Digital Security
Tools & Strategies

Dmitri Vitaliev

dmitri@equalit.ie

6765 11E9 33AC 3F9D 1A4B 0AAC 7110 EACE 6FF1 895D

DIGITAL SECURITY FOR CIVIL SOCIETY

Free. Open Source. Principled.

CENO

DEFLECT

WEB SECURITY

ORGANIZATIONAL SECURITY

SOFTWARE DEVELOPMENT

https://equalit.ie

@equalit.ie

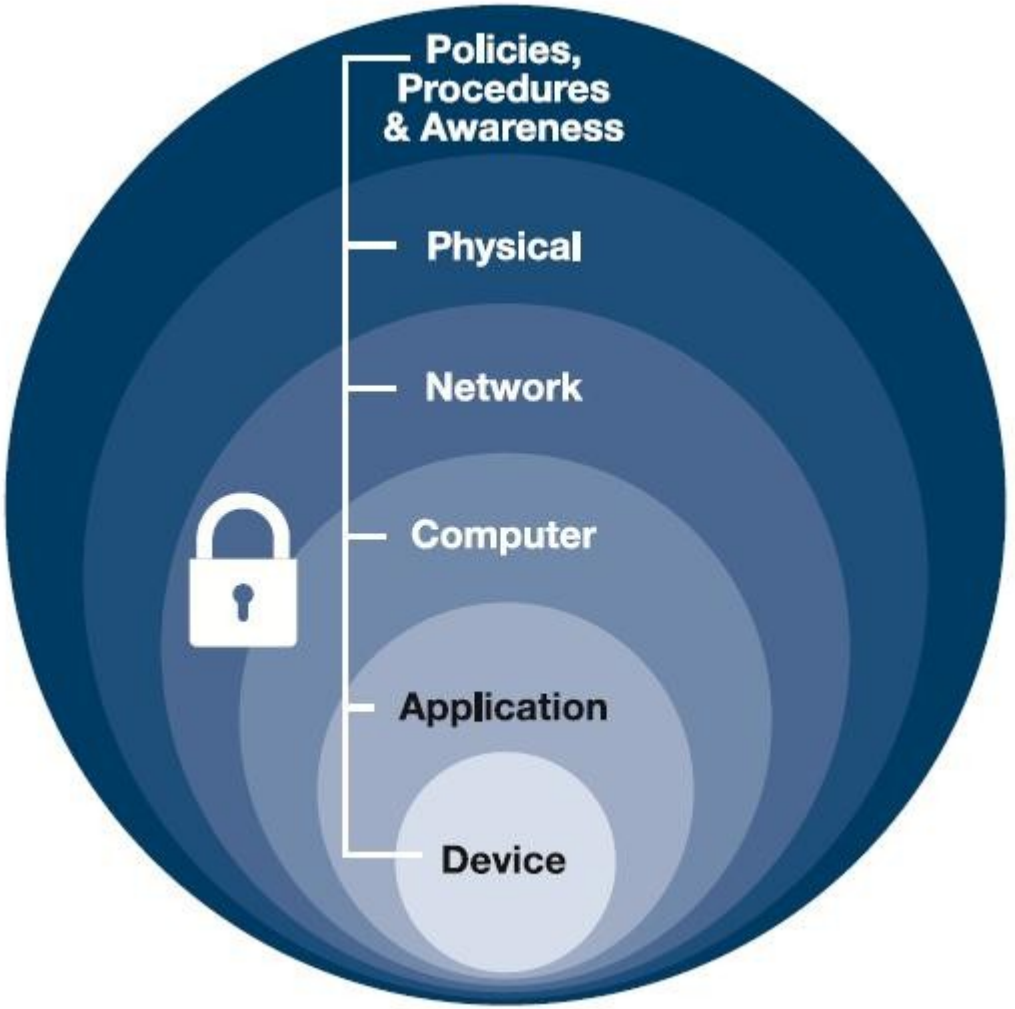
Goals

- Security as process
- The known unknowns
- Leading by example

Issues

- Hacking & spear phishing
- Surveillance & censorship
- Device security

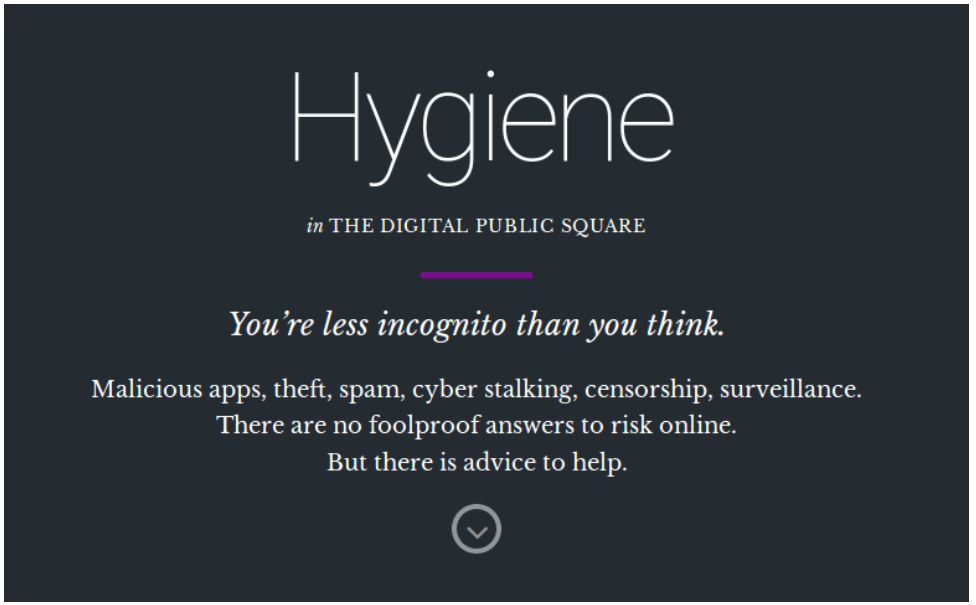
Defence in depth



https://securityinabox.org

PRISM BREAK

https://prism-break.org

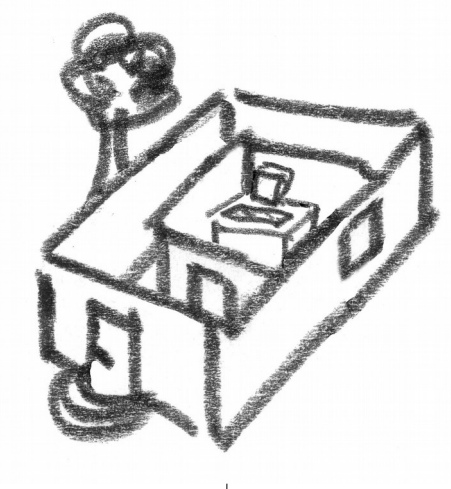


https://hygiene.digitalpublicsquare.com

Security ?

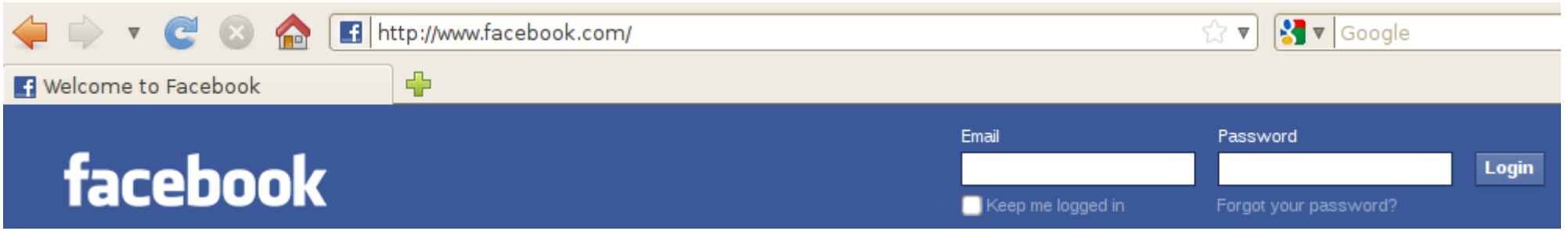
Anonymity

Privacy



Authenticity

Immunity

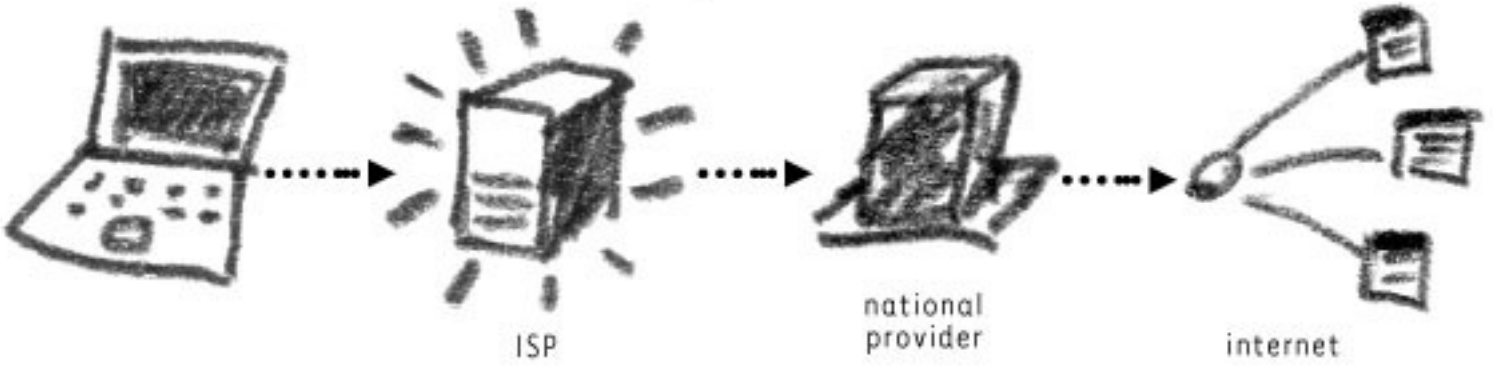


Malware

Password

IP identification

Censorship



Temporary files

Surveillance

Profiling

1. Hacking & spearphishing

Malware

XSS

Worm

RootKit

0-day exploit

Virus

Trojan

Keylogger

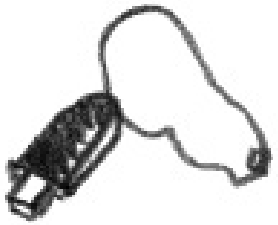
Drive-by downloader

Spyware

Backdoor

Ransomware

off-the-shelf computer surveillance technologies



Tails

theamnesicincognitolivesystem

ubuntu

Password Management

Profiling

Social Engineering

Brute Force

Phishing

Spear phishing

Honey trap

100, 000 passwords / second

Length/Variations	26	36	52	68
3	0.18 seconds	0.47 seconds	1.41 seconds	3.14 seconds
5	1.98 minutes	10.1 minutes	1.06 hours	4.0.4 hours
8	24.2 days	10.7 months	17 years	1.45 centuries
10	44.8 years	1.16 millenia	45.8 millenia	45, 582 millenia

Password Management

Mnemonics

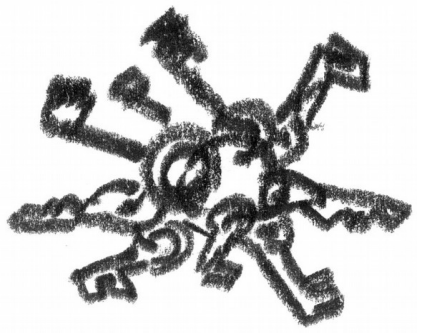
I had a dream, where all men were born equal

1haDwaMwB=

Will you still need me, will you still feed me, when I'm 64?

wysnm,wysfm,wi64?

The slings and arrows of outrageous fortune



Password Management

Google

Accounts

Account
Security
Profile and privacy
Google+
Products
Language
Data liberation

Password management Change password

2-step verification Status: ON Edit

Authorizing applications and sites Edit

Your security info protects your account

If you ever forget your password, we need a way to help you g
this to spam you—just to keep your account more secure.

Phone number

Add

Alternate email address

Add

dublindimi@hotmail.com
Delete

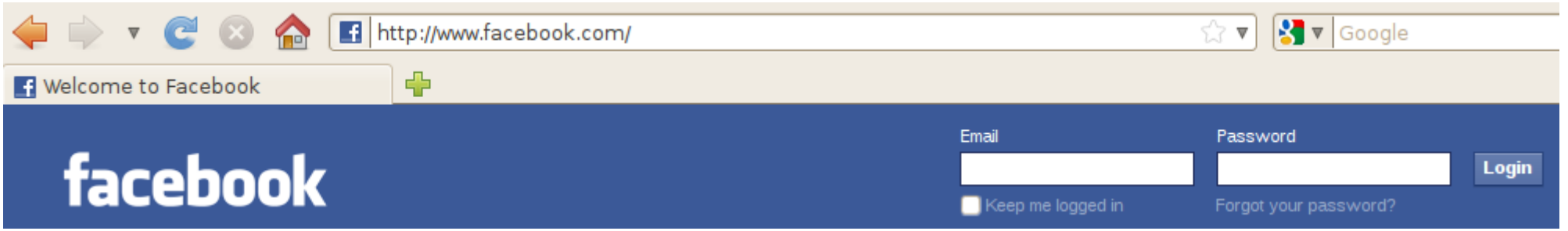
Trusted PC

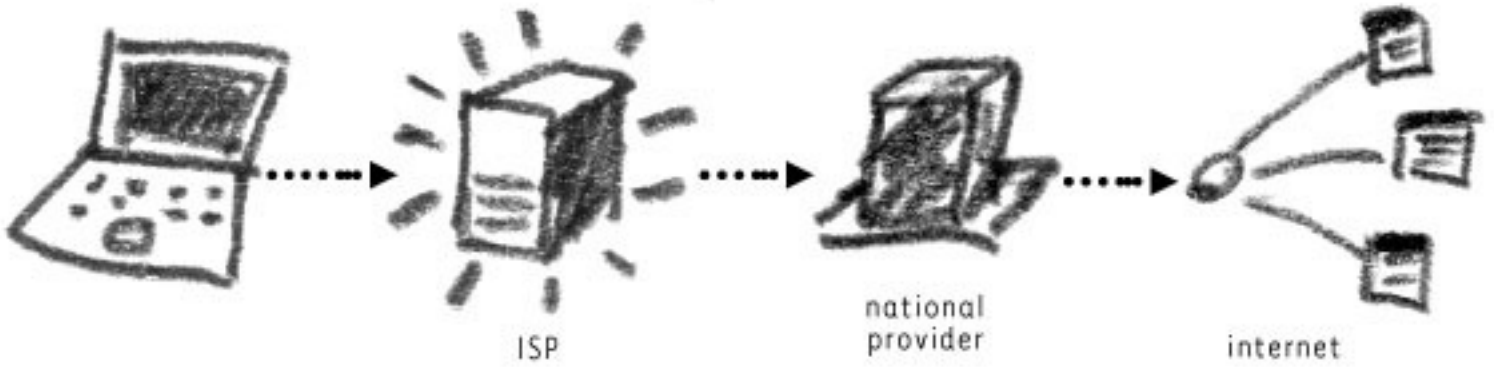
To add a trusted PC to your account, you need to access your account using Internet Explorer and have Windows Live Essentials installed.

Security question

Father's middle name?
Change

2. Surveillance & profiling



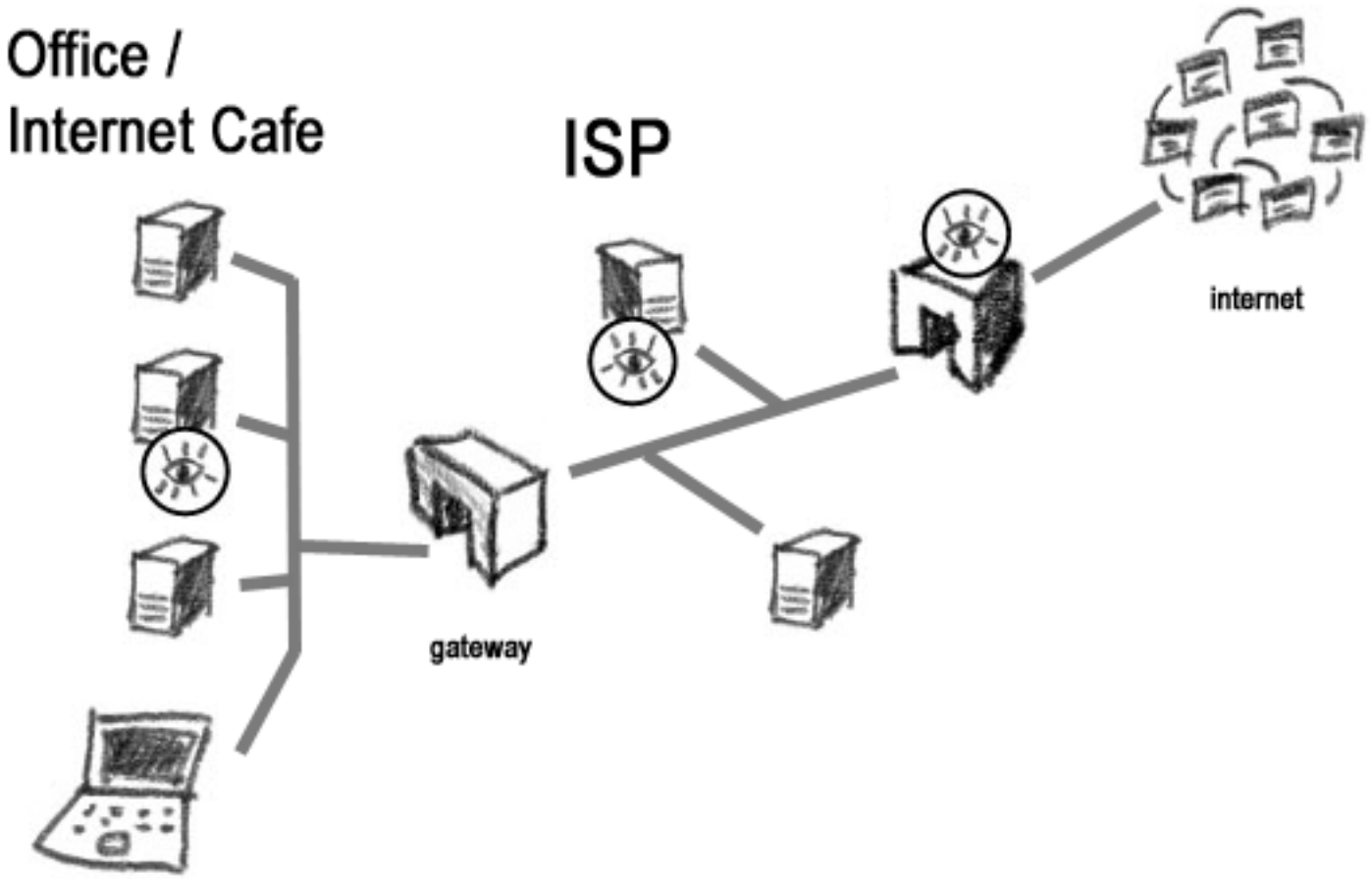


IP ADDRESS = 91.198.26.138

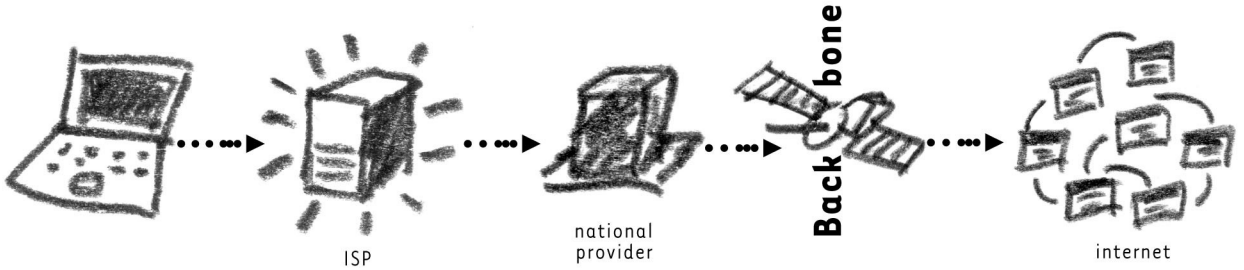
Content and application standards

Technical standards (TCP, IP, DNS etc.)

Telecommunication infrastructure



IP:91.198.26.138



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-w
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 HT
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=14
127	46.381720	euroradio.fm	192.168.1.11	TCP	http > hb-engine [SYN, ACK] Seq=0 Ack=1 Win=5840 Le
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

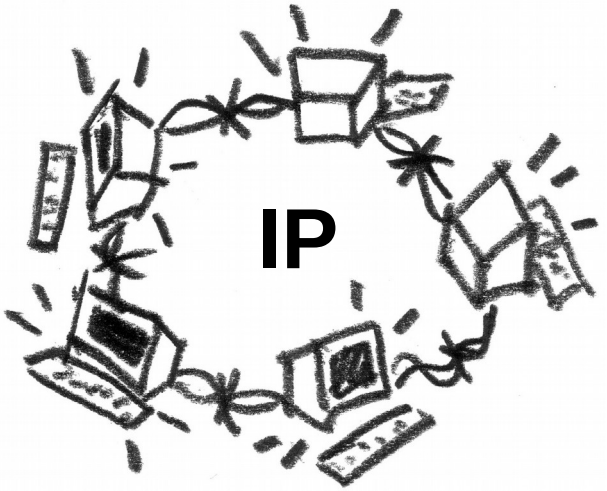
```
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://euroradio.fm/admin/login.php
Cookie: PHPSESSID=48e3ed080d2e50510271cca2131f7334
Content-Type: application/x-www-form-urlencoded
Content-Length: 170

f_is_encrypted=1&f_user_name=dmvit&f_password=KyFzt8fOfkGGeeU0fc&f_login_language=en&Login=Login&f_xkoery=f14314bf4d4a1b
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

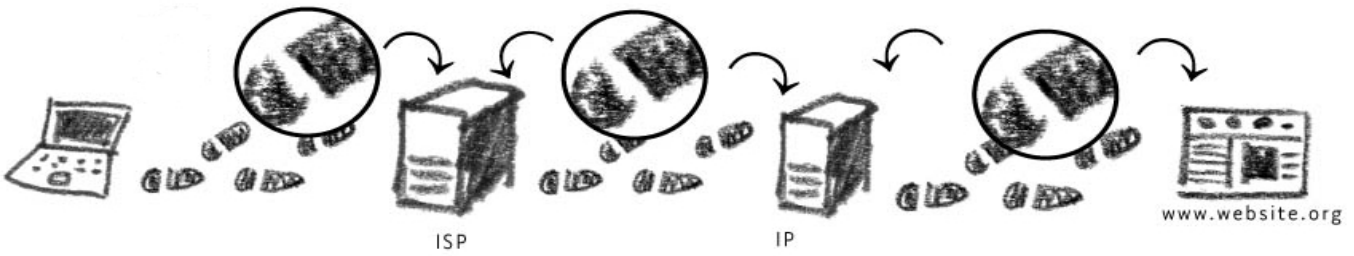
Profiling



facebook

Location

Identity



wikipedia.org/wiki/Mobile_phone_tracking

Network: MIPS, MIN, SIM
Handset: IMEI, GPS
WIFI: GPS & Crowdsourced
Hybrid: !

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Tasking Process

ONYX

CARNIVORE

ECHELON

Titan

ECHELON intercept station at Menwith Hill, England

Project 6

SORM-2

Golden shield

NATGRID

PRISM +

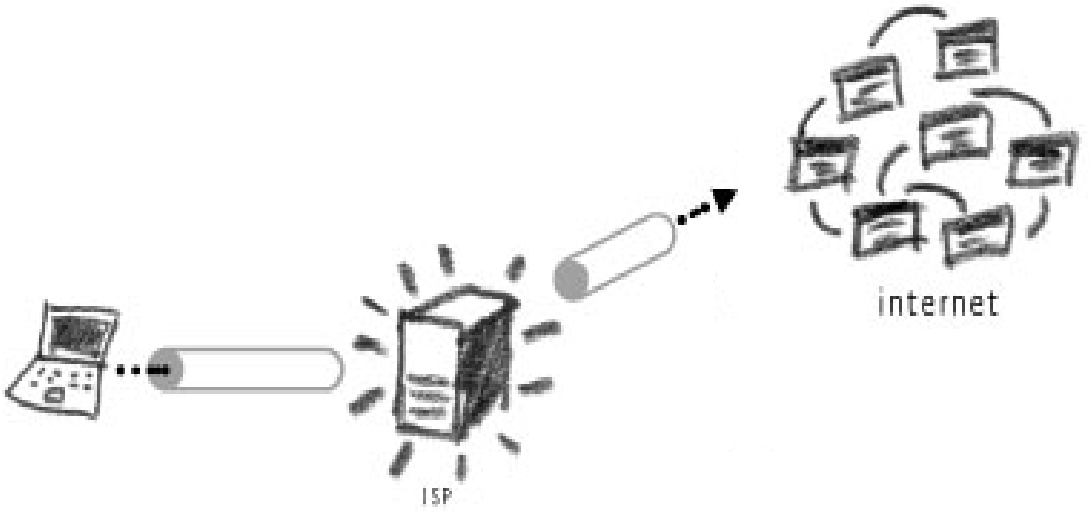
XKeyscore

Frenchelon

MUSCULAR

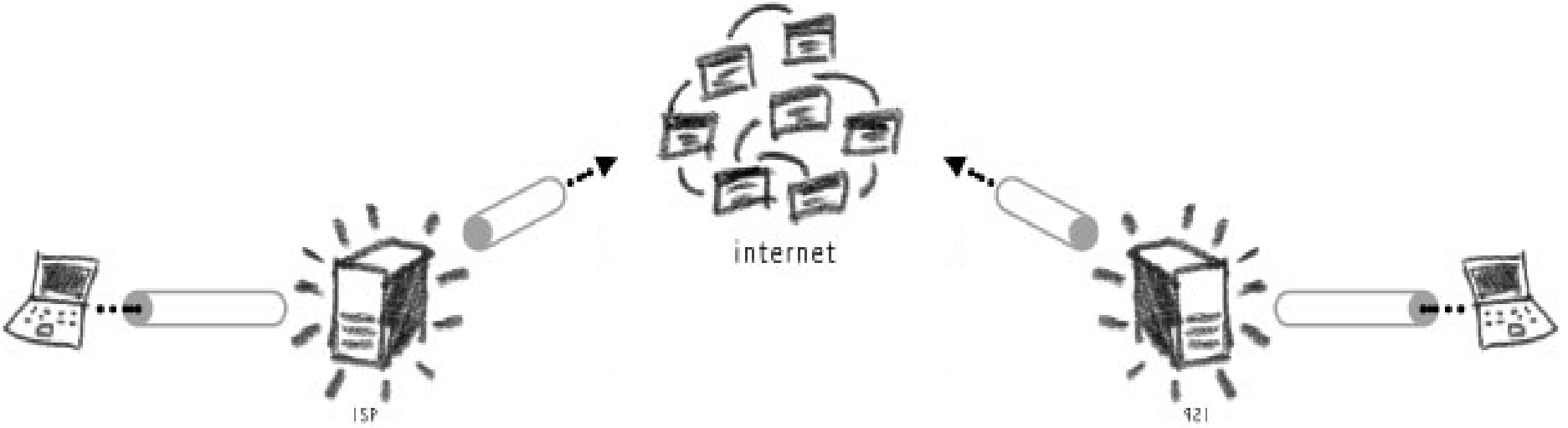
TEMPORA

Mystic

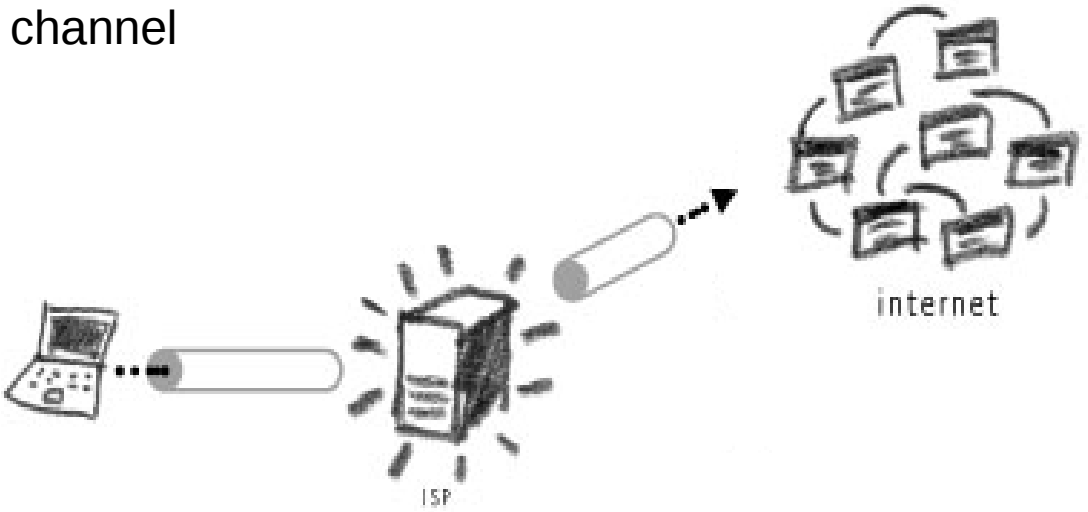


Secure Sockets Layer (SSL)

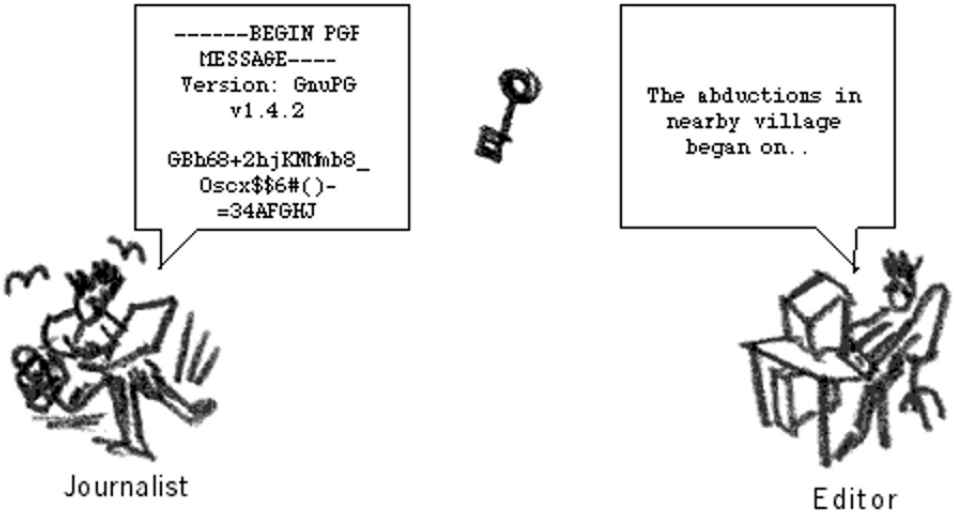
Transport Security Layer (TLS)



Encrypting the channel



Encrypting the content



PGP®

Public key encryption

Step 1: Give your public key to the sender

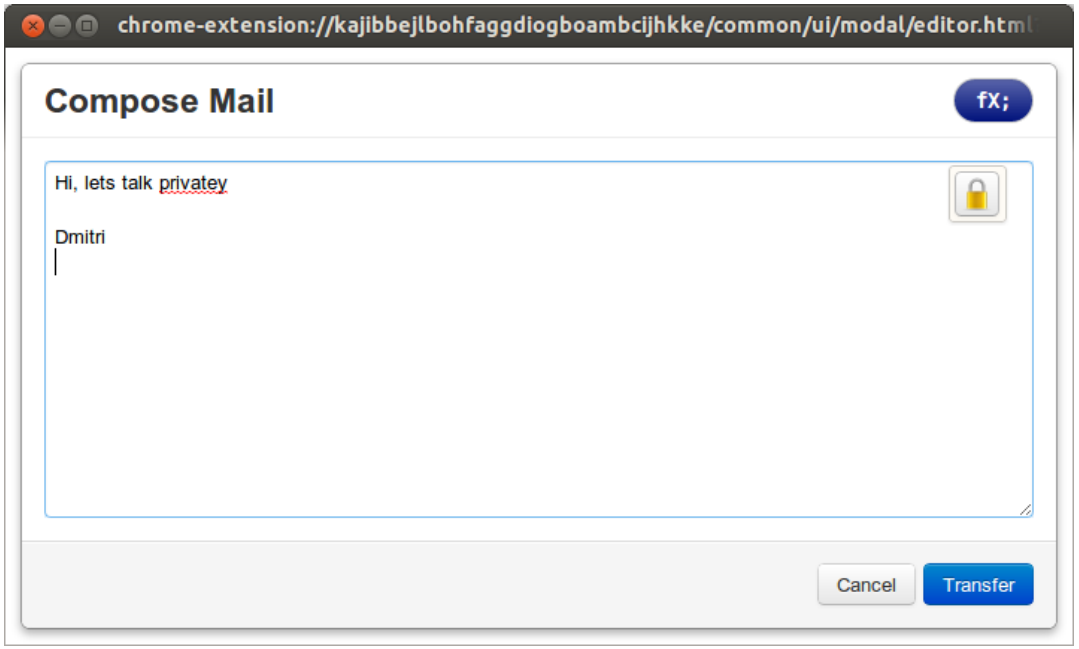
Step 2: Sender uses your public key to encrypt the plaintext

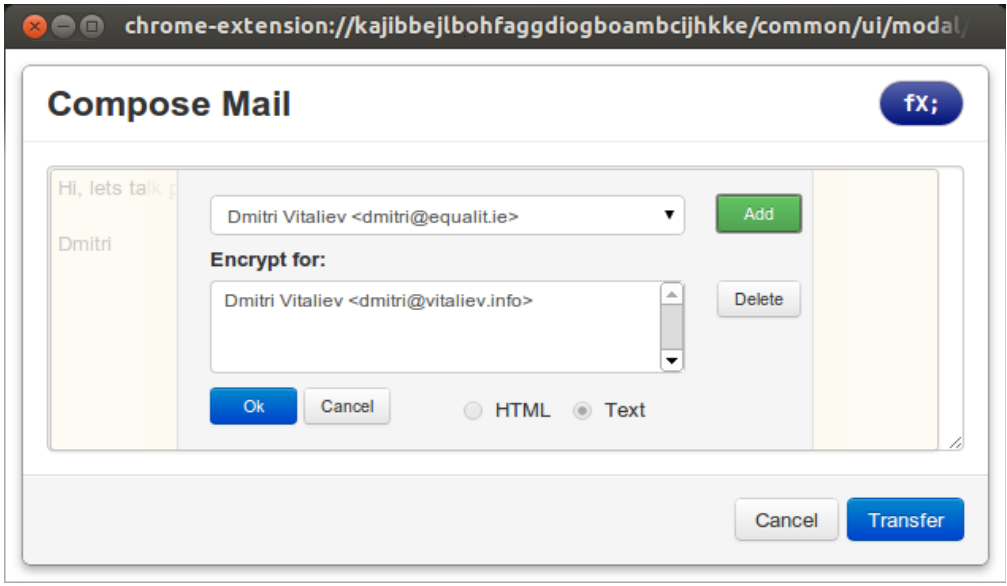
Step 3: Sender gives the ciphertext to you

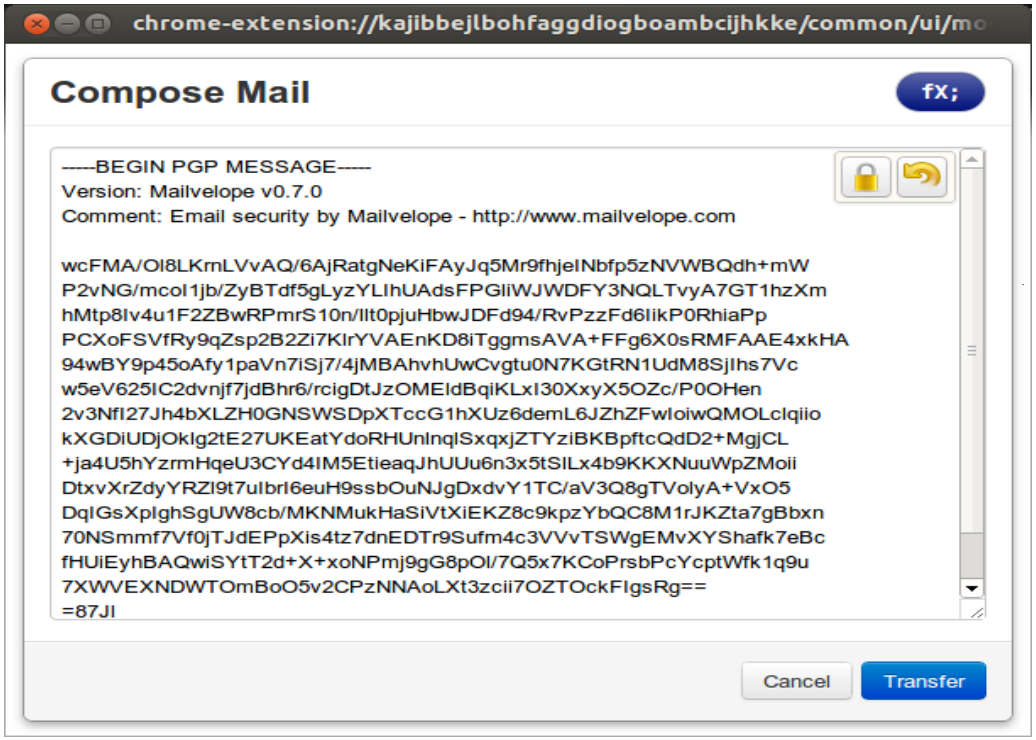
Step 4: Use your private key (and passphrase) to decrypt the ciphertext

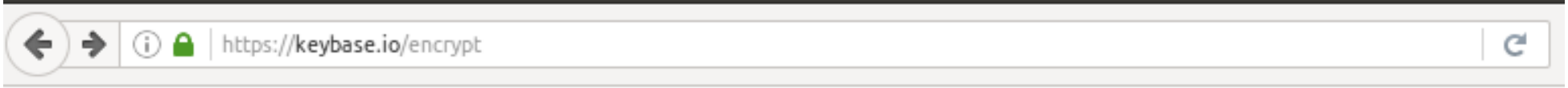
CRYPTO WARS

mailvelope.com









Keybase

Encrypt | Decrypt | Sign | Verify

Success! You can paste the below message into an email, IM, whatever.

The secret message

```
-----BEGIN PGP MESSAGE-----
Version: Keybase OpenPGP v2.0.53
Comment: https://keybase.io/crypto

wcFMA/Ol8LKrnLVvAQ//eMzItEs3puJoujrlluY77+61vQrvfLLZfTQZJRB+km6z
NbcTsi268U3cKOkg9IBdmwLkHU7VyhEqC+ge3s49/TNH//Q68HkBqBXVHf+b3OSH
Ay/GV0vvb6I9Y88OkjdzzV5uOaf1yfIyYog0trk0AQMPSlGrzLQFWWhjr1SMOv6s
qGEY03rPtweXhfjY41LYRA8rtzX3jYtq7oFWqPt8fGcMdtQh4d/XFU8qvFJsy3Kp
yj8BNHNpWK0hOfKdfDZJJeVDG66zTmuzk85bj/QbgOC2rTXRzK7g1cGQA2x4XNvg
zng2T5dy47OALYaWW2mQ6+Pk8NBUKYL5BfkbJFJPsdBr0uvDseP2r3wAM20aFmhO
FbF1JrKNzDsOAfJeFGqcHAL+aHtqobXqgtvJF36qATX3xPCQkie5m54/nALXOr0n
```

Edit | Done - nuke the plaintext

peerio

ChatSecure

SILENT CIRCLE

WhatsApp

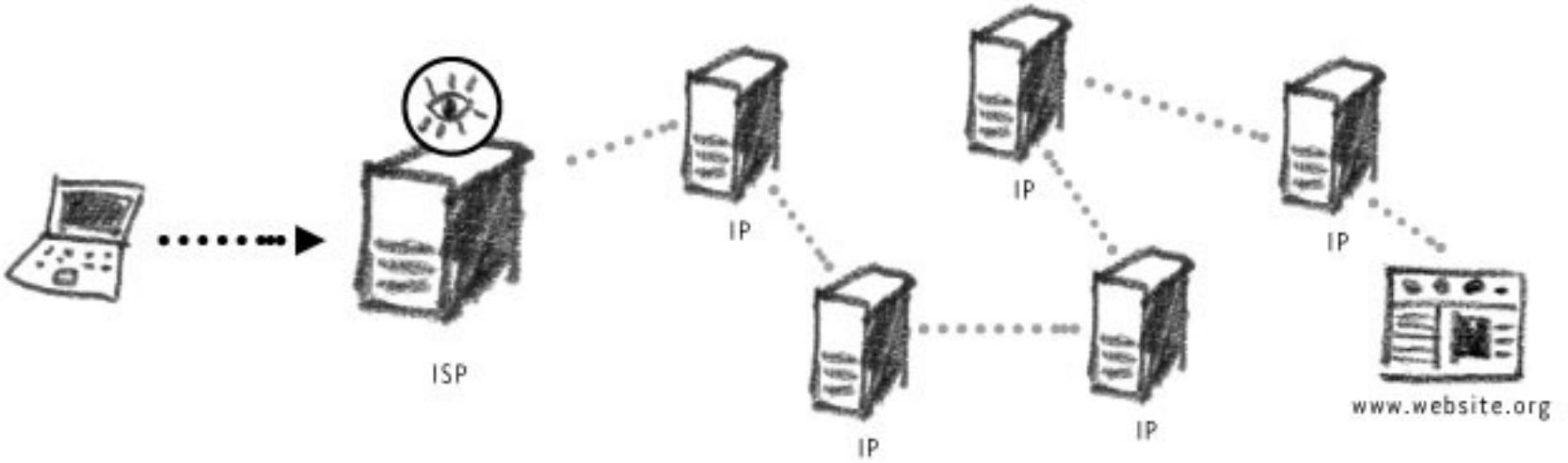
Signal Private Messenger

wire™

Telegram

Wickr

ESCAPE THE INTERNET®

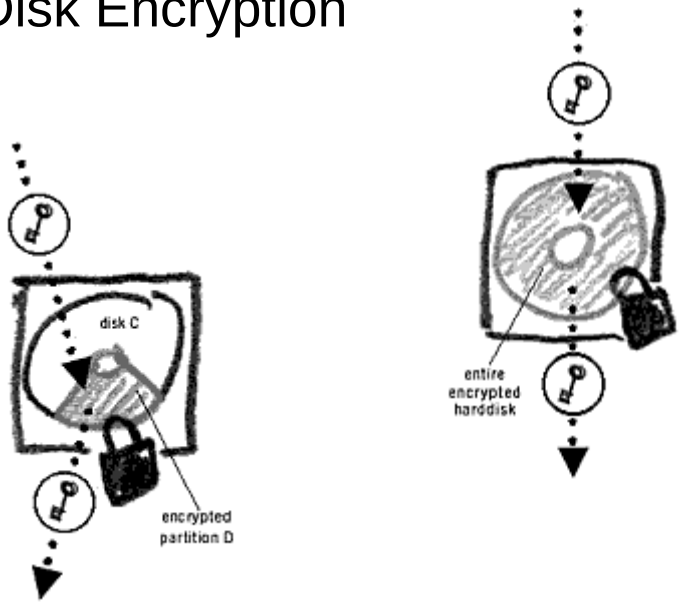

IP
IP
IP
IP
ISP
IP
www.website.org

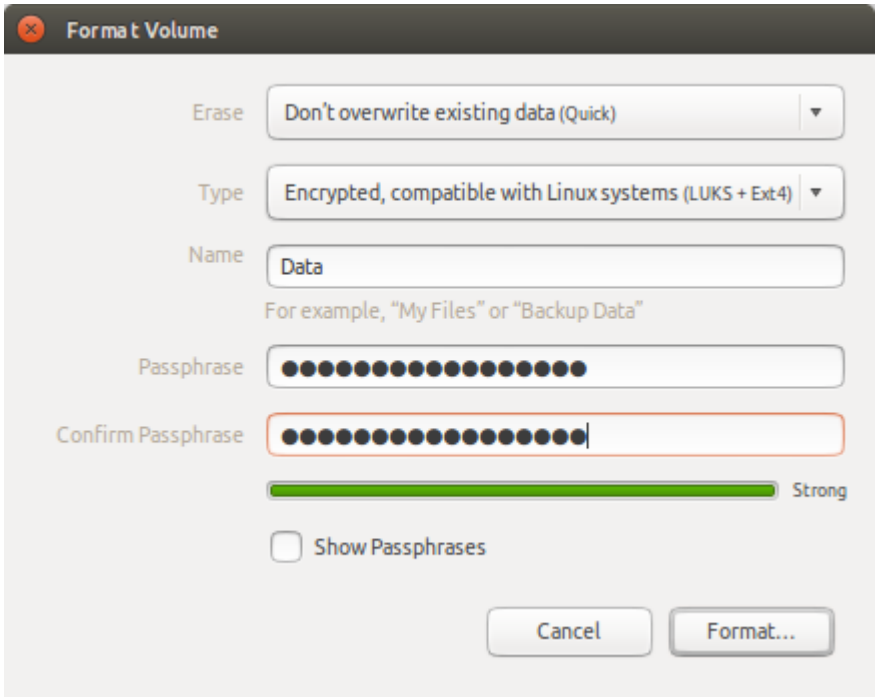

My IP Address Lookup - Community Geotarget IP Project - what country, city ip addresses map to - IP Trace - Torpark
File Edit View Go Bookmarks Tools Help
http://www.hostip.info/
hostip.info
IP Address Lookup Using the API Download Contribute Forum Privacy About
My IP Address Lookup - Geolocate Visitors by IP Address
Hostip.info is a community-based project to geolocate IP addresses, making the database freely available (see below) but it needs you to put in your city to make it work. It only takes 10 seconds, and you'll get a warm fuzzy feeling of 'doing the right thing' :-)
Try the example to the right for an IP Trace, or to Lookup IP Addresses.
We now have >850,000 entries in the database!
Geostats BETA - NEW! Map your traffic geographically.
Your IP Address: 149.9.0.59
Napoli, ITALY
Is this wrong? Make a correction
Are you a host? Netblock upload
Firefox/Mozilla Search Plugin
PLUGIN SET IT NOW
Firefox Plugin: hostipfox
Download the new plugin now and tell us what you think
Done
Tor Enabled
149.9.0.59
Adblock

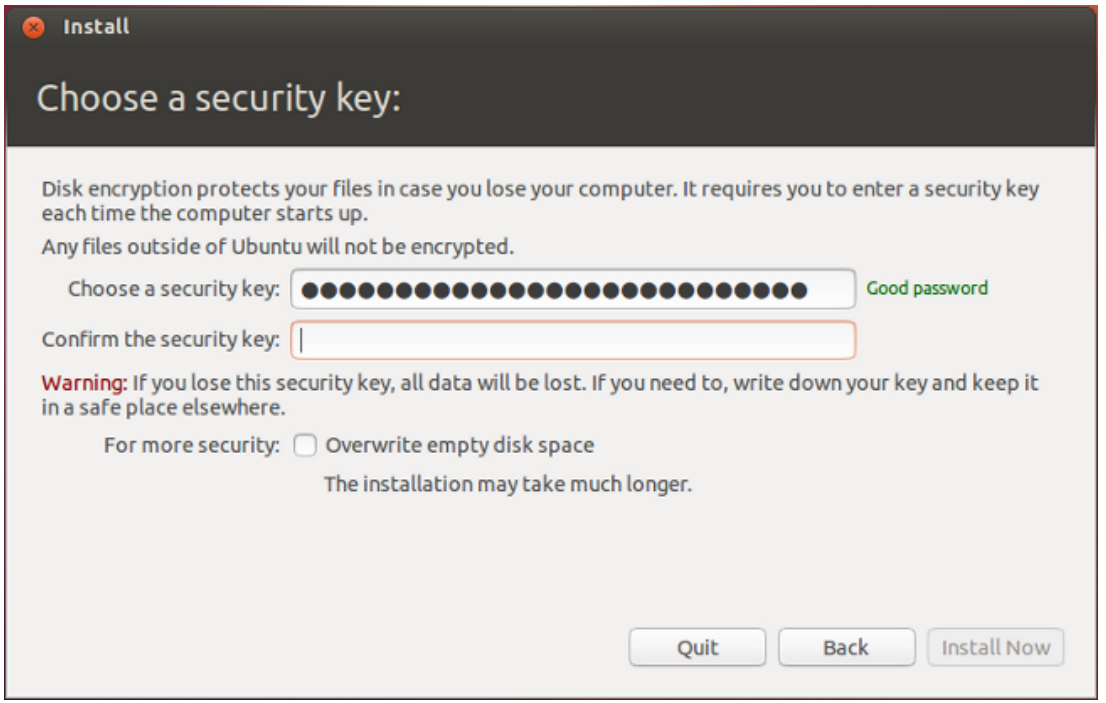

Tor

3. Device security

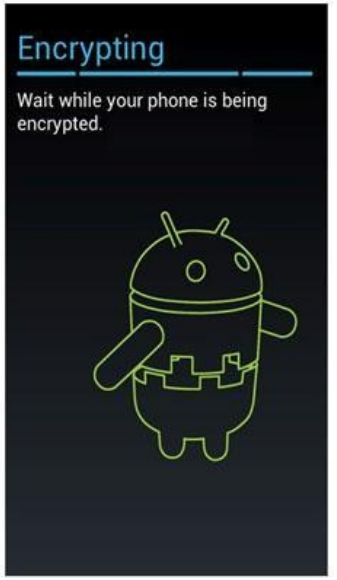
Disk Encryption

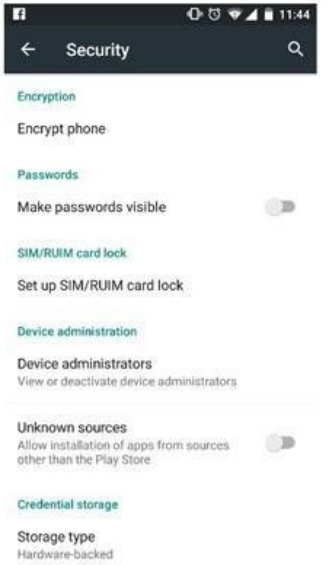


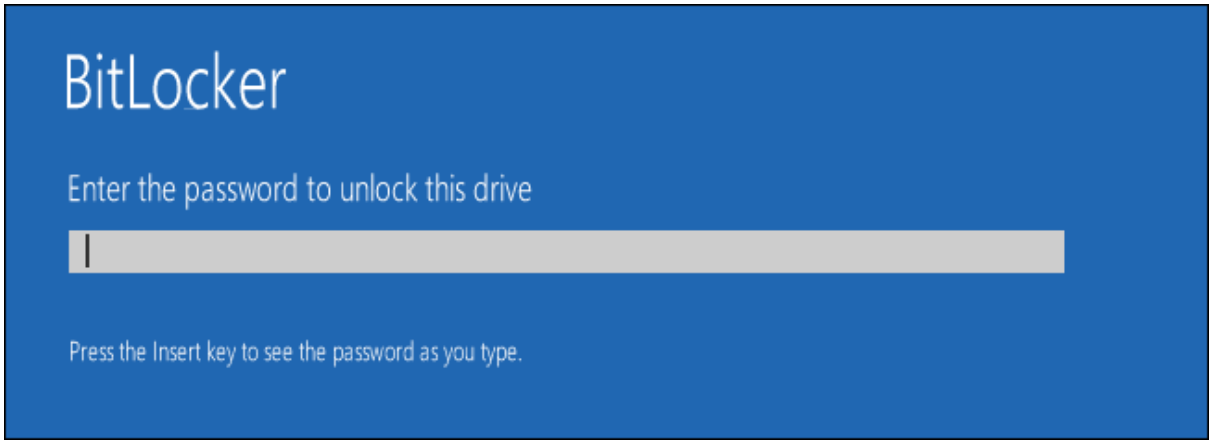





Security
Show All
General
FileVault
Firewall
FileVault secures your home folder by encrypting its contents. It automatically encrypts and decrypts your files while you're using them.
WARNING:Your files will be encrypted using your login password. If you forget your login password and you don't know the master password, your data will be lost.
A master password is set for this computer.
Change...
This is a "safety net" password. It lets you unlock any FileVault account on this computer.
FileVault protection is off for this account.
Turn On FileVault...
Turning on FileVault may take a while.
Click the lock to prevent further changes.


Encrypting
Wait while your phone is being encrypted.


11:44
Security
Encryption
Encrypt phone
Passwords
Make passwords visible
SIM/RUIM card lock
Set up SIM/RUIM card lock
Device administration
Device administrators
View or deactivate device administrators
Unknown sources
Allow installation of apps from sources other than the Play Store
Credential storage
Storage type
Hardware-backed


BitLocker
Enter the password to unlock this drive
Press the Insert key to see the password as you type.

https://securityinabox.org

http://learn.equalit.ie

https://level-up.cc

https://saferjourno.internews.org

https://help.riseup.net/en/security

https://ssd.eff.org

https://hygiene.digitalpublicsquare.com