What is the Dark Web

• Part of the Deep Web – And means that its contents are not indexed by conventional search engines such as Google, Bing and so on
  • However there are Onion search engines like Duck Duck Go which index Onion addresses for TOR Services

• It must be accessed using specific software. Normal web browsers can not access Dark Web sites

• One of the most popular resources used to access the Dark Web is TOR, formerly known as The Onion Router
**SURFACE WEB**
- Wikipedia
- Google
- Facebook
- Bing
- Amazon
- Twitter
- NYTimes
- Wired
- The Guardian

**DEEP WEB**
Medical records, subscription information, government resources, legal documents, financial records, scientific reports.

**DARK WEB**
Onion sites, drug trafficking, political protests, private communications.
What is the Dark Web

• What is it used for?
  • Many people use it just to stay anonymous.
  • Others use it to commit crimes.
  • There are also very useful benefits:
    • Citizens in oppressed countries researching science, religion, democracy and so on.
What is the Dark Web

• Is everything on the Dark Web sinister and evil?

• Not even close, many of the resources are used for good.

• Even businesses and other entities have embraced the Dark Web:
Accessing the Darkweb

• TOR – Web Browser
• I2P – Web Browser
• Freenet – Web Browser
• Tails – Live USB Operating System
• Whonix – Operating System that runs inside Windows / Mac
• Subgraph – Linux Operating System

• ... and many more
Browse Privately.
Explore Freely.
Defend yourself against tracking and surveillance. Circumvent censorship.

Download Tor Browser ↓
Welcome to the Invisible Internet

The Invisible Internet is a privacy by design, people-powered network. It is a truly free and anonymizing Internet alternative. Get I2P.

Get I2P 1.7.0
Freenet is a peer-to-peer platform for censorship-resistant and privacy-respecting publishing and communication.
Tails is a portable operating system that protects against surveillance and censorship.
whonix

The most watertight privacy operating system in the world.
Subgraph OS: Adversary resistant computing platform

Subgraph OS is a desktop computing and communications platform that is designed to be resistant to network-borne exploit and malware attacks. It is also meant to be familiar and easy to use. Even in alpha, Subgraph OS looks and feels like a modern desktop operating system.

Subgraph OS includes strong system-wide attack mitigations that protect all applications as well as the core operating system, and key applications are run in sandbox environments to reduce the impact of any attacks against applications that are successful.
On a Smartphone

• Once again, you download the product, and now use it instead of Safari or Android Browser:
On a Smartphone
On a Smartphone

DuckDuckGo

Zero-click info: what is my ip
Your IP address is 95.130.9.210 in Anonymous Proxy

   IP address lookup, location, proxy detection, email tracing, IP hiding tips, blacklist check, speed test, and forums. Find, get, and show my IP address.
   whatismyipaddress.com

2. What Is My IP Address - IP Address Tools and Info ...
   We provide IP address tools that allow users to perform an Internet Speed Test, IP address lookup, proxy detection, IP Whois Lookup, and more.
   whatismyip.com

3. What is My IP Address?
Tor – The Onion Router

• “Private access to an uncensored web”
• Began in mid 90s with researchers at US Naval Research Lab
• Utilizes onion routing to conceal travel on the internet
• Deployed in 2002 as free and open software
Tor – The Onion Router

• Began receiving funding from the Electronic Funding Frontier in 2004
• The Tor Project established as 501(c)3 nonprofit organization in 2006
• Began development of Tor Browser in 2008
How Tor works

• Three types of relay servers
  • Middle relay – Interim relays; encrypted
  • Bridge relay – Censorship circumvention tools where necessary
  • Exit relay – Final relay; traffic exits the Tor network to the public internet; unencrypted
How does Tor work?

- Free software
- More than 7,000 worldwide volunteer relays
- Tor software encrypts the original data and destination IP address, and then wraps multiple levels of encryption around it
- Each relay only decrypts the identity of the next relay
- Data will appear to originate from its Tor exit node
How big is TOR as of today?
How big is TOR as of today?
How big is TOR as of today?
How big is TOR as of today?

<table>
<thead>
<tr>
<th>Country</th>
<th>Mean daily users</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>483606 (20.24%)</td>
</tr>
<tr>
<td>Germany</td>
<td>223138 (9.34%)</td>
</tr>
<tr>
<td>Russia</td>
<td>142154 (5.95%)</td>
</tr>
<tr>
<td>India</td>
<td>102220 (4.28%)</td>
</tr>
<tr>
<td>Finland</td>
<td>96576 (4.04%)</td>
</tr>
<tr>
<td>Indonesia</td>
<td>82414 (3.45%)</td>
</tr>
<tr>
<td>France</td>
<td>80113 (3.35%)</td>
</tr>
<tr>
<td>Netherlands</td>
<td>70264 (2.94%)</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>66852 (2.80%)</td>
</tr>
<tr>
<td>Brazil</td>
<td>51703 (2.16%)</td>
</tr>
</tbody>
</table>
The anonymous Internet

Daily Tor users per 100,000
Internet users

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.oi.ox.ac.uk

Oxford Internet Institute
University of Oxford
TOR

- How does TOR work?
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 the destination server. **Green links** are encrypted, **red links** are in the clear.
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.
Tor Hidden Services

• Websites and other servers configured to only accept inbound traffic through Tor

• No exit node from Tor, so the entire connection is encrypted
TOR

• Let me draw out a better explanation

• I always use the analogy of the show Lost in Space
TOR

• So how does it change the IP addresses? And can we find any hints?

• Let’s take a look.
Some precautions

• Never let Tor open to full screen
• Never have other browsers open with Tor
• Never open downloaded files while Tor is still open
Using Tor

• Where do we get it?
  • torproject.org – always download Tor from the legitimate source
Browse Privately.
Explore Freely.

Defend yourself against tracking and surveillance. Circumvent censorship.

Download Tor Browser
Defend yourself.

Protect yourself against tracking, surveillance, and censorship.
Completing Tor Browser Setup

Tor Browser has been installed on your computer.
Click Finish to close Setup.

- Run Tor Browser
- Add Start Menu & Desktop shortcuts

Click "Connect" to connect to Tor.

Click "Configure" to adjust network settings if you are in a country that censors Tor (such as Egypt, China, Turkey) or if you are connecting from a private network that requires a proxy.

For assistance, visit support.torproject.org/#connectingtotor
Establishing a Connection

Please wait while we establish a connection to the Tor network. This may take several minutes.

Loading relay information

For assistance, visit support.torproject.org/#connectingtoTor

Cancel
Privacy is a human right

Your donation will be matched by Friends of Tor, up to $150,000.

Donate Now
Some good starting points

• One thing very unique and notable about the Dark Web is that there isn’t a really well-known place to start. For example, on the Clear Net most of us simply go to Google, Bing, Yahoo or any of the other well-known websites. The Dark Web doesn’t really have anything like that. So, we have to look for some starting points.
Some good starting points

• Onion Links
http://s4k4ceiapwwgcm3mkb6e4diqecpo7kvdnfr5gg7sph7jjppqkvwwqtyd.onion/

• The original Hidden Wiki
http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page

• The new Hidden Wiki
http://6nhmgdpnyoljh5uzr5kwlatx2u3diou4ldeommfxjz3wkhalzgjxqzd.onion/

• A good resource on the Clear Net: https://thehiddenwiki.org/
And some things you may encounter:

- Following are some items you may need to know about:
Cryptocurrency

• What is a Cryptocurrency?
• A collection of binary data which is designed to work as a medium of exchange wherein individual coin ownership records are stored in a ledger which is a computerized database using strong cryptography to secure transaction records, to control the creation of additional coins, and to verify the transfer of coin ownership. (Wikipedia)
• In common terms, it is a virtual currency that isn’t backed by any government or bank, and it is tracked by a decentralized ledger, and there is no physical form of the currency.
Cryptocurrency

• Why do people like Cryptocurrency? What are the benefits?
• There are a lot of answers to that question, some true and some completely false. However, there are some definite benefits:
  • Low transaction fees
  • Faster Processing
  • Some anonymity
  • Peer to Peer transactions
  • Accessibility
Cryptocurrency

• Why do people like Cryptocurrency? What are the benefits?
• And a lot of people look at it as an investment. Much like some people buy foreign currencies and wait for them to go up, many people do the same with cryptocurrency.

• How many cryptocurrencies exist?
  • According to CoinMarketCap, as of last night there were 18,886

Cryptocurrency

• Before we get into the different types, there are some terms that we need to learn.
• Bitcoin – The first coin that started it all. (We will get into this in more detail in a few minutes.)
• Altcoin – Any coin that isn’t Bitcoin
• Blockchain – A digital record that acts as a ledger for all of the transactions.
• Block – Blocks are made up of the transactions. And the blocks can only hold so much information, when it is full, the block is closed and a new block formed. The blocks make up the blockchain.
Cryptocurrency

• Coinbase – a very popular and decentralized cryptocurrency exchange. Coinbase itself is listed on the Nasdaq exchange.

• Cold Storage – A method of storing cryptocurrency completely offline. Believe it or not, they are physical devices:
Cryptocurrency

- DeFi – Decentralized Finance are financial activities conducted without the involvement of a bank or other financial institution.
- Ethereum – the second largest Cryptocurrency behind Bitcoin
- Hot Wallet – A cryptocurrency wallet connect to the internet. (Opposite of Cold Storage)
- Mining – The act of validating a transaction and adding it to the ledger. (Mining is not like digging to find new ones like the name would suggest.)
Cryptocurrency

• Peer to Peer – meaning the transactions occur from user to user, and there is no bank involved.
• Satoshi Nakamoto – the pseudonymous for the creator of Bitcoin
• Stablecoin – a cryptocurrency that attempts to offer stability by attaching its value to a real world asset.
Crypto tumbler or Mixer

- This is used when one of the cryptocurrencies are believed to be “tainted”. The mixer will take currencies from various people, and mix them, issuing a new currency to each person.
Crypto tumbler or Mixer

- This is used when one of the cryptocurrencies are believed to be "tainted". The mixer will take currencies from various people, and mix them, issuing a new currency to each person.

Helix made simple.

Enter the BTC address the clean coins will be sent to... Let's go!
Crypto Escrow

• This is like Escrow in the real world. Since billions have been lost by people being fooled online, you can now send your cryptocurrency to an Escrow. The Escrow will hold the currency until the seller of an item delivers proof that the item has been supplied, and then the funds are released.
This is like Escrow in the real world. Since billions have been lost by people being fooled online, you can now send your cryptocurrency to an Escrow. The Escrow will hold the currency until the seller of an item delivers proof that the item has been supplied, and then the funds are released.

100% Satisfaction
Refund Guarantee

Escrow
We work via escrow and directly

Detailed instruction
Simple and safe
Cryptocurrency

• Now that we have a few basic terms down, how did this all begin?
Bitcoin

- Bitcoin is a cryptocurrency and payment system that unveiled in January of 2009. It works without a central repository meaning that the transactions occur directly from user to user and there is no middle man, for example a bank or government.
- Bitcoin has a total of 21 million. With approximately 19 million of them in circulation.
- Current value is around 41,000 dollars.
- Market Cap of 782 billion.
Bitcoin

• You can always check on all of this:

  • https://www.coinbase.com/price

  • https://coinmarketcap.com/all/views/all/
<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Price</th>
<th>24h %</th>
<th>7d %</th>
<th>Market Cap</th>
<th>Volume(24h)</th>
<th>Circulating Supply</th>
<th>Last 7 Day</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin BTC</td>
<td>$41,122.34</td>
<td>▲ 2.58%</td>
<td>▼ 4.99%</td>
<td>$782,293,786,967</td>
<td>$27,691,599,914</td>
<td>19,010,912 BTC</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Ethereum ETH</td>
<td>$3,113.19</td>
<td>▲ 2.75%</td>
<td>▼ 2.09%</td>
<td>$375,068,865,724</td>
<td>$16,081,249,248</td>
<td>120,366,674 ETH</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Tether USDT</td>
<td>$1.00</td>
<td>▲ 0.00%</td>
<td>▲ 0.01%</td>
<td>$82,640,960,585</td>
<td>$57,883,455,843</td>
<td>82,613,836,053 USDT</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>BNB BNB</td>
<td>$423.08</td>
<td>▲ 2.21%</td>
<td>▲ 0.24%</td>
<td>$69,849,125,576</td>
<td>$1,930,260,247</td>
<td>165,116,761 BNB</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>USD Coin USDC</td>
<td>$0.9999</td>
<td>◼ 0.01%</td>
<td>◼ 0.04%</td>
<td>$50,579,315,799</td>
<td>$3,731,521,709</td>
<td>50,586,292,374 USDC</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>XRP XRP</td>
<td>$0.7231</td>
<td>▲ 1.08%</td>
<td>▼ 5.34%</td>
<td>$34,848,010,489</td>
<td>$1,681,008,582</td>
<td>48,135,209,660 XRP</td>
<td></td>
</tr>
</tbody>
</table>
Blockchain

• A blockchain is a list of growing records, known as blocks, that link to other records and blocks using Cryptography. Generally speaking it lets people see the blocks and point to the previous block along with a time stamp, but is resistant to modification. This is important because Bitcoin uses this technology to monitor the records.

• In simple terms, it allows people to see the data without replicating/modifying the data. Which of course is important when dealing with currency.
Cryptocurrency

And believe it or not, anyone can watch the transactions at anytime using a blockchain explorer:

https://www.blockchain.com/explorer
<table>
<thead>
<tr>
<th>Hash</th>
<th>Time</th>
<th>Amount (BTC)</th>
<th>Amount (USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>18fec1de4a943cb5c375fa8cda05896d7dd2789df371e82fa142ee3c8570</td>
<td>09:58</td>
<td>4.25690197 BTC</td>
<td>$260,692.38</td>
</tr>
<tr>
<td>f730b147fca105c186073d554af9c10f209a8f5df2fc553aee4681fc859032</td>
<td>09:58</td>
<td>0.00242500 BTC</td>
<td>$148.51</td>
</tr>
<tr>
<td>02001a2fc326c230d312cd1af2dcb36d4acbf05b72e343afca3b8819328e5b1f</td>
<td>09:58</td>
<td>0.01010597 BTC</td>
<td>$618.89</td>
</tr>
<tr>
<td>0a63027cebaef14c73f06145a3cb4795531ca3b93d386688a1462a40be057902</td>
<td>09:58</td>
<td>0.01521998 BTC</td>
<td>$932.07</td>
</tr>
<tr>
<td>a9965cb77bea0bca9f64681d05d5be1b5c84af7f7b0bcfd4f73274b742af57</td>
<td>09:58</td>
<td>0.00206130 BTC</td>
<td>$126.23</td>
</tr>
<tr>
<td>1030de8ef2dfaae29ff5034947b4f6c06eaa3e8b809e9367119257827e02f7</td>
<td>09:58</td>
<td>0.00128226 BTC</td>
<td>$78.53</td>
</tr>
<tr>
<td>02519be6e20c60ed5555c5613c5469231efefc38614132895bb4468f4a99df6</td>
<td>09:58</td>
<td>4.95689707 BTC</td>
<td>$303,560.03</td>
</tr>
<tr>
<td>34a86093ebd553c9a79994d4e023e7b069d12fb9c04267927ee78174efec9</td>
<td>09:58</td>
<td>261.45345704 BTC</td>
<td>$16,011,391.41</td>
</tr>
<tr>
<td>267d2f1f493ed4a97f58d59997e91326cc20f0d2ca83953aabb3b455c8e06870</td>
<td>09:58</td>
<td>2.53002084 BTC</td>
<td>$154,938.30</td>
</tr>
<tr>
<td>f5024d55b086ef1bd78ca0e3ce8ee6ca63a030b058517c7c96e0f7c032d36e</td>
<td>09:58</td>
<td>4.94682411 BTC</td>
<td>$302,948.16</td>
</tr>
<tr>
<td>3d3c7a6a7f73db5a9069c93c440a0cd575102dc4b0c76880105da7a549641</td>
<td>09:58</td>
<td>4.73058113 BTC</td>
<td>$289,700.46</td>
</tr>
<tr>
<td>6e339a8c86297b5f88a4043dbd535c1bd2ccfbb53430a297642395be16c48e3e</td>
<td>09:58</td>
<td>0.01032466 BTC</td>
<td>$632.28</td>
</tr>
<tr>
<td>6c130f8ea11238fd5cd54532d1998e80f928ea1820059392a99affa4a453c492d</td>
<td>09:58</td>
<td>0.60744774 BTC</td>
<td>$37,200.06</td>
</tr>
<tr>
<td>e42ca4bf8baa83c932df4ba92002fba167f7e35590750f9cd7dacc9f2d11a</td>
<td>09:58</td>
<td>0.03370941 BTC</td>
<td>$2,064.36</td>
</tr>
<tr>
<td>9eb620c0bf40a9f309de8ac5078537ee4f1210435d6ecf4e0b6367cd8c2badd4</td>
<td>09:58</td>
<td>0.78341760 BTC</td>
<td>$47,979.75</td>
</tr>
<tr>
<td>Hash</td>
<td>Amount</td>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>----------</td>
<td>----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>1NM7RFBu5g38TX6HT7zCTm8VYA2Bt3pv3g</td>
<td>0.00328290 BTC</td>
<td>1NDyJtNTmwk5xPNhjgAMu4Hdi9tobu1s</td>
<td></td>
</tr>
<tr>
<td>1JDRJqlpM1vAXTMar7t51veHARSB5HRHZd</td>
<td>0.02915447 BTC</td>
<td>3HZCdFLpNzJopDDMKx42waxtrMPENrvc</td>
<td></td>
</tr>
<tr>
<td>1DPdSHzg2d2YBQwJGEO7XXsMWrfATQm</td>
<td>0.01218651 BTC</td>
<td>0.00301440 BTC</td>
<td></td>
</tr>
<tr>
<td>15aX9N4HhpZjHTMG5X9LMvudBAGPn9sXKXN</td>
<td>0.00388416 BTC</td>
<td>0.00208612 BTC</td>
<td></td>
</tr>
<tr>
<td>1f99HaEl84LgNbeB5Z2UyMvXhM2hrSv</td>
<td>0.000208612 BTC</td>
<td>0.00301165 BTC</td>
<td></td>
</tr>
<tr>
<td>1vUPsT7uXQMwJWbrFPxYKkqL6Puz8unK</td>
<td>0.00208612 BTC</td>
<td>0.00301165 BTC</td>
<td></td>
</tr>
<tr>
<td>1MwEnkJGMXx1MkjPTKE2Qr0y8uaBNKivr</td>
<td>0.02413260 BTC</td>
<td>0.00403700 BTC</td>
<td></td>
</tr>
<tr>
<td>1URkKrULa9QZ2HTwvJeKJyNtZHRruux7F</td>
<td>0.00403700 BTC</td>
<td>0.00254770 BTC</td>
<td></td>
</tr>
<tr>
<td>1971voLQvKdpxKZaKLFkdZ0TaxVhKExDg</td>
<td>0.00254770 BTC</td>
<td>0.00202459 BTC</td>
<td></td>
</tr>
<tr>
<td>1Na4Rkv6Jcc7DCULdBSRfPjaWr1A8y</td>
<td>0.00202459 BTC</td>
<td>0.00202459 BTC</td>
<td></td>
</tr>
</tbody>
</table>
This address has transacted 1,165,012 times on the Bitcoin blockchain. It has received a total of 15,506,632.42108672 BTC ($950,957,103,728.05) and has sent a total of 15,465,235.71060799 BTC ($948,418,416,098.67). The current value of this address is 41,396.71047873 BTC ($2,538,687,629.38).

| Address | 1NDyJtNTjmwk5xPNhigAMu4HDHgtobu1s |
| Format | BASE58 (P2PKH) |
| Transactions | 1,165,012 |
| Total Received | 15506632.42108672 BTC |
| Total Sent | 15465235.71060799 BTC |
| Final Balance | 41396.71047873 BTC |

Fee
0.00001746 BTC
(3.987 sat/B - 1.060 sat/WU - 2946 bytes)
(4.239 sat/vByte - 2771 virtual bytes)
Cryptocurrency

You can even see the mining:
<table>
<thead>
<tr>
<th>Height</th>
<th>Hash</th>
<th>Mined</th>
<th>Miner</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>707265</td>
<td>0.722825c027a602957b218c182dd43c92a9501b3692094</td>
<td>32 minutes</td>
<td>Unknown</td>
<td>1,498,767 bytes</td>
</tr>
<tr>
<td>707264</td>
<td>0.4049cb13803a8f9afae125054f95de26e64ef3d9757e9</td>
<td>41 minutes</td>
<td>F2Pool</td>
<td>1,545,100 bytes</td>
</tr>
<tr>
<td>707263</td>
<td>0.b98388612ee0c7b0ce8205235cfdd5760fb11bf52ea</td>
<td>48 minutes</td>
<td>Unknown</td>
<td>1,466,507 bytes</td>
</tr>
<tr>
<td>707262</td>
<td>0.a78d09ea7ffcc44c6904f9085400feaddf0a371b8e7</td>
<td>1 hour</td>
<td>ViaBTC</td>
<td>1,441,425 bytes</td>
</tr>
<tr>
<td>707261</td>
<td>0.636305f2b25f9a5c49f631c3567ba9e8839404ebe</td>
<td>1 hour</td>
<td>Unknown</td>
<td>1,448,054 bytes</td>
</tr>
<tr>
<td>707260</td>
<td>0.53824781bfa10d7e16eaaf07bed014bb2e75b458879b</td>
<td>2 hours</td>
<td>ViaBTC</td>
<td>1,445,848 bytes</td>
</tr>
<tr>
<td>707259</td>
<td>0.93dfd61f208aa5c133d79b0e350755d4dd27b1ff2b96</td>
<td>2 hours</td>
<td>F2Pool</td>
<td>1,470,781 bytes</td>
</tr>
<tr>
<td>707258</td>
<td>0.19f3b0c590ae1d14d8c274cbf63213c90794ade0f49a</td>
<td>2 hours</td>
<td>AntPool</td>
<td>1,377,369 bytes</td>
</tr>
<tr>
<td>707257</td>
<td>0.47d771a8d6f4732bb32e6e1f246a57fce8676917350</td>
<td>3 hours</td>
<td>AntPool</td>
<td>1,496,174 bytes</td>
</tr>
<tr>
<td>707256</td>
<td>0.d4a9b8a94935f9672d86559dde3257820ff6500c5aa7</td>
<td>3 hours</td>
<td>Unknown</td>
<td>1,297,604 bytes</td>
</tr>
<tr>
<td>707255</td>
<td>0.8bed089031df0291c4959c184849a7e81c7c4860</td>
<td>4 hours</td>
<td>Unknown</td>
<td>1,513,270 bytes</td>
</tr>
<tr>
<td>707254</td>
<td>0.9e3f17704bd2b354e0d791d8e1ae9b3c94c7740a1590</td>
<td>4 hours</td>
<td>Unknown</td>
<td>916,798 bytes</td>
</tr>
<tr>
<td>707253</td>
<td>0.632bc2b84b626838a2734f6f1920cf63ca715a7c4e8</td>
<td>4 hours</td>
<td>Unknown</td>
<td>566,184 bytes</td>
</tr>
<tr>
<td>707252</td>
<td>0.86ed158668e010753f24aaa161b5426d04d3f9bd7f214</td>
<td>4 hours</td>
<td>AntPool</td>
<td>628,043 bytes</td>
</tr>
<tr>
<td>707251</td>
<td>0.3e03b429a0b9797858d1781e7bb3c3aa550a8bd7444e</td>
<td>4 hours</td>
<td>AntPool</td>
<td>1,347,936 bytes</td>
</tr>
</tbody>
</table>
This address has transacted 74,423 times on the Bitcoin blockchain. It has received a total of 5,216,432.36826334 BTC ($319,902,044,622.61) and has sent a total of 5,215,985.03774658 BTC ($319,874,611,707.39). The current value of this address is 447.33051676 BTC ($27,432,915.22).

<table>
<thead>
<tr>
<th>Address</th>
<th>1KFHE7wBhaENAwwwryaoccDb6qct6DbYY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>BASE58 (P2PKH)</td>
</tr>
<tr>
<td>Transactions</td>
<td>74,423</td>
</tr>
<tr>
<td>Total Received</td>
<td>5216432.36826334 BTC</td>
</tr>
<tr>
<td>Total Sent</td>
<td>5215985.03774658 BTC</td>
</tr>
<tr>
<td>Final Balance</td>
<td>447.33051676 BTC</td>
</tr>
</tbody>
</table>

Fee

0.00000000 BTC
(0.000 sat/B - 0.000 sat/WU - 415 bytes)
(0.000 sat/vByte - 388 virtual bytes)

+6.35264761 BTC
2 Confirmations
Bitcoin Miner

- So how are any of the transactions confirmed?
  - Now that we have seen the mining take place, how is it done?
Bitcoin Mining is a peer-to-peer computer process used to secure and verify bitcoin transactions—payments from one user to another on a decentralized network. Mining involves adding bitcoin transaction data to Bitcoin's global public ledger of past transactions. Each group of transactions is called a block.”
Bitcoin Miner

• Understand that this is big business for some entities. It is estimated that .1 percent of all miners control half of all of the mining capability on the planet. They use mining farms:
Bitcoin Miner

• But you can also find small operations:
Price and other details may vary based on product size and color.

Sponsored

Bitmain Antminer S19pro 110th/s ASIC Miner, 3250w Crypto BTC Bitcoin Bitmain Mining Machine in Stock

$15,669.00

Get it Thu, Nov 4 - Wed, Nov 10
FREE Shipping

Sponsored

Bitmain Antminer S19j pro 100th/s Bitcoin Miner BTC BCH Mining Asic Miner Antminer S19j Pro 100T 2950w Include PSU Power Supply

$12,995.00

Get it Wed, Nov 10 - Wed, Nov 17
FREE Shipping

M2 Pro Crypto Miner – Blockchain Multi-Token Mining: MXC, Bitcoin, DHX + More

🌟🌟🌟🌟🌟 43

$3,299.00

Get it as soon as Wed, Nov 3
$60.59 shipping
Forensic artifacts

- While there have been some developments in this area, it is far beyond the abilities of the conventional forensic labs. So we are going to focus on the ways that can be done by the average forensic labs:
  - Forensic examination of a computer / RAM dump
How are we going to start our investigation?

• RAM dump
  • What is RAM?
  • When/how do we capture RAM?
• Forensic image of computer
• Forensic extraction of mobile device
Tracking Onion Sites

• To do each of these we are going to do hands on.
• I used the following tools to complete these processes:
  • FTK Imager
  • FTK
  • Encase
Tracking Onion Sites

• So what we are going to do now:
  • Create a forensic image of a computer / RAM
  • Use forensic tools to find evidence
Volatile Data

• What exactly are we talking about?
  • Memory that will lose its contents if power is removed
    • RAM
    • Router memory
RAM – Random Access Memory

- Data can be written and read in the same amount of time regardless of what order the data is stored in.

- By contrast, with direct access memory (hard drives, CDs, etc.) data read and write speeds depend on physical location of the data on the medium.
RAM

• RAM is memory available to the operating system and programs for processing and functioning, not storage.

• Are there any other places to find artifacts?
  • Pagefile
  • Hyberfile
What is a pagefile?

• In most systems, a portion of the computer’s hard drive space is set aside as “virtual RAM” to extend the RAM capacity of the system.

• Results in additional (although slower) RAM; data is swapped back and forth from this pagefile (also called a swap file sometimes) to the RAM.
What is a Hyberfile?

• When a machine goes into Hibernation mode, it places the contents of the RAM into the Hyberfile.sys. Which is a System and Hidden file at the Root of the OS drive on Windows machines.
RAM – Random Access Memory

• Data is stored as electrical impulses which disappear when power is removed

• Everything present must, therefore, have been created since the computer was turned on
• Remember, this is memory that will lose its contents if power is removed

• We can’t seize these items and take them back to our office and examine it there – **it must be done on-scene, or it’s gone forever**
Things to remember

• You can’t put 8GB of RAM on a 4GB thumb drive (or an 8GB thumb drive, for that matter)

• This is called a memory “dump” for a reason

• You are making changes to the system