



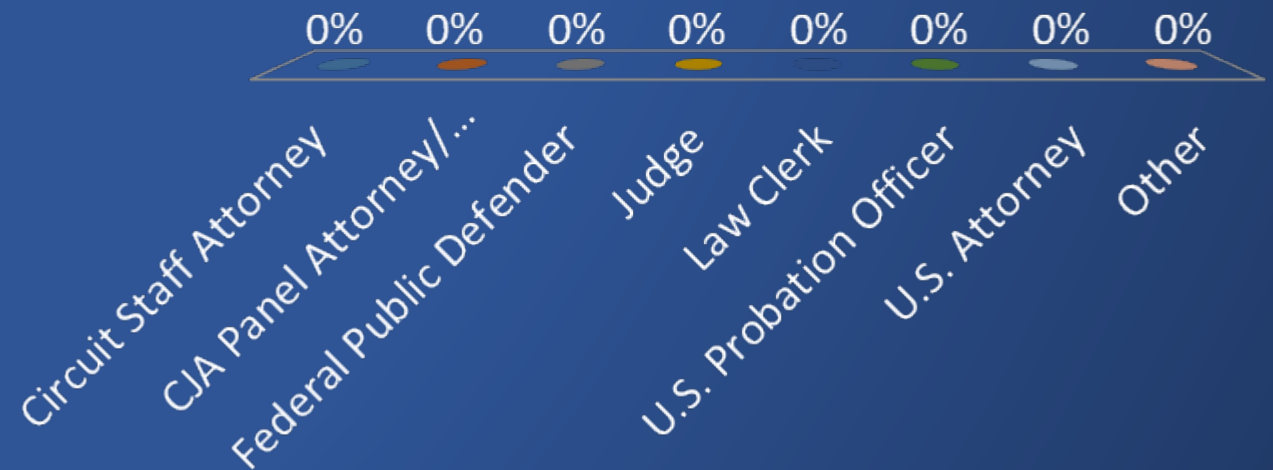


Emerging Technologies Bitcoin 101 and Ransomware

**San Antonio, TX
May 31, 2018**

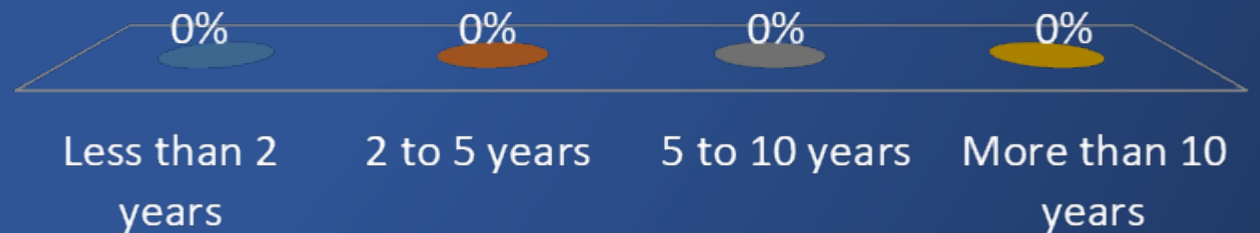
Who's in the audience?

- A. Circuit Staff Attorney
- B. CJA Panel Attorney/
Private Defense Attorney
- C. Federal Public Defender
- D. Judge
- E. Law Clerk
- F. U.S. Probation Officer
- G. U.S. Attorney
- H. Other



Years of experience with federal sentencing?

- A. Less than 2 years
- B. 2 to 5 years
- C. 5 to 10 years
- D. More than 10 years

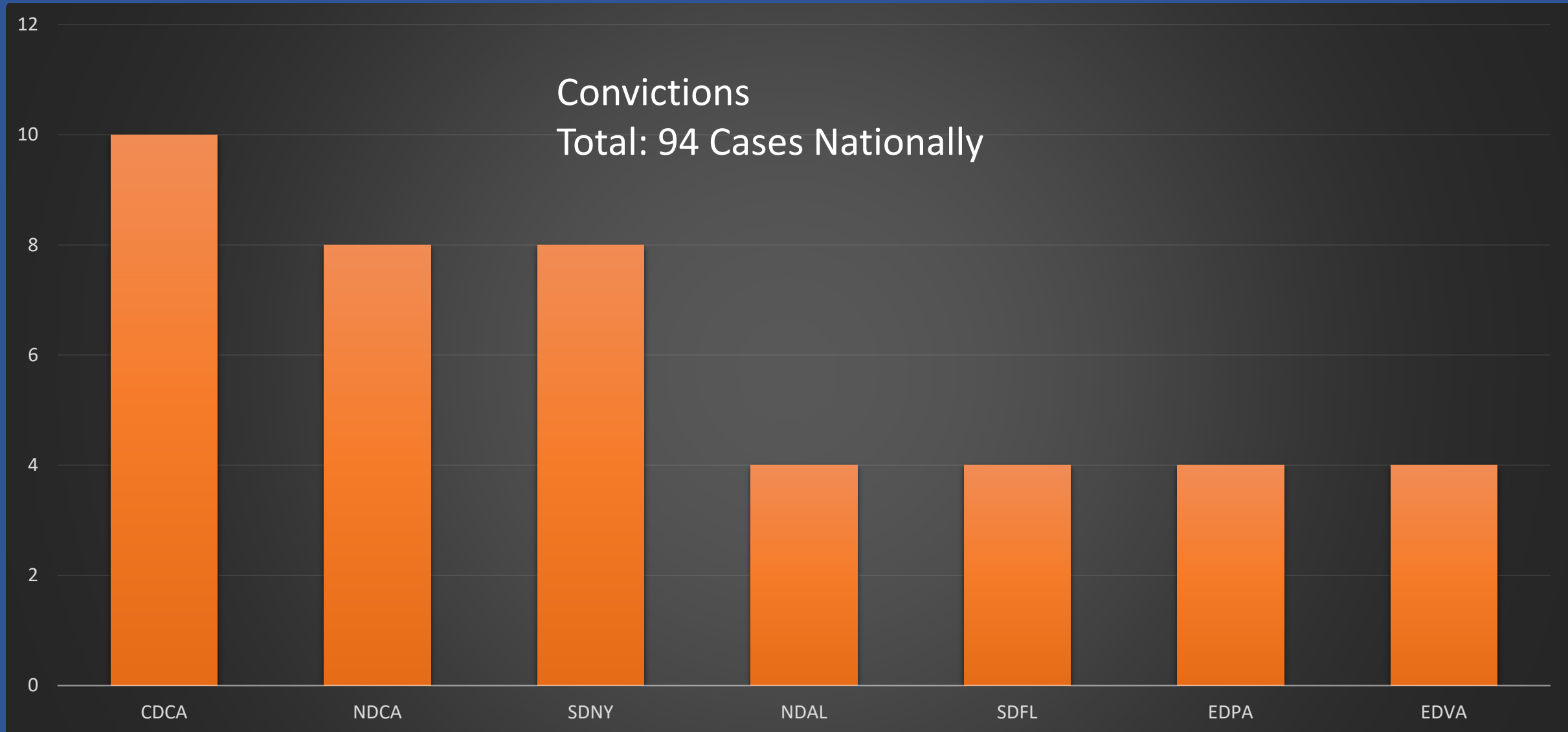


Data Breach Prosecutions -2016 & 2017 ⁵

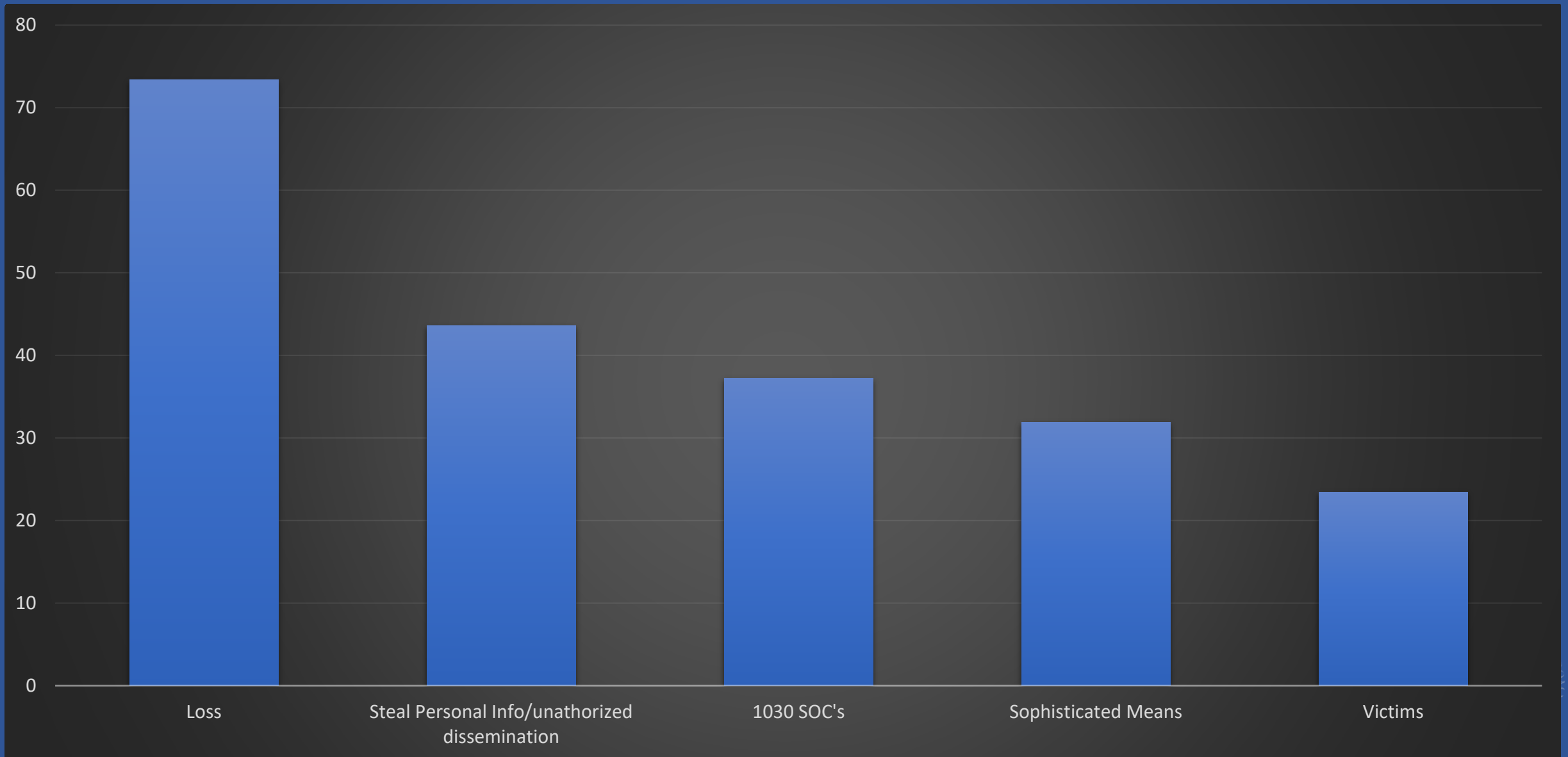


Data Breach Cases Prosecutions 2016-2017

Convictions under 18 USC § 1030 & Sentenced under §2B1.1



Most Common Chapter 2 SOC's



Chapter 3 Adjustments for 18 U.S.C § 1030 cases ⁸

| Chapter 3 Adjustment | Percent Applied in 18 U.S.C. § 1030 cases | For All Cases in 2017 |
|---|---|-----------------------|
| Abuse of Position of Trust or Use of a Special Skill | 26.6% | 2.4% |
| Aggravating Role | 7.4% | 4.7% |
| Mitigating Role | 0.0% | 8.2% |
| Obstructing or Impeding the Administration of Justice | 5.3% | 2.1% |
| Acceptance of Responsibility | 90.4% | 95.8% |



Having a Difficult Time Keeping Pace with Technology?

What is Bitcoin?
What is a Cryptocurrency?



Ransomware?

This Attachment
Seems Harmless....
Oh No....



This case involves what?
The Onion Router?



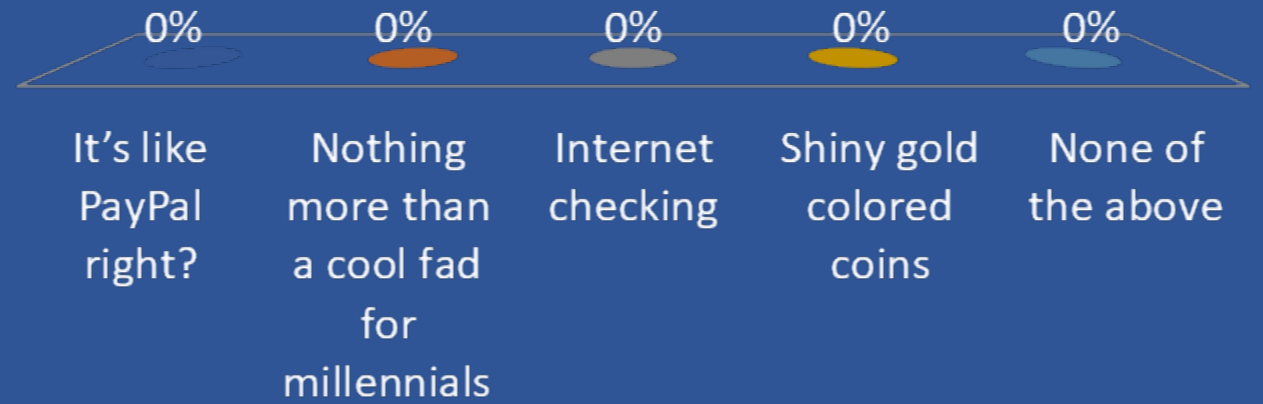
Cybercrime Cases – What is Your Comfort Level?

- A. **Excellent** – I have a Cutting Edge Knowledge of Trends and Technology.
- B. **Passable** – First Step to Learning is one Google Search Away.
- C. **Poor** – It is difficult and Overwhelming to Keep Up.
- D. **SOS** – I need help!



What is Bitcoin?

- A. It's like PayPal right?
- B. Nothing more than a cool fad for millennials
- C. Internet checking
- D. Shiny gold colored coins
- E. None of the above



When did these cases start dropping?


12

Welcome! | Silk Road

http://ianxz6zefk72ulzz.onion/index.php


Most Visited - Learn more about Tor The Tor Blog


Are you using Tor? list of TOR sites silkroad - Goo... TORDIR - Link List Welcome! | Silk Road


 **Silk Road**
anonymous marketplace

Welcome
messages(0) | orders(0) | account(฿0) | settings | log out
shopping cart (0)

Shop by category:
Cannabis(203)
Ecstasy(35)
Psychedelics(127)
Opioids(39)
Stimulants(68)
Dissociatives(9)
Other(197)
Benzos(43)


1 hit of LSD (blotter)
฿0.58


1/8 oz high quality cannabis
฿2.05


1 g pure MDMA (white)
฿1.28

Step-by-step:
1. Get **anonymous money**
2. Buy something here
3. Enjoy it when it arrives!

Vacation mode. Important info for **sellers**...

recent feedback:

| seller | rating | feedback | item |
|-----------------------------------|--------|---|----------------------|
| 1UP of Canada(97) | 4 of 5 | amazing weed. the only reason this is not a 5 is because the package was so tightly double vaccuum sealed that the product was flattened, which I know is necessary for security but it still decreases quality | item |
| CaliforniaSunrise | 5 of 5 | Fast shipping. Nice packaging. I haven't tried the chocolate yet, but it looks tasty! Smooth transaction. | item |
| Rook | 5 of 5 | all good! thanks so much! | item |
| illy | 5 of 5 | Very friendly. Fast Shipping. Great packaging. | item |
| somatik | 5 of 5 | Order arrived quickly and as described. Thanks! | item |
| gamely54 | 5 of 5 | No issue at all, I officially recommend this seller. Now go forth and purchase from him! | item |
| mellowyellow | 5 of 5 | Item arrived quickly and as described, good communication. This guy's legit. | item |
| dirtysouf(100) | 5 of 5 | looks good | item |

Ross Ulbricht

Silk Road - Life sentence related to underlying offenses facilitated through Silk Road – Drugs – Computer Hacking – Money Laundering – Fraudulent ID Documents



U.S. Immigration and
Customs Enforcement



THIS HIDDEN SITE HAS BEEN SEIZED

as part of a joint law enforcement operation by
the Federal Bureau of Investigation, ICE Homeland Security Investigations,
and European law enforcement agencies acting through Europol and Eurojust

in accordance with the law of European Union member states
and a protective order obtained by the United States Attorney's Office for the Southern District of New York
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section
issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York



[Home](#)[About Tor](#)[Documentation](#)[Press](#)[Blog](#)[Newsletter](#)[Contact](#)[HOME](#) » [PROJECTS](#) » [TORBROWSER](#)[Download](#)[Volunteer](#)[Donate](#)[Software & Services:](#) • [Nyx](#) • [Orbot](#) • [Tails](#) • [TorBirdy](#) • [Onionoo](#) • [Metrics Portal](#) • [Pluggable Transports](#) • [Shadow](#)

What is Tor Browser?

**BROWSER**

BROWSER

**DOWNLOAD**

Tor Browser

[Installation Instructions](#)[Microsoft Windows](#) • [Apple MacOS](#) • [GNU/Linux](#)

The **Tor** software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.

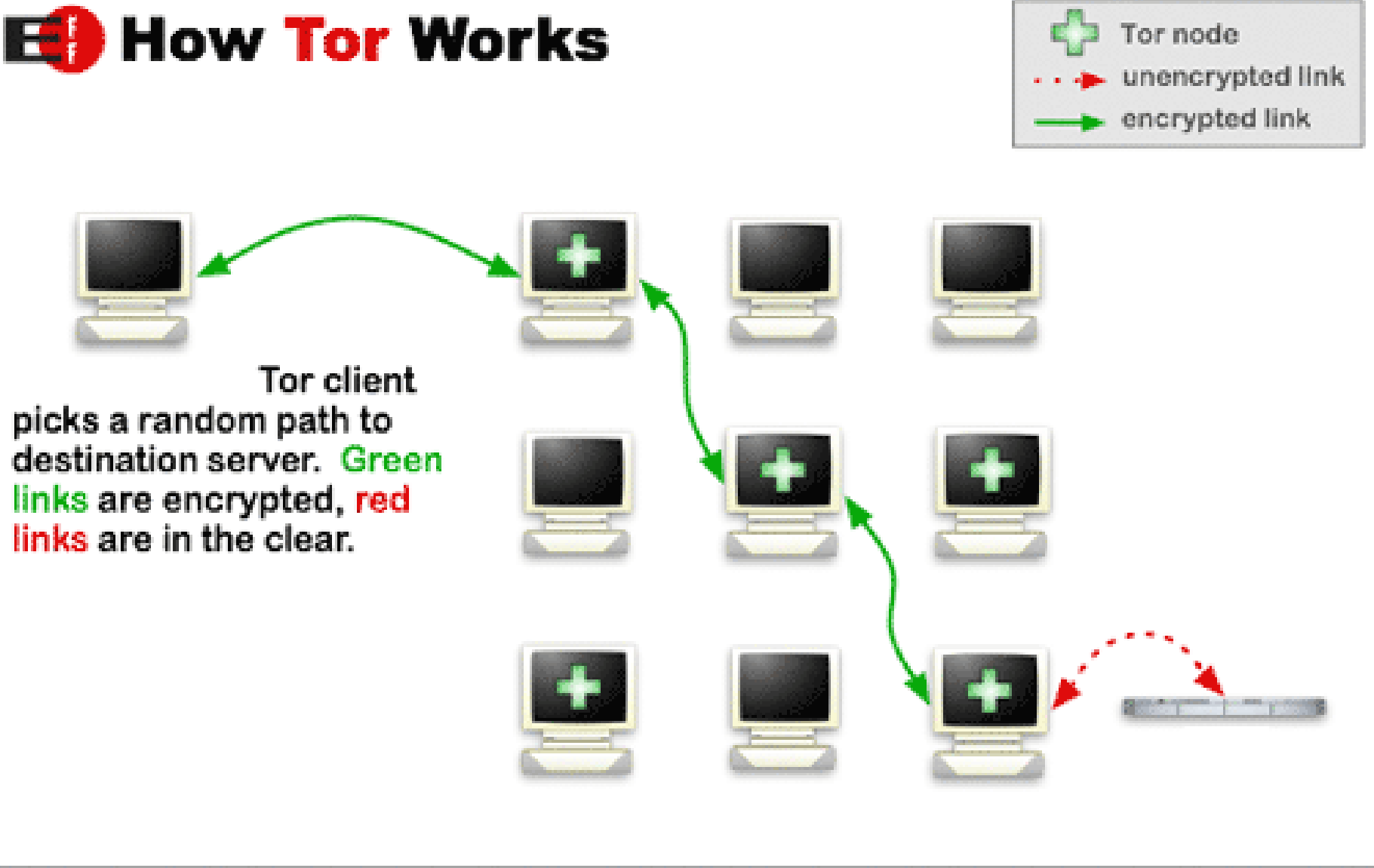
Tor Browser lets you use Tor on Microsoft Windows, Apple MacOS, or GNU/Linux without needing to install any software. It can run off a USB flash drive, comes with a pre-configured web browser to protect your anonymity, and is self-contained (portable).

[Do you like what we do? Please consider making a donation »](#)

Tor – The Onion Router



How Tor Works



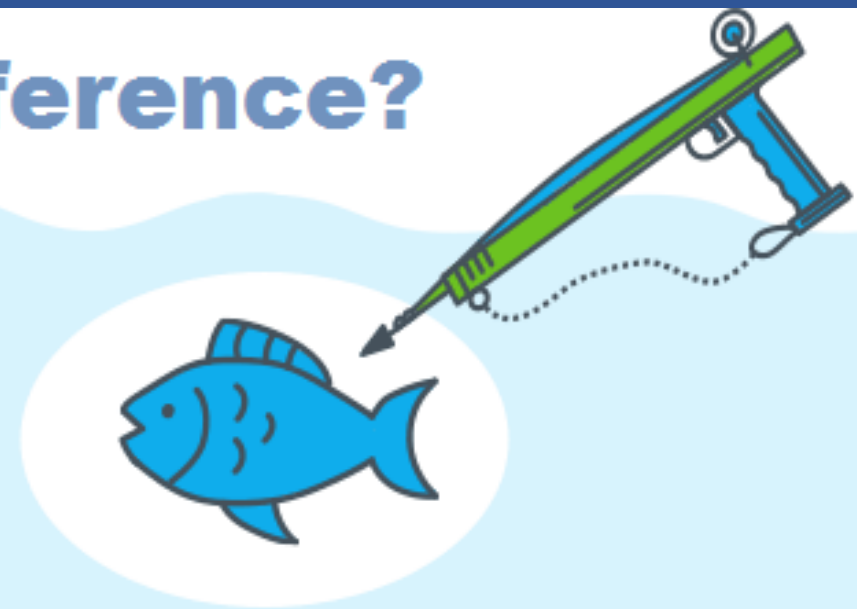
Example of Tor data transmission and encryption. Notice the red line indicating the lack of encryption outside the Tor network.

What's The Difference?



PHISHING

IS A BROAD, AUTOMATED ATTACK
THAT IS LESS SOPHISTICATED.



SPEAR-PHISHING

IS A CUSTOMIZED ATTACK ON A SPECIFIC
EMPLOYEE & COMPANY



From: "AppleID" <5i7dubsebj7p3iu7syd7oz71l@txev7wiufbg7a4qb.servicemailidsecuritywebappss.com>

Date: April 7, 2018 at 1:12:14 PM EDT

To: <[REDACTED]@yahoo.com>

Subject: [New Statement report] Your AppleID has been disabled at Sat, 07 Apr 2018, 10:12:12 AM .
Service ID#9RW3-R

Your Apple ID Has Been Disabled

Dear [REDACTED]@yahoo.com,

Review the recent login attempts on your account :

Date and Time : 07 April 2018, 10:12:13 AM

Location : Nigeria

Browser : iPhone

If you never access with the device please log into your account and verify your account.

For quick access verify your account we suggest to go to this link [Manage account >](#)

Regards

Apple Support

Phishing Attack

April 7, 2018





Payment will be raised on

5/15/2017 16:25:02

Time Left

02:23:58:28



Your files will be lost on

5/19/2017 16:25:02

Time Left

06:23:58:28



[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

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 try to decrypt some of your files **for free**. Try now by clicking <Decrypt>. 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.

How Do I Pay?



Send \$300 worth of bitcoin to this address:

[QR Code](#)

15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

Copy

Check Payment

Decrypt

ALL YOUR FILES HAVE BEEN LOCKED!

This operating system and all of important data was locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! This computer is aimed to stop your illegal activity.

To unlock your files you have to pay the penalty!

You have only 96 hours to pay the penalty, otherwise you will be arrested!

You must pay the penalty through **Bitcoin Wallet**.

To pay the penalty and unlock your data, you should send the following code:

[REDACTED]

to our agent e-mails:

thematrixhasyou9643@yahoo.com or

cremreihanob1979@yandex.ru

You will receive all necessary instructions!



HURRY UP OR YOU WILL BE ARRESTED!!!

Thank you! – Questions?



www.ussc.gov



(202) 502-4545



@theusscgov



pubaffairs@ussc.gov

Glossary

Cybercrime and Digital Forensics: An Introduction, 2nd Edition, by **Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigried-Spellar**

| | |
|--|--|
| .xxx domain | A web domain address that provides a voluntary option for individuals to host pornographic content online. |
| 1 terabyte (1 TB) | One trillion bytes. |
| 419 scams | Another term for advance fee email schemes. The name references the Nigerian legal statutes that are used to prosecute fraud. |
| Absence of a capable guardian | Variable in routine activity theory that references the lack of physical, personal, or social protection that can minimize harm to a target. |
| Access key | The password used by encryption programs that unlocks a file using the same algorithm that encrypted the information in order to decrypt it. |
| Accuracy | The integrity of the data. |
| Action Fraud | The UK national agency that handles complaints of Internet-based fraud and theft. |
| Active files | Existing files that are currently available on a hard drive, meaning they have not been deleted. |
| <i>Ad Hoc</i> phase | A term used to describe the pre-forensics age of computer forensic technologies. |
| Adam Walsh Child Protection and Safety Act | US law that, among other protections, prohibited the defense from obtaining copies of child pornography evidence, in order to limit distribution of said illicit |

materials, so long as the defense has an ample opportunity to examine the evidence at a government facility.

Admissibility The process of determining whether evidence will assist the fact finders (e.g. judge) through their decision-making process.

Advance fee email schemes A scheme where a spam mail sender requests a small amount of money up front from the recipient in order to share a larger sum of money later.

Affidavit A written, or occasionally verbal, statement to which the law enforcement officer has sworn an oath to the magistrate that the information is true and factual.

Age Verification Services (AVS) A web-based service that, upon entry into a website, verifies the age of an individual via either a valid credit card or a driver's license.

Amendment An addition or alteration to the US Constitution.

Anonymous A group that stemmed from the image board 4chan that engages in a number of hacks and attacks against targets around the world

Anti-Malware Testing Standards Organization (AMTSO) An organization that exists to provide a forum to improve the process of malware identification and product testing across the global security industry.

Anti-Phishing Working Group (APWG) A not-for-profit global consortium of researchers, computer security professionals, financial industry members, and law enforcement designed to document

| | |
|---|---|
| | the scope of phishing attacks and provide policy recommendations to government and industry groups worldwide. |
| App | A software application typically downloaded by the user that performs a certain function. |
| Apparent authority principle | US legal standard that states that if police obtain consent to search premises from someone who they reasonably believe shares a common authority over the premises then it does not violate Fourth Amendment rights even if the individual did not have the authority to give consent. |
| Appeal to higher loyalties | One of the five basic techniques Sykes and Matza developed that allows individuals to break from conformity, operating on the basis that an offense is for the greater good of the group. |
| Argot | Special language utilized by subcultures to refer to individuals in and out of the group and demonstrate connection to the subculture. |
| Arrest warrant | A signed document by a judge or magistrate authorizing law enforcement to take the person into custody. |
| Australian Federation Against Copyright Theft (AFACT) | A non-governmental federation that targets pirates in Australia and Oceania generally. |
| Authentic | A true and unaltered copy of the original data source. |
| Authenticity | The ability to prove that the evidence is genuine in a court of law. |
| BackOrifice 2000 (BO2K) | A piece of malware written by members of Cult of the |

| | |
|--|---|
| | Dead Cow which infected Microsoft BackOffice server programs. |
| Berne Convention for the Protection of Literary and Artistic Works | A legal framework created in 1986 to provide a common framework for intellectual property rights. |
| Best evidence rule | See <i>original writing rule</i> . |
| Bestiality | Experiencing sexual arousal from sex with animals. |
| Beyond a reasonable doubt | Term used to refer to the standard of proof needed in US criminal courts to show that a person on trial committed a crime. |
| BigDoggie | A website that enables individuals to access and post reviews of escort services. |
| Bill C-13 | Proposed legislation that would make it a crime to share an intimate image without the consent of the subject of the image, punishable by up to five years in prison. |
| Bill of Rights | The first ten Amendments of the US Constitution. |
| Bitcoin | A relatively anonymous form of electronic currency used by a range of actors to pay for goods. |
| Black-hat hacker | Uses techniques and vulnerabilities in order to gain access to information or harm systems. |
| Blended threat | Any form of malware that combines aspects of viruses, worms, and trojan horses together in a single tool. |
| Blind | Term used to refer to the idea that an independent forensic examiner should be completely unaware of the conclusions reached by the initial examiner. |

| | |
|---|--|
| Boot sector | A region of any sort of storage media or the hard disk of a computer that can hold code and be loaded into the computer's memory by its firmware. |
| Boot sector virus | A form of malware that operates by attempting to install code into the boot sector of either a form of storage media like a flash drive or the hard disk of the targeted computer. |
| Botnet | A form of malware that combines aspects of trojan horse programs and viruses and allows an infected computer to receive commands and be controlled by another user through Internet Relay Chat channels or the web via HTTP protocols. |
| Bridges | A hardware write blocker. |
| Bulletin board system (BBS) | A form of asynchronous computer-mediated communication used heavily during the 1980s. |
| Bureau of Customs and Border Patrol (CBP) | The US federal agency responsible for policing and managing the borders of the country and the movement of products in and out of the nation. |
| Cam whores | Performers who engage in text-based conversations with individuals viewing them on streaming-video feeds and take requests for specific behaviors or sexual acts. |
| Canadian Anti-Fraud Centre (CAFC) | A joint effort between the RCMP, Ontario Provincial Police, and the Competition Bureau, that collects reports on various forms of fraud that take place online and offline. |

| | |
|--|---|
| Canadian National Child Exploitation Coordination Center (NCECC) | The Canadian agency that serves as a focal point of contact for online exploitation cases that cross jurisdictional boundaries within Canada or internationally. |
| Capture the Flag | Competitions where hackers compete against each other individually or in teams to hack one another, while at the same time defending their resources from others. |
| Carding | When an individual sells personally identifiable information acquired in some fashion via markets operating online, most often involving the use and abuse of credit and debit card details. |
| Carding markets | Markets that enable individuals to efficiently engage in credit card fraud and identity theft with minimal effort and limited technical knowledge or skill. |
| Carnegie Mellon Report | A report published by a student at Carnegie Mellon University which suggested that over 80 percent of images on the Internet involved sexually explicit content. The findings were subsequently debunked. |
| Carrier | The transport medium for digital information. |
| Catfishing | The creation and development of relationships through social media predicated on false information. |
| Celerity | Swiftness, in the context of deterrence theory. |
| Centre for the Protection of National Infrastructure (CPNI) | The Center designed to protect UK critical infrastructure owners from emerging threats and coordinate responses in the event of a physical or cyber-based compromise. |

| | |
|---|--|
| Certainty | Refers to how likely it is that an individual will be caught and punished for an offense within deterrence theory. |
| Chain of custody | The chronological documentation of evidence as it is processed during an investigation. |
| Chaos Communication Congress (CCC) | One of the oldest and largest computer hacking and security conferences held in Europe. |
| Child Exploitation and Online Protection (CEOP) Command | The FBI-operated agency that takes reports of exploitation, abuse, and missing youth and will directly investigate threats and coordinate responses, depending on the scope of harm across multiple areas. |
| Child Exploitation Task Forces (CETF) | This FBI-operated task force provides a reactive and proactive response to online sexual exploitation cases and sex tourism practices. |
| Child love | A term used by pedophiles to describe their sexual attraction to youth. |
| Child pornography | The real or simulated depiction of sexual or sexualized physical abuse of children under 16 years of age, or who appear to be less than 16, that would offend a reasonable adult. |
| Child Pornography Protection Act of 1996 | This US Act extended existing laws regarding child pornography by establishing a new definition for this term, amending the criminal code under Title 18 to define child porn as “any visual depiction, including any photograph, film, video, picture, or computer or |

| | |
|--|--|
| | computer-generated image or picture of sexually explicit conduct.” |
| Child Protections Operations (CPO) Teams | The Australian Federal Police team that investigates and coordinates the response to child exploitation cases both domestically and internationally. |
| Child Victim Identification Program (CVIP) | A US FBI-led program that examines images of child pornography in order to determine the identity and location of child victims. |
| Children’s Internet Protection Act (CIPA) | This US federal act requires the implementation of filters in all schools that teach students from kindergarten through 12th grade. |
| Cipher | A mathematical formula (algorithm) that uses a set of rules for transforming a message. |
| Ciphertext | An illegible message. |
| Civil offense | A noncriminal offense, usually a dispute between private parties. |
| Closed source software | Software where the source code is not made available to the general public; only the object code, which restricts the ability of users to modify and share the software due to copyright infringement, is publicly shared. |
| Cloud storage | A virtual warehouse where people can store data on a network. |
| Cluster | Two or more consecutive sectors on a hard drive. |
| Code-Red Worm | A form of malware activated online on July 13, 2001 that infected any web server using Microsoft’s IIS web |

| | |
|--|---|
| | server software. |
| Collection/acquisition phase | Phase of the digital evidence collection process concerned with the retrieval and preservation of digital evidence. |
| Collision | When hashing a hard drive does not result in a unique digital fingerprint for an item, but instead the same hash value is produced. |
| Commodity | The way that the clients of sex workers describe prostitutes in online forums. |
| Communications and Multimedia Act 1998 | Malaysian act that allows law enforcement to conduct a search to compel a suspect to provide all encryption keys or passwords in order to search computerized data. |
| Compelled | Being forced to give information in the context of a police investigation or criminal court proceeding. |
| Comprehensive National Cybersecurity Initiative (CNCI) | The Presidential strategy adopted in May 2009 to strengthen America's digital infrastructure from various cyberthreats. |
| Computer-mediated communication (CMC) | Communications technologies that utilize the Internet to connect individuals, such as email, Instant Messaging Systems, and Facebook. |
| Computer as a target | When the computer or network is the aim of the attack. |
| Computer as a tool | When the computer itself is used as an instrument to commit a crime. |
| Computer as incidental | When the computer is either involved in the commission of a crime but has a smaller role, or the computer is |

| | |
|--|--|
| | being used merely as a storage device. |
| Computer contaminants | A term for a virus or malware designed to damage, destroy, or transmit information within a system without the permission of the owner. |
| Computer crime | Crime in which the perpetrator uses special knowledge about computer technology to commit the offense. |
| Computer Crime and Intellectual Property Section (CCIPS) | The sub-section of the US Department of Justice that prosecutes computer hacking cases at the federal level. |
| Computer Emergency Response Team (CERT) | An agency that serves as a coordinating point for responses to major network emergencies. |
| Computer Forensic Tool Testing project (CFTT) | Provides unbiased, open, and objective means for manufacturers, law enforcement, and the legal community to assess the validity of tools used in computer forensics. |
| Computer forensics | The investigation and analysis of media originating from digital sources in an effort to uncover evidence to present in a court of law. |
| Computer Fraud and Abuse Act (CFAA) | The first US federal law which made it illegal to engage in various forms of computer hacking and fraud. |
| Computer Security Incident Response Teams (CSIRT) | A different name for Computer Emergency Response Team. |
| Con | A computer hacking or computer security conference. |
| Concept virus | A form of malware that demonstrated the potential use of macro programming languages as a method of compromise. |

| | |
|--------------------------------|--|
| Conclusion | An overall summary of the findings derived from the examination. |
| Condemnation of the condemners | One of the five basic techniques Sykes and Matza developed that allows individuals to break from conformity, operating on the basis that those who would condemn their actions are hypocritical and doing so out of personal spite. |
| Confirmation bias | The tendency to accept information that confirms our beliefs while rejecting information that contradicts them. |
| Convention on Cybercrime (CoC) | The first international treaty designed to address cybercrime and synchronize national laws on these offenses. |
| Copyright | A legal form of protection for intellectual property that provides exclusive use of an idea or design to a specific person or company, the right to control how it may be used, and legal entitlement to payment for its use for a limited period of time. |
| Copyright Act of 1976 | The US federal law that removed the power to prosecute copyright infringement cases from state courts in 1976. |
| Copyright laws | Laws designed to protect the creators of intellectual property. |
| Coroners and Justice Act | This UK act extended the PCA to include all sexual images depicting youth under the age of 18, whether real or created. |
| Corpus delicti | Refers to the principle that a crime must be proven to |

| | |
|--|---|
| | have been committed. |
| Crack | A term that emerged within the hacker subculture to recognize and separate malicious hacks from those supported by the hacker ethic. |
| Cracker | A negative term referring to those who engage in deviant or criminal applications of hacking. |
| Crimeware | Malware that can be used as a stable platform for cybercrime, such as botnets. |
| Criminal Justice and Administration Act 2008 | This UK law criminalized the possession of extreme pornography. |
| Criminal Justice and Public Order Act | This UK act extended the PCA to include images that appear to be photos, so-called pseudo-photographs. |
| Criminal offense | The violation of a law in which a crime is committed against the state, society as a whole, or a member of society. |
| Cryptolocker | A form of malware that spreads via attachments in emails or as downloadable malware online that encrypts data on any hard drives attached to the infected system using a very strong encryption protocol and holds the user's system hostage until payment is received. |
| Cult of the Dead Cow (cDc) | A well-known hacker group in the 1990s that developed the BO2K malware. |
| Cyber trespass | The act of crossing boundaries of ownership in online environments. |
| Cybercrime | Crime in which the perpetrator uses special knowledge |

of cyberspace.

Cybercrime Act 2001

Inserted a new section into the Crimes Act 1914 giving law enforcement the ability to compel a person to provide all encryption keys or passwords when investigating a computer-related crime.

Cyber-deception and theft

All the ways that individuals may illegally acquire information or resources online.

Cyberdeviance

Any activity facilitated by technology that may not be illegal, but is not socially accepted by the majority of groups in a local area.

Cyber-porn

The range of sexually expressive content online.

Cybersmile

A charitable organization, founded in 2010, to educate the public on the harm caused by cyberbullying through service programs in schools and neighborhoods.

Cyberstalking

Online communication that may lead a victim to feel fear for their personal safety and/or experience emotional distress.

Cyberterror

The premeditated, methodological, and ideologically motivated dissemination of information, facilitation of communication, or attack against physical targets, digital information, computer systems, and/or computer programs which is intended to cause social, financial, physical, or psychological harm to noncombatant targets and audiences for the purpose of affecting ideological, political, or social change; or any utilization of digital

| | |
|-------------------------|---|
| | communication or information which facilitates such actions directly or indirectly. |
| Cyberterrorism | The use of digital technology or computer-mediated communications to cause harm and force social change based on ideological or political beliefs. |
| CyberTipline | An electronic resource operated by the US National Center for Missing and Exploited Children that provides a way for individuals to report suspected incidents of child abuse, child pornography, and sexual exploitation online. |
| Cyber-violence | The ability to send or access injurious, hurtful, or dangerous materials online. |
| Cyberwar | Term used to describe the use of cyberattacks in support of conflict between nation-states. |
| Data breaches | The illegal acquisition of mass quantities of information through hacking techniques. |
| Data recovery | Process of salvaging digital information. |
| <i>Daubert</i> hearing | A hearing in US courts to determine whether a piece of scientific evidence, a theory, or study is reliable and therefore admissible in court. |
| <i>Daubert</i> standard | The four criteria for determining whether the relevant scientific evidence, theory, or study is reliable, and therefore admissible in US courts, based on testing, publication, error rates, and acceptance of the theory or technique. |

| | |
|--|---|
| <i>Daubert</i> trilogy | The three cases that helped to establish the current interpretation of the <i>Daubert</i> standard. These cases are <i>Daubert v. Merrell Dow Pharmaceuticals</i> (1993), <i>General Electric Co. v. Joiner</i> (1997), and <i>Kumho Tire Co. v. Carmichael</i> (1999). |
| <i>Daubert v. Merrell Dow Pharmaceuticals</i> (1993) | US court case which held that any scientific expert testimony presented in federal court must undergo a reliability test. |
| Dead-box forensics | The examination of powered-down computer components. |
| DefCon | An annual computer security and hacking conference held each year in Las Vegas, Nevada. |
| Definitions | One of the four principal components of Akers's social learning theory, suggesting that the way an individual views a behavior will affect their willingness to engage in that activity. |
| Deleted files | A file whose entry has been removed from the computer's file system so that this space is now marked as usable again. |
| Denial of a victim | One of the five basic techniques Sykes and Matza developed that allows individuals to break from conformity, operating on the basis that there is no discernible victim (e.g. large corporation) or the "victim" deserved it. |
| Denial of an injury | One of the five basic techniques Sykes and Matza |

| | |
|--|--|
| | developed that allows individuals to break from conformity, operating on the basis that no one or thing will get hurt or damaged. |
| Denial of responsibility | One of the five basic techniques Sykes and Matza developed that allows individuals to break from conformity, operating on the basis that some other person, event, or situation will be directly responsible for the offense and should be blamed. |
| Denial of service | A form of cyberattack where a service or resource supported by the Internet is overloaded with requests, keeping legitimate users from access. |
| Denigration | A form of cyberbullying involving making comments about individuals' characters or behaviors that are designed to harm their reputation, friendships, or social positions. |
| De-NISTing | The process of filtering the dataset and removing non-user-created files. |
| Department of Defense Cyber Crime Center | A specialized agency run by the Air Force to perform forensic analyses and training for attacks against DoD computers and defense contractors. |
| Department of Energy | The US federal agency which oversees the production and safety of power grids and energy production. |
| Department of Homeland Security | The US federal department which houses multiple law enforcement entities and coordinates responses to cyberthreats and attacks. |

| | |
|---|---|
| Deterrence theory | This perspective argues that humans will be deterred from choosing to commit crime if they believe that punishments will be certain, swift, and proportionately severe. |
| Deviance | A behavior that may not be illegal, though it is outside of the formal and informal norms or beliefs of the prevailing culture. |
| Differential association | One of the four principal components of Akers's social learning theory, arguing that who we associate with influences our willingness to engage in crime and our exposure to definitions supporting offending. |
| Differential reinforcement | One of the four principal components of Akers's social learning theory, arguing that the punishments or positive reinforcement we receive after engaging in crime will influence our willingness to perform that act again. |
| Digital Age | The era of digital technologies. |
| Digital evidence | Information that is either transferred or stored in a binary form. |
| Digital forensics | The analysis of digital evidence, which includes network, computer, mobile device, and malware forensics. |
| Digital immigrant | Those born before the creation of the Internet and digital technologies. |
| Digital Millennium Copyright Act (DMCA) | US law designed to directly affect media piracy online through further revisions to the Copyright Act by |

| | |
|---|---|
| | extending protection to various music and performances that have been recorded in some fashion. |
| Digital native | Youths that were brought into a world that was already digital, spend large amounts of time in digital environments, and utilize technological resources in their day-to-day lives. |
| Digital piracy | A form of cybercrime encompassing the illegal copying of digital media such as computer software, digital sound recordings, and digital video recordings without the explicit permission of the copyright holder. |
| Distributed denial of service (DDoS) attack | When individuals send multiple requests to servers that house online content to the point where these servers become overloaded and are unable to be used by others. |
| Double jeopardy clause | US legal clause that states that an individual is protected from being prosecuted or punished twice for the same crime. |
| Dread Pirate Roberts | The handle for Ross William Ulbricht. Ulbricht was the site administrator for the Silk Road. |
| Drift | Term used by David Matza to refer to the transition between criminality and conformity without accepting a deviant or criminal identity. |
| Drive slack | When the operating system does not overwrite old information that was once available on the storage device between the start of the next sector and the end of the cluster. |

| | |
|--|--|
| Due process clause | US legal clause which states that the government cannot deprive someone of “life, liberty, or property” without due process, meaning the government must follow rules and procedures for conducting legal procedures to limit arbitrary decisions. |
| e-jihad | Term used to describe the use of the Internet as a venue for indoctrination and cyberattack by Islamic extremist groups. |
| Electronic Communications Privacy Act (ECPA) | The US law that enabled law enforcement to obtain the name and address of ISP subscribers, along with personal details and sensitive data. |
| Electronic Pearl Harbor | Term used to refer to an unexpected and catastrophic cyberattack against the United States. |
| Elk Cloner | An early form of malware, designed to infect Apple II computers via a floppy disk, that did not cause any actual harm but was difficult to remove. |
| EnCase [®] | A forensics tool created by Guidance Software in 1997. This automated tool can image a drive, without altering its contents, and then verify that the image is an exact copy of the original drive. |
| Encryption | The process of transforming text, such as an email, through the use of mathematical algorithms so that it is no longer legible to others. |
| Endangered Child Alert Program (ECAP) | A US FBI-led program that seeks to identify the adults featured in some child exploitation content so they may |

| | |
|--|--|
| | be brought to justice. |
| Enterprise Phase | The period of digital forensic technologies in the early 2000s marked by familiarity with digital evidence handling and the creation of tools specifically designed for digital forensic analysis. |
| Escort | A type of sex worker who operates behind closed doors and typically makes appointments with clients rather than soliciting publicly. |
| European Union Directive 2001/29/EC | Also known as the Copyright Directive, this European Union statute establishes guidelines concerning the adequate legal protection of copyrighted materials through technological means. |
| European Union Directive 91/250/EEC/2009/24/EC | A European Union statute that provides legal protection for computer programs and harmonized copyright protection across the EU. |
| Evidence integrity | The reliability and truthfulness of the evidence. |
| Examination/analysis stage | The stage of digital forensic investigation involving data recovery/extraction and analysis of digital data. |
| Exclusion | A form of cyberbullying involving intentionally keeping others from joining an online group, such as a network on Facebook or some other site online. |
| Exigent circumstance | Refers to emergency situations that allow law enforcement officers to conduct a warrantless search when they believe people are in danger or potential evidence will be destroyed. |

| | |
|--|--|
| Exploit | A program that can take advantage of vulnerabilities to give the attacker deeper access to a system or network. |
| Exploit packs | A form of malware that can infect web browsers and thereby enable remote takeovers of computer systems. |
| External hard drives | Portable storage devices located outside of the computer and are usually connected via a USB port. |
| Extraction | See <i>data recovery</i> . |
| Extreme pornography | UK-centric definition for materials produced for the purpose of sexual arousal which depicts acts that “threaten a person’s life; acts which result in or are likely to result in serious injury to a person’s anus, breasts or genitals; bestiality; or necrophilia.” |
| Fair and Accurate Credit Transactions Act of 2003 | The US law that provides multiple protections to help reduce the risk of identity theft and assist victims in repairing their credit in the event of identity theft. |
| Federal Bureau of Investigation (FBI) | A prominent US federal law enforcement agency that can be involved in the investigation of most forms of cybercrime, particularly hacking, financial crimes, and cyberterrorism. |
| Federal Bureau of Investigation’s Violent Crimes Against Children (VCAC) | This US-based law enforcement agency investigates a range of sexual offenses and criminal activities that affect youth, ranging from child pornography to sex trafficking to kidnapping. |
| Federal Rules of Evidence (FRE) | Governs the admissibility of evidence in federal court proceedings in the United States. |

| | |
|---|--|
| Federal Trade Commission (FTC) | An independent watchdog agency within the US federal government responsible for consumer protection and monitoring the business community. |
| Federation Against Copyright Theft (FACT) | The primary trade organization in the UK dedicated to the protection and management of intellectual property, notably that of film and television producers. |
| Fifth Amendment | The Fifth Amendment to the US Constitution that protects an individual from self-incrimination, double jeopardy, and deprivation of liberty without due process. |
| File | A piece of computer-based data. |
| File Allocation Table (FAT) | The type of file system used in older versions of the Windows operating systems. |
| File carving | The process of searching for a certain file signature in a hard drive and attempting to extract the associated data without regard for the file system. |
| File extension | The part of the file's name that tells the operating system what program to use to open it. |
| File sharing | The process of electronically exchanging intellectual property over the Internet without the permission of the original copyright holder. |
| File signature | An identifying value for the content of a computer file. |
| File slack | The leftover space between the end of the file and the end of the last storage unit for that file. |
| File system | The way in which data is organized and retrieved on a computer hard drive. |

| | |
|---|--|
| Financial Coalition Against Child Pornography (FCACP) | A coalition that is comprised of 39 financial institutions and Internet service providers who are jointly operating to take complaints of child pornography and disrupt the businesses that are engaged in the sale of or profit generation from this content. |
| <i>Fisher v. United States</i> (1976) | US court case which demonstrated that statements given voluntarily to police and criminal justice system actors are not protected by the Fifth Amendment. |
| Flaming | A form of cyberbullying involving engaging in online fighting where users directly target one another with angry or irritated messages, often featuring vulgar language. |
| Flash mob | Mass organizations of people who organize quickly and move rapidly through the use of online media without alerting local citizens or law enforcement. |
| FloodNet | The DDoS tool that was developed by the Electronic Disturbance Theater. The program could be downloaded directly from their website to be utilized by individuals who shared their perspectives on the use of the Internet as a space for social activism. |
| Florida Computer Crimes Act of 1978 | The US state law which was the first codified state statute regarding computer crime, involving offenses against intellectual property, offenses against computer equipment or supplies, and offenses against computer users. |

| | |
|--|--|
| Footer | The last few bytes that mark the end of a file. |
| Forensic confirmation bias | Term referencing the class of effects through which an individual's preexisting beliefs, expectations, motives, and situational context influence the collection, perception, and interpretation of evidence during the course of a criminal case. |
| Forensic science | The application of science to the law, meaning the scientific process of gathering and examining information to be used by the criminal justice system. |
| Forensic soundness | The validity of the method for collecting and preserving evidence. |
| Forensic Toolkit [®] (FTK) | Commercial software commonly used in digital forensic investigations that was created by AccessData. It is capable of imaging a hard drive, scanning slack space, and identifying steganography; however, it is also capable of cracking passwords and decrypting files. |
| Forum for Incident Response and Security Teams (FIRST) | A global organization that serves to coordinate information sharing and connections between all teams worldwide. |
| Fourth Amendment | Limits the US government's ability to search and seize evidence without a warrant. |
| Fragmented | A file that is stored in nonconsecutive sectors on a computer hard drive. |
| Fraud | Wrongful or criminal deception intended to result in financial or personal gain. |

| | |
|-------------------------------------|---|
| FRE Rule 401 | Defines relevance as the tendency to make the fact being presented in a case more or less probable. It also defines authenticity as the ability to prove that the evidence is genuine. |
| FRE Rule 702 | States that if scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education may testify thereto in the form of an opinion or otherwise. |
| FRE Rule 801 | States that hearsay is considered second-hand evidence, meaning it is testimony not based on first-hand or personal knowledge. |
| FRE Rule 901 | States “the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.” |
| Free space | The portion of the hard drive that has yet to be assigned to a partition. |
| French postcards | Images of nudes printed on postcard stock and sent through the mail to others. |
| <i>Frye</i> standard | States that scientific evidence is only admissible if it is generally accepted as reliable by the scientific community. |
| <i>Frye v. United States</i> (1923) | US court case which led to the development of the <i>Frye</i> standard for the presentation of scientific evidence. |

| | |
|--|---|
| Gatekeeper | A term used to refer to a judge in the context of assessing both the relevance and reliability of scientific evidence. |
| <i>General Electric Co. v. Joiner</i> (1997) | A US Court case that demonstrated that not only was scientific evidence under review, but so was the methodology and reliability of an expert's reasoning process. |
| General strain theory | An individual-level theory developed by Robert Agnew that discusses the role of frustrations leading to negative emotions which, if not addressed appropriately, can lead individuals to engage in crime as a response. |
| General theory of crime | Gottfredson and Hirshi's theory which argues that crime stems from low self-control and opportunities to offend. |
| Girlfriend Experience (GFE) | A term used by the customers of prostitutes to refer to a sexual experience meant to feel like a consensual relationship with no money involved. |
| Golden Age | <i>See Enterprise phase.</i> |
| Google Glass | A form of wearable technology created by the company Google. These thin glasses come with a wearable computer featuring a heads-up display that is voice activated and controlled. Users can do a variety of things while wearing Glass, including taking photos and videos, searching the Internet, checking email, and several other activities that are evolving through the creation of new applications. |

| | |
|------------------|--|
| Grand jury | A group of people that determine whether or not there is enough evidence to formally charge the individual with a crime. |
| Gray-hat hacker | A group of hackers that falls between black- and white-hat hackers who have shifting or changing ethics depending on the specific situation. |
| Grooming | The misuse of the Internet by using it to engage in inappropriate communication with children. |
| Hack | The modification or alteration of computer hardware or software to enable technology to be used in a new way, whether for legitimate or illegitimate purposes. |
| Hacker | An individual who modifies or alters computer hardware or software to enable technology to be used in a new way. |
| Hacker space | A physical location where individuals can converge to discuss technology and learn from one another. |
| Hacktivism | Using hacking techniques to promote an activist agenda or express their opinion. |
| Handheld devices | A source of potential electronic information that includes mobile phones, digital multimedia devices (e.g. iPod), digital cameras, and global positioning systems (GPS). |
| Handle | The nicknames used by individuals in on and offline environments. |
| Harassment | The repeated distribution of cruel or mean messages to a |

| | |
|-------------------------|--|
| | person in order to embarrass or annoy them. |
| Hard drives | Data storage devices used for storing and retrieving data. |
| Hardware | The tangible or physical parts of a computer system. |
| Hash | A fixed value (output) – see also <i>hashing</i> . |
| Hash algorithm | A set of calculations that takes an arbitrary amount of data (input) and creates a fixed value (output) which acts as a unique reference number for the original data. |
| Hashing | The process of creating a hash value from a variable amount of data. |
| Header | The first few bytes that mark the beginning of a file. |
| Hearsay | Term used to refer to second-hand evidence, or information obtained on a first-hand or personal knowledge basis. |
| Hidden files | Files that have been manipulated in such a way that the contents of the original file are concealed. |
| Hypothesis | A reasonable explanation as to what might have occurred or why. |
| I/O error | Input/output errors that are often the result of a bad sector on a hard drive. |
| Identification document | A document made or issued by or under the authority of a government with information concerning a particular individual intended to serve as a form of identification. |
| Identity fraud | Within the UK, this term refers to the illegal misuse of a document made or issued by or under the authority of the government. |

| | |
|--|--|
| Identity theft | Within the US, this term refers to the unlawful use or possession of a means of identification of another person with the intent to commit, aid, or abet illegal activity. |
| Identity Theft and Assumption Deterrence Act of 1998 | This US law made it a federal crime to possess, transfer, or use a means of identification of another person without authorization with the intent to commit or aid in the commission of illegal activity at the local, state, or federal level. |
| Identity Theft Enforcement and Restitution Act of 2008 | This US federal act allows offenders to be ordered to pay restitution as a penalty to victims of identity theft and enhanced existing laws regarding cybercrime. |
| Identity Theft Penalty Enhancement Act of 2003 | This US act added two years to any prison sentence for individuals convicted of a felony who knowingly possessed, used, or transferred identity documents of another person. |
| Imaging | The process of making an exact copy (bit by bit) of the original drive onto a new digital storage device. |
| Imitation | One of the four principal components of Akers's social learning theory, suggesting that an individual's first act of deviance or criminality is an attempt to model the behavior of their peers and intimate others. |
| Immigration and Customs Enforcement (ICE) | The US federal agency which manages the processing and prosecution of illegal immigrants and the movement of materials through the borders of the nation. |
| Impersonation | A form of cyberbullying involving falsely posting as |

| | |
|---|---|
| | other people to harm their reputation or social status by logging into their existing accounts to post messages or by creating fake accounts to masquerade as that person. |
| <i>In re Boucher</i> (2007) | US Court case which led to Fifth Amendment challenges to encryption protocols. |
| Incidental | When the computer is either involved in the commission of a crime in a smaller accompanying role or is being used merely as a storage device. |
| Incriminating | Information which implicates an individual in a criminal incident or wrongdoing. |
| Information Age | Period of time marked by the increased production, transmission, consumption of, and reliance on information. |
| InfraGard | A non-profit public-private partnership designed to facilitate information sharing between academics, industry, and law enforcement. |
| Intellectual property | Any work or artistic endeavor created by an individual which has been fixed in some form, such as being written down. |
| Internal hard drives | Hard drives that are installed inside a computer or device. |
| International Center for Missing and Exploited Children (ICMEC) | A non-profit agency with a similar mission to the NCMEC, though it is focused on building partnerships in a global context to better investigate child exploitation cases and build the legal capacity of nations |

so that there is consistency in laws to prosecute these offenses.

International Criminal Tribunal
The formation of a truly international court that could represent the victim nations and offenders could be a valuable tool to pursue cases where multiple nations were affected by a group of actors.

Internet Corporation for Assigned Names and Numbers (ICANN)
International organization that is responsible for the coordination and stability of the Internet over time.

Internet Crime Complaint Center (IC3)
A collaborative effort of the National White Collar Crime Center (NW3C) and the FBI operating for crime victims, consumers, and researchers to understand the scope of various forms of online fraud. Victims can contact the agency through an online reporting mechanism that accepts complaints for a range of offenses.

Internet Crimes Against Children (ICAC)
US-based local task forces that provide a mechanism for coordination between local, state, and federal law enforcement, as well as prosecutors, to combat child sex offenses.

Internet of Things
All non-computing devices connected together via the Internet, including thermostats, refrigerators, and other appliances.

Internet Watch Foundation (IWF)
A UK-based charitable organization that is focused on reducing the amount of child pornography and exploitation materials hosted worldwide, along with

| | |
|--|---|
| | criminally obscene adult content. |
| Johns | A term used to refer to the customers of prostitutes. |
| Just compensation clause | States that any property taken by the government must be for public use and the owner must be fully reimbursed its market value. |
| <i>Katz v. United States (1967)</i> | Key US court case which defined an individual's right to privacy in public spaces. |
| Key disclosure law | Legislation that mandates a person to provide encryption keys or passwords to law enforcement for digital forensic investigations. |
| Keyword search | The process of using a word or series of words to conduct a search in the entire physical drive of a computer regardless of the file systems. |
| <i>Kumho Tire Co. v. Carmichael (1999)</i> | US court case which helped inform the <i>Daubert</i> standard of evidence. |
| Lamer | A term used by hackers to refer to individuals with limited capacity and/or skills. |
| Latent | Another term for hidden. |
| Law Enforcement and CSIRT Cooperation (LECC-BoF) | A sub-group of FIRST designed to provide a venue for police and response teams to work together and create trusted relationships between these communities. |
| Law Reform Commission | Irish body of law which helped inform standards of evidence. |
| Legacy systems | Outdated computer systems, devices, or software. |
| Liberty Reserve | An electronic payment processor who is being |

| | |
|-----------------------------------|---|
| | prosecuted in the US for its role in money laundering for various forms of crime. |
| Logical extraction | The process of identifying and recovering data based on the file systems present on the computer hard drive. |
| Lori Drew | A woman alleged to have created a fictitious MySpace profile in order to harass a 13-year-old girl named Megan Meier, who eventually committed suicide as a result of contact with Drew's profile. |
| Low Orbit Ion Cannon (LOIC) | The DDoS tool that is used by the group Anonymous to support attacks against personal, industrial, and government targets around the world. |
| Macro virus | A popular way to infect systems by using a common weakness in a variety of popular programs like Excel, Word, and PDFs. |
| Macro programming language | A programming language common to Microsoft Office products that was used by virus writers to compromise user systems. |
| Magic numbers | <i>See file signatures.</i> |
| Malicious Communications Act 1998 | Enables individuals to be prosecuted for sending messages to another person for the purpose of causing fear or anxiety. Revised in 2001 to include electronic communications of any kind that convey a threat, indecent or offensive content, or information that is false. |
| Message parlor | A business that operates as a supposedly legitimate |

| | |
|---|---|
| | <p>message clinic but actually provides sexual services to clients.</p> |
| Master File Table (MFT) | <p>Contains information about all of the files, folders, and directories on a drive.</p> |
| Megan Meier | <p>A young woman who committed suicide after receiving bullying messages from a fake MySpace profile, alleged to have been created by Lori Drew, the mother of one of Megan's friends.</p> |
| Megan Meier Cyberbullying Prevention Act | <p>Proposed US federal legislation would have made it illegal for anyone to use CMC "to coerce, intimidate, harass or cause substantial emotional distress to a person," or use electronic resources to "support severe, repeated, and hostile behavior." This resolution was not successfully passed into law.</p> |
| Melissa virus | <p>A well-known virus that spread throughout the globe in the 1990s.</p> |
| Message Digest Version 5 (MD5) | <p>A type of hashing algorithm that takes a large amount of data of arbitrary length (input) and calculates a unique "fingerprint" of this data expressed as a unique combination of hexadecimal digits of a specified length (output).</p> |
| Metropolitan Police Central e-crime Unit (PCeU) | <p>The London, England police agency that responds to serious forms of cybercrime affecting citizens.</p> |
| Microsoft Digital Crimes Unit | <p>A working group created by the Microsoft corporation to combat cybercrime in conjunction with law</p> |

| | |
|--|---|
| | enforcement. |
| Mileage | Term used by the customers of prostitutes in web forums to refer to the appearance of sex workers and their deterioration in appearance over time in the sex trade. |
| <i>Miller v. California</i> | US court case which established the definition of obscene content that is still in use today. |
| Morris worm | The first worm created by Robert Morris that caused substantial harm to the Internet in the 1980s. |
| Motion Picture Association of America (MPAA) | The US association that operates to protect the intellectual property of their artists and creative producers. |
| Motivated offender | Variable within routine activity theory that constitutes any individual or group who has both the inclination and ability to commit crime. |
| MP3 format | A software standard designed to compress audio files. |
| MuTation Engine (MtE) | A polymorphic generator that not only encrypts a virus but randomizes the routine used so that it varies with each replication. |
| Napster | A popular file sharing program developed in 1999 that allowed a larger population of Internet users to engage in piracy. |
| Nation-state actor | Hackers who engage in attacks at the behest of or in cooperation with a government or military entity. |
| National Centre for Cyberstalking Research | A UK-based research center designed to address the problem of cyberstalking. |

| | |
|---|--|
| National Center for Missing and Exploited Children (NCMEC) | One of the key non-profit organizations in the US that deals with missing children and child exploitation. It performs multiple roles to facilitate the investigation of crimes against children. |
| National Crime Agency (NCA) | UK national criminal justice agency that has both national and international reach and works in partnership with law enforcement organizations to particularly focus on serious and organized crime. |
| National Crime Victimization Survey-Supplemental Survey (NCVS-SS) | A US-based survey with a nationally representative sample of respondents that demonstrates the prevalence and incidence of cyberstalking. |
| National Fraud Authority (NFA) | This UK agency was formed in 2008 in order to increase cooperation between the public and private sectors to investigate fraud. |
| National Fraud Intelligence Bureau (NFIB) | The NFIB collects information on various forms of fraud and aggregates this data along with reports from business and industry sources into a large database called the NFIB Know Fraud system. It is operated by the City of London police. |
| National Incident-Based Reporting System (NIBRS) | The US-based incident reporting system used by law enforcement agencies to collect and report data on crime. |
| National Security Agency (NSA) | The US agency which supports offensive and defensive operations in support of US military and civilian networks. |

| | |
|---|--|
| National Software Reference Library (NSRL) | The US NIST-supported reference library that maintains details on various software programs. |
| Nation-state | A nation-state is any sovereign nation with a defined territory and a governmental organizational structure. |
| Necrophilia | Experiencing sexual arousal from sex with the dead. |
| Neighborhood Children's Internet Protection Act (NCIPA) | This US law requires Internet filtering technology in public libraries to block young people from accessing harmful content, including pornographic and obscene materials. |
| Nested search | A search within a search. |
| Networking | A way in which those who have sexual attraction to children may misuse the Internet to communicate and share ideas with like-minded persons. |
| New Technology File System (NTFS) | The current file system for Windows NT operating systems. |
| No Electronic Theft (NET) Act of 1997 | A US federal law designed to increase the penalties for the duplication of copyrighted materials. |
| Non-nation-state-sponsored actor | An individual who acts without any sort of state or military backing. |
| Noob | An individuals new to hacking and with minimal knowledge of technology. |
| Object code | Code that restricts the ability of users to modify and share the software due to copyright infringement. |
| Obscene Publications Act (OPA) 1959 | Law applicable in England and Wales that indicates any article may be obscene if its effect on the audience |

| | |
|-------------------------------|--|
| | member who reads, views, or hears it is to “deprave and corrupt.” |
| Obscene Publications Act 1857 | This UK act made it illegal to sell, possess, or publish obscene material, which was not clearly defined in the law. |
| Obscenity | Term used to refer to content that may be indecent, lewd, or vulgar, which varies based on the legal standards of a given nation. |
| Observation | The first stage of the scientific method. |
| Online harassment | The repeated distribution of cruel or mean online messages to a person in order to embarrass or annoy them. |
| Open-field searches | A form of legal search that can be conducted by law enforcement without a warrant in any open field or large area that cannot be considered persons, houses, papers, or effects. |
| Open source software | Software programs that can be freely used, modified, and shared with anyone. |
| Operation Aurora | The name given to a series of cyberattacks against various major corporations to steal sensitive intellectual property information, which appeared to originate in China. |
| Operation Olympic Games | The name of a classified US military operation to disrupt the Iranian nuclear program. |
| Operation Predator | This US ICE-led program is designed to facilitate the |

| | |
|-----------------------|---|
| | investigation of child exploitation in the US and abroad. |
| Operation Rescue Me | This US FBI-led program has been in operation since 2008 to identify victims of child exploitation based on their appearance in images or video of child pornography. |
| Operation Spade | Name given to a multinational investigation of a child pornography ring operating out of multiple nations to produce content. |
| Operation: Bot Roast | An investigation conducted by the US FBI targeting botnet operators. |
| Original writing rule | States that the original evidence, rather than a duplicate, is generally required unless the duplicate can be authenticated and it can be proven that its contents are the same as the original. |
| Outing | A form of cyberbullying involving the posting of real personal information about individuals to embarrass them, such as sending images of them in states of undress, posting who they are attracted to, or information about homosexual preferences which may not be known to the general public. |
| Partition recovery | The process of evaluating the partition table and the unused space on the physical hard drive of a computer. |
| Partition table | Computer-based reference description for how the operating system has divided the hard drive into partitions. |

| | |
|--|--|
| Partitioning | The process of dividing up a computer hard drive into separate storage spaces. |
| Partitions | Separate storage spaces in a computer hard drive that determines how much space is allocated to each storage bin, or partition. |
| Password-protected files | Locked files that require a password to gain access. |
| Patent | See <i>Copyright</i> . |
| Payload | The changes that a piece of malware causes to a computer system upon activation. |
| Pedophile | An individual with a sexual attraction to individuals under the age of 18. |
| Peer-to-peer (P2P) file sharing protocols | Protocols that enable direct file sharing between two computer systems over the Internet. |
| People's Liberation Army of China (PLA) | The name of the Chinese military. |
| Peripheral device | Externally connected components that are not considered essential parts of a computer system, such as scanners, printers, and modems. |
| Personal Identification Number (PIN) | The four-digit number used as a password to secure access to bank accounts at ATMs. |
| Personally identifiable information (PII) | Information that is unique to an individual that can be used on its own or with other information to identify, locate, or contact a single individual. |
| Philippine Rules of Electronic Evidence (PREE) | This specifically outlines the admissibility rules for electronic evidence compared to the Philippine Rules of |

| | |
|---|---|
| | Evidence (PRE), which is a separate standard for non-electronic evidence. |
| Phishing | Using email messages to try to acquire bank account information or other valuable information from victims. |
| Phreak | An individual interested in using hacking techniques to exploit vulnerabilities within telephony. |
| Phreaking | The act of using hacking techniques to exploit vulnerabilities within telephony. |
| Physical extraction | The process of salvaging digital information. |
| Pirate Bay | A well-known group that enables piracy. |
| Plain view doctrine | Allows law enforcement officers to conduct a search and seizure for evidence that may not be in the search warrant but is in plain view and its incriminating nature is immediately apparent. |
| Plaintext | A legible message or piece of content. |
| Police and Justice Act 2006 | The UK law that enhanced sentences for computer hacking cases. |
| Police Intellectual Property Crime Unit (PIPCU) | A unit in the London Police that investigates and handles various forms of piracy. |
| Pornography | The representation of sexual situations and content for the purposes of sexual arousal and stimulation. |
| Prediction | A specific statement as to how you will determine if your hypothesis is true. |
| Pre-forensics | A term used to refer to the 1980s regarding digital forensic technologies, characterized by the lack of |

| | |
|---|--|
| | formal structure, protocols, training, and adequate tools. |
| Preponderance of evidence | Means it must be more likely than not that the accused in fact committed whatever acts they are accused of. |
| Preservation | Making a copy of the original data files for examination in a way that minimizes the possibility of any changes being made to the original data files. |
| PRISM program | An NSA-implemented program beginning in 2007 to collect email and other electronic communications data of all sorts, carried out through cooperative relationships with various technology companies, including Apple, Facebook, Google, Microsoft, and Skype. |
| Probable cause | Means there must be adequate reasons or justifications, rather than mere suspicion, to conduct a search. |
| Process models | Techniques and strategies designed to provide practical guidelines and procedures for conducting a digital forensic investigation. |
| Proprietary software | <i>See closed source.</i> |
| Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act (or PROTECT Act) of 2003 | This US law criminalized virtual child pornography and extended the legal definition to include “a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct.” |
| Prostitution | The practice of paying for sex, which may or may not be illegal depending on place. |
| Protection from Harassment Act | This UK law criminalized stalking and bullying in |

| | |
|--|---|
| 1997 (c40) | <p>professional settings. Section 4 of the Act criminalizes the act of putting others in fear of violence, defined as any course of conduct that would cause “another to fear, on at least two occasions, that violence will be used against him,” where the offender “is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.”</p> |
| Protection of Children Against Sexual Exploitation Act | <p>This US law made it illegal for anyone under the age of 16 to participate in the visual production of sexually explicit materials, though this was revised to the age of 18 in 1986.</p> |
| Protection of Freedoms Act 2012 | <p>Revised the Protection from Harassment Act 1997 to include language specifically related to stalking and incorporate aspects of technology into law.</p> |
| Proxy server | <p>A server that can be used to hide a computer’s location by acting as an intermediary between a computer and the servers and systems it connects to through the Internet.</p> |
| Pump and dump messages | <p>A form of spam-enabled fraud that attempts to manipulate the value of corporate stocks.</p> |
| Punternet | <p>A UK-based website designed for individuals to post reviews of escorts and sex workers.</p> |
| RAM slack | <p>When randomly selected data from RAM is stored in the file slack.</p> |
| Random Access Memory (RAM) | <p>Type of computer-based memory that stores that part of</p> |

| | |
|--|---|
| | the data that is currently being used by the computer. |
| Ransomware | Malware that demands the operator of the infected system pay in order to have their system's functionality restored. |
| Read-only | Term referencing the ability of a device to only view accessible data on a drive but not alter it in any way. |
| Reasonable expectation of privacy | The person must have exhibited an actual expectation of privacy, and the expectation must be one that society is prepared to recognize as reasonable. |
| Reasonableness clause | A search is constitutional if it does not violate a person's reasonable and legitimate expectation of privacy. |
| Recording Industry Association of America (RIAA) | A trade organization that supports the recording industry and those businesses that create, manufacture, or distribute legally sold and recorded music within the US. |
| Regulation of Investigatory Powers (RIPA) | This law mandates key disclosure so long as law enforcement obtains signed authorization from a high-ranking official. |
| Relevant | When evidence can make the facts presented in a case more or less probable; evidence that does not tend to prove or disprove a presented fact in a case is deemed irrelevant, and therefore inadmissible. |
| Reliability | The accuracy of the evidence deemed relevant to a case. |
| Repeatability | Where independent test results are obtained with the same method, on identical test items, in the same laboratory, by the same operator, using the same |

| | |
|---------------------------|--|
| | equipment within short intervals of time. |
| Report/presentation stage | The final step in the process of digital forensic investigation where the findings that are determined relevant to the investigation are finalized in a report. |
| Reproducibility | Where test results are obtained with the same method on identical test items in different laboratories with different operators using different equipment. |
| Revenge porn | Websites explicitly for individuals to post sexual images and videos they received or acquired for others to see without the consent of the creator. |
| Right to privacy | See <i>Fourth Amendment</i> . |
| Ripper | A seller in carding markets who does not provide data after being paid, is slow to respond to customers, or sells bad data and does not offer to replace their products. |
| Routine activity theory | Cohen and Felson (1979) argued that direct-contact predatory victimization occurs with the convergence in both space and time of three primary components: (1) a motivated offender; (2) a suitable target; and (3) the absence of a capable guardian. |
| Rule 34 | Online meme which states that “if it exists, there is pornographic content of it.” |
| Scareware | See <i>Ransomware</i> . |
| Scientific evidence | Information derived from the scientific method that is relevant to the facts of a case. |
| Scientific method | A process that uses strict guidelines to ensure careful |

and systematic collection, organization, and analysis of information.

Script kiddie

A derogatory term meant to shame individuals by recognizing their use of pre-made scripts or tools, their lack of skill, and the concurrent harm that they may cause.

Search

The exploration or examination of an individual's home, premises, or person to discover things or items that may be used by the government as evidence in a criminal proceeding.

Search and seizure

When law enforcement officers are identifying and collecting potential evidence to be used in the court of law.

Search incident to arrest

The process of searching a person who has been arrested for a crime.

Search warrant

A document signed by a judge or magistrate authorizing law enforcement to conduct a search.

Secret shopper schemes

A form of spam-enabled fraud where sellers pretend to operate legitimate businesses that are seeking employees who can cash checks and purchase goods with the proceeds.

Section 49 request

In the UK, a law enforcement mandate which requires encryption key disclosure so long as law enforcement obtains signed authorization from a high-ranking official using a specialized Section 49 form.

| | |
|-----------------------------|--|
| Sector | The smallest physical storage unit on a computer disk drive, which is almost always 512 bytes. |
| Secure Hash Algorithm (SHA) | A common hashing algorithm created by the US National Security Agency that creates a 160-bit value for an item using a unique combination of hexadecimal digits. |
| Seizure | The exercise of control by the government over a person or thing because of a violation of the law. |
| Self-control | The ability to constrain one's own behavior through internal regulation. |
| Self-incrimination | Giving a statement that might expose oneself to punishment for a crime. |
| Self-incrimination clause | In the US, a Fifth Amendment rule that provides defendants with protection from self-incrimination. |
| Severity | Involves the intensity of the punishment relative to the harm caused by the crime in the context of deterrence theory. |
| Sexting | The practice of sending photos or videos of individuals in provocative outfits or engaging in sexually suggestive activities through text messaging. |
| Sexual fetishes | The experience of sexual arousal or enhancement of a romantic encounter based on the integration of physical objects or certain situations. |
| Shoulder surfing | The act of stealing someone's passwords for email accounts or access to a system by looking over their |

| | |
|--|--|
| | shoulder and watching their keystrokes. |
| Silk Road | An online market developed to enable individuals to buy and sell narcotics through various mechanisms internationally. It garnered great attention from both researchers and the popular media due in part to the fact that transactions were paid using bitcoins. |
| Slack space | See file <i>slack</i> . |
| Social engineering | The use of tactics that try to fool or convince people to provide information that can be used to access different resources. |
| Social learning theory | Criminological theory created by Akers which argues that the learning process of any behavior, including crime, includes four principal components: (1) differential association; (2) definitions; (3) differential reinforcement; and (4) imitation. |
| Software | Consists of programs that include instructions which tell computers what to do. |
| Space transition theory | This theory created by K. Jaishankar argues that people behave differently while online than they otherwise would in physical space. |
| Spam | Unsolicited emails sent to large groups. |
| Spear phishing | Well-crafted and targeted spam messages that target one person or a small group. |
| Special Interest Group for Vendors (SIG Vendors) | A subgroup of FIRST that links respondents with software, hardware, and security vendors in order to |

| | |
|-------------------------------|---|
| | handle emergent threats and mitigation techniques. |
| Stalking | The use of repeated and intense harassing messages that involve threats or cause the recipient to feel fear for their personal safety. |
| Standard of proof | A continuum of probability used to assess suspicions of an individual's guilt based on the evidence presented. |
| Star Wars Kid | The name given to a video featuring a young boy flailing a stick around a room in a similar fashion to a lightsaber, which was released to the Internet by classmates without his permission and went on to become a key example of cyberbullying behavior. |
| Steganography | The practice of hiding information in such a way that others are not aware that a hidden message exists. |
| Steganography medium | The type of digital media containing a steganographic message, typically in video or picture files. |
| Stop Online Piracy Act (SOPA) | This legislation was designed to expand the capabilities of law enforcement to combat both digital piracy and online counterfeiting and would have enabled courts to order that websites be blocked in the event that they hosted or were in some way involved with either piracy or counterfeiting activities. |
| Street prostitution | Prostitutes who solicit individuals on the street. |
| Streetwalker (SW) | A term used to reference a street-walking prostitute in online forums. |
| Structured phase | A term given for the mid 1980s to describe the state of |

| | |
|--|--|
| | digital forensic technology, characterized by the harmonization between computer forensic procedure/policy and computer crime legislation. |
| Stuxnet | A computer worm that was used in attacks against the Natanz uranium enrichment facility in Iran. |
| Subculture | Any group having differentiating values, norms, traditions, and rituals that set them apart from the dominant culture. |
| Subpoena | A court order requiring a person to appear before a grand jury or produce documents. |
| Suitable target | A variable in routine activity theory referring to a person or object that has traits making him/her attractive to the offender on a wide range of factors. |
| Supervisory Control and Acquisition System (SCADA) | Computer systems that support the processes within industrial systems such as nuclear power plants, hydroelectric dams, or sewage treatment plants. |
| Survey/identification stage | The initial step of a digital forensic investigation. During this stage, law enforcement personnel and digital forensic technicians survey the physical and digital crime scene to identify potential sources of digital evidence. |
| Technicways | Term referring to the ways that behavior patterns change in response to, or as a consequence of, technological innovations. |
| Techniques of neutralization | Theory created by Sykes and Matza that focuses on how |

| | |
|---|--|
| | beliefs affect the process of deciding to commit a delinquent or criminal act. This theory assumes that most people hold conforming beliefs, but may still engage in criminal behavior occasionally through the application of definitions that justify their actions. |
| Terror | Planned acts of violence designed to promote fear or cause harm in a general population in support of a social agenda. |
| Testimonial | A statement made to law enforcement. |
| The Hacker Ethic | A series of values developed by hackers in the 1960s that espouse their beliefs about the use of technology. |
| The Hacker Manifesto | An article published in the magazine Phrack written by “The Mentor” that details his perceptions of hacking and rationalizing involvement in illegal hacks. |
| The Protection of Children Act 1978 (PCA) | The first UK legislation that made it illegal to obtain, make, distribute, or possess an indecent image of someone under the age of 18. |
| ThinkUKnow | A UK-based program designed to educate children and adults about threats to youth safety. |
| Thumb drives | <i>See USB flash drives.</i> |
| Tor | An anonymous and encrypted network used by individuals to hide their physical location. |
| Torrent | A form of file sharing that enables easy and distributed access to various intellectual property and online content, commonly used to pirate materials. |

| | |
|--------------|--|
| Trademark | See <i>Copyright</i> . |
| Traders | The misuse of the Internet by individuals who traffic in child pornography. |
| Traffic stop | Occurs when the driver of the vehicle is stopped because there is suspicion that a traffic violation has occurred or a crime is being committed. |
| Trailer | See <i>Footer</i> . |
| Transparency | Term used to describe the reporting of forensic evidence analysis findings that are detailed in such a way as to leave no mystery in the digital forensics process. |
| Travelers | The misuse of the internet by individuals who attempt to find children to molest through computer-mediated communications. |
| Tricking | A form of cyberbullying that involves convincing individuals to provide personal information about themselves in what they think is a personal conversation, which is then revealed to the general public. |
| Tricks | A term used by sex workers to describe their clients or customers. |
| Trojan | A form of malware that appears to be a downloadable file or attachment that people would be inclined to open, that when opened executes some portion of its code and delivers its payload on the system. |
| Truant | An individual who routinely skips school. |
| True threat | Term used in US law to identify statements where the |

| | |
|--|---|
| | speaker means to communicate a serious expression of intent to commit an act of violence against another person or group. |
| Truth in Domain Names Act of 2003 | A US law that makes it illegal for individuals to create domain names that are misleading or designed to directly expose individuals to pornographic content without their knowledge. |
| UK Computer Misuse Act | UK law developed in the 1990s that enabled the prosecution of computer hacking cases. |
| Unallocated space | Space on a hard drive to which data has not yet been written. |
| Unfair prejudice | A form of prejudice that could bias or confuse fact finders. |
| Uniform Crime Report (UCR) | The primary US reporting mechanism used by law enforcement agencies to collect and report data on crimes made known to the police. |
| United States Constitution | Legal document in the US that was adopted on September 17, 1787 that mandates all state judges to follow federal law in the event that conflicts arise between state and federal law. |
| United States Department of Justice (US DOJ) | The US federal department that has the responsibility to “enforce the law and defend the interests of the United States according to the law.” |
| United States Secret Service (USSS) | The US federal law enforcement agency which provides protection for the President and foreign dignitaries and |

| | |
|--|---|
| | investigates hacking and financial crime cases. |
| <i>United States v. Alkhabaz</i> | A major US federal court case that established the concept of true threats in the prosecution of stalking cases. |
| <i>United States v. Fricosu</i> (2012) | US court case that involved a woman's right to protection from self-incrimination on the basis of encrypted data on a laptop. |
| <i>United States v. Smith</i> (1998) | US court case that ruled that the warrantless search of a cell phone seized incident to arrest violates the Fourth Amendment. |
| Unverified seller | A seller in carding markets who has not provided a sample of data to a forum moderator or administrator, or alternatively offering malware or other services to be reviewed. |
| US Postal Inspection Service | The US federal agency that investigates child pornography and other crimes facilitated through the US mail. |
| USA PATRIOT Act | A US law, the Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act was passed in 2001 to support law enforcement investigations of terrorism. |
| USB flash drives | The most common removable storage device for digital media that are small, lightweight, and can easily be transported and concealed. |
| USCYBERCOM | Created in 2009 by the Pentagon in order to manage the |

| | |
|--|--|
| | defense of US cyberspace and critical infrastructure against attacks. |
| Validity | Term used to describe whether forensic evidence was collected and preserved in a manner so that an accurate conclusion can be drawn. |
| Verification | Establishes the integrity of the digital evidence by proving that the duplicate is authentic. |
| Verified seller | A seller in carding markets who has provided a sample of data to a forum moderator or administrator, or alternatively offering malware or other services to be reviewed. |
| Video cassette | A form of media utilizing magnetic tape that could record and store visual and audio content. |
| Video cassette recorders (VCRs) | A form of technology that allows individuals to watch and record media using magnetic cassette tapes. |
| Violent Crimes Against Children International Task Force (VCACITF) | The largest global task force in the world that investigates child exploitation cases. |
| Virtual Global Taskforce (VGT) | Established in 2003, an alliance of agencies and private industry that work together in order to identify, investigate, and respond to incidents of child exploitation. |
| Virus | One of the oldest forms of malware that cannot be activated or execute its payload without some user intervention, such as opening a file or clicking on an |

| | |
|------------------|--|
| | attachment. |
| Volatile | Term referring to the potential for data loss when a computer is powered off. |
| Vulnerability | Flaws in computer software, hardware, or people (in the case of social engineering or committing risky activities which open oneself to victimization). |
| Wannabe | A reference to noobs or script kiddies, referencing their limited capacity and skills. |
| Warez | Pirated software and intellectual property which was commonly used by hackers in the 1980s. |
| Warez doodz | Individuals who posted and shared programs. |
| Warrant | A signed document issued by a judge or magistrate that authorizes a specific course of action for law enforcement. |
| Warrants clause | The second clause of the Fourth Amendment indicating that a warrant or signed document issued by a judge or magistrate authorizes a specific course of action. |
| Wearable devices | Any sort of Internet-enabled device that can be worn by a person, such as a watch or pair of glasses. |
| Web defacement | An act of online vandalism wherein an individual replaces the existing HTML code for a web page with an image and message that they create. |
| White-hat hacker | A type of hacker with some skill who works to find errors in computer systems and programs to benefit general computer security. |

| | |
|---|--|
| White power | A term often associated with white supremacist groups like the Ku Klux Klan and other religious or ideologically based groups with an emphasis on the purity and separation of the white race. |
| Wiping | The process of cleaning a digital storage device to ensure that there are no remnants of data present. |
| Wire fraud | Fraud committed through the use of electronic communication. |
| Work-at-home schemes | A form of spam-enabled fraud where the seller promises recipients substantial earnings for just a few hours of work per day. |
| World Intellectual Property Organization (WIPO) | An international agency designed to support intellectual property rights. |
| Worms | A unique form of malware that can spread autonomously, though it does not necessarily have a payload. |
| Write | The process of altering or modifying data on a hard drive. |
| Write blocker | A device that allows read-only access to all accessible data on a drive, as well as prevents anything from being written to the original drive, which would alter or modify the original evidence. |
| Zeus Trojan | A form of malware that targets Microsoft Windows systems and is often sent through spam messages and phishing campaigns. |

