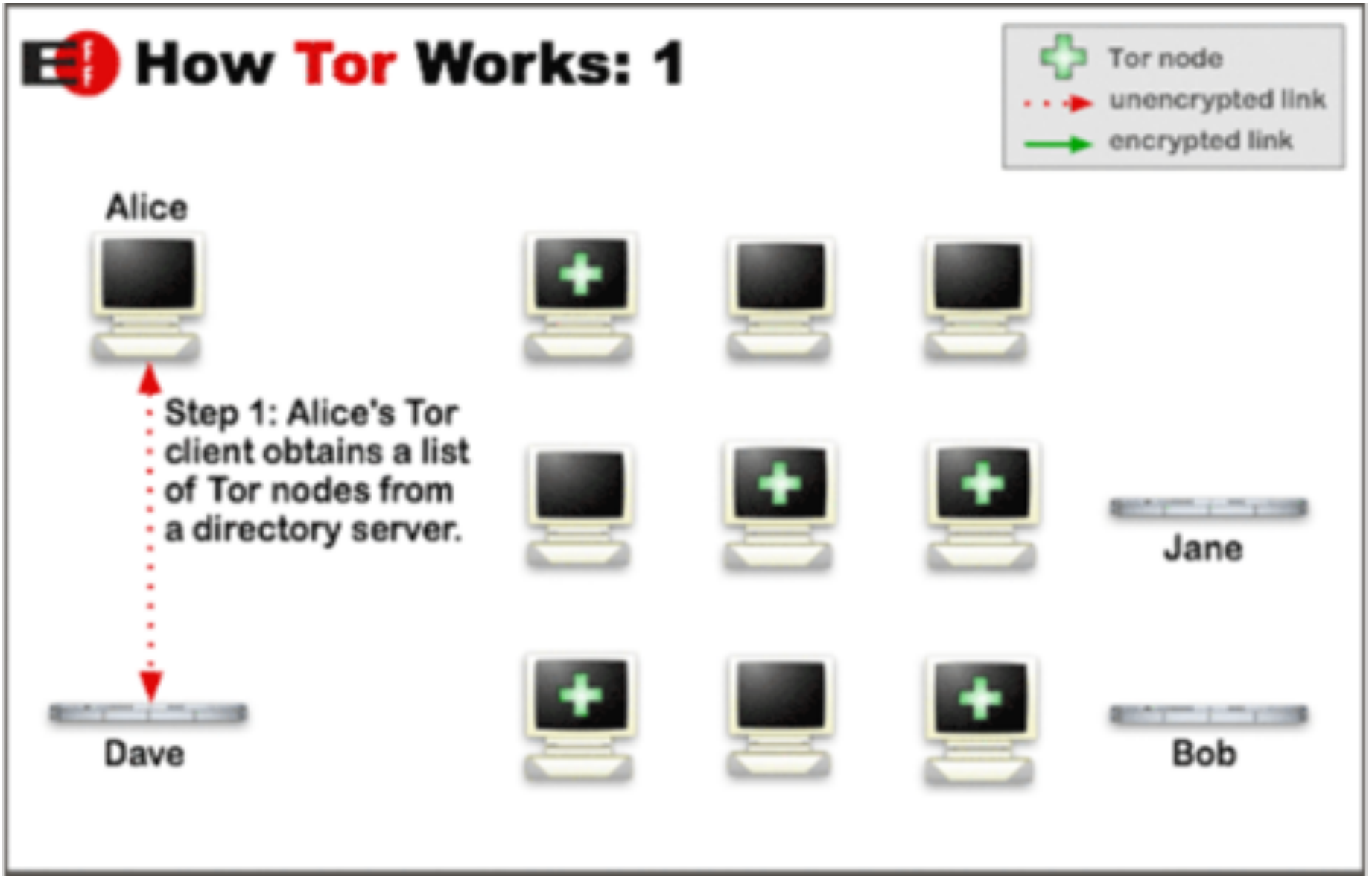
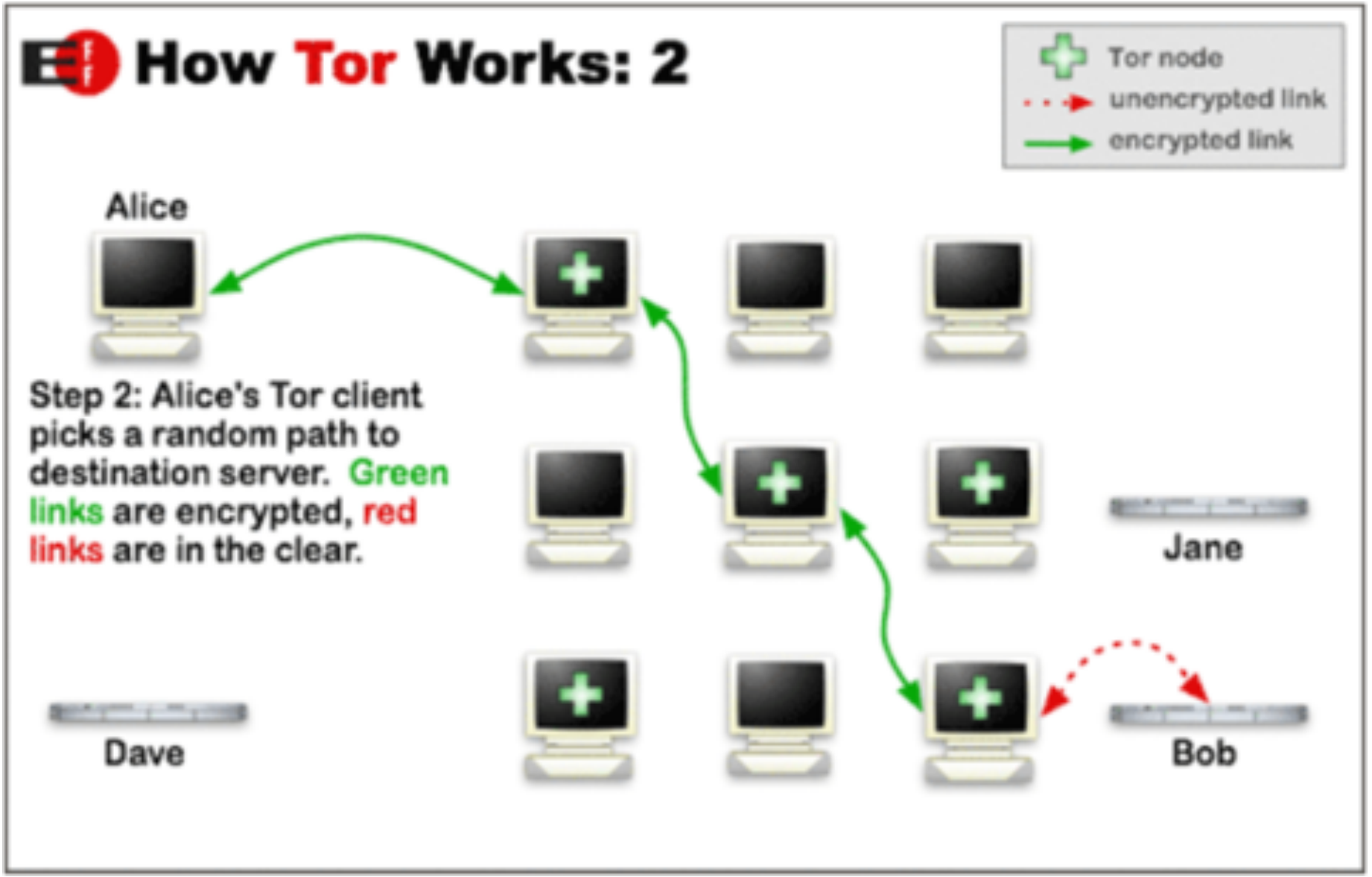
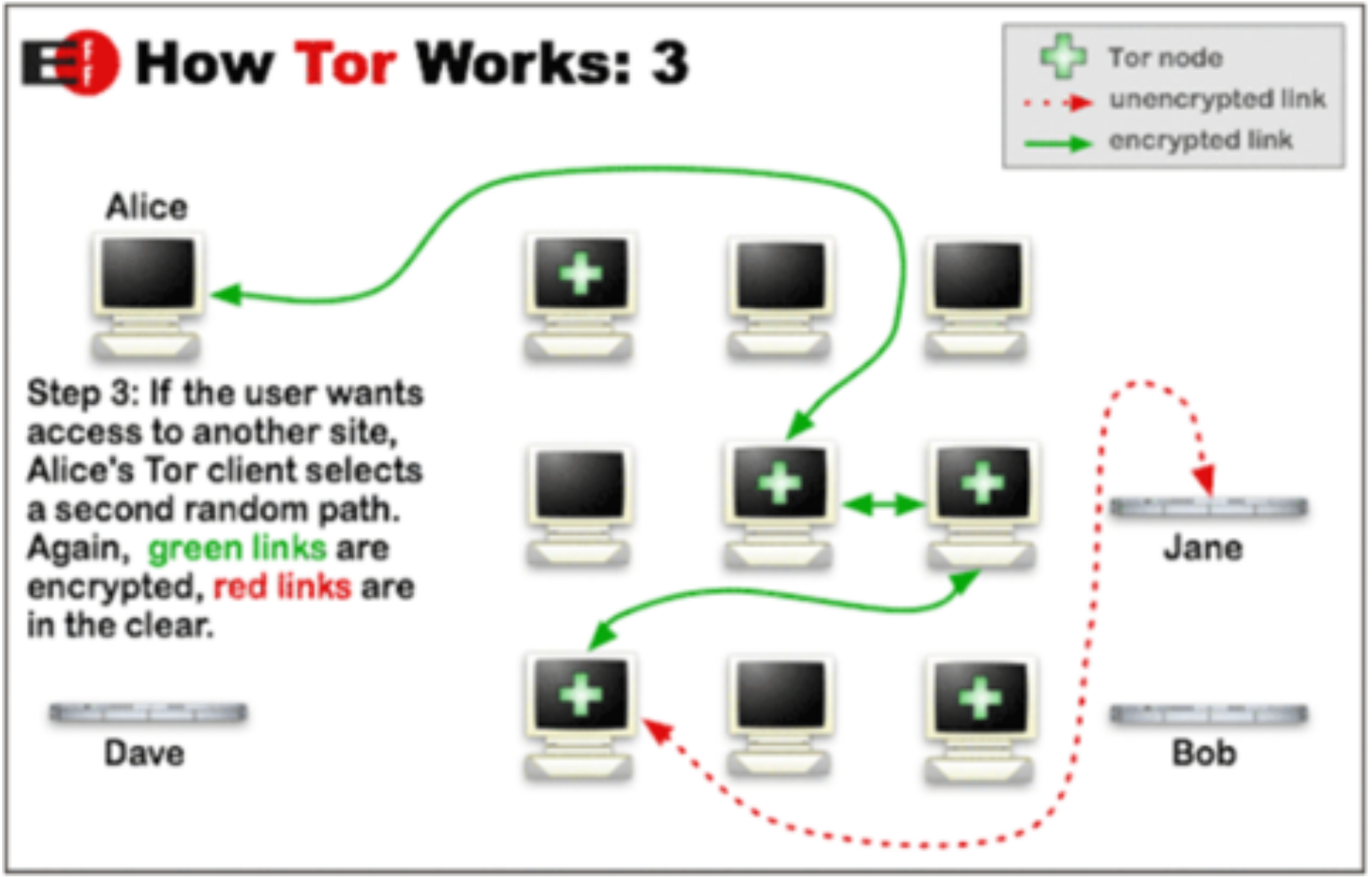

How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Dave
Jane
Bob



- Image courtesy torproject.org



- Image courtesy torproject.org

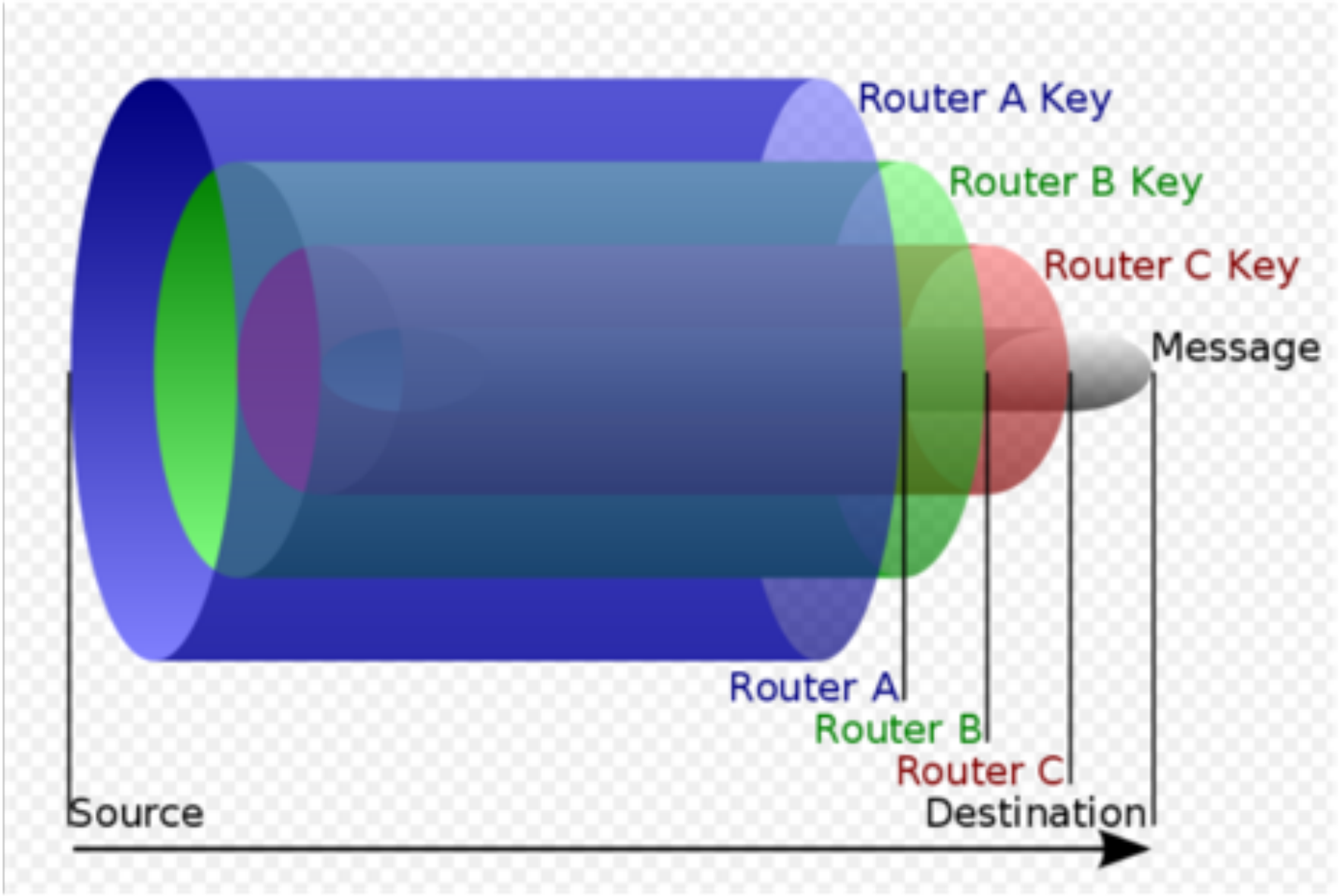


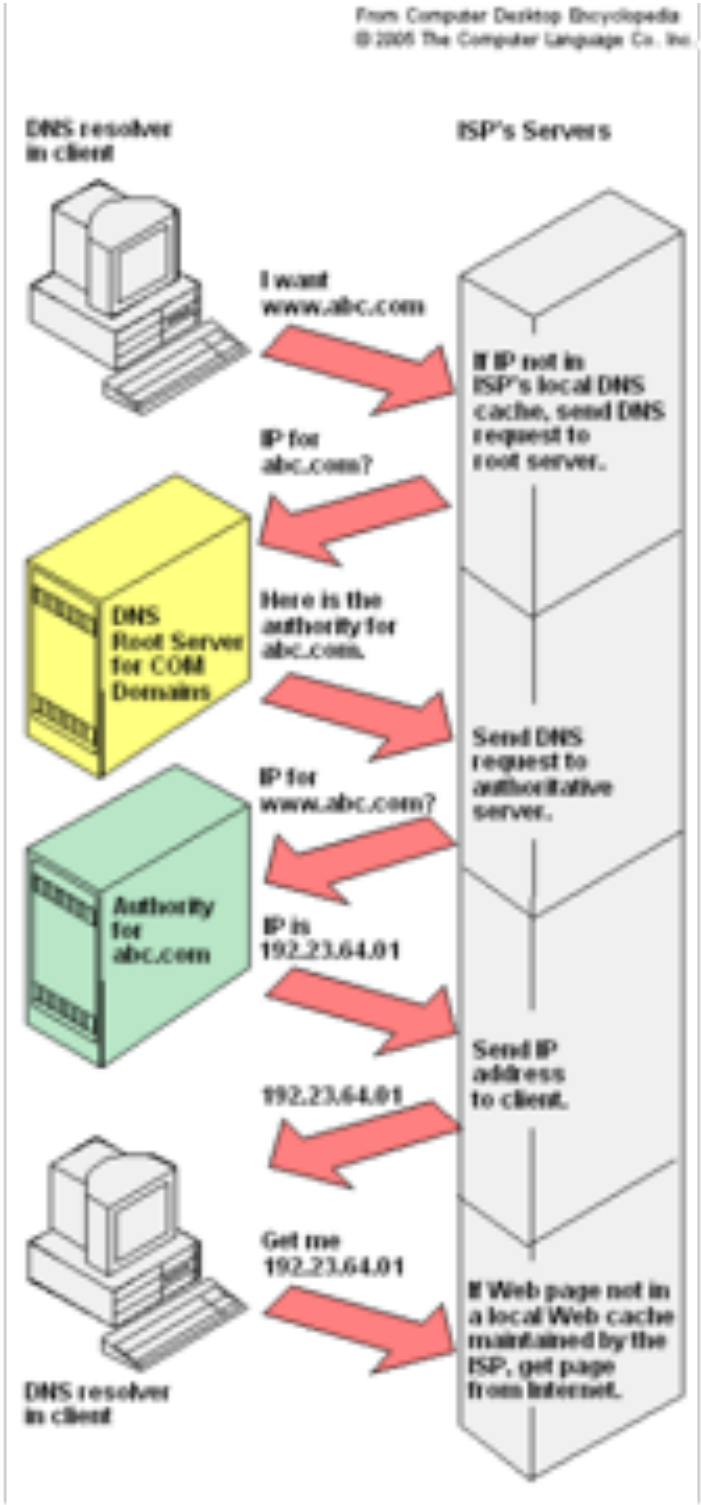
Photo courtesy Wikimedia Commons

The 3 Traditional Threats to Tor's Security:

- *DNS Leaks*
- *Traffic Analysis*
- *Malicious Exit Nodes*

Threat 1: DNS Leaks

- DNS requests not sent through Tor network by default
- Attacker could see what websites are being visited
- External software such as *Foxyproxy* and *Privoxy* can be used to route DNS requests through tor network, but this is _not_ default behavior



Threat 2: Traffic Analysis

- "Traffic-analysis is extracting and inferring information from network meta-data, including the volumes and timing of network packets, as well as the visible network addresses they are originating from and destined for"
- Tor is a low latency network, and thus is vulnerable to an attacker who can see both ends of a connection

Threat 3: Rogue Exit Nodes

- Traffic going over Tor is not encrypted, just anonymous
- Malicious exit node can observe traffic
- 2007: Swe researcher, Dan Egerstad, obtained emails from embassies belonging to Australia, Japan, Iran, India and Russia, publishes them on the net
- Sydney Morning Herald called it "*hack of the year*" in interview with Egerstad