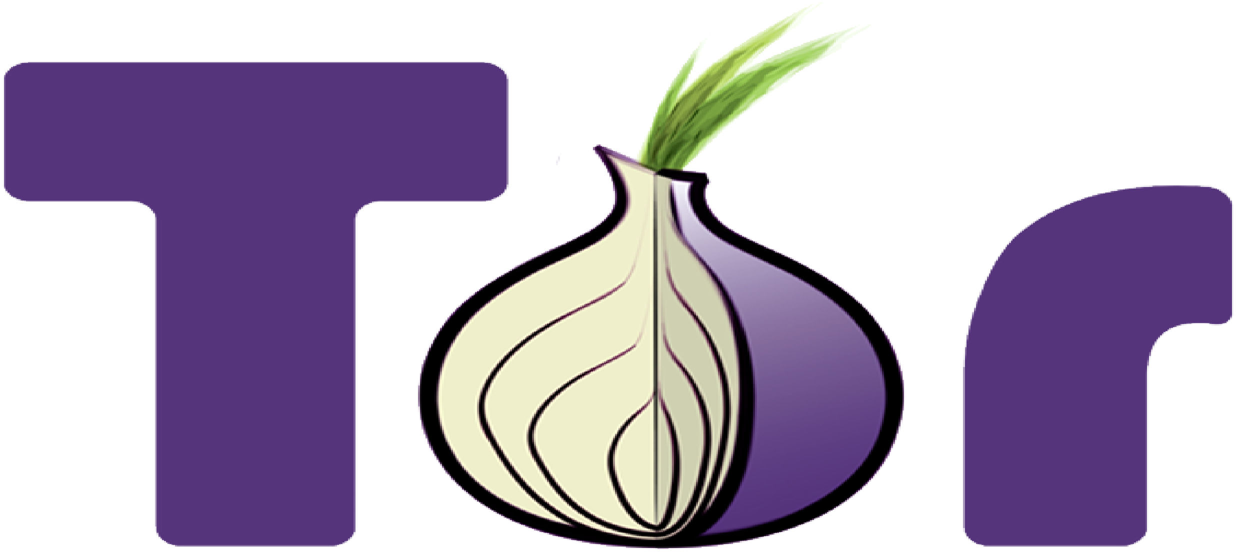
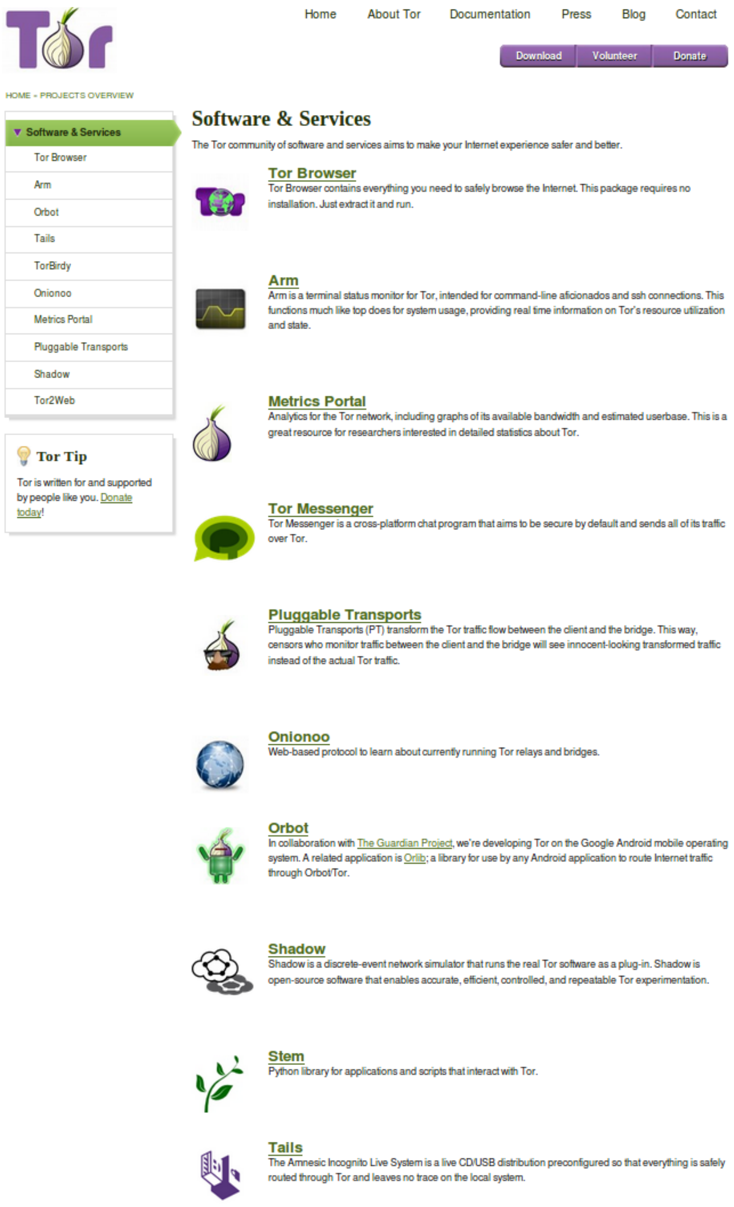


The Onion Router - Your privacy on-line

The TOR Project

The Tor Project was founded by computer scientists Roger Dingledine, Nick Mathewson and five others in December 2006. The Electronic Frontier Foundation (EFF) acted as The Tor Project's fiscal sponsor in its early years, and early financial supporters of The Tor Project included the U.S. International Broadcasting Bureau, Internews, Human Rights Watch, the University of Cambridge, Google, and Netherlands-based Stichting.net.

Not just a browser



Tor Tip

Tor is written for and supported by people like you. Donate today!

Software & Services

The Tor community of software and services aims to make your Internet experience safer and better.

Tor Browser

Tor Browser contains everything you need to safely browse the Internet. This package requires no installation. Just extract it and run.

Arm

Arm is a terminal status monitor for Tor, intended for command-line aficionados and ssh connections. This functions much like top does for system usage, providing real time information on Tor's resource utilization and state.

Metrics Portal

Analytics for the Tor network, including graphs of its available bandwidth and estimated userbase. This is a great resource for researchers interested in detailed statistics about Tor.

Tor Messenger

Tor Messenger is a cross-platform chat program that aims to be secure by default and sends all of its traffic over Tor.

Pluggable Transports

Pluggable Transports (PT) transform the Tor traffic flow between the client and the bridge. This way, censors who monitor traffic between the client and the bridge will see innocent-looking transformed traffic instead of the actual Tor traffic.

Onionoo

Web-based protocol to learn about currently running Tor relays and bridges.

Orbot

In collaboration with The Guardian Project, we're developing Tor on the Google Android mobile operating system. A related application is Orlib; a library for use by any Android application to route Internet traffic through Orbot/Tor.

Shadow

Shadow is a discrete-event network simulator that runs the real Tor software as a plug-in. Shadow is open-source software that enables accurate, efficient, controlled, and repeatable Tor experimentation.

Stem

Python library for applications and scripts that interact with Tor.

Tails

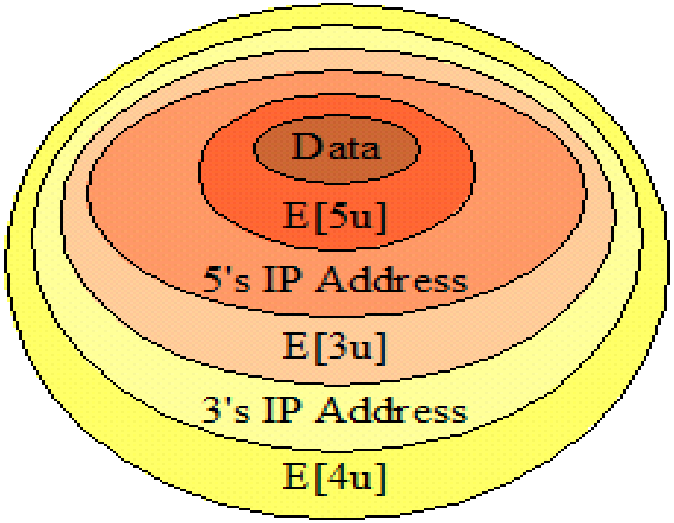
The Amnesic Incognito Live System is a live CD/USB distribution preconfigured so that everything is safely routed through Tor and leaves no trace on the local system.

What is Onion Routing?

Onion routing is an anonymous communication technique over a computer network. Messages are constantly encrypted and then sent through several network nodes called onion routers which creates a circuit of nodes.

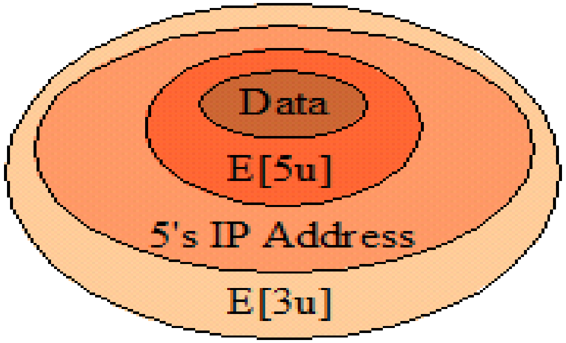
Each onion router removes a layer of encryption with its symmetric key to reveal routing instructions, and sends the message to the next router where this is process is repeated.

Thus the analogy “onion router”. This prevents these intermediary nodes from knowing the origin, destination, and contents of the message.



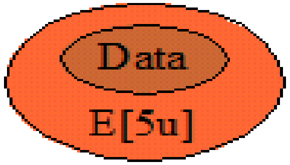
Onion Sent by Client to 4

Router 4 will decrypt the E[4u] layer using its private key, to find the next router's IP address, and encrypted data.



Onion Sent by 4 to 3

Router 3 will decrypt the E[3u] layer using its private key, to find the next router's IP address, and encrypted data.



Onion Sent by 3 to 5

Router 5 will decrypt the E[5u] layer using its private key, to find just the unencrypted data packet.

Data Sent by 5 to Target

What is Tor onion routing?

The Tor software is a program you can run on your computer that helps keep you safe on the Internet.

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world.

It prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

This set of volunteer relays is called the Tor network.

How is TOR different from other proxies?

A typical proxy provider sets up a server somewhere on the Internet and allows you to use it to relay your traffic. The users all enter and leave through the same server.

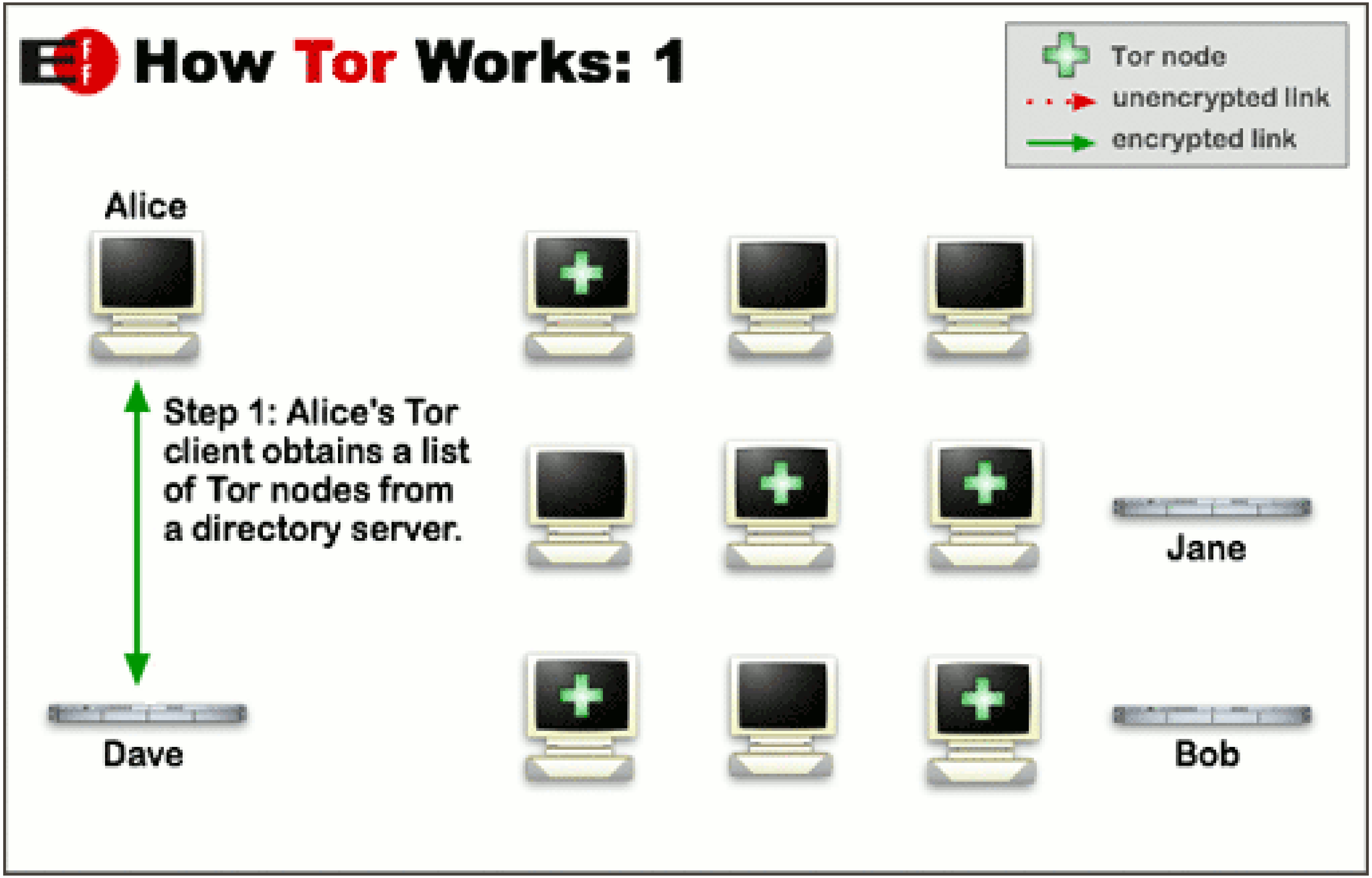
You just have to point your browser at their proxy server.

Simple proxy providers also create a single point of failure. The provider knows who you are and where you browse on the Internet. They can see your traffic as it passes through their server.

(Continued....)

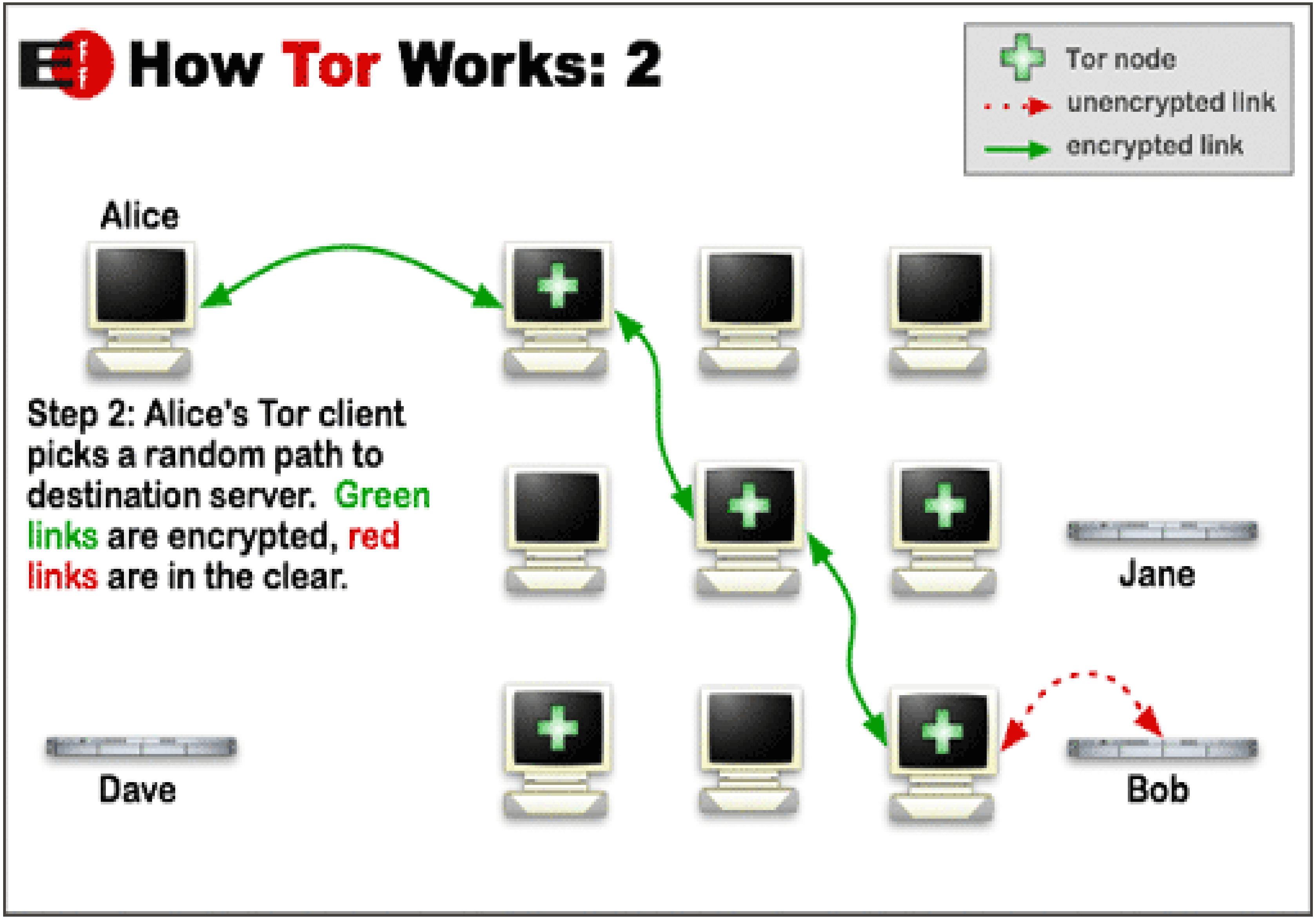
Tor passes your traffic through at least 3 different servers before sending it on to the destination. Because there's a separate layer of encryption for each of the three relays, Tor does not modify, or even know, what you are sending into it. It merely relays your traffic, completely encrypted through the Tor network and has it pop out somewhere else in the world, completely intact.

How Tor works?



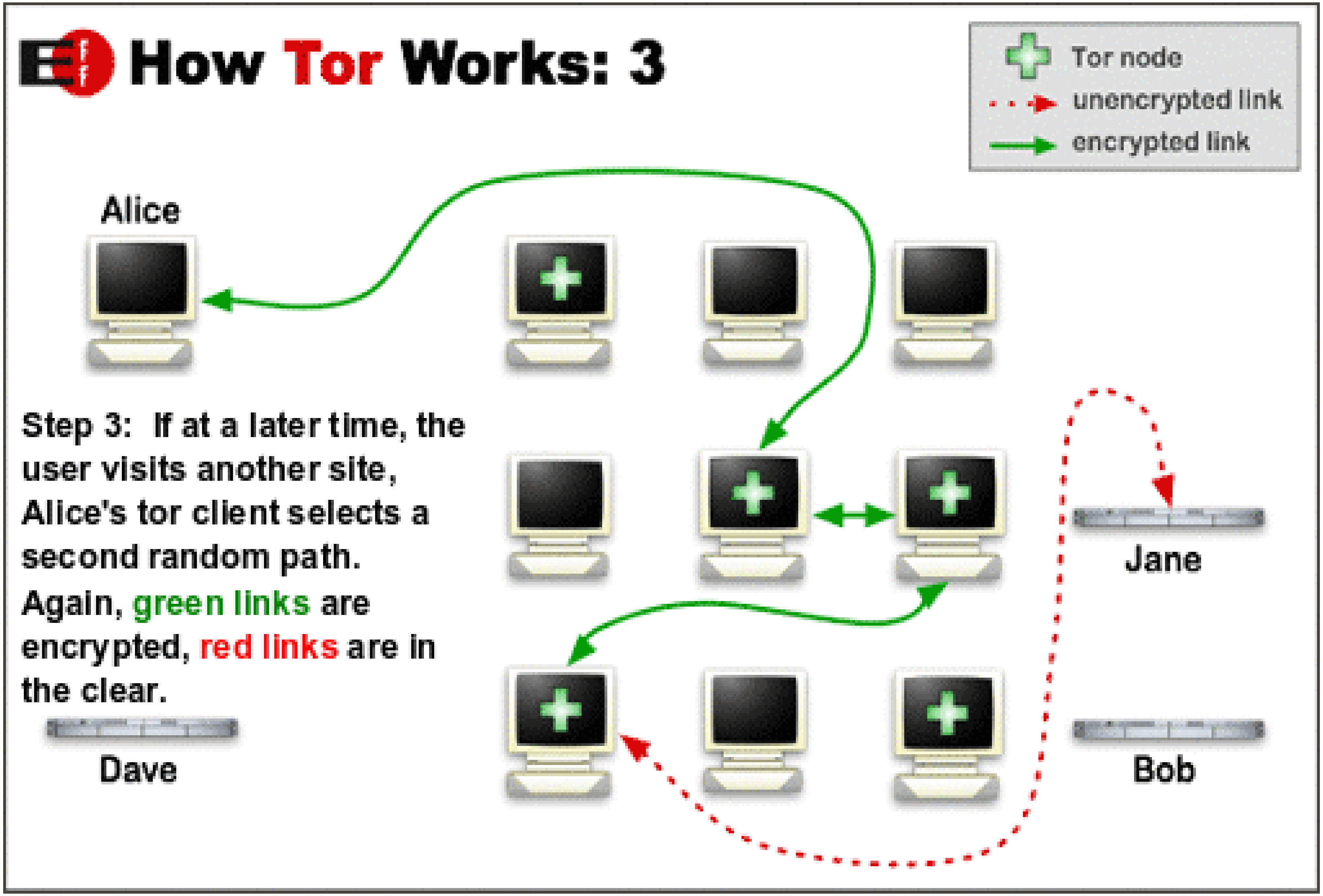
How Tor Works: 1

Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.



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.



How Tor Works: 3

Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

Advantages of Tor

Anonymity over the Internet.

Also it is the major tool to access the Deep Web, the sites which are not indexed by big search engines like Google,Yahoo,etc only because they are not allowed to. But you can access those using Tor.

It contains about 500 times more data than the surface web. We have access to only 0.03 % of data on the internet, which we call surface web. Deep web contains 7500TB of data as compared to 19TB of surface web.

Disadvantages of Tor

Tor is slow

Low latency anonymizers are prone to traffic analysis. In particular if somebody can observe your traffic and your target's traffic, he can correlate that.

Anonymous remailers avoid this problem by adding longer delays, but you can't use them for interactive applications, such as browsing the web.

Exit nodes see your traffic in plain

Tor .onion domains

Onion sites are so named because they end with “.onion” unlike normal sites which usually end with “.com” or “.net”

For eg: for accessing directory of .onion websites you have to visit **xoe9378fd000mysite.onion** by a tor enabled browser.