Global Information Assurance Certification Paper

BitTorrent & Digital Contraband

GIAC GCIA Gold Certification

Author: Kenneth G. Hartman, kgh@kennethghartman.com
Advisor: Ty Purcell
Accepted: March 27, 2016

Abstract

BitTorrent is a popular peer-to-peer file transfer program that allows participants in a swarm to exchange pieces with each other during the downloading process. Since users do not have to download all pieces from the original publisher, the downloading of very large files in an active swarm is typically faster than other methods used to distribute files. BitTorrent is often used to share pirated music and videos. Unfortunately, it is also used to distribute child pornography. Many people do not understand how the BitTorrent protocol works, including those in law enforcement and the legal profession. This lack of technical understanding combined with various legal issues can result in a weak case against those that are truly guilty or an inadequate defense of those that are not. This paper explains the technology, the investigative process, and the legal issues surrounding BitTorrent with a goal of improving the base knowledge of those on both sides of the legal dialectic process.

1. Introduction

BitTorrent is a popular peer-to-peer file transfer program that allows participants in a swarm to exchange pieces with each other during the downloading process. Since users do not have to download all pieces from the original publisher, the downloading of very large files in an active swarm is typically faster than other methods used to distribute files (Liberatore, Erdely, Kerle, Levine, & Shields, 2010).

BitTorrent was not necessarily designed for privacy although some might confuse it with "The Onion Router" which many people abbreviate as "TOR." The protocols are vastly different, and the only common characteristic is that they are both used to traffic in digital contraband.

There are two forms of digital contraband in the United States—copyright infringing (CI) material and child pornography (CP) (Borges, Houssain, Patton, & Masal, 2011). Copyright infringement is a civil infraction that may involve substantial fines whereas possession or distribution of CP is a criminal violation with serious repercussions, including incarceration (Dept. of Justice, n.d.) and registration on the sex offenders list (Dept. of Justice, n.d.).

A report published in 2010 (Layton & Watters) stated that 89% of all of the torrents in a random sample of 1000 were CI with 43.4% being movies, 29.1% TV shows, and music accounting for 16.5%. Organizations representing the copyright owners monitor the BitTorrent ecosystem to identify IP addresses that appear to be transmitting the copyright-infringing media that they own. They will work with Internet service providers to issue a Digital Millennium Copyright Act (DMCA) takedown notice to the likely party involved (Borges et al., 2011).

While CP is a small fraction of the overall BitTorrent traffic (Layton & Watters, 2010), it is investigated aggressively in the United States and many places around the world. Because the stakes are much higher in cases involving CP than CI, this paper focuses mostly on the investigative techniques, tools, and legal issues regarding cases involving BitTorrent and Child Pornography. However, the reader should note that much of the earlier research into combating CI laid the technical foundation for policing CP in the BitTorrent ecosystem.

2. Rationale & Ethical Considerations

Before diving into the technological and legal aspects, it is important to consider the societal problem of child pornography along with the ethical considerations of presenting this technical information.

2.1. The Growing Problem of Child Pornography

According to the SumAll Foundation, the growth in the number of child porn images that pedophiles have shared on the internet has quadrupled between 2007 and 2011. They state that 30% of the victims are under 13 years old and that 7% of the victims are younger than an age of six (Patterson, n.d.). The project by the SumAll Foundation utilized source data to create a profile of a child pornography consumer. One researcher on the project commented on the discovery that "the consumer is more or less an average guy who kind of clicks into darker and darker content was pretty shocking" (Patterson, n.d., para. 18). Another researcher said, "the keywords, sites, and file names were pretty creepy, especially when you consider how average a child porn surfer is" (Patterson, n.d., para. 20).

In the U.S., the vast majority of CP is investigated by the 61 Internet Crimes Against Children (ICAC) Task Forces. Brad Russ is the Director of the National Criminal Justice Training Center, which includes the ICAC Task Force Training & Technical Assistance program (NCJTC, n.d.). According to Russ, there were 7386 arrests in 2013 for child exploitation. He also stated that, based on known CP images and video downloads that they have tracked to individual computers, an estimated 50,000 people are trading illegal images at any one time (Johnson, 2014).

2.2. Child Porn Trafficking is a Heinous Crime

As the SumAll researcher stated above, the search terms and file names are creepy, not to mention the images. Pictures and videos are tightly controlled in a child pornography case. Law enforcement investigators must collect, collate and analyze every picture, video, or story to prosecute a case involving CP. Researchers have identified that exposure to abused children is a very severe stressor for police officers and that anger and "intense moral disgust" are natural reactions. The tight deadlines and limited budgets can mean that the few investigators with the forensics expertise can be immersed in the

material for long hours over a sustained period. The researchers note that this exposure can have adverse psychosexual and interpersonal effects on the investigator (Powell, Cassematis, Benson, Smallbone, & Wortley, 2015). Not only are the investigators sparing the rest of us from having to subject ourselves to this imagery, but they are also sometimes able to rescue the victim depicted in the imagery.

2.3. Ethical Considerations

Friends and family members will often ask criminal defense lawyers why they would help defend someone who in all likelihood is a child sex offender. A technical expert that is assisting defense counsel needs to address the same questions.

In the U.S., there is an adversarial legal system by design. This structure provides a mechanism for those that have been accused to present their case and ensures that the government protects their constitutional rights. It reduces the likelihood that law enforcement will punish an innocent person. The defense attorney plays a significant role in ensuring that the prosecution does not cut corners while trying to prove their case beyond a reasonable doubt (Viswanathan, Ellis, Howell, Stark, & Berry, n.d.).

Since crimes such as the distribution of child pornography are so heinous, they are sometimes used to frame an adversary. An example of this is a wife who was judged to have planted CP on the husband's computer to try to win a multi-million-dollar divorce settlement and full custody of the four children (Blair, 2007). Another example is where the courts accused a UK man of planting CP on his boss's laptop and then tipping off the police. Until the truth came out a year later, the supervisor was shunned and scorned (Stokes, 2010).

The seriousness of the charge and the heinous nature of the crime can blind one to the truth regarding the facts. This tendency is called "confirmation bias" and it can influence our thought process and decision making. The result of confirmation bias could be a miscarriage of justice including the incarceration of innocent people (Van Oirschot, 2015).

Furthermore, the law is not always settled on matters involving current technology; this includes issues around high-tech crimes involving child pornography (Eggestein & Knapp, 2014). Also, the technological concepts of the BitTorrent protocol

and the significance of the detailed information collected as evidence may not be fully understood by the parties involved, resulting in costly mistakes and damaging the public trust (Liberatore et al., 2010a).

3. Understanding BitTorrent

Many people do not understand how the BitTorrent protocol works. This group includes those in law enforcement and the legal profession. Some people will not use it and are scared of the technology (Klein, 2015). Others avoid it altogether because of its reputation as a piracy tool (Patrizio, 2014). However, BitTorrent does have legitimate uses. For example, it is the fastest way to download a Linux distribution (Linux Tracker, n.d.) and Windows 10 has options to use the BitTorrent protocol to download updates from peers on the same network or over the Internet (Leather, 2015). Many online games incorporate the BitTorrent protocol, including World of Warcraft (Layton & Watters, 2010).

In a conventional file download, each client that wants a copy of the file connects directly to its server and downloads it. This results in a considerable consumption of upload bandwidth for the server when it is hosting a large file that many people want (Layton & Watters, 2010). To download a file using BitTorrent, a client joins a swarm of other peers and obtains pieces of the file from other members of the swarm. The swarm relieves the peer that hosted the initial copy of the content from having to use anywhere near as much upload bandwidth as a conventional file transfer (Cohen, 2003).

3.1. Iterated Prisoners Dilemma

When Bram Cohen conceived BitTorrent, he understood that the majority of peers in a BitTorrent swarm would have an asynchronous connection to the Internet with much less upload bandwidth than they would have for downloading. Therefore, he created an incentive mechanism so that peers that are willing to share the pieces they have would be granted priority in downloading the pieces they are seeking (Cohen, 2003).

This incentive mechanism is called “tit-for-tat” and is based on a game theory concept called the “prisoner’s dilemma.” In this scenario, two parties have the opportunity to exchange their items to maximize their individual outcomes. Each

participant must decide whether or not to pass along one piece without knowing if the other party will send a piece to them. If both prisoners decide not to send a piece, neither party gains or loses anything. If both prisoners send a piece, then both benefit. Now, if one party sends a piece but the other does not, the prisoner that refrained from sending a piece gained at the expense of the prisoner that did. When the participants play the game for multiple rounds with each prisoner remembering the outcome of the previous round, it is called an "iterated prisoner's dilemma (IPD)" (Jun, 2005).

As a result of computer simulations that Axelrod and Hamilton (The evolution of cooperation) performed in the early 80s, the tit-for-tat strategy proved to be the best technique for winning the most IPD tournaments. The algorithm is simple. In the initial exchange, always cooperate. In following moves, copy the move that the other player performed (Jun, 2005).

The tit-for-tat strategy is not designed to prevent freeriding but to incentivize sharing for the benefit of the swarm (Jun, 2005). As will be discussed below, this incentive to share can often mean the difference between a charge of CP possession and a charge of CP distribution which is much more severe. Furthermore, investigators can benefit from freeriding by collecting evidence without distributing CP back out to the swarm, which would violate the law.

3.2. The BitTorrent Protocol

3.2.1. Pieces and Blocks

To distribute a file, the BitTorrent client breaks the file into several pieces of equal size according to a "metainfo" file. Members of the swarm announce which pieces they have and which pieces they want. Pieces are further divided into 16 kB "blocks" to facilitate distribution (Cohen, 2003). Bram Cohen's original design anticipated that the size of a piece would be 250 kilobytes, but observation demonstrates variance in the wild, particularly for small torrents and torrents over 10 Gb (Hartman, 2016).

After selecting a rare piece to download, a peer makes a direct TCP connection to another peer that has that piece and downloads the blocks that comprise the piece in sequential order. After receiving all of the blocks for the piece, the client assembles them

and checks the resulting SHA1 hash against the hash recorded in the metainfo file to verify its integrity (Liberatore et al., 2010a).

If the two hash values do not match, the client will discard that piece and download it again, but this time from another peer. This feature of the protocol prohibits a bad actor from corrupting the pieces distributed in the swarm (Layton & Watters, 2010).

3.2.2. Metainfo File

Anyone can publish digital media by creating a "metainfo" file which lists the files he or she intend to distribute. This small descriptor file has a ".torrent" file name extension and can be distributed using email or an instant message in addition to being posted on a website (Reddy & Kamath). The metainfo file lists the file names in the order that they appear in the torrent and the corresponding file size of each. The metainfo file also lists the SHA1 hash for each piece in consecutive order. The algorithm concatenates all of the files together and then divides the result into multiple pieces of equal size, calculating the hash of each piece for the metainfo file. The last piece contains the remainder of the content. Thus, it may be smaller than the others in the torrent. It is important to remember that the SHA1 hashes are of the pieces of the bundled files and are not hashes of the individual files. The metainfo file does not contain any of the torrent payload, just information about the torrent, including the URLs of any trackers (Cohen, 2008). Trackers coordinate the activity of the peers in the swarm and Section 3.2.3 discusses them in greater detail below. To see an example of a metainfo file that has been parsed to extract its detail, visit this blog posting: http://www.kennethghartman.com/parse-bittorrent-metainfo-files/.

An "infohash" is a SHA1 hash of the key information in the metainfo file which BitTorrent uses to identify it uniquely. A tracker uses this 160-bit fingerprint to track which torrents each client is interested in (Layton & Watters, 2010).

3.2.3. Peers

All participants in the swarm for a particular metainfo file are "peers." A peer with all of the pieces is called a "seed" or a "seeder." A peer that is still seeking pieces is known as a "leecher," although some use this term as a derogative to refer to a peer that

is unwilling to upload pieces. This ambiguity could be problematic in a court of law, so it is best to define the meaning of "leecher" whenever it is used (Layton & Watters, 2010).

After a leecher has accumulated all of the pieces in the torrent, it becomes a seed. At this point, peers frequently leave the swarm, although it is considered good etiquette to upload for a period after completing a download. Frequently, seeding happens until the user gets back to their computer and terminates the BitTorrent session (Cohen, 2003).

3.2.4. Piece Selection

The BitTorrent protocol is designed to maximize the entropy of the swarm. Therefore, peers select pieces to download using a "rarest-first" policy. If multiple pieces are rare and possessed only by a single seed, then a random piece is chosen for download. BitTorrent clients follow the rarest first policy unless the peer is acting as a seed, has less than four pieces, or is almost done downloading the full torrent and has requested all remaining sub-pieces (Konrath, 2007). The rarest first policy does a good job of making sure that only new pieces are uploaded by the seed since other pieces are available from other peers in the swarm. This policy is important since the original seed may leave before all peers have a full download (Cohen, 2003).

3.2.5. Choking & Tit-for-Tat

Section 3.1 introduced the tit-for-tat policy in the context of the discussion on the Iterated Prisoner's Dilemma game theory. Programmatically, this is implemented by keeping track of how much data a remote peer has uploaded. If the amount of data uploaded by a peer is not above a threshold, the remote peer may be choked in favor of the best remote peers (Liberatore et al., 2010a).

3.2.6. Optimistic Un-Choking

When a peer chokes a remote peer, it is a temporary refusal to cooperate in the iterated prisoner's dilemma by not uploading a piece. When the peer unchokes a remote peer and uploads to it, it is because it was one of the most cooperative remote peers. The number of simultaneous upload connections is configurable, but by default, it is set to four. Occasionally, to determine if there are better peers than the ones it is actively using, a peer will perform an "optimistic unchoke" and upload a piece to a remote peer. One

can think of an optimistic unchoke decision as always cooperating on the first move in the iterated prisoner's dilemma (Cohen, 2003) as if the player caught amnesia or suddenly forgave all past selfishness on the part of the remote peer.

3.2.7. Upload Only (as a Seed)

After a peer has all the pieces, it is a seed. Now, the seed selects peers who have the best upload rates and prefers peers to which others are not currently uploading (Cohen, 2003). While this feature of the BitTorrent protocol maximizes the health of the swarm, it also works to the advantage of a criminal investigator collecting evidence.

3.2.8. Peer Message Exchange

To exchange pieces, a peer connects directly to the IP address and port of a remote peer using information provided by the tracker about participants in the swarm. After a successful handshake, the peers exchange a bitfield message that lists the pieces possessed by each. After that, as new pieces arrive, the peers update each other as to their holdings (Liberatore et al., 2010a).

The handshake message contains the infohash of the torrent as well as a peer identification field that the peer uses to identify itself in the swarm. The bitfield is a data structure that uses a single bit to indicate the possession of each piece as represented in the metainfo file. After both peers exchange bitfield messages, each peer notifies the other of the pieces that it seeks. If a peer is in an unchoked state, it will send a piece request and then download the blocks for that piece (Bauer, McCoy, Grunwald, & Sicker, 2009).

While all this is configurable, a peer normally limits its connections to 55, 30 of which will be outbound connections to other peers. This setting leaves the remaining 25 for incoming connection requests (Konrath, 2007).

3.2.9. Trackers

To get a list of the peers currently participating in the swarm for a particular torrent, the peer contacts one of the trackers included in the metainfo file. Trackers are servers that maintain a list of the peers that have pieces of the torrent, based on its infohash (Layton & Watters, 2010). The message to the tracker contains the Peer ID, its IP address, and port number as well as the list of pieces it has already downloaded. The

response from the tracker lists the IP address and listening port number of a subset of the peers interested in the file. The response may also contain the Peer IDs. Peers will periodically contact the tracker to refresh its list of peers and provide an update on its download progress (Liberatore et al., 2010a).

The update interval is defined by the tracker and is typically 15 to 30 minutes. Excessive connections to the tracker may be blocked to prevent a denial of service attack (Layton & Watters, 2010). However, if a peer does not continue to reconnect for an update, the tracker will assume that the peer has abandoned the swarm. The size of the swarm can vary all the way up to thousands of peers, but the tracker limits the list sent to on each request to 50 random peers by default (Konrath, 2007).

3.2.10. Peer List Pollution

In an attempt to confound organizations that monitor BitTorrent for copyright infringement, certain trackers such as the Pirate Bay (Ernesto, 2008), will intentionally insert some random but valid IP addresses into the list that they return to peers (Borges et al., 2011). This list can include the IP addresses of the computers of people who are not even aware that BitTorrent even exists (Ernesto, 2008).

3.2.11. Distributed Hash Table & Peer Exchange

There are two extensions to the BitTorrent protocol that allow it to function without a Tracker. These "gossip-based" methods are known as Peer Exchange (PEX) and Distributed Hash Table (DHT). With DHT, all peers that support this extension share in the responsibility for handling the tracking function (Liberatore et al., 2010a). However, this feature is hampered by firewalls and network address translation (Santos, Cordeiro, Gaspary, & Barcellos, 2010). PEX enables peers to share their list of peers with each other without the need for a tracker (Liberatore et al., 2010a). Note that there are still privacy issues with DHT and PEX because peers are informing on each other.

3.3. The BitTorrent Ecosystem

3.3.1. BitTorrent Clients

On July 2, 2001, Bram Cohen announced the availability of his new "BitTorrent" application (Cohen, 2001). Originally the app was open-source, but now it is not. To avoid confusion with the BitTorrent protocol, most everyone refers to this app as the

"mainline" client. Since that time, more than thirty-five other applications have emerged with a variety of features and licenses (Comparison of BitTorrent clients, n.d.). Among the clients considered the most popular in 2016, are uTorrent, Vuze, Deluge, and BitComet (Fisher, 2016). A comparison of the various features of each BitTorrent client is outside the scope of this paper.

3.3.2. Remote Control

A noteworthy feature of many modern BitTorrent clients is the ability to remote control them. For example, both uTorrent (How do I set up µTorrent Remote?, n.d.) and Vuse (Vuze Remote, n.d.) allow the user to control them via a web browser or a smartphone. In fact, the Google Play Store has an extensive list of Android Apps for remotely controlling BitTorrent clients (BitTorrent Remote Apps, n.d.). Transmission is another popular client, particularly for Linux and Macintosh. Transmission has a remote command line interface (Kerr, Elsasser, Petit, & Livingston, 2008), making it attractive for scripting and automated acquisition systems (Kammerstetter, Platzer, & Wondracek, 2012).

Given the current state of mobile device security and the well-known problems of password sharing and password reuse, BitTorrent remote control features make it difficult for forensic investigators who have the onus of placing the suspected perpetrator in control of the device found with CP.

3.3.1. Seedboxes

A seedbox is a dedicated BitTorrent client, typically provisioned as a multitenant server by a cloud service provider, for the purpose of uploading and downloading torrents. This arrangement offers a high-speed connection to the Internet and allows its users to manage the client remotely using a command line interface or a web browser (Seedbox Guide, 2015).

3.3.2. Communities

Although many websites which host torrent files are open to the public, there are many private communities as well. A private community is essentially a portal that requires user registration before one can publish or download a metainfo file. Each community has its membership rules. Although the portal may be private, the torrent

files it hosts may also reference trackers external to the community, thereby leaking information about the community's existence (Santos et al., 2010).

3.3.3. Bundling

Legitimate publishers will frequently bundle less popular content into the same torrent as popular content. Publishers use this tactic because studies demonstrate that the download time for the unpopular content is shorter than before they bundle it. This improvement is because the swarm has more participants—even though the resulting download is larger (Menasche, 2009). Further research should be performed to determine to what extent CP secretly hitchhikes along with copyright infringing material in bundled torrent files.

3.4. Malware & BitTorrent

It is common wisdom that malware is rampant in BitTorrent. A frequently cited study from 2008 determined that 18% of all the executable programs distributed via BitTorrent contain malware (Berns & Jung). Another study claimed that 14.5% of the files in their sample of approximately 400 downloads contained zero-day malware. This study defined zero-day malware to be malware that is not detectable by current antivirus signatures or other malware detection techniques as of the day it was discovered (Vegge, 2009). Zero-day malware is like cancer, in that it is impossible to prove that it is not present, but sometimes it is.

3.4.1. Malware in Pirated Software

BitTorrent users that seek out pirated software or tools that help them circumvent copy protection, such as key generators and cracks, are frequently targeted with malware. This malware often adds the infected system to a botnet that criminals can use for a variety of malicious purposes (Kammerstetter et al., 2012).

Generally speaking, those engaged in software piracy are usually not computer experts (Limayem, 2004) and given this lack of security expertise are unlikely to protect their systems from the malware found in key generators and cracks (Kammerstetter et al., 2012).

A common trick used to entice pirates is to embed malware in a file that claims to be a slightly newer version of an application that is very popular in the BitTorrent ecosystem. By using a P2P file sharing systems, such as BitTorrent, malware creators can entice users to download and run the infected malware on their own, without worrying about creating a propagation mechanism (Berns & Jung, 2008).

3.4.2. Malware from Viewing Images & Videos

Sometimes an executable program that is designed to look like an image or a video file. When clicked the malware will install. The average user will not suspect anything other than that the file was corrupted during the download. Another tactic is to publish a torrent with content that is roughly the size of a popular movie title. When the user tries to watch the movie, it will launch a pop-up window instructing the user to install a new video codec from a malicious URL (Cuevas, Kryczka, González, Cuevas, & Azcorra, 2014). Certain types of video files may contain malicious hyperlinks that automatically load in a browser, infecting the computer with a "drive-by attack." Examples of this are Real Media files (Lemos, 2006), QuickTime MOV files (Cortes, 2010), and Windows Media Player WMP files (Cuevas et al., 2014).

3.4.3. Malware installed along with the BT Client

Berns & Jung note that some BitTorrent clients may even install malware along with the application (Searching for malware in BitTorrent, 2008). This issue was first observed in 2007 when attackers bundled malware with the Torrent 101, TorrentQ, Get-Torrent, and BitRoll clients (Ernesto, 2007). More recently, an installer for Xunlei spread malware to thousands of Microsoft Windows and Android users in China (Gibbs, 2013) and the installer for uTorrent was discovered to install a cryptocurrency mining software that it hid from the Windows Control Panel (Hruska, 2015).

3.4.4. Malware that Propagates via BitTorrent

Although originally designed to spread via an infected instant messaging client, the Impard-A virus could seed itself using the BitTorrent Mainline client (Berns & Jung, 2008). The PUSHBOT worm propagates using BitTorrent as instructed by the command-and-control server by creating a metainfo file and then joining the swarm (Tamana, 2013).

Worms that propagate via peer-to-peer protocols such as BitTorrent can be very efficient because there is no need to probe random addresses since there is widespread adoption of peer to peer networking. A worm can find potential victims by sending requests to a tracker and can infect the files exchanged (Luo, 2014).

3.4.5. BitTorrent Installed by Botnets

In 2005, a worm that propagated over Instant Messenger installed a modified BitTorrent client that it infected with the lockx.exe rootkit. This worm infected thousands of machines, adding them to a botnet that was then used to push video files out to the zombie computers. As a result, several BitTorrent users reported that mysterious movies were uploaded to their machine without their involvement (Roberts, 2005).

A more modern example is a variant of the KOOBFACE worm that propagates via sharing application files that contain a Trojan BitTorrent client. Users are infected when they download Trojanized metainfo files or when they execute the application files that contain the hidden BitTorrent client. As it turns out, the client is a version of uTorrent that runs in the background without the user's knowledge. Upon being launched, the uTorrent client downloads the infected application files, becomes a seed, and waits for further instructions from the botnet command-and-control server (Baltazar, 2011).

Organized crime routinely distributes illegal media using the zombie computers that comprise a botnet. These criminals can use the compromised computer as a seedbox, storing and distributing the digital contraband using BitTorrent and other peer-to-peer networks. This widespread tactic creates an enormous challenge to law enforcement (Eggestein & Knapp, 2014).

3.4.6. Botnets Controlled by BitTorrent

Researchers have shown that it is possible to control a botnet using tasks encoded in a metainfo file and that the botnet can coordinate work amongst the peers using BitTorrent (Durand, 2015). They embedded encrypted instructions in the metainfo file in the section that normally contains a SHA1 hash of each of the pieces.

Alternatively, an innocent BitTorrent tracker can be used as a covert channel to control a botnet. Communication with infected peers can go undetected due to the natural traffic patterns of the swarm (Cunche, 2014).

4. Investigating Digital Contraband

4.1. Evidence

An investigator will collect two types of evidence, direct evidence and hearsay. In network forensics, information gathered via a direct TCP connection to a process on a remote computer committing a crime is direct evidence. However, if one computer (that is not under the control of the police investigator) is relaying information about a remote computer under investigation, that is considered hearsay. For example, data from a BitTorrent tracker about a leecher's participation in a swarm is considered hearsay. However, if the investigator uses that information to connect directly to the peer and can download some or all of the file containing contraband, that is direct evidence (Liberatore et al., 2010a).

Although hearsay is not admissible as evidence in court, it does have value as a lead that helps investigators generate a hypothesis about the criminal act. In the United States, courts will not accept evidence that has not been obtained via valid legal procedures such as a search warrant or subpoena unless investigators observed it in plain view (Liberatore, Levine, & Shields, 2010).

There are certain exceptions to the rule against hearsay. An important one is that records maintained by regularly conducted business processes are admissible (Federal Rules of Evidence, Rule 803.6). It is this exception that allows law enforcement to subpoena the logs of the DHCP server from the Internet service provider showing which account holder held the lease for a particular IP address.

4.2. The Investigative Process

The National Institute of Justice has created various instructional materials to help law enforcement follow sound procedures for the collection of criminal evidence from computers and networks. One such document is titled "Forensic Examination of Digital Evidence: A Guide for Law Enforcement" (National Institute of Standards and

Technology (NIST), 2004). This document provides a complete overview of the various phases of a forensic criminal investigation along with specific guidance on the acquisition and handling of digital forensic evidence.

At a high-level, the steps for performing an investigation of CP in peer-to-peer networks is to generate leads, then to select promising leads for additional investigation. As part of this step, the investigator will verify that the subject IP address is within the jurisdiction. Next, the investigator will have the court issue a subpoena to the Internet service provider to obtain the service address that corresponds to the IP address under investigation. After obtaining the physical address, a search warrant will be issued to permit law enforcement to search the premises for child pornography and any computers, smartphones, or digital media that might contain it (Liberatore et al., 2010b).

Police at the site will create an inventory of the evidence collected. The investigators that are executing the search warrant will typically perform an initial on-site scan of the equipment taken into custody using forensic software tools. After that, the evidence will be transported to a digital forensic lab for a more detailed analysis and a report will be prepared (NIST, 2004).

4.2.1. Files of Interest

The National Center for Missing and Exploited Children (NCMEC) has compiled a repository of child sexually exploitive digital media. This repository indexes the files of interest (FOI's) by a cryptographic hash digest. Over time, these files have been acquired through previous investigations, Internet downloads, and seized media. This system allows an investigator to query the NCMEC registry using just the digest to see if the file is in their records (Liberatore et al., 2010a).

4.2.2. Locate Candidates & Assign by Jurisdiction

As mentioned above, investigations involving CP in the United States are conducted by one of the sixty-one Internet Crimes Against Children (ICAC) task forces. These teams collaborate by sharing tools, techniques, and status updates on the cases they are investigating. The ICAC task forces monitor the BitTorrent ecosystem, along with other popular peer-to-peer networks, looking for activity involving known FOIs. Because the purpose of BitTorrent is to disseminate files, the investigators simply need to

observe the public activity in the ecosystem to collect evidence. Case law considers this type of evidence as collected in "plain view" similar to a police officer that "walks a beat" (Liberatore et al., 2010a).

At this phase, both hearsay and direct evidence will be collected during the monitoring process. Next, a subset of the candidate IP addresses is selected for further investigation based on the quantity of FOI's and historical behavior of the candidate (Liberatore et al., 2010a).

4.2.3. Investigate Suspect

Based on geolocating the IP address, The ICAC task force that has jurisdiction will commence an investigation. In an attempt to obtain direct evidence, the investigator will attempt direct connections as a BitTorrent peer to verify that the suspect has possession of CP, or is distributing it.

During the direct connection, a handshake probe will be attempted with the suspect. This probe includes a bogus bitfield message so that the investigator seems to have pieces to share and in return receives a bit field message from the remote peer that is sometimes questionably used as direct forensic evidence that the peer had possession of contraband (Bauer et al., 2009).

The investigator will log which pieces of the torrent that the suspect claims to have possession of and will attempt a single-source download by taking advantage of optimistic unchoking while refusing to share (Liberatore et al., 2010a). This work is accomplished using a BitTorrent forensic tool called "Roundup Torrential Downpour," discussed in detail below.

In addition to logging the bitfield that it exchanged with the suspect, the software will log the BitTorrent Peer ID, the application version, and any other potentially corroborating evidence communicated by the remote peer (Liberatore et al., 2010a).

At this stage of the investigation, a warrant is not required because RoundUp is collecting the evidence in plain view by interacting with the suspect publicly as a typical BitTorrent peer in the swarm. The goal is not to make an arrest yet; it is to obtain a search warrant by collecting enough evidence to meet the probable cause standard. This

standard means that there is a "fair probability" that additional evidence will be found when the search warrant is executed (Hurley et al., 2013).

4.2.4. Subpoena Internet Service Provider

Once enough evidence has been collected to establish probable cause, the investigators will present that evidence to a judge to obtain a subpoena for records from the ISP associated with the unidentified suspect's IP address in an attempt to get the account holder's name and service address. Because most Internet service providers use DHCP, the subpoena will typically request detail about the DHCP lease (Liberatore et al., 2010a).

If the logs from the ISP contain the MAC address associated with the DHCP lease, it will most likely be the MAC address of a router rather than the suspect's personal computer. Nonetheless, this will usually be verified during the execution of the search warrant. During testimony, it is important not to conflate the IP address of the router with the IP address of the device that is found to have CP, even if that means describing how network address translation works to the jury.

4.2.5. Search Warrant of Suspect's Premises

Assuming the results of the subpoena on the ISP show that the service address is still under the jurisdiction of the unit performing the investigation, they will obtain a search warrant specifying the physical address and targeting all electronic devices or digital media that could contain CP as well as anything else that provides evidence of intent. The objective of the search warrant is to obtain evidence to be produced in a criminal trial (Liberatore et al., 2010a).

4.2.6. Examination of Evidence

As part of the on-site examination of evidence, the investigator seeks to correlate their observations as a remote peer to the evidence obtained during the search. For example, to validate the merits of the search warrant, the investigator will look for the file of interest in the seized evidence that he or she attempted to download when remotely connected. Of course, they will also look for other contraband and indicators that demonstrate that the suspect knew he was in possession of the CP. For example, search

terms in the web browser cache are often used as indicators of intent (Liberatore et al., 2010a).

4.2.7. Legal constraints

Unlike the criminals who traffic in child porn, law enforcement must obey the law. This constraint means they must be positive that when they use BitTorrent that they will not share pieces of CP files back out to the swarm (Liberatore et al., 2010a). It also means that investigators must not collect information by using technology that is not being utilized by the general public as a means to avoid obtaining a search warrant. For example, investigators cannot manipulate protocols in ways that the protocol specification had not anticipated (Liberatore et al., 2010b). In other words, criminal investigators cannot use hacking techniques on vulnerabilities to gain access to a computer system to perform a warrantless search. This requirement also means that Roundup Torrential Downpour must behave no more invasively than other BitTorrent clients.

4.3. Tools & Techniques

After recognizing the need to develop software that could help automate the detective work involved in collecting evidence of child abuse from peer-to-peer networks, law enforcement agencies partnered with Oak Ridge National Library in 2009 to create the first iteration of the tools (Borges et al., 2011). As a result of this partnership and grants from various government agencies, law enforcement now has a suite of tools for Gnutella, eMule, Ares, as well as BitTorrent. These tools, known as the RoundUp suite, have been used to identify 850 contact offenders that were sharing child pornography and to rescue 230 children. The RoundUp Suite is available to law enforcement at no cost and so far has been used to generate over 10,300 search warrants (Liberatore, Levine, Wallach, Wolak, & Kerle, 2015).

Worldwide, more than 7000 investigators have been trained on the RoundUp suite of tools (Liberatore et al., 2015). Authorized members of law enforcement with the prerequisite computer networking knowledge can participate in a two-day course on RoundUp for BitTorrent offered by the ICAC Task Force (Find a Class, n.d.)

Without a doubt, RoundUp has made a significant difference in law enforcement's battle against child pornography. However, not much is known about this toolset, and there is speculation that there was at one point an FBI directive to prevent disclosing its existence (Brenner, 2015a). One defendant even tried unsuccessfully to subpoena the source code for RoundUp-Gnutella (Brenner, 2015b).

4.3.1. Roundup Torrential Downpour

Interested parties can glean some information on Roundup Torrential Downpour from press releases and peer-reviewed articles. A 2011 press release stated that the software focuses on new torrent files announced in Really Simple Syndication protocol (RSS) feeds, and it promptly investigates the Internet addresses of the peers in the swarm to create a list of suspects for further investigation (Greenmeier, 2011).

The developers of RoundUp-Gnutella state that it is written in Java and performs IP geolocation. They indicate that relevant data can be downloaded as a CSV file or posted to a central server for collaboration with other law enforcement officers. They go on to state that the tool that they are developing to aid BitTorrent investigations will have similar functionality (Liberatore et al., 2010a).

An important feature of the BitTorrent investigative software is the ability to do a *single source download*, which means that it attempts to download all the pieces from the targeted remote peer without uploading any. RoundUp does this by taking advantage of the optimistic unchoke behavior designed into the BitTorrent protocol. The developers note that a single source download may take a very long time for large files in a swarm that has a small number of participants. They indicate that a solution to this is to prioritize portions of the torrent that serve as the best "smoking gun." (Liberatore et al., 2010a). In other words, this means that Torrential Downpour does not necessarily use the "rarest first" algorithm, but instead focuses on specific pieces within the torrent, selecting them by the SHA1 hash. Because the single source download may take more than twenty-four hours, it is reasonable to conclude that the software that performs this function is running on a dedicated system that can change IP addresses as needed to operate in a covert manner.

4.3.2. The Big Database

Observers can infer that there is a centralized component to the investigative BitTorrent system architecture from the open source information. This functionality is in addition to the local systems that perform the single source downloads under the control of individual investigators and the distributed components that perform the monitoring of the BitTorrent ecosystem. This central database coordinates the activities of investigators by allowing them to record the results of their investigations and to follow the progress of colleagues through a browser-based user interface (Liberatore et al., 2010a).

This "centralized database" is a search and analytics platform that apparently is built on top of Apache Solr (Hink, n.d.). The system has been used to predict the type of content based on the name of the file as well as to create predictive models of the behavior of contact offenders, based on the content they share (Liberatore et al., 2015).

4.3.3. The Distributed Monitoring Framework

The monitoring process consists of crawling torrent indexers or monitoring their RSS feeds for specific keywords to find metainfo files of interest. Next, the trackers will be queried for a list of peers corresponding to each torrent. The system verifies each IP address by connecting to it and obtaining the bitfield message exchanged during the handshake to address the issue of trackers polluting the list of peers. By examining the bitfield responses of all the peers in the swarm over time, this monitoring process provides a global picture of the activity, complete with whois data, presented in Google Earth (Borges et al., 2011).

The BitStalker project initially developed this probing technique for tracking copyright infringing materials. That system, built in 2009, used a desktop PC to monitor 20,000 peers every five minutes. Because the active monitoring required an upload and download of fewer than 300 bytes, the researchers pointed out that it could be cost effectively scaled to tens of millions of peers using public cloud resources, such as Amazon EC2 (Bauer et al., 2009).

Another recommendation from the BitStalker researchers is to distribute the monitoring function across a large number of IP addresses to avoid detection based on an analysis of tracker list (Bauer et al., 2009). Thus, it is reasonable to suspect that law

enforcement has deployed the monitoring agents at a variety of ISPs and cloud service providers.

4.3.4. Tagging Traffickers of CP

Another innovative tactic used to combat digital child pornography is to use tagging. This method works much like the technique used to track fish and wildlife with the use of unique identifiers to study movement patterns. An investigator can tag a remote computer over the network in a manner that is undetectable to its owner or even a third party looking for the tags. However, tags found by a forensic investigator during a warranted search are strong evidence that the computer system was indeed interacting with law enforcement while participating in the BitTorrent swarm (Liberatore et al., 2010b).

Tags are specific patterns of bits that are unique to a given interaction. The tags are inserted into the suspect's hard drive through the proper functioning of the BitTorrent software without making unauthorized access. Tags can be used to demonstrate a pattern of intentional behavior, especially if the quantity increases over time. The tagging vector is selected based on the features of the protocol. For example, with BitTorrent, peers will inform each other of their peer ID. The application stores this data in a log that an investigator can analyze upon seizure of the computer. RoundUp manipulates the tag so that it will be unique to the specific interaction and records it in the central database (Liberatore et al., 2010b).

This twenty-byte peer ID is generated by a peer before it joins a torrent. It typically identifies the client software version and includes a random string (Pontes, 2009). Using the peer ID as a tag is just one example. In practice, anything that the remote connection can use to manipulate what gets recorded in the log files or the cache could be used for tagging. These destinations are selected such that removing the tagged files would degrade the performance. Another example of a tag could be specific combinations of ports and the IP addresses that RoundUp reports are peers that have pieces of interest to the suspect. IPv6 addresses work well for this due to the decreased probability of a collision. It is even better, but not necessary, if these IP addresses are under the control of law enforcement. Also, certain BitTorrent clients perform a reverse DNS lookup on the IP addresses of peers that connect to them. The presence of the

domain name corresponding to the investigator's system in the DNS cache confirms that connection with the investigator did indeed occur, and is in itself a tag (Liberatore et al., 2010b). Note that there are quite likely other tags that investigators have not disclosed in the peer-reviewed literature.

Recording the tags in the central repository allows law enforcement to leverage the power of this technique across the entire ICAC community. This procedure ensures that tags are unique and captures the date and rationale as to why the investigator placed the tag. It helps investigators determine the history of the computer, which in the case of a mobile device may have traveled across many different jurisdictions, used several different IP addresses, or even different peer-to-peer networks (Liberatore et al., 2010b).

4.3.5. Honeypots & Honeynets

Because there is nothing illegal about standing up a fake website that purports to offer child pornography but does not, law enforcement has also employed this tactic. These websites might contain bogus torrent files as well as links to other websites and trackers, creating what is known as a honeynet (Eggestein & Knapp, 2014).

It is also conceivable that a BitTorrent tracker could be a honeypot, and similar to Descarte's Evil Demon (The Argument from Deception, n.d.), manipulate the subject peer's entire sense of reality regarding the swarm. In fact, it is easy to make a torrent file seem very popular, giving the would-be downloader a false sense of security because "everyone is doing it." If one controls the bit torrent tracker, it can be done by a simple change to the code or by manipulating the file that the tracker uses to maintain its list of peers (Berns & Jung, 2008).

4.3.6. Sybil Attacks

In a Sybil attack, a peer uses multiple identities to gain an advantage in a P2P file sharing network; for example, by exploiting the optimistic unchoke mechanism in BitTorrent (Pontes, 2009). It is unknown whether or not Torrential Downpour presents multiple identities to the swarm when performing a single source download, although it is quite conceivable.

4.3.7. Eclipse Attack

An eclipse attack is similar to a Sybil attack, except that multiple Sybils act in a coordinated manner to control the target peer's perception of the swarm, preventing it from receiving all pieces of the torrent. This manipulation is typically accomplished by falsifying the bitfield messages and referring the target to seek pieces only from other peers participating in the attack. However, the targeted peer will also receive a randomly generated peer list from the tracker. Therefore, the greater the number of coordinated peers in the swarm as a percentage of the whole, the more likely the peer list will contain only the attacking peers (Konrath, 2007). In addition to refusing to share, coordinated peers can reinitiate the handshake sequence multiple times, in what the literature refers to as a "chatty peer attack" (Balhara, 2016).

The open source information is unclear as to whether or not the distributed monitoring agent peers controlled by ICAC perform an eclipse attack to inhibit the spread of child pornography, but the courts would most likely consider it to be legal as long as the Sybils do not upload pieces of actual CP.

4.3.8. Pollution

Torrent poisoning is a common tactic employed by antipiracy organizations to thwart P2P file sharing by corrupting the payload data or using misleading file names. Another tactic is to insert a large amount of erroneous information into the servers that index torrent files, requiring a user to download several bogus files in an attempt to find what they are looking for (Balhara, 2016). It is not known to what extent ICAC has resorted to these more active measures to inhibit the spread of CP. In fact, these counter-measures would require that a downloader would have to be very motivated to find what they are looking for, thereby further establishing intent.

5. Legal Considerations

5.1. Legal Defenses

In preparation for criminal trial, it is important to consider the strategy that defense counsel will use to create some reasonable doubt in the minds of the jury. Among these are the "some other dude did it" defense and the "Trojan horse" defense.

5.1.1. "Some Other Dude Did It"

One strategy that many criminal defense attorneys prefer over simply claiming that the prosecution's case is inadequate would be to provide an alternate story that provides a plausible explanation for all of the evidence (Tenney, Cleary, & Spellman, 2009).

In refuting this defense strategy, the prosecution must rule out other people in the household besides the suspect who may have had access to the device that contains the CP. Depending on the nature of the evidence, it may also be important to prove that the device was connected to the router at the time the investigator conducted a single source download. This is where the tags come in, although the technical details may create confusion for the jury. Lastly, the ability to remote control many of the more popular BitTorrent clients could also become a hurdle without corroborating evidence such as an organized archive of CP.

5.1.2. Trojan Horse Defense

The "Trojan Horse Defense" was named after two separate cases in the UK wherein the defendants were acquitted of charges of possession of child pornography because analysts found Trojan horse malware on their computers. The first instance involved fourteen child porn images and a single Trojan (Leyden, 2003). In the second case (BBC News, 2003), 172 images were found along with eleven Trojan horse programs, each capable of remote control.

The Trojan Horse Defense is a specific application of the more general "some other dude did it" defense but has the advantage of providing a single alternate explanation that is less abstract than an unknown perpetrator. Although lawyers refer to it as the "Trojan horse Defense," in common use, it applies to a defense based on any malware including a virus, a worm or even browser hijacking. It also plays on a common fear about getting hacked that may resonate with members of the jury. To refute this defense, prosecutors must establish that the accused has a pattern of behavior consistent with this crime, separate from the capabilities of malware (Brenner, Carrier, & Henninger, 2004).

A Trojan Horse Defense requires technical expertise in computer and network forensics as well as a significant amount of preparation and investigation (Brenner et al., 2004). Defendants would not use this argument if it were not a legitimate and successful defense. Given the sophistication of today's malware and its prevalence in the BitTorrent ecosystem, this strategy should be evaluated by both sides that are arguing the case.

5.1.3. Chewbacca Defense or Counter

One technique that may be used to belittle the Trojan Horse Defense is to claim that the defense is trying to baffle the jury with technical details. This tactic is sometimes called the "Chewbacca Defense" and gets its name from a South Park episode which lampooned Johnny Cochran. In this spoof during the closing arguments, Cochran repeats multiple times, "It does not make sense" and then proclaims, "If Chewbacca lives on Endor, you must acquit! The defense rests" (South Park, n.d., n.p.).

5.2. Legal Issues

Some of the questions that litigants may need to resolve in a legal case involving BitTorrent pertain to exactly when do digital bits become child pornography? For example, what if:

- A defendant claims that he did not know that the partially downloaded BitTorrent payload was CP, is that a valid argument if his decision to download was based on only the hexadecimal infohash and not an incriminating torrent file name?
- What if that partially downloaded chunk of data will not render in a video player installed on his computer? How does one prove the user knew what it was?
- What if the only CP found on the computer is in unallocated space? Does this prove a user knew about it?

6. Conclusion

It is clear that BitTorrent does not provide any privacy protection, but it is still used by some to traffic in digital contraband. The ecosystem is rife with polluted content

and malware. Law enforcement has created effective tools to police this digital ecosystem in an attempt to catch the sexual predators of children. However, knowledgeable defense teams must balance that power to protect the rights of the accused, and possibly innocent victims of malware and botnets.

7. References

Axelrod, R., & Hamilton, W. D. (1981). The evolution of cooperation. *Science*, 1390-1396.

Balhara, P. (2016). A Review on Torrent & Torrent Poisoning over Internet. *International Journal of Computer Science & Management Studies, IJCSMS, Vol. 22, Issue 01*. Retrieved from http://www.ijcsms.com/abstractdetails.aspx?abs=873

Baltazar, J. (2011, August 17). *KOOBFACE Propagates via Torrent P2P File Sharing*. Retrieved from Trend Micro, TrendLabs Security Intelligence Blog: http://blog.trendmicro.com/trendlabs-security-intelligence/koobface-propagates-via-torrent-p2p-file-sharing/

Bauer, K., McCoy, D., Grunwald, D., & Sicker, D. (2009). BitStalker: Accurately and efficiently monitoring bittorrent traffic. *Information Forensics and Security, 2009. WIFS 2009. First IEEE International Workshop on*, pp. 181-185. IEEE. Retrieved February 6, 2016, from https://cs.uwaterloo.ca/~k4bauer/papers/bauer-wifs09.pdf

BBC News. (2003, July 31). *Man cleared over porn 'may sue'*. Retrieved from BBC News: http://news.bbc.co.uk/2/hi/uk_news/england/devon/3114815.stm

Berns, A., & Jung, E. (2008). *Searching for malware in BitTorrent.* University of Iowa, Tech. Rep. UICS-08-05, April, 24.

BitTorrent Remote Apps. (n.d.). Retrieved from Google Play: https://play.google.com/store/search?q=bittorrent%20remote&c=apps&hl=en

Blair, L. (2007, September 25). *Travel big's divorce ruling ends hellacious court trip*. Retrieved from New Your Post: http://nypost.com/2007/09/25/travel-bigs-divorce-ruling-ends-hellacious-court-trip/

Borges, R., Houssain, K., Patton, R., & Masal, Y. (2011). BitPredator: A Discovery Algorithm for BitTorrent Initial Seeders and Peers. *International Conference on Advanced Computer Theory and Engineering. 4th (ICATE 2011).* ASME Press. Retrieved February 6, 2016, from https://ebooks.asmedigitalcollection.asme.org/content.aspx?bookid=487&sectionid=38793947

Brenner, S. (2010, February 22). *Kyllo and "A Forensic Software Program"*. Retrieved February 6, 2016, from CYB3RCRIM3: http://cyb3rcrim3.blogspot.com/2010/02/kyllo-and-forensic-software-program.html

Brenner, S. (2015, April 17). *Child Pornography, RoundUp and the Franks hearing*. Retrieved from TruthMovement: http://www.truthmovement.us/2015/04/child-pornography-roundup-and-franks.html

Brenner, S. (2015, September 7). *Source Code, RoundUp and the 4th Amendment*. Retrieved from TruthMovement: http://www.truthmovement.us/2015/09/source-code-roundup-and-4th-amendment.html

Brenner, S. W., Carrier, B., & Henninger, J. (2004). The Trojan horse defense in cyber crime cases. *Santa Clara High Tech L.J. 1*. Retrieved from http://digitalcommons.law.scu.edu/chtlj/vol21/iss1/1/

Cohen, B. (2001, July 2). *BitTorrent - a new P2P app*. Retrieved from Yahoo Groups, P2P Talk: https://groups.yahoo.com/neo/groups/decentralization/conversations/topics/3160

Cohen, B. (2003). Incentives build robustness in BitTorrent. *Workshop on Economics of Peer-to-Peer Systems, Vol 6*, (pp. 68-72). Retrieved from http://www.bittorrent.org/bittorrentecon.pdf

Cohen, B. (2008, January 10). *The BitTorrent Protocol Specification*. Retrieved from BitTorrent.org: http://www.bittorrent.org/beps/bep_0003.html

Comparison of BitTorrent clients. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Comparison_of_BitTorrent_clients

Cortes, B. (2010, August 6). *Trojanized .MOV Files FAQ*. Retrieved from Trend Micro: http://blog.trendmicro.com/trendlabs-security-intelligence/trojanized-mov-files-faq/

Cuevas, R., Kryczka, M., González, R., Cuevas, A., & Azcorra, A. (2014). TorrentGuard: Stopping spam and malware distribution in the BitTorrent ecosystem. *Computer Networks*, 59, 77-90.

Cunche, M. K. (2014). Asynchronous covert communication using bittorrent trackers. *High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC, CSS, ICESS),*

2014 IEEE Intl Conf on (pp. 827-830). IEEE. Retrieved from https://hal.inria.fr/hal-01053147/file/Hidden_Channel_Tracker_short.pdf

Dept. of Justice. (n.d.). *Citizens guide to US Federal law on child pornography*. Retrieved from The United States Department Of Justice: https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography

Dept. of Justice. (n.d.). *Sex offender registration and notification act (SORNA)*. Retrieved from The United States Department of Justice: https://www.justice.gov/criminal-ceos/sex-offender-registration-and-notification-act-sorna

Durand, A. G. (2015). BitWorker, a Decentralized Distributed Computing System Based on BitTorrent. *Wired/Wireless Internet Communications*, 151-164. Retrieved from http://link.springer.com/chapter/10.1007/978-3-319-22572-2_11

Eggestein, J. V., & Knapp, K. J. (2014). Fighting Child Pornography: A Review of Legal and Technological Developments. *The Journal of Digital Forensics, Security and Law: JDFSL*, 9(4), 29. Retrieved from http://ojs.jdfsl.org/index.php/jdfsl/article/viewFile/247/235

Ernesto. (2007, August 2). *TorrentSpy advertises malicious BitTorrent client*. Retrieved from TorrentFreak: https://torrentfreak.com/torrentspy-advertises-malicious-bittorrent-client/

Ernesto. (2008, October 20). *Pirate Bay Tricks Anti-the-Pirates With Fake Peers*. Retrieved from torrentfreak.com: https://torrentfreak.com/the-pirate-bay-tricks-anti-pirates-with-fake-peers-081020./

Federal Rules of Evidence, Rule 803.6. (n.d.). Retrieved from https://www.law.cornell.edu/rules/fre/rule_803

Find a Class. (n.d.). Retrieved from Internet Crimes Against Children Task Force: https://www.icacregistration.org/public/FindAClass.aspx

Fisher, S. (2016, March 2). *12 Best Free Torrent Clients*. Retrieved from About.com: http://freebies.about.com/od/Free-Torrent-Clients/tp/free-torrent-clients.htm

Gibbs, S. (2013, October 15). *Google-backed BitTorrent client spread malware to Windows PCs and Android devices*. Retrieved from The Guardian: http://www.theguardian.com/technology/2013/oct/15/google-bittorrent-malware-windows-android-xunlei-china

Greenmeier, L. (2011, November 7). *Cops Enlist Data-Tracking Software in the Fight against Child Predators*. Retrieved from Scientific American: http://www.scientificamerican.com/article/software-against-p2p-bittorrent-abuse/

Han, J. K. (2012). Bundling practice in bittorrent: What, how, and why. *ACM SIGMETRICS performance evaluation review*, 40(1), 77-88.

Hartman, K. G. (2016, March 19). *Are BitTorrent Pieces 250Kb Long?* Retrieved from www.kennethghartman.com: http://www.kennethghartman.com/are-bittorrent-pieces-250kb-long/

Hink, R. C. (n.d.). *Raymond C Borges Hink*. Retrieved February 6, 2016, from MindSumo.com: https://www.mindsumo.com/user/29045

How do I set up µTorrent Remote? (n.d.). Retrieved from uTorrent Help Center: http://help.utorrent.com/customer/portal/articles/733246

Hruska, J. (2015, March 6). *uTorrent accused of bundling cryptocurrency malware with popular BitTorrent client*. Retrieved from ExtremeTech: http://www.extremetech.com/computing/200602-utorrent-accused-of-bundling-cryptocurrency-malware-with-popular-bittorrent-client

Hurley, R., Prusty, S., Soroush, H., Walls, R. J., Albrecht, J., Cecchet, E., . . . Wolak, J. (2013). Measurement and analysis of child pornography trafficking on P2P networks. *Proceedings of the 22nd international conference on World Wide Web* (pp. 631-642). International World Wide Web Conferences Steering Committee. Retrieved from https://www.ncjrs.gov/pdffiles1/ojjdp/grants/248597.pdf

Johnson, k. (2014, May 15). *Clandestine websites fuel 'alarming' increase in child porn*. Retrieved from USA Today: http://www.usatoday.com/story/news/nation/2014/02/19/child-pornography-dark-web/5184485/

Jun, S. &. (2005). Incentives in BitTorrent induce free riding. *Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems* (pp. 116-121). ACM. Retrieved from http://www.cs.duke.edu/courses/fall05/cps296.1/papers/jun-p2p-econ.pdf

Kammerstetter, M., Platzer, C., & Wondracek, a. G. (2012). Vanity, cracks and malware: Insights into the anti-copy protection ecosystem. *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 809-820). ACM. Retrieved from http://www.syssec-project.eu/m/page-media/3/kammerstetter-ccs12.pdf

Kerr, C., Elsasser, J., Petit, E., & Livingston, M. (2008, July 21). *transmission-remote(1) - Linux man page*. Retrieved from Die.net: http://linux.die.net/man/1/transmission-remote

Klein, A. (2015, September 15). *Internet Piracy: Should I be scared when I'm downloading torrents?* Retrieved February 13, 2016, from Quora: https://www.quora.com/Internet-Piracy/Should-I-be-scared-when-Im-downloading-torrents

Konrath, M. A. (2007). Attacking a Swarm with a Band of Liars: evaluating the impact of attacks on BitTorrent. *Peer-to-Peer Computing, 2007. P2P 2007. Seventh IEEE International Conference on* (pp. 37-44). IEEE.

Layton, R., & Watters, P. (2010). *Investigation into the extent of infringing content on BitTorrent networks.* Internet Commerce Security Laboratory.

Leather, A. (2015, March 6). *Windows 10 To Use BitTorrent-Style P2P To Deliver Updates*. Retrieved February 13, 2016, from Forbes: http://www.forbes.com/sites/antonyleather/2015/03/16/windows-10-to-use-bittorrent-style-p2p-to-deliver-updates/

Lemos, R. (2006, November 15). *Malware goes to the movies*. Retrieved from SecurityFocus: http://www.securityfocus.com/news/11424

Leyden, J. (2003, April 24). *Trojan defence clears man on child porn charges*. Retrieved from The Register: http://www.theregister.co.uk/2003/04/24/trojan_defence_clears_man/

Liberatore, M., Erdely, R., Kerle, T., Levine, B. N., & Shields, C. (2010). Forensic investigation of peer-to-peer file sharing networks. *Digital Investigation, 7*, pp. S95-S103. Retrieved from http://www.dfrws.org/2010/proceedings/2010-311.pdf

Liberatore, M., Levine, B. N., & Shields, C. (2010). Strengthening forensic investigations of child pornography on p2p networks. *Proceedings of the 6th International Conference* (p. 19). ACM.

Liberatore, M., Levine, B. N., Wallach, H., Wolak, J., & Kerle, T. (2015, January). *RoundUp Predictive Tool (RPT) Project: Final Report.* Retrieved February 6, 2016, from National Criminal Justice Reference Service: https://www.ncjrs.gov/pdffiles1/ojjdp/grants/248596.pdf

Limayem, M. K. (2004). Factors motivating software piracy: a longitudinal study. *Engineering Management, IEEE Transactions on*, 51(4), 414-425.

Linux Tracker. (n.d.). Retrieved from http://linuxtracker.org/: http://linuxtracker.org/

Luo, J. X. (2014). Modeling and defending against adaptive BitTorrent worms in peer-to-peer networks. *CM Transactions on Autonomous and Adaptive Systems (TAAS)*, 9(1), 5. Retrieved from http://dl.acm.org/citation.cfm?id=2567925

McCoy, D., Bauer, K., Grunwald, D., Kohno, T., & Sicker, D. (2008, July). Shining light in dark places: Understanding the Tor network. *Privacy Enhancing Technologies*, (pp. 63-76).

Menasche, D. S. (2009). Content availability and bundling in swarming systems. *Proceedings of the 5th international conference on Emerging networking experiments and technologies* (pp. 121-132). ACM. Retrieved from https://web.cs.umass.edu/publication/docs/2009/UM-CS-2009-010.pdf

National Institute of Standards and Technology (NIST), & United States of America. (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* Retrieved from https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

NCJTC. (n.d.). *NCJTC Leadership*. Retrieved from https://www.ncjtc.org/Pages/NCJTC_Leadership.aspx

Patrizio, A. (2014, October 24). *BitTorrent Beginner's Guide: Everything You Need to Know*. Retrieved from Tom's Guide: http://www.tomsguide.com/us/bittorrent-how-to-guide-torrent,review-2429.html

Patterson, D. (n.d.). *Child Pornography and the Internet*. Retrieved from SumAll.org: http://www.sumall.org/child-pornography-data/

Piatek, M. K. (2008, July). Challenges and directions for monitoring P2P file sharing networks, or, why my printer received a DMCA takedown notice. *HotSec*.

Pontes, F. B. (2009). Bittorrent needs psychiatric guarantees: Quantifying how vulnerable bittorrent swarms are to sybil attacks. *Dependable Computing, 2009. LADC'09. Fourth Latin-American Symposium on* (pp. 65-72). IEEE.

Powell, M., Cassematis, P., Benson, M., Smallbone, S., & Wortley, R. (2015). Police Officers' Perceptions of their Reactions to Viewing Internet Child Exploitation Material. *Journal of Police and Criminal Psychology, 30(2)*, pp. 103-111.

Reddy, S. V., & Kamath, P. (n.d.). *BitTorrent: Peer-to-Peer File Sharing.* Retrieved from savadivirender.com: http://www.savadivirender.com/bittorrent.pdf

Roberts, P. F. (2005, December 21). *Botnet Uses BitTorrent to Push Movie Files*. Retrieved from eWeek: http://www.eweek.com/c/a/Security/Botnet-Uses-BitTorrent-to-Push-Movie-Files

Santos, F. R., Cordeiro, W. L., Gaspary, L. P., & Barcellos, M. P. (2010). Choking polluters in bittorrent file sharing communities. *Network Operations and Management Symposium (NOMS), 2010 IEEE* (pp. 559-566). IEEE. Retrieved from https://www.researchgate.net/profile/Marinho_Barcellos/publication/220707965_Choking_polluters_in_BitTorrent_file_sharing_communities/links/0046351ce183bc191e000000.pdf

Seedbox Guide. (2015, September 10). *What is a seedbox?* Retrieved from Seedbox Guide: http://seedboxgui.de/guides/what-is-a-seedbox/

Siganos, G., Pujol, J. M., & Rodriguez, P. (2009). Monitoring the bittorrent monitors: A bird's eye view. *Passive and Active Network Measurement*, (pp. 175-184).

Singh, A. (2006). Eclipse attacks on overlay networks: Threats and defenses. *IEEE INFOCOM*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.124.3679

Slot, M., Costa, P., Pierre, G., & Rai, V. (2009). Zero-day reconciliation of bittorrent users with their isps. *Euro-Par 2009 Parallel Processing*, (pp. 561-573). Springer Berlin Heidelberg. Retrieved from http://research.microsoft.com/en-us/um/people/pcosta/papers/slot09zeroday.pdf

South Park. (n.d.). *The Chewbacca Defense*. Retrieved from South Park Studios: http://southpark.cc.com/clips/103454/the-chewbacca-defense

Steel, C. M. (2015). Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms. *Child abuse & neglect, 44*, pp. 150-158.

Stokes, J. (2010, August 6). *A simple plan to ruin your boss: plant child porn on his PC*. Retrieved from Ars Technica: http://arstechnica.com/tech-policy/2010/08/disgruntled-brit-plants-child-porn-on-bosss-computer-calls-cops/

Tamana, N. (2013, July 9). *WORM_PUSHBOT.CY*. Retrieved from TrendMicro Threat Encyclopedia: http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/worm_pushbot.cy

Tenney, E. R., Cleary, H. M., & Spellman, B. A. (2009, July 1). *"This Other Dude Did It!" A Test of the Alternative Explanation Defense*. Retrieved from The Jury Expert: http://www.thejuryexpert.com/2009/07/this-other-dude-did-it-a-test-of-the-alternative-explanation-defense/

The Argument from Deception. (n.d.). Retrieved from Theory of Knowledge: http://www.theoryofknowledge.info/scepticism/sceptical-arguments/the-argument-from-deception/

Van Oirschot, M. (2015, January 8). *Why do we still have a cognitive bias that makes us send innocent people to jail? – Explanations of the confirmation bias*. Retrieved from The Inquisitive Mind: http://www.in-mind.org/blog/post/why-do-we-still-have-a-cognitive-bias-that-makes-us-send-innocent-people-to-jail

Vegge, H. H. (2009). Where only fools dare to tread: An empirical study on the prevalence of Zero-Day malware. *Internet Monitoring and Protection, 2009. ICIMP'09. Fourth International Conference on*, 66-71.

Viswanathan, B., Ellis, J., Howell, M., Stark, M., & Berry, G. (n.d.). *Why do good lawyers support/defend criminals?* Retrieved from Quora: https://www.quora.com/Why-do-good-lawyers-support-defend-criminals

Von Oech, R. (2007, March 6). *The Red Queen Effect*. Retrieved February 13, 2016, from Creative Think: http://blog.creativethink.com/2007/03/the_red_queen_e.html

Vuze Remote. (n.d.). Retrieved from Vuse: http://www.vuze.com/products/vuze-remote

Last Updated: March 20th, 2018

Upcoming Training

SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Abu Dhabi 2018	Abu Dhabi, United Arab Emirates	Apr 07, 2018 - Apr 12, 2018	Live Event
SANS London April 2018	London, United Kingdom	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
Baltimore Spring 2018 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Apr 23, 2018 - Apr 28, 2018	vLive
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201805,	May 02, 2018 - Jun 14, 2018	vLive
Community SANS Virginia Beach SEC503	Virginia Beach, VA	May 07, 2018 - May 12, 2018	Community SANS
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
SANS Oslo June 2018	Oslo, Norway	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
Minneapolis 2018 - SEC503: Intrusion Detection In-Depth	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	vLive
SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LA	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
San Antonio 2018 - SEC503: Intrusion Detection In-Depth	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
Community SANS Columbia SEC503	Columbia, MD	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS Virginia Beach 2018	Virginia Beach, VA	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, Japan	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, Netherlands	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS London September 2018	London, United Kingdom	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NV	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS Stockholm 2018	Stockholm, Sweden	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced