



UNIVERSIDAD  
DE GRANADA

# INTERNET PROFUNDA – RED TOR

---

Fundamentos de Redes

Carmen Rosa López - Ignacio Vellido Expósito

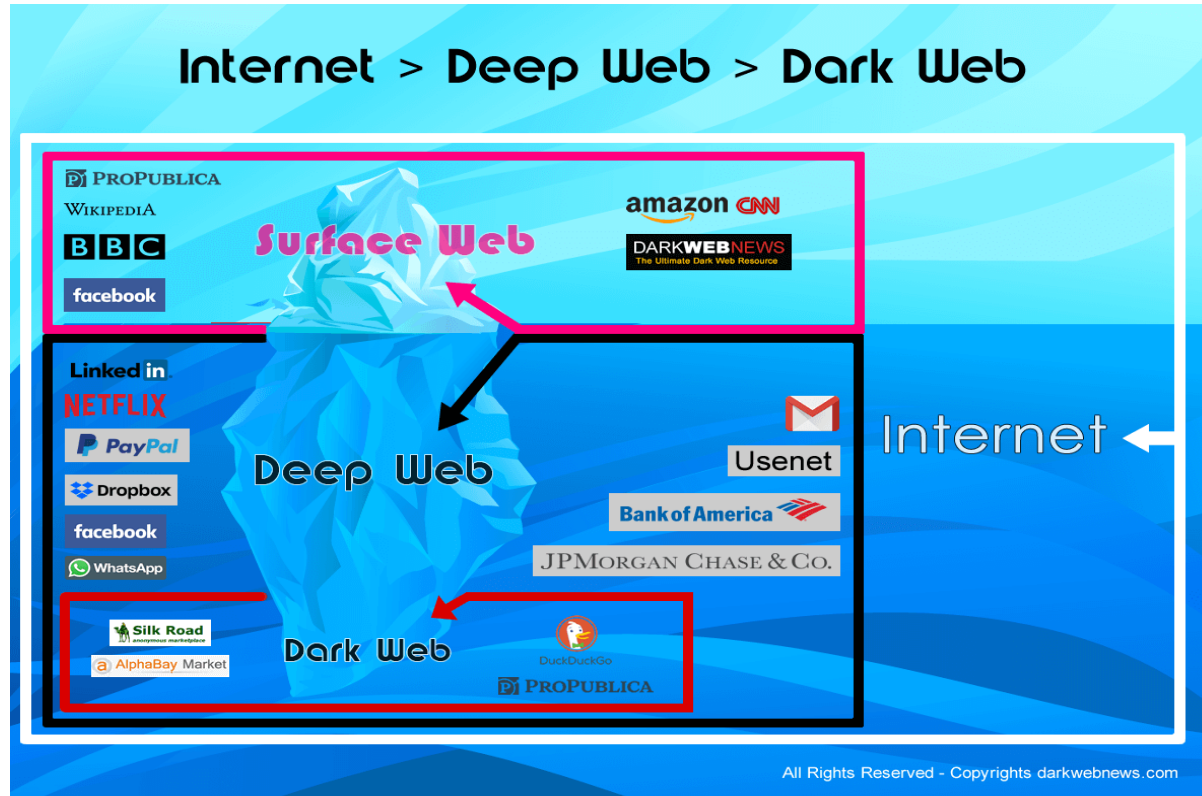
# Índice

1. Niveles de Internet
2. Red Tor
  - 2.1. Protocolos
  - 2.2. Enrutamiento de Cebolla
  - 2.3. Servicios Ocultos (.onion)
3. Ventajas e inconvenientes
4. Referencias



 Demostración con Wireshark

# Niveles de Internet



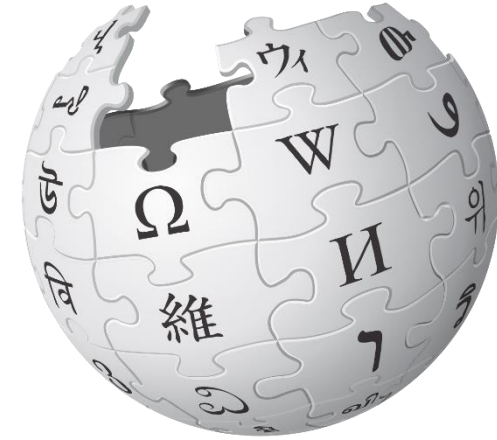
Web Superficial → 4%

Web Profunda → 96%

Web Oscura → 6%

# | Internet Superficial

Google



YouTube

facebook®

ebay™



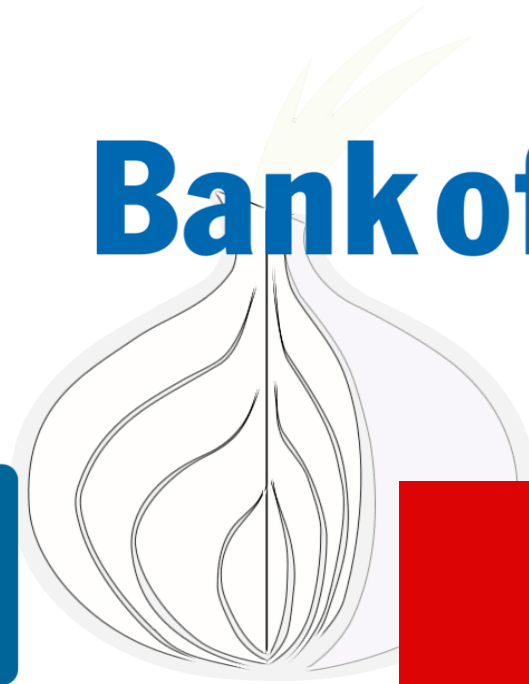
# Deep Web



**Bank of America**



**Linked in**



**NETFLIX**



# Dark Web



# ¿Qué es Tor?



## The Onion Router

- Mantiene la privacidad del usuario
- Busca el anonimato

# Red Tor



## Financiación:

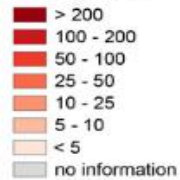
- Personales
- Mozilla
- Google
- ...



# Red Tor

## The anonymous Internet

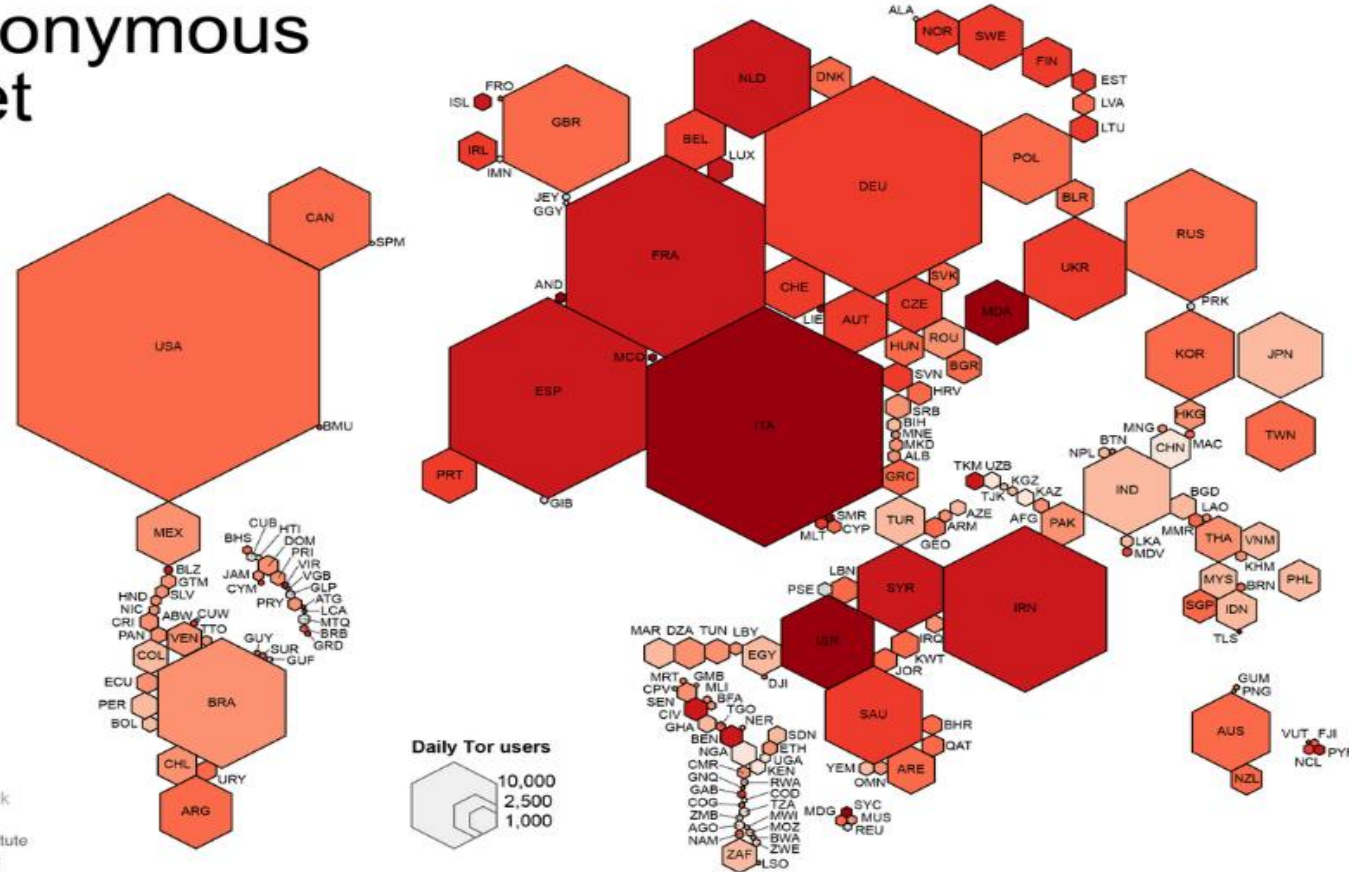
Daily Tor users  
per 100,000  
Internet users



Average number of  
Tor users per day  
calculated between  
August 2012 and  
July 2013

data sources:  
Tor Metrics Portal  
metrics.torproject.org  
World Bank  
data.worldbank.org

by Mark Graham  
(@geoplace) and  
Stefano De Sabbata  
(@maps4thought)  
Internet Geographies at  
the Oxford Internet Institute  
2014 • geography.oii.ox.ac.uk

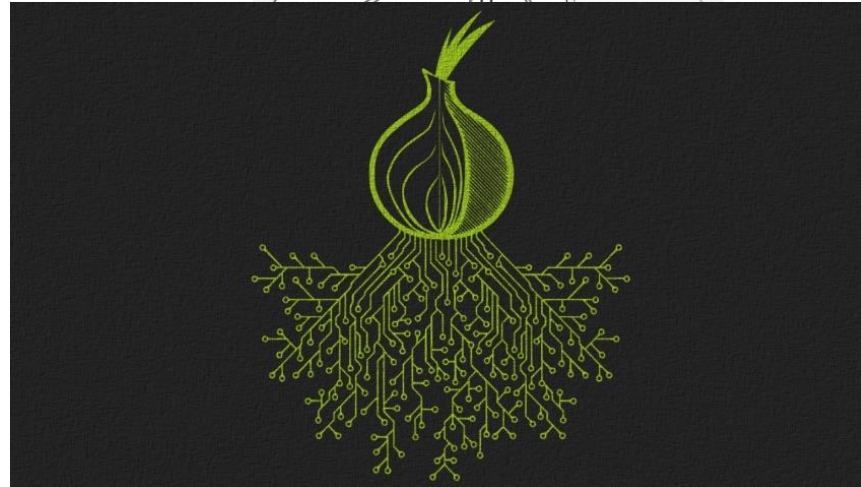


# Red Tor

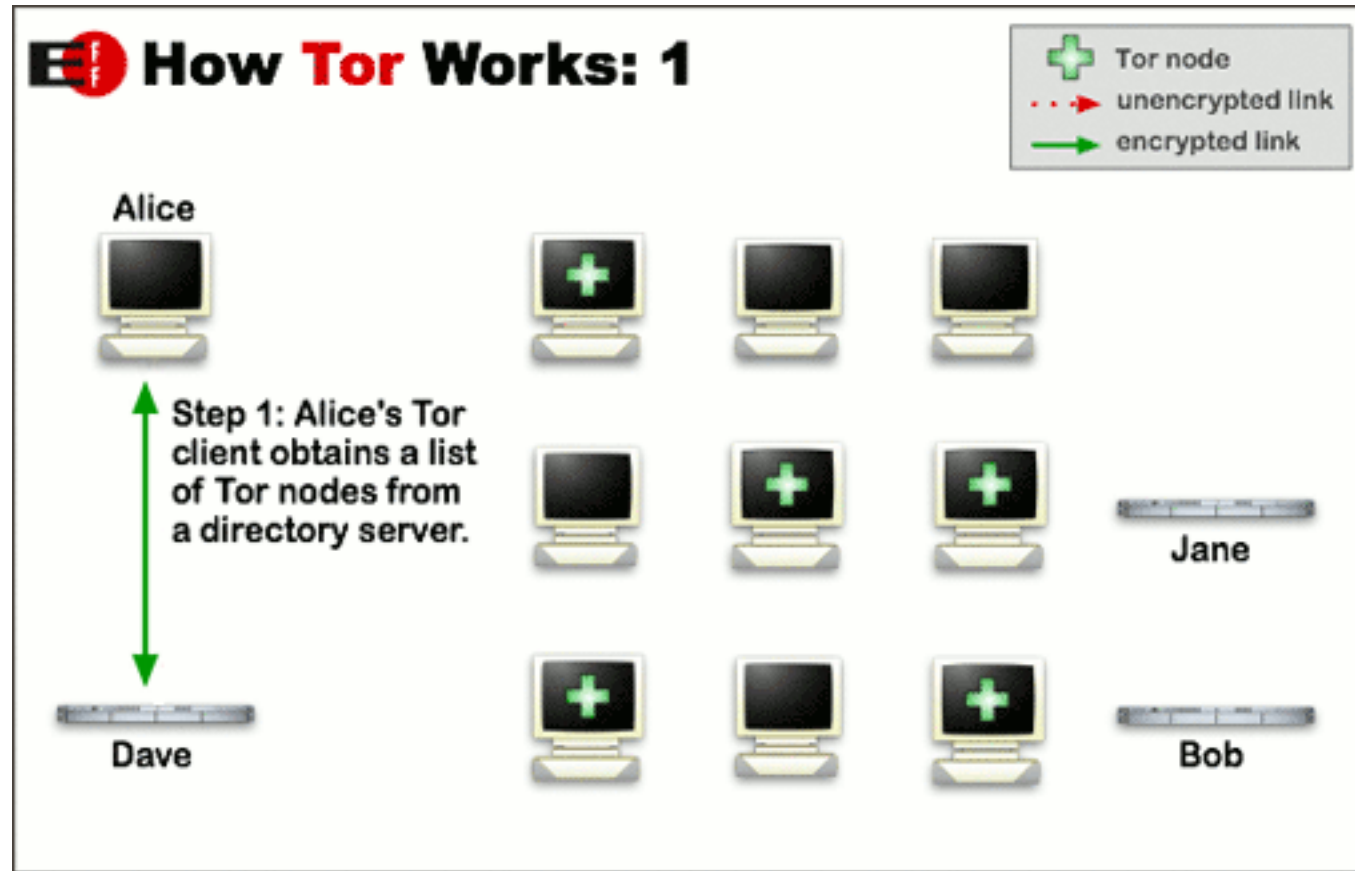


# ¿Cómo funciona Tor?

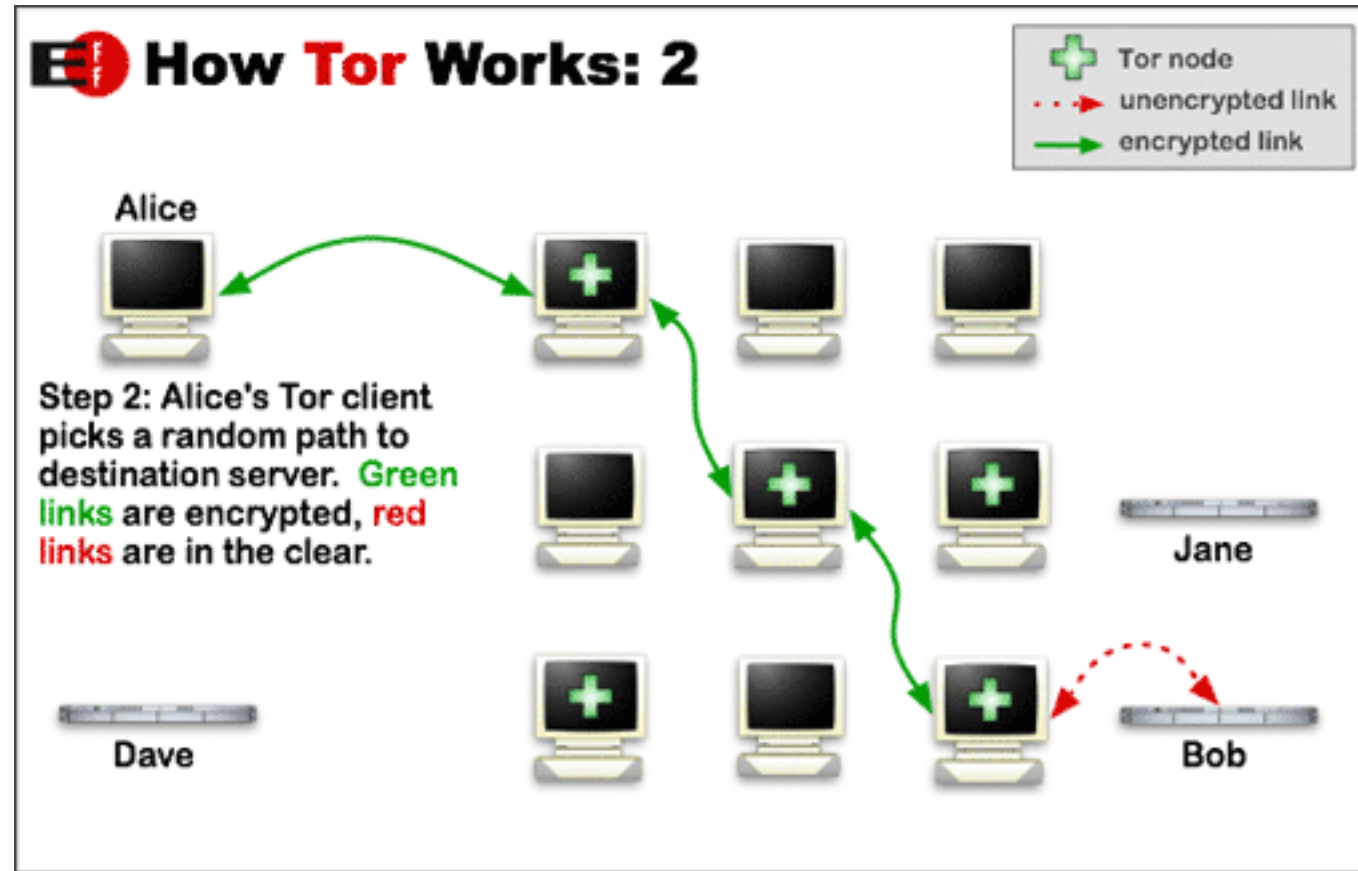
- Se basa en un método por capas
- Encripta cada comunicación



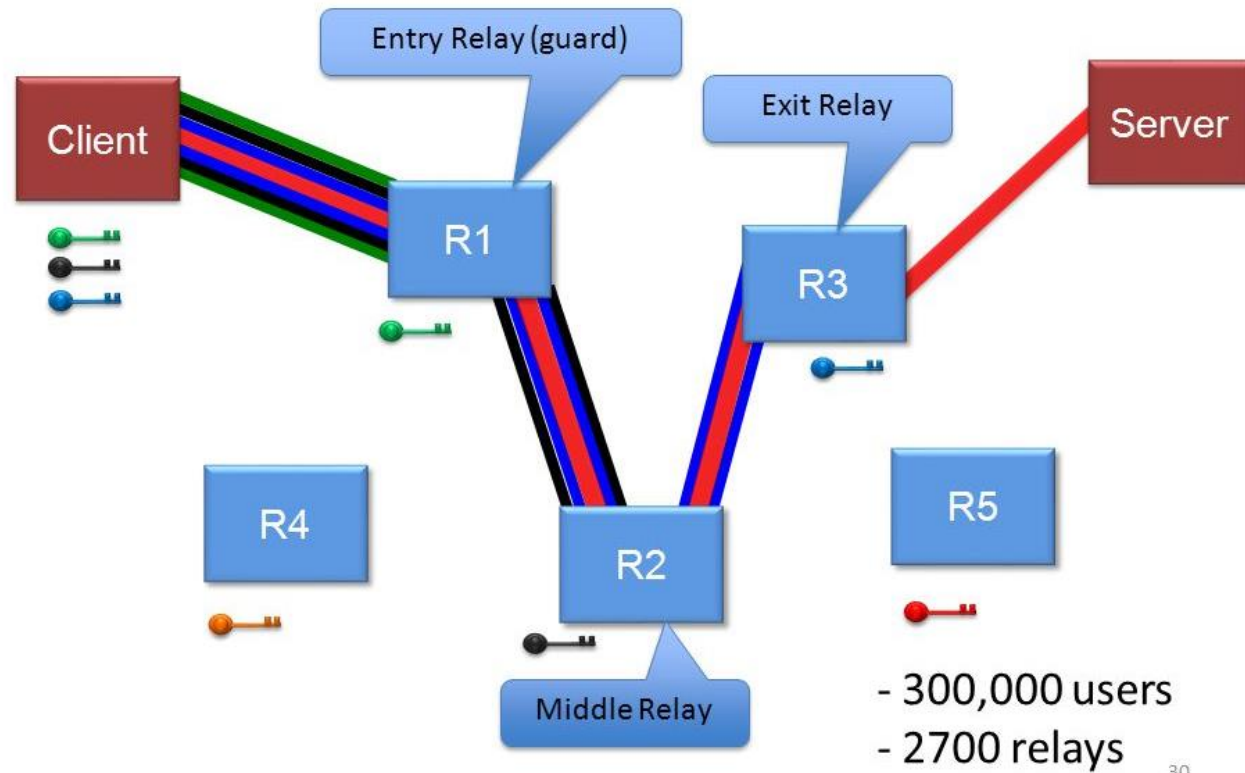
# Enrutamiento de Cebolla



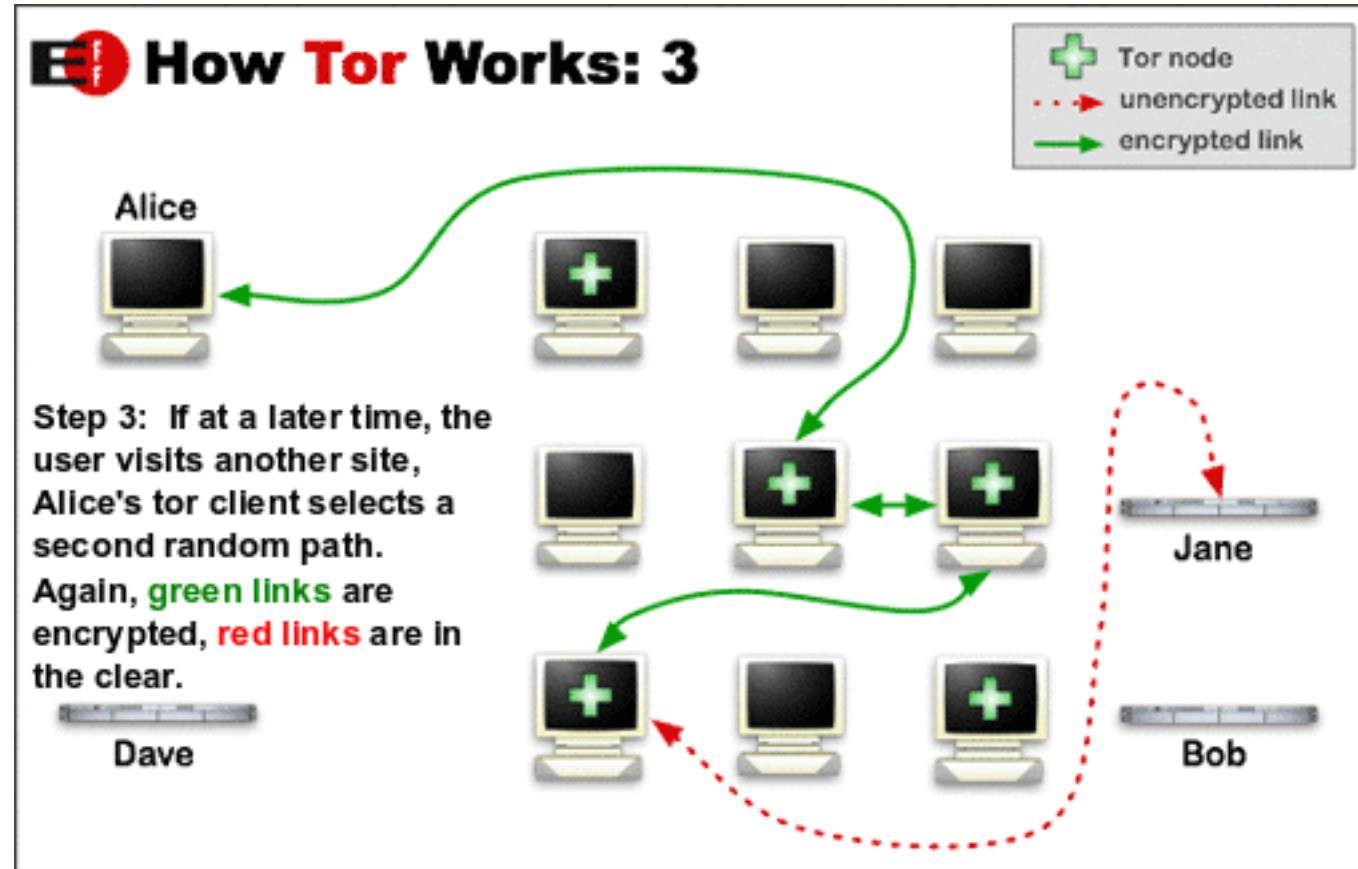
# Enrutamiento de Cebolla



# Enrutamiento de Cebolla

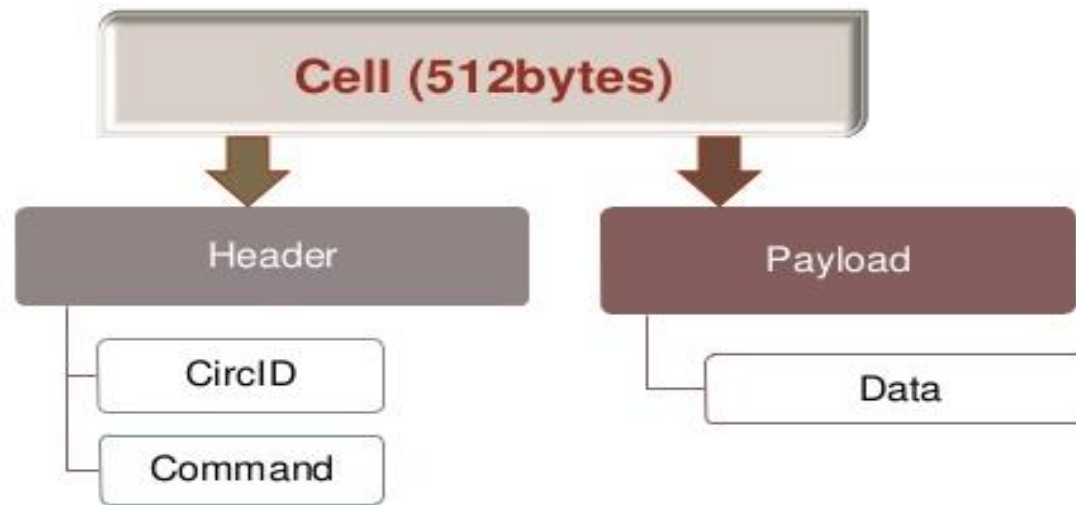


# Enrutamiento de Cebolla





# Células

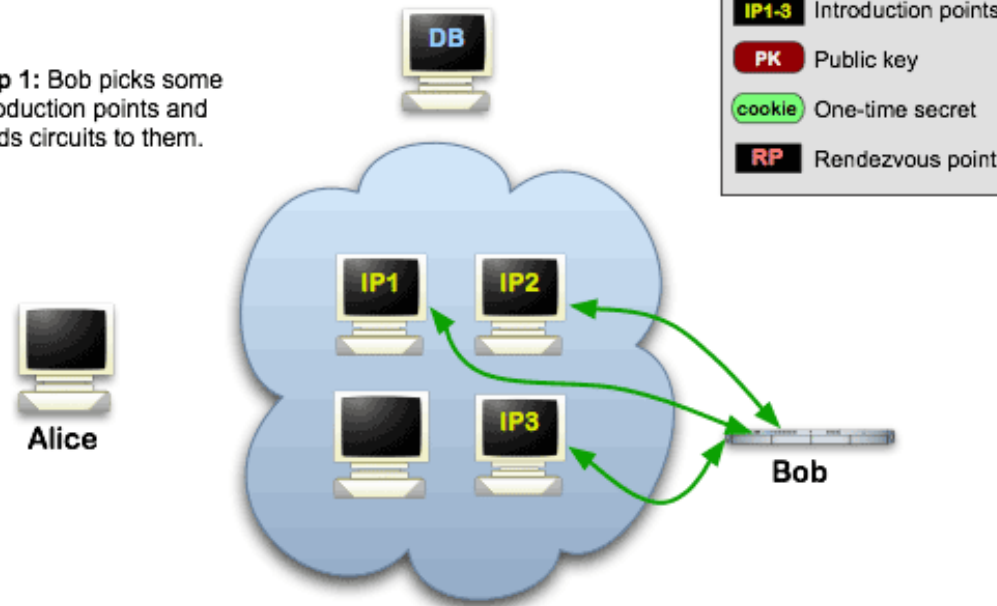




# Servicios ocultos

## Onion Services: Step 1

**Step 1:** Bob picks some introduction points and builds circuits to them.

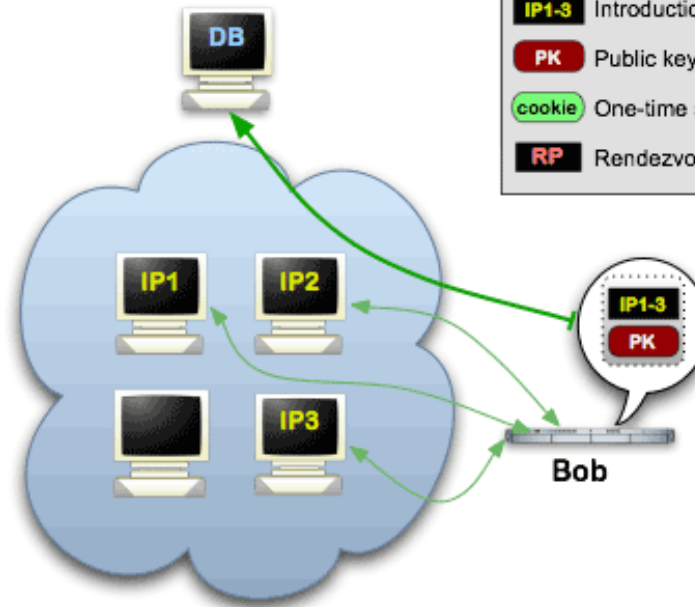


# Servicios ocultos

## Onion Services: Step 2

**Step 2:** Bob advertises his service -- XYZ.onion -- at the database.

Alice

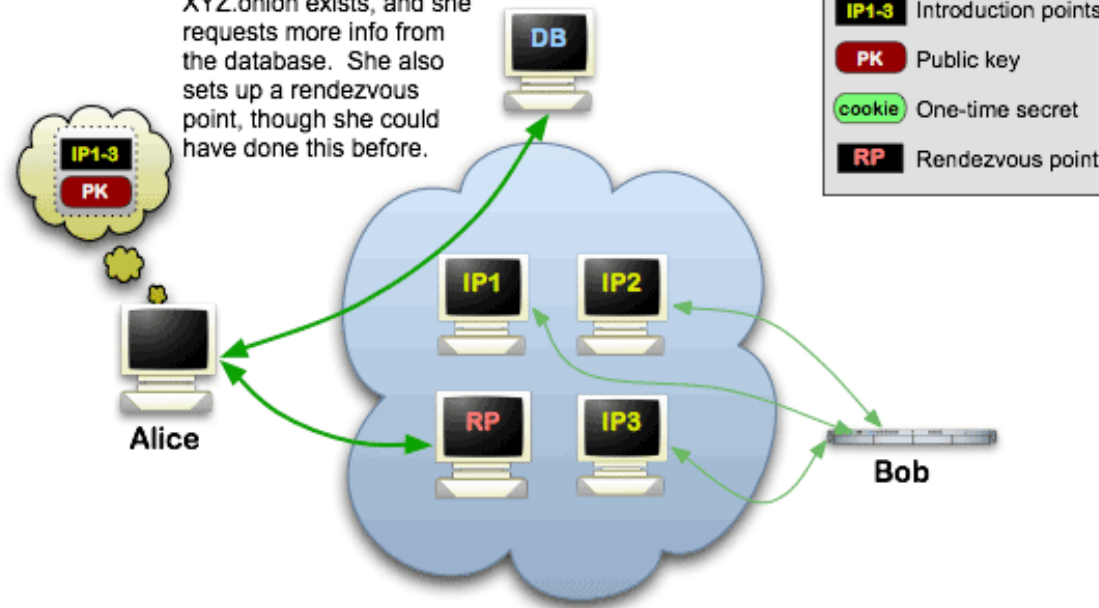


# Servicios ocultos



## Onion Services: Step 3

**Step 3:** Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.

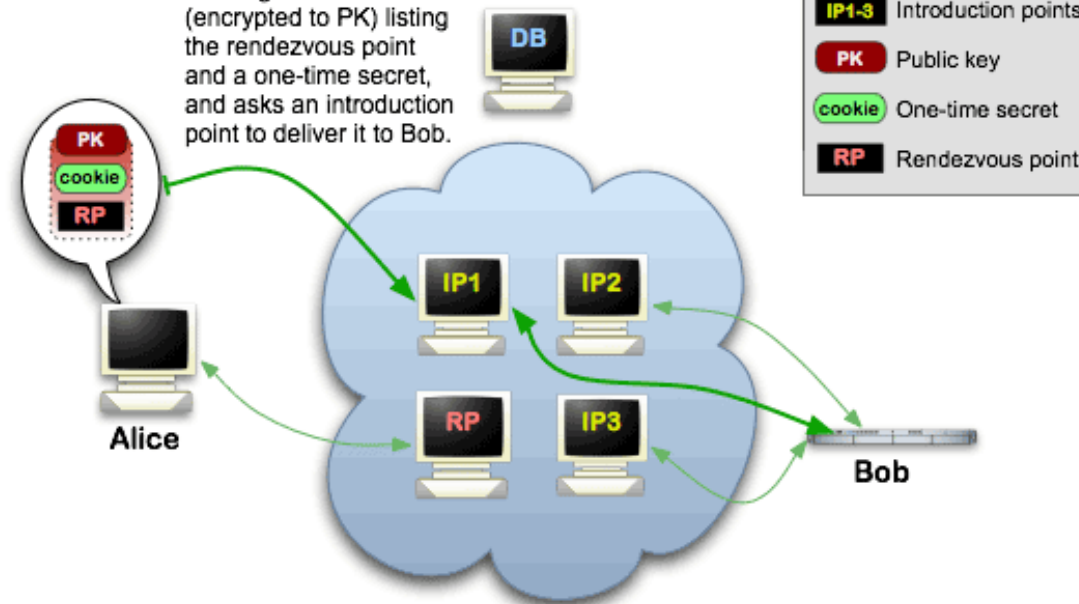


# Servicios ocultos



## Onion Services: Step 4

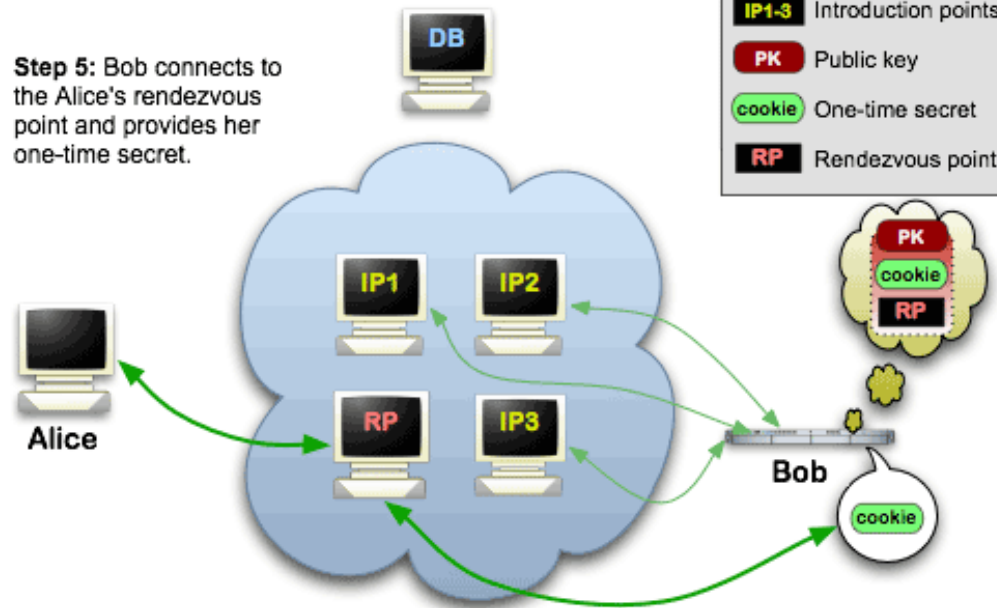
**Step 4:** Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.



# Servicios ocultos

## Onion Services: Step 5

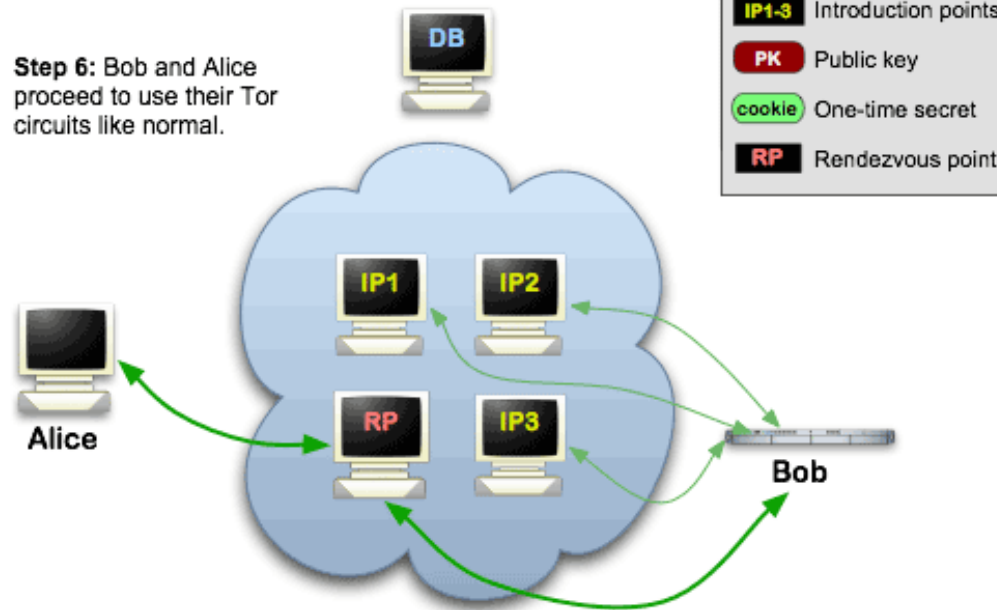
**Step 5:** Bob connects to the Alice's rendezvous point and provides her one-time secret.



# Servicios ocultos

## Onion Services: Step 6

**Step 6:** Bob and Alice proceed to use their Tor circuits like normal.

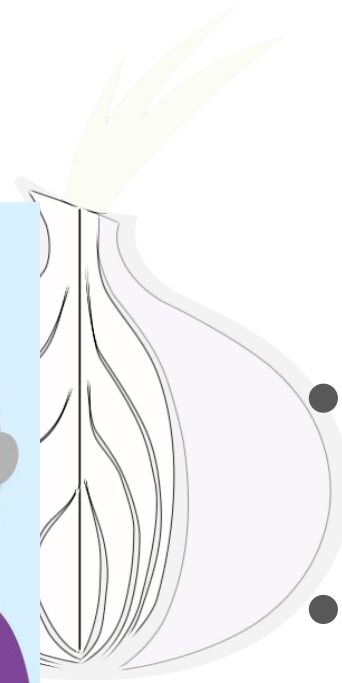
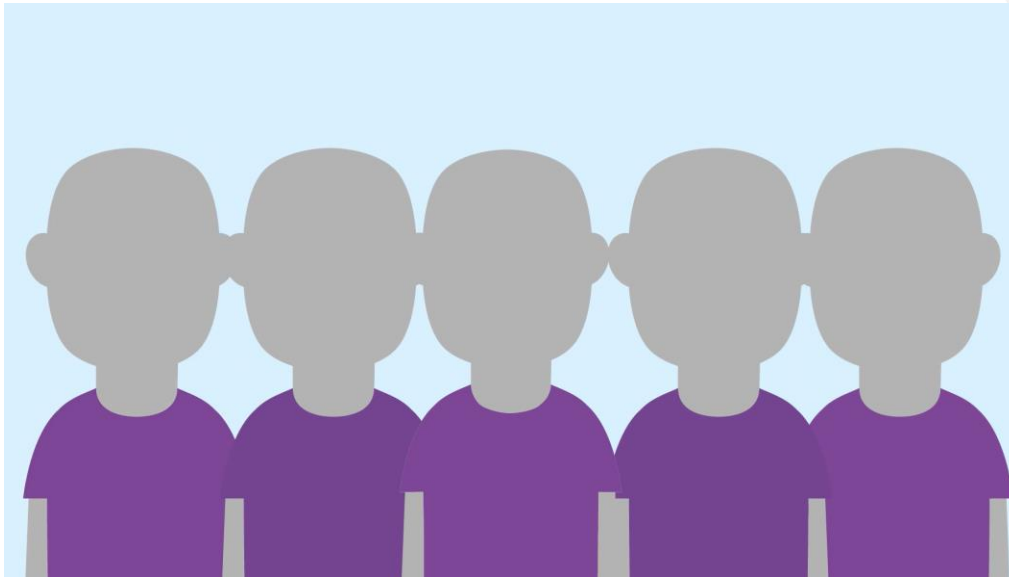


# Pero... ¿son todo ventajas en Tor ?



# Pero... ¿son todo ventajas en Tor ?

## Ventajas



- Seguridad
- Privacidad

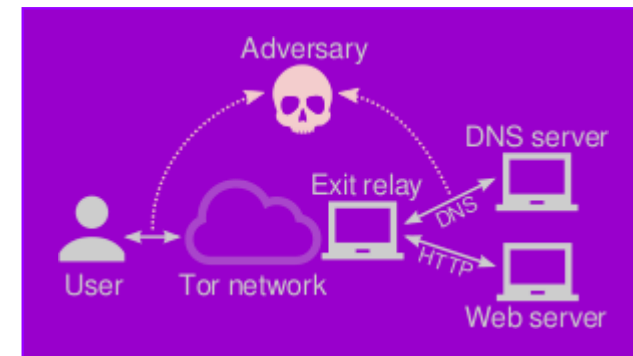


# Pero... ¿ es todo ventajas en Tor ?

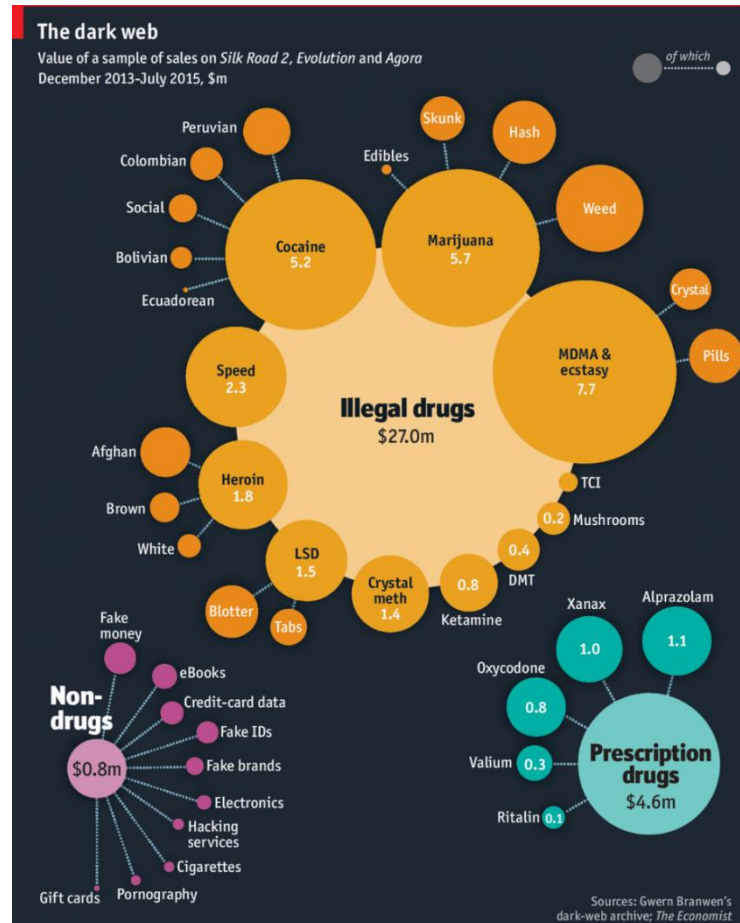
## Inconvenientes



- No es 100% fiable
- Negocios ilegales



# Darknet Markets



# Referencias

- <https://www.torproject.org/>
- <https://gitweb.torproject.org/>
- <https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt>
- <http://geography.oii.ox.ac.uk/the-anonymous-internet/>
- <https://github.com/torproject/torspec/blob/master/rend-spec-v3.txt>





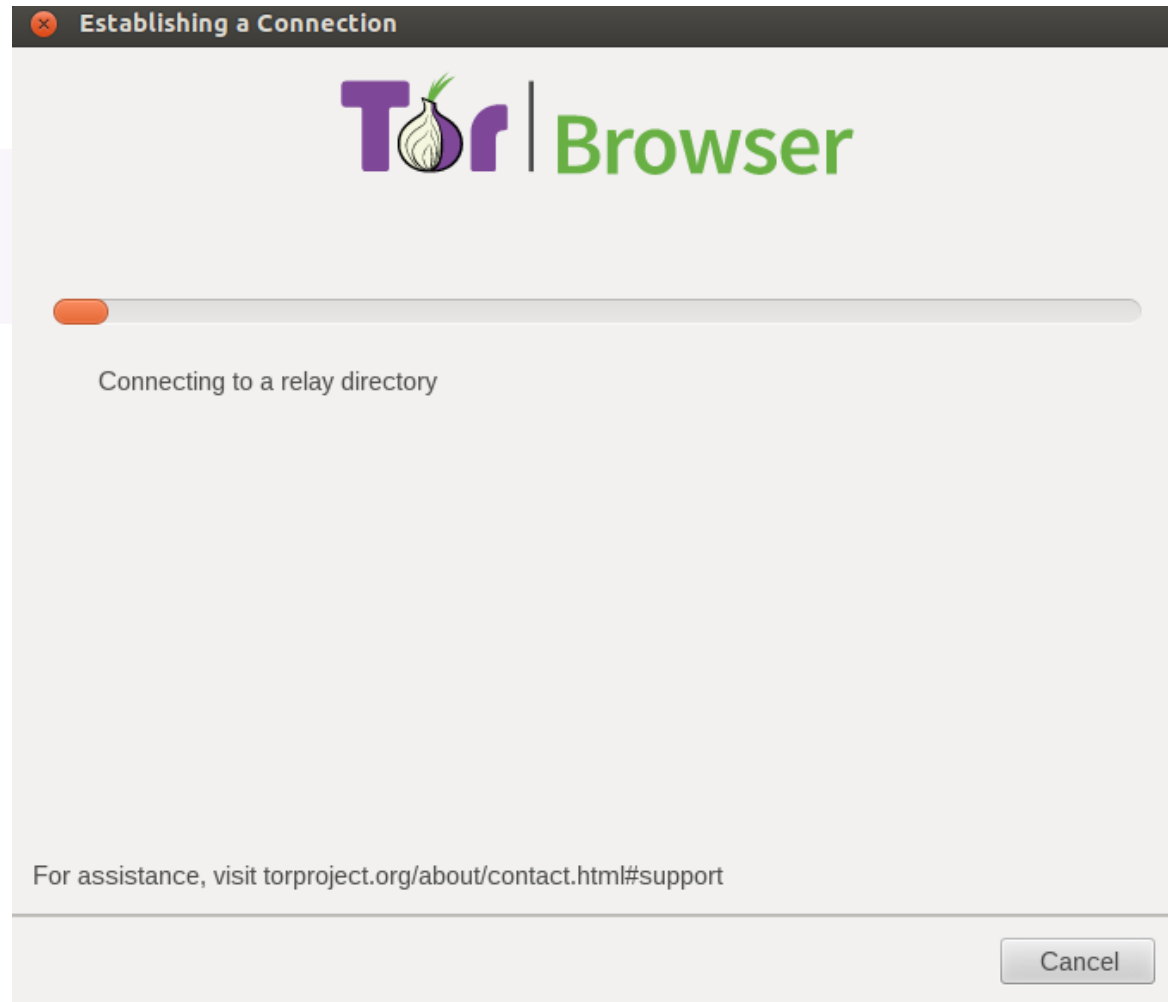
UNIVERSIDAD  
DE GRANADA

# DEMOSTRACION CON WIRESHARK

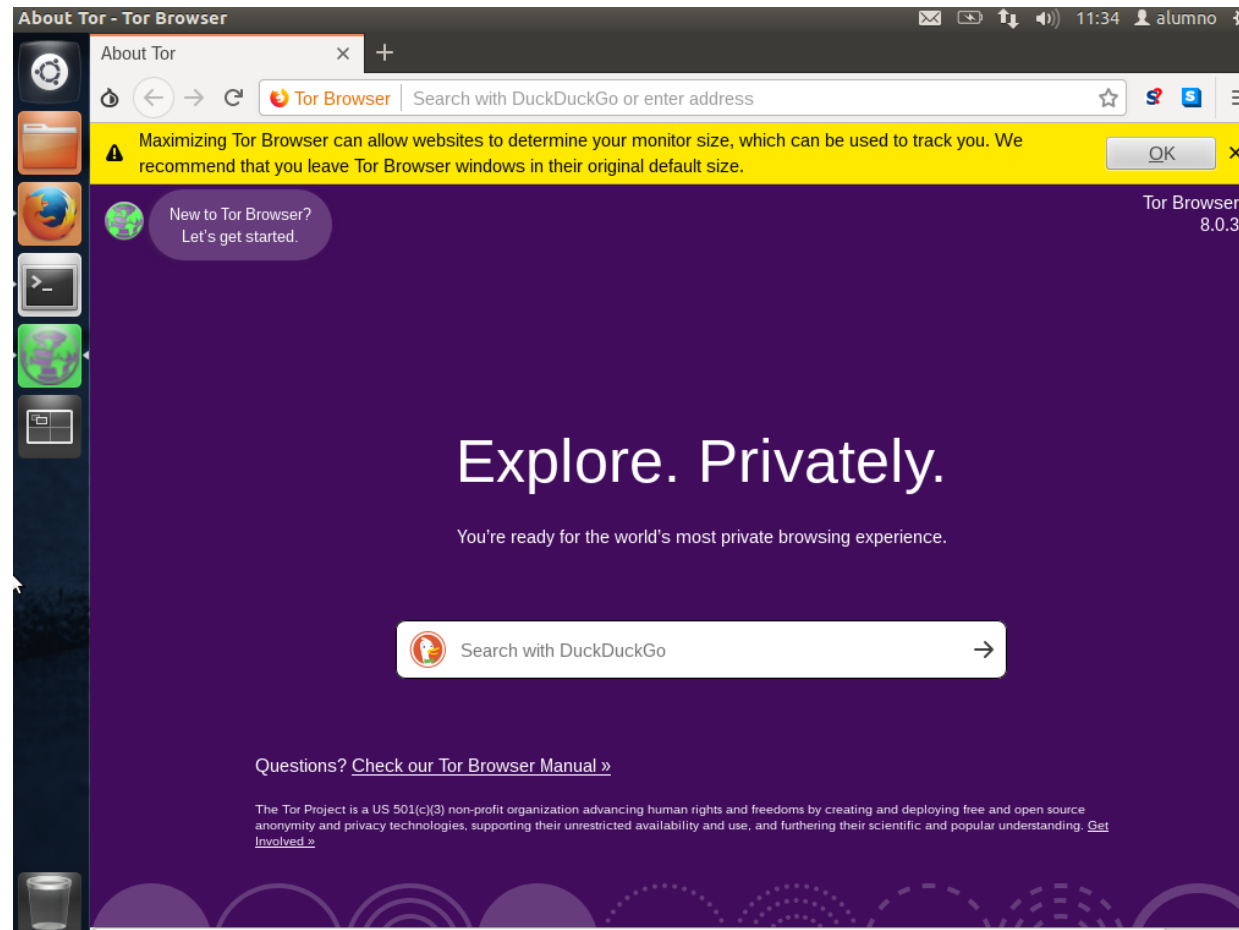
---

Internet Profunda – Red Tor

# Demostración



# Demostración



# Demostración

eth1 [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	128.31.0.39	TCP	74	35453 > bacula-dir [SYN] Seq=0 Win=14600
2	0.762028	212.129.57.254	10.0.2.15	TLSv1.2	597	Application Data
3	0.762043	10.0.2.15	212.129.57.254	TCP	54	39876 > etlservicemgr [ACK] Seq=1 Ack=54
4	4.254906	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
5	4.255186	212.129.57.254	10.0.2.15	TCP	60	etlservicemgr > 39876 [ACK] Seq=544 Ack=
6	4.633642	212.129.57.254	10.0.2.15	TLSv1.2	597	Application Data
7	4.633655	10.0.2.15	212.129.57.254	TCP	54	39876 > etlservicemgr [ACK] Seq=544 Ack=
8	4.636056	10.0.2.15	212.129.57.254	TLSv1.2	1111	Application Data
9	4.636286	212.129.57.254	10.0.2.15	TCP	60	etlservicemgr > 39876 [ACK] Seq=1087 Ack=
10	4.937740	212.129.57.254	10.0.2.15	TCP	1474	[TCP segment of a reassembled PDU]
11	4.937763	212.129.57.254	10.0.2.15	TCP	1474	[TCP segment of a reassembled PDU]
12	4.937770	10.0.2.15	212.129.57.254	TCP	54	39876 > etlservicemgr [ACK] Seq=1601 Ack=
13	4.937803	212.129.57.254	10.0.2.15	TLSv1.2	841	Application Data
14	4.941756	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
15	4.941963	212.129.57.254	10.0.2.15	TCP	60	etlservicemgr > 39876 [ACK] Seq=4714 Ack=
16	4.952011	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
17	4.952460	212.129.57.254	10.0.2.15	TCP	60	etlservicemgr > 39876 [ACK] Seq=4714 Ack=
18	5.233253	212.129.57.254	10.0.2.15	TLSv1.2	597	Application Data
19	5.240606	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
20	5.240885	212.129.57.254	10.0.2.15	TCP	60	etlservicemgr > 39876 [ACK] Seq=5257 Ack=
21	5.273486	212.129.57.254	10.0.2.15	TLSv1.2	597	Application Data

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Ethernet II, Src: CadmusCo\_aa:4b:39 (08:00:27:aa:4b:39), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 128.31.0.39 (128.31.0.39)

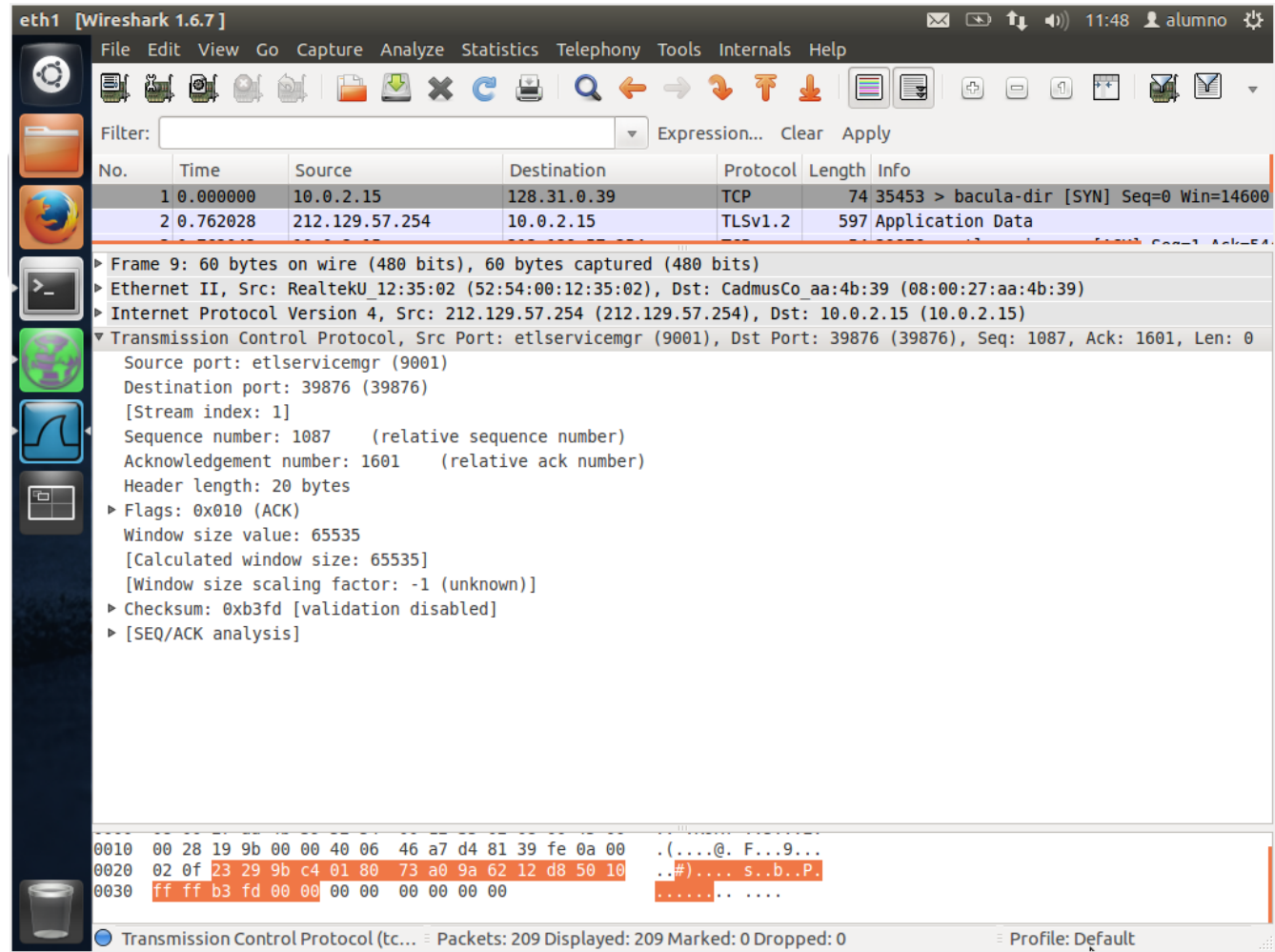
Transmission Control Protocol, Src Port: 35453 (35453), Dst Port: bacula-dir (9101), Seq: 0, Len: 0

0000 52 54 00 12 35 02 08 00 27 aa 4b 39 08 00 45 00 RT..5... '.K9..E.  
0010 00 3c 48 8a 40 00 40 06 65 dd 0a 00 02 0f 80 1f .<H.@. e.....  
0020 00 27 8a 7d 23 8d b1 c0 7d 43 00 00 00 00 a0 02 .'}.#... }C.....  
0030 39 08 8c 83 00 00 02 04 05 b4 04 02 08 0a 00 02 9.....  
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

File: "/tmp/wireshark\_eth1\_20181... Packets: 209 Displayed: 209 Marked: 0 Dropped: 0 Profile: Default



# Demostración





# Demostración

eth1 [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
2	0.762028	212.129.57.254	10.0.2.15	TLSv1.2	597	Application Data
4	4.254906	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
6	4.633642	212.129.57.254	10.0.2.15	TLSv1.2	597	Application Data
8	4.636056	10.0.2.15	212.129.57.254	TLSv1.2	1111	Application Data
13	4.937803	212.129.57.254	10.0.2.15	TLSv1.2	841	Application Data
14	4.941756	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
16	4.952011	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
18	5.233253	212.129.57.254	10.0.2.15	TLSv1.2	597	Application Data
19	5.240606	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
21	5.273486	212.129.57.254	10.0.2.15	TLSv1.2	597	Application Data
22	5.274353	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
24	5.322075	212.129.57.254	10.0.2.15	TLSv1.2	597	Application Data
25	5.322957	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
27	5.354905	212.129.57.254	10.0.2.15	TLSv1.2	597	Application Data
28	5.356937	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
30	5.411922	212.129.57.254	10.0.2.15	TLSv1.2	597	Application Data
32	5.576266	212.129.57.254	10.0.2.15	TLSv1.2	1111	Application Data
34	5.578176	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
36	5.998335	212.129.57.254	10.0.2.15	TLSv1.2	597	Application Data
42	6.041259	212.129.57.254	10.0.2.15	TLSv1.2	777	Application Data
44	6.113301	212.129.57.254	10.0.2.15	TLSv1.2	1474	Application Data
48	6.145347	212.129.57.254	10.0.2.15	TLSv1.2	687	Application Data
50	6.461488	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data

▼ Frame 50: 597 bytes on wire (4776 bits), 597 bytes captured (4776 bits)  
Arrival Time: Nov 21, 2018 11:44:00.703514000 CET

0000 52 54 00 12 35 02 08 00 27 aa 4b 39 08 00 45 00 RT..5...'.K9..E.  
0010 02 47 42 cf 40 00 40 06 db 53 0a 00 02 0f d4 81 .GB.@.@.S.....  
0020 39 fe 9b c4 23 29 9a 62 21 b1 01 80 ad 17 50 18 9...#).b!.....P.  
0030 ff ff 1c c8 00 00 17 03 03 02 1a 54 41 c2 10 88 .....TA...

File: "/tmp/wireshark\_eth1\_20181... Packets: 209 Displayed: 209 Marked: 0 Dropped: 0 Profile: Default



# Demostración

eth1 [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	212.129.57.254	10.0.2.15	TLSv1.2	597	Application Data
2	0.000015	10.0.2.15	212.129.57.254	TCP	54	39876 > etlservicemgr [ACK] Seq=1 Ack=54
3	1.146077	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
4	1.146867	212.129.57.254	10.0.2.15	TCP	60	etlservicemgr > 39876 [ACK] Seq=544 Ack=
5	2.281048	212.129.57.254	10.0.2.15	TLSv1.2	597	Application Data
6	2.281064	10.0.2.15	212.129.57.254	TCP	54	39876 > etlservicemgr [ACK] Seq=544 Ack=
7	2.281423	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
8	2.281733	212.129.57.254	10.0.2.15	TCP	60	etlservicemgr > 39876 [ACK] Seq=1087 Ack=
9	2.592664	212.129.57.254	10.0.2.15	TCP	1474	[TCP segment of a reassembled PDU]
10	2.592674	212.129.57.254	10.0.2.15	TLSv1.2	205	Application Data
11	2.592680	10.0.2.15	212.129.57.254	TCP	54	39876 > etlservicemgr [ACK] Seq=1087 Ack=
12	2.668666	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
13	2.668905	212.129.57.254	10.0.2.15	TCP	60	etlservicemgr > 39876 [ACK] Seq=2658 Ack=
14	2.679265	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
15	2.679612	212.129.57.254	10.0.2.15	TCP	60	etlservicemgr > 39876 [ACK] Seq=2658 Ack=
16	2.690477	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data
17	2.690769	212.129.57.254	10.0.2.15	TCP	60	etlservicemgr > 39876 [ACK] Seq=2658 Ack=
18	2.976439	212.129.57.254	10.0.2.15	TLSv1.2	597	Application Data
19	3.014222	10.0.2.15	212.129.57.254	TCP	54	39876 > etlservicemgr [ACK] Seq=2716 Ack=
20	3.134237	212.129.57.254	10.0.2.15	TLSv1.2	1111	Application Data
21	3.134251	10.0.2.15	212.129.57.254	TCP	54	39876 > etlservicemgr [ACK] Seq=2716 Ack=
22	3.136983	10.0.2.15	212.129.57.254	TLSv1.2	1111	Application Data
23	3.137210	212.129.57.254	10.0.2.15	TCP	60	etlservicemgr > 39876 [ACK] Seq=4258 Ack=

Frame 1: 597 bytes on wire (4776 bits), 597 bytes captured (4776 bits)

Ethernet II, Src: RealtekU 12:35:02 (52:54:00:12:35:02), Dst: CadmusCo aa:4b:39 (08:00:27:aa:4b:39)

0000 08 00 27 aa 4b 39 52 54 00 12 35 02 08 00 45 00 ...K9RT ..5...E.  
0010 02 47 1b a5 00 00 40 06 42 7e d4 81 39 fe 0a 00 ...G....@. B~.9...  
0020 02 0f 23 29 9b c4 01 83 cb 2f 9a 63 c0 b7 50 18 ...#).... ./..C..P.  
0030 ff ff c0 57 00 00 17 03 03 02 1a fb 44 e3 42 d4 ...W.... ..D.B.

File: "/tmp/wireshark\_eth1\_20181..." Packets: 29 Displayed: 29 Marked: 0 Dropped: 0

Click to change configuration profile



# Demostración

eth1 [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	212.129.57.254	10.0.2.15	TLSv1.2	597	Application Data
2	0.000015	10.0.2.15	212.129.57.254	TCP	54	39876 > etlservicemgr [ACK] Seq=1 Ack=54
3	1.146077	10.0.2.15	212.129.57.254	TLSv1.2	597	Application Data

► Frame 1: 597 bytes on wire (4776 bits), 597 bytes captured (4776 bits)

► Ethernet II, Src: RealtekU\_12:35:02 (52:54:00:12:35:02), Dst: CadmusCo\_aa:4b:39 (08:00:27:aa:4b:39)

► Internet Protocol Version 4, Src: 212.129.57.254 (212.129.57.254), Dst: 10.0.2.15 (10.0.2.15)

► Transmission Control Protocol, Src Port: etlservicemgr (9001), Dst Port: 39876 (39876), Seq: 1, Ack: 1, Len: 543

▼ Secure Sockets Layer

▼ TLSv1.2 Record Layer: Application Data Protocol: http

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 538

Encrypted Application Data: fb44e342d480ac3d6d2d17cdfc89be52720e2e3c522cf1d...

0020 02 0f 23 29 9b c4 01 83 cb 2f 9a 63 c0 b7 50 18 ..#)...../.C..P.

0030 ff ff c0 57 00 00 17 03 03 02 1a fb 44 e3 42 d4 ...W...D.B.

0040 80 ac 3d 6d 2d 17 cd ff c8 9b e5 27 20 e2 e3 c5 ..m-...'...

0050 22 cf 1d a2 ff 25 d0 c5 6b 8a 6d 7b 10 64 be a1 "...%. k.m{.d..

Transmission Control Protocol (tc... Packets: 29 Displayed: 29 Marked: 0 Dropped: 0

Click to change configuration profile



# Demostración

The screenshot displays the Tor Browser window. The address bar shows a secure connection to `yjuwkcxlgo7f7o6s.onion`. A pop-up window titled "Tor Circuit" is visible, showing the path of the connection: This browser → France (212.129.57.254, Guard) → Poland (193.111.26.37) → Netherlands (185.62.188.252) → Relay → Relay → yjuwkcxlgo7f7o6s.onion. Below the circuit diagram is a blue button labeled "New Circuit for this Site" and a note: "Your Guard node may not change. [Learn more](#)".

Another pop-up window titled "Permissions" is also visible, stating: "You have not granted this site any special permissions." The background shows the "Index of /" page for the .onion site, listing files like `amnesia.boum.onion`, `arm/`, `monthly-report-`, `tor-package-arc`, and `README.txt`.

The status bar at the bottom indicates "Transmission Control Protocol (tc...)" and "Packets: 817 Displayed: 817 Marked: 0". The profile is set to "Default".

