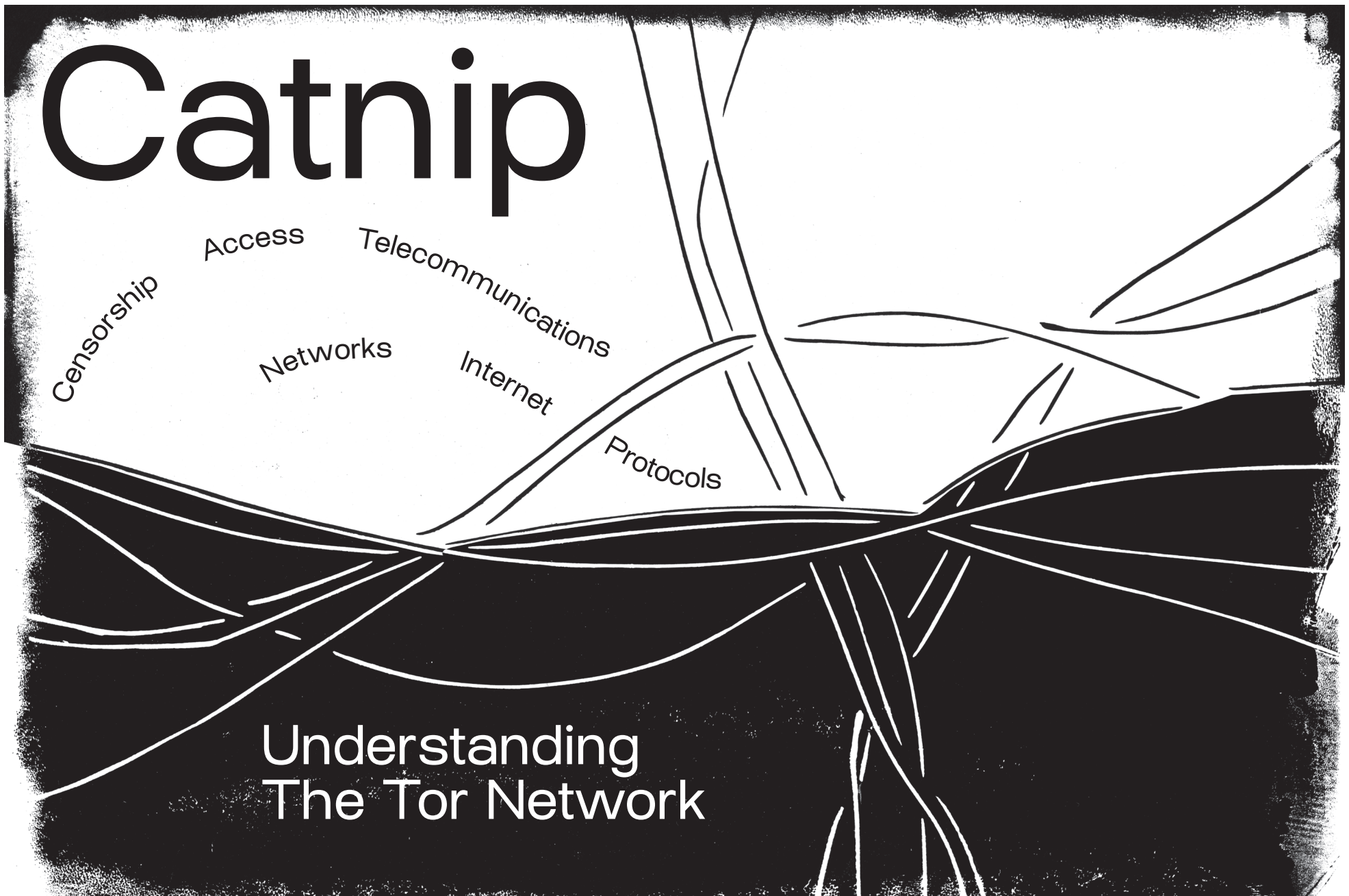
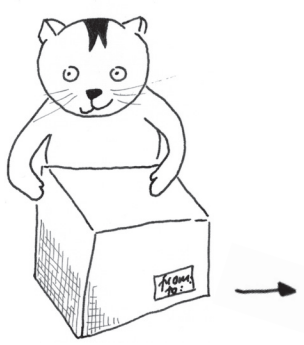
Catnip

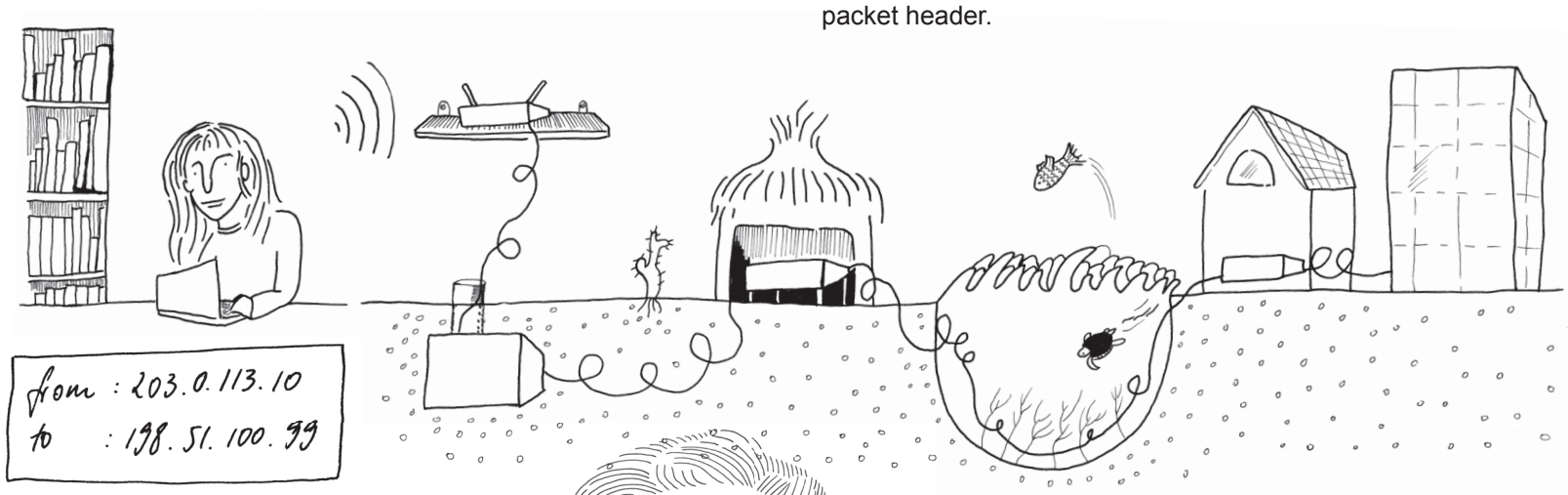


Understanding The Tor Network

Data travels in packets. And each packet has a tag, or packet header, indicating its source and destination address.



There are no direct connections on the Internet, packets travel through intermediary networks and routers, all of which read the packet tag in order to route the packets to their destination.



All of them know where they received the packet from and the source and destination information contained in the packet header.

All of these intermediaries can copy, store or even alter packets.

This is a problem when states, institutions, employers, parents, network or server operators want to stop us accessing certain content on the Internet through filtering, blocking or throttling Internet traffic.

Attempts to censor content can happen at any stage: at the source, at intermediate routers, or at the destination. These interventions are made by parties operating the routers, the servers or the network equipment that data packets travel through.

To circumvent blocking and filtering, the Tor network (The Onion Router) can be used to anonymize Internet traffic by hiding source and destination addresses.

Tor is a global network of computers running Tor software. As of 2018, there are around 6200 “Tor nodes” - machines that make up the Tor network.

The

Any computer can run the Tor software and become a node.

Think of the Tor software on a node like a cellar where data packets intended to travel over the Tor network are treated.

A Tor circuit

Using Tor, data packets are sent over the Internet's infrastructure like any other packet.

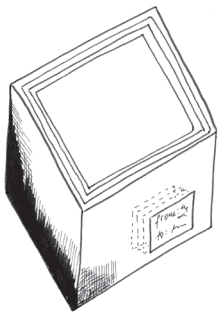
But packets traveling through the Tor network are routed randomly through three nodes (also called relays or hops) before reaching their final destination.

This route, called Tor circuit, is changed every ten minutes to make it harder to observe for potential eavesdroppers.

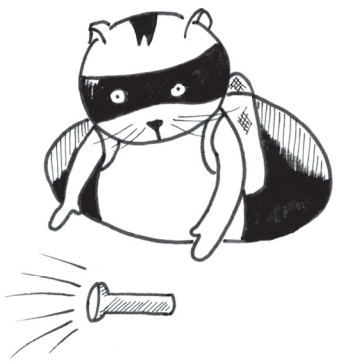
To route the packets down a random path, they are packed like an onion: each is wrapped into three encrypted layers containing a dedicated packet tag.

But only a partial route is encoded on these tags, so that none of the relays know the entire path a packet takes.

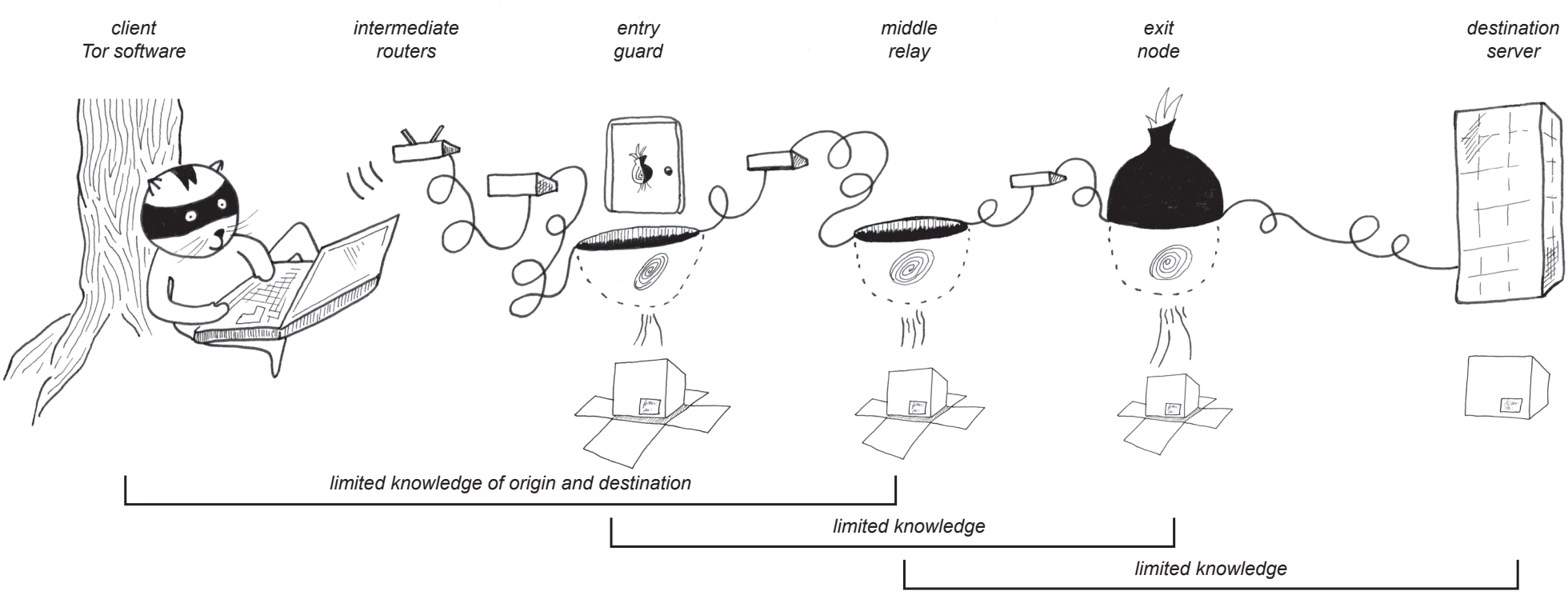
At each relay a single layer is peeled off and the packet is then sent to the next relay written on the tag of the underlying layer. This unwrapping and preparing to relay the packets is managed by the Tor software of the node. All that is visible from the outside is that obscure cargo is sent from place to place.



Because of this, the Tor network is often pejoratively called the "dark net".



When we say that Tor packet layers are encrypted, it means that only the relay with the correct private encryption key is able to unwrap the corresponding layer.

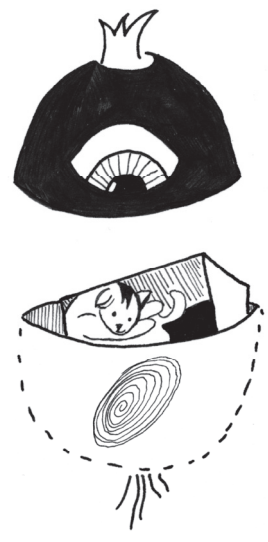


Tor network

Using Tor, the sender of packets remains anonymous because each intermediary only knows the location of the immediately preceding and following nodes.

Packets which are destined for a website or email server on the clearnet will leave the Tor network after the last hop. These packets appear to originate from the exit node, which is a special Tor node.

Currently there are about 860 exit nodes on the Tor network.

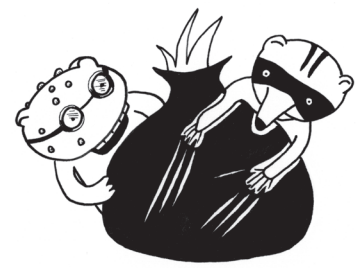


It is important to note that if the initial request that was made didn't use transport or end-to-end encryption, the package contents are visible to the exit node.

Limitations

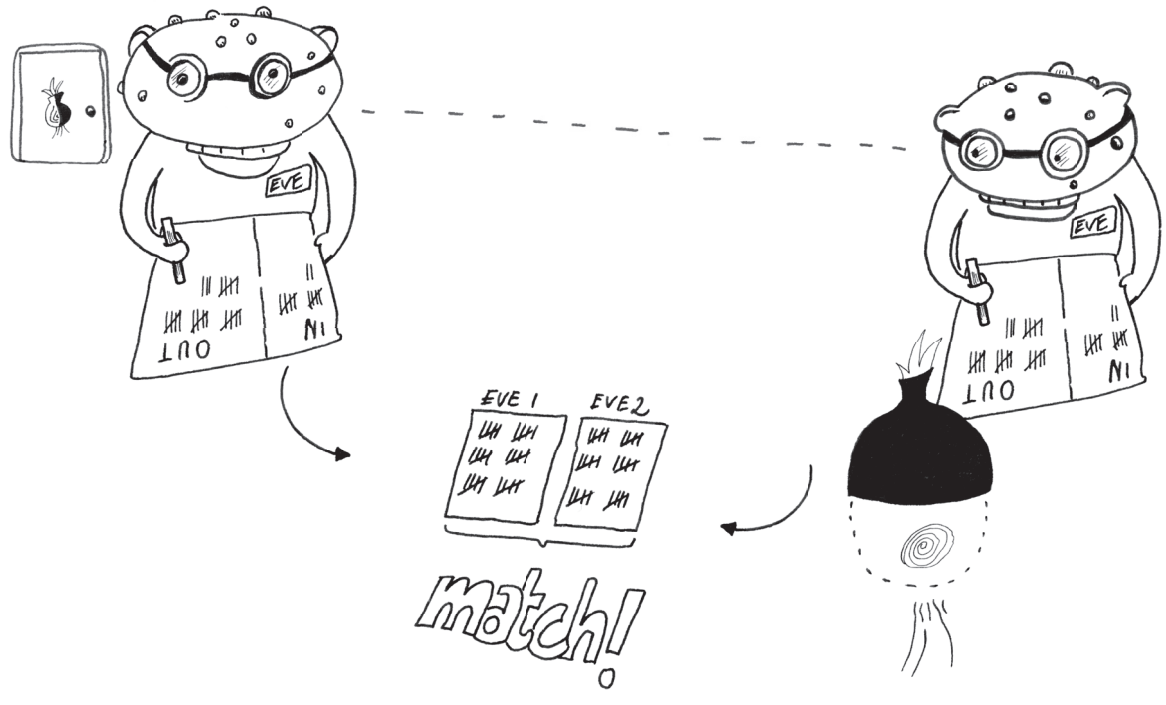
Because Tor is a privacy and anonymity enhancing tool, it's used for many different things, but it is important to have clear expectations about what Tor is unable to do or in which cases it does not protect your identity or your data.

First, remember that everybody running the Tor software on their server can become a node. This means that there might be eavesdroppers or other malicious entities running Tor nodes. If the same entity could control more than one relay for each Tor circuit, that entity could know everything about you and your traffic.



Just having access to an exit node can sometimes be enough for them to know who you are, if you login to a website without using encryption, for example. So, secondly, it's critical to always use encryption on top of using Tor.

Adversaries can even infer on the contents of encrypted packets by closely monitoring the size, timing, and quantity of ingoing and outgoing packets at both origin and destination, performing a targeted traffic analysis. Tor cannot protect from such attackers.



Blocking Tor

In some countries and on some networks known entrances to the Tor network are censored. In this case bridges have to be used as entry points. Bridges are Tor relays that aren't listed in the public main Tor directory. Using bridges, it becomes harder for ISPs and censors to block access to the Tor network. However, when bridge addresses become known to censors, they can equally get blocked.

The same is true for exit nodes. As their addresses are publicly known, it is easy to block packets that originate from an exit node from accessing a website or a server on the clearnet.

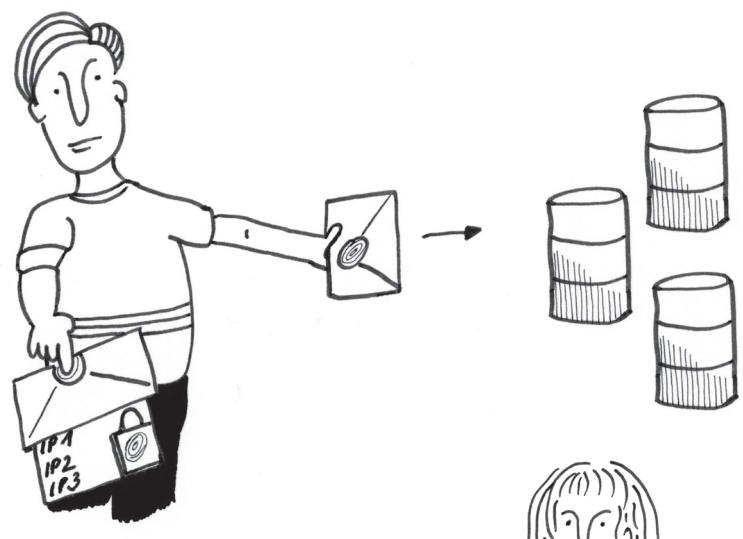
Onion services

Within the Tor network, services can be provided which keep traffic end-to-end encrypted and hidden within the network so that the server's location can be hidden in the same way that the client's location is hidden.

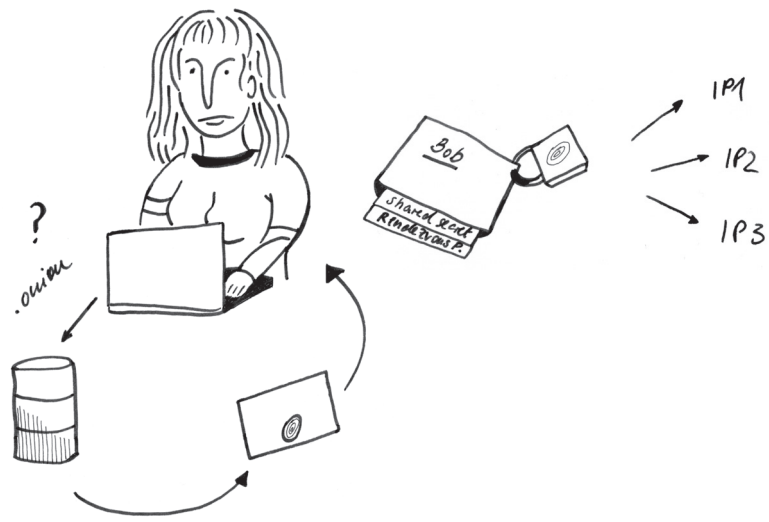
These services use the top level domain .onion.

When Bob proposes an onion service, webserver.onion, their Tor software randomly picks several relays, builds a 3-hop circuit to them, and asks them to act as introduction points.

Now Bob's Tor software prepares a descriptor message containing the names of the introduction points, as well as the public key belonging to his service. He signs this descriptor message and sends it to a distributed database within the Tor network.



Alice has read about webserver.onion and wants to visit it. Her Tor software sets up a rendezvous point within the network and then asks the database for a signed message from webserver.onion.



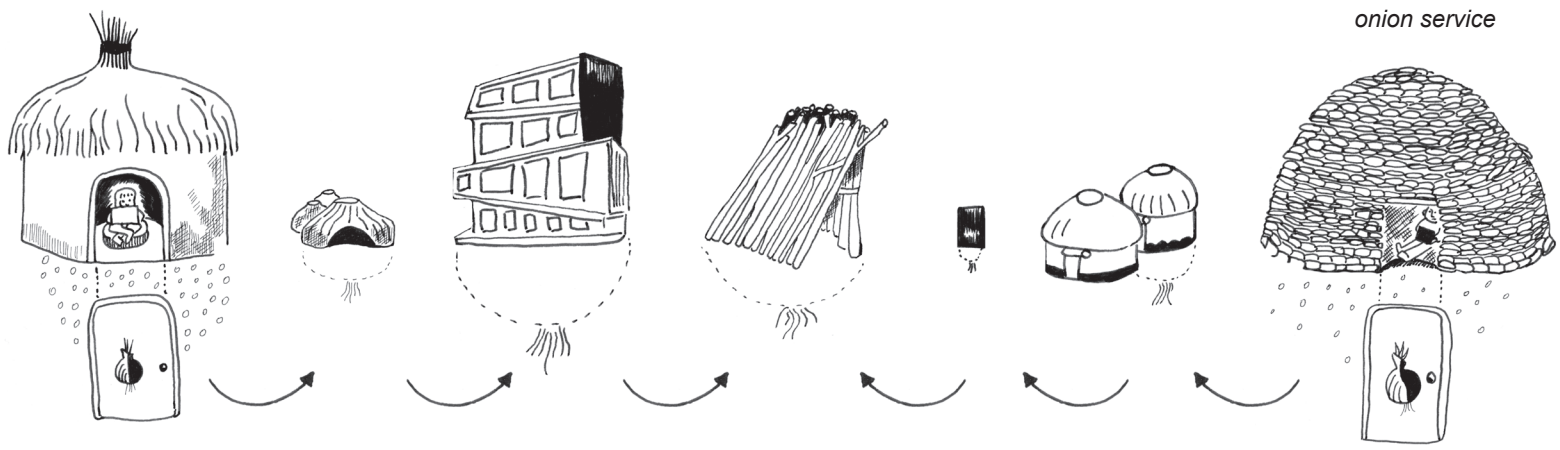
When she receives this message, her software can create an introduction message containing a one-time shared secret, encrypted to the public key of Bob's onion service, which she found in the descriptor message. She can send the introduction message to the mentioned introduction points, asking them to relay it to Bob.

Because Bob has established a Tor circuit to these points, they send the message to him through three relays, none of which know the entire path to Bob. Bob stays anonymous.

Bob's onion service decrypts Alice's introduction message and finds the address of the rendezvous point and the one-time secret in it.

Bob can now connect to the rendezvous point, and include Alice's one-time secret in his first rendezvous message. The rendezvous point will inform Alice's Tor client when this happens.

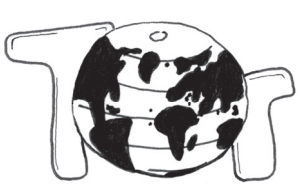
From now on, both Alice and Bob can communicate, each using their own three relay Tor circuit to the rendezvous point which relays their end-to-end encrypted messages.



Using the Tor network

Tor can be configured at the network level, manually, by modifying the way a device or router sends and receives all of its traffic.

Or, there are software applications that make using the Tor network easy:



TorBrowser to avoid tracking as you browse the web.

Torbirdy with Thunderbird to send and receive emails over Tor.

OnionShare to share files anonymously.

Orbot & Orfox or Onion Browser to use Tor on the smartphone.

Tails, an out-of-the box operating system that makes all network traffic automatically go through the Tor network.

Because Tor currently uses TCP (Transmission Control Protocol) as its packet transport protocol, applications based on UDP (User Datagram Protocol) such as video calls or torrenting don't work over Tor.

Imprint

By ARTICLE 19, first published June 2018. Published under Creative Commons License CC-BY-SA 4.0.
Thank you to Ulrike Uhlig for contributions to research and illustrations and to Daniel Kahn Gillmor and Intrigeri for contributing technical expertise.

ARTICLE 19

Want more catnip?
https://catnip.article19.org