DEF CON

DC 0471

TRIVANDRUM

29th September, 2018

Entering the gates of Valhalla and taking uncle jim off our backs

Alosh K Jose,EY

OKAY PEOPLE , LET’S START

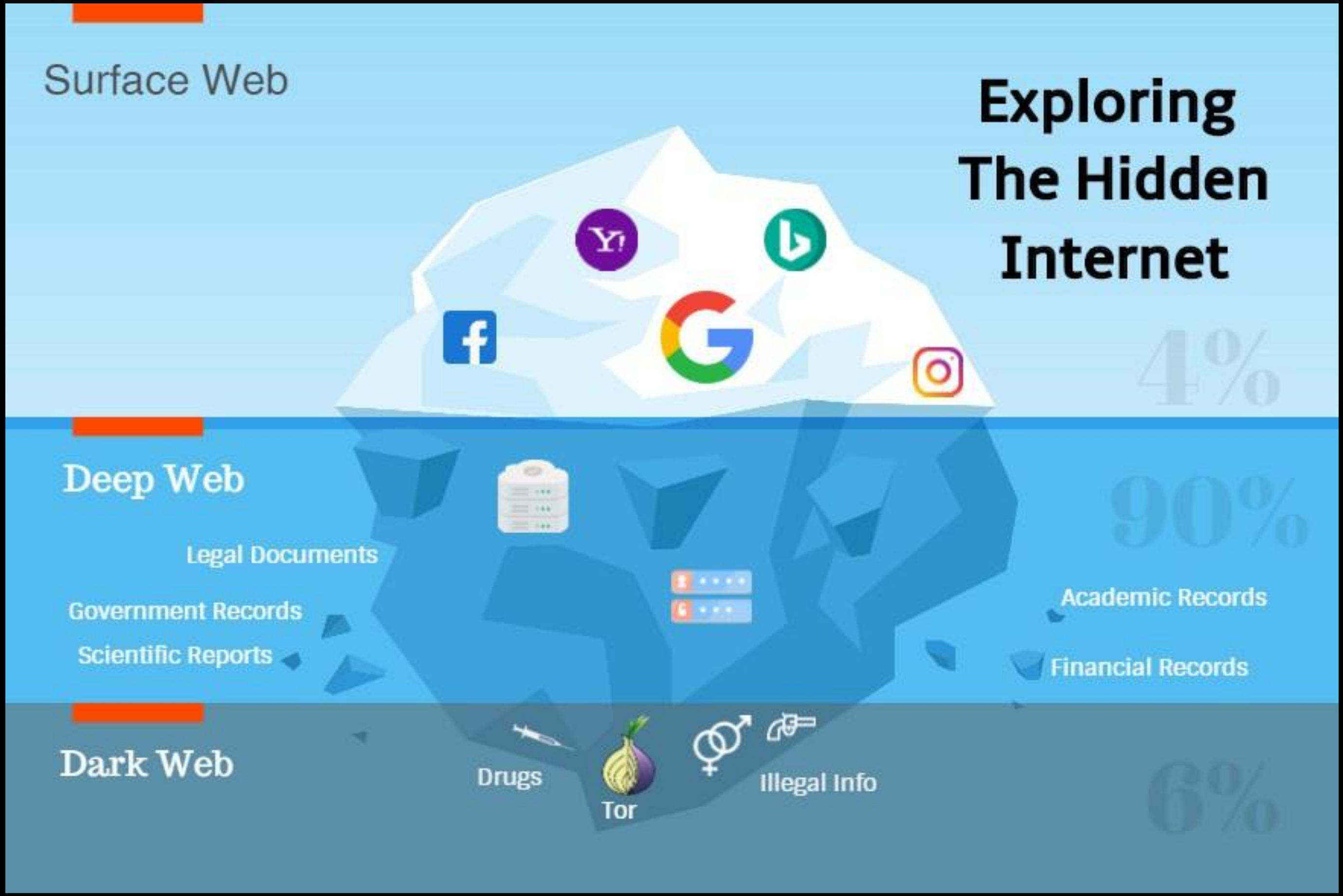
COME TO THE DARKSIDE
WE HAVE COOKIES

Welcome to the Dark side.
We've been expecting you.

Disclaimer

This slide presentation might include not limited to porn,drugs and all kinds of other illegal crap ** no seriously it has some fucked up shit so I suggest people who are not comfortable being with the dark side should leave , it also includes how to be anonymous and save your ass for the most part.

So what the hell is DARKNET? Any idea?



Exploring The Hidden Internet

Surface Web

4%

Deep Web

90%

Legal Documents

Government Records

Scientific Reports

Academic Records

Financial Records

Dark Web

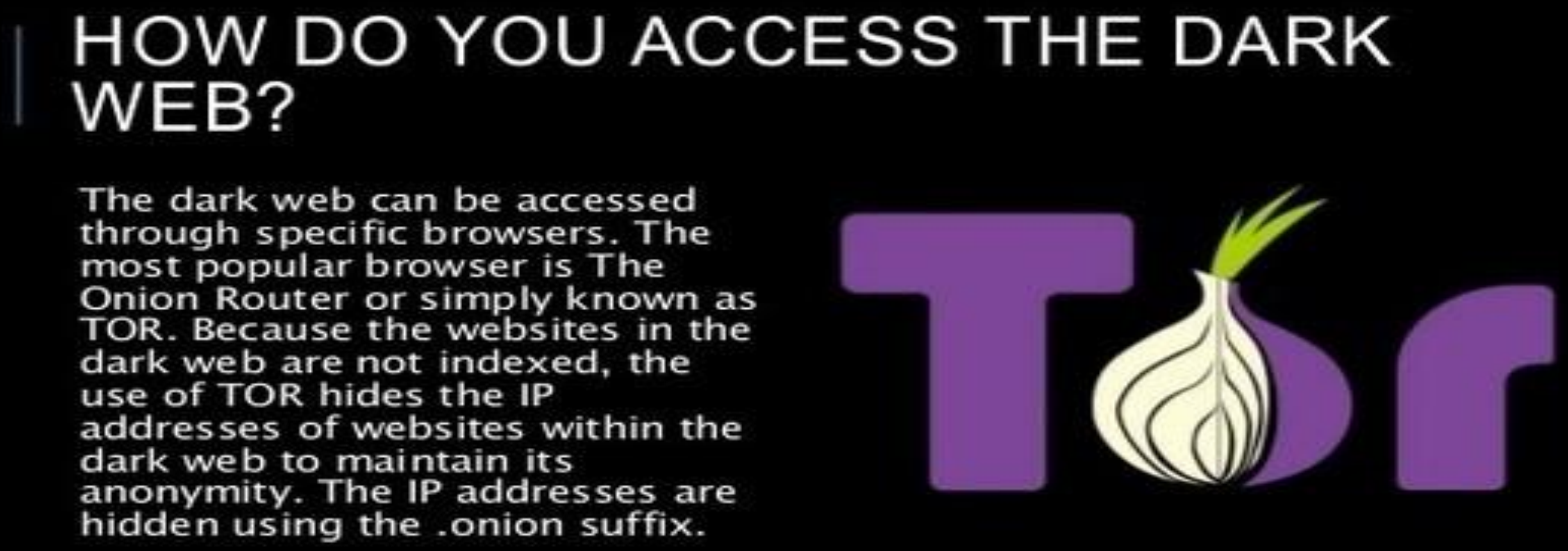
6%

Drugs

Tor

Illegal Info

How Do I Access it ? Well



HOW DO YOU ACCESS THE DARK WEB?

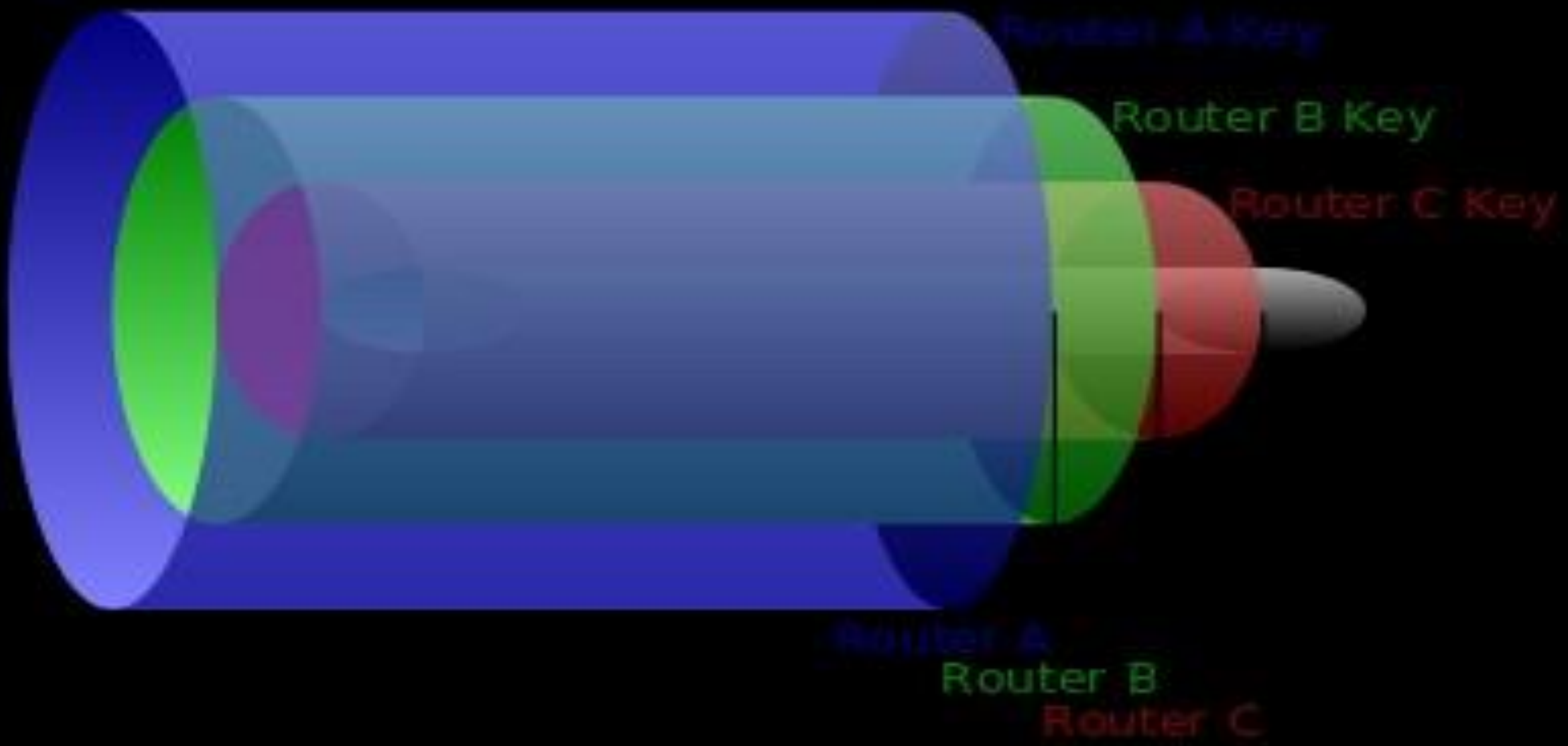
The dark web can be accessed through specific browsers. The most popular browser is The Onion Router or simply known as TOR. Because the websites in the dark web are not indexed, the use of TOR hides the IP addresses of websites within the dark web to maintain its anonymity. The IP addresses are hidden using the .onion suffix.

LETS DIVE DEEP

Tor is free software for enabling anonymous communication. Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace Internet activity to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms" Tor's intended use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

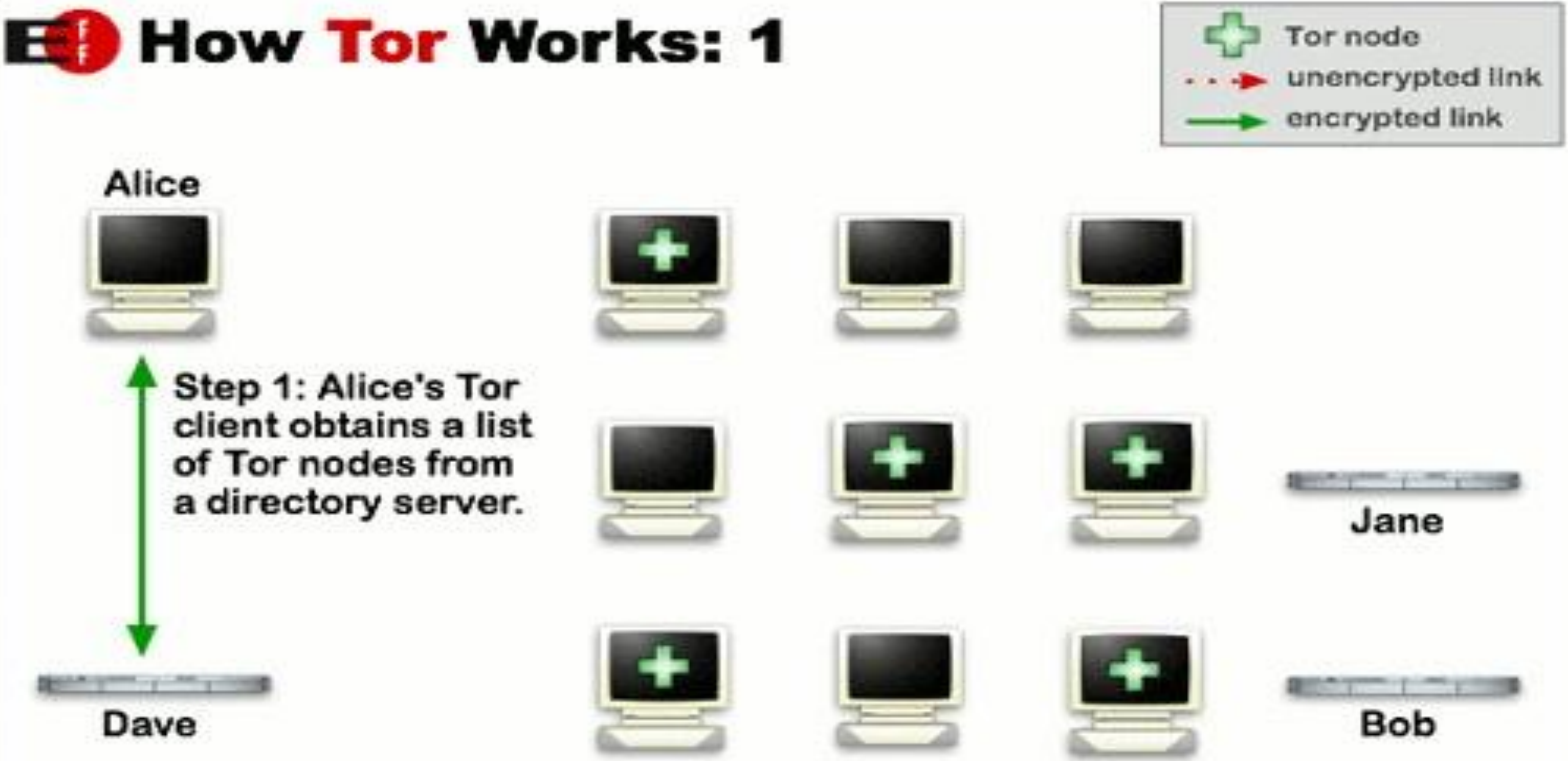
How does it work ?

Onion routing is implemented by encryption in the application layer of a communication protocol stack, nested like the layers of an onion. Tor encrypts the data, including the next node destination IP address, multiple times and sends it through a virtual circuit comprising successive, random-selection Tor relays. Each relay decrypts a layer of encryption to reveal the next relay in the circuit to pass the remaining encrypted data on to it. The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing or knowing the source IP address. Because the routing of the communication is partly concealed at every hop in the Tor circuit, this method eliminates any single point at which the communicating peers can be determined through network surveillance that relies upon knowing its source and destination


Router A Key
Router B Key
Router C Key
Router A
Router B
Router C

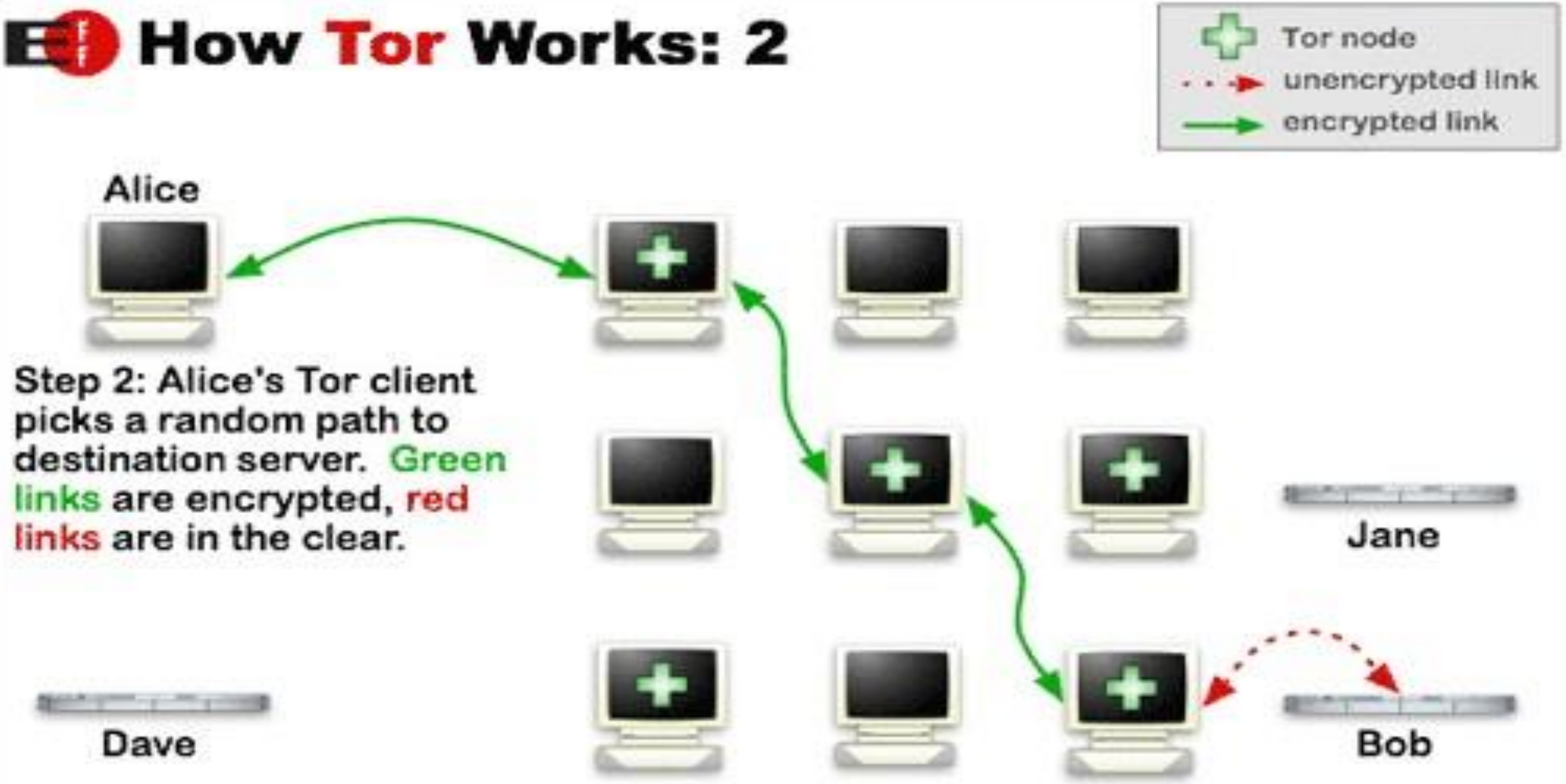
To create and transmit an onion, the originator selects a set of nodes from a list provided by a "directory node". The chosen nodes are arranged into a path, called a "chain" or "circuit", through which the message will be transmitted. To preserve the anonymity of the sender, no node in the circuit is able to tell whether the node before it is the originator or another intermediary like itself. Likewise, no node in the circuit is able to tell how many other nodes are in the circuit and only the final node, the "exit node", is able to determine its own location in the chain

How Tor Works: 1



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

How Tor Works: 2

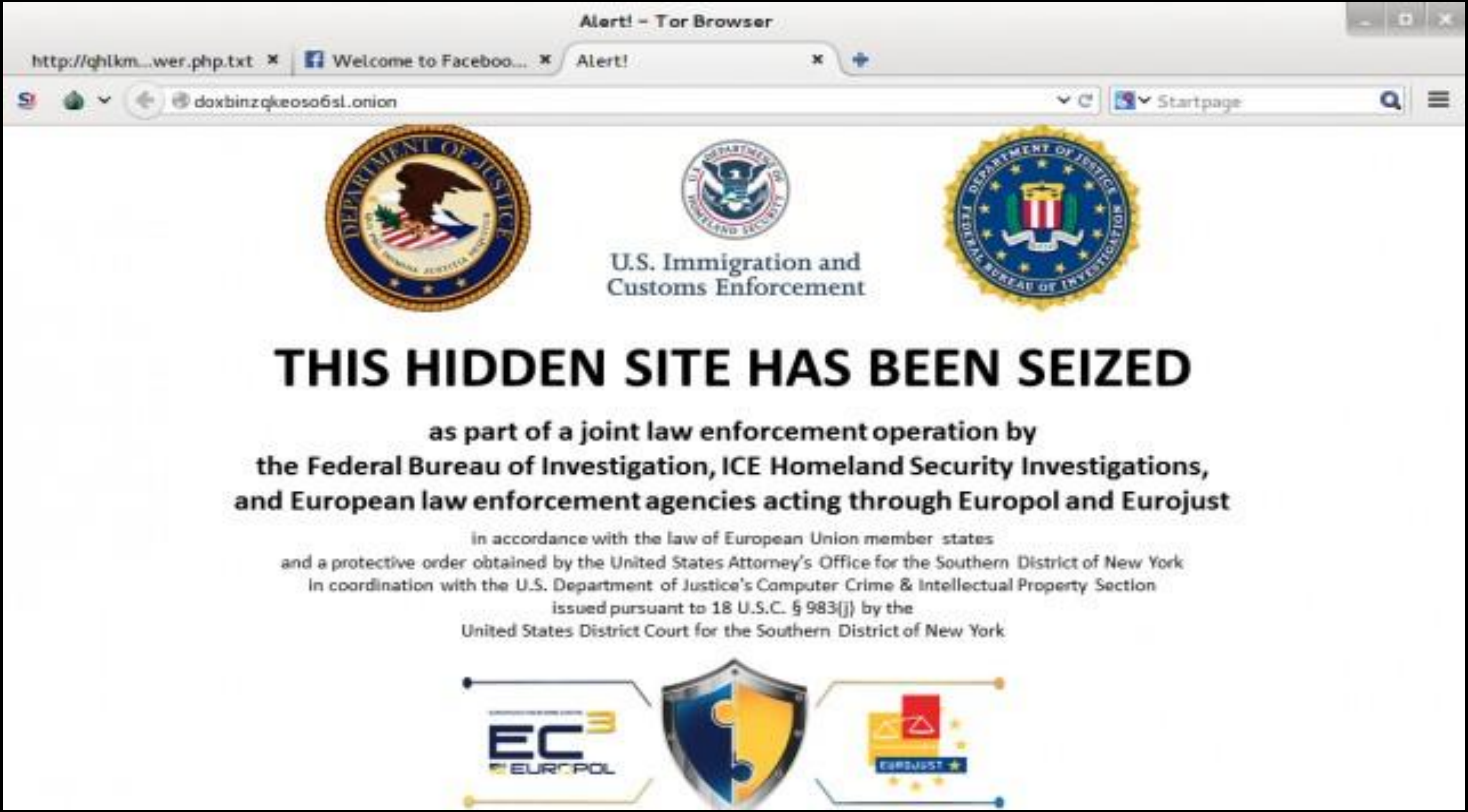


Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

THESE PRESENTATIONS ARE AWESOME
JUST KIDDING, I'M BORED
quickmeme.com

LET THE FUN
BEGIN!
makeameme.org

TOR LIVE DEMO



THIS HIDDEN SITE HAS BEEN SEIZED

as part of a joint law enforcement operation by the Federal Bureau of Investigation, ICE Homeland Security Investigations, and European law enforcement agencies acting through Europol and Eurojust

in accordance with the law of European Union member states
and a protective order obtained by the United States Attorney's Office for the Southern District of New York
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section
issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

Does TOR really makes you anonymous?

Does TOR really makes you anonymous

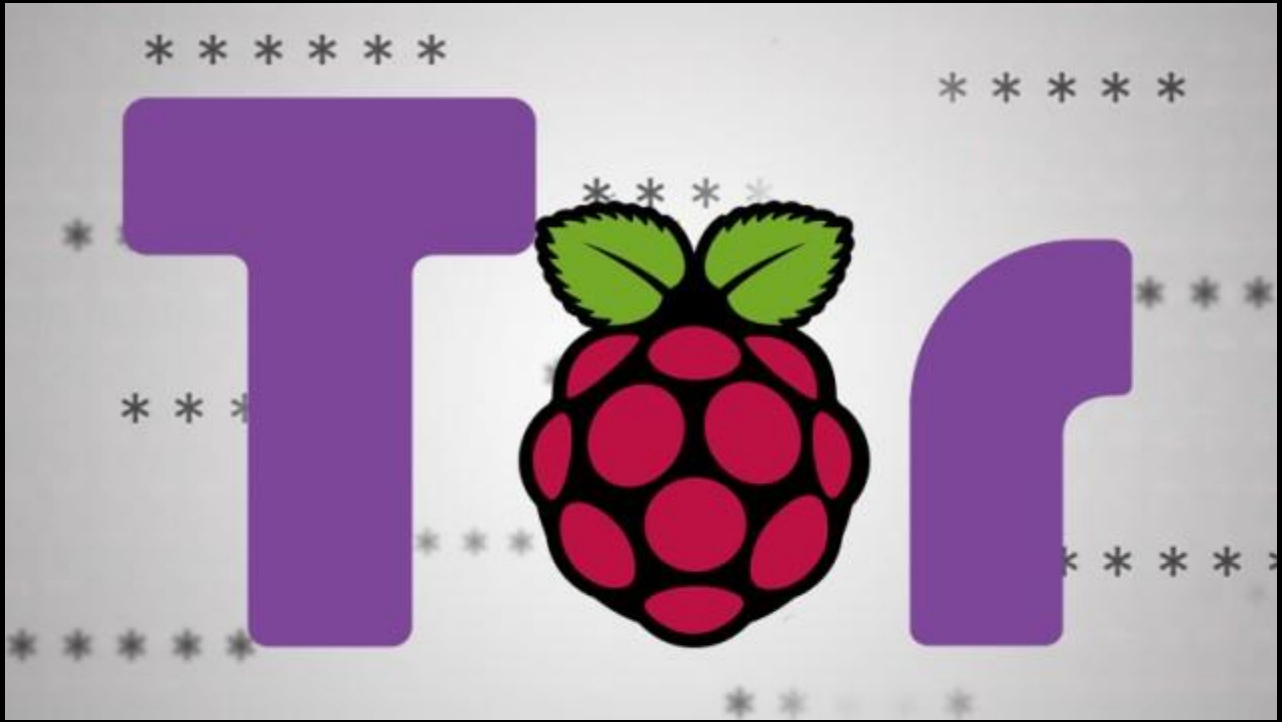
NOPE

why?

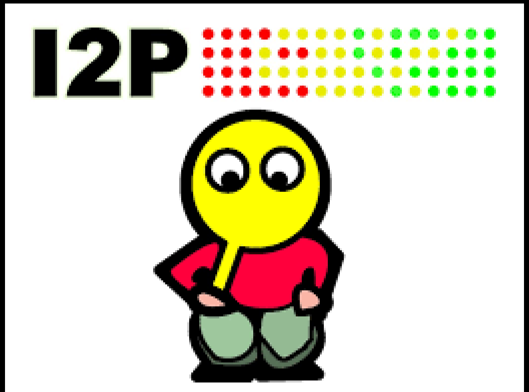
Timing analysis

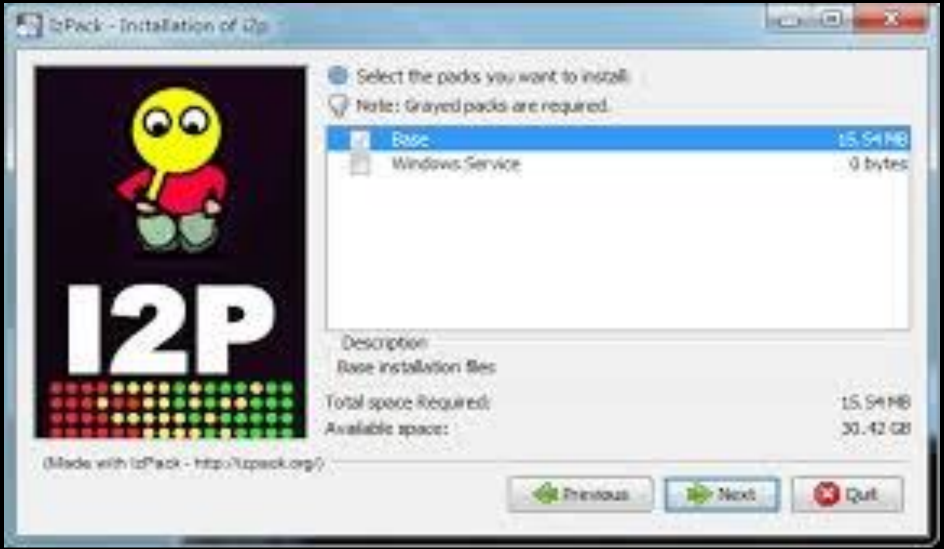
There is no protection for stupidty. NEVER USE javascript,adobe and other dynamic content while over TOR

Exit node vulnerability


T r

I2P




IzPack - Installation of i2p

Select the packs you want to install.

Note: Grayed packs are required.

☑	Base	15.54 MB
□	Windows Service	0 bytes

Description

Base installation files

Total space Required: 15.54 MB

Available space: 30.42 GB

(Made with IzPack - http://izpack.org/)

I2P

The Invisible Internet Project (I2P) is an anonymous network layer that allows for censorship-resistant, peer to peer communication. Anonymous connections are achieved by encrypting the user's traffic (by using end-to-end encryption), and sending it through a volunteer-run network of roughly 55,000 computers distributed around the world. Given the high possibility of paths the traffic can transit, a third party watching a full connection is unlikely. The software that implements this layer is called an "I2P router", and a computer running I2P is called an "I2P node". I2P is free and open source, and is published under multiple licenses.

Garlic routing

Garlic routing is a variant of onion routing that encrypts multiple messages together to make it more difficult for attackers to perform traffic analysis and to increase the speed of data transfer.

"garlic routing" as an extension of onion routing, in which multiple messages are bundled together. He called each message a "bulb", whereas I2P calls them "garlic cloves". All messages, each with its own delivery instructions, are exposed at the endpoint. This allows the efficient bundling of an onion routing "reply block" with the original message.

Aw, jeez
Not this shit again!
www.funnymemes.net

i2p demo

freenet

Freenet is a peer-to-peer platform for censorship-resistant communication. It uses a decentralized distributed data store to keep and deliver information, and has a suite of free software for publishing and communicating on the Web without fear of censorship.Both Freenet and some of its associated tools were originally designed by Ian Clarke, who defined Freenet's goal as providing freedom of speech on the Internet with strong anonymity protection

UGH! So BORED!

HERE COMES THE HOTSTEPPER

Tails
theamnesicincognitolivesystem

How really serious i am about privacy and anonymity

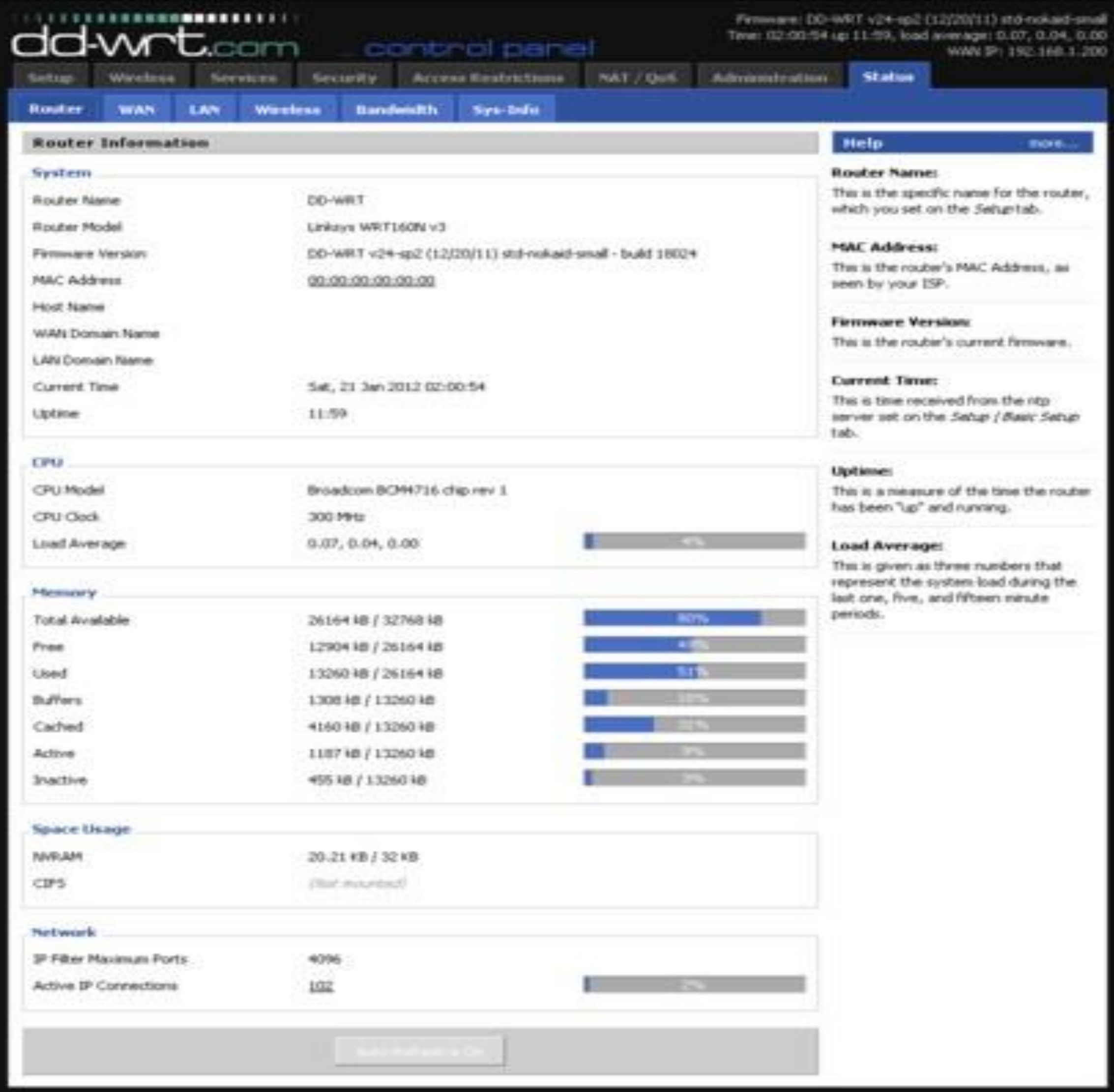
Heard of LUKS? LUKS over LVM ? LUKS NUKE?

DD-WRT
POWER TO THE ROUTER
www.DD-WRT.com

DD-WRT

DD-WRT is one of a handful of third-party firmware projects designed to replace manufacturer's original firmware with custom firmware offering additional features or functionality.

Among the standard features common to all versions of DD-WRT are: access control, bandwidth monitoring, quality of service, WPA/WPA2 (personal and enterprise), the iptables firewall, Universal Plug and Play, Wake-on-LAN, Dynamic DNS, AnchorFree VPN, wireless access point configuration, multiple SSIDs, overclocking, transmission power control, and the ability to link routers. A telnet daemon is also standard. A few examples of optional features are a wireless distribution system and support for RADIUS and XLink Kai networks. DD-WRT's support for OpenVPN, WireGuard enables both protocols to pass all network traffic through a virtual private network



Firmware: DD-WRT v24-sp2 (12/20/11) std-nokaid-small
Time: 02:00:54 up 11:59, load average: 0.07, 0.04, 0.00
WAN IP: 192.168.1.200

Router Information

System

Router Name	DD-WRT	
Router Model	Linksys WRT160N v3	
Firmware Version	DD-WRT v24-sp2 (12/20/11) std-nokaid-small - build 18024	
MAC Address	00:00:00:00:00:00	
Host Name		
WAN Domain Name		
LAN Domain Name		
Current Time	Sat, 21 Jan 2012 02:00:54	
Uptime	11:59	

CPU

CPU Model	Broadcom BCM4716 chip rev 1	
CPU Clock	300 MHz	
Load Average	0.07, 0.04, 0.00	4%

Memory

Total Available	26164 kB / 32768 kB	80%
Free	12904 kB / 26164 kB	49%
Used	13260 kB / 26164 kB	51%
Buffers	1308 kB / 13260 kB	10%
Cached	4160 kB / 13260 kB	31%
Active	1187 kB / 13260 kB	9%
Inactive	455 kB / 13260 kB	3%

Space Usage

NVRAM	20.21 KB / 32 KB	
CIFS	(Not mounted)	

Network

IP Filter Maximum Ports	4096	
Active IP Connections	102	2%

Router Name:
This is the specific name for the router, which you set on the *Setup* tab.

MAC Address:
This is the router's MAC Address, as seen by your ISP.

Firmware Version:
This is the router's current firmware.

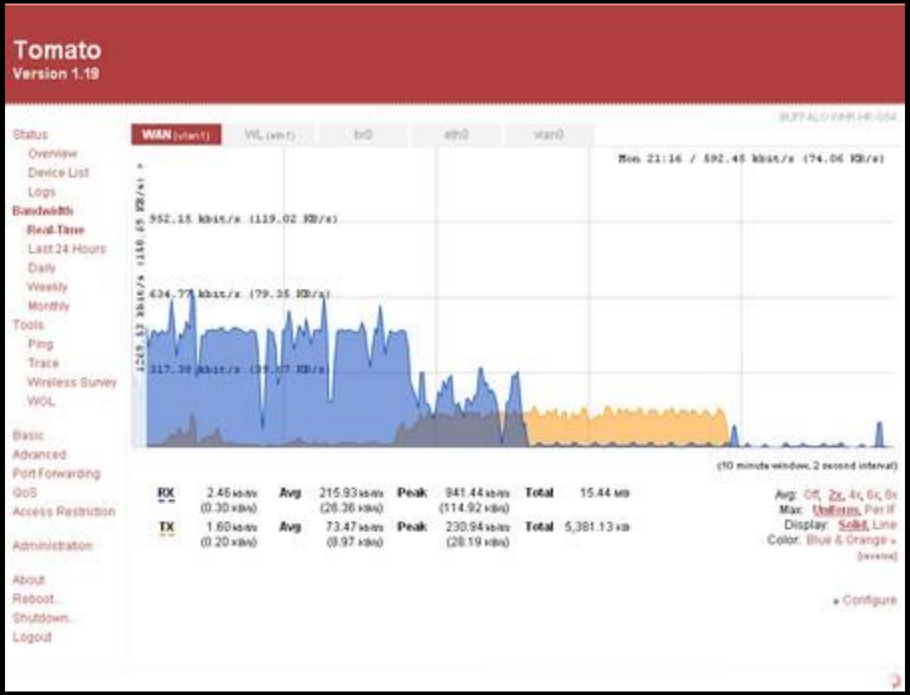
Current Time:
This is time received from the ntp server set on the *Setup / Basic Setup* tab.

Uptime:
This is a measure of the time the router has been "up" and running.

Load Average:
This is given as three numbers that represent the system load during the last one, five, and fifteen minute periods.

Tomato

Tomato is a partially free HyperWRT-based, Linux core firmware distribution for a range of Broadcom chipset based wireless routers, most notably the older Linksys WRT54G series, Buffalo AirStation, Asus routers and Netgear WNR3500L. Among other notable features is the user interface, which makes heavy use of Ajax as well as an SVG-based graphical bandwidth monitor.



RX	2.46 kbit/s (0.30 KB/s)	Avg	215.93 kbit/s (26.36 KB/s)	Peak	941.44 kbit/s (114.92 KB/s)	Total	15.44 MB
TX	1.60 kbit/s (0.20 KB/s)	Avg	73.47 kbit/s (8.97 KB/s)	Peak	230.94 kbit/s (28.19 KB/s)	Total	5,381.13 KB

Features

Netfilter/iptables with customizable settings, IPP2P and l7-filter,SMB client,Advanced port forwarding, redirection, and triggering with UPnP and NAT-PMP,

SNORT

Snort and hardening of ip tables

Snort's open source network-based intrusion detection system (IDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching and matching.

The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, semantic URL attacks, buffer overflows, server message block probes, and stealth port scans.

Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified.

IPTABLES

This Linux based firewall is controlled by the program called iptables to handles filtering for IPv4, and ip6tables handles filtering for IPv6.

https://haveibeenpwned.com/

Do you guys know about this site ?

check your mail ids

DO NOT reuse passwords

anonymizer scripts

https://github.com/ruped24/toriptables2

https://github.com/Hackplyers/4nonimizer

https://github.com/ParrotSec/anonsurf/blob/master/anonsurf.sh

and so many more

VPNS proxies and all other shits

USE A PAID VPN service if something is given for free the item being sold is you or find a good free vpn list (you will find it eventually and you will know when you have found it)

Will i say what I am using and showing you my dump of free ultra anonymmous proxies or how i compile fresh list of proxies : NOPE

Proxychains-ng

proxychains-ng is a proxy server that supports HTTP (S), SOCKS 4 and SOCKS5 internet protocols, works on Linux / GNU, BSD and Mac OS X distributions (Unix platforms). Proxychains-ng allows any TCP connection made by a given program to follow a series of proxies (from the mentioned protocols) to its destination. The list of proxies is defined beforehand.

Proxychains is written in C

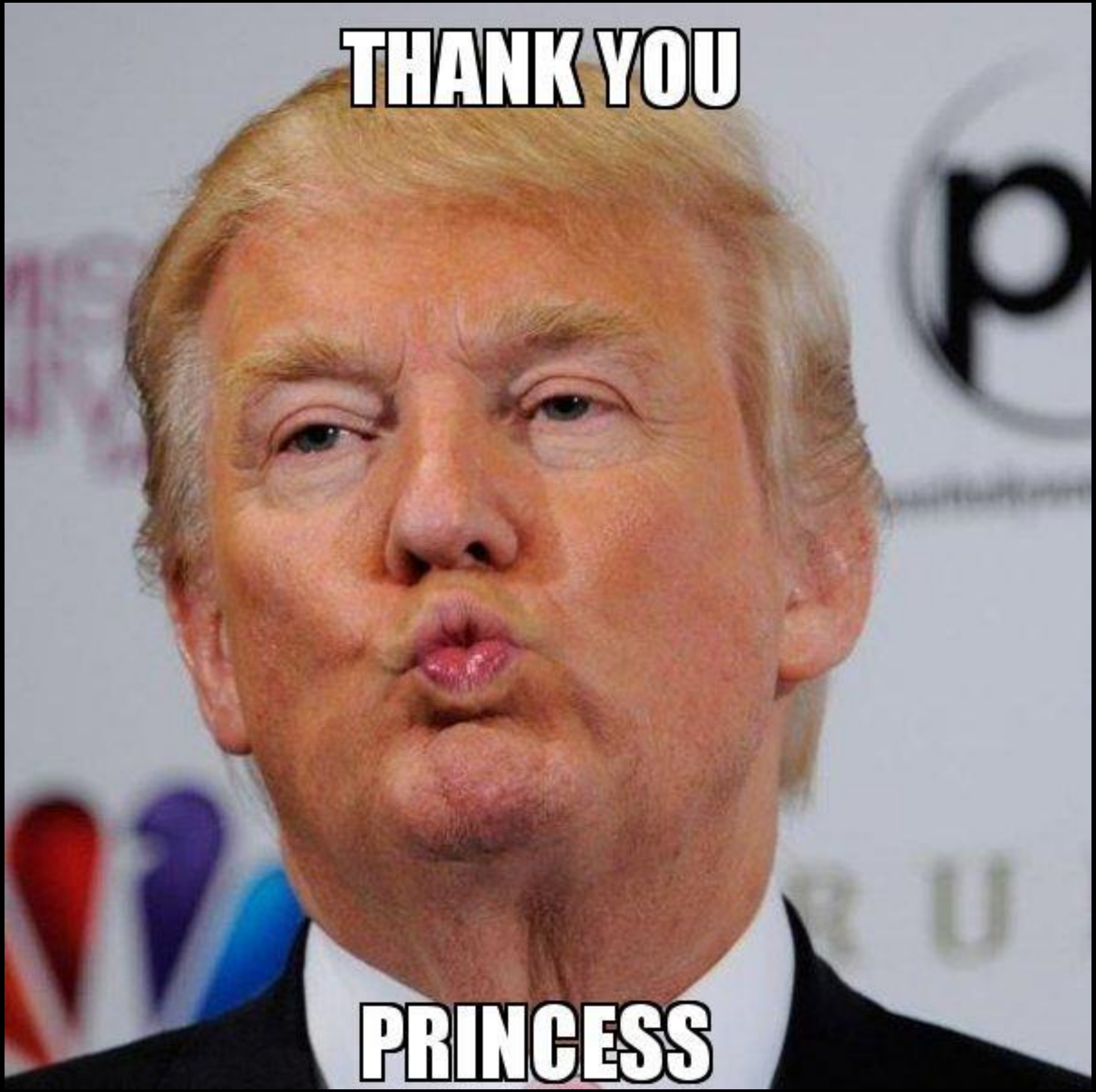
Features

The possibility to link several types of proxies at the same time HTTP-SOCKS4 - SOCKS5

Different chaining options: random (random), strict (Strict), dynamic (dynamic), random.

Resolve DNS (UDP) requests through proxy.

Set the length of the chain (number of chained proxies).



THANK YOU
PRINCESS

Questions? Comments? Feedback