

Deep Web

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus



Deep Web

<https://doi.org/10.5281/zenodo.4302267>

<https://github.com/mikel-egana-aranguren/EHU-SGSSI-01>



Zer da Deep Web?

Ohiko sare ezaguna (Clearnet):

- Helbide ezagunek osatzen dute (adibidez: www.ehu.eus)
- HTML edukia indexatuta daude eta bilaketak egiteko aukera ematen dute, interesatzen zaiguna aurkitzeko

Zer da Deep Web?

Internet bidez zuzenean eskuratu ezin diren eduki guztiek osatzen dute Deep Web (Internet sakona)

Uste da existitzen den eduki guztitik:

- %10 Clearnet-en dago (ezagutzen dugun internet)
- 90% Deep Web-en

Zer da Deep Web?

Deep Web-ko edukia:

- Informazio konfidentziala edo babestua (bilatzaileek ez dute indexatzen, eta ezin da zuzenean eskuratu):
 - Osasun-erregistroak
 - Erregistro akademikoak
 - Bankuko datuak
 - ...

Zer da Deep Web?

Deep Web-ko edukia:

- Informazio "soltea": estekatuta ez dagoen HTML artxiboa, adibidez
- HTML ez diren formatuetan nabigatzaile batek irakurri ezin duen informazioa
- Eduki argitaraezina (Zentsura): libreki argitaratu ezin diren edukiak, ekar ditzakeen ondorioengatik

Zer da Deep Web?

Deep Web-ko edukia:

- Legez kanpoko edukia eta/edo eduki desatsegina (Darknet)
 - Arma, droga eta pertsonen trafikoa
 - Material pedofiloa
 - Malwarea
 - Hacker, mertzenario eta abarren alokairua
 - Snuff pelikulak

Zer da Deep Web?

Web mailak

- 1 maila: Webgune oso ezagunak eta publiko guztientzakoak
- 2 maila: Webgune ezezagunak eta gune pornografikoak
- 3 maila (Hemen Deep Web hasten da): Pribatutasuna eta anonimotasuna behar ditu (eduki sentsibleak)
- 4 maila: Proxy bat behar du. Maila arriskutsua (legez kanpoko edukiak)
- 5 maila: Gobernuaren eta militarren sekretuak
- ???

Sarbideak

Deep Web-era sartzeko, software berezi bat behar da, pribatutasuna, anonimotasuna eta proxy lana egingo dituen

Deep Webeko hainbat edukitarako sarbidea emango duten aukera desberdinak daude: TOR, I2P, Freenet, Zeronet

TOR

The Onion Router (TOR)

Nabigazio-sare anonimoa

Sarean nabigatzen duten paketeen jatorria eta helmuga ezkutatzen ditu
(nahiz eta jatorria identifikatzeko moduak egon)

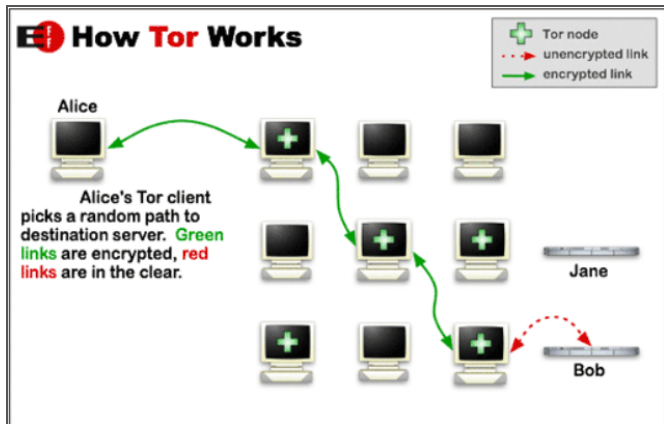
TOR

TOR sisteman sartzeko software espezifiko bat behar da:

- TOR Browser: web nabigatzailea
- Tails (The Amnesic Incognito Live System): USB baten exekutatzen den sistema eragilea

TOR

Konexio bat egin behar den bakoitzean, bide aleatorio bat kalkulatzen da nodoen artean



TOR

Informazioa geruzatan zifratzen da (tipula bat bezala) nodoen gako publikoekin; horrela, nodo bakoitzak hurrengo nodoa soilik zein den daki, ez bide osoa

TOR

TOR sarea erabiliz, beste era batera eskuraezinak izango ziren URL-tara jo daiteke:

- .onion domeinua
- URL alfanumerikoak: <http://3g2upl4pq6kufc4m.onion/>

TOR

Edukiak aurkitzeko, bilatzaile espezifikoak edo URLak biltzeko guneak erabili behar dira:

- Torch bilatzailea (<http://xmh57jrznw6insl.onion/>)
- The Hidden Wiki (<http://kpvz7ki2v5agwt35.onion>)

I2P (Invisible Internet Project)

Modu anonimoan nabigatzeko beste sare bat da

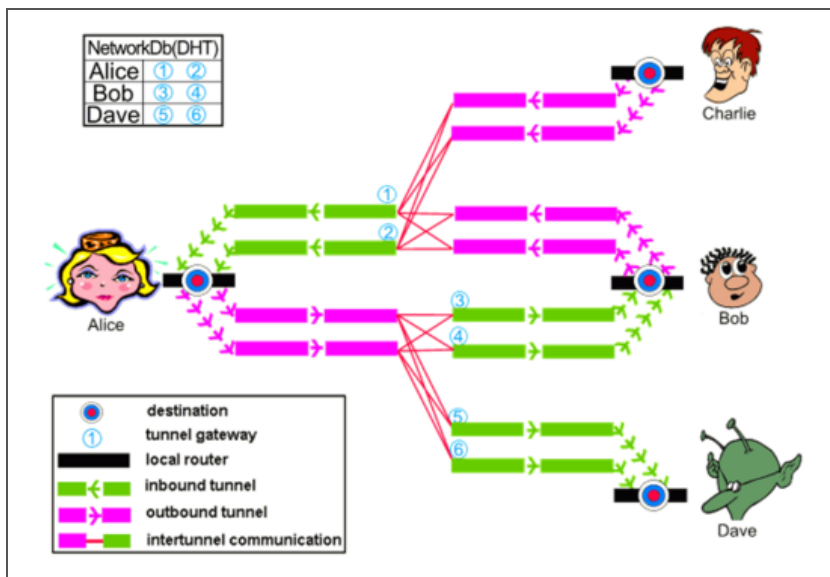
Erabiltzeko, zure routerra instalatu behar duzu

(<https://geti2p.net/es/download>)

Nodoen artean hedatutako Datu-base erabiltzen du

I2P (Invisible Internet Project)

Banatutako datu-basean oinarrituta erabakitzen da bidea

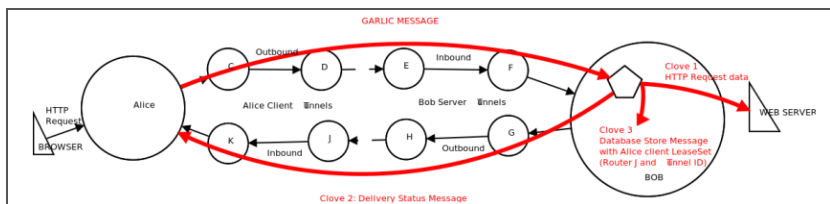


I2P (Invisible Internet Project)

Garlic bideratzeko protokoloa erabiltzen du

Informazioa geruzaka zifratzen da, jarraitu beharreko bidea adieraziz

Hainbat mezu taldeka daitezke (baratxuri baten hortzak, adibidez) elkarrekin zifratu eta deszifratzen direnak (baratxuri osoa)



I2P (Invisible Internet Project)

I2P sarea erabiliz, beste era batera eskuraezinak izango ziren URL-tara jo daiteke:

- .i2p domeinua
- URL alfanumerikoak baina “ulergarriak”: <http://lawiki.i2p>

I2P (Invisible Internet Project)

Tokiko izenen fitxategi bat erabiltzen da, addressbook izenekoa.

Helbide berriak sar daitezke, helbide repositorioetara sartu, etab.

Bilatzailea: <http://eepsites.i2p>

URLen biltegia: I2P Name Registry (<http://inr.i2p>)

Freenet

Informazioa biltegitratzeko sare banatua da, anonimotasuna ematen du
P2P sare egituratu gabea da. Nodoek ez dute hierarkiarik:

- Bilatzen den edukia izan dezakete
- Beste nodo batera bidal dezakete aurkitzeko

Freenet

Erabiltzeko software berezi bat deskargatu behar da

([https://freenetproject.org /](https://freenetproject.org/))

Partekatu nahi den banda-zabalera konfiguratu behar da

Freenet

Zein nodotara konektatu hauta daiteke:

- Denak / lagunak
- Zein nodori konektatzen garen arabera eskuragarri eduki gehiago edo gutxiago edukiko dugu

Freenet

Freeneten eduki bat argitaratzean, nodoen bidez hedatzen da

Edukiak biltzeko guneak daude:

- Enzo's index (kategoriatan antolatua)
- The Filtered Index (ez du eduki sentziblerik)

Zeronet

Anonimotasunik gabeko sare banatua da (Tor erabiltzea gomendatzen da anonimotasuna lortzeko)

P2P sare egituratu gabea da. Nodoek ez dute hierarkiarik:

- Bilatzen den edukia izan dezakete
- Beste nodo batera bidal dezakete aurkitzeko

Erabiltzeko software berezi bat deskargatu behar da (<https://zeronet.io/>)

Zeronet

URL-ak bitcoin helbideak dira:

- .bit domeinua
- "zite" deiturikoak

Nabigatzeko aholkuak

Ez erabili Windows

Makina birtualak edo live USB erabili

100% seguruak diren gauzak bakarrik deskargatu

Ez igo dokumentuak (Kontuz metadatuekin)

Ohiko zerbitzuetara ez konektatu (sare sozialak, posta,...)

Ez egin ezer ez ilegala