# Cyber Crime and TOR

SHEFFIELD ETHICAL STUDENT HACKERS

# The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is **VERY** easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.
- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.
- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

# Code of Conduct

- Before proceeding past this point you must read and agree our Code of Conduct, this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.

- Code of Conduct can be found at https://wiki.shefesh.com/doku.php?id=code_conduct

# Just to re-iterate

- We do not condone the purchase, use or (re-)distribution of illegal articles such as narcotics or weapons.
- This session is only for educational purposes – for the understanding of how to protect yourself and others from crime.
- There are very few/no reasons to use TOR in an open, democratic society; don’t give yourself reasons to be a suspect.

- Code of Conduct can be found at https://wiki.shefesh.com/doku.php?id=code_conduct

# Onion Routing

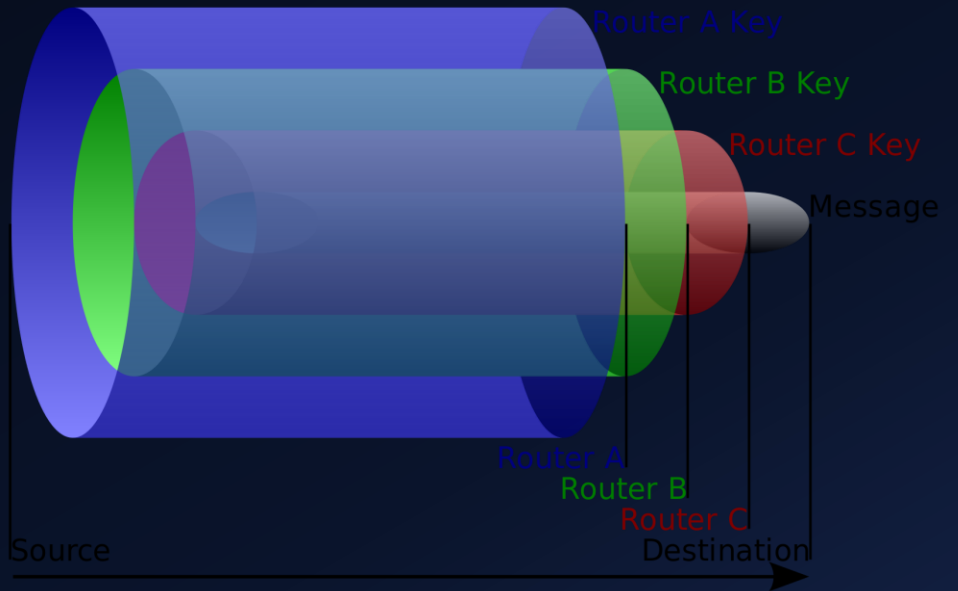
## A QUICK EXPLANATION

# A brief history

- Invented by U.S. Naval Research Laboratory, developed further by DARPA.
- Released to the public and maintained by the EFF since 2002.
- Majority of funding still comes from US + Swedish Governments.

# Why onion?

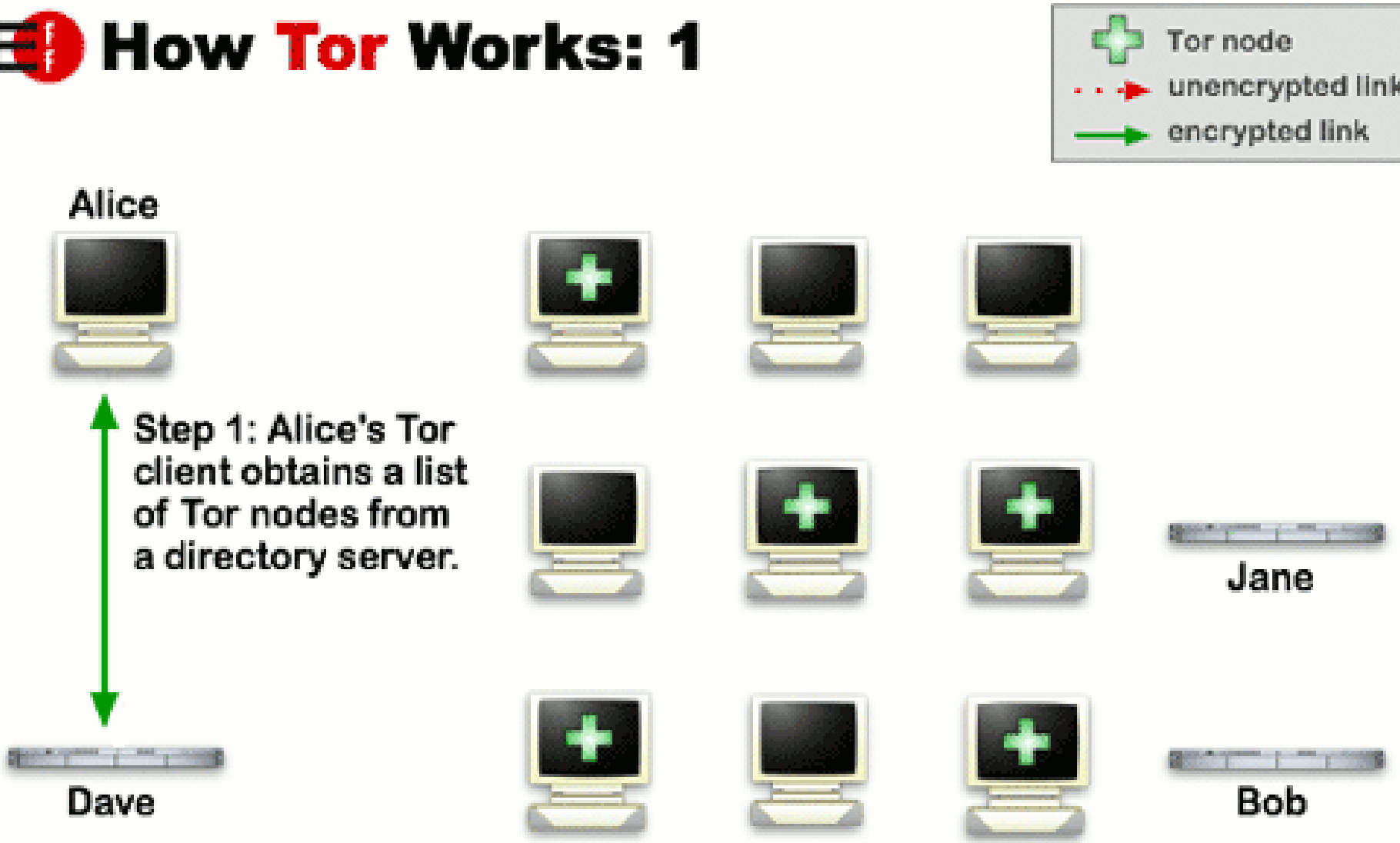
- Think of layers of an onion as analogy:
  - Keep peeling layers off until you reach the middle
- Tor is similar, there are at least 3 layers concealing the information
- Data is encrypted 3 times using 3 different keys for 3 different nodes

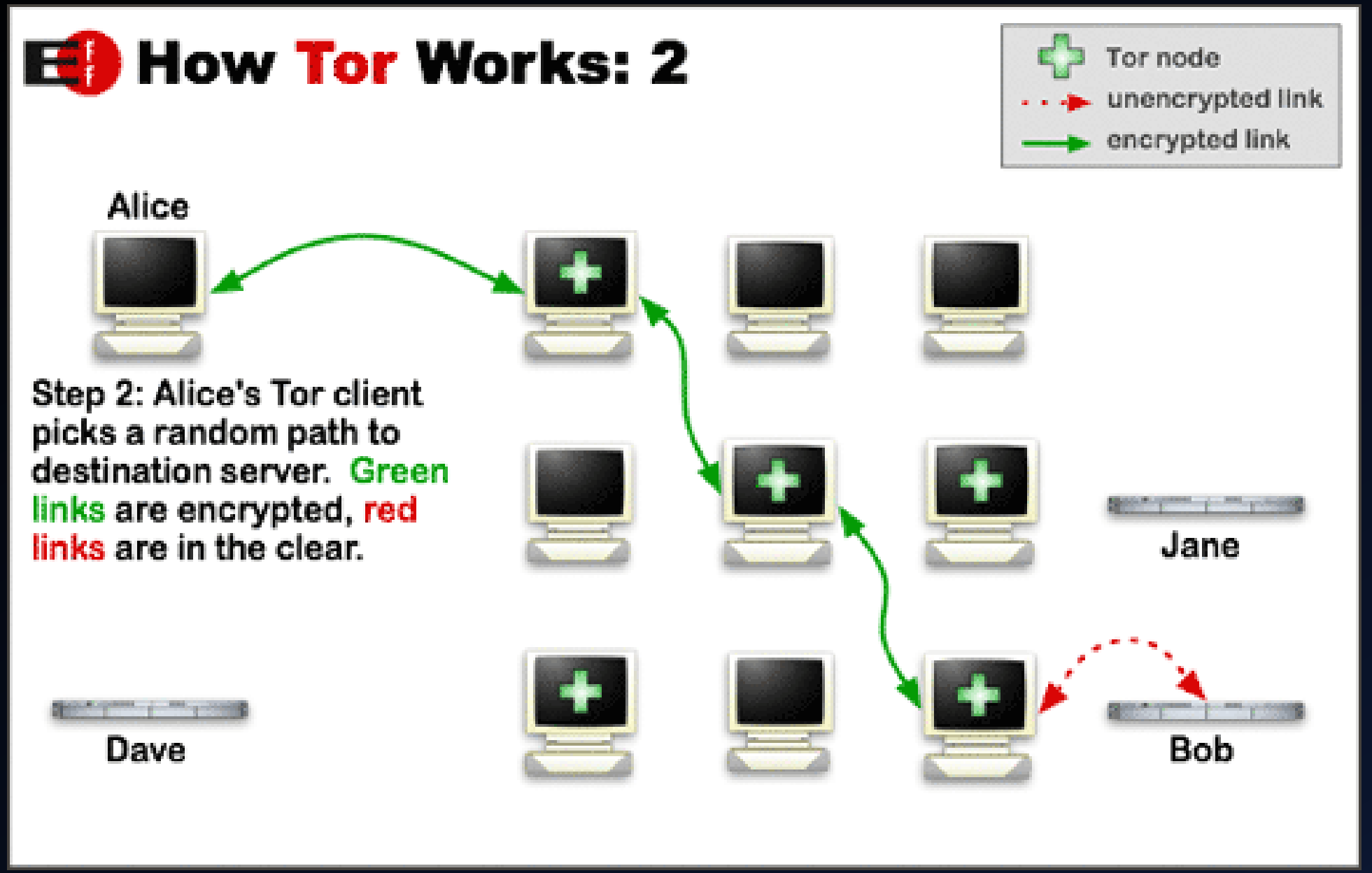


# Routing through the Tor network

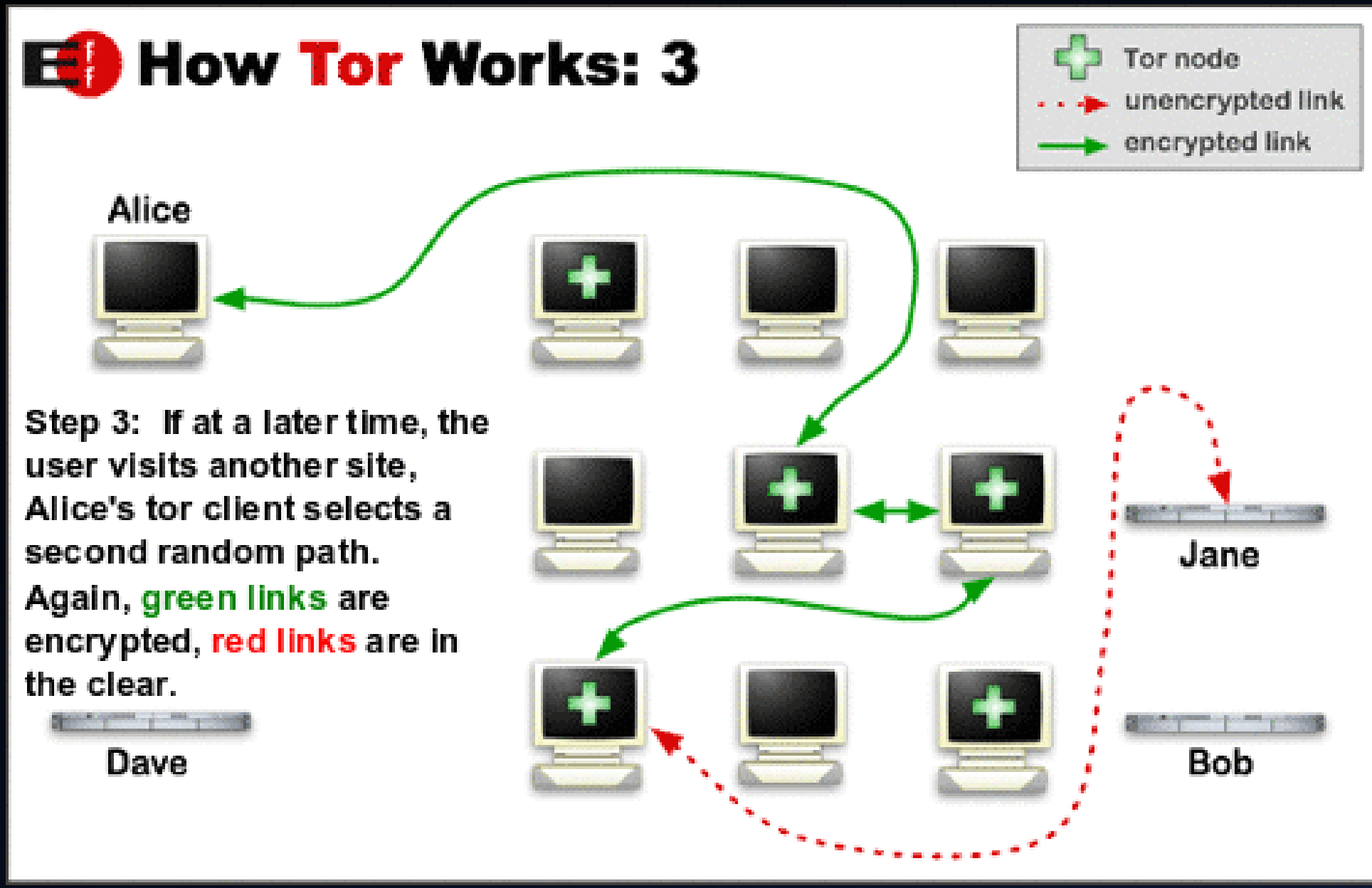
- As a client, you connect through an Entry (Guard) node, this node decrypts the top layer of the ‘onion’ to reveal the next destination
- Reaches 2nd node, second layer decrypted to reveal next destination. Sees source as previous node, so no link back to client
- Reaches 3rd (Exit) node, third layer decrypted to reveal target.
- Data received by target, sees source as Exit node.

# How Tor Works: 1




How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

# How Tor Works: 3



# Can you identify any potential flaws?

- Easy to detect when someone is connecting to the Tor network, narrow down suspects.
- Incredibly slow – AOL-reminiscent experience.
- “If you actually look in to where these Tor nodes are hosted and how big they are, some of these nodes cost thousands of dollars each month just to host because they're using lots of bandwidth, they're heavy-duty servers and so on. Who would pay for this and be anonymous?” – Tor cannot enforce encryption between exit and target.
- **Some protocols expose IP addresses, BitTorrent etc**
- Heartbleed

# Deep Web vs Dark Web

- Just a quick clarification as these terms get thrown about incorrectly a lot:
- Deep Web:
- *The deep web, invisible web, or hidden web are parts of the World Wide Web whose contents are not indexed by standard web search engines.*
- Dark Web:
- *The portion of the Internet that is intentionally hidden from search engines, uses masked IP addresses, and is accessible only with a special web browser:* ***part of the deep web****.*

# The 1st year stoner OpSec toolkit

- Abundance of information available on the clear web.
- /r/DarkNetMarkets and /r/DNMUK before being taken down.
- YouTube guides, reviews.
- Blindly follow instructions – some configurations aren’t great

# Typical set-up

- Tor Browser – Based on Firefox.
- OpenPGP – Encrypting communication between parties.
- Bitcoin Wallet.

# Tails OS

- Tails (The Amnesic Incognito Live System) is a non-persistent, security-focused Linux distro.
- Non-persistent = no data is saved unless user explicitly sets it up to do so.
- All traffic forced to go through Tor.

- Widespread use.

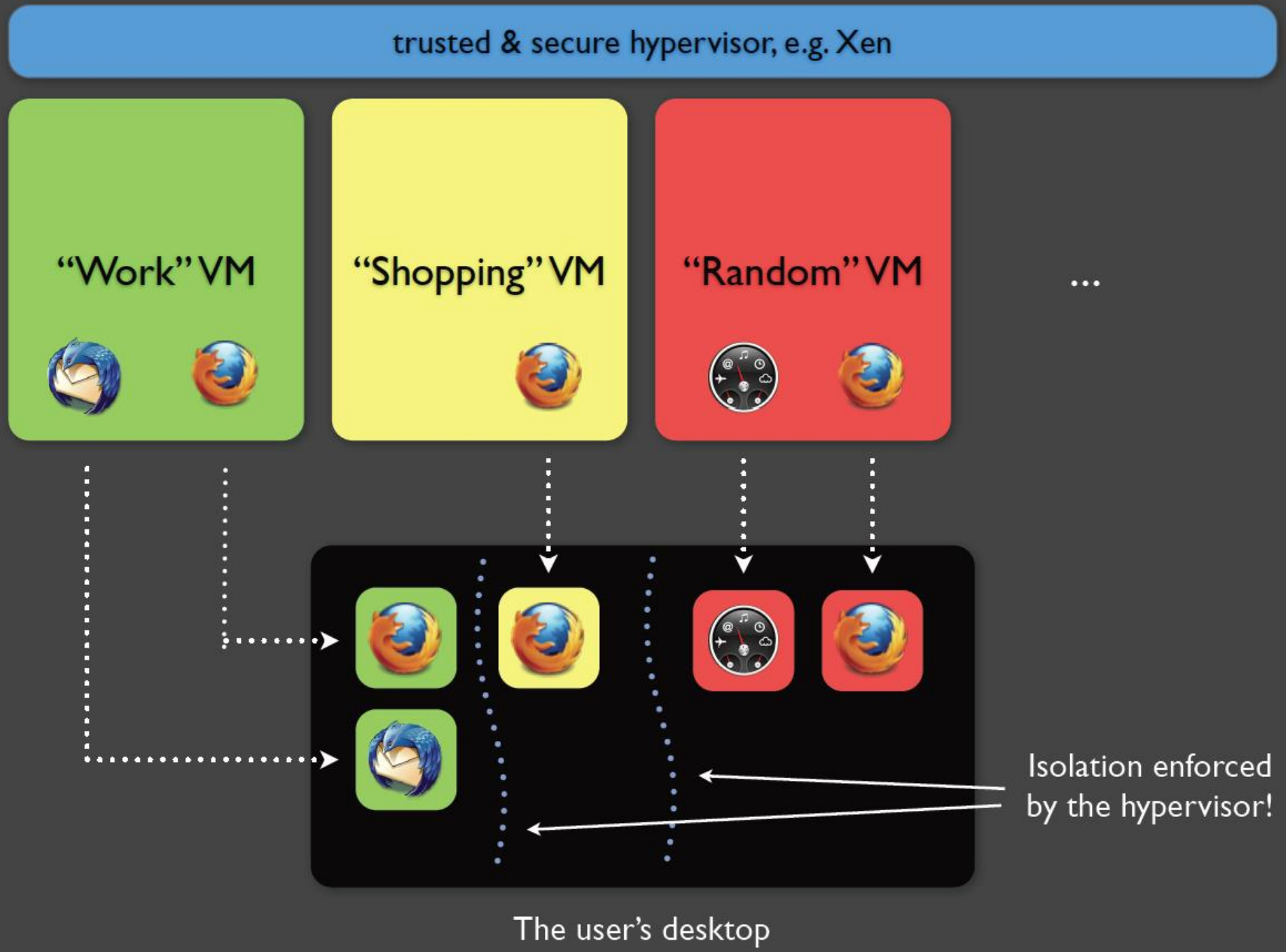
# Whonix

- Two Virtual Machines based on VirtualBox, one virtual machine acts as a gateway and the other as a client.
- Client is only connected to gateway for network so all network traffic is forced to go through Tor.
- Easy to set up, noob-friendly.

- Only as secure as the Host OS it’s operating on.

# Qubes OS

- Qubes is a ‘reasonably secure operating system’, a virtualization based on Xen Hypervisor. Isolates systems for fine control.
- Much more advanced option than other two, higher barrier of entry.
- Whonix can run on top of Qubes, alleviating some of the worries with an insecure host OS.


trusted & secure hypervisor, e.g. Xen
"Work" VM
"Shopping" VM
"Random" VM
...
Isolation enforced by the hypervisor!
The user's desktop

# The Currencies of The Dark Web

- Typically Bitcoin is used – ubiquitous, easily obtained, fairly ‘anonymous’.
- Ethereum, Monero and Bitcoin Cash are sometimes also used due to smaller transaction fees and faster processing times.

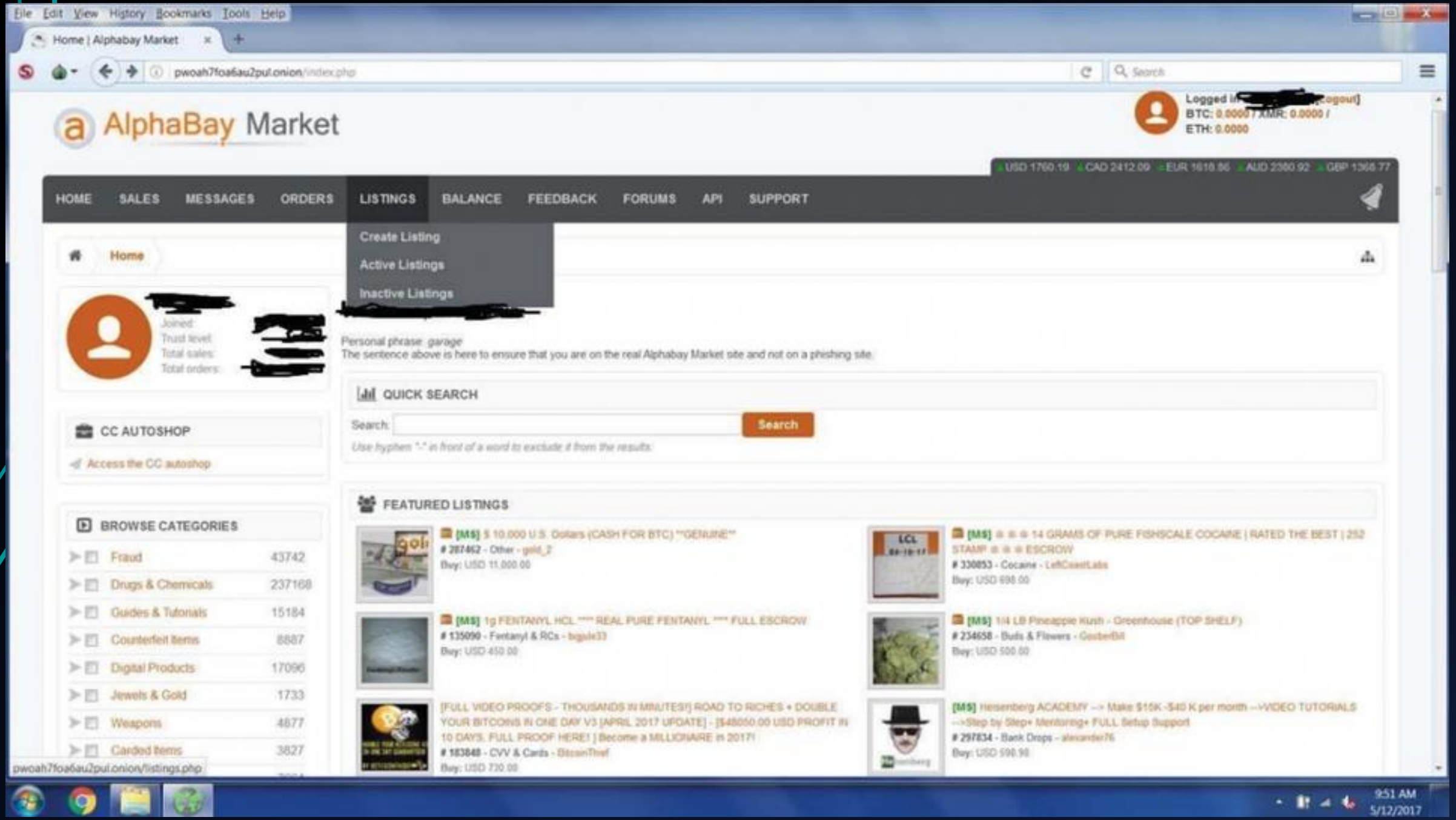
# Bitcoin Tumblers

- A user can send their bitcoins to a tumbler service.
- Bitcoins are ‘mixed’, exchanged to obfuscate the trail back to the original source.
- Makes it harder for law enforcement to follow the trail of money exchanges.

- Digital money laundering.

# Dark Net Markets

- The ‘eBays’ of the Dark Web.
- If it exists, it’s available:
  - Drugs
  - Child Pornography
  - Weapons
  - Human Trafficking
  - Hacking Services
  - Assassinations
  - Fake IDs
  - Fake Currencies


File Edit View History Bookmarks Tools Help
Home | Alphabay Market
pwoah7foa6au2pul.onion/index.php
AlphaBay Market
Logged in
BTC:
ETH: 0.0000
USD 1760.19 CAD 2412.09 EUR 1618.86 AUD 2380.92 GBP 1366.77
HOME SALES MESSAGES ORDERS LISTINGS BALANCE FEEDBACK FORUMS API SUPPORT
Create Listing
Active Listings
Inactive Listings
Home
Joined:
Trust level:
Total sales:
Total orders:
Personal phrase: garage
The sentence above is here to ensure that you are on the real Alphabay Market site and not on a phishing site.
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 43742
Drugs & Chemicals 237168
Guides & Tutorials 15184
Counterfeit Items 8887
Digital Products 17096
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 - bigpile33
Buy: USD 450.00
[MS] 1/4 LB Pineapple Kush - Greenhouse (TOP SHELF)
# 234658 - Buds & Flowers - GovBet
Buy: USD 500.00
[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 720.00
[MS] Heisenberg ACADEMY --> Make $15K -$40 K per month --VIDEO TUTORIALS -->Step by Step+ Mentoring+ FULL Setup Support
# 297834 - Bank Drops - alexander76
Buy: USD 590.90
pwoah7foa6au2pul.onion/listings.php
9:51 AM
5/12/2017

# How a Dark Net Market works

- Sellers pay a bond to the market as a show of ‘trust’.
- Buyer registers on the site using pseudonym, finds product and purchases.
- Buyer sends Bitcoin to the market’s Bitcoin wallet, seller is informed.
- Buyer encrypts address/details using seller’s PGP public key.
- Seller sends product/service, ‘stealth’ used.
- Buyer confirms, transaction finalised, Bitcoin released to seller.

# ‘Stealth’

- For drugs, stealth is utilised to avoid detection by postal services.
- Multitude of methods, standard procedures involve:
  - Mylar (BoPET) sealed, gas and aroma barrier
  - Printed address labels – no handwriting identification
  - Decoys – hiding drugs inside other items, or birthday cards for LSD
  - Non-tracked mail services
  - Dropping off at various post boxes/offices, avoiding regular patterns

# All sounds safe enough – how do you get caught?

- Dark Net Markets do get shut down, primary motivations for law enforcement are Fentanyl, SOC and terrorism. See AlphaBay and Hansa Markets.
- Clear Net behaviours on the Dark Net – same usernames, mannerisms, piecing together tiny amounts of data
- Traffic patterns, can infer what is going on.
- Sellers being busted for other crimes, their poor OpSec -> your demise.
- Same can apply to your own poor OpSec, should you commit other offences.

# The technology likely won’t let you down

- Human nature will. People are inherently clumsy and lazy, there will be slip-ups eventually.
- Some sellers take breaks to try and avoid being overworked, leading to potential mistakes.

# Big Busts - AlphaBay

- LE tracked down who was operating the site -> in the early days headers on password reset emails contained ‘Pimp_Alex_91@hotmail.com’
- Looking at HaveIBeenPwned, this email was found in a few different leaks, possibly re-used passwords?
- Found text files which “identified the passwords/passkeys for the AlphaBay website” – poor OpSec for someone operating a $23million market. Accounts showed all the assets purchased.
- LE then controlled the market, collected information and shut it down.

# Big Busts – Hansa Market

- Immediately after the shutdown of AlphaBay, most users flocked to Hansa Market, a much smaller and newer market which promised to be more ‘secure’.
- Dutch LE already seized control of the site and had been operating and monitoring it for some time. Collected information as the mass migration occurred, shut it down.

# What’s Next?

- Information collected from these operations have lead to significant arrests, likely many more than have been publicly attributed to.
- With time and more data, LE will likely track down most-wanted targets.
- Small-time users may not face consequences due to resource constraints but AI and emerging technologies could help. Some users make it too easy, not using PGP or just simply making horrific mistakes.

# THANK YOU

*Sheffield Ethical Student Hackers*

- Remember, you may be technically proficient – what you have learned today could allow you to commit serious crime with a degree of anonymity.
- A lot of cyber-security jobs require security clearance/background checks – event the smallest of misdemeanors will make you ineligible.
- Use your skills for good.