OFFICE OF THE INSPECTOR GENERAL

U.S. Department of Education

Technology Crimes Division

Fraud And The Darknets

Thomas Harper
Assistant Special Agent in Charge
Technology Crimes Division

What is an OIG?

- Established by Congress
- Independent agency that reports to Congress
- Agency head appointed by the President and confirmed by Congress
- Mission: protect the taxpayer's interests by ensuring the integrity and efficiency of the associated agency

Technology Crimes Division

- Investigate criminal cyber threats against the Department's IT infrastructure, or
- Criminal activity in cyber space that threatens the Department's administration of Federal education assistance funds
  - Investigative jurisdiction encompasses any IT system used in the administration of Federal money originating from the Department of Education.

Work Examples

- Grade hacking
- Computer Intrusions
- Criminal Forums online selling malware
- ID/Credential theft to hijack Student Aid applications
- Misuse of Department systems to obtain personal information
- Falsifying student aid applications by U.S. government employees
- Child Exploitation material trafficking

OFFICE OF THE INSPECTOR GENERAL
U.S. Department of Education
Technology Crimes Division

Fraud and the Darknets

Special Thanks
to
Financial Crimes Enforcement Network
(FINCEN)

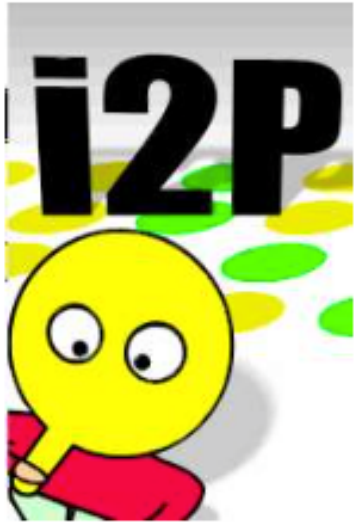
Fraud and the Darknets

- What are Darknets
- How Do They work
- Accessing Darknets
- Navigation, Sources, Discovery
- Darknet Marketplaces

What are Darknets?

- Cypherspace or Anonymous networks
- Accessible through specialized software
- Enable access to hidden websites/services
- Enable anonymous web surfing
- NOT the Deep Web

Darknets



Where Do They Come From?

- 1995 Office of Naval Research Funding
- 1997 DARPA High Confidence Networks Program
- 1999 funding suspended; research continues
- 2000 Java Anon Proxy (Mixing) Implemented
- 2001 DARPA Fault Tolerance Networks Program
- 2003 ONR, NRL, DARPA funds
- 2004 Tor released under MIT free/open License
- Research Continues…

Who Uses Darknets?

- Governments
- Academia
- Media
- Political Groups
- Businesses
- Hackers
- Criminals

Who Uses Darknets?

Tor Researcher Who Exposed Embassy E-mail Passwords Gets Raided by Swedish FBI and CIA

BY KIM ZETTER 11.14.07 4:13 PM

Dan Egerstad, the Swedish computer security consultant I interviewed in August who obtained log-in and password information for 1,000 e-mail accounts belonging to foreign embassies, corporations and human rights organizations, had his house raided on Monday by Swedish officials, who took him in for questioning.

Egerstad (at right) said that on Monday morning as he was leaving his apartment in Malmo to move his car, he opened his front door to find five plainclothes men standing at the entrance. Four of the agents showed him identification but one of them wouldn't show him identification or give his name. He says the four with IDs belonged to the Swedish National Police (the country's domestic agency), and the fifth one was an agent of the SAPO (Sweden's CIA). The agents had driven to Malmo from Stockholm to conduct the raid.

http://www.onion-router.net/History.html

Why Care?

- Child Porn
- Illicit Services
- Darknet Marketplaces
- Cybercrime

Why Care?

Professional Contract Killer

We operate worldwide . Hit men with professional background
(no criminals, no cops)
We guarantee a quick execution of your problem (within 40 days).

Minimum age of target: 18

Conditions: 50% in advance for job preparation,
50% 30 days after first payment (just before the job)
(We don't accept payments after the job, because
some clients didn't pay after job conclusion)

Contact: charon2000@tor.org
email us:
photo: upload the photo in http://xfq5l5p4g3eyrct7.onion.to and copy the relative link. Paste this link in the mail with the information about the target!!!
information: give us all the information you have about the target
(example: name, address, age etc.)

Targets:
Cost for any civilian: 1.800 bit coin
Cost for businessmen/political figures: 4.000 bit coin
Cost for celebrities: 10.000 bit coin

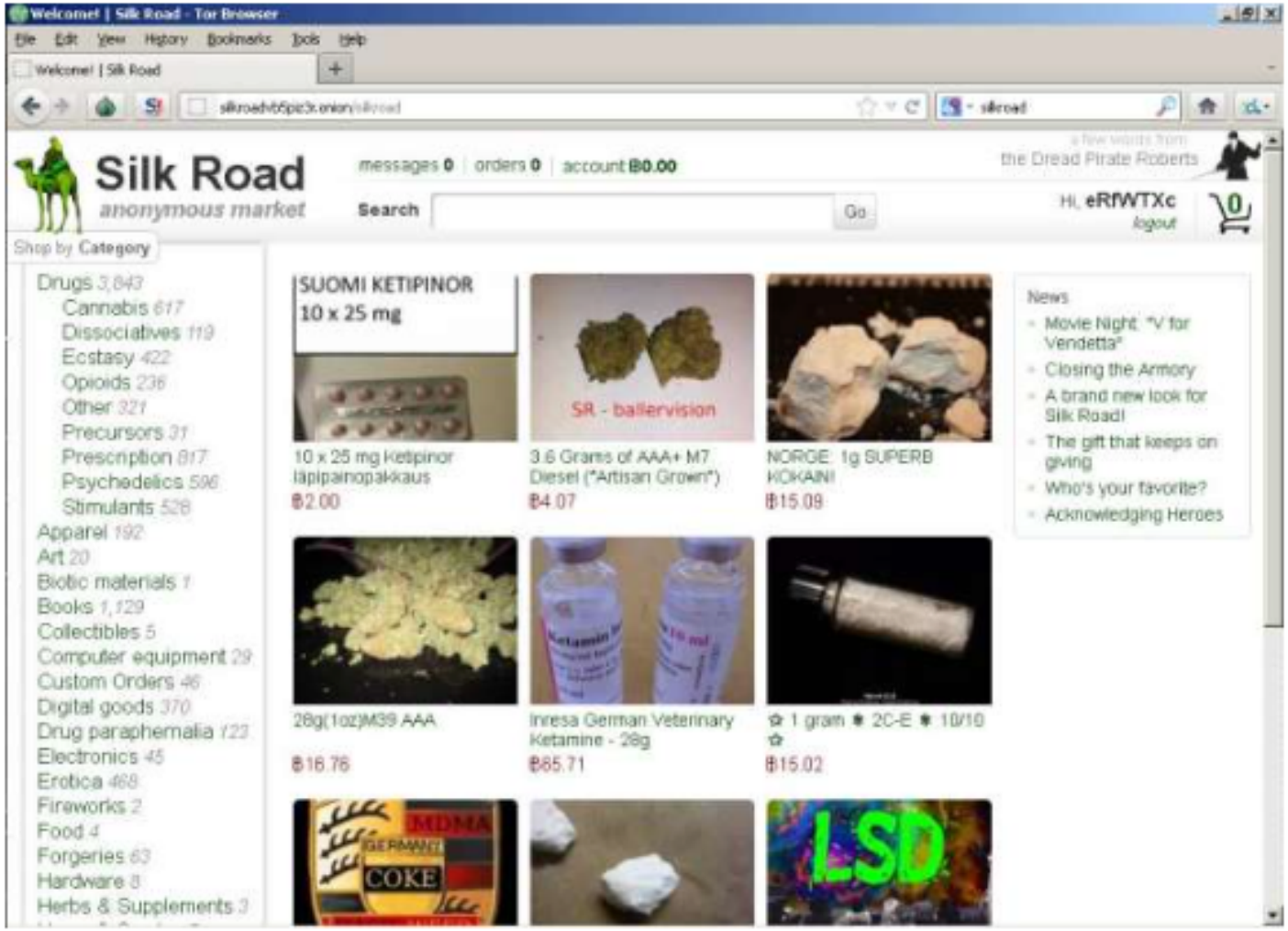
http://en.wikipedia.org/wiki/File:PPTMooresLawai.jpg

OFFICE OF THE INSPECTOR GENERAL

U.S. Department of Education

Technology Crimes Division

Why Care?

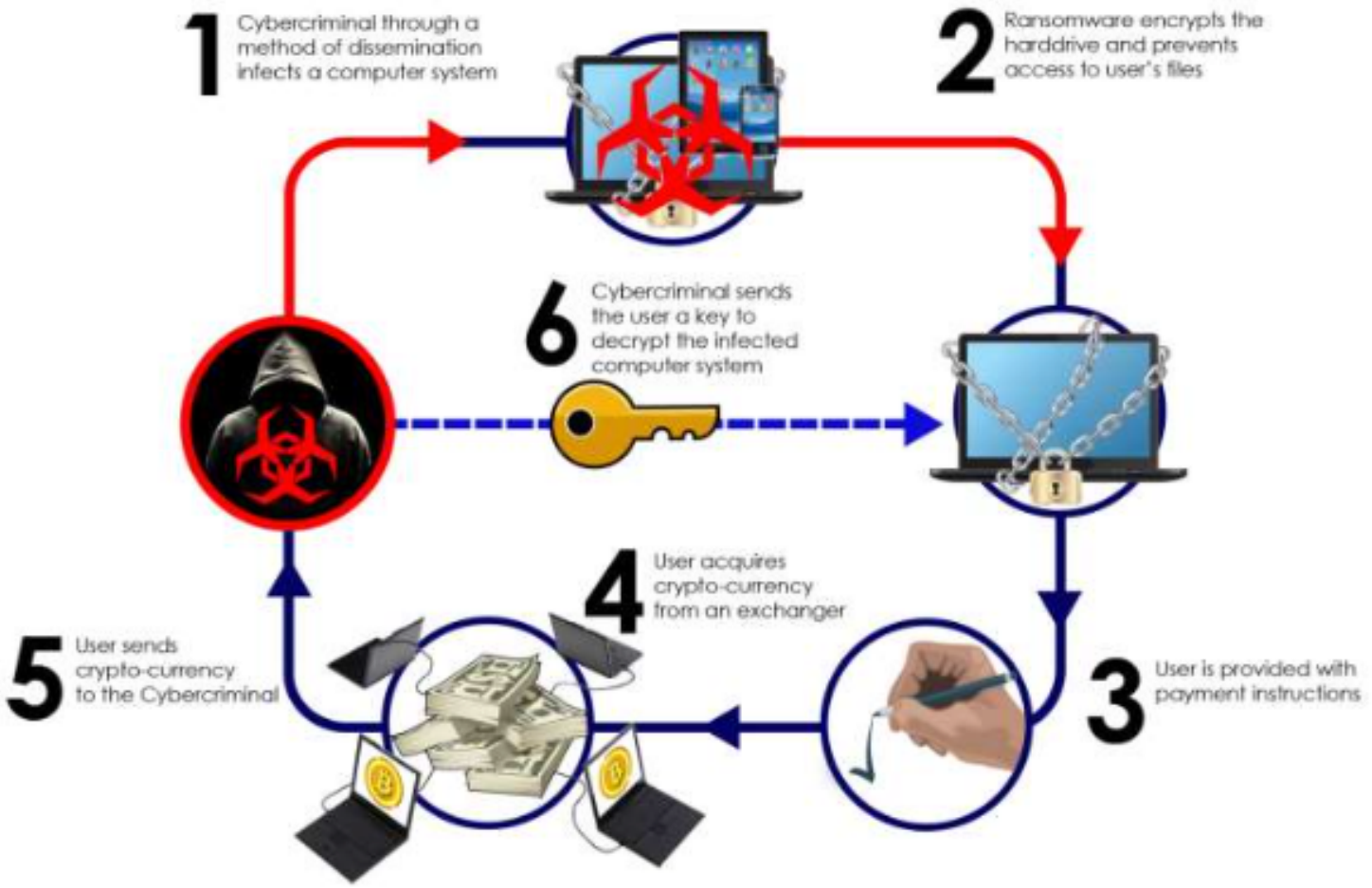


OFFICE OF THE INSPECTOR GENERAL

U.S. Department of Education

Technology Crimes Division

Why Care?

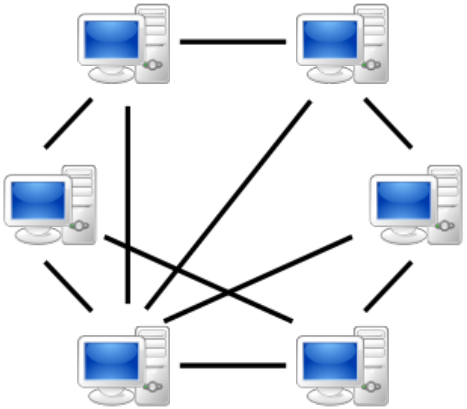


How Do Darknets Work?

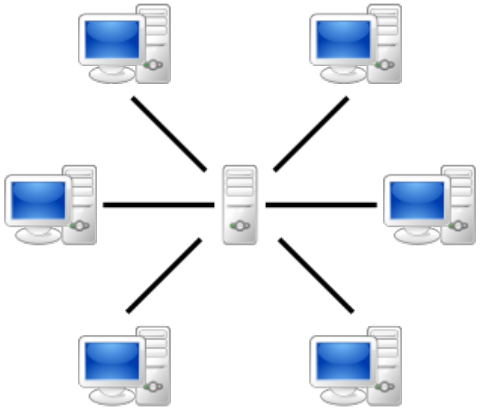
- Anonymous P2P
- Nodes / IP Addresses
- Types of Anonymity Communications
- Future Trends

What is “P2P”?

Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or work loads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes.



VS

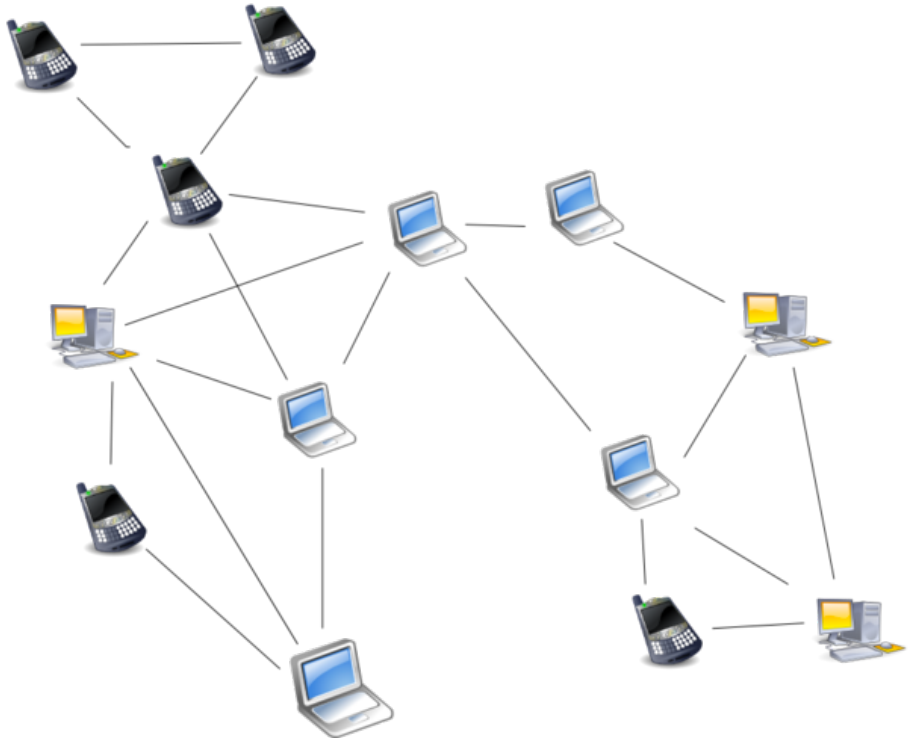


https://en.wikipedia.org/wiki/Peer-to-peer

How do peers talk?

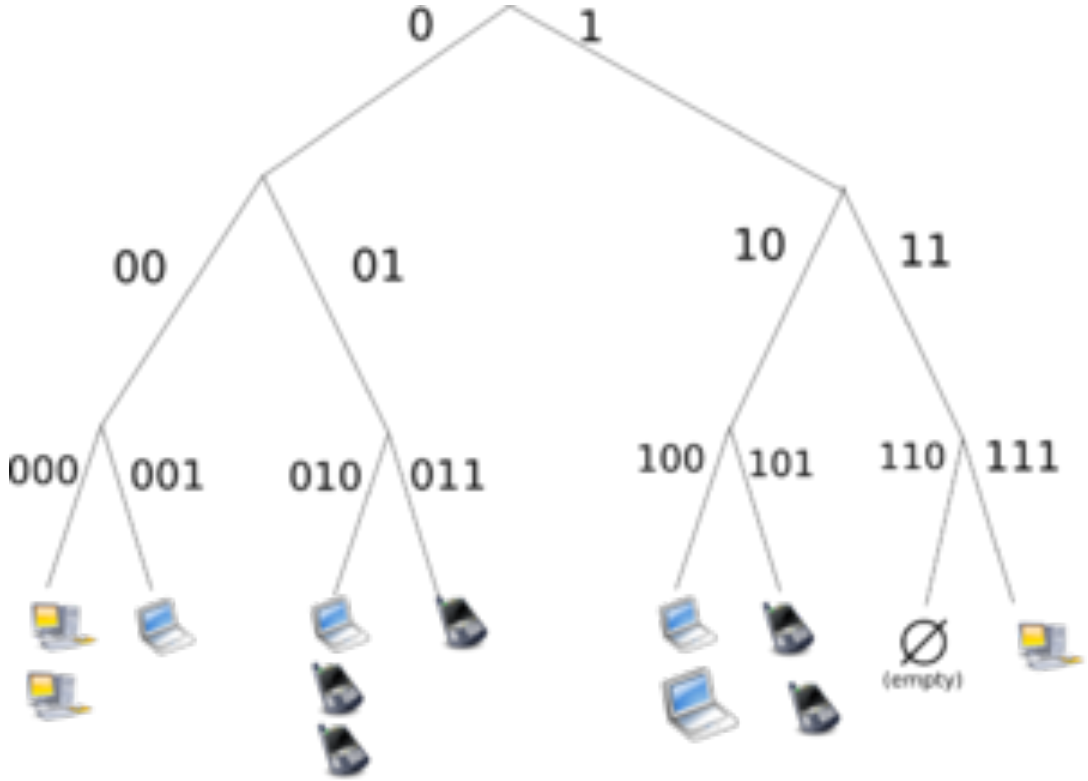
- Special software (limewire, bearshare, utorrent)
- Connects initially to closest peer to search for resources or download peer list
- After initial connection, peer list is updated as needed.
- Peer mapping is done by IP address

P2P Unstructured Network



https://en.wikipedia.org/wiki/Peer-to-peer

P2P Structured Network



https://en.wikipedia.org/wiki/Peer-to-peer

What is an IP address?

- **An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network (such as the Internet) that uses the Internet Protocol for communication.**

https://en.wikipedia.org/wiki/IP_address

What is geolocation?

- **Geolocation is the identification of the real-world geographic location of an object, such as a radar source, mobile phone or Internet-connected computer terminal.**
- **IP address location data can include information such as country, region, city, postal/zip code, latitude, longitude and timezone.**

https://en.wikipedia.org/wiki/Geolocation

Why is geolocation important?

- **By identifying where online visitors really are, geolocation can protect banks from participating in the transfer of funds for illicit purposes.**
- **More and more prosecuting bodies are bringing cases involving cyber-crimes such as cyber-stalking and identity theft. It is imperative that prosecutors provide the background IP data necessary to link a suspect to a particular crime.**

https://en.wikipedia.org/wiki/Geolocation_software

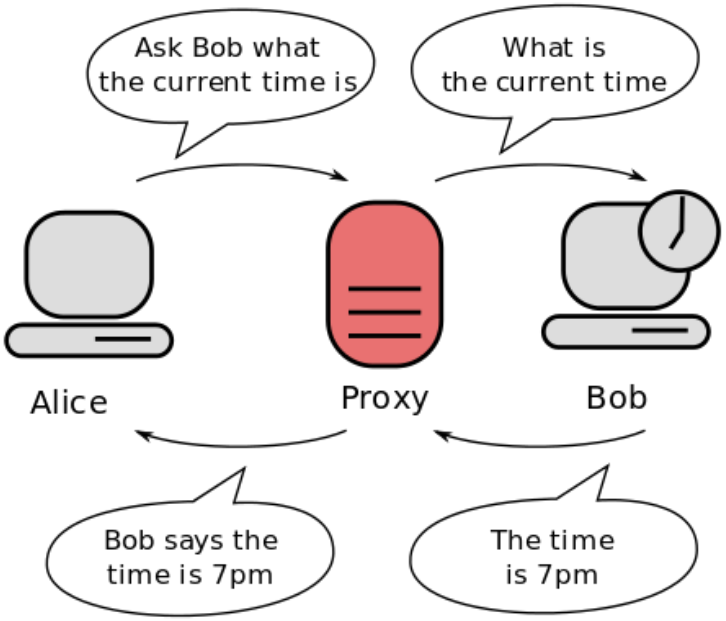
Why is geolocation important?

- **Detect possible credit card fraud by comparing the user's location to the billing address on the account or the shipping address provided.**
- **Used in fraud detection to match billing address postal code or area code.**
- **Used to prevent “phishing” attacks, money laundering and other security breaches by determining the user's location as part of the authentication process.**
- **Used as an investigatory tool, tracking the Internet routes of online attackers to find the perpetrators and prevent future attacks from the same location.**

https://en.wikipedia.org/wiki/Geolocation_software

What is a proxy?

- **In computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.**



Which IP address will Bob's computer associate with the time request?

https://en.wikipedia.org/wiki/Proxy_server

Anonymity Technology

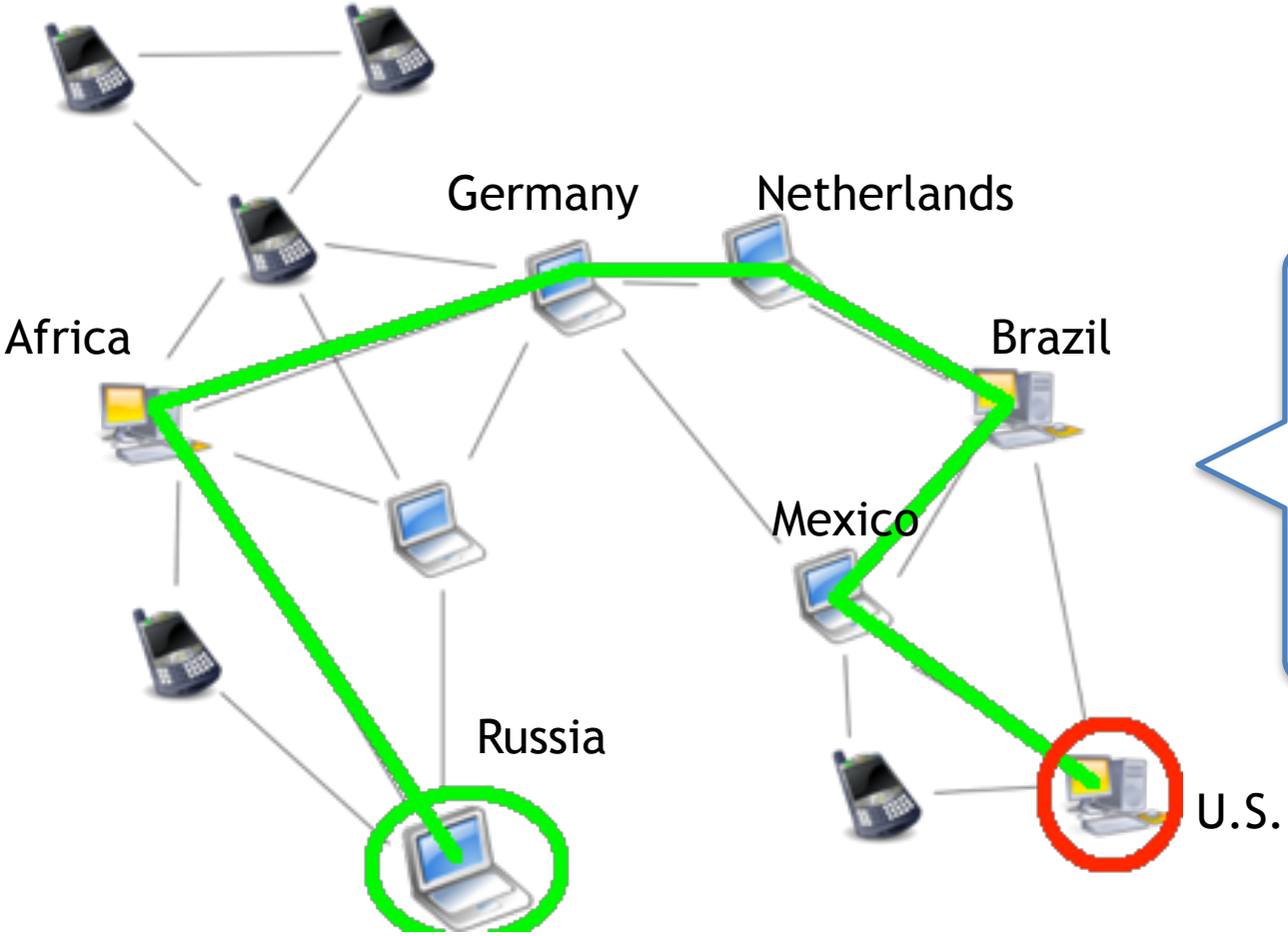
- Anonymous P2P: distributed application in which the nodes or participants are anonymous. Anonymity of participants is usually achieved by special routing overlay networks that hide the physical location of each node from other participants.

OFFICE OF THE INSPECTOR GENERAL

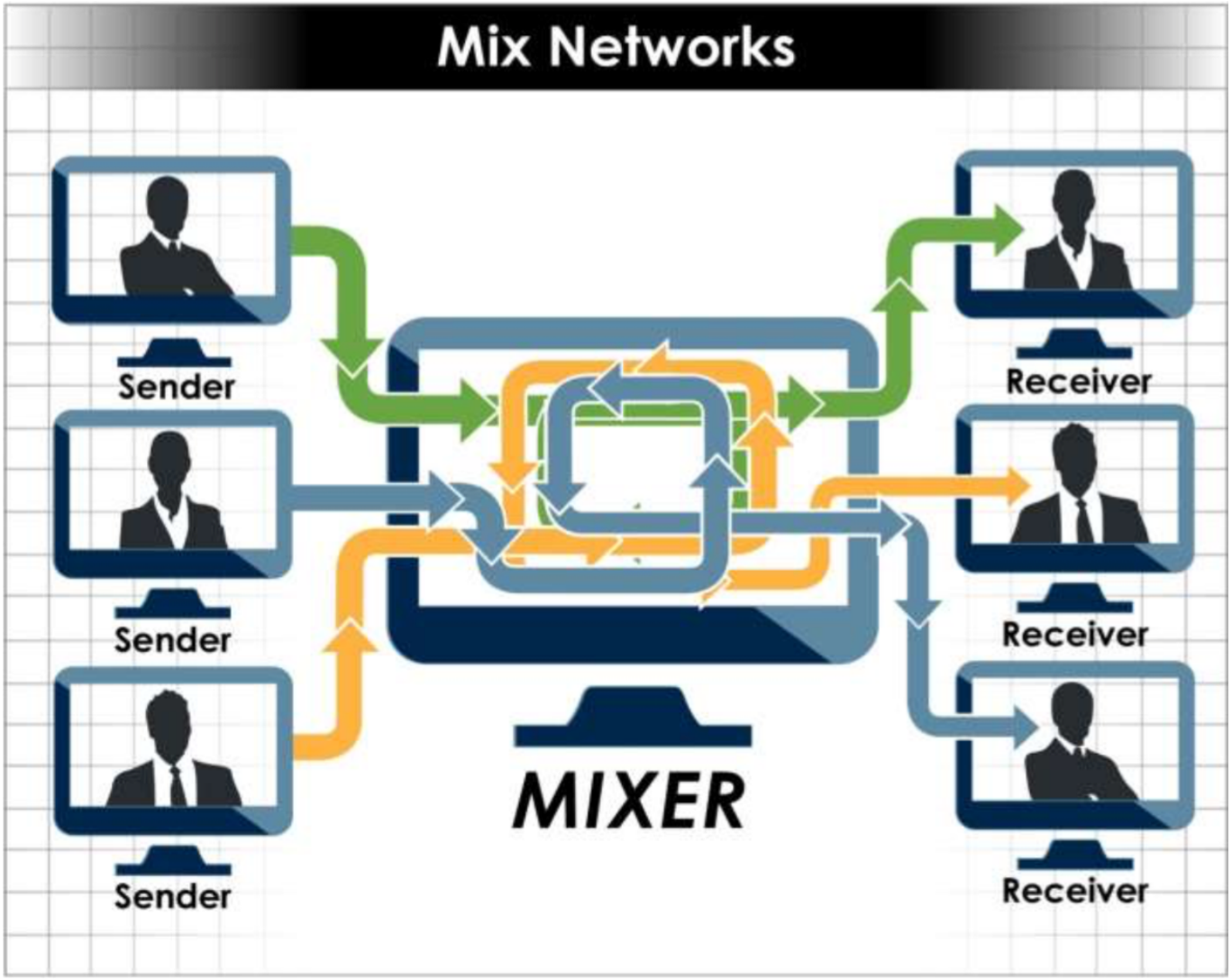
U.S. Department of Education

Technology Crimes Division

Anonymity Technology



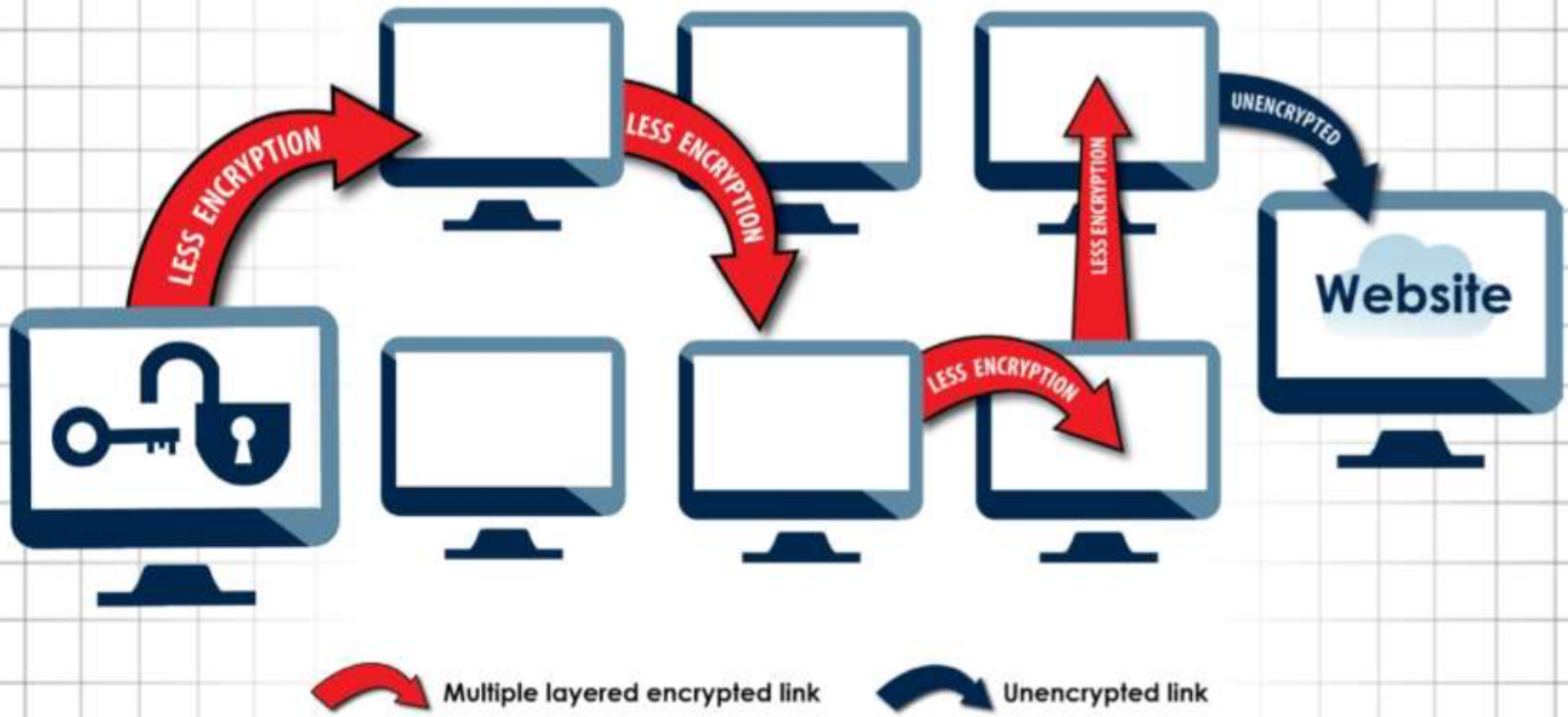
What source IP address will the endpoint see? Where will it geolocate?

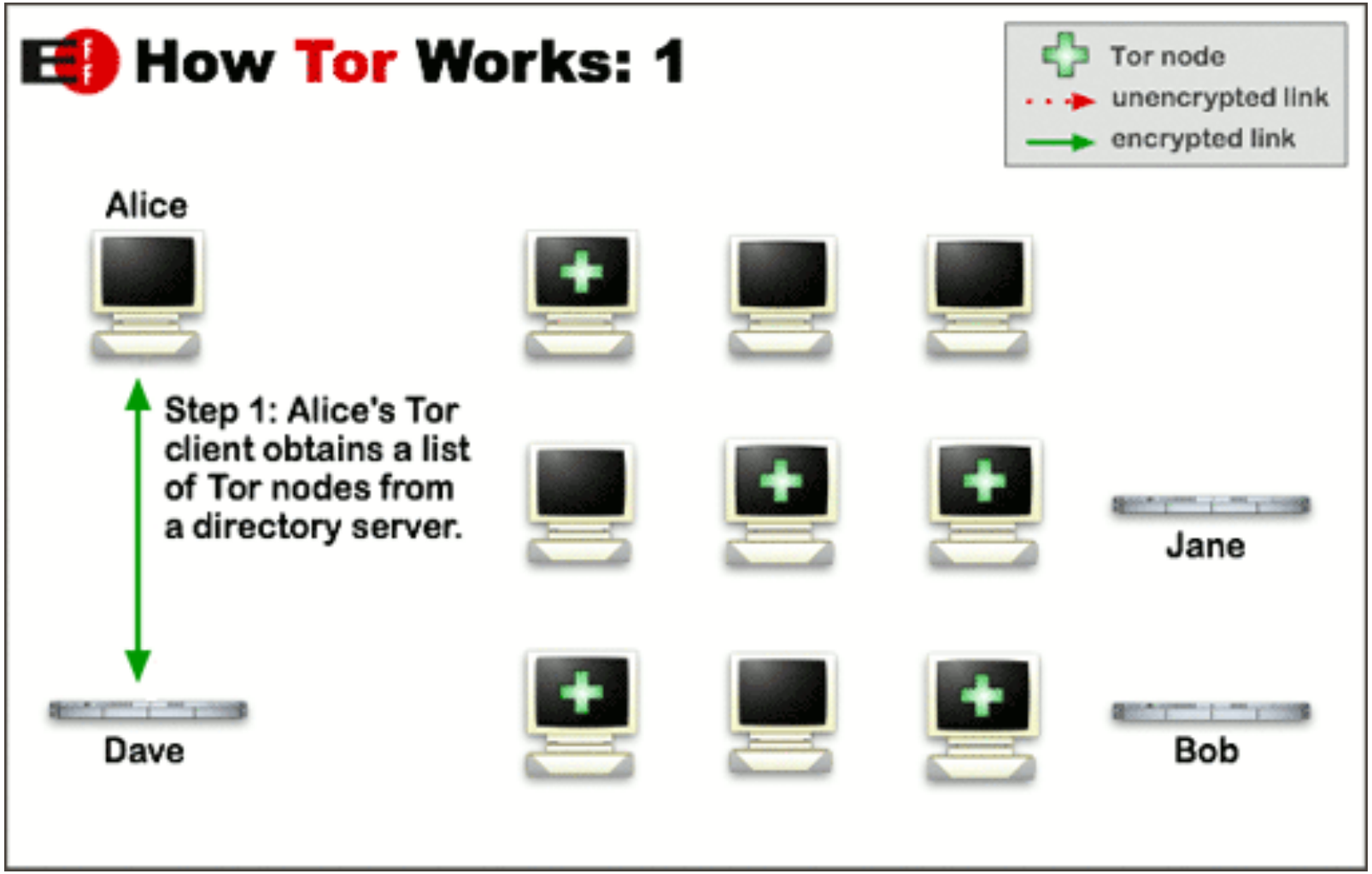

Mix Networks
Sender
Sender
Sender
MIXER
Receiver
Receiver
Receiver

Onion Routing

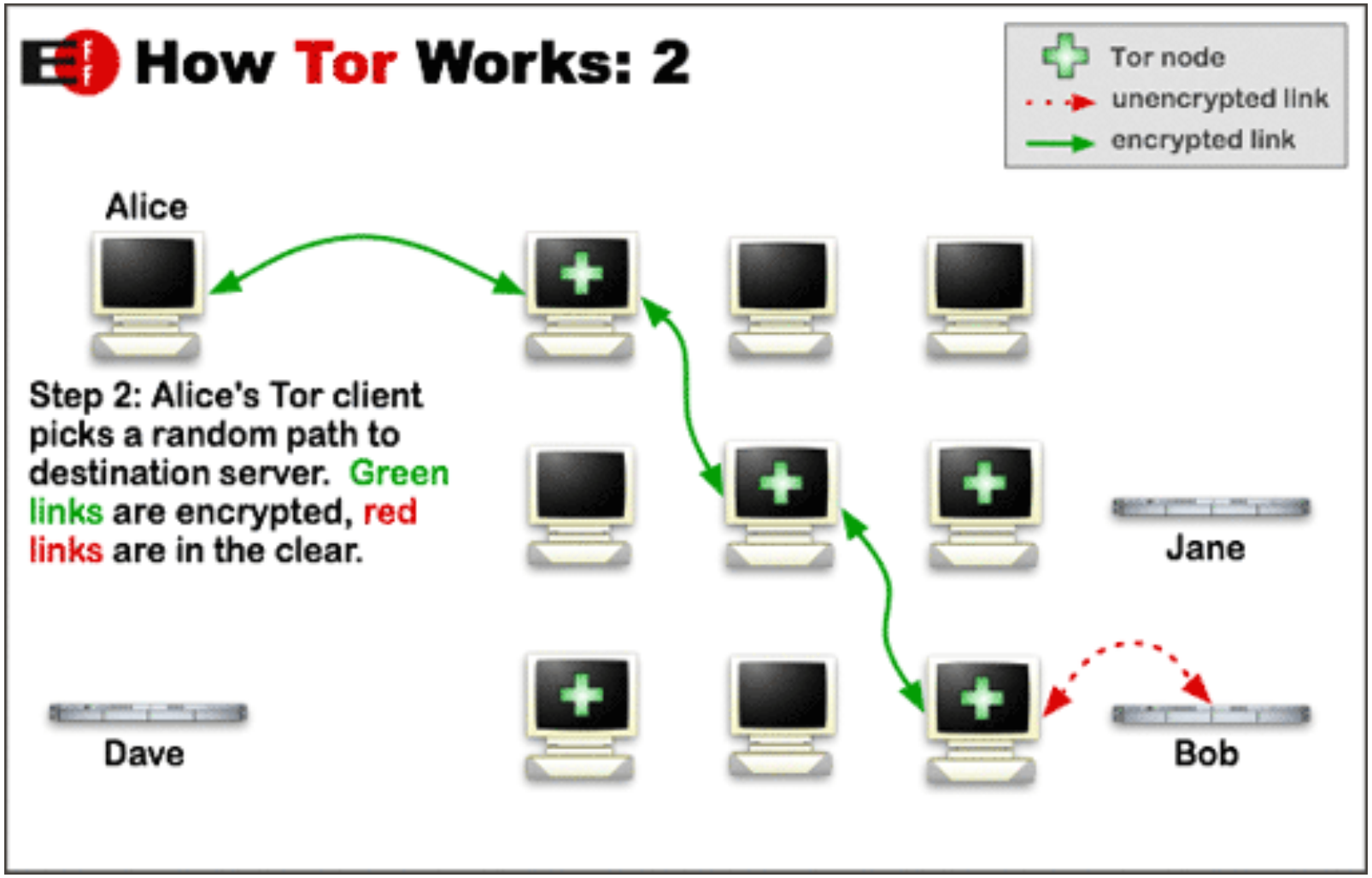
- a technique for anonymous communication over a computer network. Messages are repeatedly encrypted and then sent through several network nodes. Each node removes a layer of encryption to uncover routing instructions, and sends the message to the next router where this is repeated. This prevents these intermediary nodes from knowing the origin, destination, and contents of the message

Onion Routing

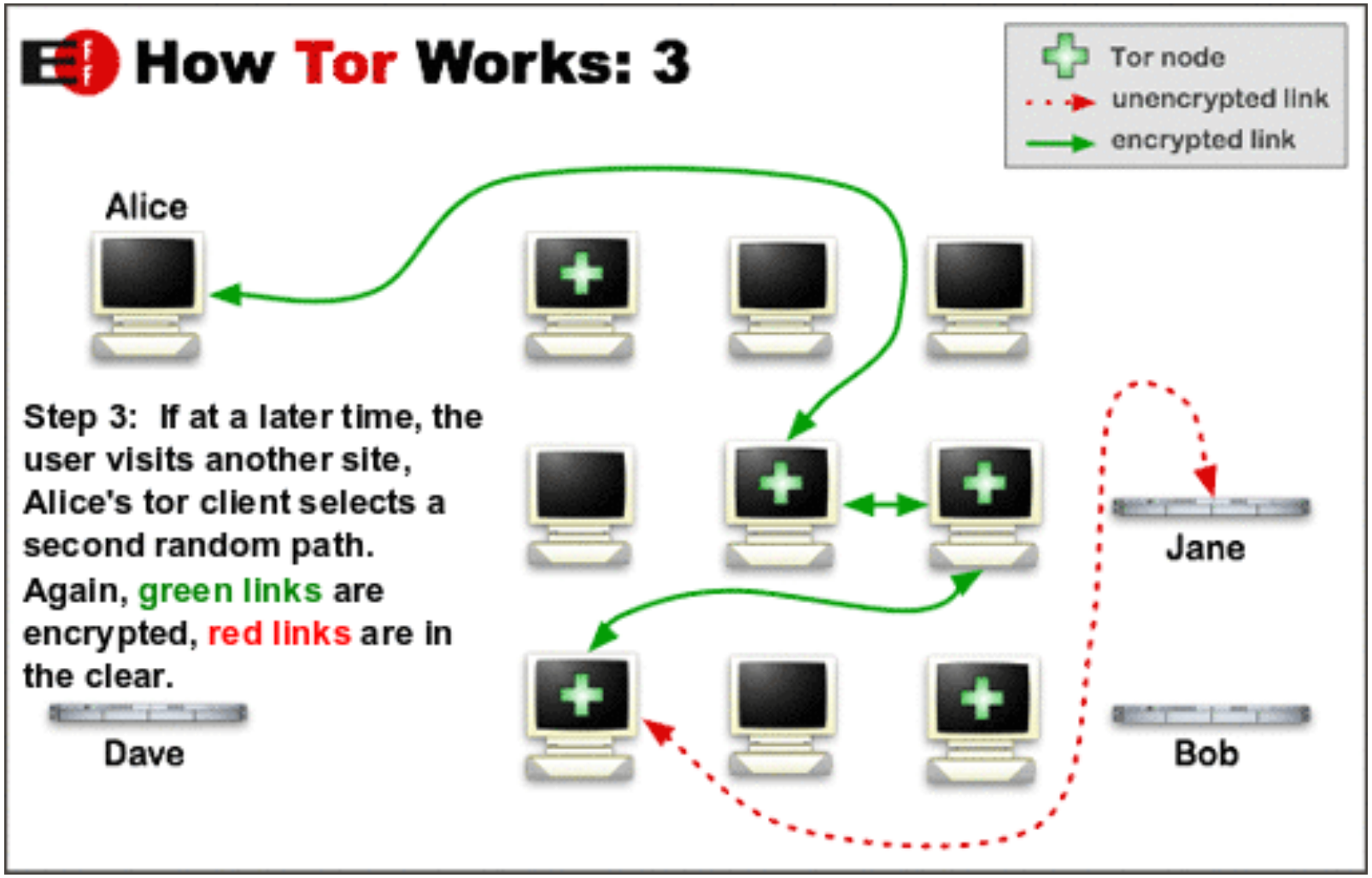




https://tor.eff.org/about/overview.html.en



https://tor.eff.org/about/overview.html.en



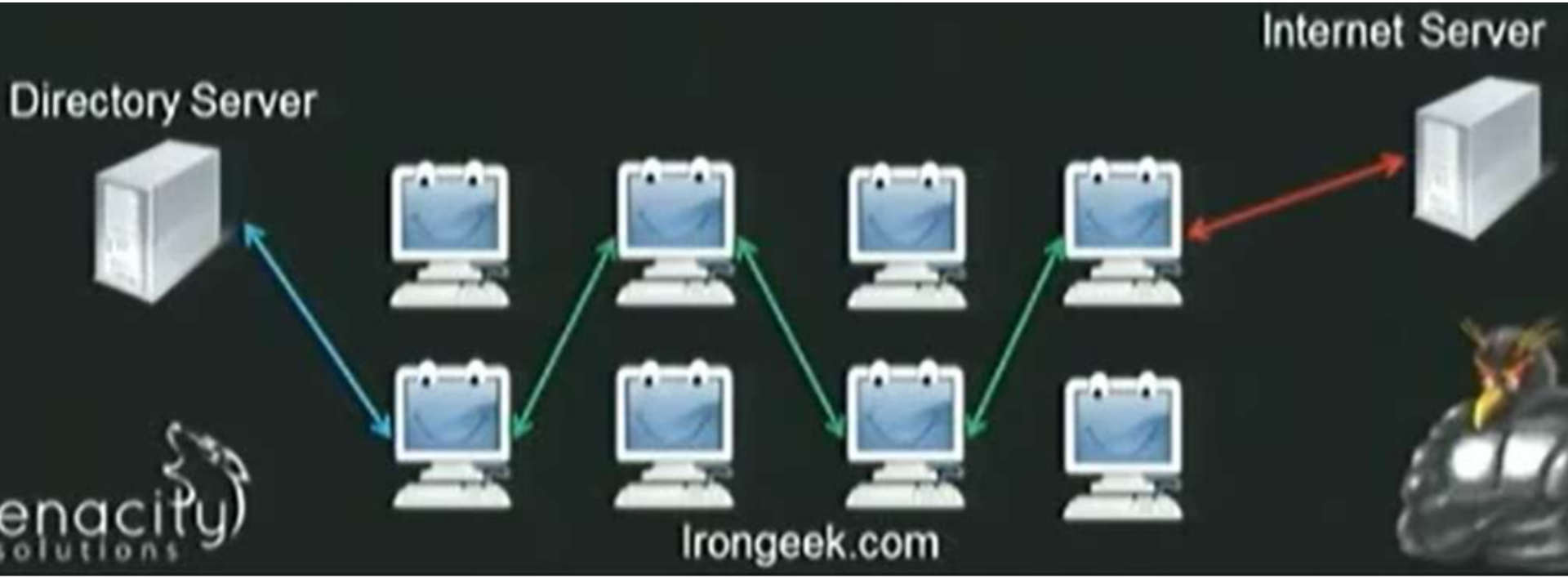
https://tor.eff.org/about/overview.html.en

OFFICE OF THE INSPECTOR GENERAL

U.S. Department of Education

Technology Crimes Division

Unidirectional Tunnel



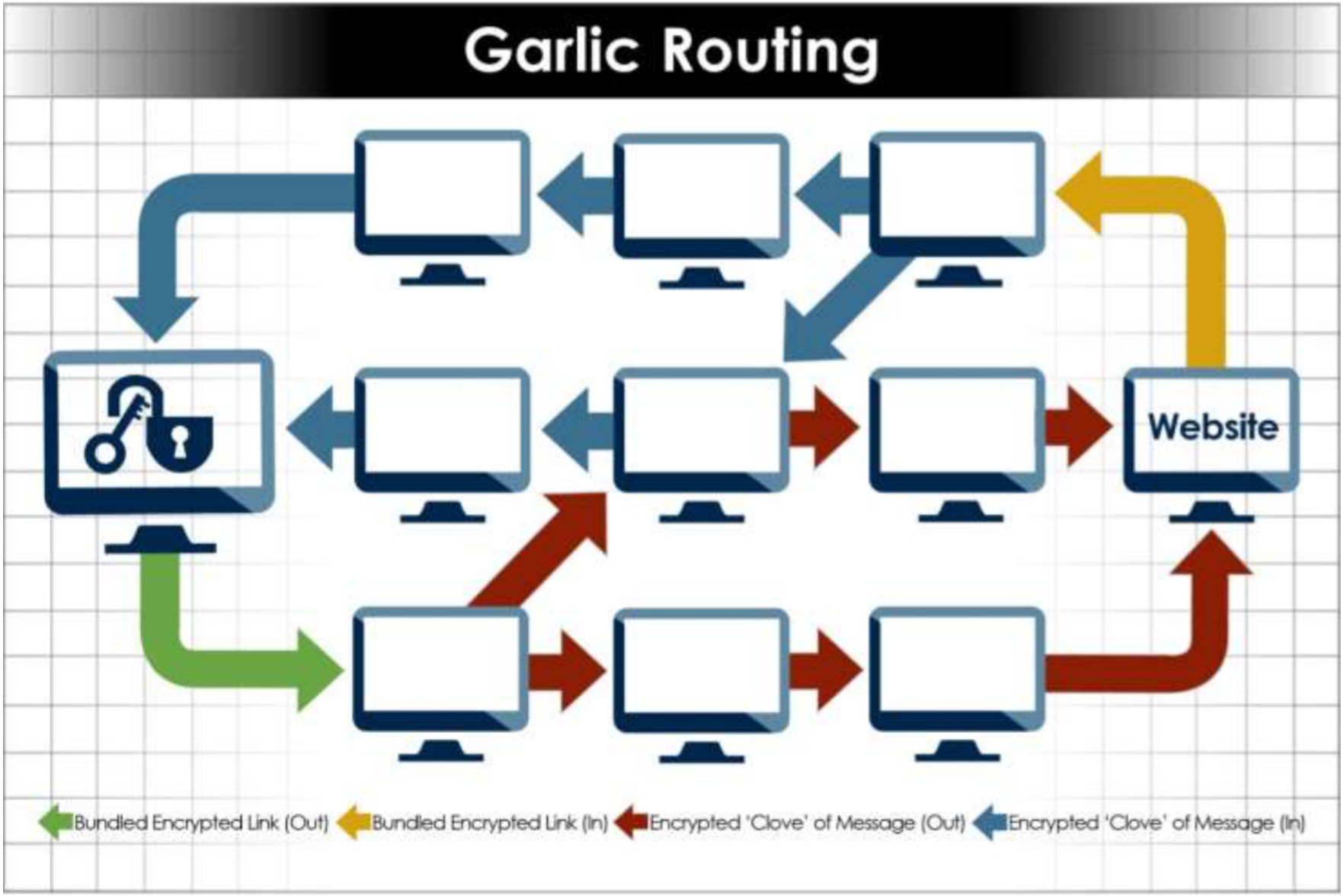
Garlic Routing

- a variant of onion routing that encrypts multiple messages together to make it more difficult for attackers to perform traffic analysis.

OFFICE OF THE INSPECTOR GENERAL

U.S. Department of Education

Technology Crimes Division

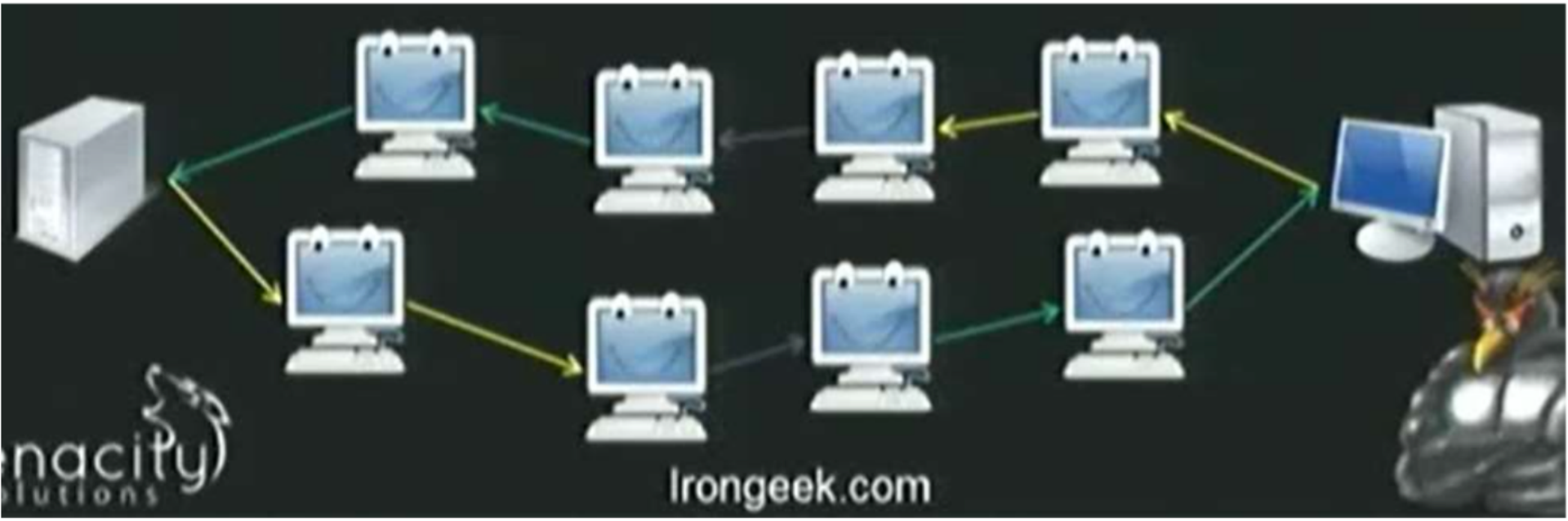


OFFICE OF THE INSPECTOR GENERAL

U.S. Department of Education

Technology Crimes Division

Bi-directional Tunnel



The Future?

- Research on the underlying technology such as routing and encryption continues
- New Darknets Evolve
- Trend towards Decentralized/Distributed Technology Implementations Schemes
- Harder to “De-Anonymize”
- More Robust

OFFICE OF THE INSPECTOR GENERAL
U.S. Department of Education
Technology Crimes Division

Navigating Darknets

General Access
How are they different from the Clearnet?

Navigating Darknets

- Steps to Access a Darknet
- Darknet website domain extensions
- Comparison of Darknets
- Sources for Darknet website addresses

OFFICE OF THE INSPECTOR GENERAL

U.S. Department of Education

Technology Crimes Division

Accessing Darknets

Accessing Darknets

- Tor
  - Tor Bridge (Clearnet access proxy website)
  - Vidalia (Installed desktop/laptop software)
  - Orbot (Installed mobile device software)
  - Tails (Anonymizing operating system)
- I2P (eepsite.com)
- CJDNS (Hyperboria)
- Freenet

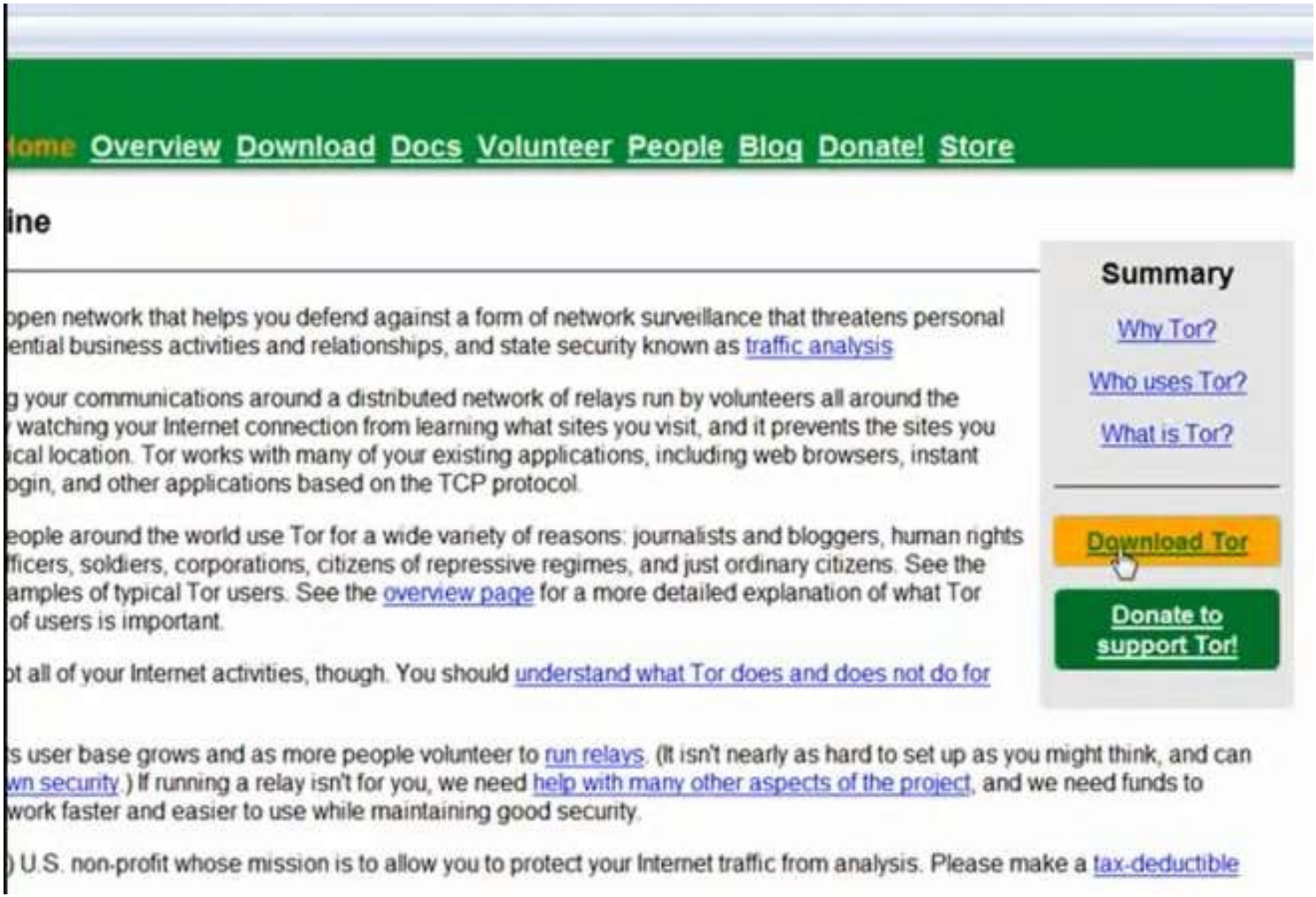
Tor Bridges

- Onion.cab
- Onion.to

Tor: Vidalia

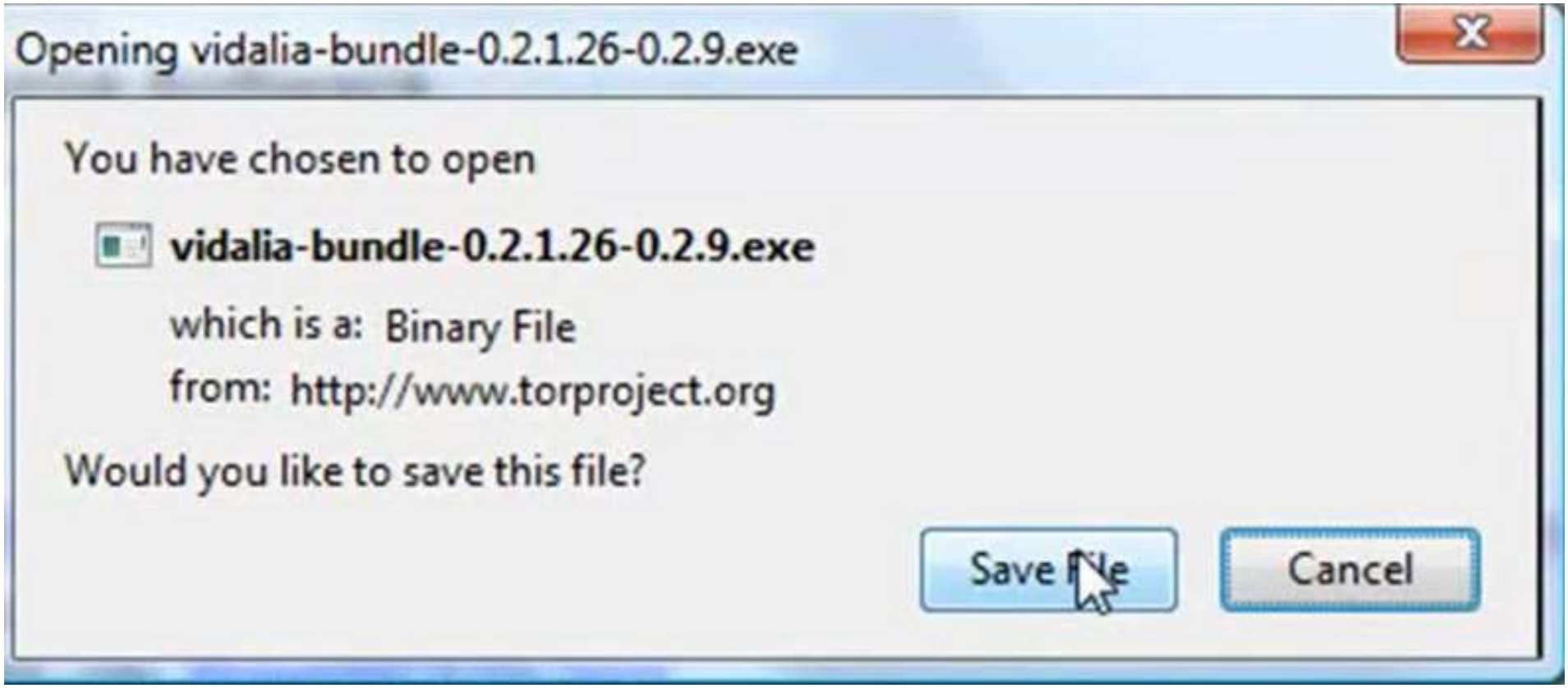
desktop/laptop software

Tor: Vidalia download

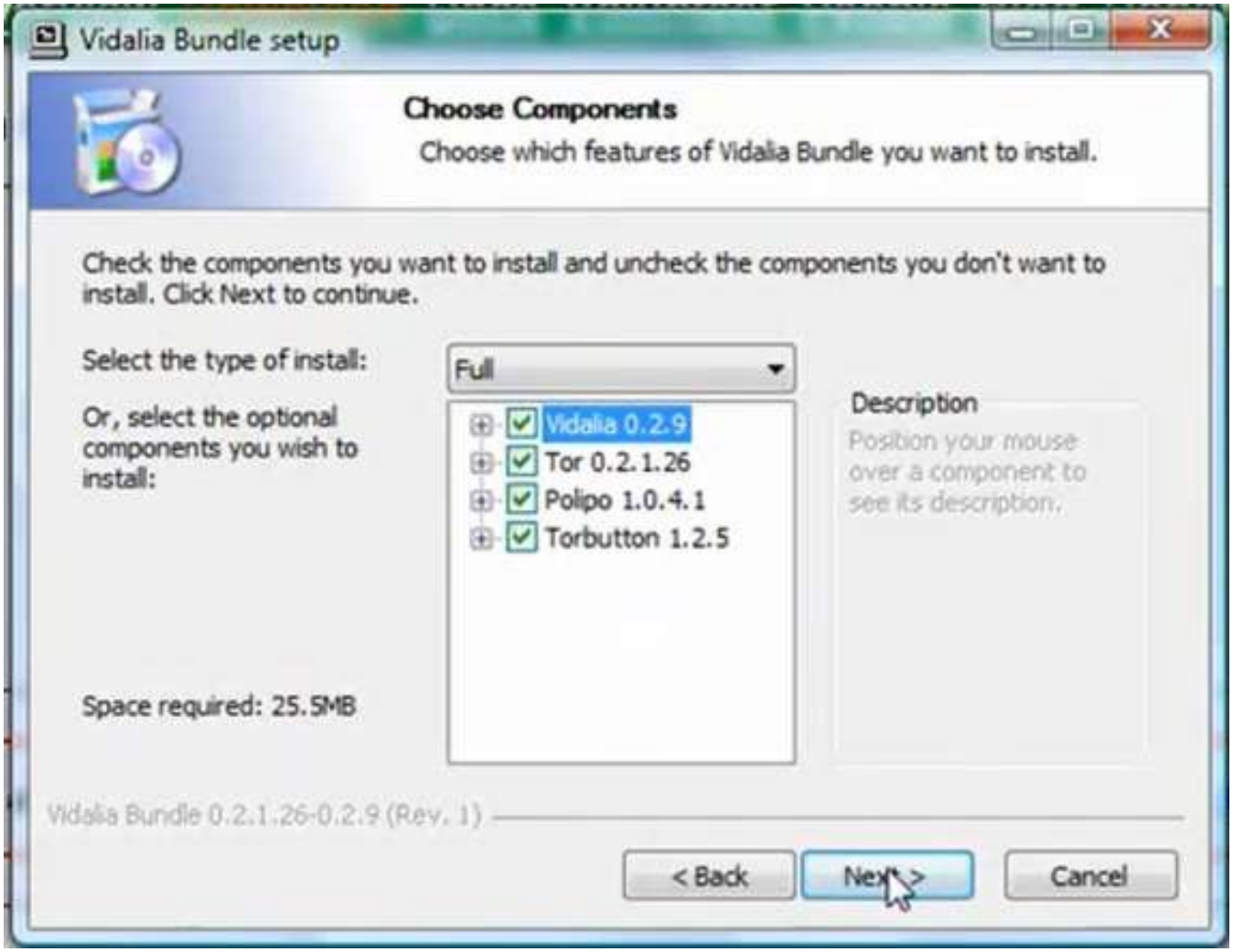


Tor: Vidalia download

Tor: Vidalia install



Tor: Vidalia install



Tor: Vidalia running

OFFICE OF THE INSPECTOR GENERAL

U.S. Department of Education

Technology Crimes Division

Tor: Vidalia running

Congratulations. Your browser is configured to use Tor.

Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously.

Your IP address appears to be: **37.130.227.133**

This page is also available in the following languages:

عربية (Arabiya) Burmese česky dansk Deutsch Ελληνικά (Ellinika) English español Estonian فارسی (Fārsī) suomi français Italiano 日本語 (Nihongo) norsk (bokmål) Nederlands polski Português Português do Brasil română Русский (Russkij) Thai Türkçe українська (ukrajins'ka) Vietnamese 中文(简)

Tor: Orbot

mobile device software

https://www.youtube.com/watch?v=WftnnG0Sgl8

I2P

Invisible Internet Project

I2P

- Primarily Java-based client software to install
- Does not have a large number of exit nodes like Tor.
- Designed for encrypted connections and communications in almost a closed environment.
- Reliability is questionable

http://www.eepsite.com
https://geti2p.net/en/faq

CJDNS

Hyperboria
(Project Meshnet)

CJDNS

- Client software to install
- Uses IPV6 technology with encryption
- All communications are encrypted end-to-end with public key encryption
- Distributed hash table in order to create a structured P2P network.
- Not designed to integrate with the Clearnet like Tor
- CJDNS network is called a “mesh”
- Hyperboria is currently the largest mesh.

Freenet

File sharing through distributed storage

Freenet

- Client software to install
- Designed to sit on top of the Clearnet
- Primarily a file sharing network
  - each peer has a set amount of dedicated storage space for encrypted Freenet data
  - copies or parts of copies of a file are stored all over the network.
  - attrition of stored data over time if it is not requested and re-written to storage space.
- Limited messaging services are available

Darknet website extensions

	Name	Web extension
Tor	Tor Link	.onion
I2P	eepsite	.i2p
CJDNS	none	none
Freenet	none	none

Comparison of Darknets

	Anon Proxy	Access From Clearnet	Hidden Services	Comm Platform
Tor	yes	yes	yes	yes
I2P	limited	no	yes	yes (in network only)
CJDNS	no	no	yes	yes (in network only)
Freenet	no	no	yes	yes (in network only)

Sources for Darknet website addresses

- Tor:
  - ahmia.fi
  - deepdotweb.com
  - The Hidden Wiki (hidden service on Tor)
- All:
  - Pastebin
  - Wikis
  - Forums

OFFICE OF THE INSPECTOR GENERAL
U.S. Department of Education
Technology Crimes Division

Darknet Marketplaces

Hidden markets for Illicit Goods and Services

Darknet Marketplaces

- Definitions
- How they Work
- Chokepoints
- Sources
- Future Trends

What is a Darknet Marketplace?

- hidden websites (within darknets) allowing users to anonymously exchange value with other users for the purchase of illicit goods and services from participating vendors or sellers.
- Silk Road/DPR first DM launched in Feb 2011
- Most take bitcoin or other crypto-currency as a form of exchange

How do they Work?

- Buyers
  - Users who wish to purchase illicit goods or services must register with a username and password, are issued a crypto-currency account that they must fund, and will often provide a mailing address to sellers from whom they make purchase
- Sellers
- Marketplace Administrators

How do they Work?

- Buyers
- Sellers
  - vendors of illicit goods and services must register with a username and password and are issued a crypto-currency account. Sellers post goods for sale via the marketplace and are responsible for getting goods to buyers. Sellers are rated on reliability
- Marketplace Administrators

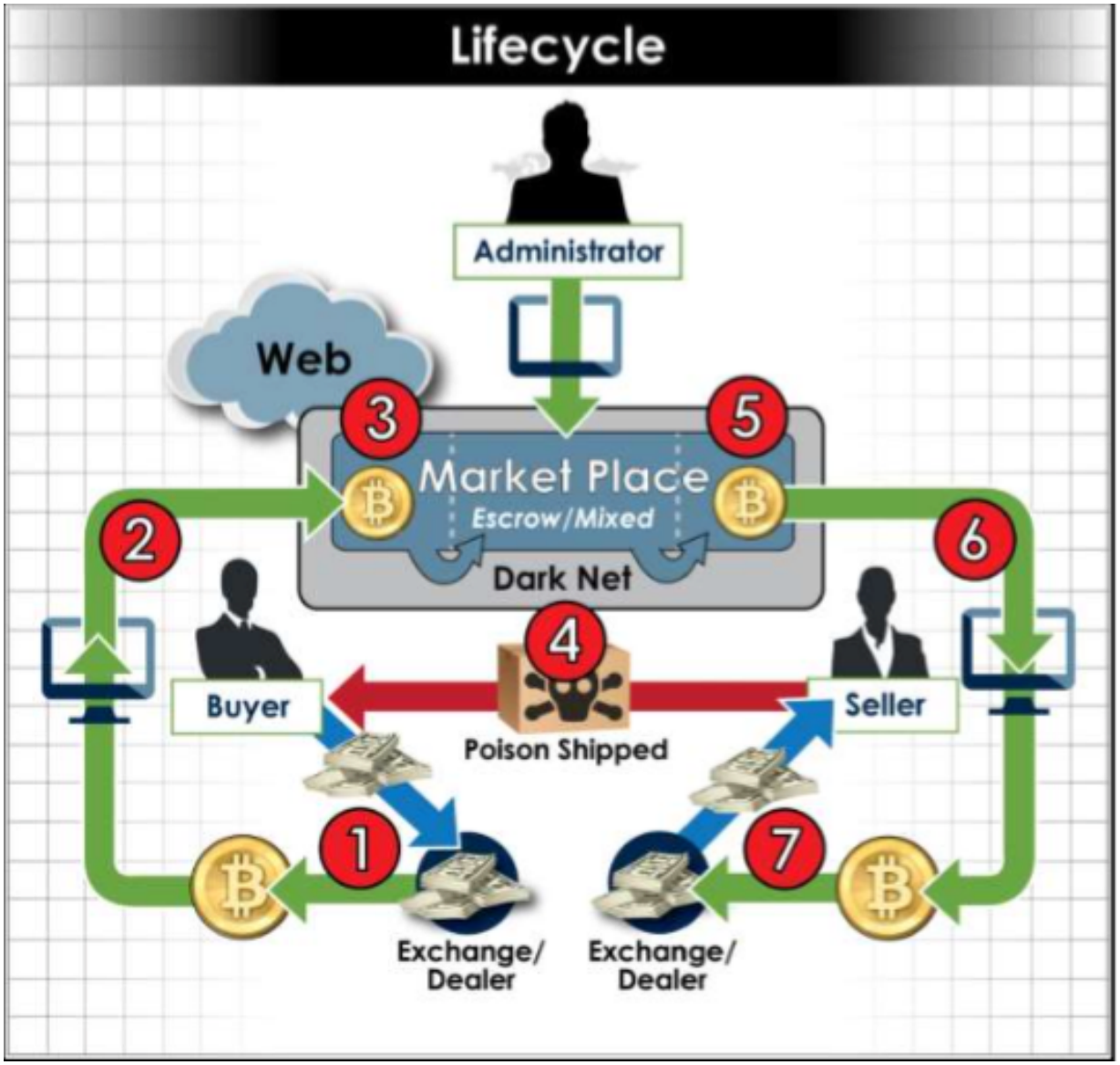
How do they Work?

- Buyers
- Sellers
- Marketplace Administrators
  - person or persons responsible for the operation of the marketplace to include website technical maintenance, resolution of disputes, and IT security. The administrator collects fees and/or commission on all transactions and acts as an escrow between buyers and sellers. In some cases, darknet marketplace administrators have stolen from their customers

OFFICE OF THE INSPECTOR GENERAL

U.S. Department of Education

Technology Crimes Division



Chokepoints

- Anything physical if you can locate it:
  - mail
  - buyer/seller computer
  - marketplace admin computer
- PGP keys
- Bitcoin addresses
- Bitcoin exchangers
- EXIF data from pictures

Darknet vulnerabilities

Darknet vulnerabilities

- Untrusted exit points
- malware (phone home)
- SSL Strip
- DNS Leaks
- Bad configurations
- Distributed Hash Tables (Structured P2P)
- IRC username

OFFICE OF THE INSPECTOR GENERAL
U.S. Department of Education
Technology Crimes Division

Tor: Tails

Anonymizing Operating System

Thank You!

- Questions?
- 1-800-MISUSED
- www.ed.gov/oig
- my email address: thomas.harper@ed.gov