ANONYMOUS SURFING AND MESSAGING

Your Instructor

James Dill, Deputy Chief, Retired
PA Office of Attorney General

Instructor and SME for – Professional Law Enforcement Training, LLC

President of Innovative Technology & Investigative Solutions, LLC

jdill@itis-llc.com
717-884-8167
Survey

• On a Scale from 1 to 5 rate your technology skills

Anonymous Surfing

• In the United States, the use of privacy tools is not restricted.
• It is embraced by privacy organizations to prevent governments and hackers from spying.
• It is said to be used by students, journalists, whistle blowers, and anyone who has a need for privacy.
• However, it has become a very popular tool for criminals.
Proprietary Messaging Apps

- App based messaging
- Both the sender and receiver must have app.
- Often encrypted
- Use the data network on cell phones (similar to email)
- Carriers can’t track and have no records of these proprietary messages
App Messaging Services

- WhatsApp
- Jaxtr
- Kik Messenger – Photo Bomb
- Viber (phone & text)
- Text Plus
- TxtDrop
- Hide My Text
- iMessenger
- Shady SMS
- SMS Calculator
- Many Hidden

Apps use a smartphone's data plan or Wi-Fi to transmit and receive messages, a feature that appeals to individuals looking to avoid text messaging by phone service providers.

Message Content

- With many proprietary messaging apps such as Kik the conversations are ONLY stored on the devices of the users involved in the conversation.
- The app creators do not see or store chat message text or content in their systems, and don’t have access to this information.
No Phone Number Necessary

- Username identify users not phone numbers.
- This allows users with no cellular data plan to use WiFi to send texts.
- Popular with devices such as iPods, iPads, Kindle Fire, etc. that do not have cellular connectivity.

Encrypting & Self Destructing Messaging Apps

ITIS, LLC  All Rights Reserved
Encryption

• In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor.

• End to end encryption (E2EE) - Continuous protection of transmitted information by encrypting it at the origin and decrypting at its destination.
  – No third party or back door methods of unencrypting.
• Many social media messaging services are employing E2EE

Self Destructing Text Messages

• Enables the user to send text messages that will delete after a certain time limit.
• Sender set the “lifespan” or time limit or “delete on read”
• Once a message expires it is also purged from the servers where the text messages are stored.
Self Destructing Text Messages

- Tiger Text CNN Video
- FBI Intel Report

CoverMe Private Text Messaging

Lock up Secret Contacts, Photos & Videos

Secure Messaging
- Send self-destructing messages
- Remotely wipe/recall messages
- Military grade encryption

Secure Phone Calls
- VoIP avoids phone networks
- Leave no carrier call logs
- Military-grade call encryption
- Instant, crystal clear sound

Powerful Access Control
- Password access control
- Main and decoy passwords
- Intruder photo capture & GPS
- 'Shake to Lock' feature

ITIS, LLC  All Rights Reserved
Telegram Secure Messaging App

Cyber Dust

Every spoken word isn’t recorded. Why should your texts

ITIS, LLC  All Rights Reserved
The service enables users to send out fleeting messages that appear one line at a time to safeguard the application against screenshot saving.
How to defeat screenshot detection

• Once you received the Snapchat put phone in airplane mode.
• Open Snapchat & take screenshot.
• Log off & close app.
• Go to Application Manager & clear data.
• Take phone out of airplane mode
• Log back into Snapchat – photo won’t even be opened.

SnapHack App

Other Apps created to defeat Snapchat:
• Snapsaved,
• Snapsave,
• SnapSave,
• Snapchat Save Pic,
• Snap Save,
• Snapkeep,
• SnapBox,
• SnapSpy,
• KeepSnap,
• Snapchat Saver,
• Save My Snaps.

Note: many of these have been shutdown
Kik Messenger – Photo Bomb

Photo Bomb
for Kik Messenger

This is a test drive of Photo Bomb, a website optimized for Kik. For the full mobile experience complete with effortless sharing, we recommend getting Kik Messenger.

Wickr - The Anti Forensic App

• Military-grade encryption of text, picture, audio and video messages.
• Encrypts, shreds, hashes and rewrites deleted files.
• Sender-based control over who can read messages, where and for how long.
• Wickr deletes all metadata from your pictures “Leaves No Trace”.
• Soon computer browser and Email plugins
Safe Slinger

- **SAFESLINGER App For Mobile Devices**
  
  - SafeSlinger makes sending secure messages easy. Just keep your passphrase a secret, and only you and the other party can read messages. Messages cannot be read by your cellular carrier, Internet provider, employer, or anyone else.
  
  - Developed by Carnegie Mellon University

Mobile Apps

- **Signal Private Messenger (iPhone & Android)** - a voice over Internet protocol (VoIP) program that encrypts phone calls and messaging.
- **Their servers are built from the ground up with no back doors.**
- **Part of Whisper Systems Mobile Security**
- **Commercial Version “Silent Circle”**
Facebook Messenger deploys Signal Protocol for end to end encryption

- **Signal Protocol** powers a private messaging app, Signal. The protocol is designed from the ground up to make seamless end-to-end encrypted messaging possible and to make private communication simple.

- To amplify the impact and scope of private communication, **WhisperSys** also collaborate with other popular messaging apps like WhatsApp, Google Allo, and now Facebook Messenger to help integrate Signal Protocol into those products.

Facebook Messenger Secret Conversation

- Available for iOS or Android
- Encryption IS NOT the default mode it must be activated.
- Doesn't encrypt previous messages.
- Does not work with Group Messages.
- Has a self-destruct feature that can be set from 5 seconds to 1 day
- Demo
Understanding IP Addressing

How Do They Work?

**PROXY SERVERS & ONION ROUTING (TOR)**

IP Addressing

- IP address, or "internet protocol address", is a unique identifying number given to every single computer on the Internet. Like a car license plate, an IP address is a special serial number used for identification.

- Any machine connected to the Internet has an IP address: Xbox games, cell phones, fax machines, and even soda pop dispensers have IP addresses.
IP Version 4

- IP addresses have two common formats. IP version 4 addresses are comprised of four numbers-only segments separated by dots:
  - e.g. 127.0.0.1
  - e.g. 253.16.44.22
  - e.g. 72.48.108.101

IP Version 6

- IP version 6 addresses are more complex. IPv6 addresses are comprised of 8 segments:
  - e.g. 3ffe:1900:4545:3:200:f8ff:fe21:67cf
  - e.g. 21DA:D3:0:2F3B:2AA:FF:FE 28:9C 5A
Internet Service Provider

• Your ISP has a block of IP addresses to lend.
• Those ISP's, in turn, assign the IP addresses to every server and every internet user who logs on.
• An IP Address can be: "Dynamic or Static"
• An agency or company can serve as their own ISP.
• How do you determine what IP Address you are broadcasting to the public: www.whatismyipaddress.com

"Whois"

• "Whois" is a service that basically answers the question "who is X" where X is an IP address, a domain name, and several other things.
• The world is divided into five Regional Internet Registry Networks (RIRs)
• ARIN, the American Registry for Internet Numbers, is a good place to start, but remember there are other RIRs.
Regional Internet Registry System-RIR

- African Network Information Center (AFRINIC) for Africa
  [http://whois.afrinic.net](http://whois.afrinic.net)
- American Registry for Internet Numbers (ARIN) for the US, Canada, parts of the Caribbean, and Antarctica. [http://whois.arin.net](http://whois.arin.net)
- Asia-Pacific Network Information Centre (APNIC) for Asia, Australia, New Zealand, and neighboring countries: [http://whois.apnic.net](http://whois.apnic.net)
- Latin America and Caribbean Network Information Centre (LACNIC) [https://whois.lacnic.net](https://whois.lacnic.net)
- Réseaux IP Europeens Network Coordination Centre (RIPE NCC) for Europe, Russia, the Middle East, and Central Asia [http://whois.ripe.net](http://whois.ripe.net)
This is typical of what you’ll get: information that identifies the ISP who owns the “block” of IP addresses that contains the IP address that you asked about. In this case, the block is owned by Verizon Wireless and includes all IP addresses from 72.96.0.0 through 72.127.255.255.

With a court order, law enforcement would then approach the ISP for more detailed information about who that IP address was assigned to at the time in question.

Another Tool - Reverse DNS Search

- **DNS** is the mapping of a domain name, like “askleo.com”, to an IP address.
- **Reverse DNS** does, as its name implies, the reverse: given an IP address, it finds the domain name that has been assigned as the primary identifier.
- I’ll use a tool from a third-party vendor this time, [http://whois.domaintools.com](http://whois.domaintools.com) to search for an IP address & the domain name: [http://pacfe.org](http://pacfe.org)
Anonymous Surfing
Proxy Server

• In the United States, the use of privacy tools is not restricted.
  – A proxy is a computer network that allows its customers to make indirect network connections to the Internet.
  – Proxy Servers act as an intermediary and intercept all messages entering and leaving the network. It effectively hides the true network addresses.
  – Proxy Servers come in a few varieties

Proxy Servers - How it Works
Website-Based Proxy Servers

- A website-based proxy server provides a place for you to enter the URL of a website that you wish to visit anonymously.
- When you submit the form, the website proxy server makes a request for the page that you want to visit.
- The proxy usually does not identify itself as a proxy server and does not pass along your IP address in the request for the page.
- Many Proxy services keep NO records
  - Hide My Ass
  - Hide.me
  - Dozens of others

Browser-Configured Proxy Servers

- You configure the settings of a Browser to use the address of the proxy server
Proxy Server Using a VPN

- **VPN – Virtual Private Network**
  - A VPN is an application that protects your data and identity over public networks such as the Internet and wireless hotspots.
  - A VPN uses a system of special protocols to create an encrypted tunnel that transports data securely.
  - VPN services offer up different "gateway" cities, allowing you to choose where the IP address assigned.
  - **Video tutorial**

Examples of VPNs

- VyprVPN
- PureVPN
- Hide My Ass
- Proxify
- Spotflux
- Many others
The Internet we see is only a small percentage of the actual Internet!

The Deep Web is that part of the World Wide Web that is NOT indexed by major search engines such as Bing & Google.

The Dark Web is the encrypted portion of the Internet that can only be accessed via a special Browser such as TOR.
The Dark Web

• Many criminals use the Dark Web as a means of avoiding Law Enforcement.
• According to the survey conducted by researchers Daniel Moore and Thomas Rid (in their book Cryptopolitik and the Darknet), it is found that 57% of the Dark Web is occupied by unauthorized contents like Pornography, Illicit Finances, Drug Hub, Weapon Trafficking, counterfeit currency flow and many more.
• **Tor**, or “onion routing” is a free, open-source program developed by the United States Navy Research Laboratory in the mid-1990’s to hide communication. The Laboratory publicly released the code for Tor under a free license in 2004.

• It bestows online anonymity via a circuit of multilayered, encrypted connections routed through a worldwide volunteer network of servers in order to conceal a user’s location or usage from anyone conducting network surveillance or traffic analysis.
How TOR Works

How Tor Works: 2

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

How Tor Works: 3

Alice

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.

Jane

Dave

Bob
TOR Surges Since Snowden

The Tor Project - https://metrics.torproject.org/

TOR & VPN
Double Encryption

VPN + Tor Network Map

ITIS, LLC All Rights Reserved
Ross Ulbricht was the man behind Silk Road, the internet’s biggest market for illegal drugs — which was hosted on the dark web. Ulbricht was caught by the FBI in 2013 and sentenced to life in prison.

Perhaps the most famous site on the dark web was the first Silk Road. Source: AP

Getting to The Dark Web

• **Use Extreme Caution!!!** You can easily fall prey to malware, a virus, or a government honeypot.
• **Download the TOR browser**
  – [https://www.torproject.org/](https://www.torproject.org/)
  – Launch it
• **Find .onion sites**
  – One way is to go to [www.Pastebin.com](http://www.Pastebin.com)
  – Search for .onion
Getting to the Dark Web

• However, there are Deep Web Search Engines that crawl over the TOR network and bring the same result to your regular browser. Such as: Onion.City
• Example (launch from TOR Browser)
  – http://tfwh3y7tdfzljmat.onion/index.php
  – http://jh32yv5zgayyts3.onion/ (.Onion Link List and Reviews)
  – https://facebookcorewwwii.onion/

Smokeables

Welcome to Smokeables! Finest Organic Cannabis, shipping from the USA!

Original OG Kush

We are one of the few online dealers having access to original OG Kush clones. Get yourself some of the original OG Kush.

We only grow in soil wth organic nutrients.

<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 ounce of OG Kush</td>
<td>250 USD = 0.812 B</td>
<td>1</td>
</tr>
<tr>
<td>5 ounces of OG Kush</td>
<td>500 USD = 1.624 B</td>
<td>1</td>
</tr>
</tbody>
</table>
Orbot is a free proxy app that empowers other apps to use the internet more securely. Orbot uses Tor to encrypt your Internet traffic and then hides it by bouncing through a series of computers around the world.

Law Enforcement Crackdown
Operation Hyperion

- **October 31, 2016 ICE.gov Press release.**
  - A globally coordinated law enforcement action against the buyers and sellers of illicit drugs and other illegal activities using Darknet global marketplaces was conducted Oct. 22 to 28, 2016.
  - Illegal drugs continue to be the biggest item purchased and sold on Darknet marketplaces, law enforcement agencies around the world are also seeing counterfeit prescription drugs and other counterfeit items, dangerous and deadly synthetic drugs like Fentanyl, deadly toxins, fake and stolen identities, identity documents and stolen credit card data, as well as illegal services like computer hacking, murder for hire and money laundering.
  - Operation Hyperion resulted in a number of law enforcement leads on cases related to the buying and selling of illicit drugs and other goods on the Darknet. This operation will also help law enforcement agencies continue to combat the trafficking of illicit goods and services on the Darknet through the identification of new smuggling networks and trends.
**Operation Hyperion**

- Law enforcement agencies participating in the operation included: U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI), U.S. Customs and Border Protection (CBP), U.S. Postal Inspection Service (USPIS), Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), U.S. Secret Service (USSS), Internal Revenue Service – Criminal Investigation Division (IRS-CI) Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and various state and local entities.

- International partners included Europol the United Kingdom’s National Crime Agency; Australian Federal Police; New Zealand Police and New Zealand Customs Service; Canada's Royal Canadian Mounted Police, Canada Post and Canada Border Services Agency; The Netherlands; French Customs National Intelligence and Investigations Directorate; Finnish Customs; Swedish Police Authority and Swedish Customs; Ireland’s Garda National Drugs & Organised Crime Bureau; and Spain’s Guardia Civil.

- The operation was supported by CBP’s National Targeting Center and coordinated by HSI’s Cyber Division.

---

**Feds Seize AlphaBay & Hansa Markets**

July 2017
Feds first quietly take down AlphaBay driving the business to Hansa. Then Feds took control over Hansa & kept it running for a month to covertly monitor activities of criminals.
Identifying Criminals on the Dark Web

- Police used a novel technique to unmask suspects—a booby-trapped file that drug dealers downloaded to their computers.
  - Drug dealers selling their wares on Hansa could download the file for a summary of their recent transactions.
  - Police altered the file and included a program that would cause the computer to connect to a server outside of TOR thus enabling police to identify the IP address.

Ways to Defeat TOR - Malware Operation Pacifier

- In 2015, the FBI operated one of the Internet’s largest child pornography websites (Playpen), allowing users to download thousands of illicit images and videos.
- FBI agents seized and took control of a child pornography site but left it online to catch users who would otherwise remain hidden behind TOR. In each case, the FBI infected the sites with software (malware) that punctured that security, allowing agents to identify hundreds of users.
- Over 1000 Child Pornography arrests worldwide made, but not without controversy.
FBI Operation Pacifier

FBI are being challenged on two fronts. A Federal Judge, in Tacoma, ruled they must reveal the Source Code for the malware they used. In addition, defense counsels are challenging the jurisdiction of the Federal Magistrate.

Ricochet - Anonymous IM Using TOR

Anonymous instant messaging for real privacy

Ricochet is a different approach to instant messaging that doesn’t trust anyone in protecting your privacy.

- Eliminate metadata. Nobody knows who you are, who you talk to, or what you say.
- Stay anonymous. Share what you want, without sharing your identity and location.
- Nobody in the middle. There are no servers to monitor, censor, or hack.
- Safe by default. Security isn’t secure until it’s automatic and easy to use.
Ricochet

- Ricochet uses the Tor network to reach your contacts without relying on messaging servers.
- It creates a hidden service, which is used to rendezvous with your contacts without revealing your location or IP address.
- Instead of a username, you get a unique address that looks like ricochet:rs7ce36jsj24ogfw.
- You can see when your contacts are online, and send them messages. Your list of contacts is only known to your computer - never exposed to servers or network traffic monitoring.
- Everything is encrypted end-to-end, so only the intended recipient can decrypt it, and anonymized, so nobody knows where it’s going and where it came from.

Ways to Defeat TOR Using UCs & CIs

- Drug ring using TOR for anonymity exposed - April 2012
  - Eight men on three continents arrested in $1M drug ring; proxy servers hid identities
  - DEA didn't break the case by penetrating TOR.
  - The ring was busted through the efforts of an undercover agent who "infiltrated" the operation in Los Angeles, according to U.S. Attorney's Office spokesperson Gymeka Williams.
Ways to Defeat TOR
Time Correlation

- A Harvard student was arrested and charged with making a bomb threat that caused the evacuation of four buildings and disrupted the university during final exams.
- He used Gorilla Mail & TOR to mask his IP address.
- FBI checked University Servers to see who was online & using TOR at the time the bomb scare came in.
- They identified a student who matched the criteria and he confessed during interrogation.

TOR Alternatives

I2P is an anonymous peer-to-peer distributes communication layer which is built using the open source tools. It is a complete Tor alternative.
OTHER PRIVACY TOOLS

TAILS
The Amnesic Incognito System

• Tails is one of the best Tor alternatives available out there.
• It is a live operating system which could be started from any computer using a USB drive, DVD or a SD card.
• It has in-built pre-configured apps that give you the services of a web browser, IM client, office suite, editors for image and sound etc.
• It uses Tor's services for providing the anonymity but adds extra security layers.
• This could be used anywhere without leaving any trace.

ITIS, LLC All Rights Reserved
Search Engines That Won’t Track Your Activity

• Most search engines track and report your activity.
• Tracker-less search engines are also popular in the TOR culture – like:
  – Disconnect
  – DuckDuckGo
  – IXQuick

Questions