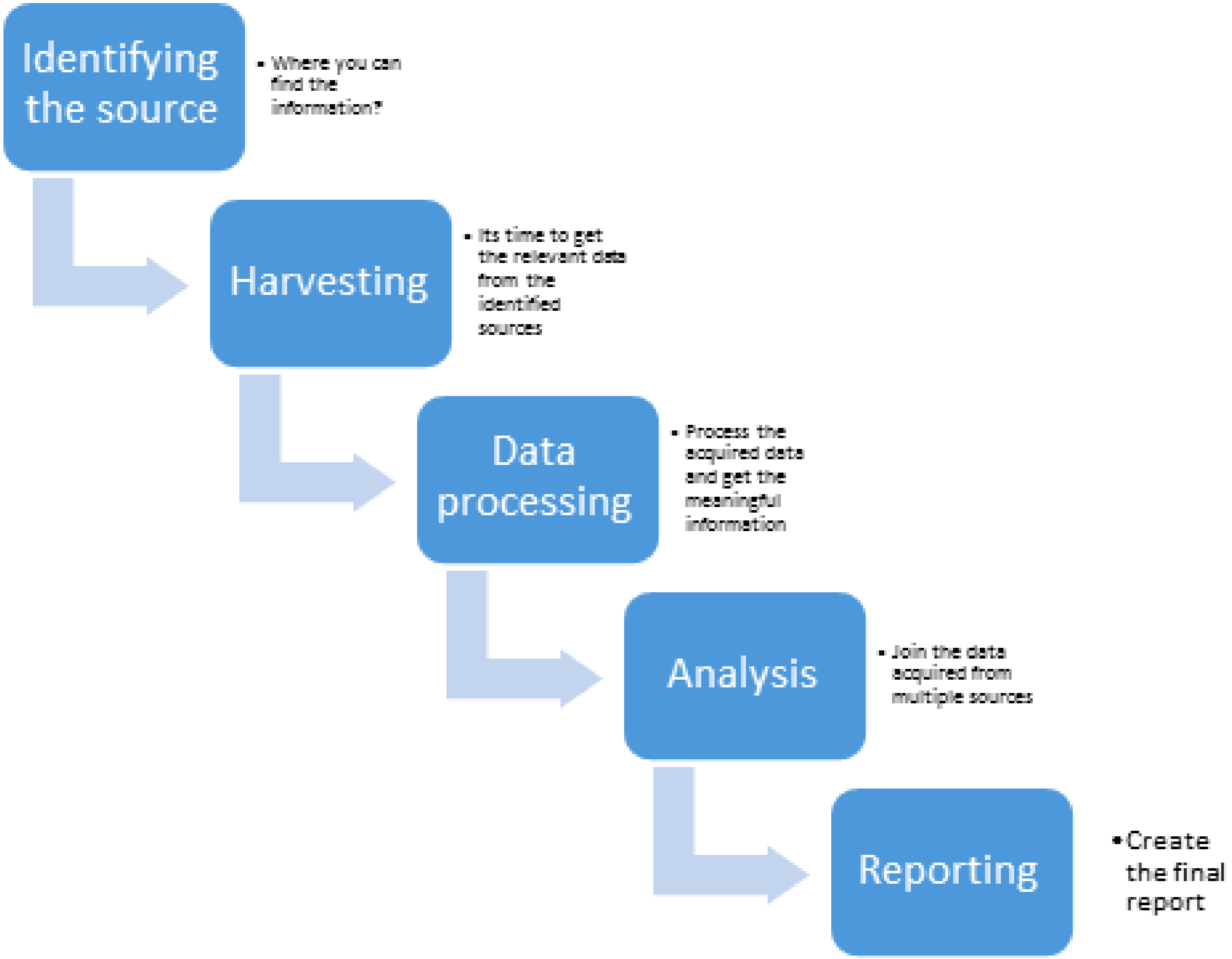
- Client proxy establishes key + circuit with Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2
- Etc.
- Client applications connect and communicate over TOR circuit


Router A Key
Router B Key
Router C Key
Message
Router A
Router B
Router C
Source
Destination

Open source intelligence (OSINT)

Open source intelligence (OSINT) is a form of intelligence collection management that involves finding, selecting, and acquiring information from publicly available sources and analyzing it to produce actionable intelligence.

OSINT Process



Identifying the source

- Where you can find the information?

Harvesting

- Its time to get the relevant data from the identified sources

Data processing

- Process the acquired data and get the meaningful information

Analysis

- Join the data acquired from multiple sources

Reporting

- Create the final report

The Web of Documents

- Surface Web
- – The web as we know it
- Deep Web

  – The web we all have access to
- Dark Web

  – The web where the darkness rule

Surface Web

- All indexed by search engines
- Is it bad? No
- Is it secure? Hardly, Yes
- Is this the majority? No

Deep Web

- Everything that sits behind password
- protected walls …
- Is it bad? Yes and No
- Is it secure? Relatively speaking, Yes
- Is this the majority? Yes (~94%)

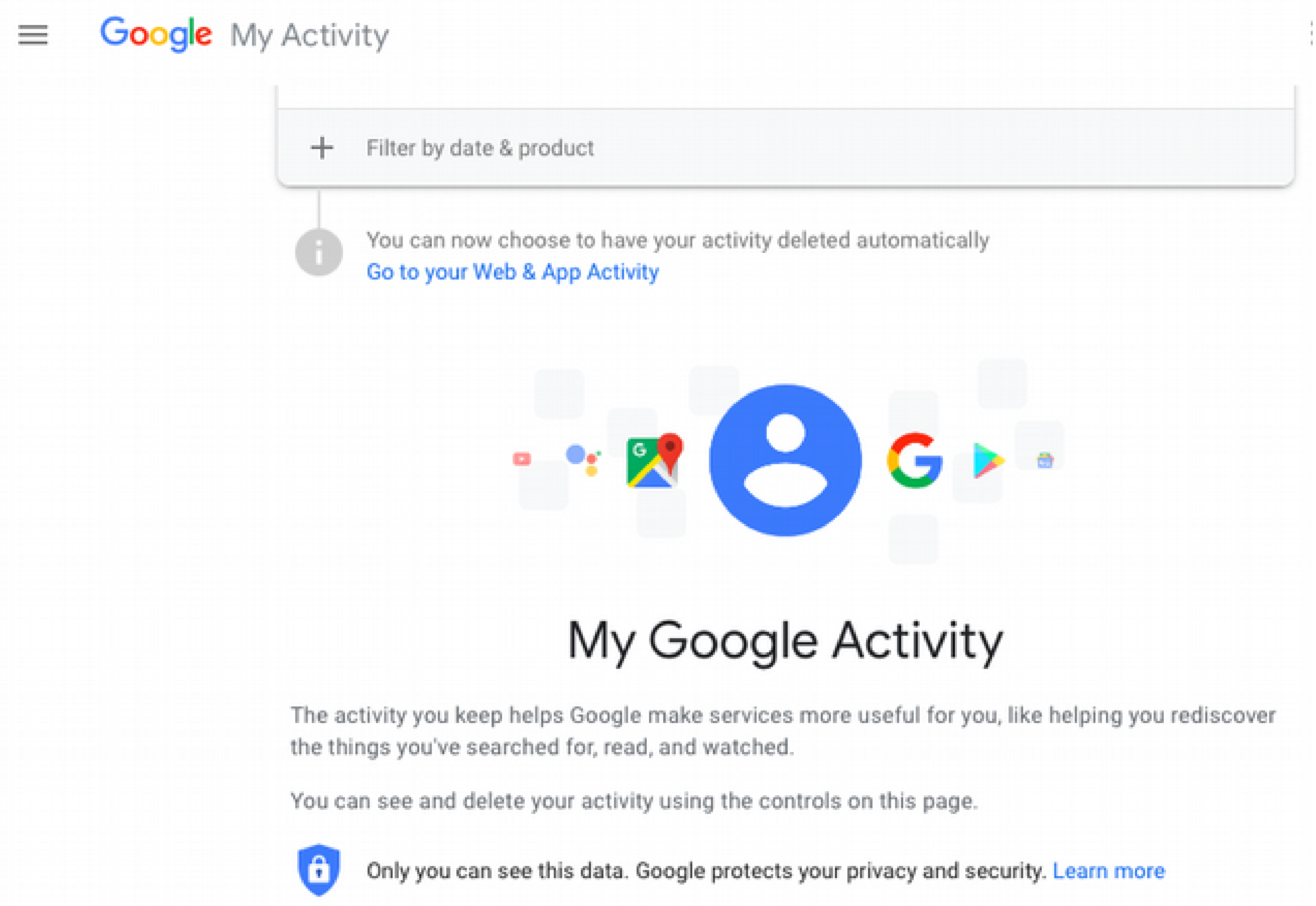
Dark Web

- Everything that you hear in movies ...
- Is it bad? Yes
- Is it secure? Yes
- Is this the majority? We don't know

Search Engines

Google, Bing, Yahoo – all the major search engines track your search history and build profiles on you, serving different results based on your search history.

myactivity.google.com



You can now choose to have your activity deleted automatically

Go to your Web & App Activity

My Google Activity

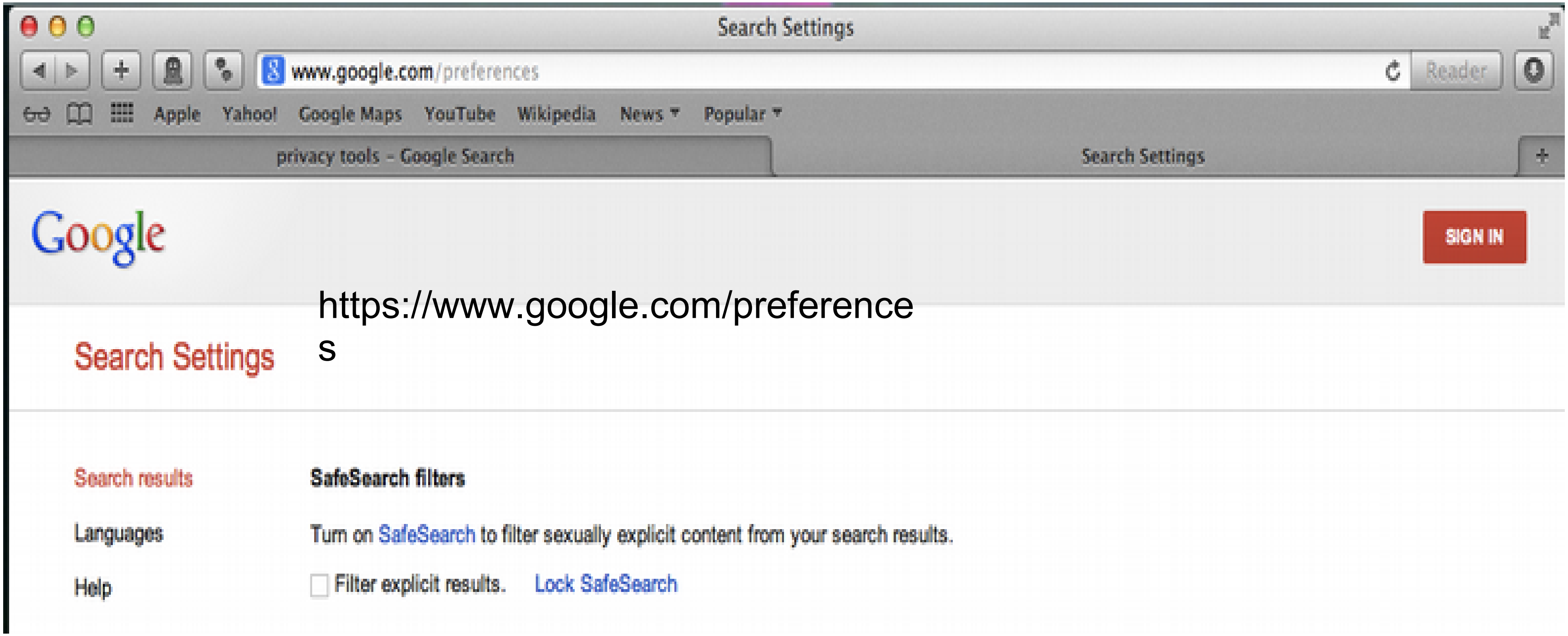
The activity you keep helps Google make services more useful for you, like helping you rediscover the things you've searched for, read, and watched.

You can see and delete your activity using the controls on this page.

Only you can see this data. Google protects your privacy and security. Learn more

Search Setting

https://www.google.com/preferences



https://www.google.com/preference
s

Search Settings

Search results

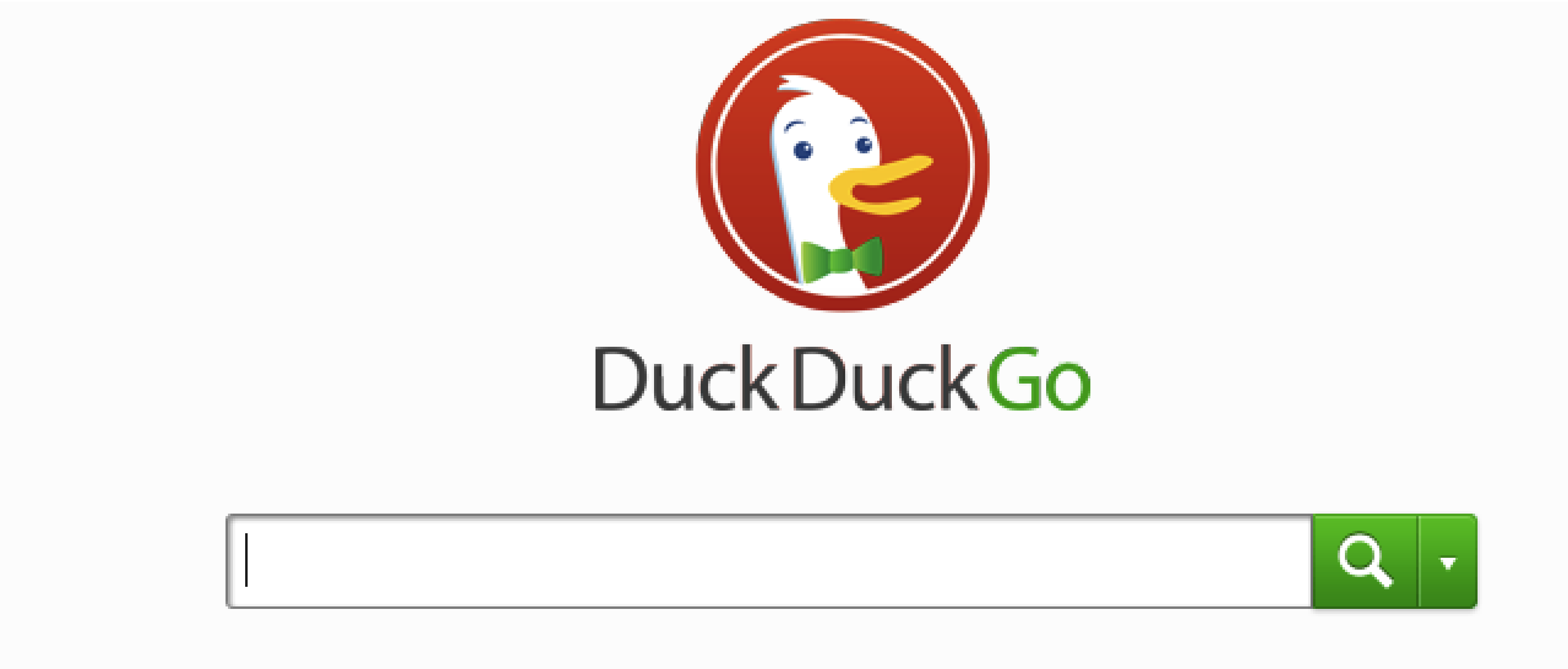
Languages

Help

SafeSearch filters

Turn on SafeSearch to filter sexually explicit content from your search results.

□ Filter explicit results. Lock SafeSearch


DuckDuckGo

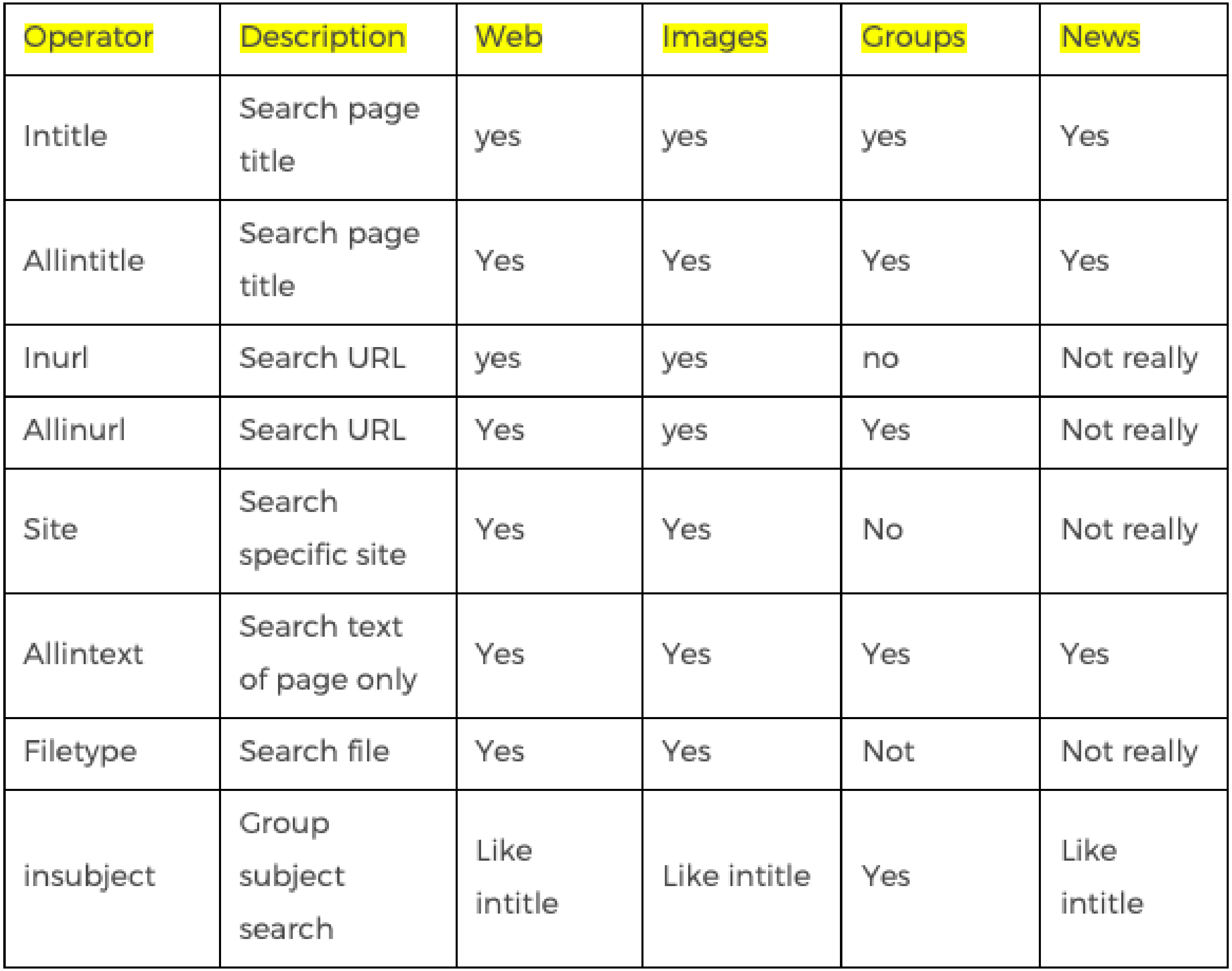
Google Dorks -Google Hacking

Google Dorks can help a user to target the search or index the results in a better and more efficient way.

Let us say that the user wants to search for the word usernames but only requires the results with PDF files and not websites.

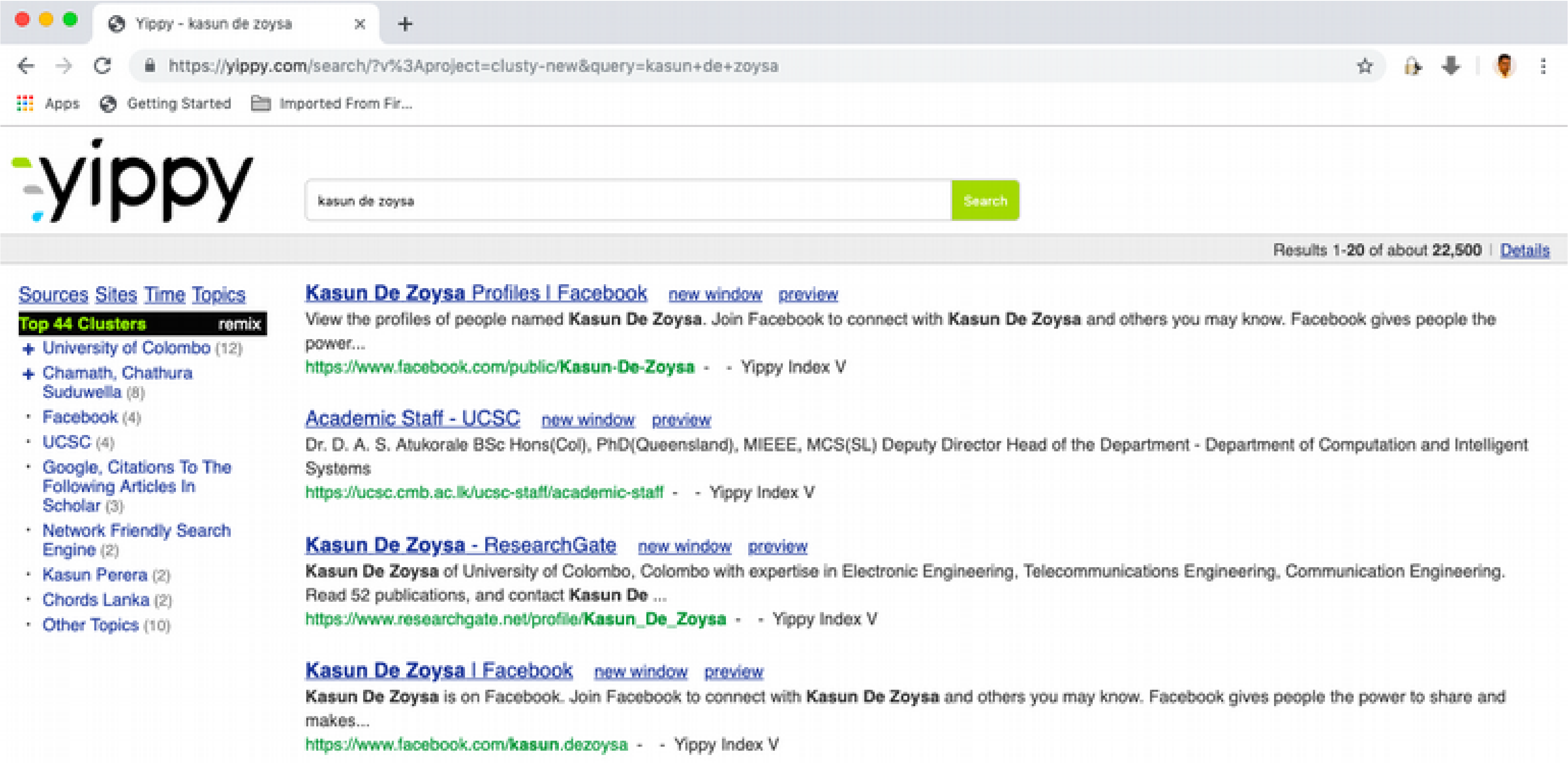
Usernames Filetype:pdf

Advance search operator – Google



Operator	Description	Web	Images	Groups	News
Intitle	Search page title	yes	yes	yes	Yes
Allintitle	Search page title	Yes	Yes	Yes	Yes
Inurl	Search URL	yes	yes	no	Not really
Allinurl	Search URL	Yes	yes	Yes	Not really
Site	Search specific site	Yes	Yes	No	Not really
Allintext	Search text of page only	Yes	Yes	Yes	Yes
Filetype	Search file	Yes	Yes	Not	Not really
insubject	Group subject search	Like intitle	Like intitle	Yes	Like intitle

Yippy Clustering Search Engine


Yippy - kasun de zoysa
https://yippy.com/search/?v%3Aproject=clusty-new&query=kasun+de+zoysa
Apps
Getting Started
Imported From Fir...
yippy
Search
Sources Sites Time Topics
Top 44 Clusters
remix

kasun de zoysa

Results 1-20 of about **22,500** | Details

- University of Colombo (12)
- Chamath, Chathura Suduwella (8)
- Facebook (4)
- UCSC (4)
- Google, Citations To The Following Articles In Scholar (3)
- Network Friendly Search Engine (2)
- Kasun Perera (2)
- Chords Lanka (2)
- Other Topics (10)

Kasun De Zoysa Profiles | Facebook new window preview

View the profiles of people named **Kasun De Zoysa**. Join Facebook to connect with **Kasun De Zoysa** and others you may know. Facebook gives people the power...

https://www.facebook.com/public/**Kasun-De-Zoysa** - - Yippy Index V

Academic Staff - UCSC new window preview

Dr. D. A. S. Atukorale BSc Hons(Col), PhD(Queensland), MIEEE, MCS(SL) Deputy Director Head of the Department - Department of Computation and Intelligent Systems

https://ucsc.cmb.ac.lk/ucsc-staff/academic-staff - - Yippy Index V

Kasun De Zoysa - ResearchGate new window preview

Kasun De Zoysa of University of Colombo, Colombo with expertise in Electronic Engineering, Telecommunications Engineering, Communication Engineering. Read 52 publications, and contact **Kasun De** ...

https://www.researchgate.net/profile/**Kasun_De_Zoysa** - - Yippy Index V

Kasun De Zoysa | Facebook new window preview

Kasun De Zoysa is on Facebook. Join Facebook to connect with **Kasun De Zoysa** and others you may know. Facebook gives people the power to share and makes...

https://www.facebook.com/**kasun**.dezoysa - - Yippy Index V

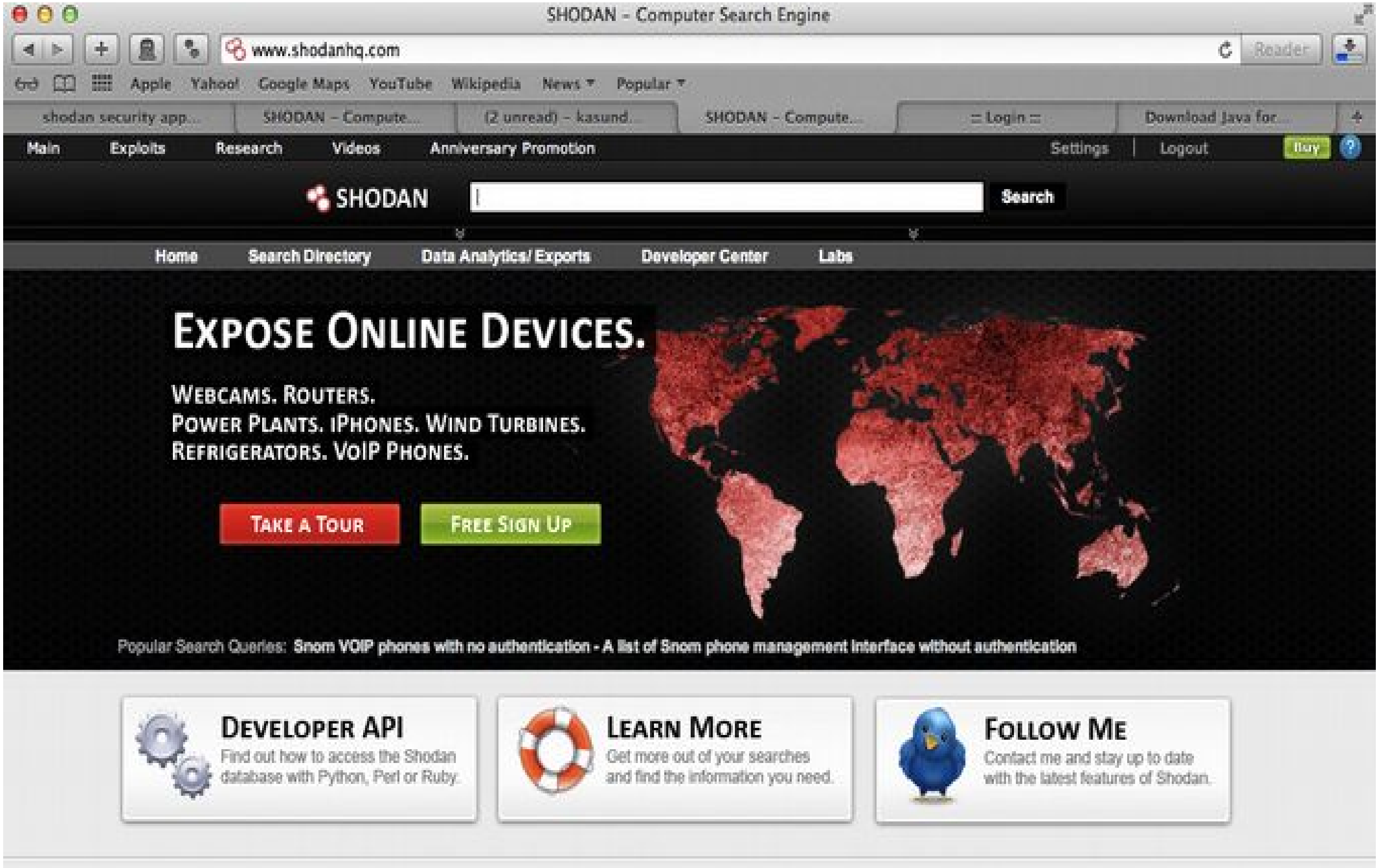
TheHarvester

TheHarvester is a tool, written by Christian Martorella, that can be used to gather e-mail accounts and subdomain names from different public sources (search engines, pgp key servers).

- DEMO:

```
theHarvester -d cmb.ac.lk -l 500
-b google
```

www.shodanhq.com



EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

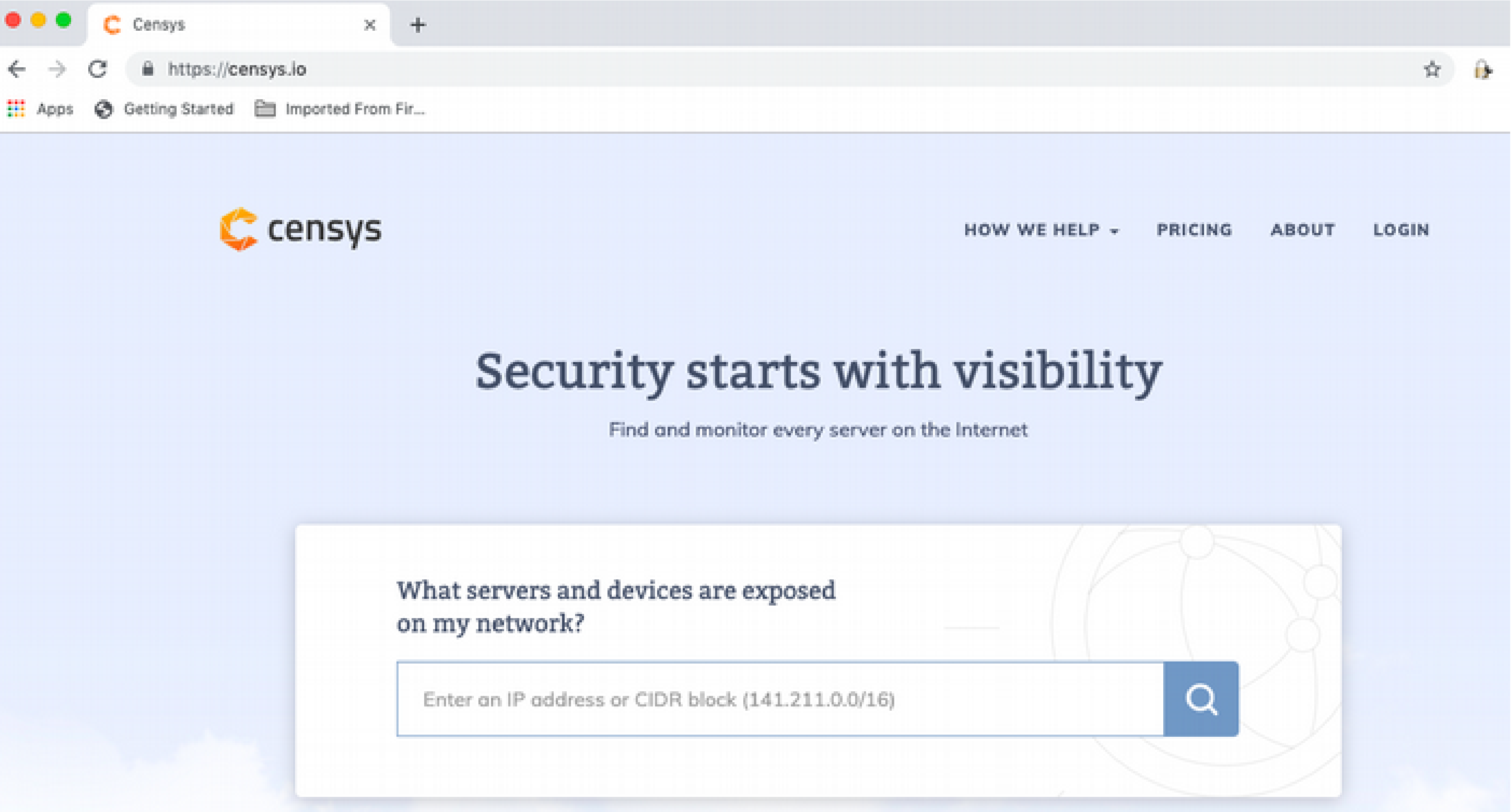
Popular Search Queries: Snom VOIP phones with no authentication - A list of Snom phone management interface without authentication

DEVELOPER API
Find out how to access the Shodan database with Python, Perl or Ruby.

LEARN MORE
Get more out of your searches and find the information you need.

FOLLOW ME
Contact me and stay up to date with the latest features of Shodan.

censys.io



Censys

https://censys.io

Security starts with visibility

Find and monitor every server on the Internet

What servers and devices are exposed on my network?

Enter an IP address or CIDR block (141.211.0.0/16)

```
location.country_code: LK and protocols:
("23/telnet" or "21/ftp")
```

http://www.tweetstats.com/

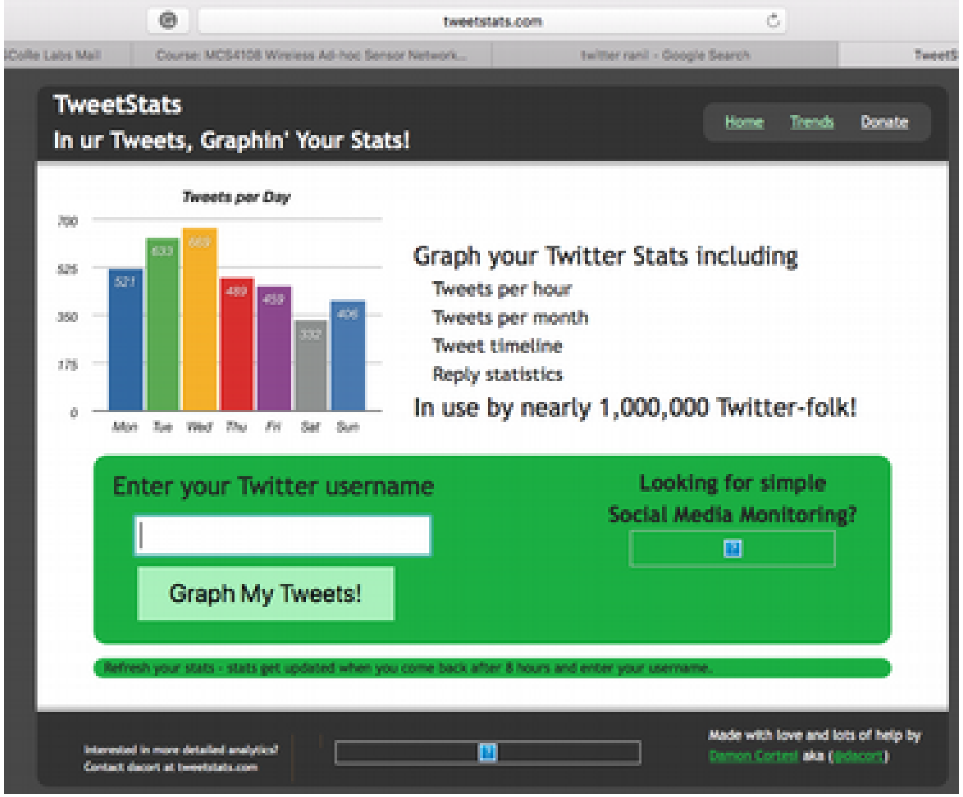
http://www.mytwitterbirthday.com

https://sociograph.io/

https://likealyzer.com/

SOCIOGRAPH

Analytics for Facebook Groups and Pages



TweetStats

In ur Tweets, Graphin' Your Stats!

Graph your Twitter Stats including

Tweets per hour
Tweets per month
Tweet timeline
Reply statistics

In use by nearly 1,000,000 Twitter-folk!

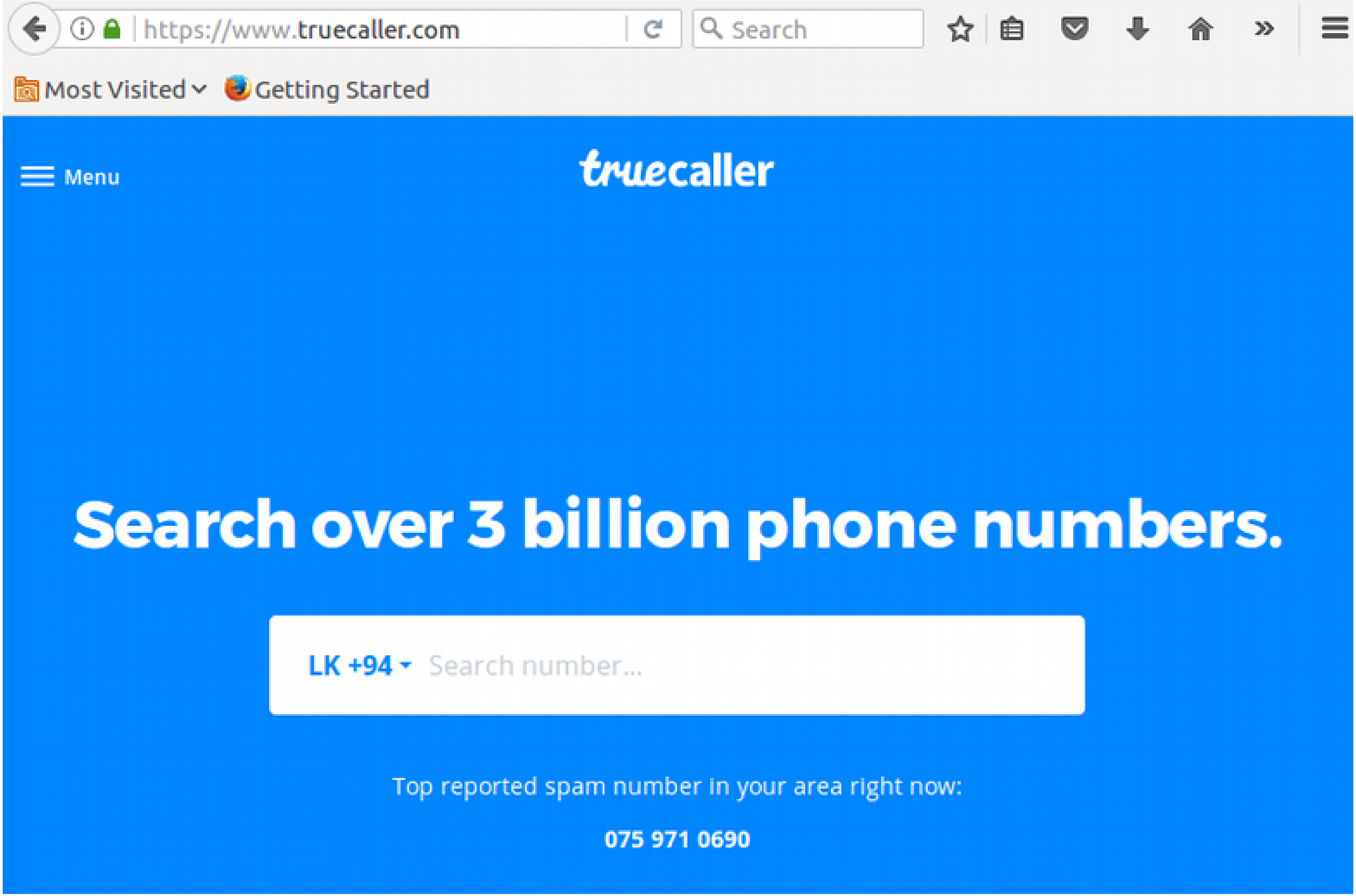
Enter your Twitter username

Looking for simple Social Media Monitoring?

Refresh your stats - stats get updated when you come back after 8 hours and enter your username.

Interested in more detailed analytics?
Contact dacort at tweetstats.com

Made with love and lots of help by
Damon Cortesi aka (@dacort)



Search over 3 billion phone numbers.

Top reported spam number in your area right now:

075 971 0690

e-mail: kasun@ucsc.cmb.ac.lk