

# Rise of the Underdark

This presentation was created by Tim Leonard and is protected via the Bitcoin BlockChain by [www.proofofexitence.com](http://www.proofofexitence.com).

This presentation is designed to help bankers understand the sophistication carders and thieves use to acquire data and avoid detection. All local laws apply and nothing in this presentation should be used for illegal or malicious purposes. The images used in this presentation are for educational purposes only. Fair use applies. Tim Leonard is providing this education for the greater good.

The views and opinions expressed, in this presentation, are not those of Commercial Bank of Texas.

# Objectives

- Opsec and Tradecraft
- Anonymous IDs
- Burner Phones
- Tails Operating System
- TOR
- Onion Browsers
- Anon Emails and PGP
- Bitcoins
- The Dark Web / Underdark
- Carding and Agent Handling

# OpSec

Processes used to protect information that can be used against us. **OPSEC** challenges us to look at ourselves through the eyes of an adversary .



LEO and LEA

# Tradecraft

*“Tradecraft, within the intelligence community, refers to the techniques used in modern espionage and generally, the activity of intelligence.”* - Wikipedia, September, 2014

Agent Handling

**Eaves  
Dropping**

Concealment

Analytics

Black Bag Ops

INTERROGATION

**Surveillance**

Cryptography

Computer Espionage

Dead Drops

Front Organization

# Deep Web | Dark Web | Underdark

\*\*\*\*\* WARNING \*\*\*\*\*

- Drugs, Human trafficking, copyrighted media, pornography, weapons, political dissidents, stolen credit cards
- Websites end in .onion
- Only accessible with Tor

Keep Your Mouth Shut!



There is no such thing as a safe  
computer or cell phone.

Anon IDs



# Anon IDs

- A separate email is not enough
- Build elaborate online personas
- Understand the Psychology of IDs
- Lighting, Sounds, Clothes, Smells
- Writing styles ( Stylometrics)
- Believe your own lies

# Allen Anderson



Update Profile Picture

**Allen Anderson** [Update Info](#) [View Activity Log](#) [...](#)

[Timeline](#) [About](#) [Friends 79](#) [Photos](#) [More ▾](#)

-  [Sales Manager at Automax](#)   
2013 to present
-  [Studied Business at Southwest Tennessee Community College](#)
-  [Lives in Memphis, Tennessee](#)
-  [In a relationship](#)
-  [From Memphis, Tennessee](#)  
Born on February 10, 1980 (35 years old)

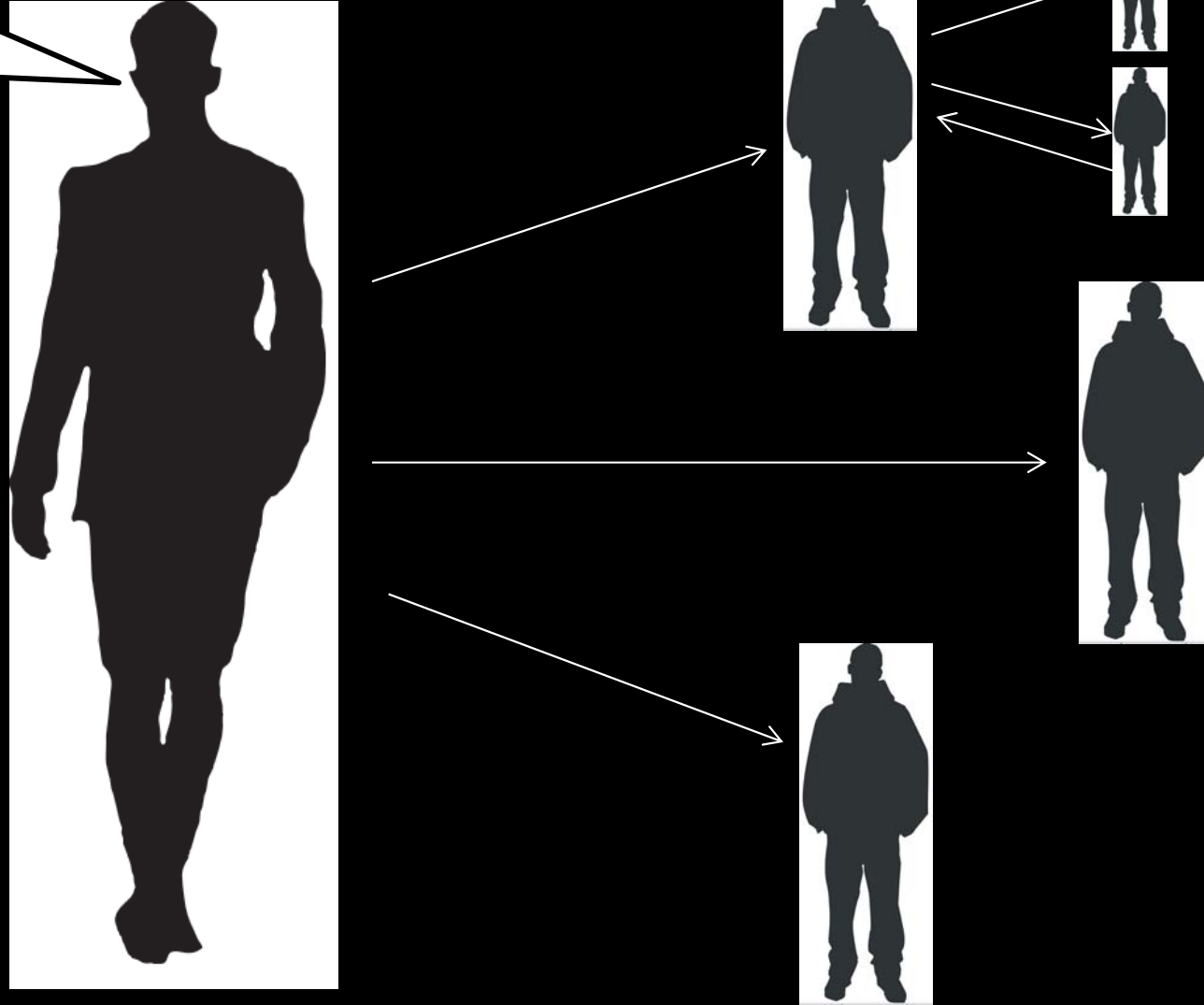
# Anon IDs

- Keep Separate “Golden Rule”
- Operate in large metropolitan areas
- Burner Phones, Laptops, Tails
- Public Wifi
- Anon Emails / Social Networking
- Encrypt Everything 4096 if Possible
- Dead Drops

# Anon IDs

“It only takes one slip to compromise your true identity”

I don't know those fools.



# Burner Phones



# Burner Phone Rules

- Cash only + No loyalty cards
- Purchase far from home
- No smart phones or GPS (getting harder)
- Removable battery!
- 60+ days till activate
- Personal “No Call List”
- Leave your regular phone at home
- Buy other stuff with only cash



# Tracking Cell Phones

- Cell Towers
- GPS
- Wifi Networks
- Bluetooth

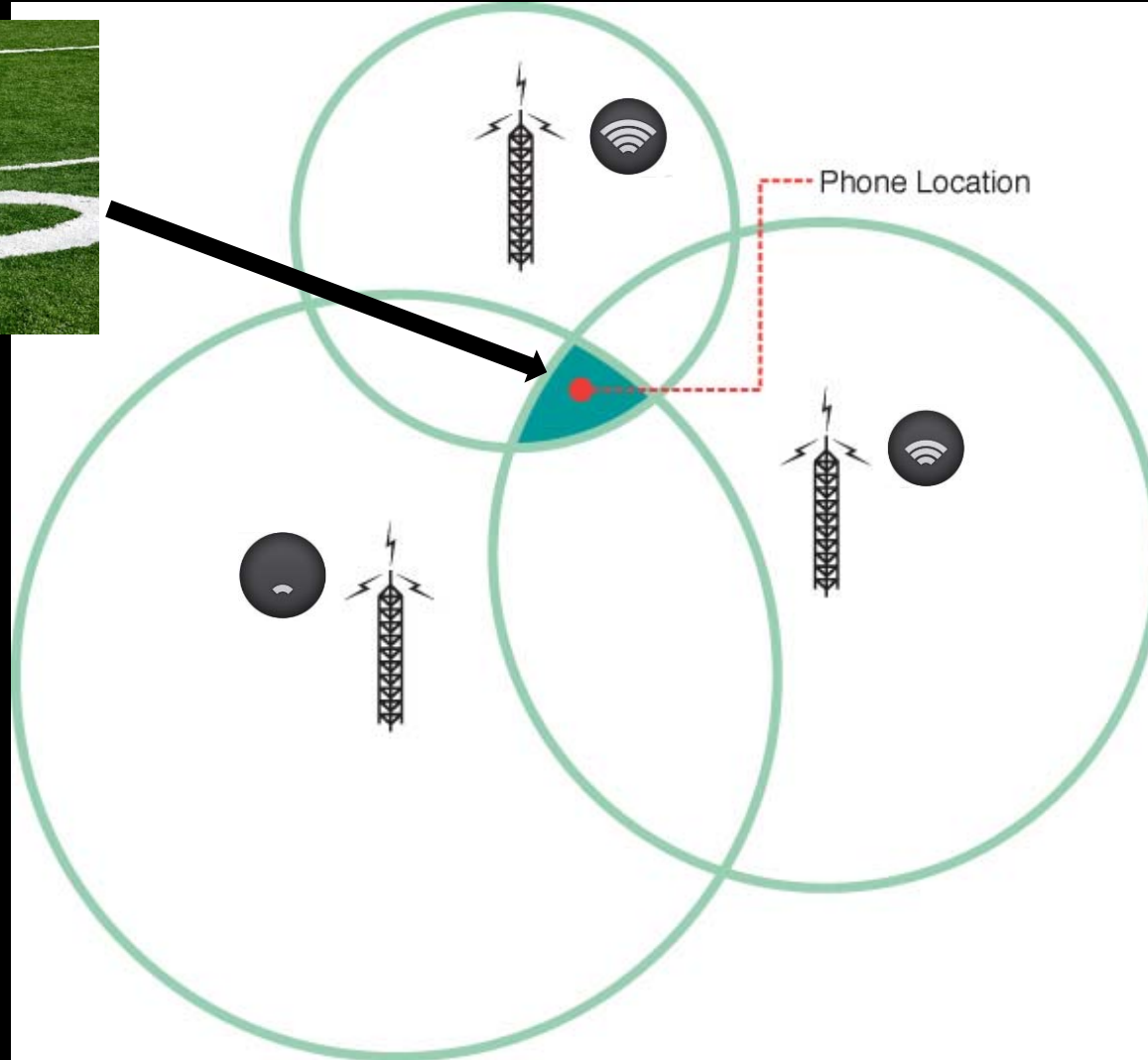


Accuracy

# Tracking: Cell Towers

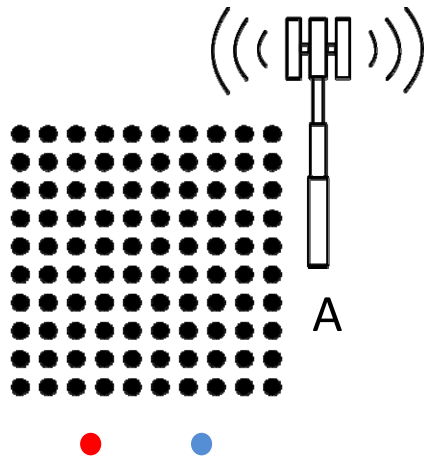


50 – 100 M

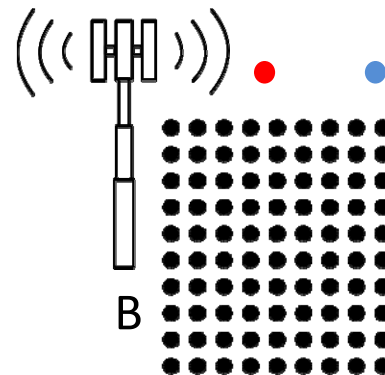
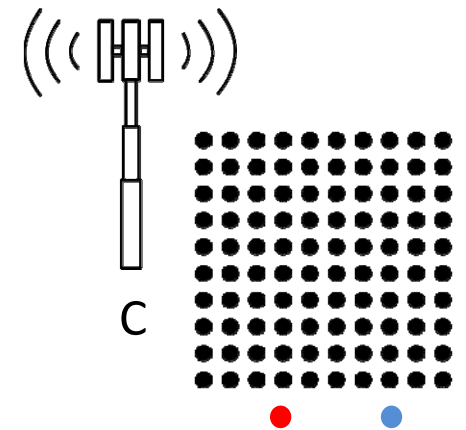


Antenna Density and Location Antennae

# Tracking: Tower Dumps



Red = Burner  
Blue = Personal



# Tracking: Tower Dumps

## How “cell tower dumps” caught the High Country Bandits—and why it matters

Fishing expeditions can pay dividends—but do they need a warrant?

by Nate Anderson - Aug 29, 2013 7:00am CDT

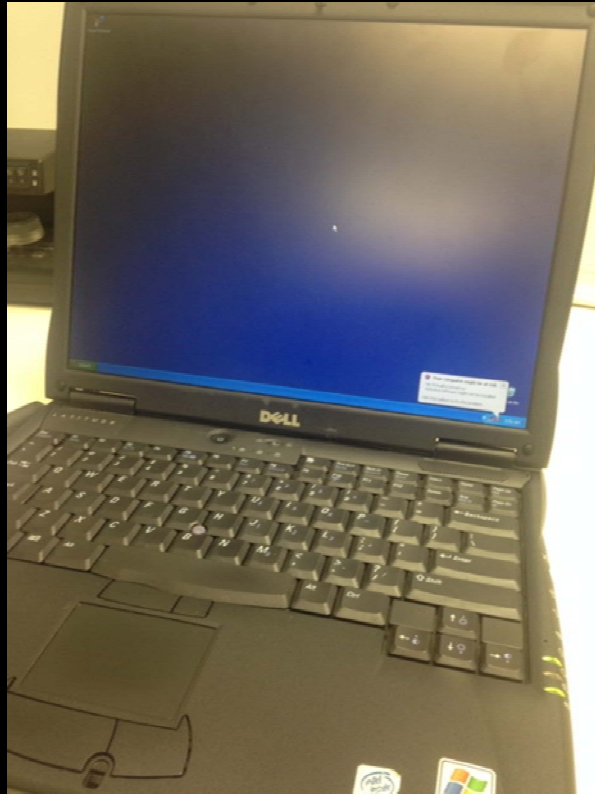
Share Tweet 172



Surveillance footage of one of the robbers.

On February 18, 2010, the FBI field office in Denver issued a ["wanted" notice](#) for two men known as "the High Country Bandits"—a rather grandiose name for a pair of middle-aged white men who had been knocking down rural banks in northern Arizona and Colorado, grabbing a few thousand dollars from a teller's cash drawer and sometimes escaping on a stolen all-terrain vehicle (ATV).

# Burner Laptop Rules

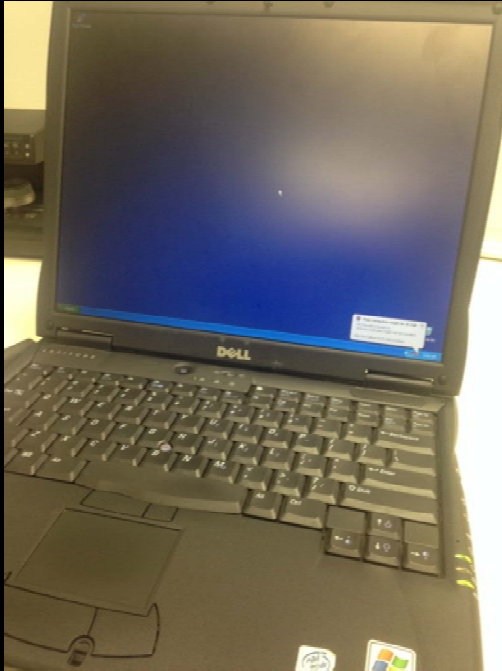


- Pay Cash
- DBAN old hard drive
- Never use at house
- Walk away if needed
- Removable HDs are nice
- Legit O.S. can decoy
- Be aware of identifying info
- Use Public Wifi



[www.dban.org](http://www.dban.org)

# Burner Laptop



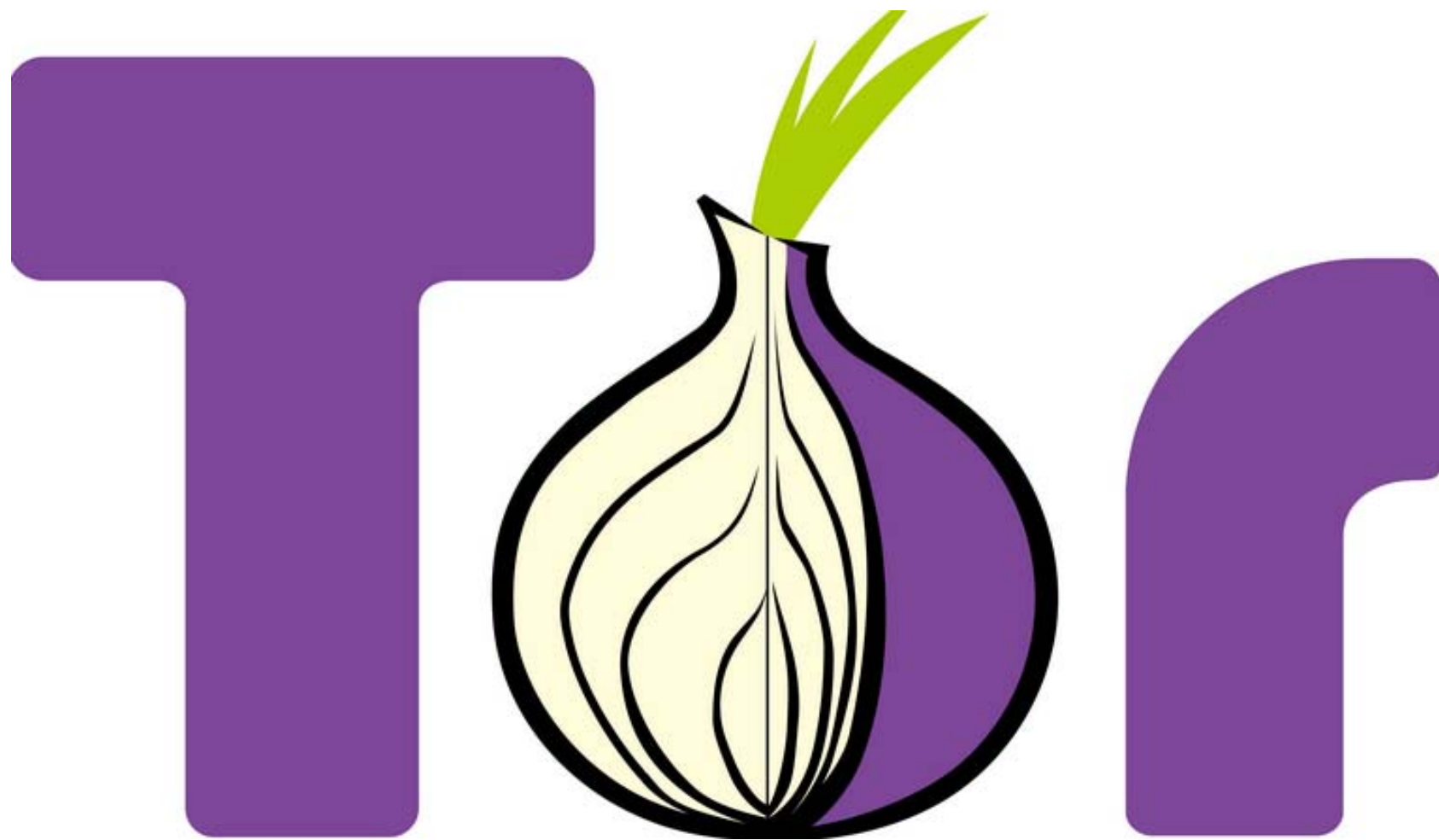
1



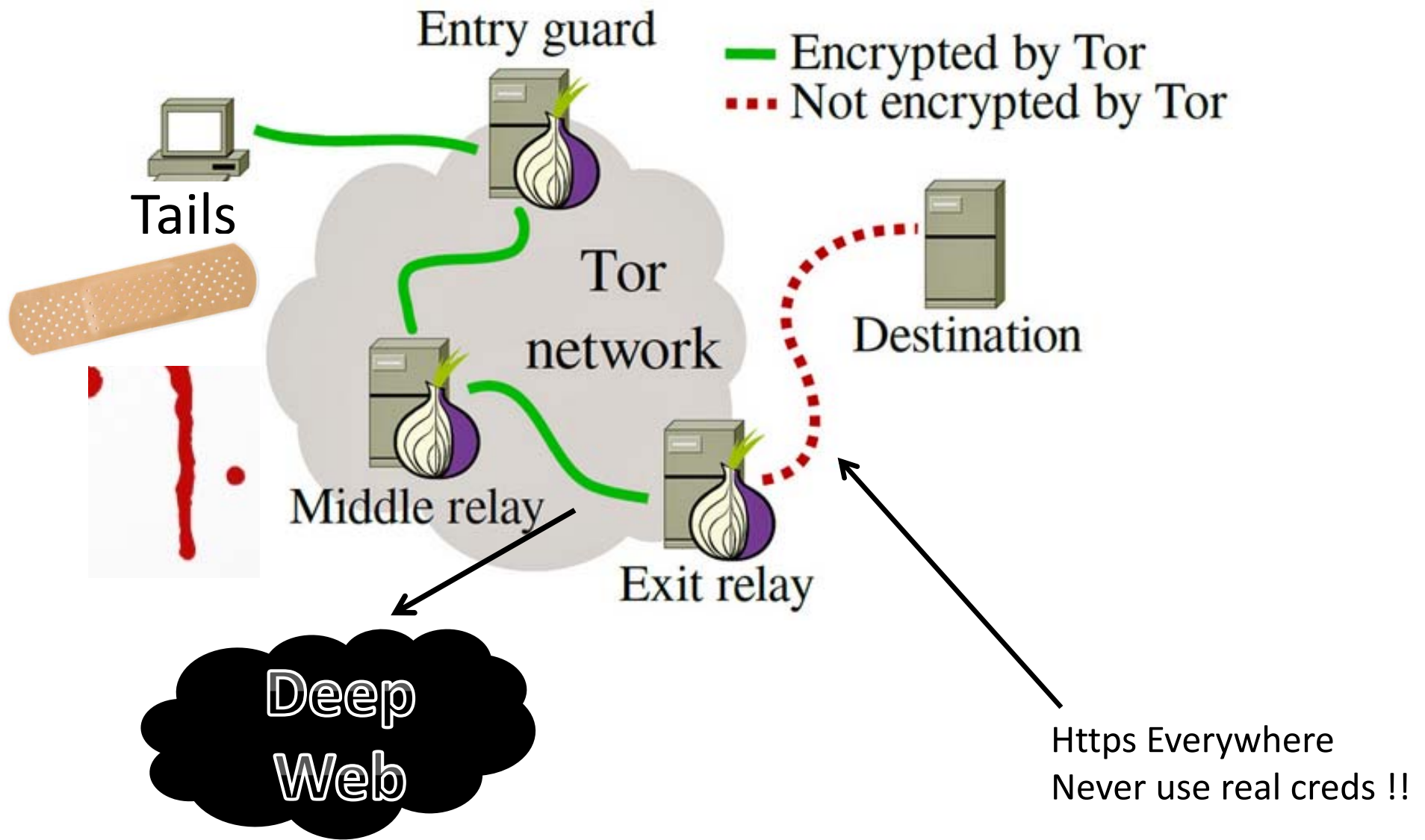
2



3



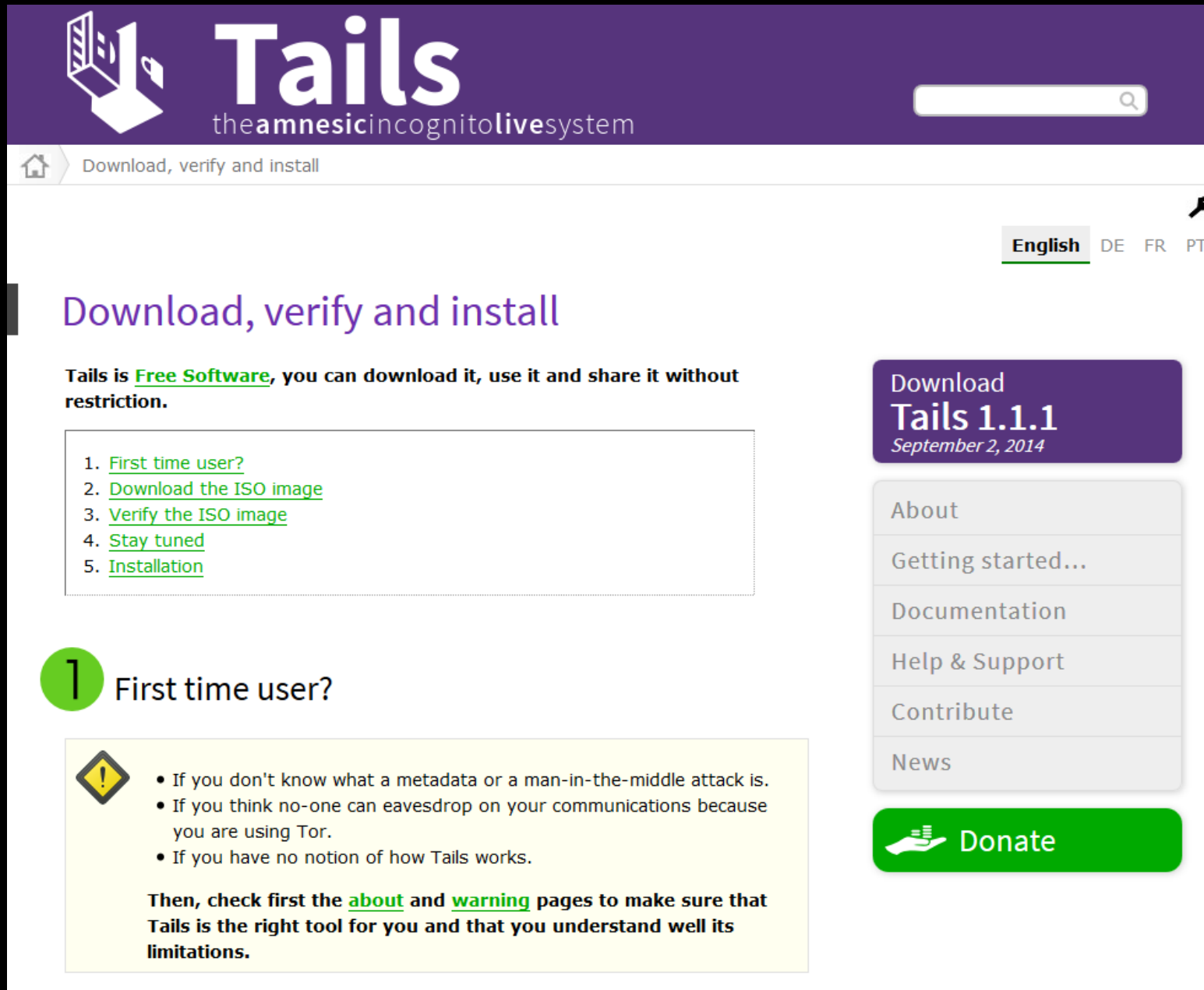
**THE ONION BROWSER**



# THE ONION BROWSER



# Verify Tails and Build USB



The screenshot shows the Tails website homepage. At the top, there is a purple header with the Tails logo (a laptop with a padlock) and the text "Tails the amnesic incognito livesystem". A search bar is located in the top right corner. Below the header, a navigation bar contains a home icon and the text "Download, verify and install". On the right side of the navigation bar, there are language selection options: "English" (highlighted), "DE", "FR", and "PT".

## Download, verify and install

Tails is **Free Software**, you can download it, use it and share it without restriction.

1. [First time user?](#)
2. [Download the ISO image](#)
3. [Verify the ISO image](#)
4. [Stay tuned](#)
5. [Installation](#)


**1** First time user?

- If you don't know what a metadata or a man-in-the-middle attack is.
- If you think no-one can eavesdrop on your communications because you are using Tor.
- If you have no notion of how Tails works.

Then, check first the [about](#) and [warning](#) pages to make sure that Tails is the right tool for you and that you understand well its limitations.

**Download Tails 1.1.1**  
*September 2, 2014*

- About
- Getting started...
- Documentation
- Help & Support
- Contribute
- News

 Donate

## 2 Download the ISO image



You will download Tails in the form of an ISO image<sup>+</sup>: a single file that you will later burn on a DVD or install onto a USB stick or SD card.

### Direct download

LATEST RELEASE

**Tails 1.1.1 ISO image**



CRYPTOGRAPHIC SIGNATURE

**Tails 1.1.1 signature**



If you're not sure what the cryptographic signature is, please read the part on [verifying the ISO image](#).

SHA256 CHECKSUM

```
e38c289a83fe67cc8358e702f3a19071  
050925ffd33355cfe7c43df1592b93f4
```

List of current [known issues](#) in Tails.

### BitTorrent download

LATEST RELEASE

**Tails 1.1.1 torrent**



CRYPTOGRAPHIC SIGNATURE

The cryptographic signature of the ISO image is also included in the Torrent.

Additionally, you can verify the [signature of the Torrent file](#) itself before downloading it.

SEED BACK!

Seeding back the image once you have downloaded it is also a nice and easy way of helping spread Tails.

# Let's Recap

Burner Phone  
Burner Laptop  
Tails USB Key  
Public Wifi  
Cash  
Coffee !!




# Stanford University Surveillance Law

by Jonathon Mayer

 coursera

Decrypting Your Devices (Fifth Amendment Privilege) (10:51)

[Help Center](#) 

Compelled

Self-Incriminating

Testimony



03:05 / 10:51



# Stanford University Surveillance Law

by Jonathon Mayer

coursera

Compelled Biometric Decryption (3:28)

[Help Center](#)

In order to be eligible for Fifth Amendment protection,  
a security feature must involve a mental secret.

Deep Web

# Two Rules When Operating In The Deep Web

1. No pornography
2. No politics





# Silk Road

anonymous market

messages 0 | orders 0 | account ₪0.0000

Search

Go

Shop by Category

- Drugs 12,072
  - Cannabis 2,821
  - Dissociatives 200
  - Ecstasy 1,290
  - Intoxicants 63
  - Opioids 362
  - Other 31
  - Precursors 86
  - Prescription 3,674
  - Psychedelics 1,303
  - Stimulants 1,425
  - Tobacco 316
- Apparel 530
- Art 14
- Biotic materials 2
- Books 1,161
- Collectibles 21
- Computer equipment 106
- Custom Orders 80
- Digital goods 852
- Drug paraphernalia 440
- Electronics 165



Vallium (Apaurine) 10mg x 100.  
₪1.6865



Oxycontin 30 mg "Roxys" Pharmacy Fresh Free Ship!  
₪0.4260



10 Grams Pure Crystal Meth Methamphetamine  
₪6.1324



1.5 GRAMS DUTCH WEED GROWN IN ITALY!!!  
₪0.1678



Prima Lux Slims 6 (10 packs x 20 cigarettes)  
₪0.3166



[HGH] Human Growth Hormone 200iu Set (8iu x  
₪7.5712

- From the fo
- New disp
  - Try Tails
  - secure C
  - Who's yo
  - Acknowl



- [Main Page](#)
- [Country index](#)
- [About us](#)
- [Contact us](#)

[page](#)

[discuss](#)

[view source](#)

# WikiLeaks

“ ... could become as important a journalistic tool as the Freedom of Information Act. ”

— Time Magazine

[Get involved](#)

[Submit](#)

[Browse by](#)

[Contact](#) • [Donate](#) • [Contribute](#) • [Follow](#)

[documents](#)

[Country](#) • [Region](#) • [Language](#) • [Year](#)

# McDumpals



**WALLET**

**\$0.00**

add funds

**CART**

**0**

view items

BROWSE DUMPS

WHOLESALE

**ACCOUNT**

CHECKER

SUPPORT

## Account

Orders Payments Wallet Cart

Bins  Expires from

\* Checks price: \$0.2  
\* Dumps from packs are not refundable  
\* Citibank is currently not refundable  
\* Maestro is currently not refundable

10 records per page

Track 2 Country Brand Type Category Exp. date Code Name Checker

No data available in table

Showing 0 to 0 of 0 entries

# Anon Emails

- Create multiple emails across different providers.
- Create a PGP key for each email address to encrypt traffic. Use at least 4096 bit.
- Do not publish your public key to key servers.
- Never mail to or from your personal email.
- Use separate burner phones to authenticate.



# Pretty Good Privacy (PGP)

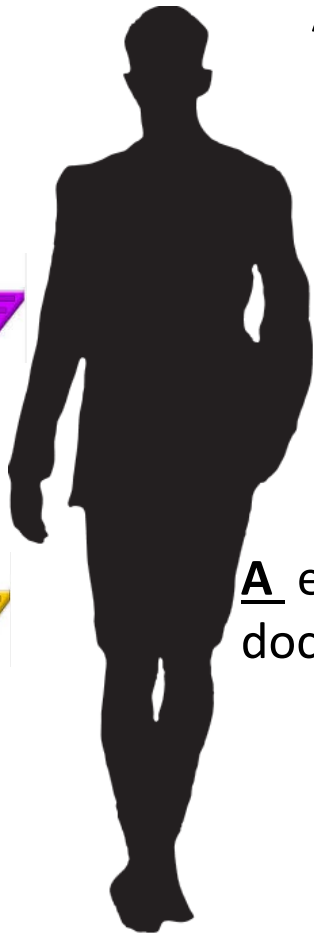
A and B agree to exchange public keys



Public Key



Private Key



A

A uses B's public

key to encrypt document  
A emails Encrypted document to B  
document emailed to B with private key



B



Public Key



Private Key

# PGP Cont.

- Encrypt everything!
- Encryption is worthless with weak passwords.
- If your private keys are compromised so is your encryption.
- Never use any personal identifying info even if it is encrypted.
- Change your keys often.

# PGP Encrypted Email

-----BEGIN PGP MESSAGE-----

Version: GnuPG v2.0.20 (MingW32)

hQEMA5EOTKIA1RLeAQgAk0+I4DzLmyygCxWs/f+R0XjVtJIFp5010gjhcZC5+h58  
9vqKZF51ld/+2vi/Jzt6vfSW2ORqPRfkeVcWCzZ4FS6RcHX6d9IkBHENDf6/US+o  
IZnqTOx/QIcEvhVqpgEs0iO1yjQ5GyPpUhPwiNchoWcEyjp6p6OjdXSnVXpR8Kw1  
6ssbTFIZOx7b0500VNH6dExhV9D86OqkGnhE7ap8IH5J8uzUJD1pPdNiRQRTu+Qv  
vb30kBQ34egGY5avJKBk88ybtXEBfaWKREbGtZaClkAOXNPjfaEmar/ENx6ceKUF  
UzEbJl7j520JFCHGEGdpQufzC8IrPazfw2XnxzZOMdLpAVzyKMr3+SENCsere+vN  
K48dKwosb0gIWFPVtWZh7swEtTRiMnyP7NkHB3PlQ3gtx7N04a5yPQJq0JBUoq0E  
S1Dv5K2q2gSL+HiCj31lDIltMHkbNGtJDP+/4ETgScId9lAKvr6FK9mzLYrp09gz  
+Y8g6Lgz+Ib6YWhQuwyG4ObqkIywZeBvtQ5yWLk9HdrOiqpBFhzLcKfs60NzWUNd  
cZIELVn7cqsS1IYBw0CtqAb80vrX6zxIS6MTjNzIwQGwcbH0uaA3ctgGbnF7/E0n  
sx8jBCA/8+nACuR3ZEmDqrhCZRvHEUWgo7tBa4Hi8oJ3JaxiO3xMJmulsN2PDyg/  
dj+AG6hVJidNBdvBQmFOCdcDTAaBSMPxHeZQeEKoHXG6l7QQR9ZsHuN+1+tRPTZy  
1dXWZwcz9Ei55+vO2xwIjVpYfjQT11qofHbVOftn61LSVuLtTnLDP+pVW6tmalai  
zGrqrBK9gm0A7XqIpIF7LqurDVODH0+NvYC75xQwHPOQ7An9P8JUvjmWUbPEZsBJ  
lmwb3weQ9WorCYHX2SC16gTLFaKAvyRZyCkivdy2HZQJFnOuCtxN49Kwr37zcam2  
Ic9+8IwQcEzwcMO+0W1VumPsTTglnWEXu5JQ1OZC2Oa+6laa5XxbmV0b059P25O+  
gKpfQUgVNUF0IicVYCEzH+cZjZ8+JtL+WilO7gsQAYa4w/eP/nRQXKVgA==  
=ZZ4U

-----END PGP MESSAGE-----

# Let's Recap

Burner Phone  
Burner Laptop  
Tails USB Key  
Public Wifi  
Cash  
Tor  
Anon Emails  
PGP Keys  
Coffee !!





# BitCoin

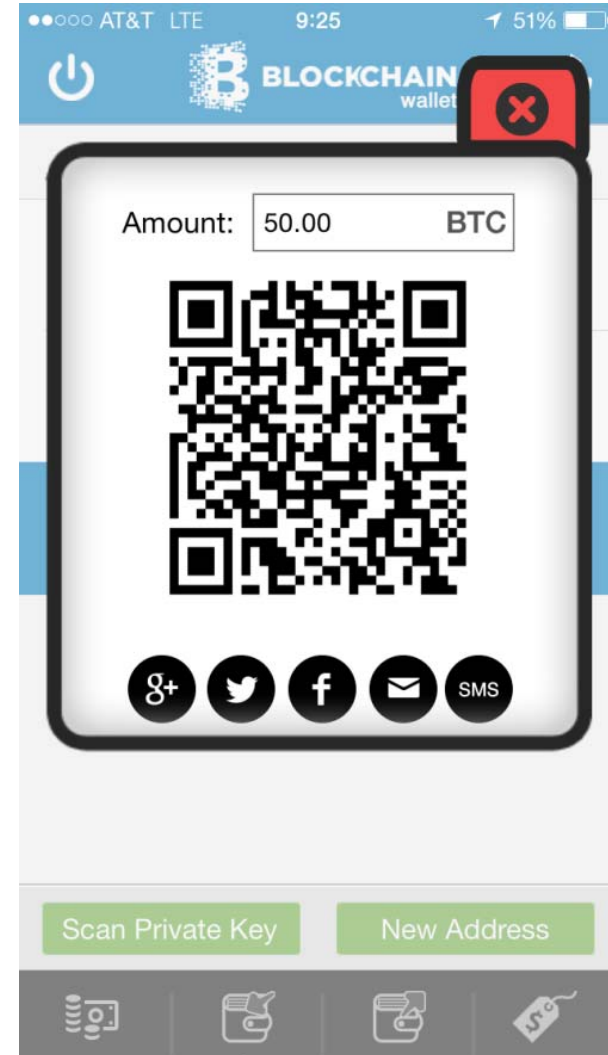


Satoshi Nakamoto

# What Bitcoin Is

- A decentralized digital currency
- Not under control of any govt. or central authority
- You can obtain them P2P, by selling services or products, or from on ramps.
- 1CvSGR947LmbRzRNciDmJcXyVoTGfJxdEg

# Bitcoin Cont.



# Bitcoin Mixing Services

Carding



Portable Magnetic Stripe Readers

[Tyner Weekly Specials Click Here](#)

Closed September 26

US and Canada 800-640-9792

International 469-952-2527

[Monthly Specials](#)

[Card Readers \(desktop\)](#)

[Portable Magnetic Stripe Readers](#)

[Card Writers](#)

[Card Reader Bundles](#)

[Card Super Bundles](#)

[Embossers](#)

[Time and Attendance](#)

[Tippers](#)



[Cash Payments](#)

[Home Page](#)

[Contact Us](#)

[Terms Of Sale](#)

Hours: Monday - Friday, from 8am to 4:00pm Central

These magnetic card reader products are new and original, and come complete with software, cables, and power cord sets.

model	<a href="#">Mini400-2G</a>	<a href="#">Mini400b Bluetooth</a>	<a href="#">MSR600 (mini600) with LCD display</a>	<a href="#">MSR500M (mini123)</a>	<a href="#">MSR500EX (mini123ex) Extreme</a>	<a href="#">MSR400U (mini400) USB</a>	<a href="#">TA32 (PMR600)</a>
size	L 2.5 x W 0.7 x H 1.0 inch (L 6.6 x W 1.9 x H 2.5 cm)	L 3.25 x W 0.75 x H 1.0 inch L 8 x W 1.5 x H 2.5 cm	2.25" x 1.80" x 0.75"	1.7" x 1.2" x 1.45"	1.6" x 0.8" x 1.2" (L 4.7 x W 2.2 x H 3.1 cm)	3.23" x 0.75" x 1.0"	3.25" x 0.8" x 1.05"
memory	2 million	512k	512k	512k	512k	512k	512k
tracks	1, 2, & 3	1, 2, & 3	1, 2, & 3	1, 2, & 3	1, 2, & 3	1, 2, & 3	1, 2, & 3
swipes stored	8200	2000	2000 - 3000	2000 - 3000	3000	2000 - 3000	1,000 - 3,000
color	black	black	black	black	black	black	black
computer interface	USB	Bluetooth and USB	USB	serial or USB	USB	USB	USB
software	yes	yes	yes	yes	yes	yes	yes
weight		1.8 oz	1.9 oz	1.8 oz	1.2 oz	1.7 oz	1.8 oz
date/time	yes	yes	yes	yes	yes	yes	yes
Retail	\$575	\$565	\$340	\$275	\$395	\$325	\$355
September Special	<b>\$270</b>	<b>\$315</b>	<b>\$300</b>	<b>\$200</b>	<b>\$210</b>	<b>\$210</b>	<b>\$275</b>

There are other places in the deep web

## Card Encoder



# Dead Drops

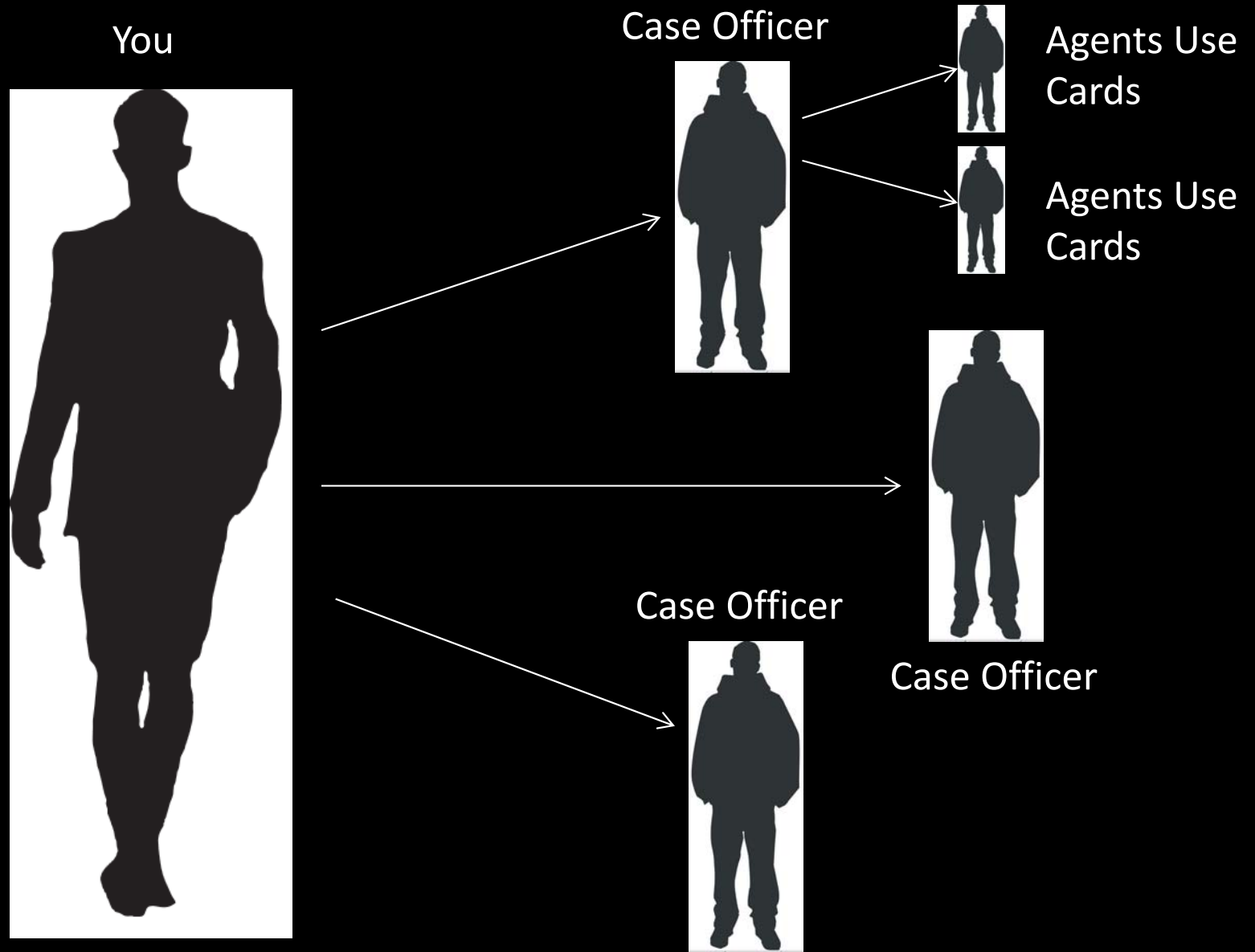
- Packages should be shipped to vacant houses
- Track packages online and get quickly
- Use Tor to track packages
- Remember “Golden Rule”
- Use Mules/Runners to get packages for you
- The more layers the more anon. but more complex to manage
- Don't get lazy!



# Counter Surveillance Routes

# Agent Handling

“It only takes one slip to compromise your true identity”



A scenic sunset over a body of water. The sun is a large, bright yellow orb on the right side of the horizon, casting a shimmering reflection on the water. The sky is a mix of blue and orange, with large, white, fluffy clouds on the left. In the foreground on the left, there is a tree with yellow autumn leaves and a dark, rocky shore.

# Good Side of the Darknet

# Russia might ban Tor and virtual private networks

By Joel Hruska on February 13, 2015 at 12:21 pm | [67 Comments](#)



## Share This Article



Vladimir Putin's reign over Russia has been marked by attacks on independent journalism, the invasion of Georgia and the Ukraine, state approval of violence against gays and

lesbians, and the most bloated, corrupt Winter Olympics in history, so it's not particularly surprising to see the Kremlin preparing to move against Tor and VPN services.

Privacy and Anonymity = Freedom

Demo