Welcome to Today's
IRS Web Conference

# Understanding the Basics of the Dark Web

Philip Yamalis
Stakeholder Liaison

The original live broadcast of this web conference included an interactive polling feature which is disabled in this archived version.

IRS

Media: SBSE.SL.Web.Conference.Team@IRS.gov

## Internal Revenue Service

# Cyber Crimes

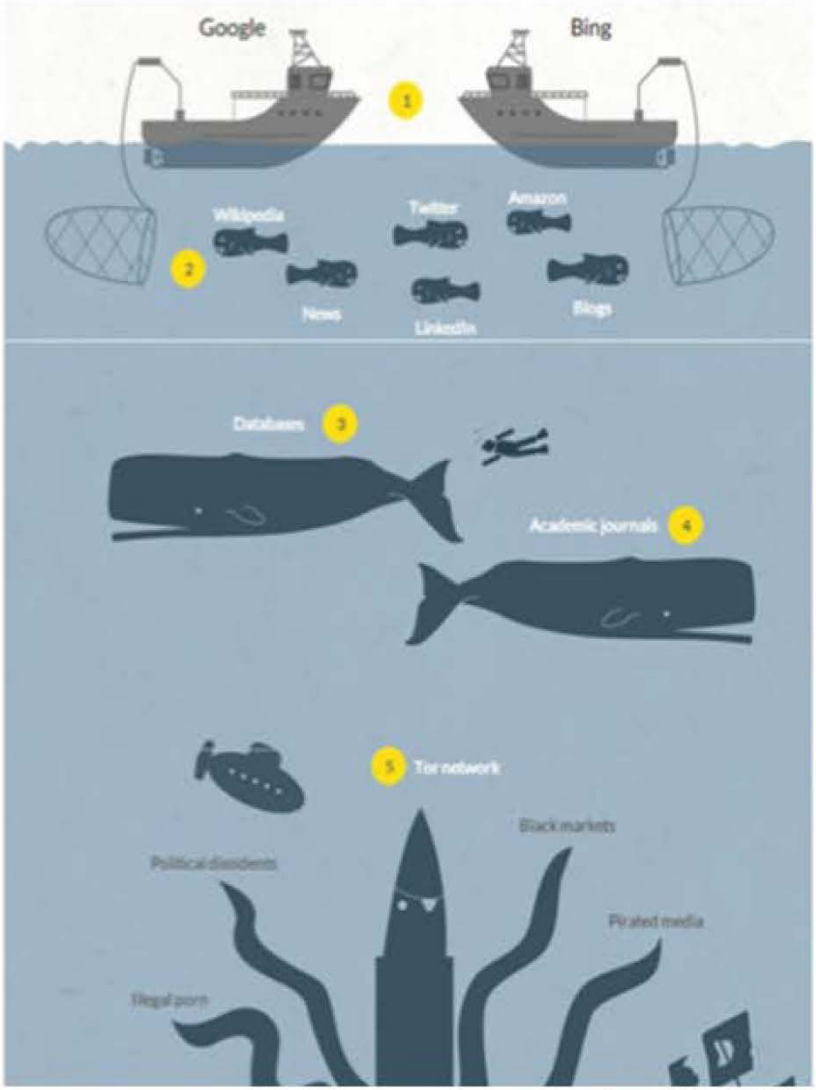
## James Daniels

# Deep/Dark Web

## Surface Web v Deep Web v Dark Web

**Surface Web**
Social media sites, sites indexed by search engines

**Deep Web**
Private databases, forums, password protected sites



Graphic: CNN

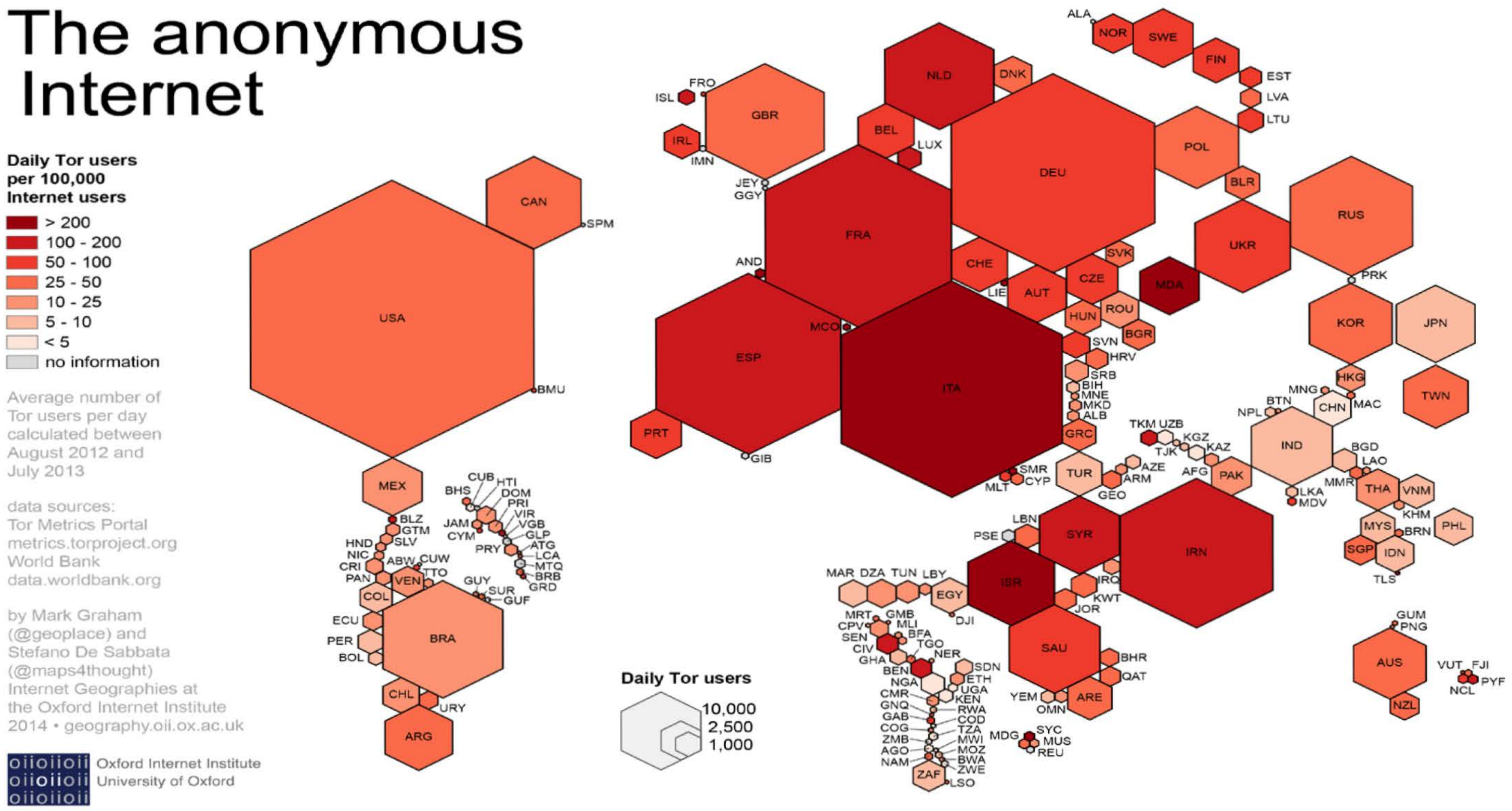
**Dark Web**
Only accessible via special software; intentionally hidden; anonymous

# Surface Web

# Deep Web

# Dark Web

# Dark Web



## The anonymous Internet

**Daily Tor users per 100,000 Internet users**

- ■ > 200
- ■ 100 - 200
- ■ 50 - 100
- ■ 25 - 50
- ■ 10 - 25
- ■ 5 - 10
- ■ < 5
- ■ no information

Average number of Tor users per day calculated between August 2012 and July 2013

data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org

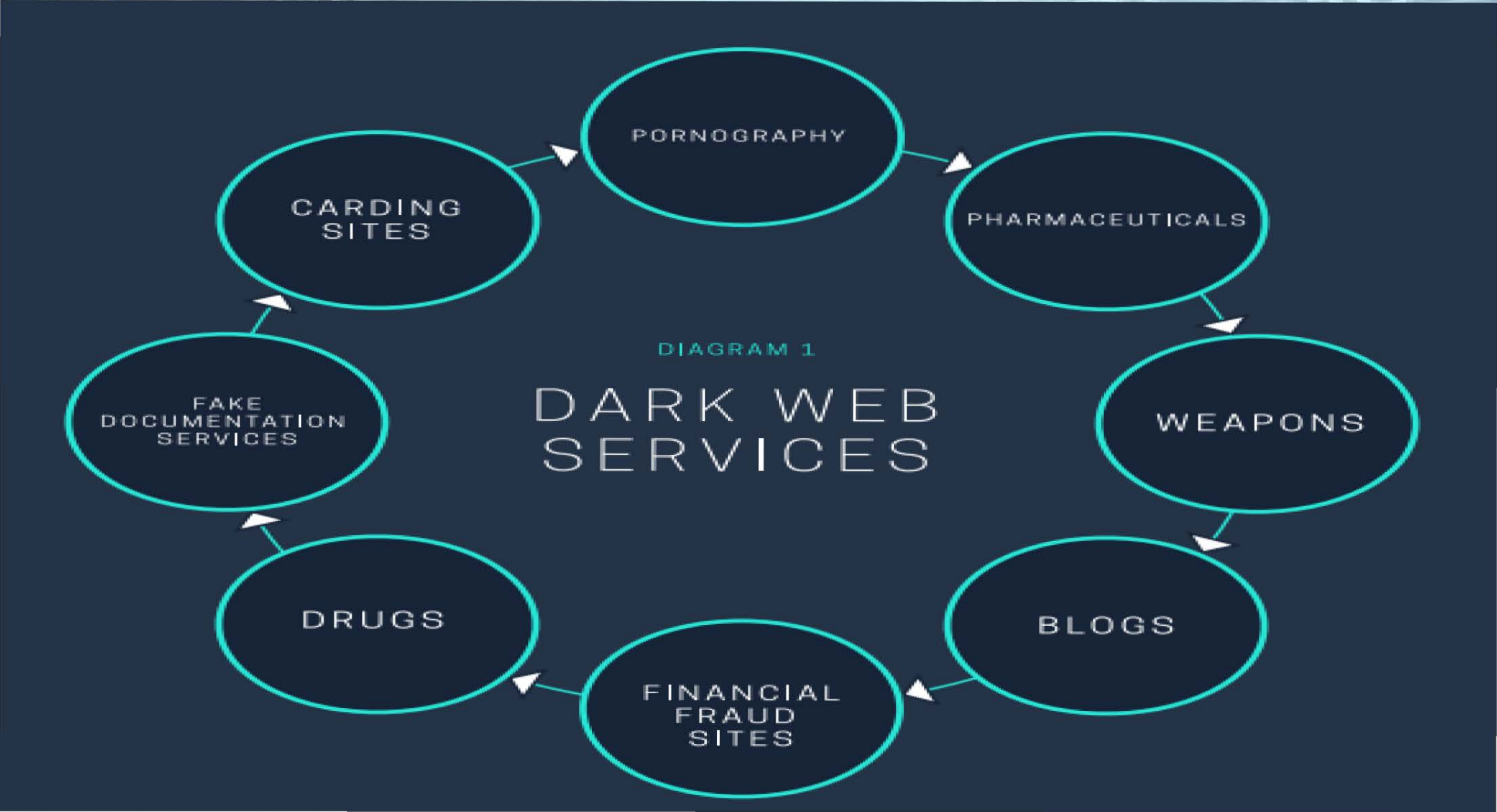
by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
2014 • geography.oii.ox.ac.uk

Oxford Internet Institute
University of Oxford

**Daily Tor users**

10,000
2,500
1,000

# Dark Web


PORNOGRAPHY
PHARMACEUTICALS
WEAPONS
BLOGS
FINANCIAL FRAUD SITES
DRUGS
FAKE DOCUMENTATION SERVICES
CARDING SITES
DIAGRAM 1
DARK WEB SERVICES

# Polling Question

What type of activities occur on the Dark Web?

a) Drug sales

b) Weapon sales

c) Money laundering

d) All of the above

# Accessing the Dark Web

- Requires software running on computer or Tails and usb
  - The Onion Router (Tor) is most popular
  - Others include:1P2 and Freenet
- Uses encryption and proxies/relays to conceal a user's location and usage
  - More than 2.5 million daily users

Tor

https://www.torproject.org/

I2P

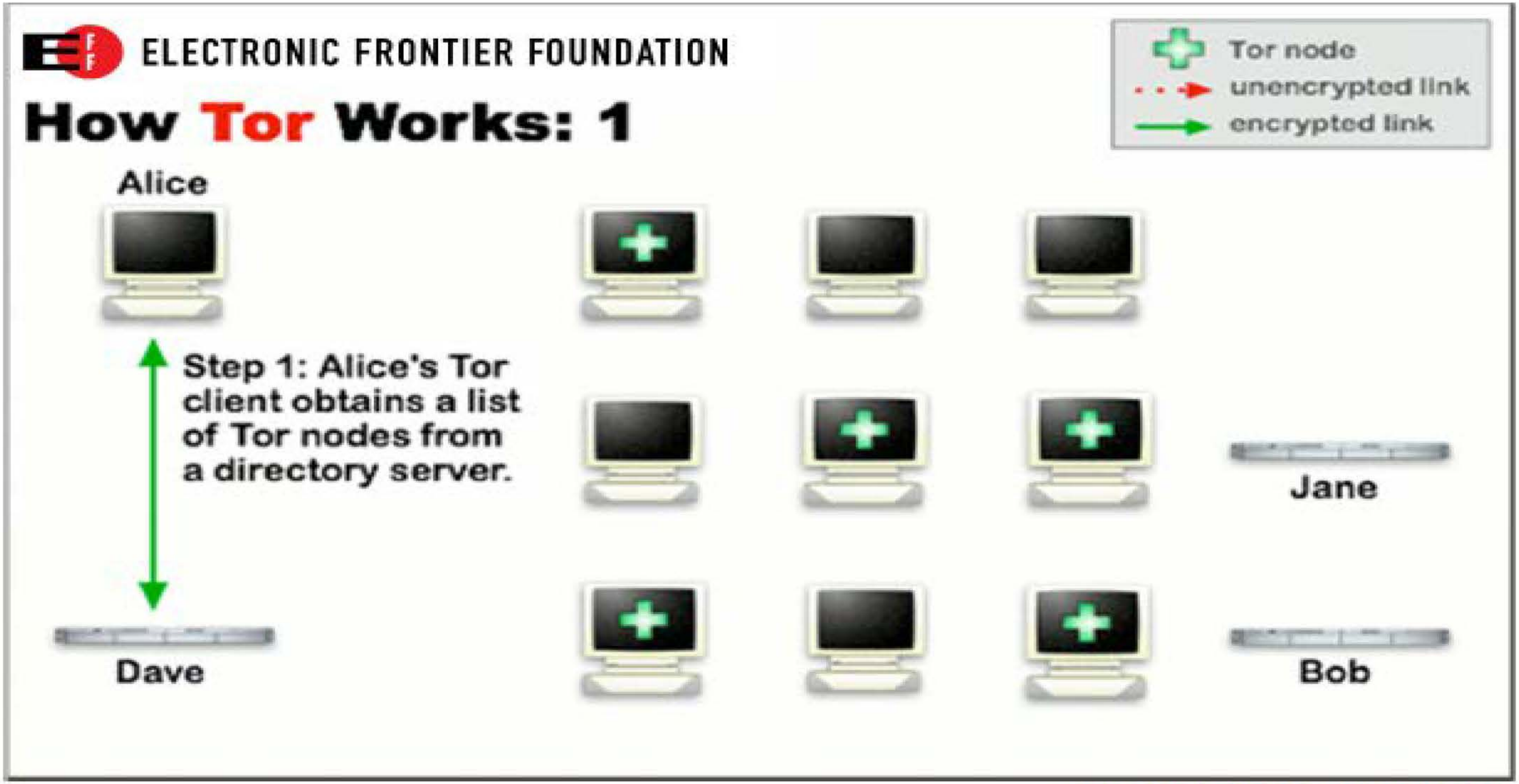
https://geti2p.net/en/

The Freenet Project

https://freenetproject.org/

The remainder of the presentation will focus on Tor; however, the same concepts apply to the others

# How Tor Works



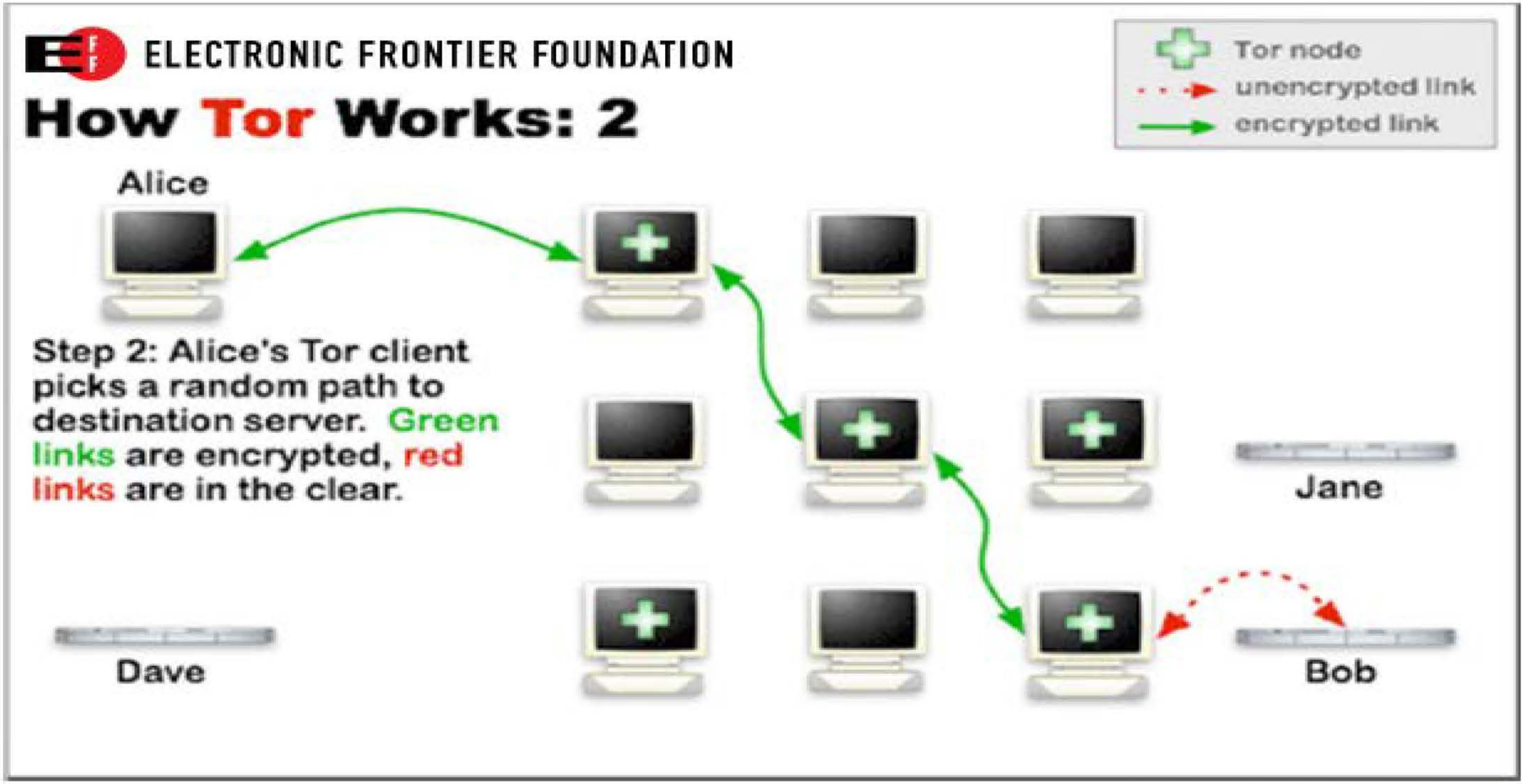
ELECTRONIC FRONTIER FOUNDATION

How Tor Works: 1

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

Graphic: www.torproject.org

# How Tor Works



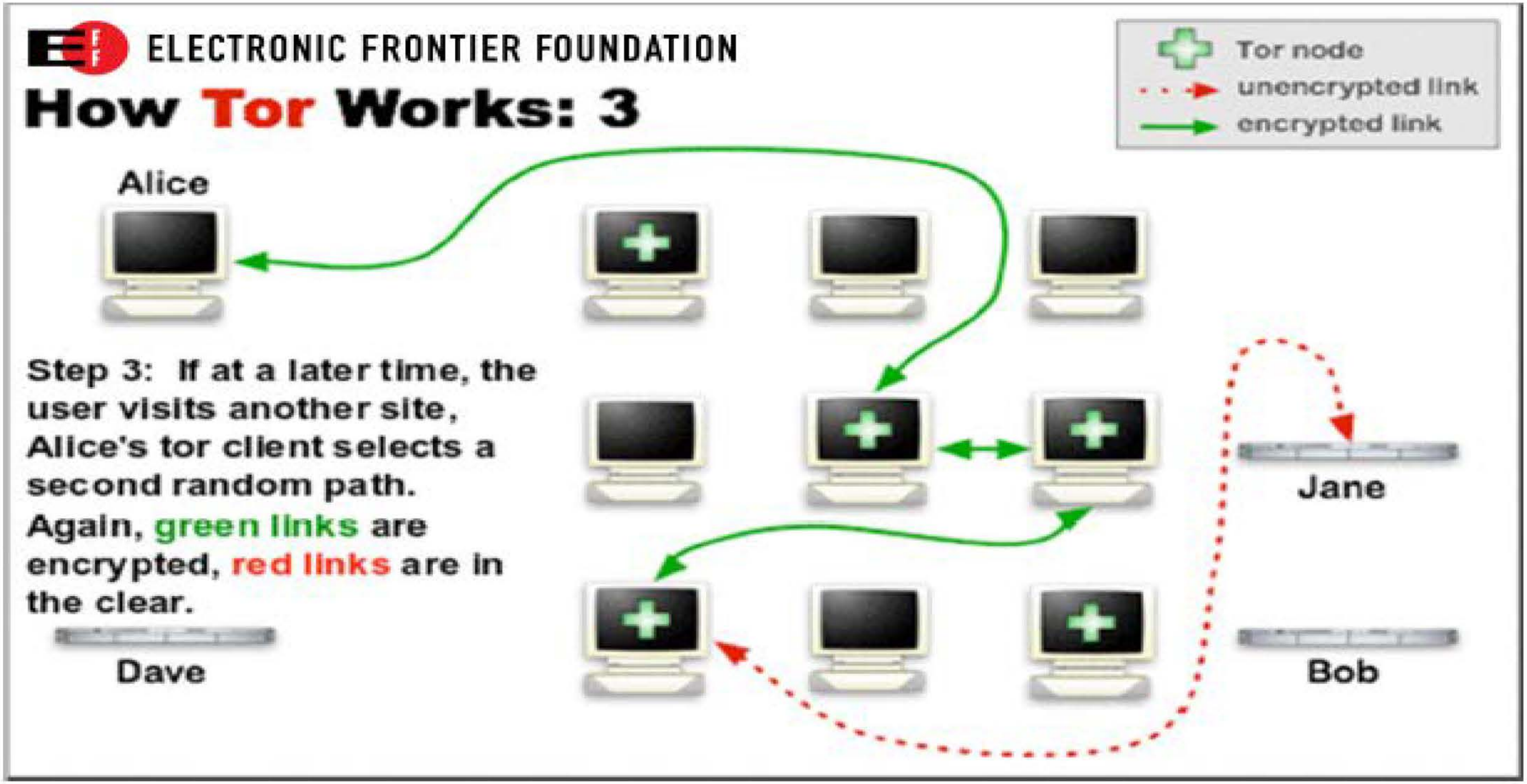
ELECTRONIC FRONTIER FOUNDATION

**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.

Graphic: www.torproject.org

# How Tor Works



ELECTRONIC FRONTIER FOUNDATION

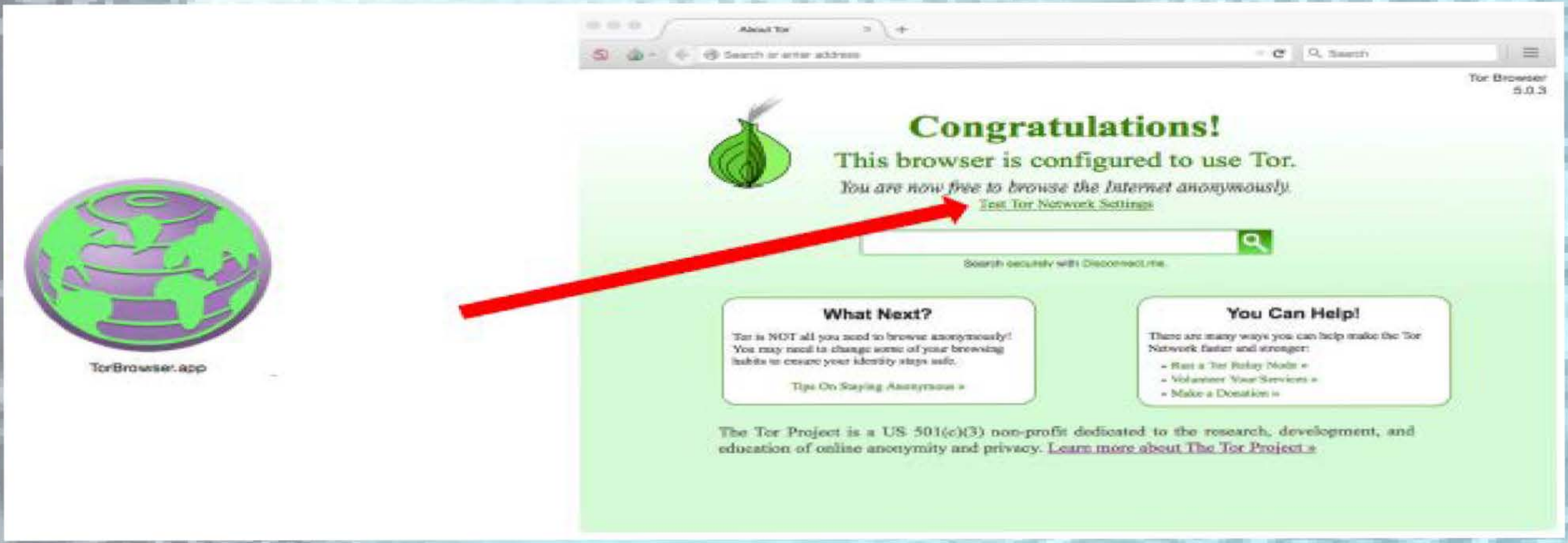
How Tor Works: 3

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.

Graphic: www.torproject.org

# Tor Browser

- **Web browser based on Mozilla Firefox and pre-configured to protect your anonymity (Tor, scripting disabled, plugins, etc.)**



Congratulations!

This browser is configured to use Tor.

*You are now free to browse the Internet anonymously.*

Test Tor Network Settings

Search securely with Disconnect.me.

**What Next?**

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

**You Can Help!**

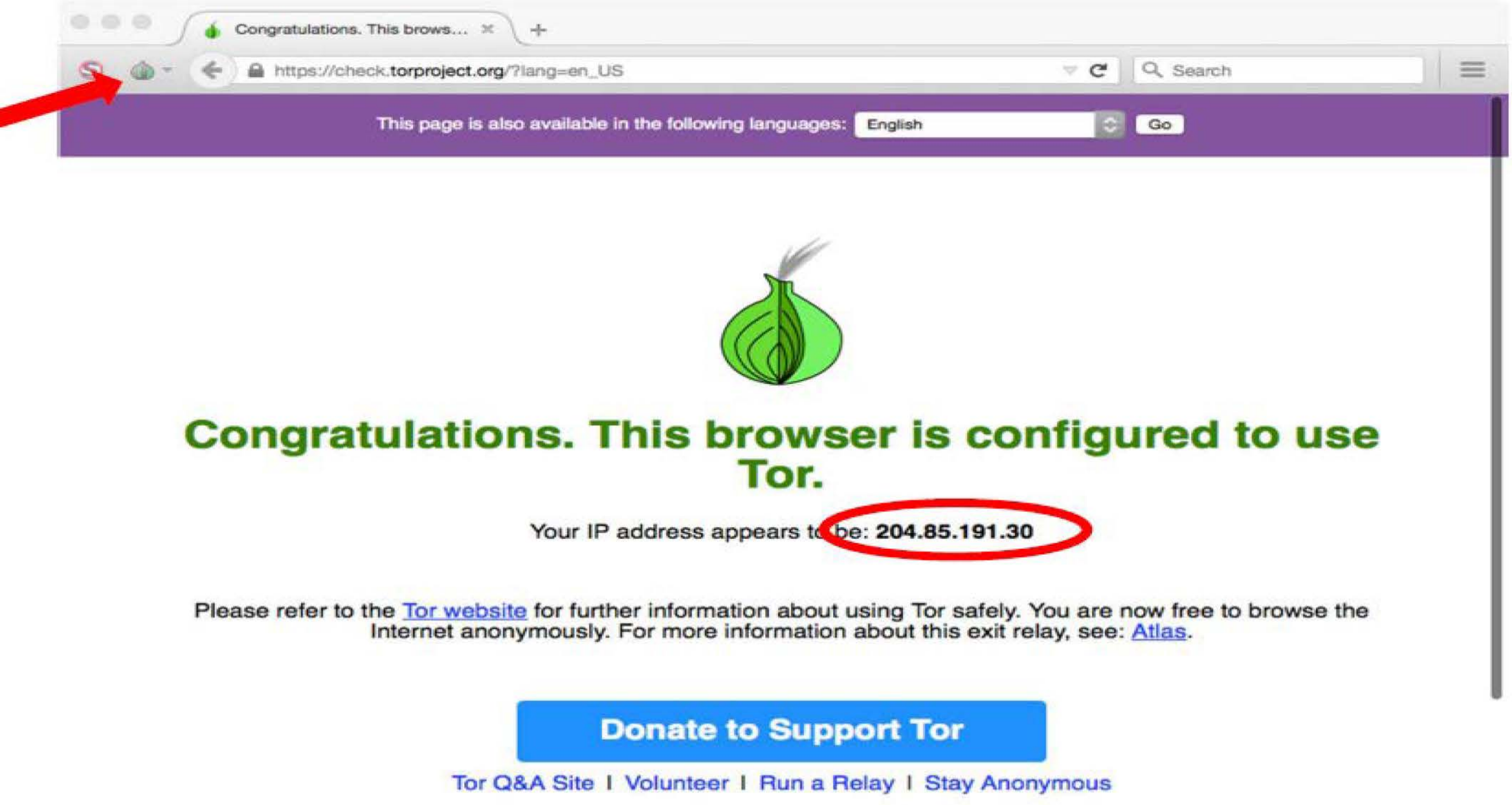
There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

- **Note: does not protect your computer from malware, viruses, etc.**

# Tor Browser



Congratulations. This brows...
https://check.torproject.org/?lang=en_US
Search

This page is also available in the following languages: English Go

## Congratulations. This browser is configured to use Tor.

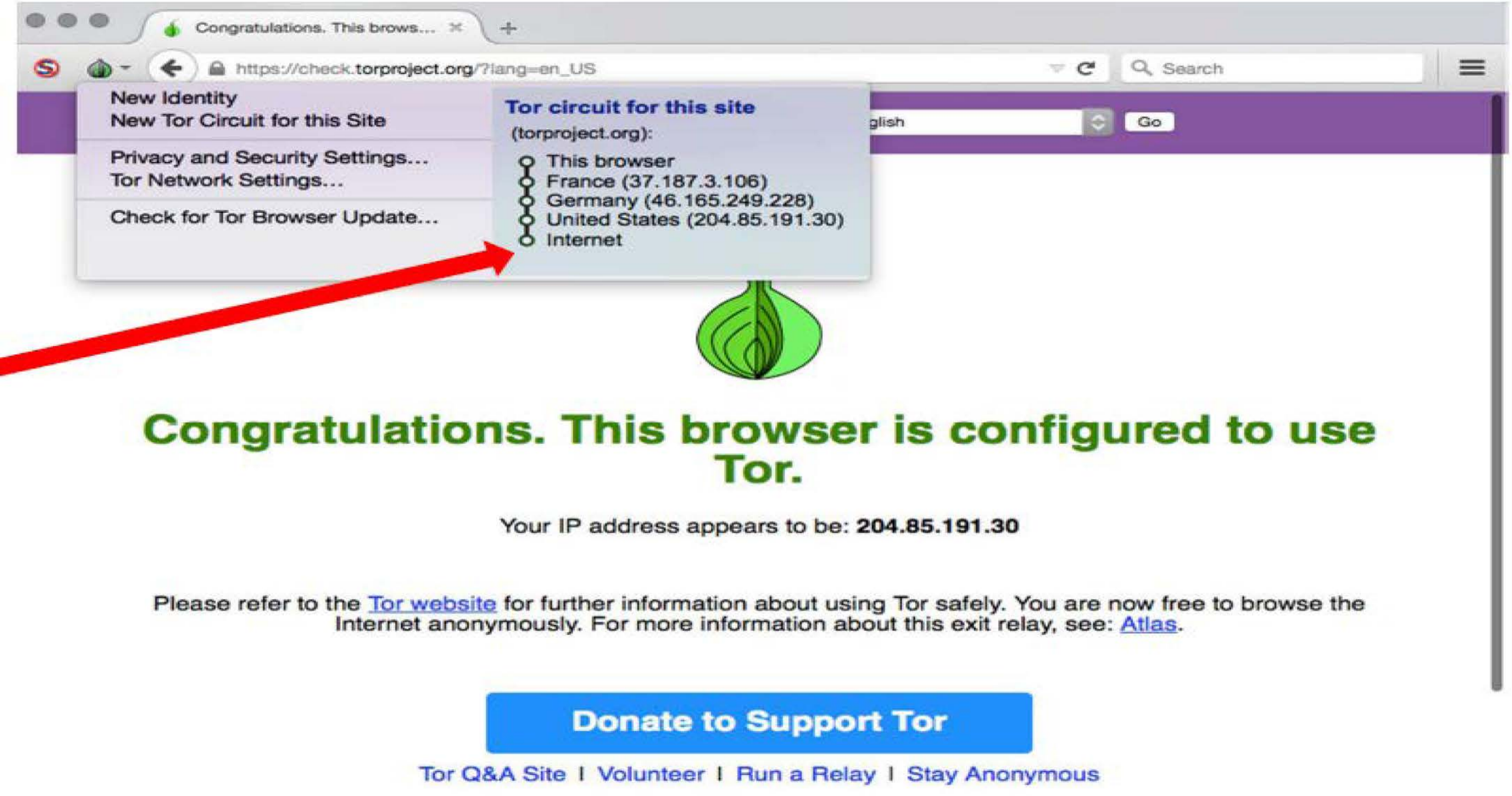
Your IP address appears to be: **204.85.191.30**

Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: Atlas.

**Donate to Support Tor**

Tor Q&A Site | Volunteer | Run a Relay | Stay Anonymous

# Tor Browser


Congratulations. This brows...
https://check.torproject.org/?lang=en_US
Search
New Identity
New Tor Circuit for this Site
Privacy and Security Settings...
Tor Network Settings...
Check for Tor Browser Update...
glish
Go
Donate to Support Tor
Tor Q&A Site | Volunteer | Run a Relay | Stay Anonymous

Tor circuit for this site (torproject.org):

- This browser
- France (37.187.3.106)
- Germany (46.165.249.228)
- United States (204.85.191.30)
- Internet

Congratulations. This browser is configured to use Tor.

Your IP address appears to be: **204.85.191.30**

Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: Atlas.

# Polling Question

The Dark Web can be accessed through which web browser?

a) Chrome

b) Firefox

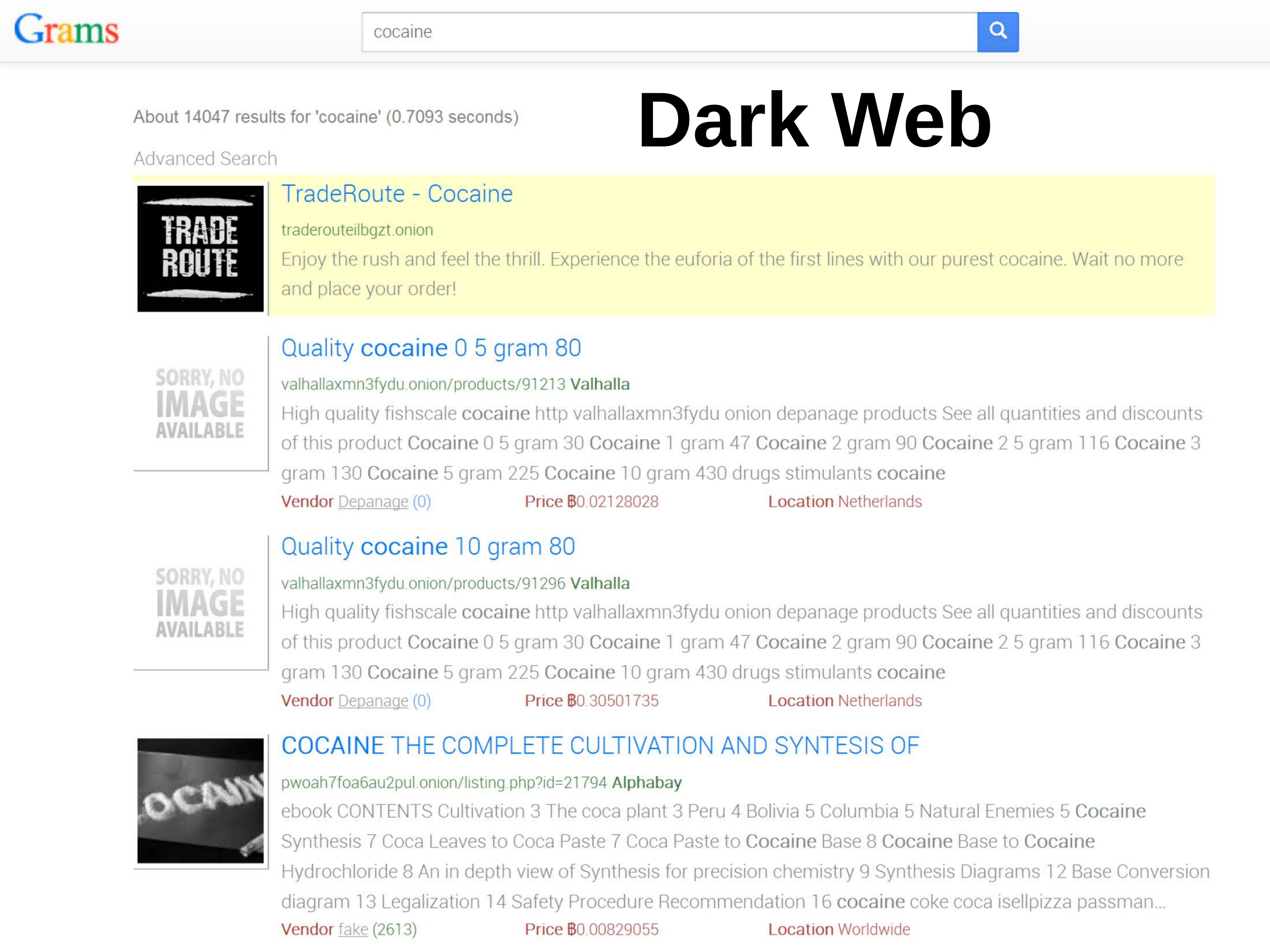
c) Tor

d) Explorer

# Searching the Dark Web

- Onion URL Repository
- Uncensored Hidden Wiki
- notEvil
- ParaZite
- TorLinks

# Dark Web



About 14047 results for 'cocaine' (0.7093 seconds)

Advanced Search

TradeRoute - Cocaine

traderouteilbgzt.onion

Enjoy the rush and feel the thrill. Experience the euforia of the first lines with our purest cocaine. Wait no more and place your order!

Quality **cocaine** 0 5 gram 80

valhallaxmn3fydu.onion/products/91213 **Valhalla**

High quality fishscale **cocaine** http valhallaxmn3fydu onion depanage products See all quantities and discounts of this product **Cocaine** 0 5 gram 30 **Cocaine** 1 gram 47 **Cocaine** 2 gram 90 **Cocaine** 2 5 gram 116 **Cocaine** 3 gram 130 **Cocaine** 5 gram 225 **Cocaine** 10 gram 430 drugs stimulants **cocaine**

Vendor Depanage (0) Price ฿0.02128028 Location Netherlands

Quality **cocaine** 10 gram 80

valhallaxmn3fydu.onion/products/91296 **Valhalla**

High quality fishscale **cocaine** http valhallaxmn3fydu onion depanage products See all quantities and discounts of this product **Cocaine** 0 5 gram 30 **Cocaine** 1 gram 47 **Cocaine** 2 gram 90 **Cocaine** 2 5 gram 116 **Cocaine** 3 gram 130 **Cocaine** 5 gram 225 **Cocaine** 10 gram 430 drugs stimulants **cocaine**

Vendor Depanage (0) Price ฿0.30501735 Location Netherlands

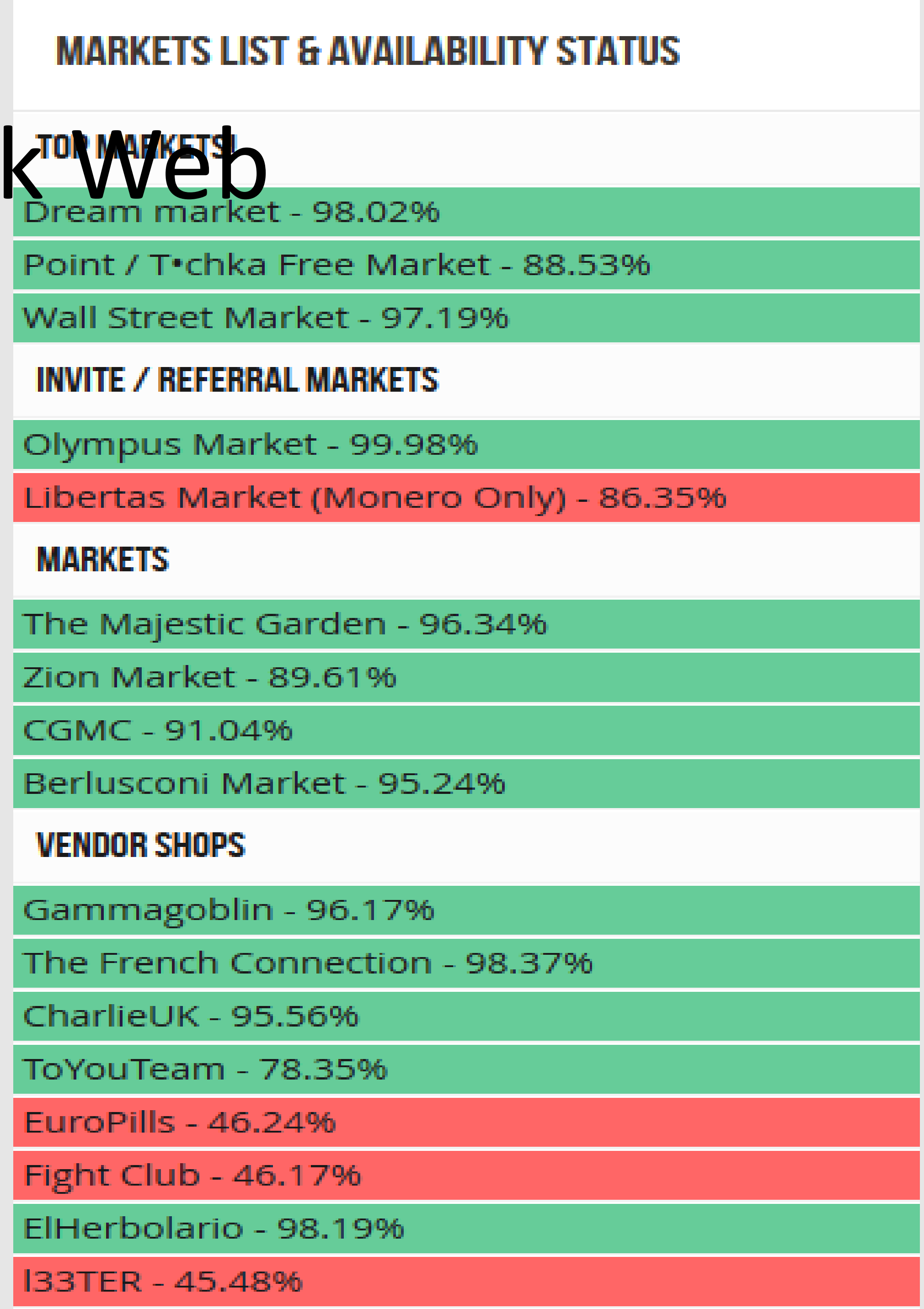
**COCAINE** THE COMPLETE CULTIVATION AND SYNTESIS OF

pwoah7foa6au2pul.onion/listing.php?id=21794 **Alphabay**

ebook CONTENTS Cultivation 3 The coca plant 3 Peru 4 Bolivia 5 Columbia 5 Natural Enemies 5 **Cocaine** Synthesis 7 Coca Leaves to Coca Paste 7 Coca Paste to **Cocaine** Base 8 **Cocaine** Base to **Cocaine** Hydrochloride 8 An in depth view of Synthesis for precision chemistry 9 Synthesis Diagrams 12 Base Conversion diagram 13 Legalization 14 Safety Procedure Recommendation 16 **cocaine** coke coca isellpizza passman...

Vendor fake (2613) Price ฿0.00829055 Location Worldwide

# Dark Web



## MARKETS LIST & AVAILABILITY STATUS

### TOR MARKETS

🟩 Dream market - 98.02%

🟩 Point / T•chka Free Market - 88.53%

🟩 Wall Street Market - 97.19%

### INVITE / REFERRAL MARKETS

🟩 Olympus Market - 99.98%

🟥 Libertas Market (Monero Only) - 86.35%

### MARKETS

🟩 The Majestic Garden - 96.34%

🟩 Zion Market - 89.61%

🟩 CGMC - 91.04%

🟩 Berlusconi Market - 95.24%

### VENDOR SHOPS

🟩 Gammagoblin - 96.17%

🟩 The French Connection - 98.37%

🟩 CharlieUK - 95.56%

🟩 ToYouTeam - 78.35%

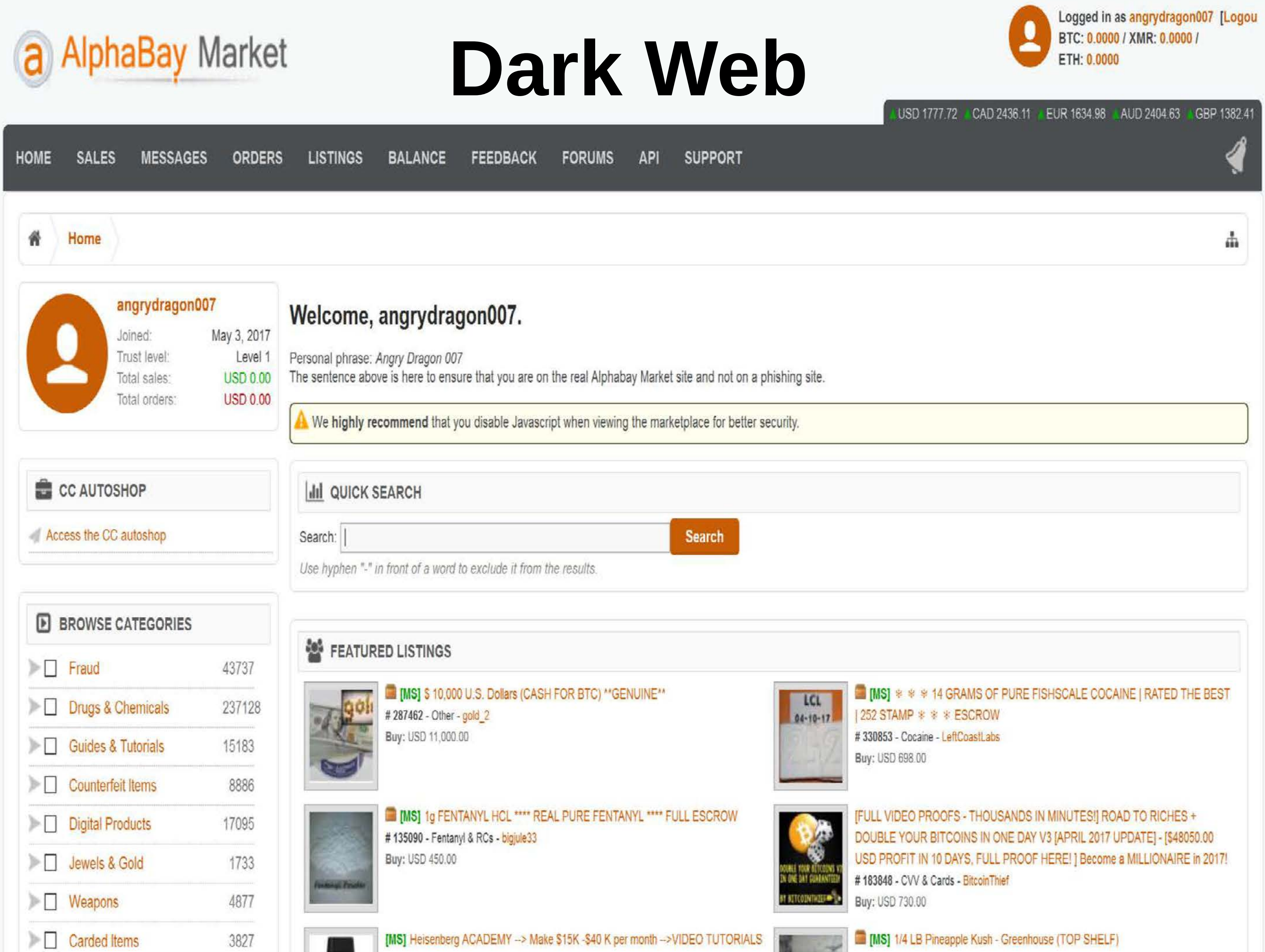
🟥 EuroPills - 46.24%

🟥 Fight Club - 46.17%

🟩 ElHerbolario - 98.19%

🟥 l33TER - 45.48%

# Dark Web



AlphaBay Market

Logged in as angrydragon007 [Logou

BTC: 0.0000 / XMR: 0.0000 /

ETH: 0.0000

USD 1777.72 CAD 2436.11 EUR 1634.98 AUD 2404.63 GBP 1382.41

angrydragon007

|  |  |
|---|---|
| Joined: | May 3, 2017 |
| Trust level: | Level 1 |
| Total sales: | USD 0.00 |
| Total orders: | USD 0.00 |

## Welcome, angrydragon007.

Personal phrase: *Angry Dragon 007*

The sentence above is here to ensure that you are on the real Alphabay Market site and not on a phishing site.

⚠ We **highly recommend** that you disable Javascript when viewing the marketplace for better security.

### CC AUTOSHOP

Access the CC autoshop

### QUICK SEARCH

Search: | Search

*Use hyphen "-" in front of a word to exclude it from the results.*

### BROWSE CATEGORIES

|  |  |
|---|---|
| □ Fraud | 43737 |
| □ Drugs & Chemicals | 237128 |
| □ Guides & Tutorials | 15183 |
| □ Counterfeit Items | 8886 |
| □ Digital Products | 17095 |
| □ Jewels & Gold | 1733 |
| □ Weapons | 4877 |
| □ Carded Items | 3827 |

### FEATURED LISTINGS

[MS] $ 10,000 U.S. Dollars (CASH FOR BTC) **GENUINE**
# 287462 - Other - gold_2
Buy: USD 11,000.00

[MS] ✻ ✻ ✻ 14 GRAMS OF PURE FISHSCALE COCAINE | RATED THE BEST | 252 STAMP ✻ ✻ ✻ ESCROW
# 330853 - Cocaine - LeftCoastLabs
Buy: USD 698.00

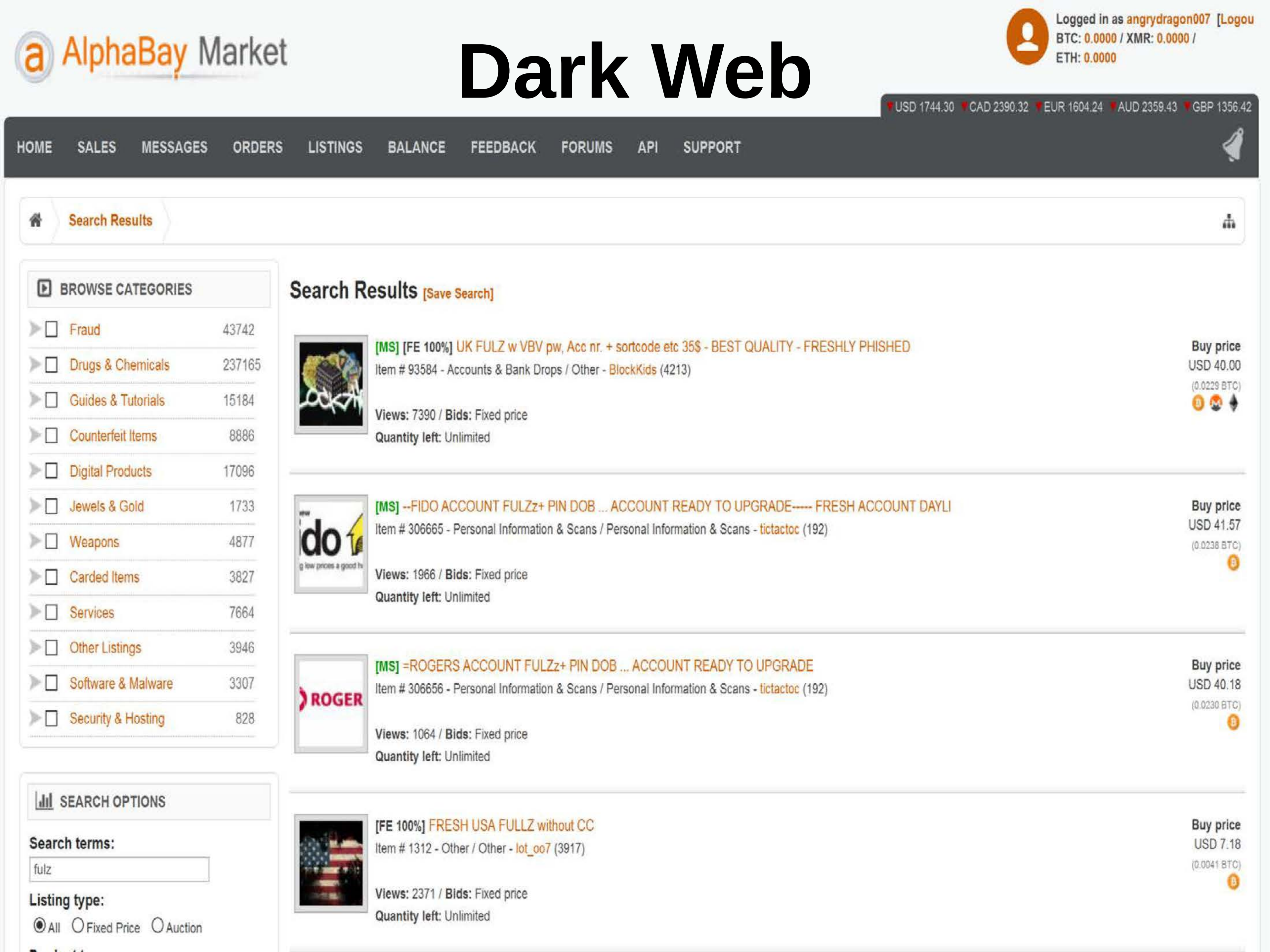
[MS] 1g FENTANYL HCL **** REAL PURE FENTANYL **** FULL ESCROW
# 135090 - Fentanyl & RCs - bigjule33
Buy: USD 450.00

[FULL VIDEO PROOFS - THOUSANDS IN MINUTES!] ROAD TO RICHES + DOUBLE YOUR BITCOINS IN ONE DAY V3 [APRIL 2017 UPDATE] - [$48050.00 USD PROFIT IN 10 DAYS, FULL PROOF HERE! ] Become a MILLIONAIRE in 2017!
# 183848 - CVV & Cards - BitcoinThief
Buy: USD 730.00

[MS] Heisenberg ACADEMY --> Make $15K -$40 K per month -->VIDEO TUTORIALS

[MS] 1/4 LB Pineapple Kush - Greenhouse (TOP SHELF)

# Dark Web



AlphaBay Market

Logged in as angrydragon007 [Logou
BTC: 0.0000 / XMR: 0.0000 /
ETH: 0.0000

USD 1744.30 CAD 2390.32 EUR 1604.24 AUD 2359.43 GBP 1356.42

Search Results

BROWSE CATEGORIES

| | |
|---|---|
| □ Fraud | 43742 |
| □ Drugs & Chemicals | 237165 |
| □ Guides & Tutorials | 15184 |
| □ Counterfeit Items | 8886 |
| □ Digital Products | 17096 |
| □ Jewels & Gold | 1733 |
| □ Weapons | 4877 |
| □ Carded Items | 3827 |
| □ Services | 7664 |
| □ Other Listings | 3946 |
| □ Software & Malware | 3307 |
| □ Security & Hosting | 828 |

SEARCH OPTIONS

Search terms:

fulz

Listing type:

● All ○ Fixed Price ○ Auction

Search Results [Save Search]

[MS] [FE 100%] UK FULZ w VBV pw, Acc nr. + sortcode etc 35$ - BEST QUALITY - FRESHLY PHISHED
Item # 93584 - Accounts & Bank Drops / Other - BlockKids (4213)
Views: 7390 / **Bids:** Fixed price
**Quantity left:** Unlimited
Buy price
USD 40.00
(0.0229 BTC)

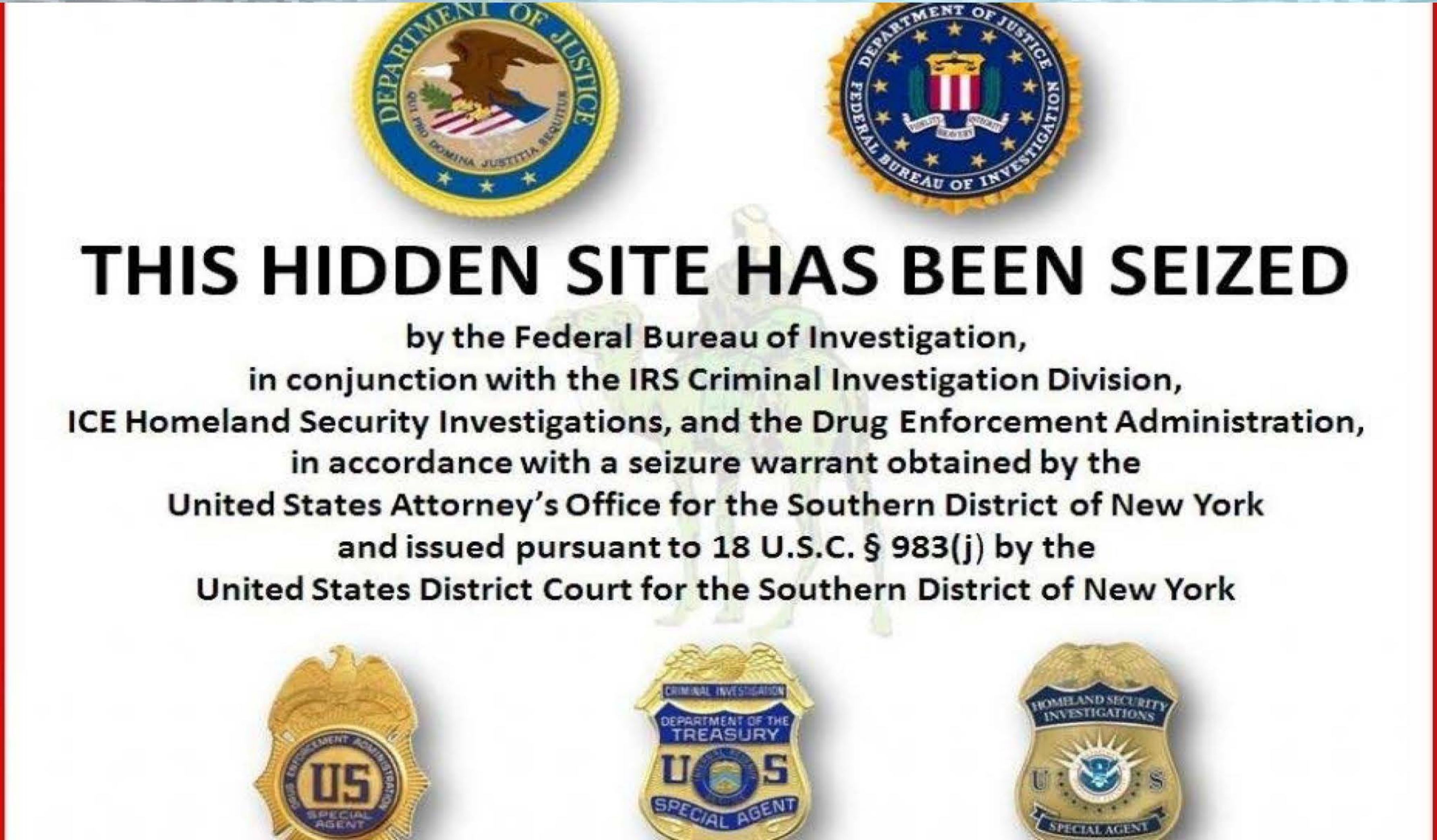
[MS] --FIDO ACCOUNT FULZz+ PIN DOB ... ACCOUNT READY TO UPGRADE----- FRESH ACCOUNT DAYLI
Item # 306665 - Personal Information & Scans / Personal Information & Scans - tictactoc (192)
Views: 1966 / **Bids:** Fixed price
**Quantity left:** Unlimited
Buy price
USD 41.57
(0.0238 BTC)

[MS] =ROGERS ACCOUNT FULZz+ PIN DOB ... ACCOUNT READY TO UPGRADE
Item # 306656 - Personal Information & Scans / Personal Information & Scans - tictactoc (192)
Views: 1064 / **Bids:** Fixed price
**Quantity left:** Unlimited
Buy price
USD 40.18
(0.0230 BTC)

[FE 100%] FRESH USA FULLZ without CC
Item # 1312 - Other / Other - lot_oo7 (3917)
Views: 2371 / **Bids:** Fixed price
**Quantity left:** Unlimited
Buy price
USD 7.18
(0.0041 BTC)

Silk_Road_Seized_1000x600.jpg

# Dark Web



THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
US
SPECIAL AGENT
CRIMINAL INVESTIGATION
DEPARTMENT OF THE TREASURY
U S
SPECIAL AGENT
HOMELAND SECURITY INVESTIGATIONS
U S
SPECIAL AGENT

# Polling Question

What is the name of a Dark Net Market?

a) Amazon

b) Google

c) Alphabay

d) Ethereum

# Dark Web
# Opioid Crisis

The PoliceChief

# Dark Web
# Opioid Crisis

# Dark Web
# Opioid Crisis

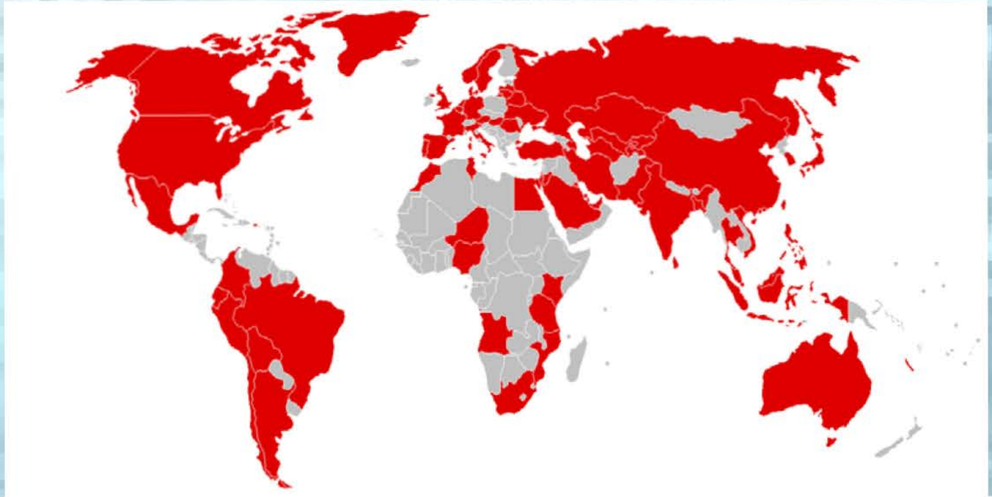
Homeland Security Investigations
Cyber Crimes Center
U.S. Immigration and Customs Enforcement
U.S. DEPARTMENT OF HOMELAND SECURITY

PoliceChief

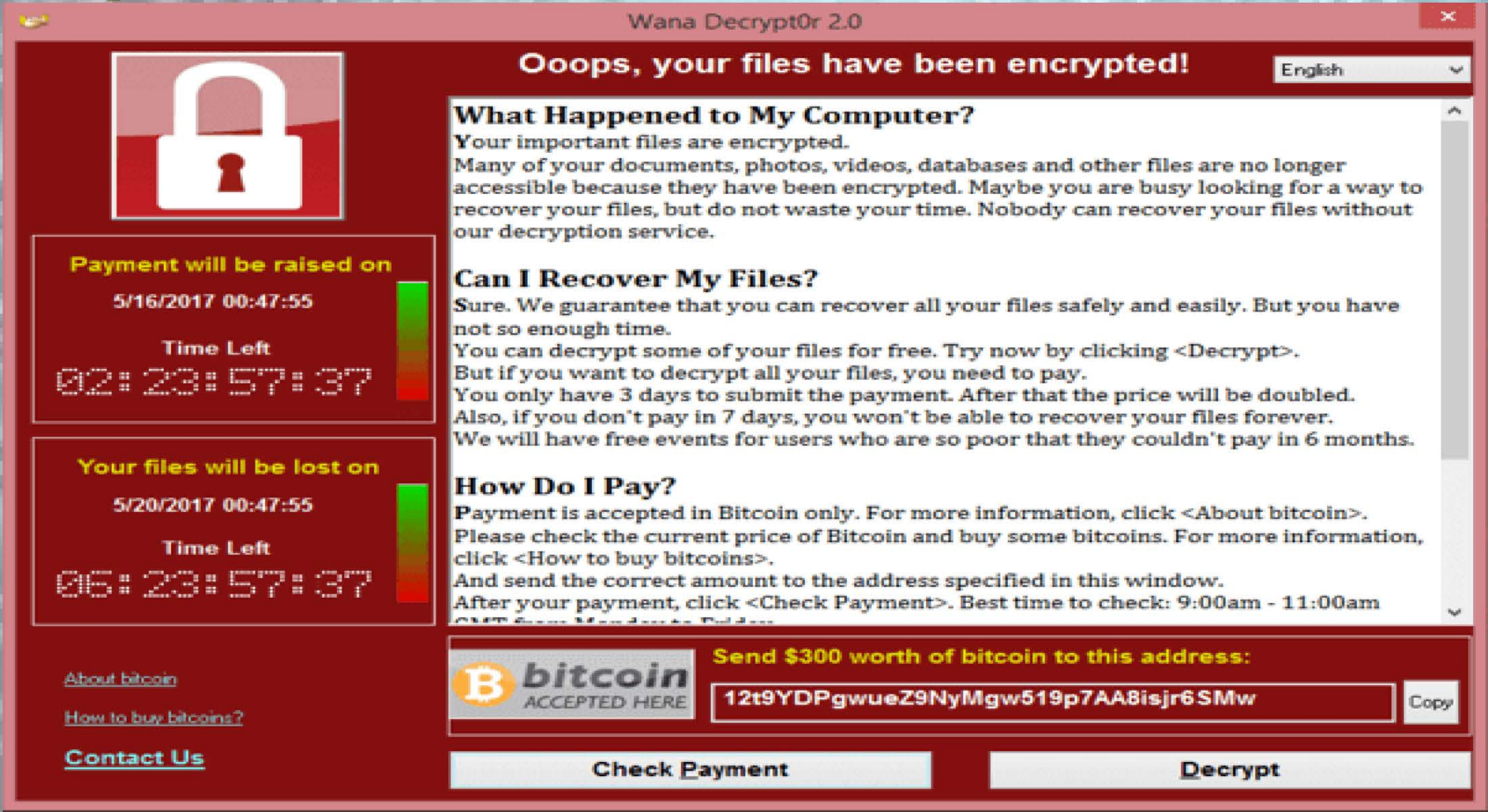
# Dark Web
# Opioid Crisis

# Ransomware

# WannaCry



# Ransomware



Ooops, your files have been encrypted!

**What Happened to My Computer?**

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

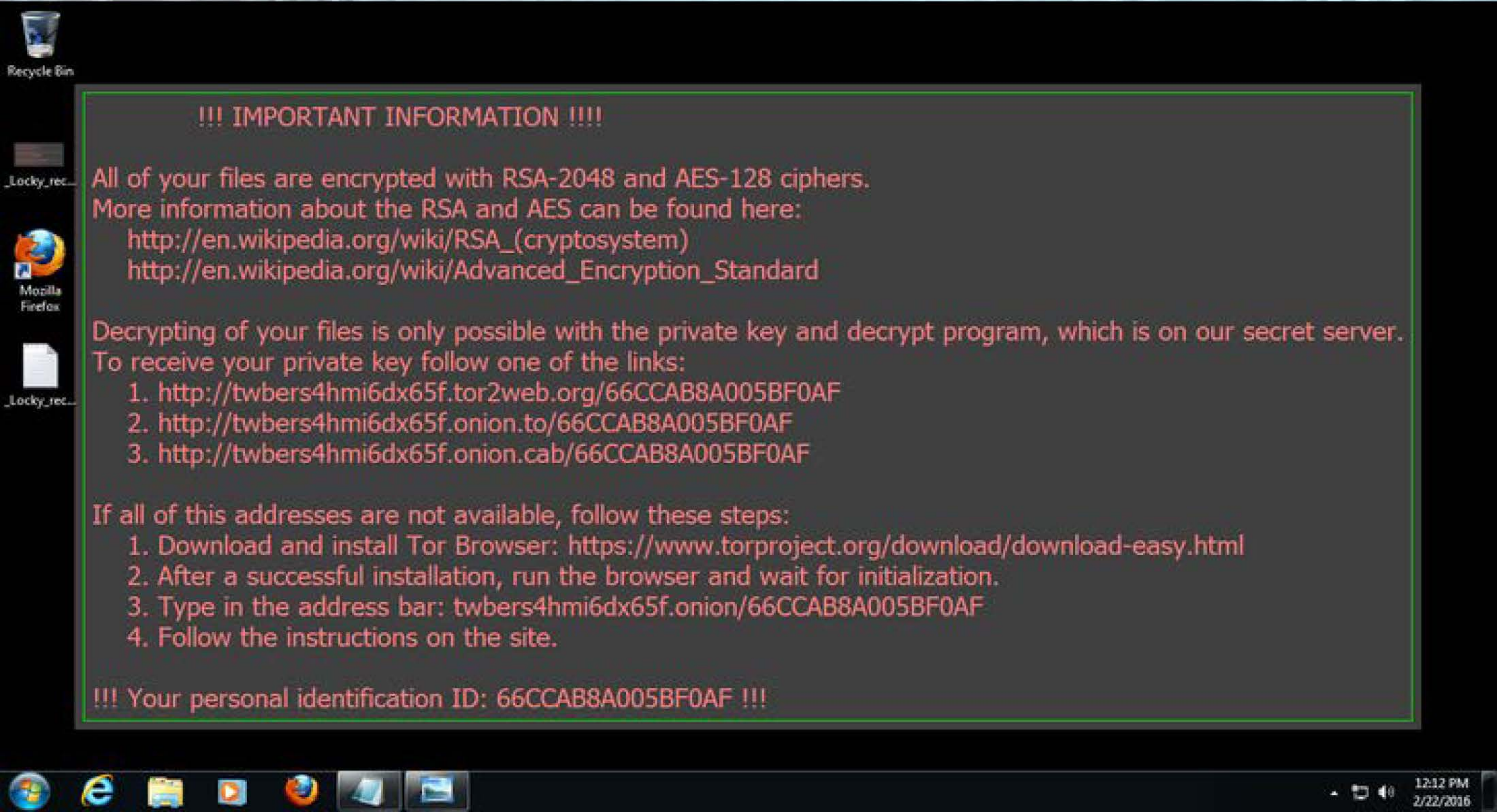
Time Left

06:23:57:37

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

# Dark Web



!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:

1. http://twbers4hmi6dx65f.tor2web.org/66CCAB8A005BF0AF
2. http://twbers4hmi6dx65f.onion.to/66CCAB8A005BF0AF
3. http://twbers4hmi6dx65f.onion.cab/66CCAB8A005BF0AF

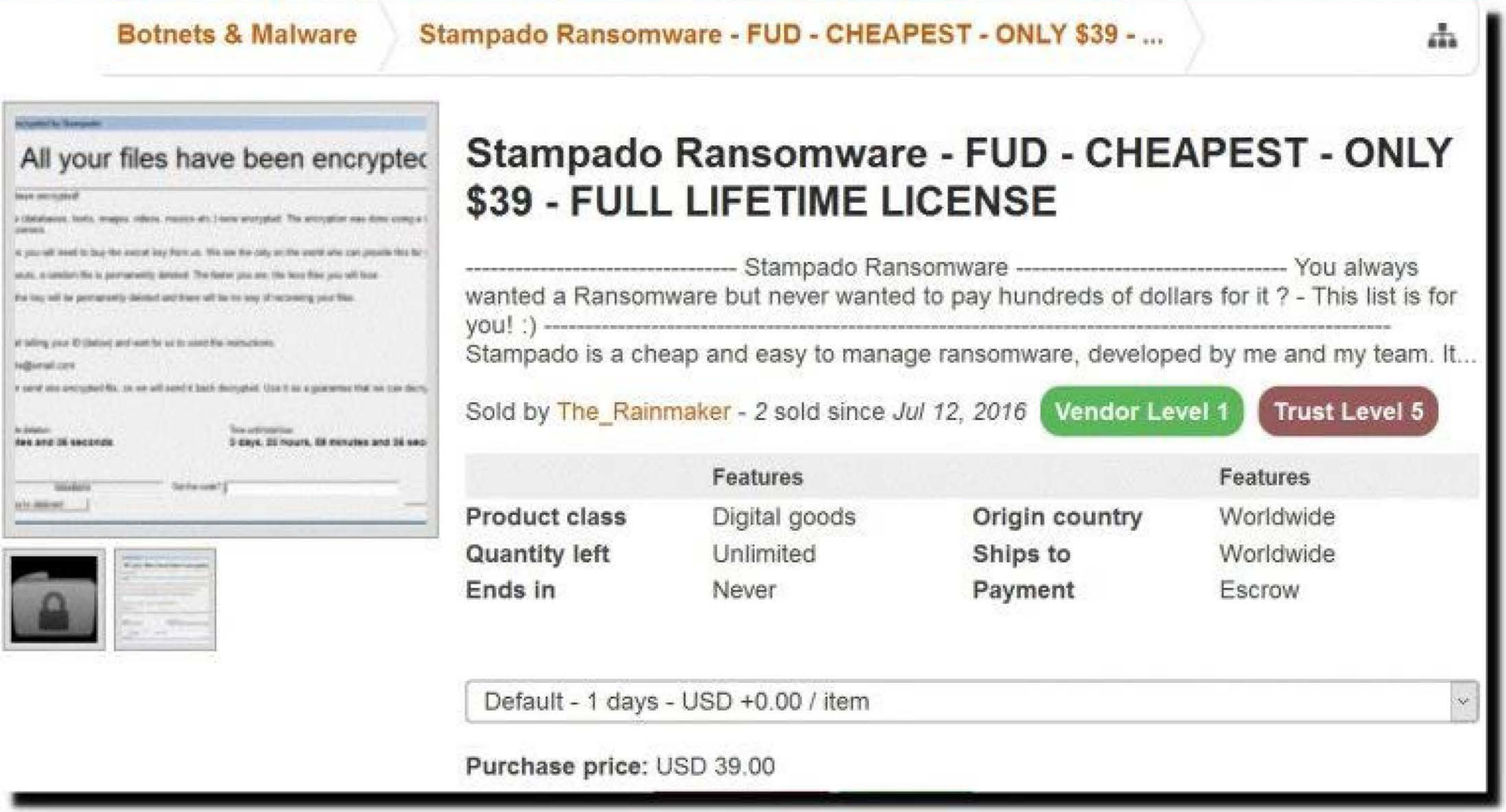
If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: twbers4hmi6dx65f.onion/66CCAB8A005BF0AF
4. Follow the instructions on the site.

!!! Your personal identification ID: 66CCAB8A005BF0AF !!!

# Dark Web

# Dark Web



Botnets & Malware › Stampado Ransomware - FUD - CHEAPEST - ONLY $39 - ...

All your files have been encryptec

## Stampado Ransomware - FUD - CHEAPEST - ONLY $39 - FULL LIFETIME LICENSE

--------------------------------- Stampado Ransomware --------------------------------- You always wanted a Ransomware but never wanted to pay hundreds of dollars for it ? - This list is for you! :) ------------------------------------------------------------------------------------------------------
Stampado is a cheap and easy to manage ransomware, developed by me and my team. It...

Sold by The_Rainmaker - *2 sold since Jul 12, 2016* **Vendor Level 1** **Trust Level 5**

| | Features | | Features |
|---|---|---|---|
| **Product class** | Digital goods | **Origin country** | Worldwide |
| **Quantity left** | Unlimited | **Ships to** | Worldwide |
| **Ends in** | Never | **Payment** | Escrow |

Default - 1 days - USD +0.00 / item

**Purchase price:** USD 39.00

# Dark Web

# Polling Question

What do hackers use to encrypt files and force someone to pay to have them unencrypted?

a) Miners

b) Hackware

c) Ransomware

d) Ransom Code

# Q & A Session

Philip Yamalis

Stakeholder Liaison

and

James Daniels

Program Manager – Cyber Crimes

IRS – Criminal Investigation

# Most Important Points

- Surface web has only around 5% of the data stored on the internet

- Special software like the Tor browser is used to access the dark web

- Don’t click on links from unknown people or email addresses

# Thank You!