CRYPTO PARTY

hands-on!

People coming together and help each other installing software that helps you to be not that much spied any more by your own government (ICMS), foreign governments (NSA etc) and the service providers (BSNL, vodafone, etc) you are using.

Here For You to Serve

sva@ccc.de – twitter@sva

thupten104@gmail.com

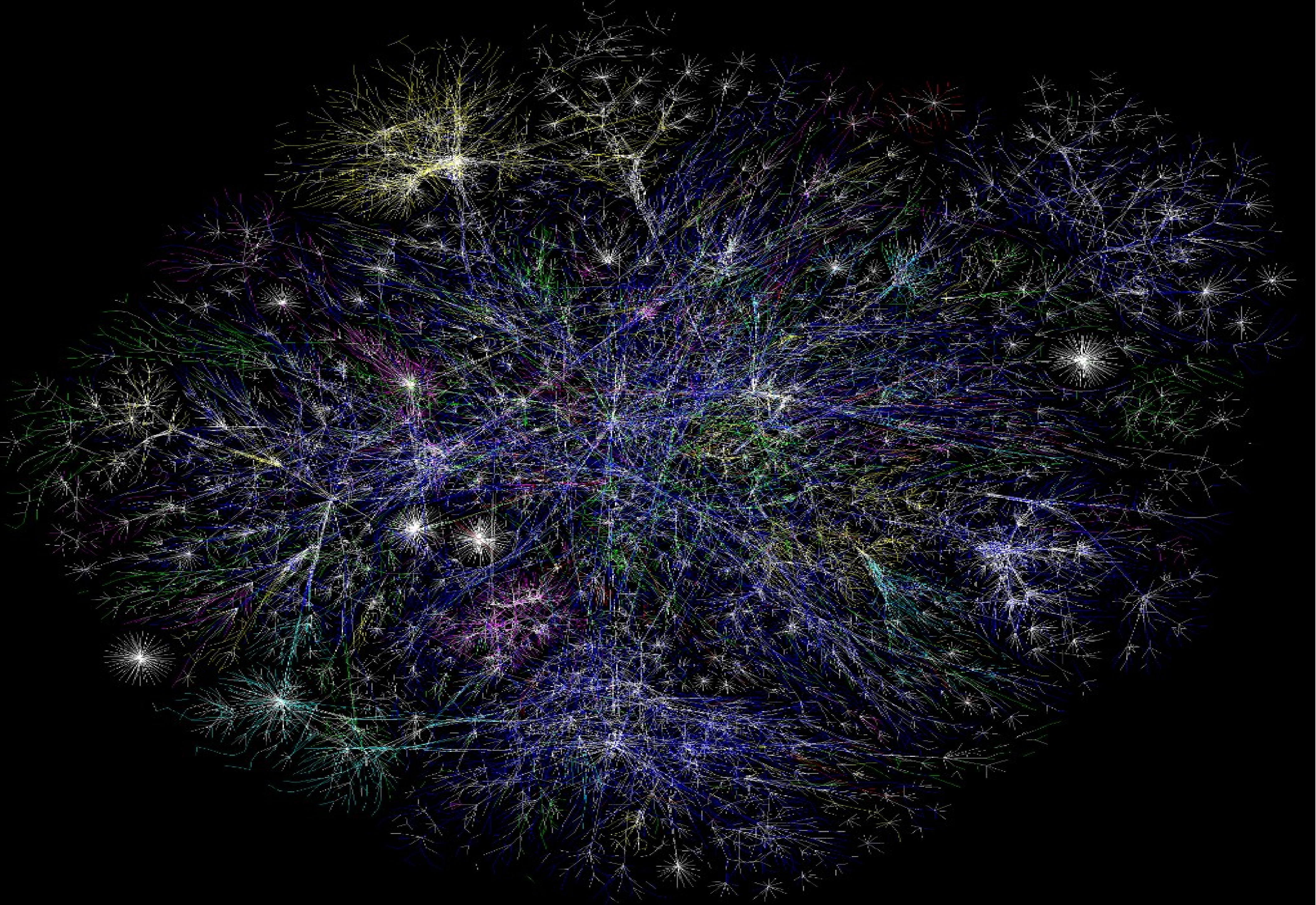
beli@cis-india.org

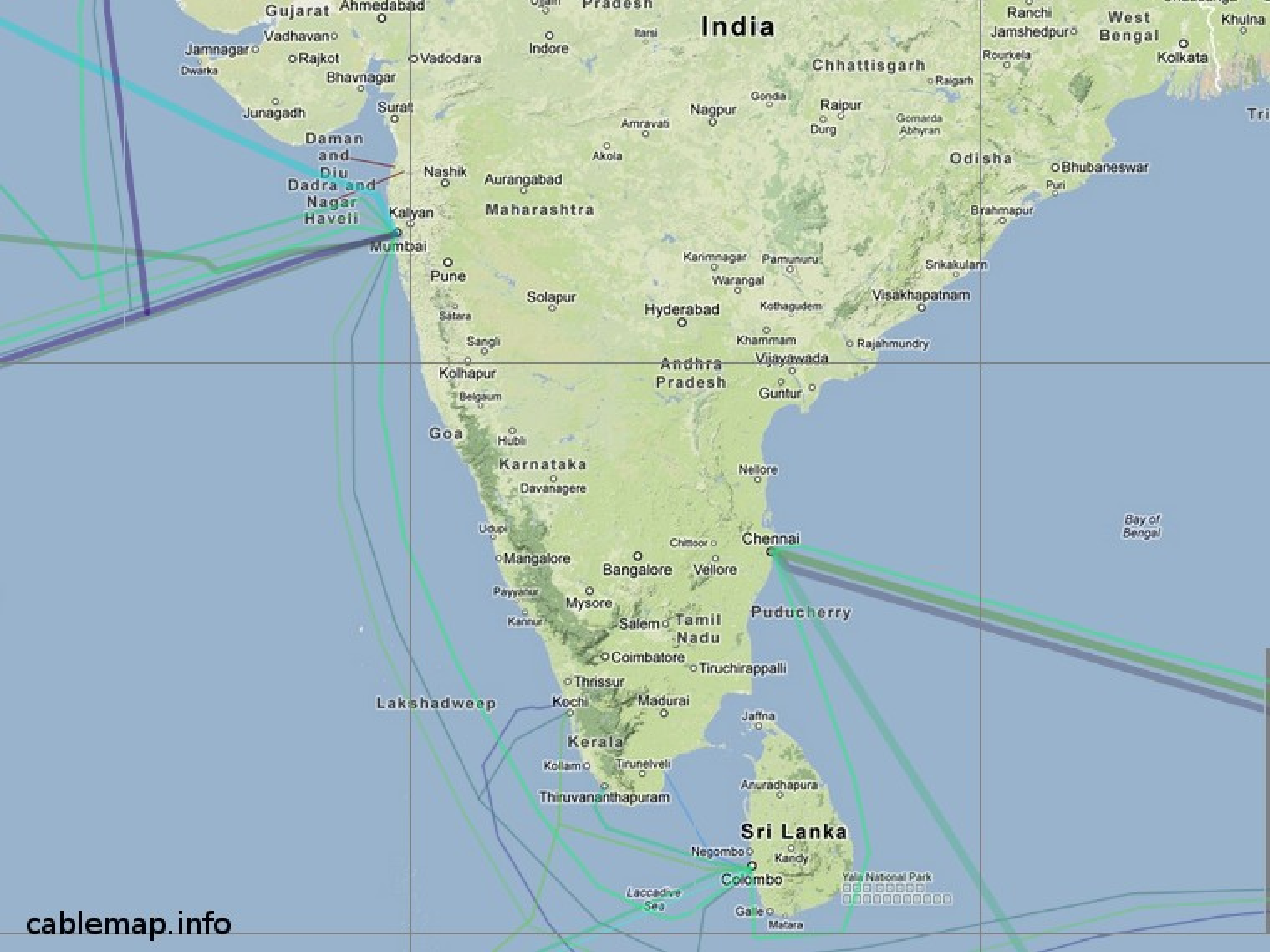
santosh@hackerearth.com – twitter@importerror

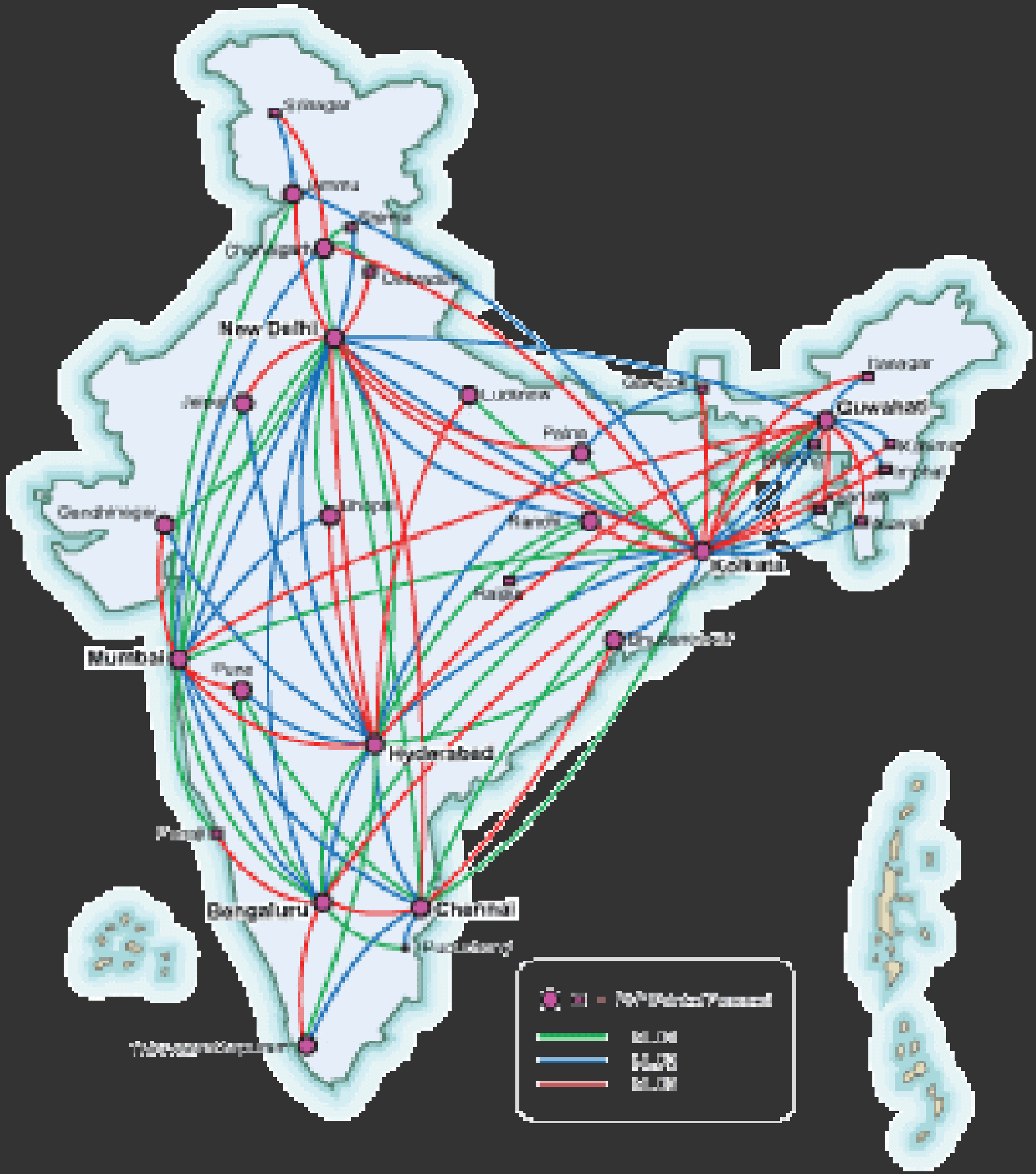
Way To Go

* The Internet
* What to we use there?
* How does that look like?
* Alternatives
* What is Cryptography?
* E-Mail / GPG
* Passwords/-phrases

* Software – how to choose
* Anonymity – Tor
* File encryption + deletion
* Web Browsing
* Text Messaging + Voice
* Android

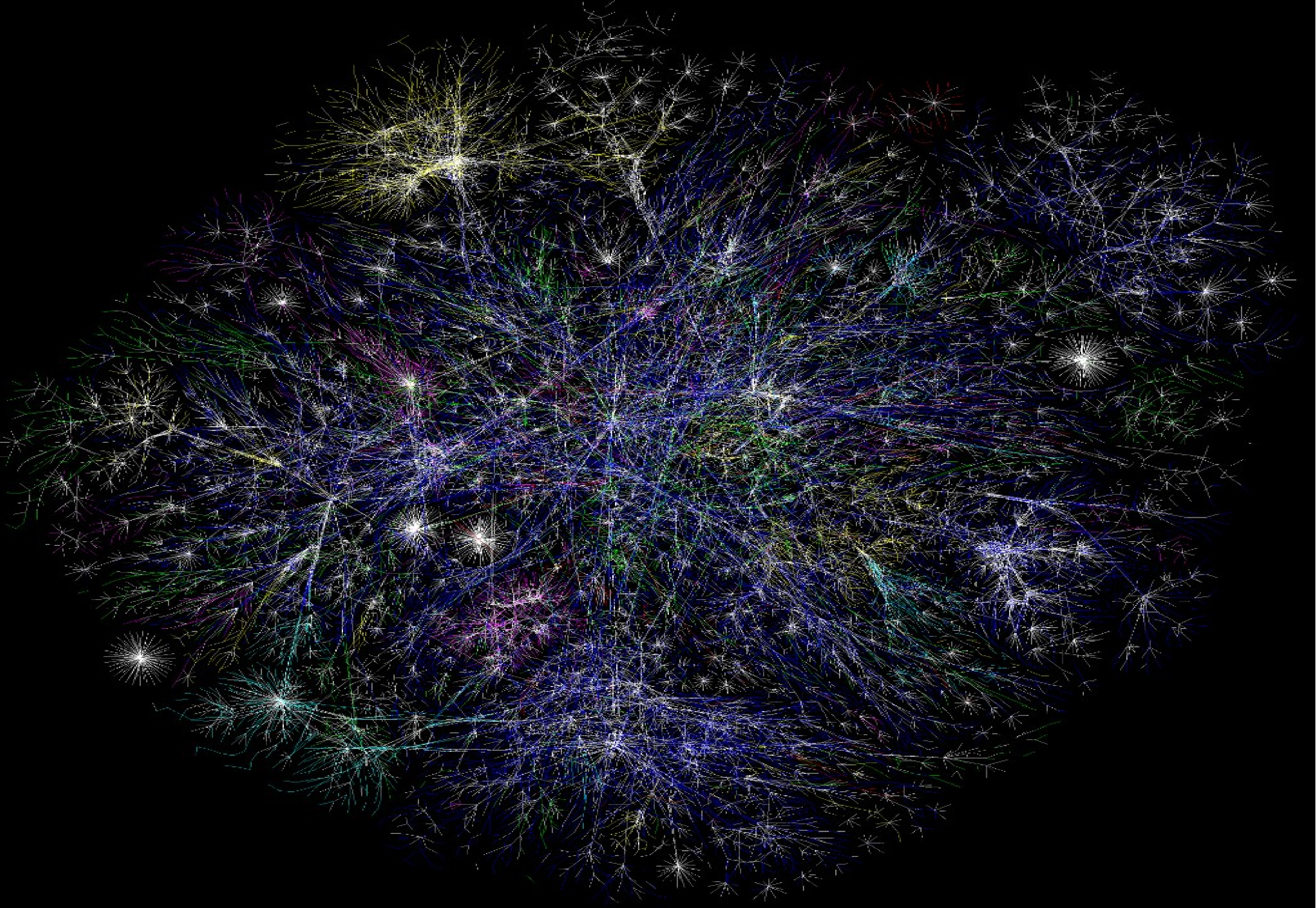


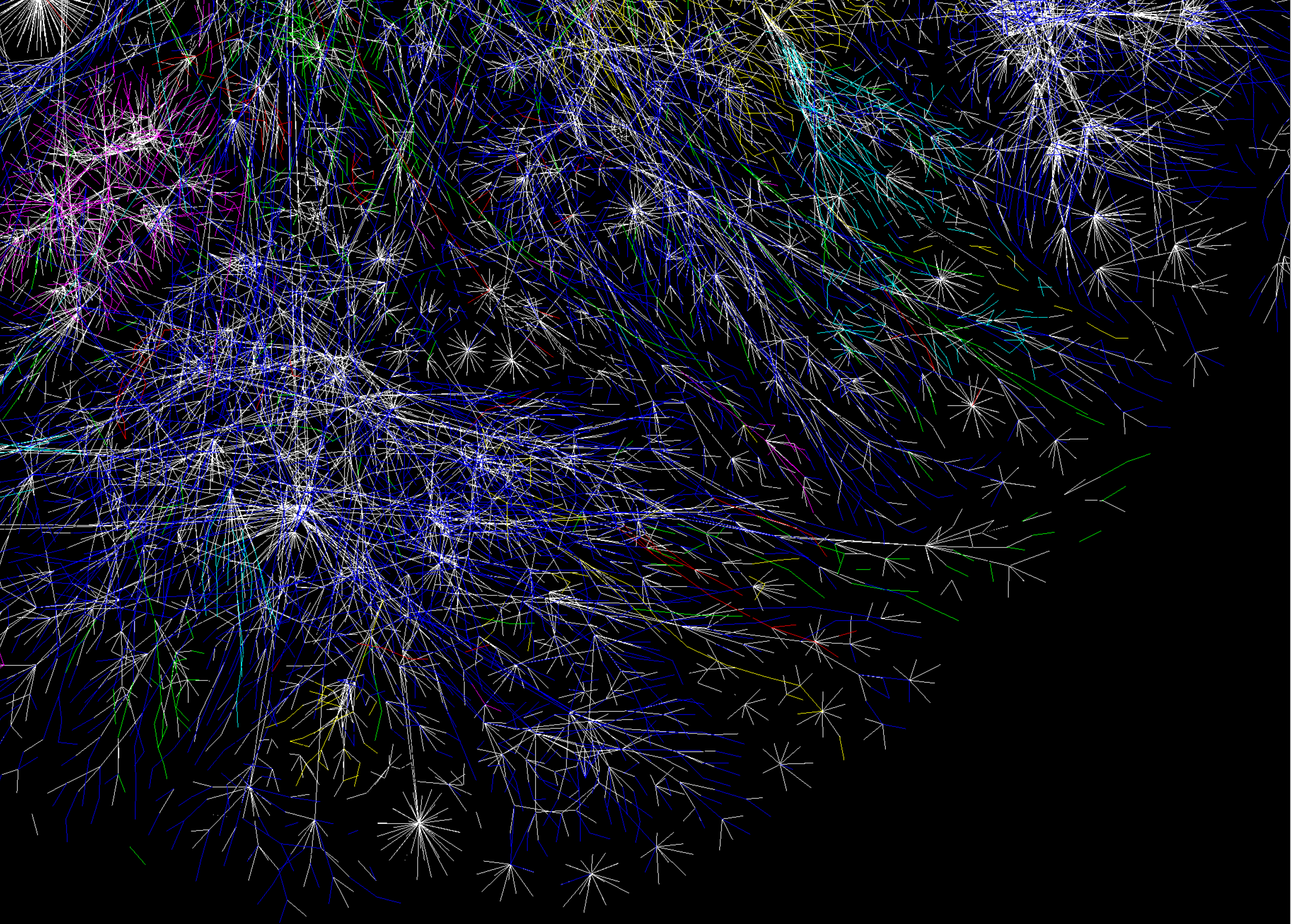

India
Gujarat
Ahmedabad
Pradesh
Vadhavan
Jamnagar
Rajkot
Dwarka
Vadodara
Indore
Itarsi
Bhavnagar
Junagadh
Surat
Daman and Diu
Dadra and Nagar Haveli
Nashik
Aurangabad
Kalyan
Mumbai
Maharashtra
Pune
Satara
Solapur
Sangli
Kolhapur
Belgaum
Goa
Hubli
Karnataka
Davanagere
Udupi
Mangalore
Payyanur
Kannur
Mysore
Bangalore
Lakshadweep
Kochi
Thrissur
Kerala
Kollam
Thiruvananthapuram
Tirunelveli
Madurai
Coimbatore
Salem
Tamil Nadu
Tiruchirappalli
Chittoor
Vellore
Chennai
Puducherry
Nellore
Andhra Pradesh
Guntur
Vijayawada
Khammam
Rajahmundry
Hyderabad
Kothagudem
Warangal
Karimnagar
Pamururu
Visakhapatnam
Srikakulam
Brahmapur
Puri
Bhubaneswar
Odisha
Amravati
Akola
Nagpur
Gondia
Raipur
Durg
Chhattisgarh
Raigarh
Gomarda Abhyran
Ranchi
Jamshedpur
Rourkela
West Bengal
Kolkata
Khulna
Tri
Bay of Bengal
Jaffna
Anuradhapura
Sri Lanka
Negombo
Kandy
Colombo
Yala National Park
Laccadive Sea
Galle
Matara
cablemap.info

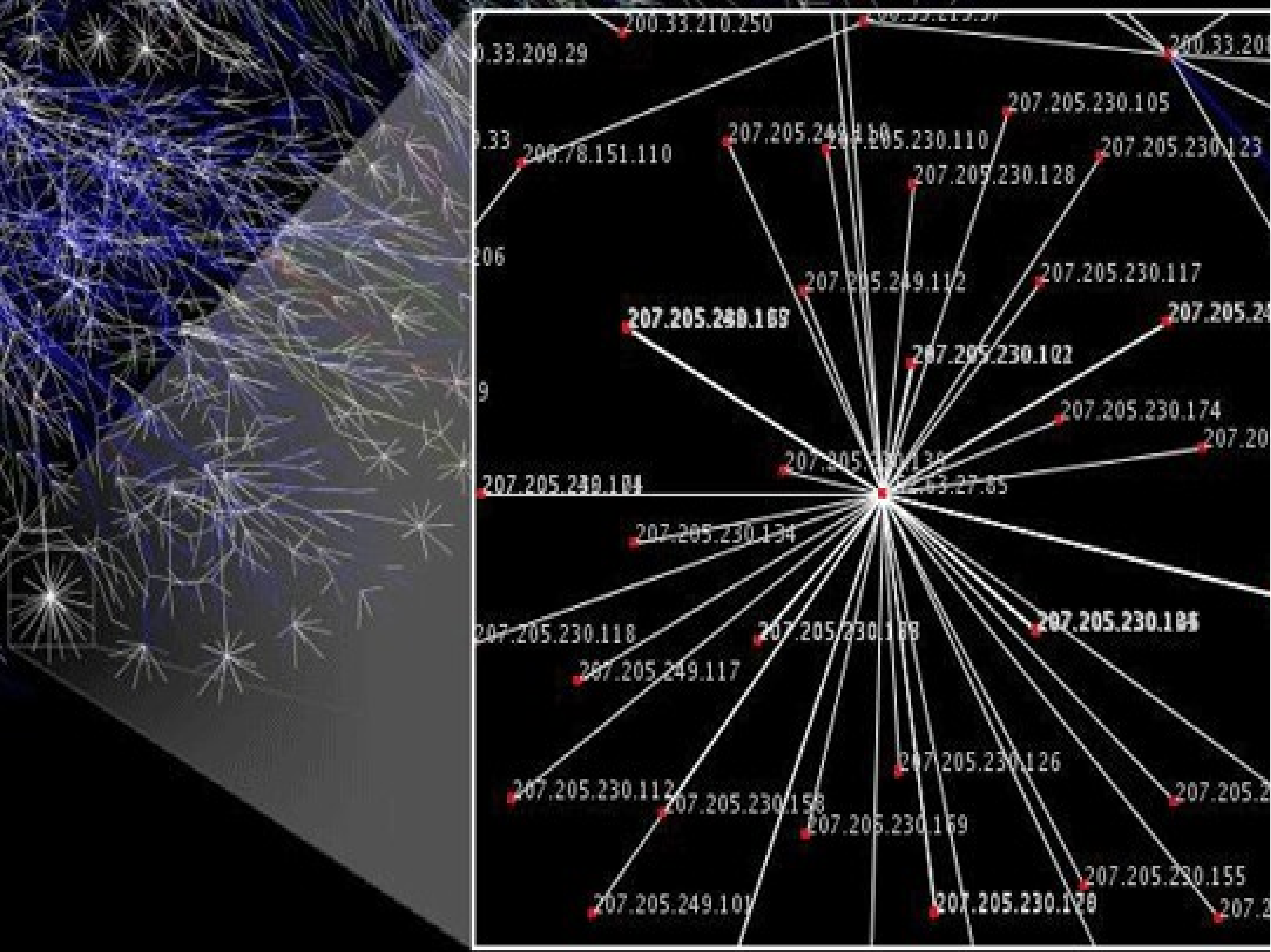


Multiple 10G Connecting all the State Capitals

Gigabit Connectivity to all the 640 Districts






200.33.210.250
0.33.209.29
200.33.20
207.205.230.105
207.205.230.110
207.205.230.123
200.78.151.110
207.205.230.128
207.205.249.112
207.205.230.117
207.205.230.102
207.205.230.174
207.205.230.134
207.205.230.118
207.205.249.117
207.205.230.126
207.205.230.112
207.205.230.158
207.205.230.169
207.205.230.155
207.205.249.101
207.205.230.128

Problem:

IF

you are connected to the Internet

THEN

the Internet is connected to you!

=> you are a part of this network-of-networks

You are here

Map of the Internet. The Opte Project, www.opte.org

What do we do there?

- read & write
- information
- places and maps
- emails
- speaking (instant msg or voice over internet)
- watching pictures
- connect to old friends
- regional, national and international news
- news of people, things and gadgets
- watch the news online
- entertaining
- listen to music
- listen to podcasts
- education
- buying things or services (e.g. travel)
- online banking
- how-tos and do-it-yourself information
- looking for a job or a place to live

So What?

YES
WE SCAN
DIGITALE GESELLSCHAFT

So What?

We show a lot on ourselves:

Our way of living
Our way of thinking
What we are interested in
Things we plan to do
What we are thinking of

We leave our thoughts!

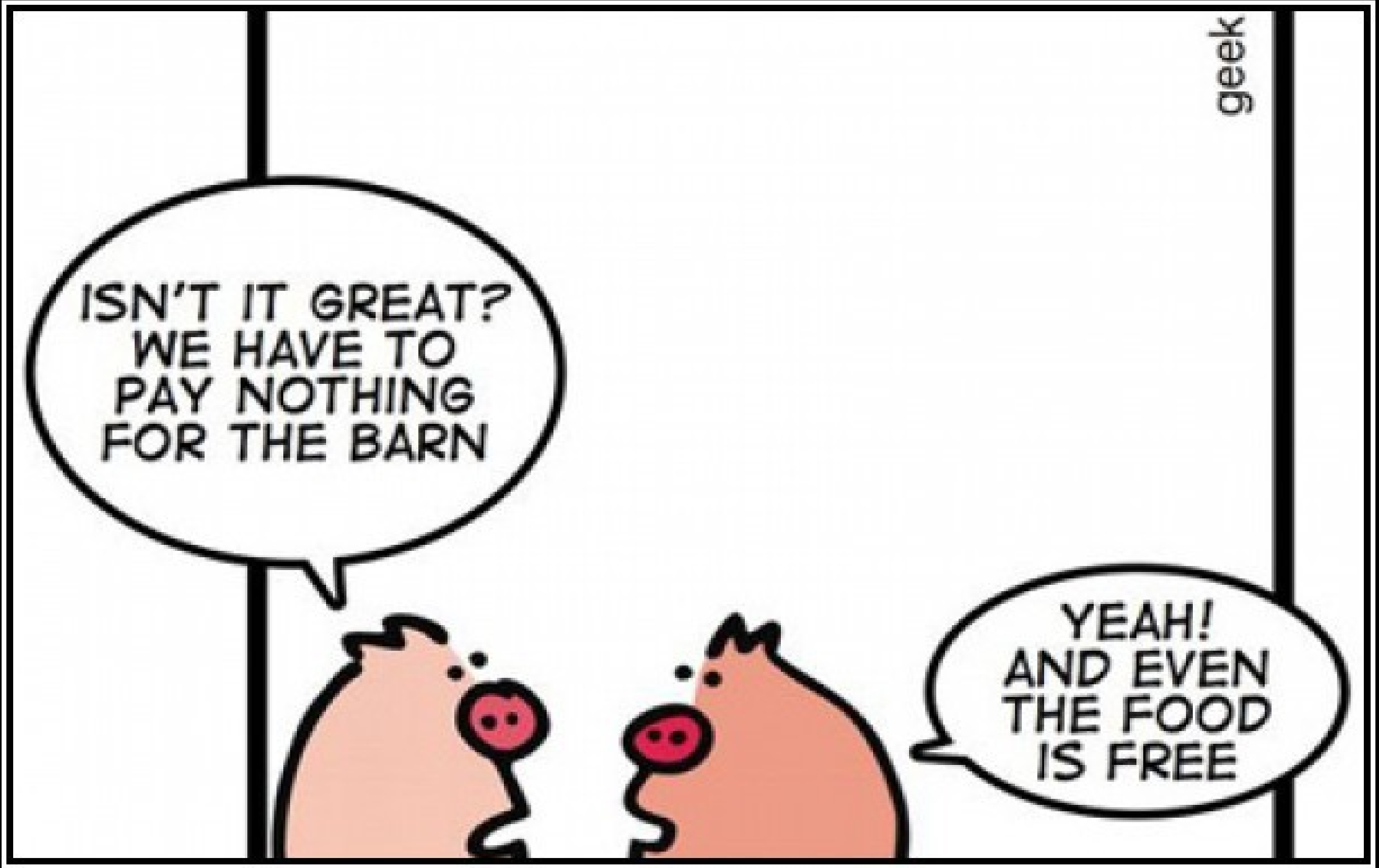
What are we Using?

Services.

Mostly webbased

We are using websites

OIL MAKE UP TANK 150L
Google


ISN'T IT GREAT? WE HAVE TO PAY NOTHING FOR THE BARN
YEAH! AND EVEN THE FOOD IS FREE
geek

FACEBOOK AND YOU

If you're not paying for it, you're not the customer. You're the product being sold.

What to do?

- ixquick.com
- startpage.com
- duckduckgo.com
- metager.de/en

➔ More Privacy
(they promise)

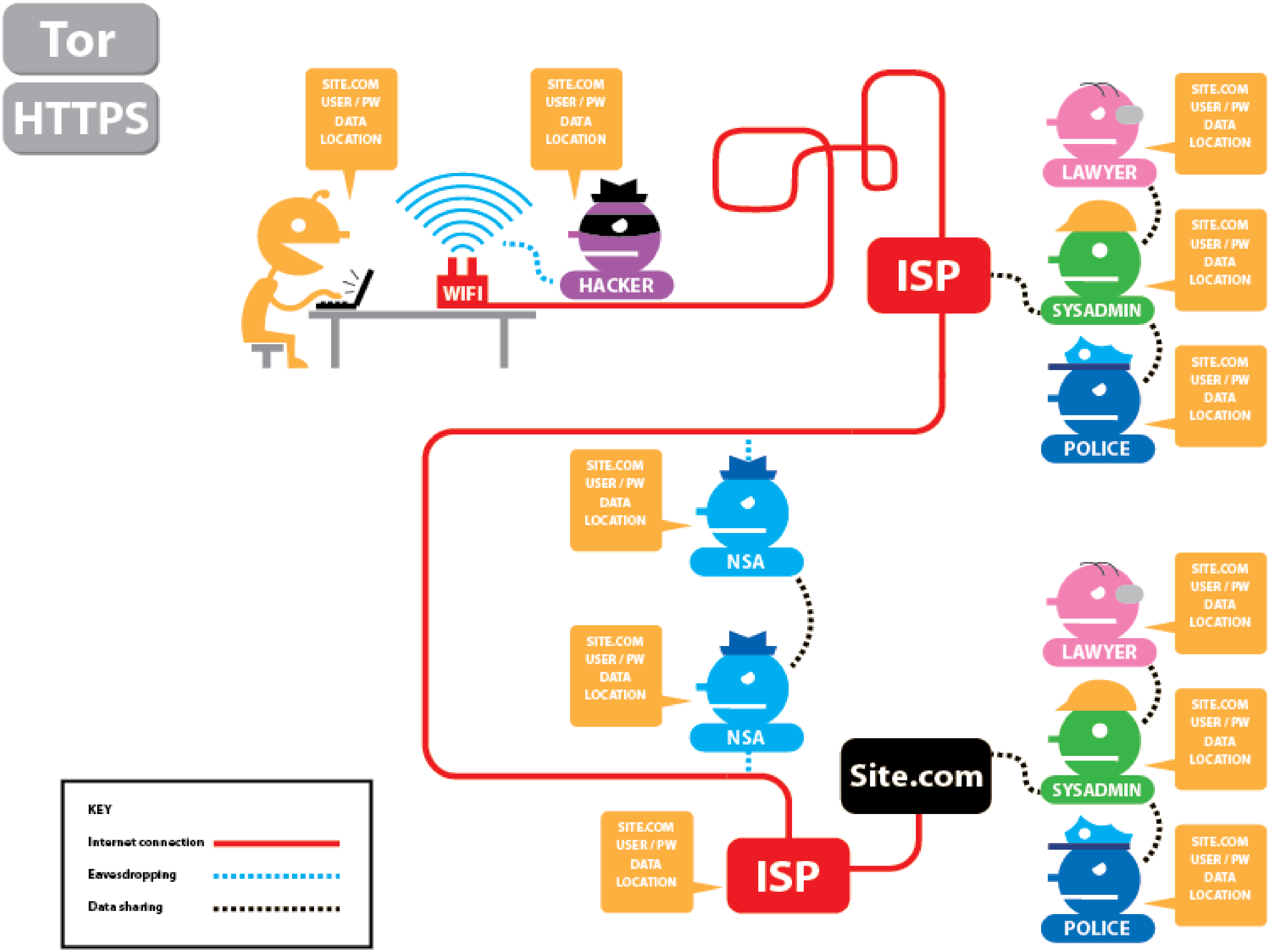
- ecisoa.org
- ecosearch.org
- goodsearch.com

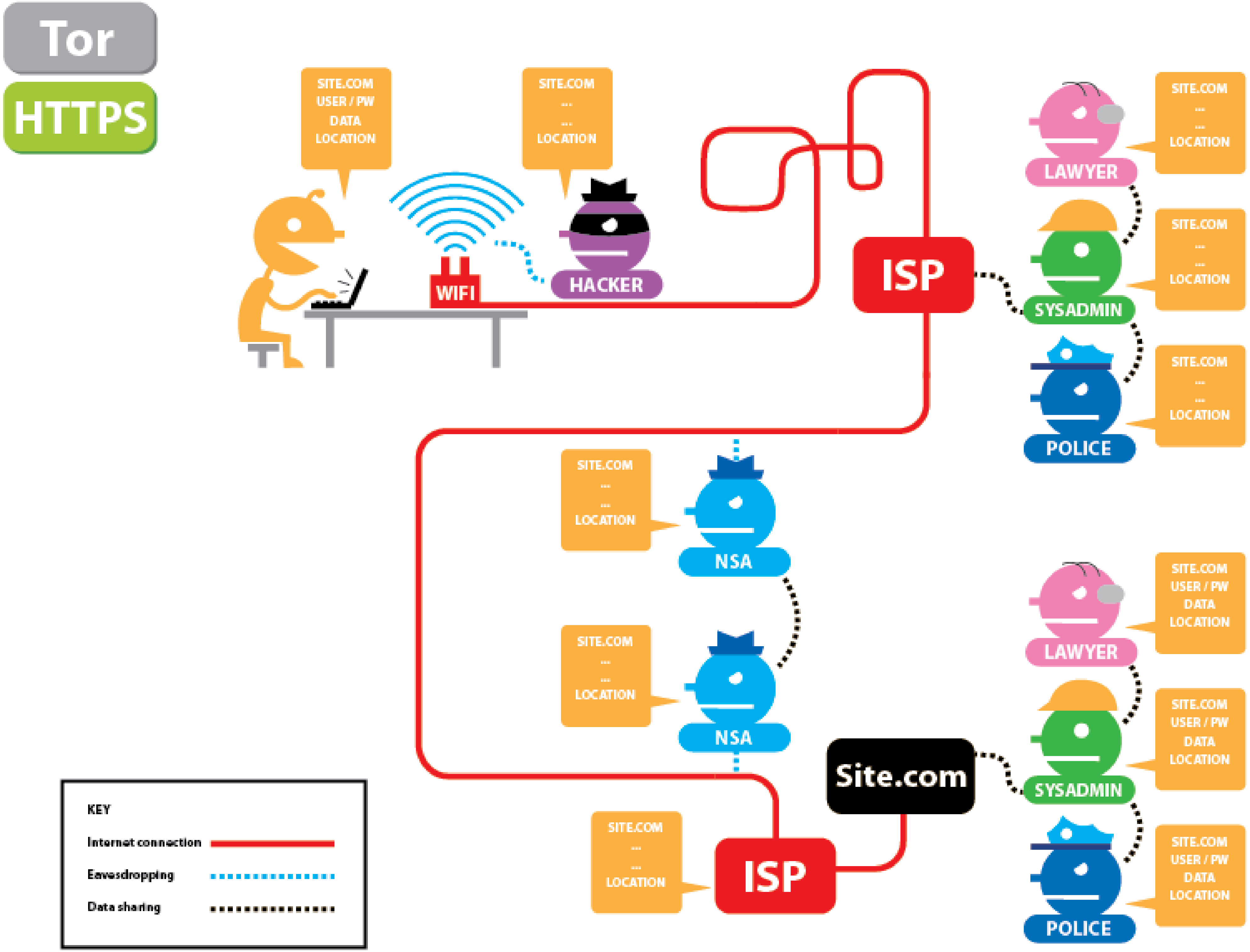
➔ Spending your data
Data = Money is
spend for the “good”

What to do?

Use https://
Instead of http://

The communication between
your computer and the server
is encrypted.


Tor
HTTPS
SITE.COM USER / PW DATA LOCATION
SITE.COM USER / PW DATA LOCATION
WIFI
HACKER
ISP
LAWYER
SITE.COM USER / PW DATA LOCATION
SYSADMIN
SITE.COM USER / PW DATA LOCATION
POLICE
SITE.COM USER / PW DATA LOCATION
SITE.COM USER / PW DATA LOCATION
NSA
SITE.COM USER / PW DATA LOCATION
NSA
LAWYER
SITE.COM USER / PW DATA LOCATION
Site.com
SYSADMIN
SITE.COM USER / PW DATA LOCATION
SITE.COM USER / PW DATA LOCATION
ISP
POLICE
SITE.COM USER / PW DATA LOCATION
KEY
Internet connection
Eavesdropping
Data sharing


Tor
HTTPS
SITE.COM
USER / PW
DATA
LOCATION
SITE.COM
...
...
LOCATION
WIFI
HACKER
ISP
SITE.COM
...
...
LOCATION
LAWYER
SITE.COM
...
...
LOCATION
SYSADMIN
SITE.COM
...
...
LOCATION
POLICE
SITE.COM
...
...
LOCATION
NSA
SITE.COM
...
...
LOCATION
NSA
SITE.COM
USER / PW
DATA
LOCATION
LAWYER
SITE.COM
USER / PW
DATA
LOCATION
SYSADMIN
Site.com
SITE.COM
USER / PW
DATA
LOCATION
POLICE
SITE.COM
...
...
LOCATION
ISP
KEY
Internet connection
Eavesdropping
Data sharing

What to do?

Use Cryptography

Lock your data away

What is Crypto?

mathematical way to make
the data only readable for:

the one sending it
the one receiving it

=> end-to-end encryption

Basic Principles

Confidentiality

(no one else can read it)

Integrity

(no one else can modify)

Authentication

(message is from the one person)

“How much detail do I need to understand about the tools I want to use?”

Depends on your intentions.

I dont wanna be watched easily & complete.

=> Every little use of cryptography helps

I want to be completely protected.

=> You have to learn & understand lots details

Be Aware!

you are never “safe”
technology can fail.

It can fail any time.
Without you even noticing.

Never Forget!

encrypt (or encode)

=> Code

or Key

Simple encoding/key:

Hello

:

:

olleH

Software Helps:

Hello

:

:

hQEMAy4io41ThT7gAQgAqF7ljcgd

Private Means...

...just you & me have the key
noone else can listen

:

:

uSMWsh3zbWke8DUmY+Lf9Ssy2waJkE+gaJKhxplD6CWfL96vgXn3N/bBVg2+SCmt
UV/btwupjojluio1cLS0X85glj85sfeALHZGDzRTe7kuMXSqY9A+ZEpYIGybGkLk
8EjFZOqgDNRZRVe2mXpu7EOEwXEuIl2cANk5iXaVanAHGSMubUEzwkZWxvfHdPSZ
DWK9AYBRyIr62k8W7/rvpI8T8RtuinPbVWl5sLe7/x0smFvVfYj0Cy+UakOLgN08
4yghqyWWY7Hzc1Xq+UQrVib8CVnk5h/WQotuOshBmdLpAWMYkbNV3eJMxQ4xqx0u

But...

...everyone knows that the two of us are talking to each other

:

:

metadata stays plain text, like time, place, IP, system, etc.

(everything besides the main body of your email/text)

(sometimes you might wanna add anonymity)

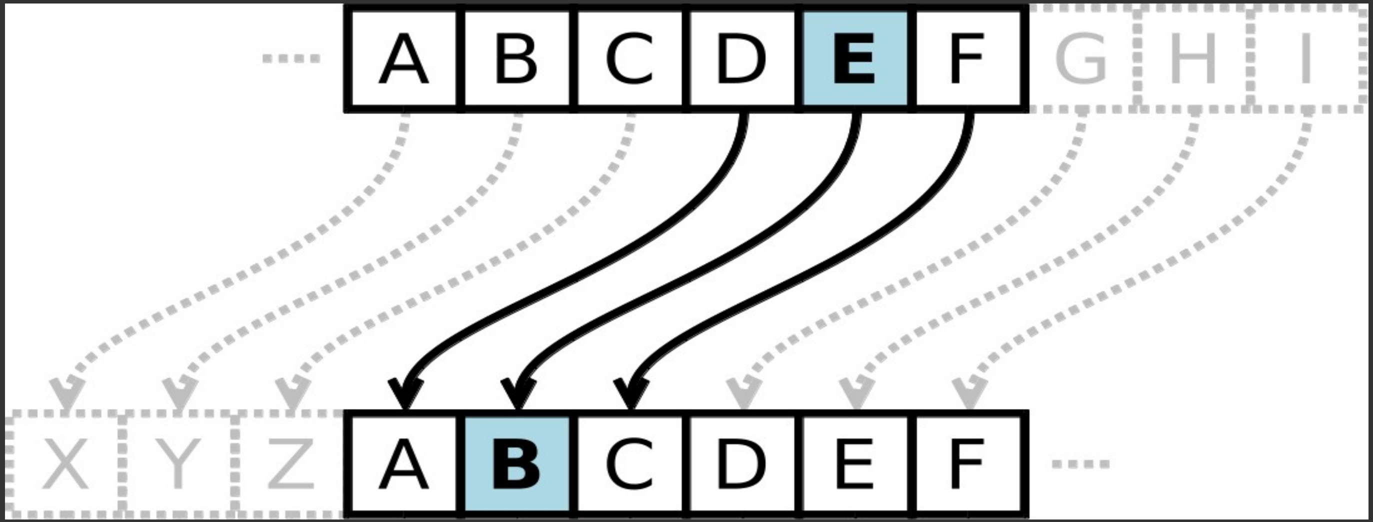
E-Mail

GPG

Asymmetric Encryption

Symmetric Encryption

The way Julius Caesar did
2000 years ago



Hello
:
:
Ebiil

key/code == “alphabet: left-shift-3”

Both sides have to know key/code=> symmetric

Asymmetric Encryption: Keys

Often known as “puplic-key-encryption”

everyone has own key-pair:

puplic key

available
for everyone

secret key

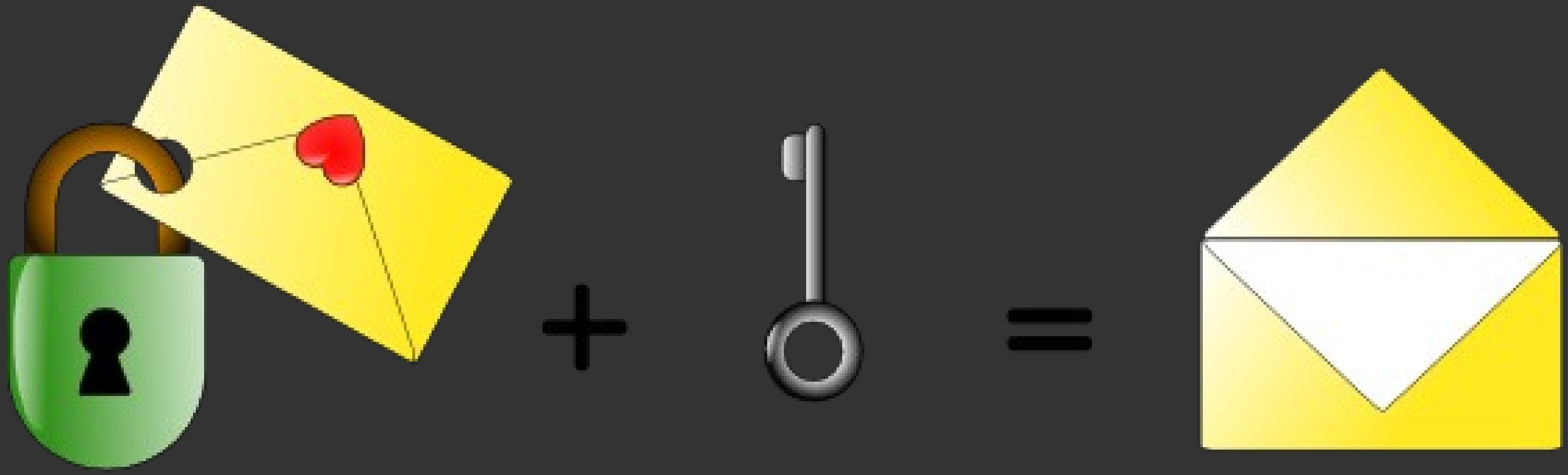
kept as
a secret

Asymmetric Encryption: En-crypt

Bob uses the open lock / public key from Alice to lock/encrypt the message.

Once closed, he is not able to open it any more.

Asymmetric Encryption: De-crypt



Alice uses her secret key to unlock/ decrypt the message from Bob.

Alice is the only one able to open this message.

Asymmetric Encryption: Sign

But, the analogy will not fit for the next layer of understanding. Usually an encrypted text is **encrypted with the recipients public key** and **signed with your private key**.

Alice		Bob
private		public
	X	
public		private

Asymmetric Encryption: Sign

This works like a seal of wax on ancient letters

Alice		Bob
private		public
	X	
public		private

E-Mail

transferred as plain text

content

metadata

whole route

everything

Service Providers?
=> TRUST!

- Use a friends mail server
- Pay for the service
- Combine the above
- Use mail server from a non-profit organization (and donate if possible)
- Use a mail server from a profit organization that earns money with services
- Find list of those on cryptoparty.in/brief => email

Content in an Envelope?

1. **Install mail client** + (add-on, if applicable)
   (e.g. mozilla.org/thunderbird + enigmail)
2. **Install** GnuPG (gnupg.org)
3. Choose **password**/passphrase
4. Generate **key**-pair, publish public key

Use! (that we do tonight)

choose a good passphrase

This is important for every service you are using.

Do not use the same password everywhere!

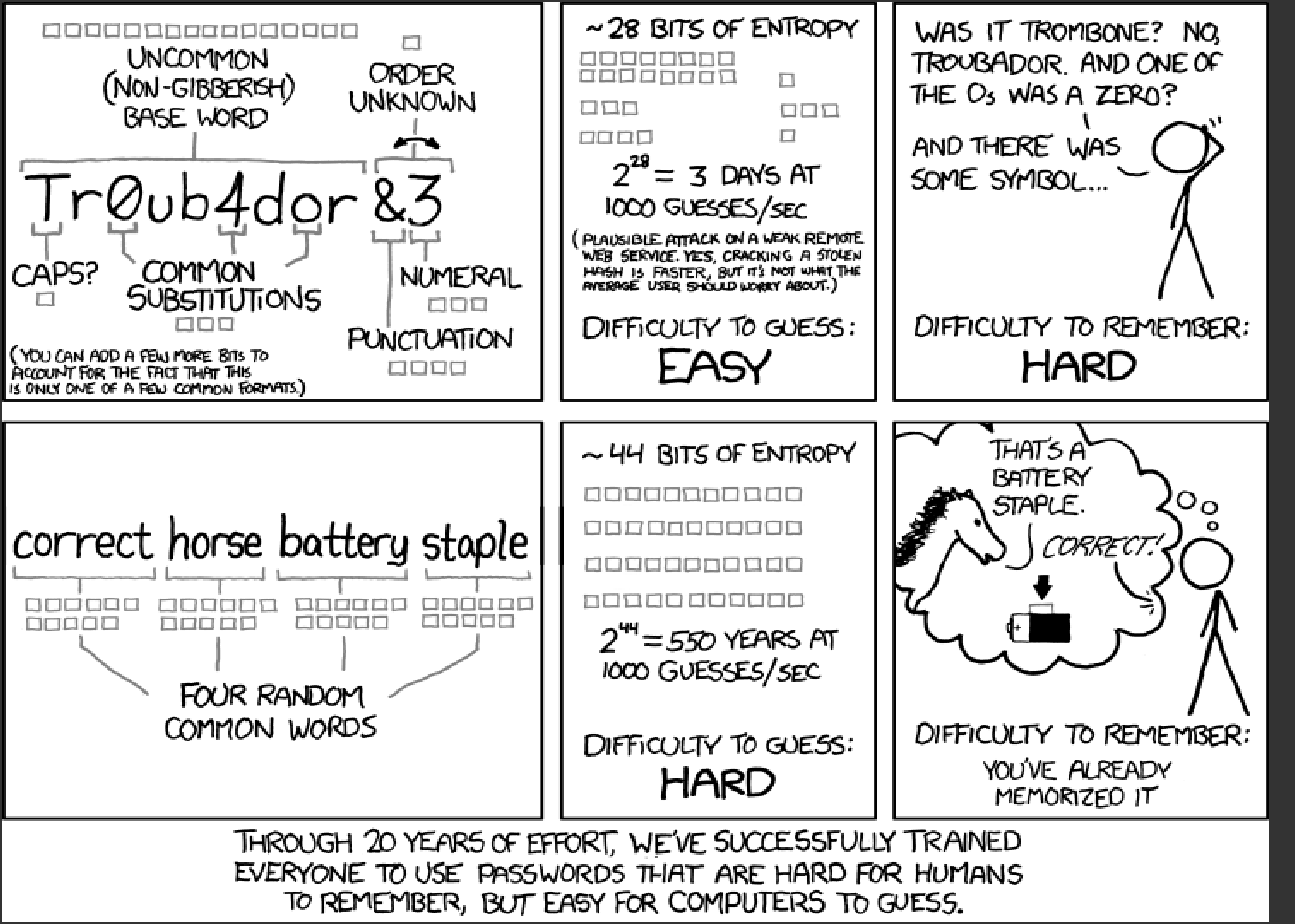
Add some special characters!

The longer the better!

Choose any:

Sentence you like AND Song AND Saying AND

any other language (transformed in latin letters)


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Passphrase: Some Rules

Difficult for a computer to guess:

Make it long – the longer the more time it takes

Make it complex – use upper cases, numbers etc.

Difficult for others to figure out:

Make it practical – sentences just serve fine

Don't make it personal – don't include personal info

Keep it secret – don't share your password

Minimise damage if someone does learn it:

Make it unique – not the same password everywhere

Keep it fresh – change on regular basis

(from: securityinabox.org)

Passphrase: Software Helps

KeePass

Free, open source, cross-platform, light-weight password management utility.

Encrypted database is protected by a single master password and/or key file.

Strictly local, not in the cloud.

Software

We always need to know some background

How can I decide, if something is “secure”?

- The **older** a product, the more likely it is secure -
- Where does it **come from**, who is developing it -
- Check the news, if there is **new developments** -
- If it is not **open source**, don't use it -

Download?

Ok, but where to dowload it from?

Use Wikipedia as a source to get linked to the project website.

DO NOT use any random software-download-site!

Open Source

Independent researchers can verify that the source code does not contain any security flaw or secret 'backdoor'.

You can never be totally sure…

TRUST

PGP/GPG Why two names?

PGP == Pretty Good Privacy

Created by Phil Zimmermann in 1991
see RFC 1991 (came 1996)
Zimmermann had been a long-time anti-nuclear activist, he created PGP
that people might securely use BBSs and securely store messages and files

OpenPGP == standard/specification

see RFC 2440 (1998) and 4880 (2007)

GPG == Gnu Privacy Guard

Created by Werner Koch 1999
from Free Software Foundation
(most common implementation of PGP)

PGP/GPG Key Length

Enigmail provides RSA by default, with the option of 1024, 2048, 4096 bits.

Via Snowden we learned, that “strong crypto” is still unbreakable, even for NSA.

300 bits is breakable with a normal PC in few hours, 512 bits can be factored in few weeks.

PGP/GPG Key Length/1024

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.14 (GNU/Linux)

mI0EU1EpkAEEALyXzjKHGIMabjpz1LdXy3Hhpqor85kBi6l83Rllxx+XCbGBsirq
oeSFE98Nk+PLjuT0ImZ6jI8dFWTawXAf0MPrAeqktbGMkYGnQ9bER/+Yg+6B+sRZ
hBywaFZTZOL7FGYEa02oby+6yX20tm+T109T4fBZ4JrOCiaV0zY1XWINABEBAAG0
MWJlLnN2YSAobm8gcGFzc3dvcmQgLSB0ZXN0IDEwMjQpIDxzdmFAbXVjLmNjYy5k
ZT6IvgQTAQIAKAUCU1EpkAIbIwUJCWYBgAYLCQgHAwIGFQgCCQoLBBYCAwECHgEC
F4AACgkQWRXgJrwUA5DNQwQAojA4rPIqZu8tOT54O2xz1vnDB9JqIu4kLh9FRiuc
lSoBtbe1k6Ws7wOOsv2ZH5md/WG2byBUKb0TSLYSmSMYBuDLB4ZhOkGr4A7DN/a8
RaiypiMRJfhkITE83hgwdP5kQRVVmdMEXoH4HlCjS2MgxqdJ1dAf/x+gohTMxf6p
CXC4jQRTUSmQAQQA2TDFKLJ8wpFR5qPZO4/7CgagcX4hvydC+Z7kwNfeUgxE7+6m
GkuUa246tHVww3wdFHQTqivU1W4v7zU3pgdfahPyUoinO6ph1iK76pIAge0AcNII
7wCP4Eln99qPXmh01dl7BWveAgIxKEf2E7MJ6epvZ3lAdV/GKvLG1qSioM0AEQEA
AYilBBgBAgAPBQJTUSmQAhsMBQkJZgGAAAoJEFkV4Ca8FAOQ/HED/jUw5jbblx8U
E43Si4ZJWVNPYngtDMDFNxwUJAmvE8Cfm1tVwCsbnEAu5RQC9CV+tZNo3W3w8w2m
a8bNaIQJ50TWoKvI6XoH4vsPRpG0YMVHJkEDB0PtAYMA4yp7fiF7Gfp5htqJJ+KA
Shz78ZJSH536V9eR+ZDcLU/2qdzefFgQ
=C6Zs
-----END PGP PUBLIC KEY BLOCK-----
```

PGP/GPG Key Length/2048

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.14 (GNU/Linux)

mQENBFNRKr0BCACjy7oXeQUX/LcEZVZ5hKuIwjd3z7Swi13nztHulfb17hKHaldR
9EOqOQYzz23XwXR7NqSizl8348a/1bWs+/ID+5UerVcH3kUI0Y8Vn8smnCzIvTbR
8NT2g+5WCA+Ia6jhOlNSw3tBYi1HAVhlqL0UloP7Fy1v0SH2VKvEW1y2EJ6Ujgek
xsC+PQzAjqQZqDv1i/WHXGlCcO0mH+TBHP3VL7q2RZLcIZuUmitpTXyVVWoY0BR6
+heF+Twz4moIYtg2QtZY3o3AhCr2C2yMWgAessgYYDc+efiSb7VaCMJxch0oE/0/
+LZdUL3K7TdXoz2Ztvs6qCe/PSvWZf0LZMRNABEBAAG0MWJlLnN2YSAobm8gcGFz
c3dvcmQgLSB0ZXN0IDIwNDgpIDxzdmFAbXVjLmNjYy5kZT6JAT4EEwECACgFAlNR
Kr0CGyMFCQlmAYAGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJEGngsFiDqYEx
12oIAIST1H4lZIuRSIh60yO7A/p319454xvKjCfzYOSjBsXtCvAj5i2HXNubZyQn
hndfTo6UfFGY2B4oPw4nNQrynjG+4zEoWD/7AAtwYcjXDBId9G/NjGIugSXMCQLt
fEN66mS2Pk7f3876t38ZoJQjAguOIp2byHopyAh++cNP8e5iw9m1DC8QHtFGPhbp
inr0G5cIkWYcDoaoAufenPDnbRNMgtv4w7SRxejper6xZvYOA7CR5MCZbLjHF2C0
//9oKDg31O1bF86uwiDacZT3bO3U/bXZvpiaMDnt5B6WQXSU6VlC3yAJA1fdcXL8
kLICZ7e/zWI6kdiQjIf5W32aHzG5AQ0EU1EqvQEIALgeMo+thcnzIno8sw1kI4+x
nIHrxURcI//8TAAY6uxlQMWyyBkITPykjva4y/8ROIk74qnSjPUduIt9ZHuy3BkD
vTv9khEN8arLFFj44HXJJXvVvzWkuoSCMZSneDCwD74vn3w++3NvAp150BG3/5eh
nW9oib74YlU6sJa2vjpcG+vDwJX0RqoE8jBxm0N9UxhmCfFn7lQRl+76L33aGAXc
QmhNnAITNL2Rqse6DGK0GmjDG1eZrms+f+Ea5H83h29GhuqfZiz3FCrnxNipd+jp
qHbNiyPBd6Aj5FCV4BnY8FbwfarIeEjDQVnA2FylBnhMzmCKk8fil1NCD83BgMkA
EQEAAYkBJQQYAQIADwUCU1EqvQIbDAUJCWYBgAAKCRBp4LBYg6mBMfd/B/9EXCQy
yghe9sSxxyMpZNq2A4Q34aKwjfEZwjtvUihJcZbfC2CubTYYX/xpe4D0YH2dhaBx
qIA+Rt1jbc86D0i2shJHl/qiI7zbZX62FJ4dJc+trHBjbZScobRGpH4vtXCj2Qfw
UA5GPNaQ9pmjhZgU9EEJBA/eG5oXRksOOq5MW9vwQrp/SWEtekU9APH466i0ExGd
bQIN41t6AgdFO478I+UBISGFpT/3WXiOAMoAYNCfkof2jff4rayM6vGP5hM5/UQN
N8LW294m/9YXP4OVYST605Vb8f5AUAK37mWXNf1eniuBDcgUQW6WhoQN1b6Rq+xB
T734CkMi7/YhAekm
=vU0K
-----END PGP PUBLIC KEY BLOCK-----
```

PGP/GPG Key Length/ 4096

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.14 (GNU/Linux)

mQINBFNRK4EBEADLASHcvcZvtJ/LwKExgxONuHHIiTNIaIx0hTsRMq5xR2YV2UGi
yF1Ece20yCk98QTX72Jvhd7sarEgF+i3xEuYtVDPXbI4P4aj6gTGFElaHccYu1lz
ju9nzjaLMrF7+3lYfLo5mqAdjdYI2UWLHccYGKHUdDTHF83WshBdBdFagQqu9jPT
S3VfbWAV84AURnfOx/35msukvHgXhHuhd130ncBYZVhBUsnYET4ZSgNRLZleU/P+
LuYIt+30/KNJMYgdEUmo69lglRBBrgyfiA8yhbEn9FfiWd14+HvjKHTtjC+TrKYB
97/FY461o9KwsMwMoJ5tCYquOgjXZVsLLQqVMZZSRhNbmdtSmMtog8JM8TVQbPYy
9q4TFkJBUmEMB2tHWqJUZ1ErsZKYr0SzfmAfOYMaKBKOmokUG9TYcgD4r53/2bOl
xlEtrOYFLpjyFanrbLux/1AEXOB+1mFS4ZyRYJZ3Qlf1/UevQl/XfXnq6KU/FxHk
f7MqIuTgetDYYODfYCnx4XQ2I5e7uFzJWq4LDR7BFl01z+/0rmrm97RsCTY+y+re
Na90q4S9mFUVyUIEvp8ulbv+KY7h37MT/DuA4N87BlkpIttBQNEygj2D+MLx+BWX
4KJoG7PBNpnrVKT0DMdgv/jzMNIhYTCORgVWRFedyz6565y4mPVSdUAPJQARAQAB
tDFiZS5zdmEgKG5vIHBhc3N3b3JkIC0gdGVzdCAyMDk2KSA8c3ZhQG11Yy5jY2Mu
ZGU+iQI+BBMBAgAoBQJTUSuBAhsjBQkJZgGABgsJCAcDAgYVCAIJCgsEFgIDAQIe
AQIXgAAKCRCYPFwWrKFVueUxD/9U+l5YeTFyJYpL5qpm2j9pElC8eeOjYDRIMrpm
3c/VIlEkR2lNqCOIjTo2SnU/uXySJg9wSRixmcRWZTwHnNdw3YEfJP7+VUC38Sxv
n6Gqw4fhoqT2opAYUevCQhIgKUKvtmUU2nkKL9Zc1e+Wzha321ifIZraWBYLxVN+
0mu6XKbkPnNHq+UiXUECHupDL3kTI24d88tOx0dw+XjOIAL9jS+yCkaDlpaEc/da
8Ogqdmqa+NSgWC58lZXJIHGAZFHvRdmuV7BdmM6a/xNa+1aiRfsrs/BNuRuuLNDw
rwX430aHKhf01aq4FQQYatnG0nshncuESXdQ1hR309c1QU3Ffi91ElDj29kgUIwT
nohMkD6saE3IXLHJSNQRyHh7Q2g/RFRXMfZzfeeT7EzDwYXppj51Eqw1YKo/celF
n+PzJq2MEGg5CIzskI/cVvxZQvMlUs31Hg9e41lmNia8oNTcEGXnDqkZup55eXLq
N911XQb4+7lIVSiVw1k6yDf3iRQ2UEsYKmLsAQz0RDoz8pHi/DvoKGwlGpjLPMcM
A+aG5FB5axpE/TlxXat52qT09EF8cuKoTbRdXAakEeNeFUAd8ElENZlEo+i05yna
K50pXGJJApSXwa9csKSItECoc6RPu0rYMLKmO20JWT0FJTnbsAbpr/okydpt4XLb
aiWpqLkCDQRTUSuBARAA1raf6LA2Vb4U0vuaIeO+dRwVJHpLdTVNA4YN1XSStkVJ
zzsTVTfearPCDomISzB0VPFQrQVS+sM80zZHnIbgyUQmKXG+KbOs8pP+fQWaJCw4
TjFQMAvlu3PQ8svVWjGPnXRpQUjZ4BjsZv+3kFTs2GQpSQhIYDspC33OqfdADXIf
/J+1O4nxCLnEkxld1dUkZ4FNdaWCTAz37NrQ5V6A6Md3enzATx4e7LiVkfTeyh2x
3Iyfs9TVBVi7TKQzKKRpx1xrJKmZSCtFCRmn1IblDpDEjk6ymg2O5cyKr0JOleEJ
Ff41eW6GlG7uuCWVfoOIEtOkejaU1XWqWZ9YJ7p0P2FaZh3er1vvGkF5hsm8CotH
jKbt1Y2b6pp0V9EJf6HXugbdi1HZSKX8wKHwvh44uPfs+NVSodkgxnLxCfZGH7V4
RJlIu918yi/vD4jv2UN5JsEtXPipqVcmeOGaKxYIz9b6WL5SHcmCDNzopM0anDhN
UROFQ9qlgQZn4BTpVRae4FW2c1NZIaZrKpF9rl2asyWwzwgWBIWlSAy8AjZjRH/4
J2n5XCxLhcoWNGdNZpq4xAJqC+979s1rSJN8Fa2Wl4Hd9MigE4rzuN4Q9qnDYtgN
iU6aMTb1tsp58QDG7n+pupA4k3jfTa0yH42spf7L8FXf6nfn8gsBMFxMv1RLEx0A
EQEAAYkCJQQYAQIADwUCU1ErgQIbDAUJCWYBgAAKCRCYPFwWrKFVuWzpEACRMLbI
Redzqu+6ps21oex0DqXcSyZ+3arh0EhhnvjR+sXhB9xtY6FRUb60KgyYbfwr4Dup
WTP3qmthgQvERABKgQ/ujcTJVYYFWnPkb03judWFZBGJvpMHpVSakvhW37p77xHz
9B3l6XOpOFjopV/yuEGk6yqAaXGNFxXM6u990/tF969xfyiSMFeB5opiQlYDCANK
AF6ywi3JBnG43b6Yd9MSaB0bxCLc4tkWfQfVAJSKSODhrKJBF0s+MFVr+XRJV347
iyUNO5t3+Qgz/BnYqeM15Ck+sbz3LkEzaMe+f/1xoMkxQ2+sMX8UwWhVVDoe0/fP
26x6Thu4K+ZQM6+8NQOOwmnBQkKXKvu99gxrV1II+c3EqIXKicpGjA9ly6xnZ3WK
GRTydnpXM2bhm2qd2QHVK5HOjIee5fMElSKJ9PqVZuUAAiV+s2GTYfr5bza+WuG1
qZRgo1lLx/l9q3EX1ce8IdaDgbIRaz3lTWbLdzgAho4gxtED4+h6WUD4LOonWXDc
/TKDADe+xC5nJE8DdpEtFm1c51meTdvtCN5uiYgX9AKAeBVaG/UP23qXz0PdeJLJ
iuSx1GSn3wPn+hcXx5I5wAatbN5QMrWPLWb21Dl7Wm/vVGFLaFI7F9qqUfe4kCPR
4xxONiUP86SZV5HM9sv8QwRv1rYL95lWuxQp1w==
=m/ON
-----END PGP PUBLIC KEY BLOCK-----
```

PGP/GPG

[x] pretty old, widely used ever since

[x] free/libre open source software

[x] private persons (with a cause)
and foundations

[x] nothing in the news, still unbroken

Remember...

...everyone knows that the two of us are talking to each other

:

:

metadata stays plain text, like time, place, IP, system, etc.

(everything besides the main body of your email/text)

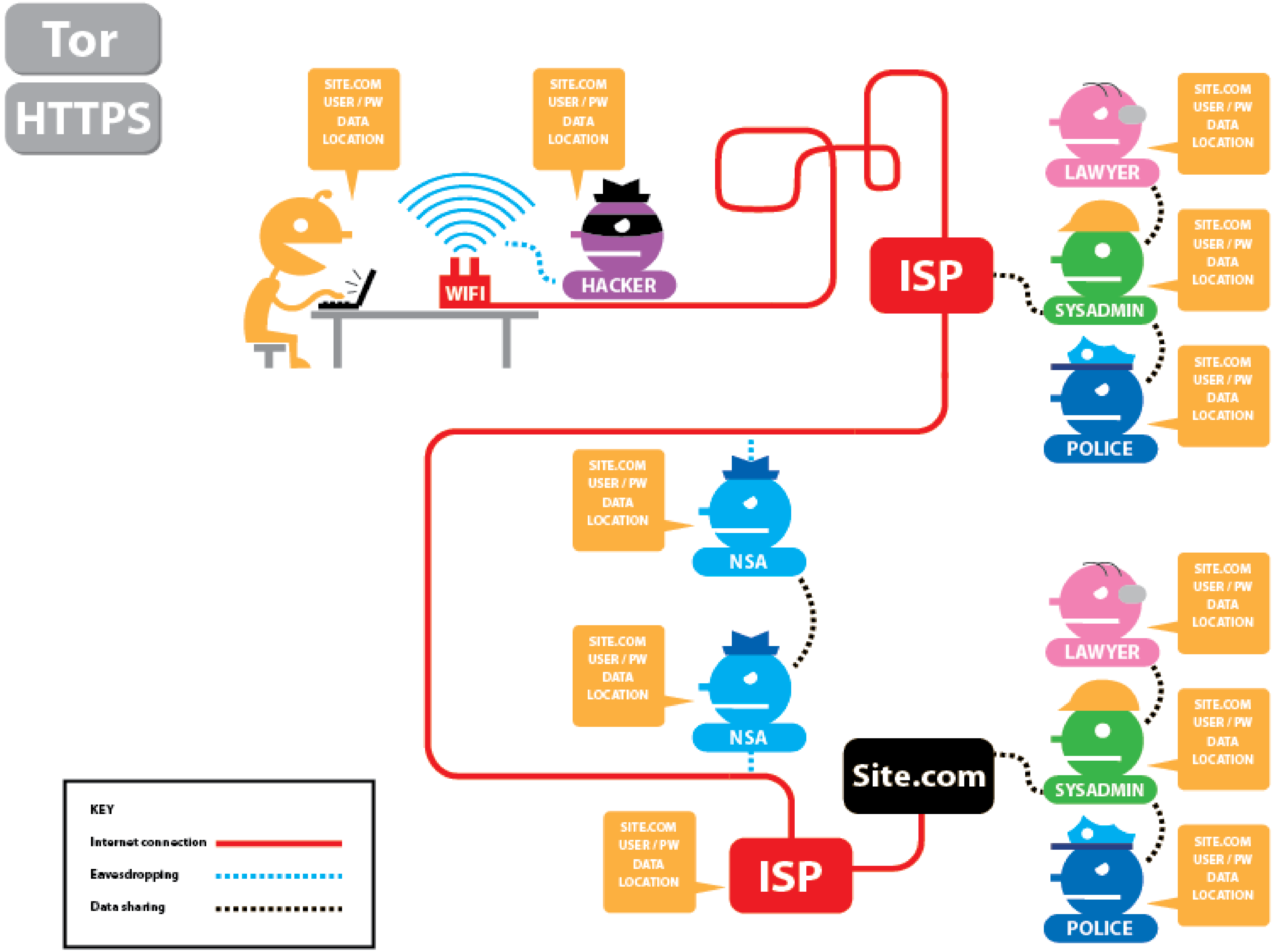
(sometimes you might wanna add anonymity)

Anonymity

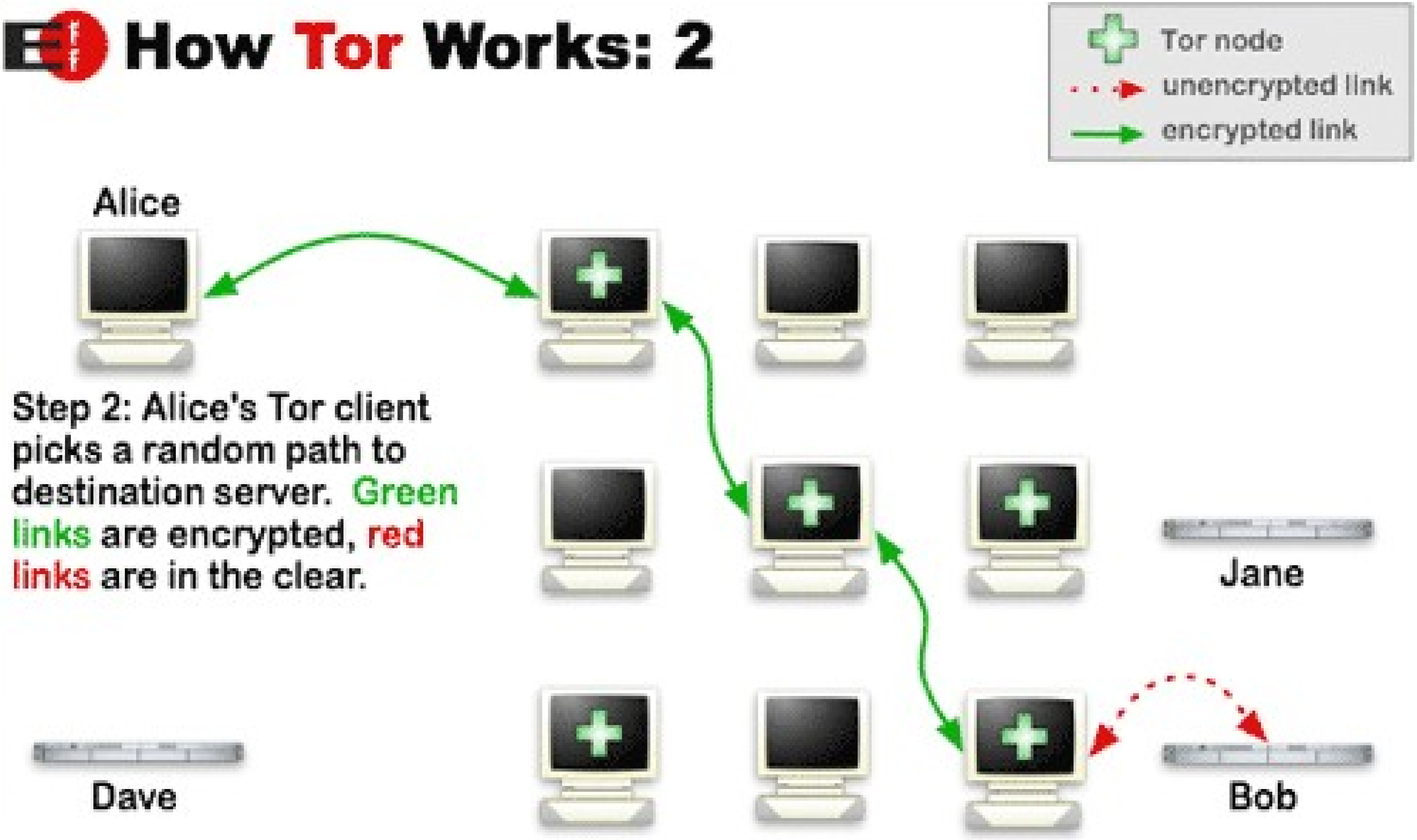
VPN – Virtual Private Network

(“Tunnel”)

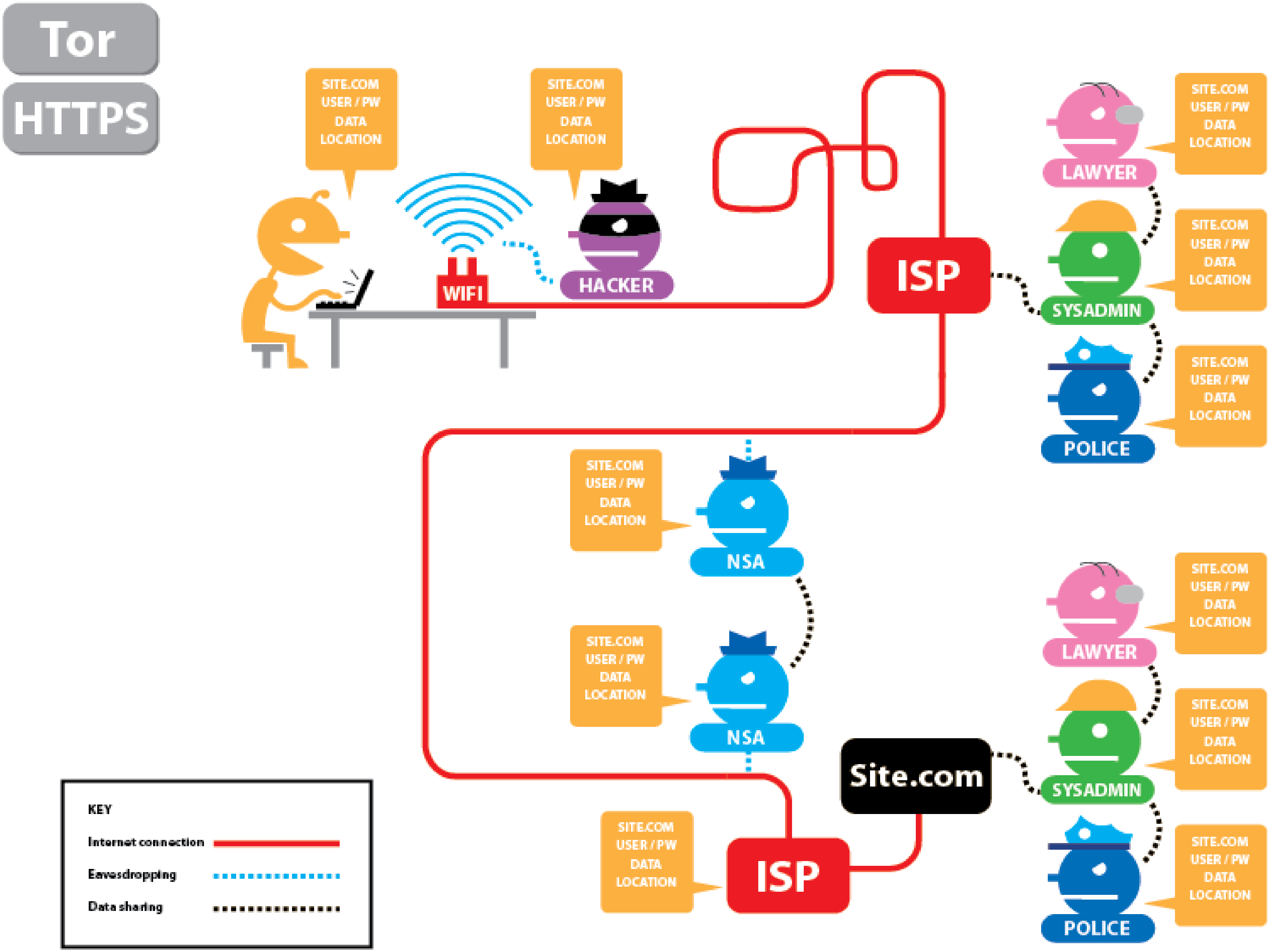
TOR – The Onion Router

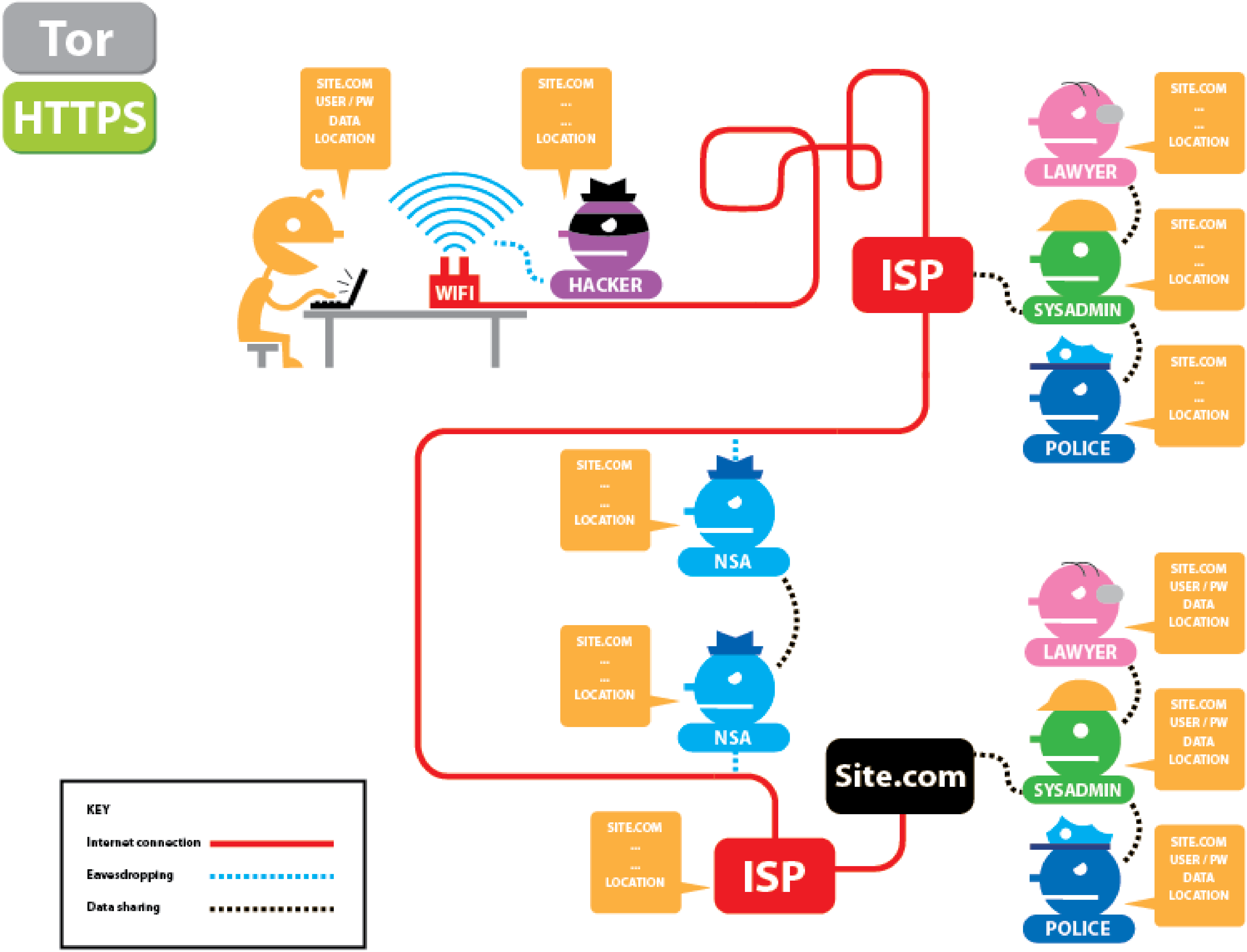

Tor
HTTPS
SITE.COM USER / PW DATA LOCATION
SITE.COM USER / PW DATA LOCATION
WIFI
HACKER
ISP
SITE.COM USER / PW DATA LOCATION
LAWYER
SITE.COM USER / PW DATA LOCATION
SYSADMIN
SITE.COM USER / PW DATA LOCATION
POLICE
SITE.COM USER / PW DATA LOCATION
NSA
SITE.COM USER / PW DATA LOCATION
NSA
SITE.COM USER / PW DATA LOCATION
LAWYER
SITE.COM USER / PW DATA LOCATION
SYSADMIN
SITE.COM USER / PW DATA LOCATION
POLICE
Site.com
SITE.COM USER / PW DATA LOCATION
ISP
KEY
Internet connection
Eavesdropping
Data sharing

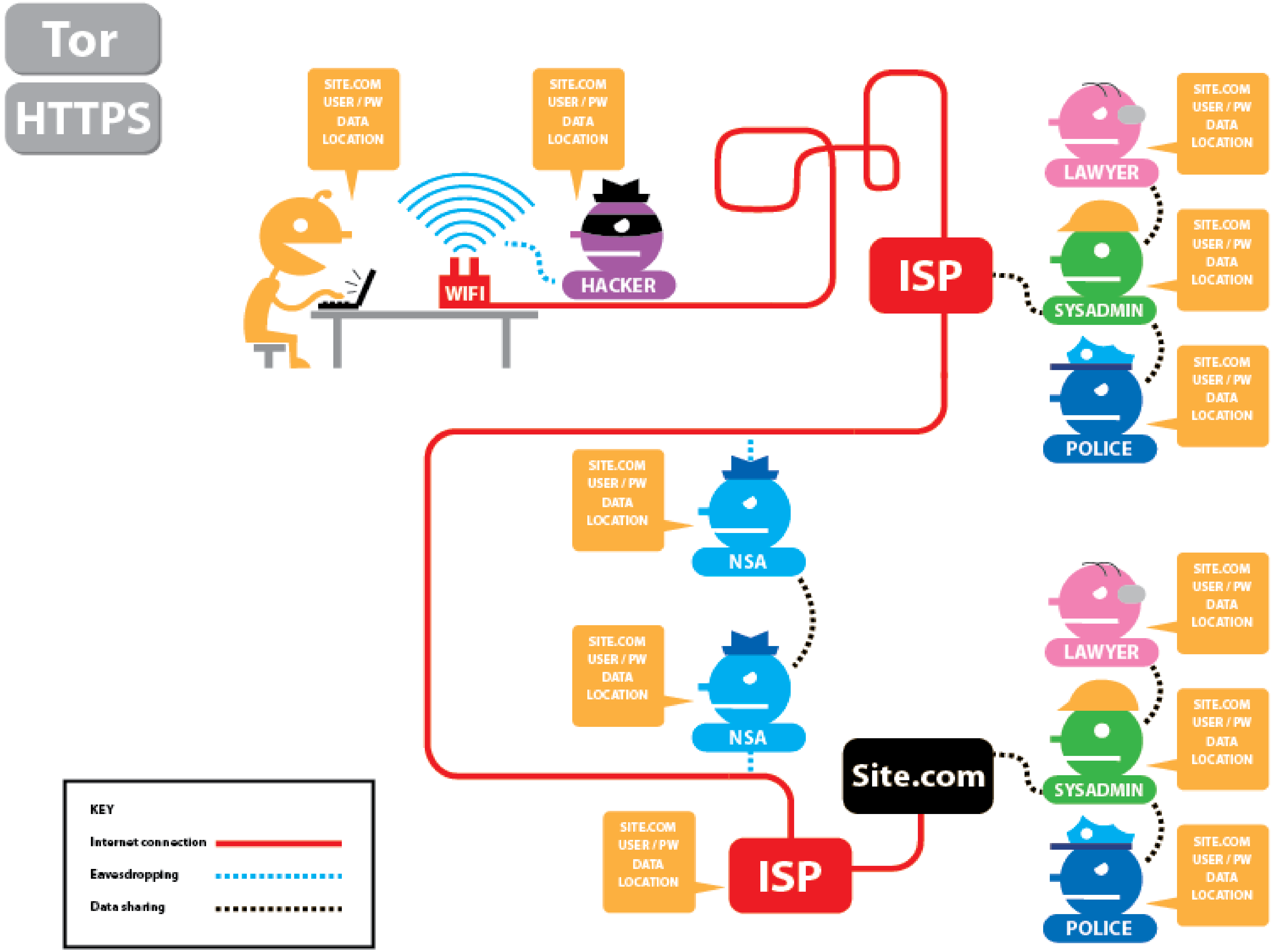
How Tor Works: 2

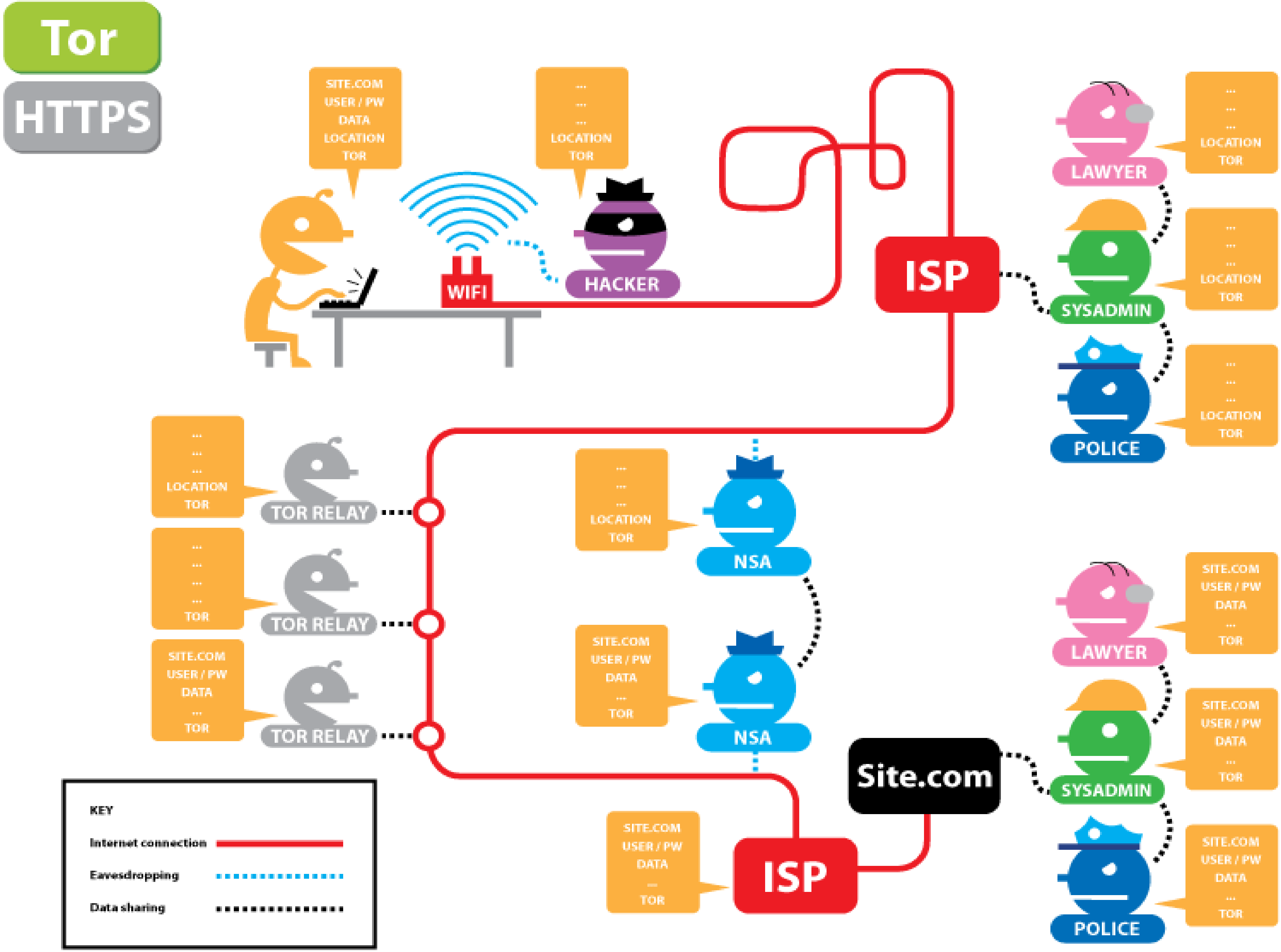


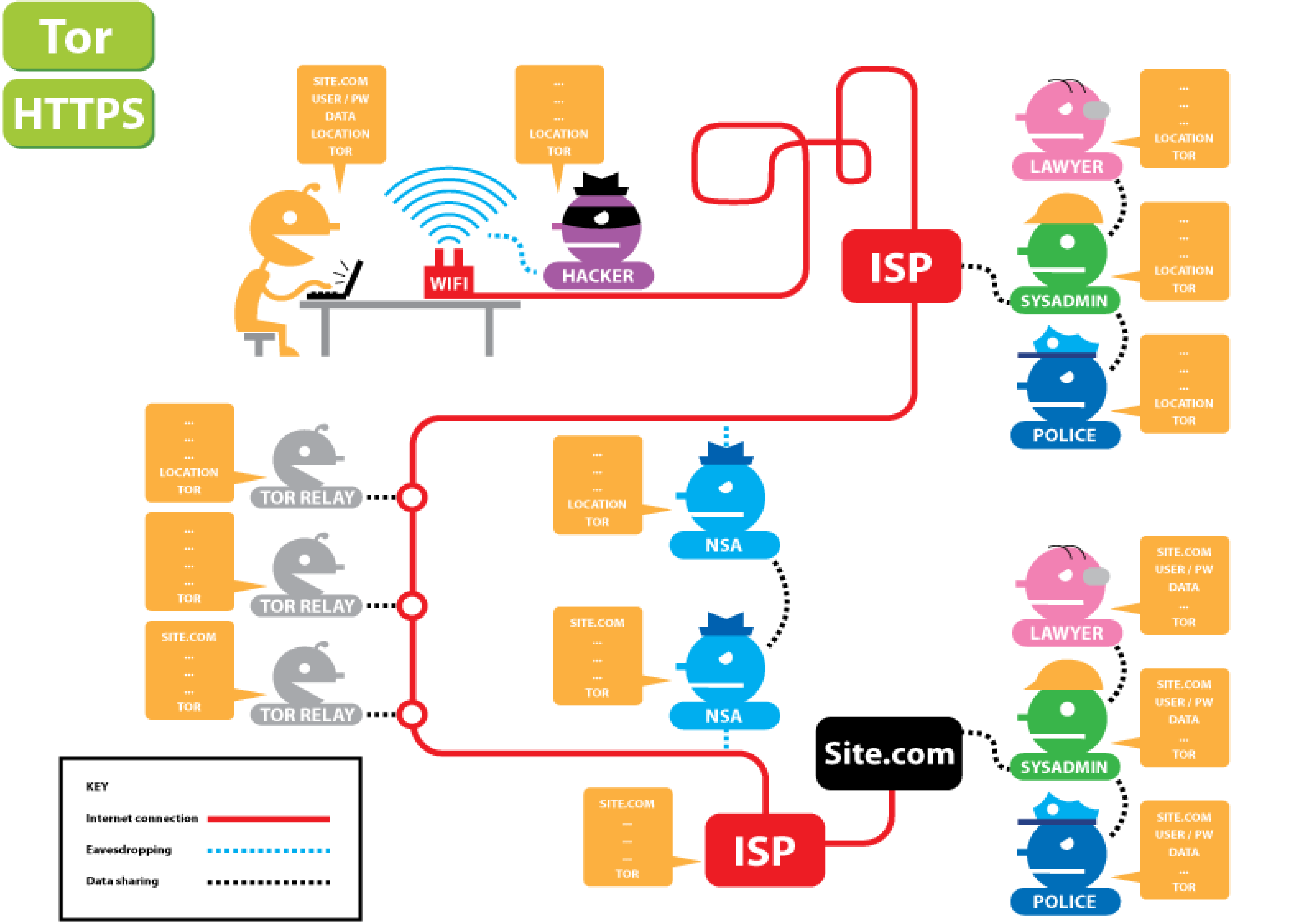
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.


Tor
HTTPS
SITE.COM USER / PW DATA LOCATION
SITE.COM USER / PW DATA LOCATION
WIFI
HACKER
ISP
LAWYER
SITE.COM USER / PW DATA LOCATION
SYSADMIN
SITE.COM USER / PW DATA LOCATION
POLICE
SITE.COM USER / PW DATA LOCATION
SITE.COM USER / PW DATA LOCATION
NSA
SITE.COM USER / PW DATA LOCATION
NSA
LAWYER
SITE.COM USER / PW DATA LOCATION
SYSADMIN
SITE.COM USER / PW DATA LOCATION
Site.com
POLICE
SITE.COM USER / PW DATA LOCATION
SITE.COM USER / PW DATA LOCATION
ISP
KEY
Internet connection
Eavesdropping
Data sharing


Tor
HTTPS
SITE.COM
USER / PW
DATA
LOCATION
SITE.COM
...
...
LOCATION
WIFI
HACKER
ISP
LAWYER
SITE.COM
...
...
LOCATION
SYSADMIN
SITE.COM
...
...
LOCATION
POLICE
SITE.COM
...
...
LOCATION
NSA
SITE.COM
...
...
LOCATION
NSA
SITE.COM
...
...
LOCATION
ISP
SITE.COM
...
...
LOCATION
Site.com
LAWYER
SITE.COM
USER / PW
DATA
LOCATION
SYSADMIN
SITE.COM
USER / PW
DATA
LOCATION
POLICE
SITE.COM
USER / PW
DATA
LOCATION
KEY
Internet connection
Eavesdropping
Data sharing


Tor
HTTPS
SITE.COM
USER / PW
DATA
LOCATION
SITE.COM
USER / PW
DATA
LOCATION
WIFI
HACKER
ISP
LAWYER
SITE.COM
USER / PW
DATA
LOCATION
SYSADMIN
SITE.COM
USER / PW
DATA
LOCATION
POLICE
SITE.COM
USER / PW
DATA
LOCATION
SITE.COM
USER / PW
DATA
LOCATION
NSA
SITE.COM
USER / PW
DATA
LOCATION
NSA
LAWYER
SITE.COM
USER / PW
DATA
LOCATION
SYSADMIN
SITE.COM
USER / PW
DATA
LOCATION
Site.com
POLICE
SITE.COM
USER / PW
DATA
LOCATION
SITE.COM
USER / PW
DATA
LOCATION
ISP
KEY
Internet connection
Eavesdropping
Data sharing


Tor
HTTPS
SITE.COM
USER / PW
DATA
LOCATION
TOR
...
...
...
LOCATION
TOR
WIFI
HACKER
ISP
...
...
...
LOCATION
TOR
LAWYER
...
...
...
LOCATION
TOR
SYSADMIN
...
...
...
LOCATION
TOR
POLICE
...
...
...
LOCATION
TOR
TOR RELAY
...
...
...
...
TOR
TOR RELAY
SITE.COM
USER / PW
DATA
...
TOR
TOR RELAY
...
...
...
LOCATION
TOR
NSA
SITE.COM
USER / PW
DATA
...
TOR
NSA
Site.com
SITE.COM
USER / PW
DATA
...
TOR
LAWYER
SITE.COM
USER / PW
DATA
...
TOR
SYSADMIN
SITE.COM
USER / PW
DATA
...
TOR
POLICE
SITE.COM
USER / PW
DATA
...
TOR
ISP
KEY
Internet connection
Eavesdropping
Data sharing


Tor
HTTPS
SITE.COM
USER / PW
DATA
LOCATION
TOR
...
...
...
LOCATION
TOR
WIFI
HACKER
ISP
...
...
...
LOCATION
TOR
LAWYER
...
...
...
LOCATION
TOR
SYSADMIN
...
...
...
LOCATION
TOR
POLICE
...
...
...
LOCATION
TOR
TOR RELAY
...
...
...
...
TOR
TOR RELAY
SITE.COM
...
...
...
TOR
TOR RELAY
...
...
...
LOCATION
TOR
NSA
SITE.COM
...
...
...
TOR
NSA
SITE.COM
...
...
...
TOR
ISP
Site.com
SITE.COM
USER / PW
DATA
...
TOR
LAWYER
SITE.COM
USER / PW
DATA
...
TOR
SYSADMIN
SITE.COM
USER / PW
DATA
...
TOR
POLICE
KEY
Internet connection
Eavesdropping
Data sharing

Use Tor!

1. Download from torproject.org
2. Install
3. Read the warning note
4. Use!

(instead of your normal browser)

Operating Systems

use open source.

check the project/people.

TRUST.

contribute and serve.

Operating Systems

use tails as a live system when there is something really serious for you...

tails.boum.org

File Encryption

<u>TrueCrypt</u>

e.g. makes hidden-hidden volumes

<u>FileVault</u> (for apple)

<u>LUKS</u>

Linux system for encrypted disks

<u>Full Disc encryption</u>

(comes nowadays e.g. with Ubuntu normal installer by default)

<u>GPG</u> can also be used for files

File Deletion

Overwrite, overwrite and overwrite.

Don't forget all those /tmp files.
Plenty of software exists.

Destroying physically might also be
a good idea, sometimes.
(letting a HDD fall while its running: good trick)

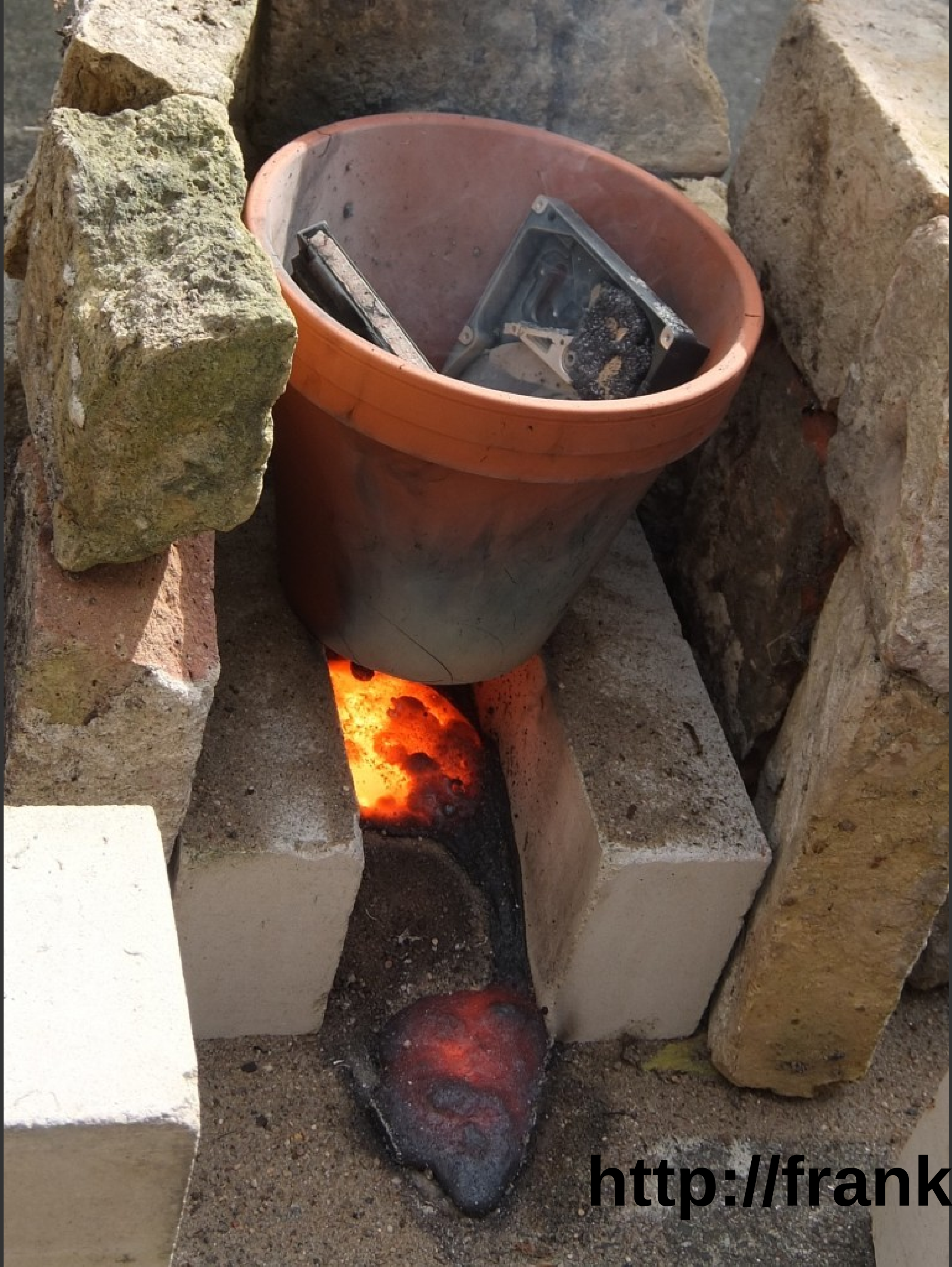
burn
HDDs
with

Thermite....

http://frank.geekheim.de

burn
HDDs
with

Thermite



http://frank.geekheim.de

http://frank.geekheim.de

http://frank.geekheim.de

http://frank.geekheim.de

http://frank.geekheim.de

http://frank.geekheim.de

Web Browsing

Already mentioned

https://

Tor

Browser Plugins

See list on

cryptoparty.in/brief#browser_plugins

e.g.

* HTTPS-everywhere
* Disconnect and Ghostery

Direct Messaging

Example: Skype

Already proofen that
they read the messages!

(and India, US, UK read anyway)

Use XMPP/Jabber

- Install client / app (e.g. pidgin)
  - http://en.wikipedia.org/wiki/Comparison_of_instant_messaging_clients
- Choose a provider
  - jabber.org, jabber.ccc.de, riseup.net, dukgo.com
  - See huge list on: xmpp.net

Add Encryption

Off The Record Messaging
(OTR)

1. Install OTR-Plugin in your client/app

2. Use it!

(Works for every Instant Messaging protocol that is supported by the client, e.g. g-talk, fb-chat, IRC)

Off the record?

Yes!

It is just a session-key

It will be thrown away afterwards

So you can always say „it wasn't me!”

(that is not possible with GPG though)

Group Messaging

Jabber/xmpp can have chatrooms.

IRC (Internet Relay Chat) is 25yrs old and is still very alive. Very decentral, one can make an own network.

(Mailinglists can be encrypted, too)

Voice

Jabber/xmpp, can also do voice and video, see e.g. http://jit.si

Mumble: designed for team speak,
simple to admin,
is encrypted.

Ekiga: SoftPhone, Video Conf,
Instant Messenger

Android

GPG: **K9** (email) + **APG** (gpg)

IM: **TextSecure** (OTRs msgs)

TOR: **Orbot** works with: Orweb, Firefox,

Gibberbot, DuckDuckGo (search engine), Twitter

Android

Play Store: **F-Droid**, only FLOSS apps

Voice: **RedPhone** encrypts voice (over IP)

SIP: **Csimple** encrypts SIP („OSTN-Project”)

ObscuraCam: blurres automatically faces etc

OsmAnd: editable map, very good in himalaya

Android

Needs to be kept clean.

Don't trust google, but here you have to.

Check cyanogenmod for your device.

Think about physical security.

What happens in case of loss?

Android

All software will be new on the marked, so how can I decide here what software to use?

Check the technology

(e.g. OTR on IM sounds reasonable).

Check the project/people.

TRUST.

CONTRIBUTE. SERVE.

CONTRIBUTE.

SERVE.

sva@ccc.de — twitter@sva
thupten104@gmail.com
beli@cis-india.org
santosh@hackerearth.com
— twitter@importerror

THX
<3

DROP OUTS

ALL THE protocols

„Simpler is safer and easier.”

e-mail wasn't invented to transport attachments.
FTP (File Transfer Protocol) was invented at the same time nearly 50yrs back!

Please use the whole Internet!

direct messaging

Example: Skype

Already proofen that
they read the messages!

(and India, US, UK read anyway)

use xmpp/jabber

- Install client / app (e.g. pidgin)
  - http://en.wikipedia.org/wiki/Comparison_of_instant_messaging_clients
- Choose a provider
  - jabber.org, jabber.ccc.de, riseup.net, dukgo.com
  - See huge list on: xmpp.net

Extensible Messaging and Presence Protocol (XMPP)

communications protocol (1999) real-time instant messaging (IM), presence information, contact list maintenance.

Extensible, also used for publish-subscribe systems, signalling for VoIP, video, file transfer, gaming, Internet of Things, social networking services.

XMPP is an open standard and interoperates with other organizations' implementations.

add encryption

Off The Record Messaging
(OTR)

1. Install OTR-Plugin in your client/app

2. Use it!

(Works for every Instant Messaging protocol that is supported by the client, e.g. g-talk, fb-chat, IRC)

off the record?

Yes!

It is just a session-key

It will be thrown away afterwards

So you can always say „it wasn't me!”

(that is not possible with GPG though)

group messaging

Jabber/xmpp can have chatrooms.

IRC (Internet Relay Chat) is 25yrs old and is still very alive. Very decentral, one can make an own network.

(Mailinglists can be encrypted, too)

voice

Jabber/xmpp, can also do voice and video, see e.g. http://jit.si

Mumble: designed for team speak,
simple to admin,
is encrypted.

Ostel for android
https://guardianproject.info/wiki/Ostel

Drop outs

Maybe still useful

Drop outs

Maybe still useful

Video

- Maybe the video of diffie-hellmann?
- https://www.youtube.com/watch?feature=player_detailpage&v=YEBfamv-_do#t=126s

risk management

It is all about the assets, you want to protect.
Knowledge is power.
Always think on the weakest link.
Simpler is safer and easier.
More expensive doesn't mean more secure.
What's secure today may not be secure tomorrow.

There is no perfect security,
it's always a Trade-Off.
=> Security is a process!
(also: encrypt it or don't keep it!)

(ssd.eff.org)

ressources:

cryptoparty.in/brief
Also: /documentation or /handbook

securityinabox.org/ focused on the "global south", Unfortunately screenshots etc are outdated.

ssd.eff.org/ focused on US

prism-break.org/ list of alternatives

(many more linked from there)

who are you?

1. Who are you?
e.g. name, profession, main interests,...

2. Why are you here, what group do you see yourself?
e.g. (A) just wanna have more privacy / (B) for me it is serious...

4. What crypto do you already use? Can you show/teach?
e.g. email (gpg), webbrowsing (tor/https/plugins), chat (jabber, otr, cryptocat), connection (vpn), file-encryption (truecrypt, etc), full disc encryption, mobile (android: sms, voice), etc...

5. What do you wanna learn?
(see above)

6. Witch operating system(s) do you run? (PC + smartphone)
e.g. Windows, OSX, Linux (Ubuntu), Android, iPhone, Blackberry,...

install GnuPG

The one that is doing the encryption.

http://www.gnupg.org

windows:
http://www.gpg4win.org/

Mac:
https://gpgtools.org/

1984
WAS
NOT
SUPPOSED
TO BE AN
INSTRUCTION
MANUAL

to encode

no secret key, but code
provides only obfuscation
by transformation

2-way-function (encode, decode)
e.g.: base64, ASCII

to encrypt

with secret key
supports confidentiality
transformation

2-way-function (encrypt, decrypt)
e.g.: AES, DES, RC4

to hash

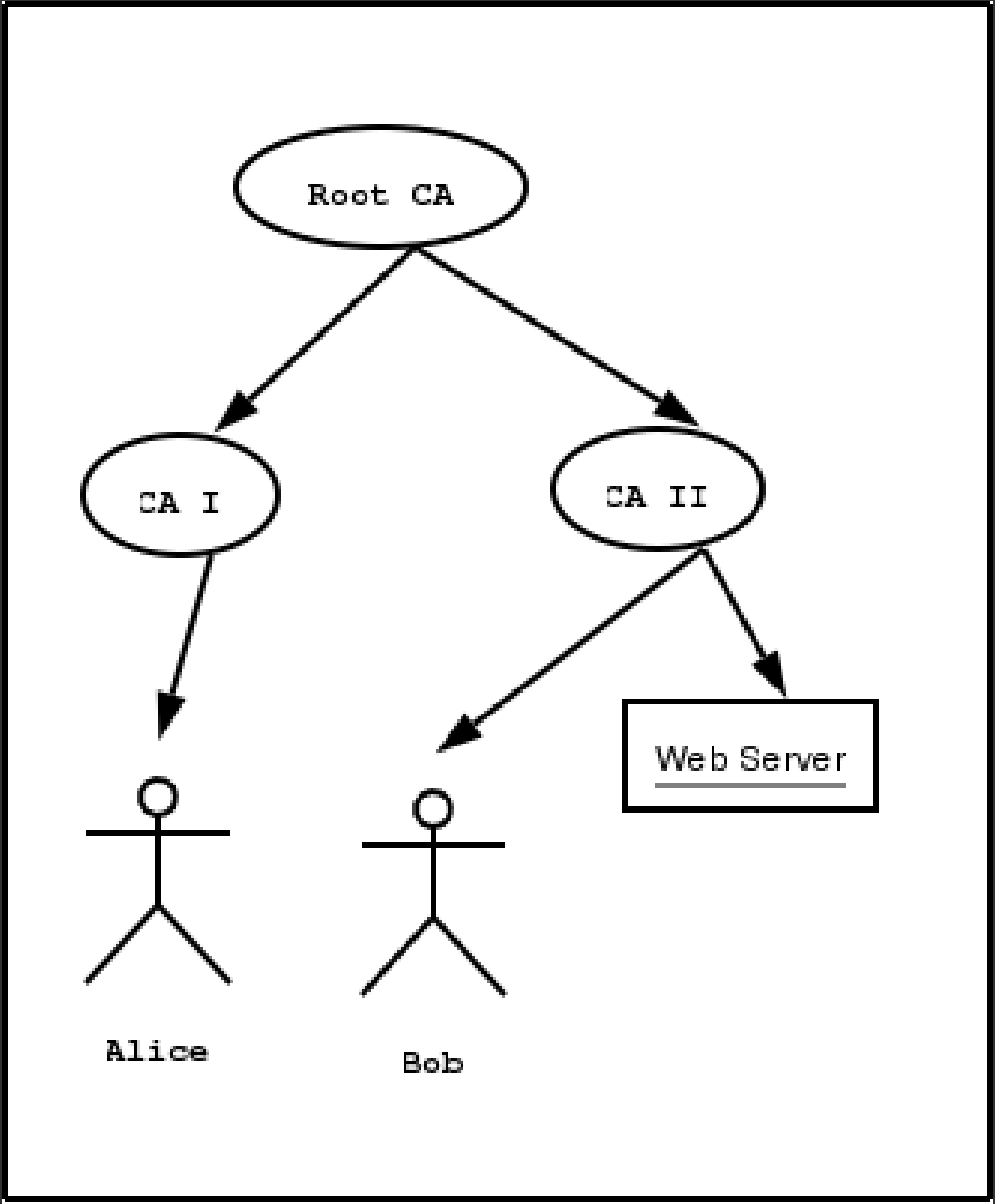
calculates a fixed size value
(like cross sum 5 from 23)
supports integrity
shortening/abbreviation

1-way-function
e.g.: md5, sha512

to sign

encrypting the hash
(key, confidential/trust, 2-way)

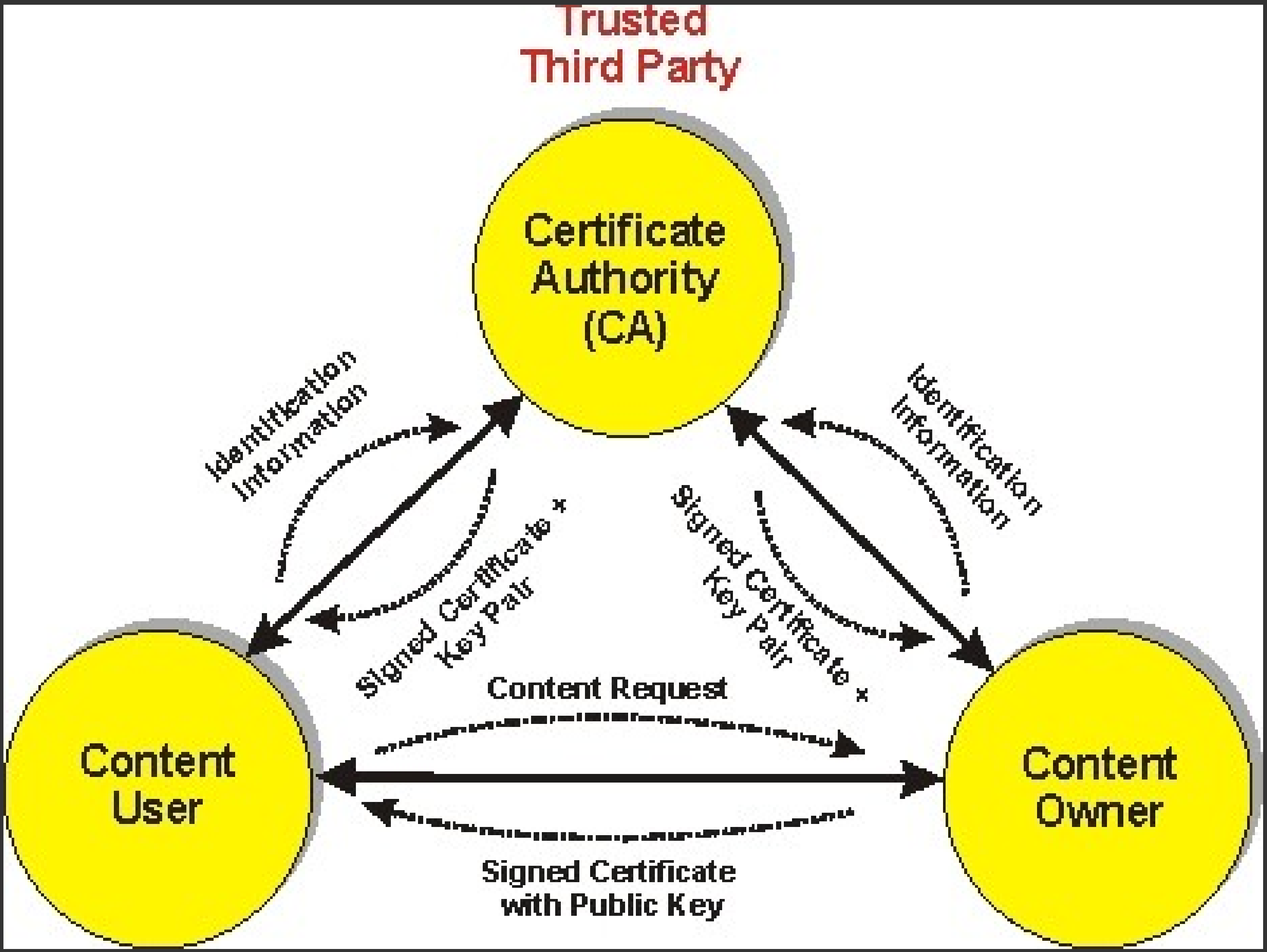
supports integrity+auth
e.g.: HMAC, DSA



Two typical X.509 Certification paths

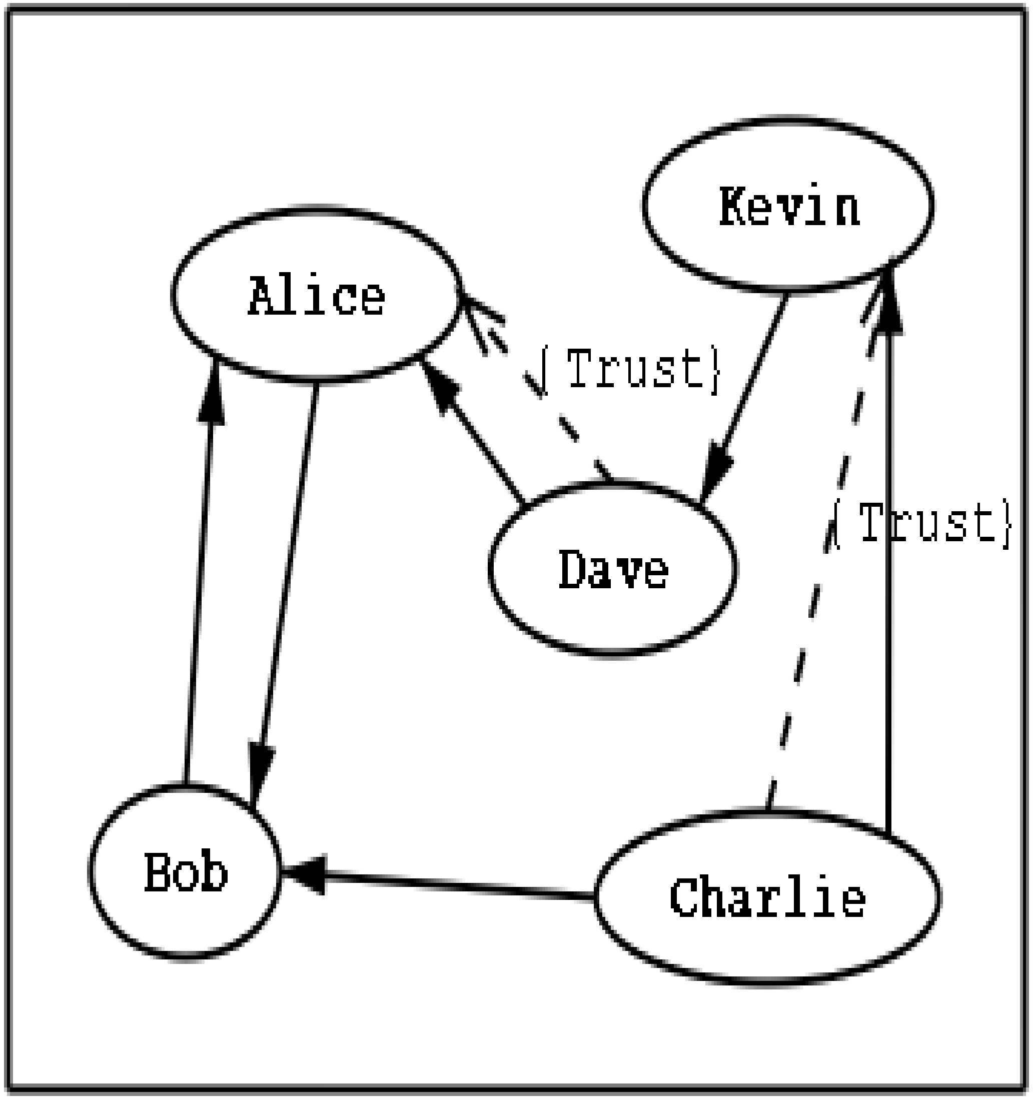
CA

- Centralized
- Digital certificates required
- Issued by a third party (cost)
- Third party has trust of sender and addressee


Trusted
Third Party
Certificate Authority (CA)
Identification Information
Signed Certificate + Key Pair
Identification Information
Signed Certificate + Key Pair
Content Request
Content User
Content Owner
Signed Certificate with Public Key

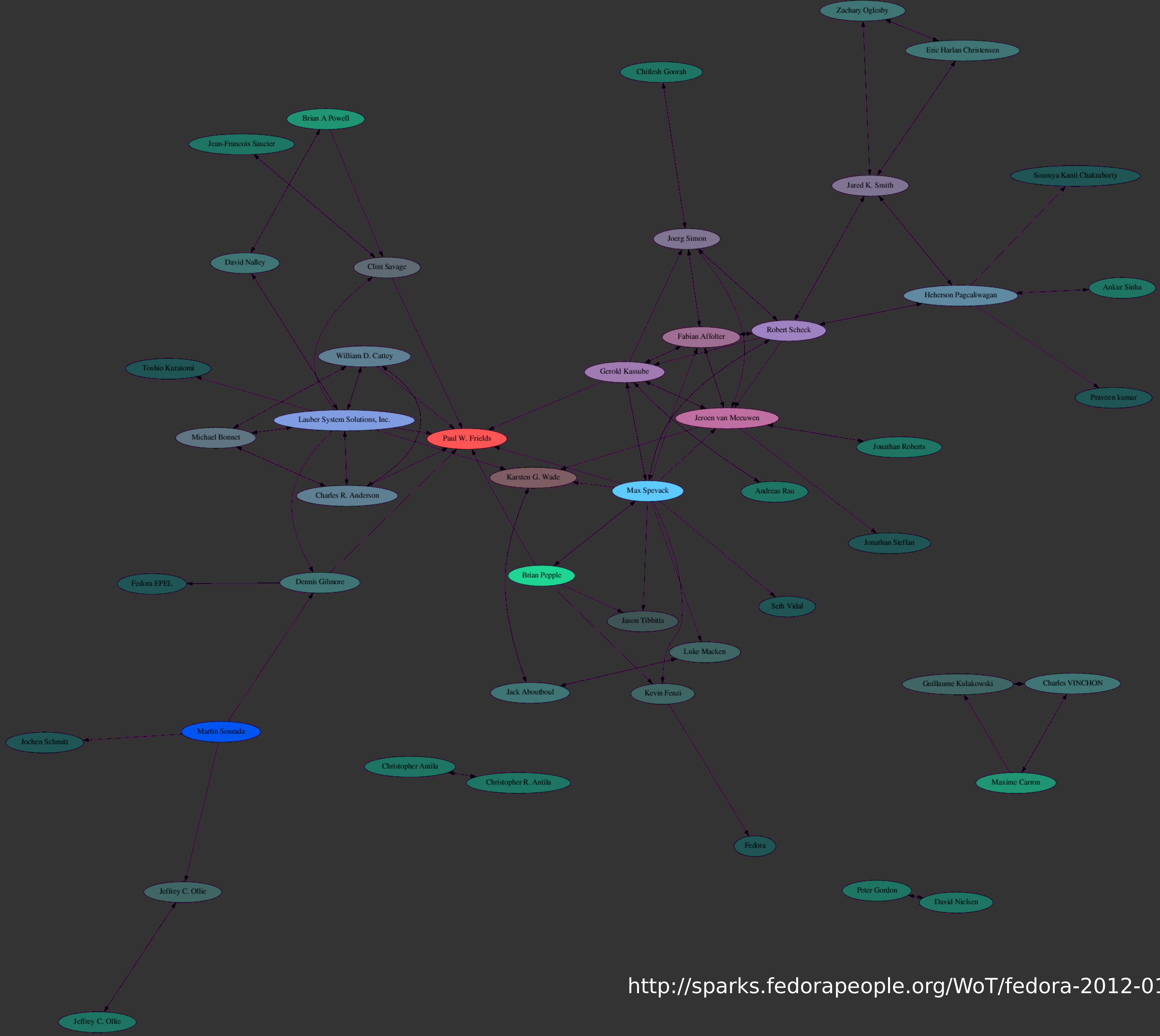
http://www.althos.com/sample_diagrams/ag_Digital_Certificate_Operation_low_res.jpg

web-of-trust



An example of the web of trust model

- Decentralized
- “fault-tolerant web of confidence”
- Helpful when people do not actually meet
- Shows social web, too



http://sparks.fedorapeople.org/WoT/fedora-2012-01-07.gif

trust models - why?

There are plenty of reasons for and against those trust models.

“subkeys without a properly trusted master key makes much sense”

Please discuss!

trust - implementation

You sign the key of an other person
by checking / proving the fingerprint,
with the help of your key.

Then you are now part
of the web-of-trust.

subkeys - what?

Subkey is like a “child-key” of a key.

You can have many such subkeys.

Main key is called masterkey.

Master key: Sign, Certify, Authorize

Sub key: Sign, Encrypt

(only master key can sign someone else's key)

subkeys - why?

Make it easy to manage multiple keys.

You cannot trust all your systems, subkeys provide a way to have different trust levels for different purposes (e.g.: Android phone).

subkeys - how?

By default, GPG master key is only for *sign, certify, authorize*

Implicitely created: related subkey for *encryption*

That means we see two keys in `gpg --list-keys <ID>` output (or in the "key properties" in thunderbird).

subkeys - how?

Creating another subkey for *sign:*
Allows you to sign messages
with the trust level of master key,
can be used to sign messages only.

Creation of subkey requires
secret master key.
Once we have create the subkeys
(for *encryption* and for *sign*)
we delete master secret key.

trust models

Remember the basic principles:

- Confidentiality
  no one else can read it
- Integrity
  no one else can modify
- Identity/authorization/authentication
  message is from the one person

trust models

Auth: How do you know that the sender is actually the one he claims to be?

Certificate Authority (CA)
=> depends on trusted third party

Web-Of-Trust
=> depends on mutual trust

generate keys

Choose “OpenPGP” in the thunderbird menu
Choose “key management”
Choose “generate”
Choose “new key pair”
Choose “advanced” => 4096 RSA

(plenty of tutorials with screenshots etc. in the web)

use!

Publish your public key:
Keymanagement => right click on your key
=> “Upload public keys to keyserver”

Send your public key to the one next to you:
“Send public key by email”

Import the key you got from the one next to you:
Right click on attachement “Import key”

Send an encrypted mail to the one next to you:
Write email, choose encryption, choose key, send.