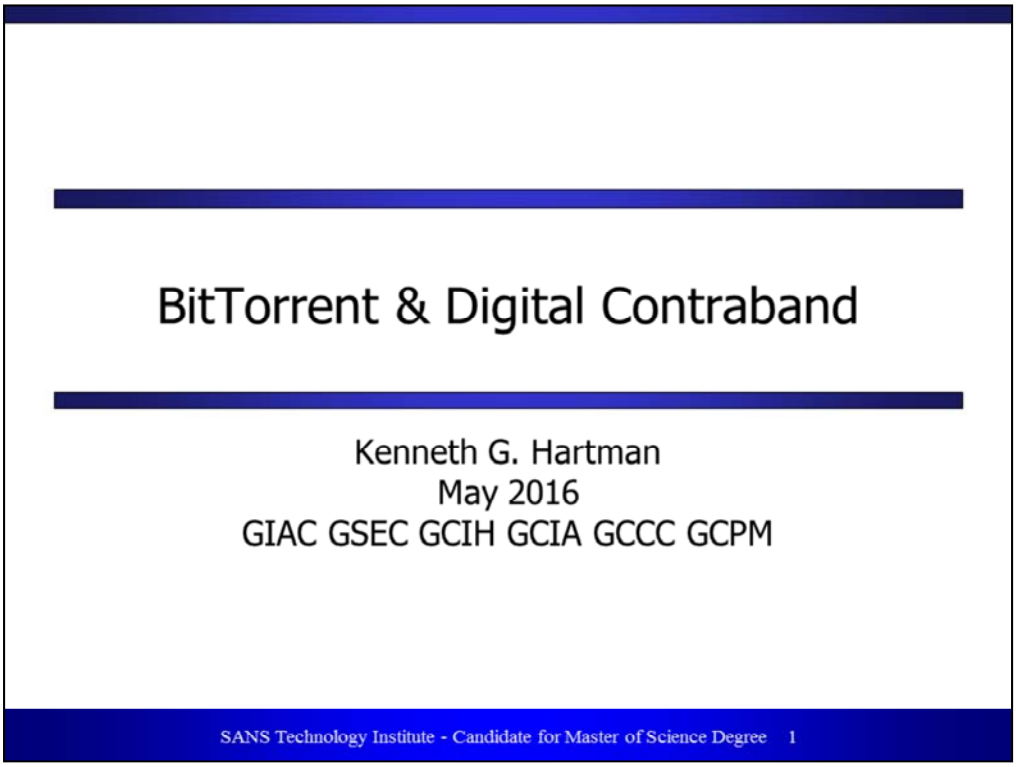
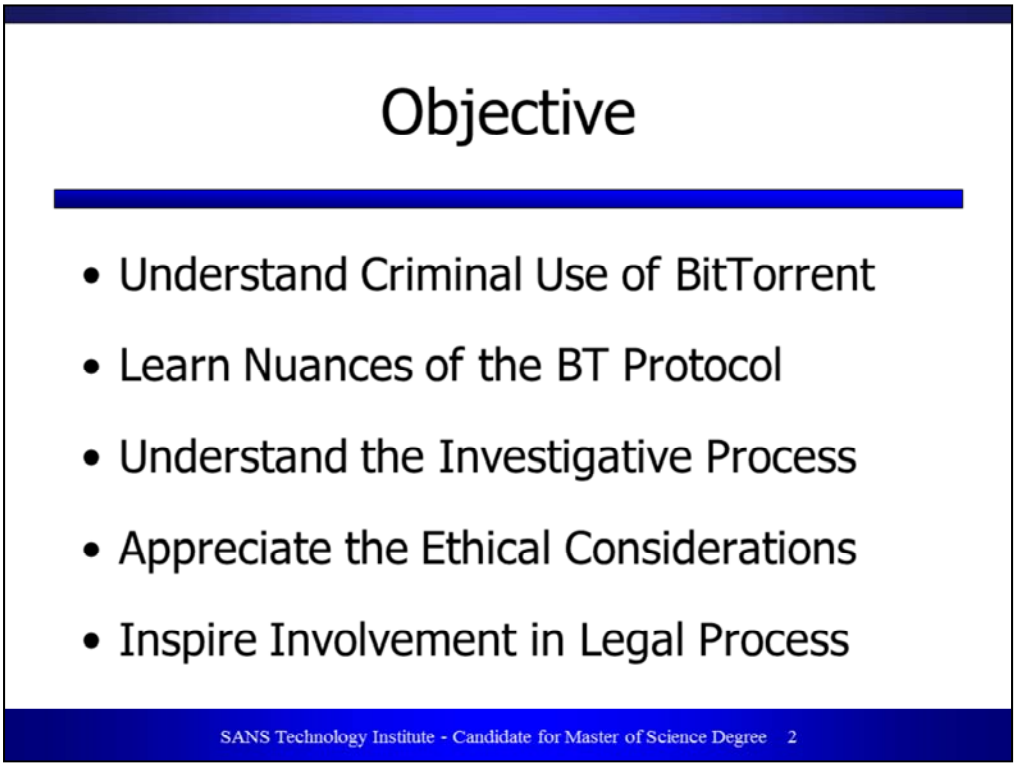


Abstract

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 talk explains the technology, the criminal investigative process, and the legal and ethical issues surrounding BitTorrent with a goal of improving the base knowledge of those on both sides of the legal process.

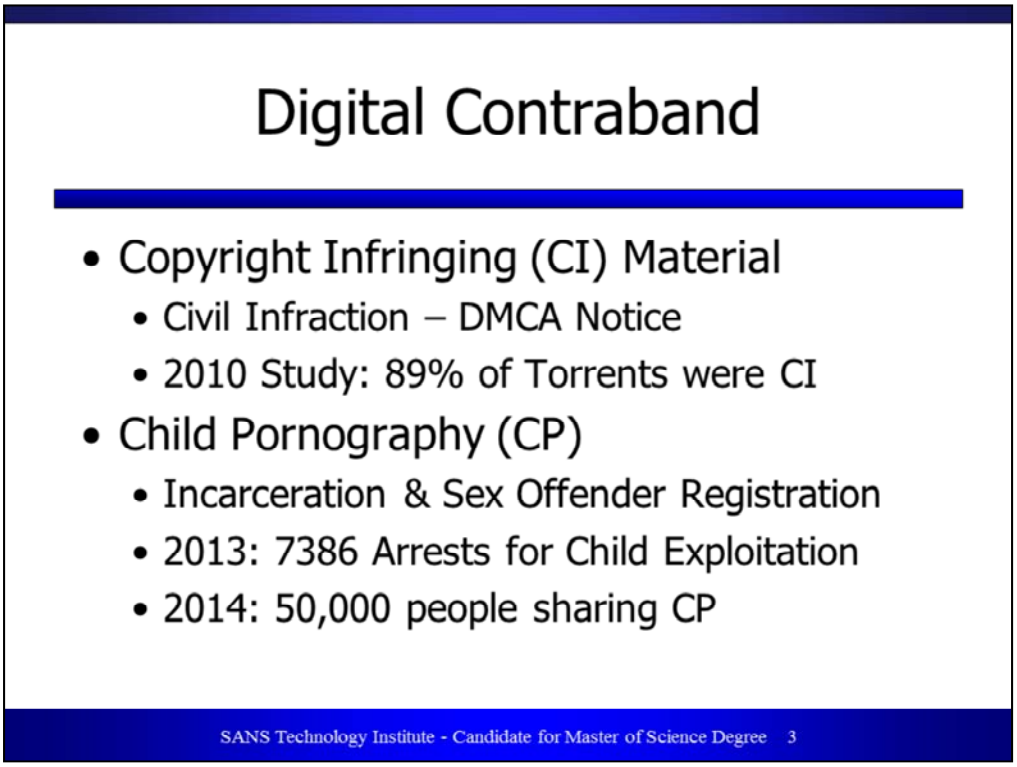
Kenneth G. Hartman is the Senior Product Manager for Cloud Security and Privacy for SAP Ariba. Ken's mission is "I help my company earn and maintain the trust of our customers in our products and services." Toward this end, Ken drives a variety of privacy and data protection initiatives while managing the product security roadmap.

Ken holds a BS Electrical Engineering from Michigan Technological University and has earned the CISSP, as well as multiple GIAC security certifications. He is also a Certified Professional in Healthcare Information Management Systems (CPHMIS) and served on the Health Information Management Systems Society (HIMSS) Privacy & Security Committee in 2012.



During this talk, I will provide a look behind the scenes into a law enforcement investigation of digital contraband involving BitTorrent. Along the way, I will cover a variety of technical details regarding the BitTorrent Protocol and will demonstrate why a deep technical understanding of technology can make or break a criminal case.

I served as a "Non-testifying expert consultant" for the defense team in a criminal case, and I will talk about my decision to serve in this capacity as opposed to being an expert witness or conversely shunning the case. And lastly, I want to inspire other security professionals to consider this type of work so that justice will be served.



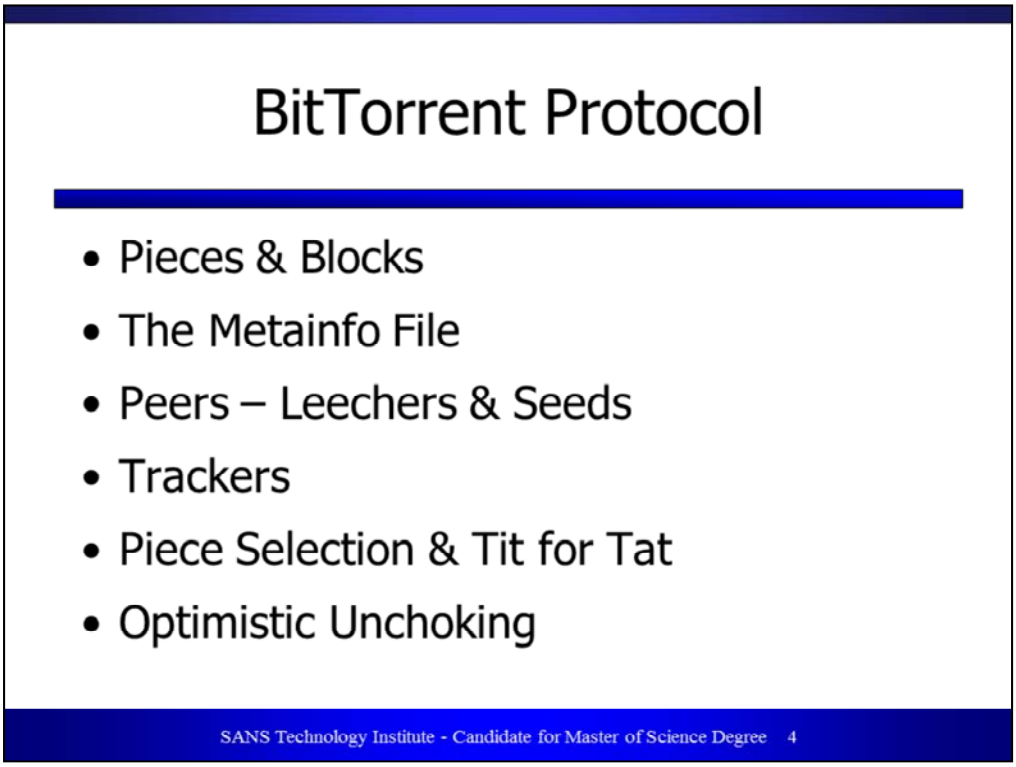
According to a 2010 study of a random sample of 1000 torrents, 89% were CI with 43.4% being movies, 29.1% TV shows, and music accounting for 16.5%.

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.

According to the Internet Crimes Against Children (ICAC) Task Force, there were 7386 arrests in 2013 for child exploitation. They also claim 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.

Child Sexual Abuse is a heinous crime, and there increasingly more severe sentences for possession, distribution, and production of child sexually abusive materials. Persons who are found guilty of a crime involving CP are also required to register as a Sex Offender in the state that they live.

Much of the earlier research into combating CI laid the technical foundation for policing CP in the BitTorrent ecosystem



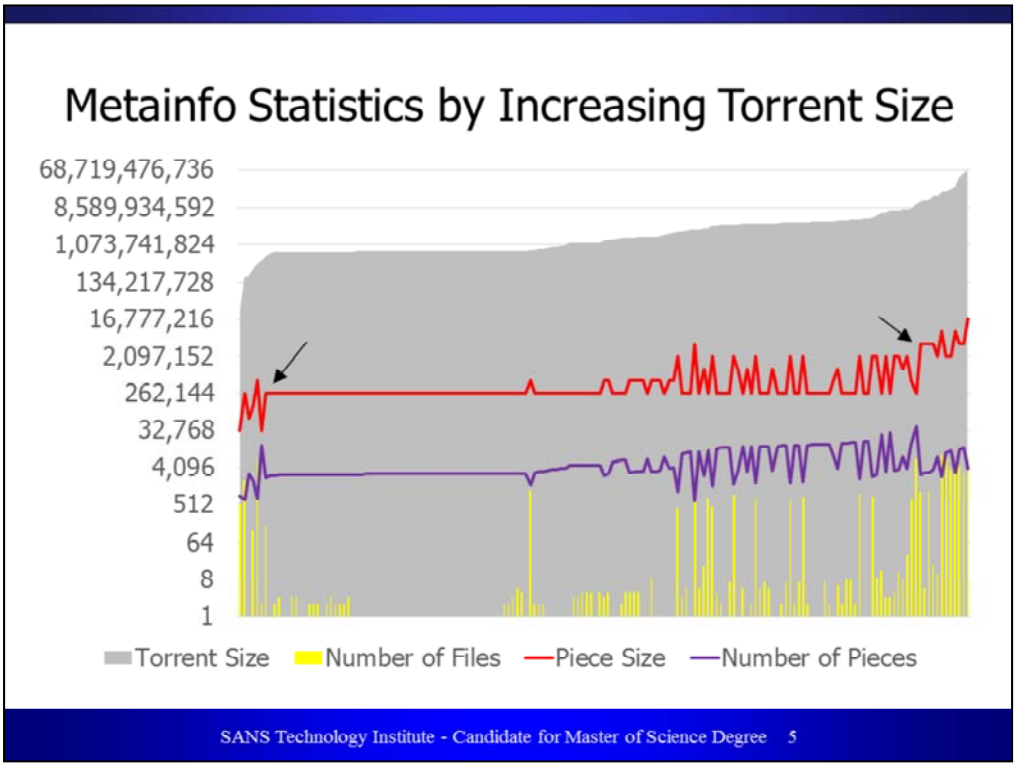
To distribute a file, the BitTorrent client breaks the file into several pieces of equal size according to a "metainfo" file. Members of the swarm announce which pieces they have and which pieces they want. Pieces are further divided into 16 kB "blocks" to facilitate distribution.

Anyone can publish digital media by creating a "metainfo" file. 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

BitTorrent is a peer to peer networking protocol, and there are two types of peers: Leechers and Seeds. A seed is a peer that has possession of all of the pieces and is making them available to the other peers in the swarm. Conversely a leecher is a peer without all of the pieces, but some use this term (imprecisely) to connote a peer that is downloading without uploading.

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.

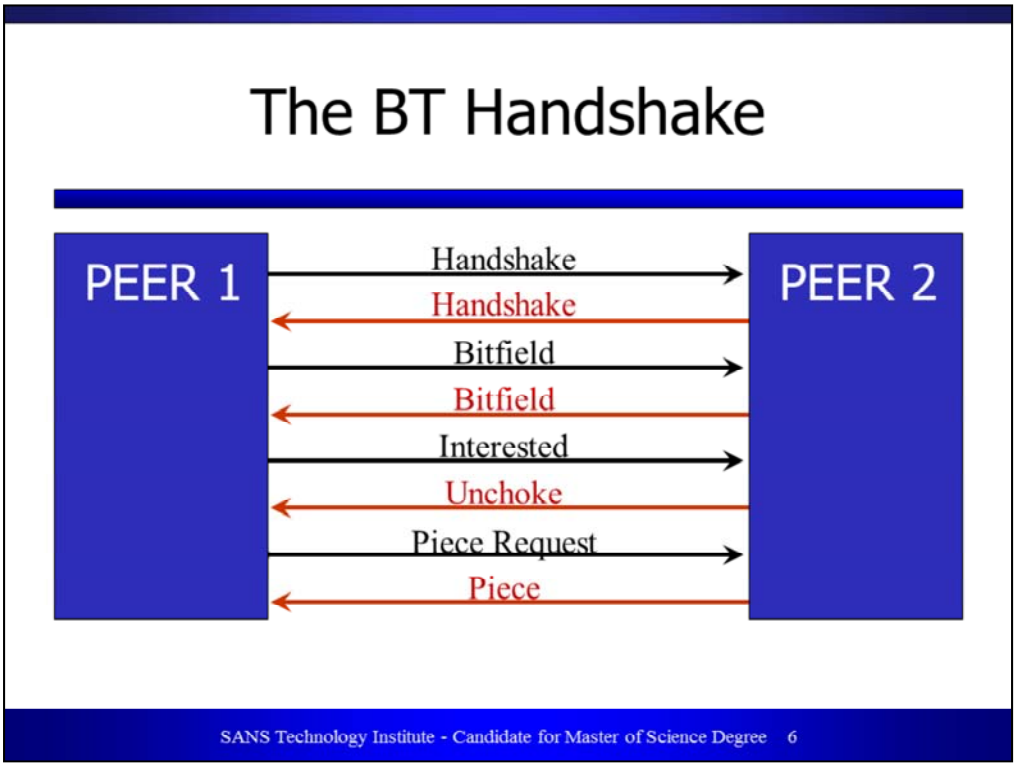
The incentive mechanism built into BitTorrent to encourage sharing is called "Tit-for-Tat." This algorithm identifies the peers that are most willing to share and that have the best upload bandwidth and chokes the rest. However, once every 30 seconds to peer will perform an "optimistic unchoke" on a random peer in an attempt to discover an even better peer to exchange pieces with.



I took a look at 169 torrent files that I downloaded via a script from legittorrents.com to see if the average piece size was actually 250 Kb long and it does indeed seem to be that for files larger than ½ GB up to about 10 Gb.

After 10 Gb, most torrents will have a larger piece size to keep the number of pieces to a manageable amount.

Another point, illustrated by this graph is that the number of files in the torrent, has no bearing on either the piece size or number of pieces.

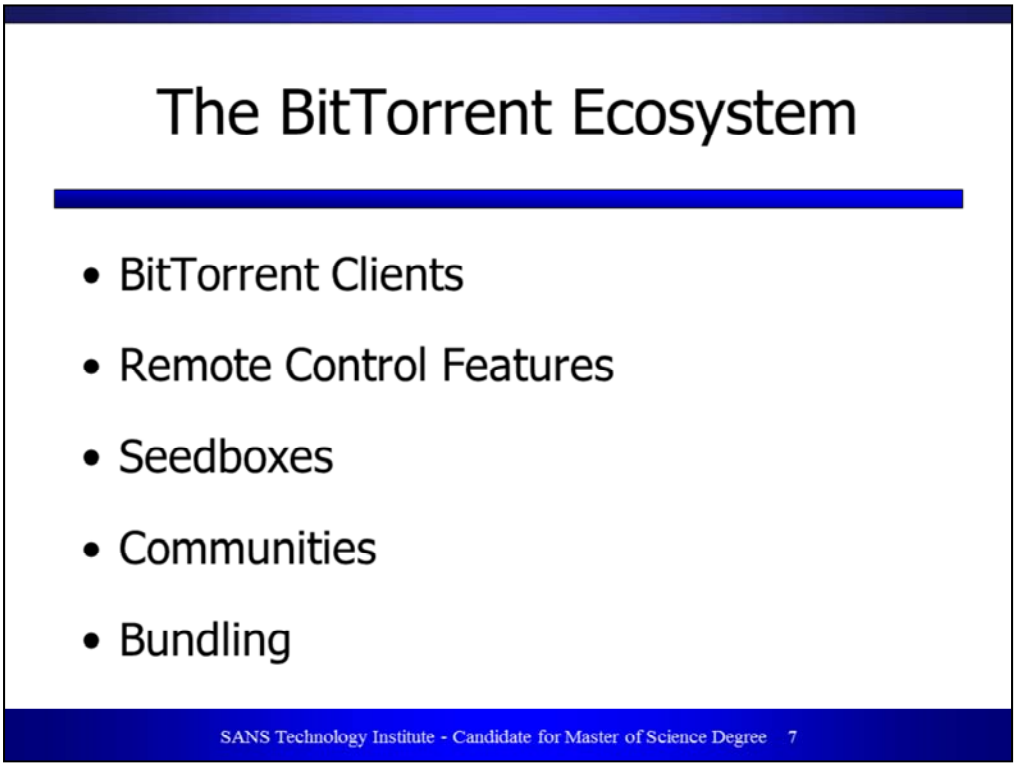


Peers initiate communication with each other by exchanging handshake messages. The handshake consists of a plain text protocol identifier string, the Infohash, and a peer identification field.

After the handshake, the peers exchange a bitfield message that compactly describes the pieces that each peer has obtained.

Now, each peer knows which pieces the other peer can offer, and the initiator (Peer 1) sends an interested message to notify the other peer that it would like to download pieces.

Peer 2 responds with an unchoke message only if it is willing to share pieces with Peer 1. Upon receiving an unchoke message, the leecher asks for specific blocks of the piece it is seeking.

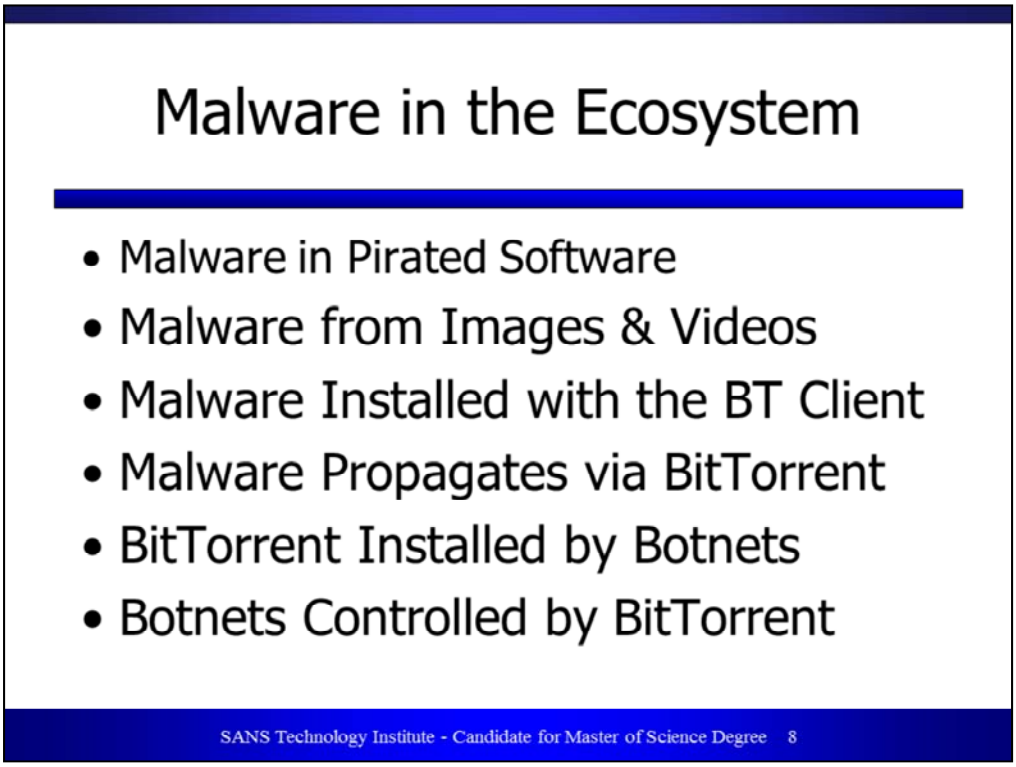


There are more than thirty-five BitTorrent clients, each with a variety of features and licenses. Among the clients considered the most popular in 2016, are uTorrent, Vuze, Deluge, and BitComet. Some of these clients also have remote control features, allowing the client to be controlled by either a web page or a smartphone app. At least one app, Transmission, also has a command line interface, that allows it to be scripted or accessed over SSH. 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.

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.

A private community is a web portal that requires user registration before one can publish or download a metainfo file. Although the portal may be private, the metainfo files it hosts may also reference trackers external to the community, thereby leaking information about the community's existence.

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.



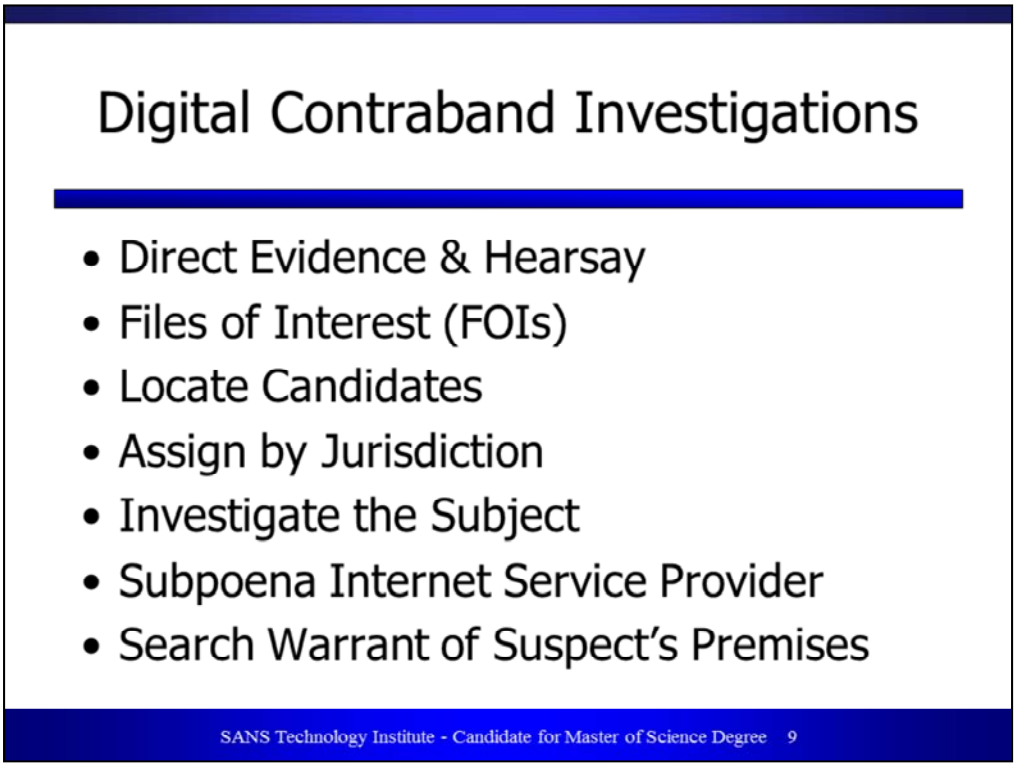
A frequently cited study from 2008 determined that 18% of all the executable programs distributed via BitTorrent contain malware. Another study found that 14.5% of the files in their sample of approximately 400 downloads contained zero-day malware.

Some BT users seek pirated software or key generators or cracks, that are frequently loaded with malware. Sometimes an executable program that is designed to look like an image or a video file. When clicked the malware will install.

Certain types of video files may contain malicious hyperlinks that automatically load in a browser, infecting the computer with a "drive-by attack."

Some BitTorrent clients may even install malware along with the application. This issue was first observed in 2007 when attackers bundled malware with the Torrent 101, TorrentQ, Get-Torrent, and BitRoll clients. In 2013, an installer for Xunlei spread malware to thousands of Microsoft Windows and Android users in China. Certain malware uses BT as the propagation mechanism. Examples of this are the Impard-A virus and the PUSHBOT worm.

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. In 2011, a variant of the KOOBFACE worm was found to contain a hidden BT client. Lastly trackers and metainfo indexers can unwittingly become a C&C server for BotNets due to the nature of the BT protocol.



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.

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.

Based on geo-locating 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 and is distributing it.

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. Based on the results of the Subpoena, a search warrant will be obtained to search the subject's premises for 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.

STATE OF MICHIGAN 86th JUDICIAL DISTRICT	AFFIDAVIT FOR SEARCH WARRANT	CASE NO.

Police Agency: Michigan State Police Computer Crimes Unit

Report Number: CCU-[redacted]

Detective [redacted] Affiant(s), state that:

1. The **PERSON, PLACE, OR THING TO BE SEARCHED** is described as and is located at:

Charter Communications
12405 Powerscourt Drive
St. Louis, MO 63131
FAX: 314-909-0609

2. The **PROPERTY** to be searched for and seized, if found, is specifically described as:

Any and all records identifying the physical access point of the IP address [redacted] including subscriber information, physical home address, telephone numbers, billing history, credit card and or payment information, all email addresses, all Charter email content (Inbox, Outbox, Drafts, Saved, Any and all Folders, and Deleted), upload and download usage, logging information, modem device information and any other information maintained by or within the databases of Charter Communications.

3. The **FACTS** establishing probable cause or the grounds for the search are:

1) Your Affiant, Detective [redacted] hereinafter referred to as Affiant, has been a law enforcement officer for approximately [redacted] years, the last [redacted] of which with the [redacted] Police Department. Since [redacted] Affiant has been assigned to the Michigan Department of State Police, Internet Crimes Against Children (ICAC) Task Force. Affiant is currently conducting an investigation of possible violation of MCL Section 750.145c "Child Sexually Abusive Activity or Material."

2) Your Affiant is familiar with and has been trained to conduct investigations using Peer to Peer (P2P) file sharing, specifically different clients that operate on the BitTorrent file sharing network. BitTorrent programs are typically free to download and used for the exchange of files between computer users.

3) A growing phenomenon on the Internet is peer to peer (P2P) file sharing. P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software from a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. BitTorrent, one type of P2P software, sets up its searches by keywords typically on torrent websites. The results of a keyword search are displayed to the user. The website does not contain the files being shared only file referred to as a Torrent. The user then selects a .torrent file(s) from the results for download. This .torrent file contains instructions on how a user can download the file(s) referenced in the Torrent. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) sharing the actual files (not the torrent file but the actual files referenced in the .torrent file using any BitTorrent client.)

This affidavit consists of: 3 pages.

[redacted]
Affiant Detective [redacted]

Review on: _____
Date

By: _____
Prosecuting Official

Subscribed and sworn before me on: [redacted]
Date

[redacted]
Judge/Magistrate

STATE OF MICHIGAN 86th JUDICIAL DISTRICT	AFFIDAVIT FOR SEARCH WARRANT	CASE NO.

4) For example, a person interested in obtaining child pornographic images would open the BitTorrent website on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The results of the search are returned to the user's computer and displayed on the torrent site. The user selects a .torrent from the results displayed the file(s) he/she wants to download. Once the .torrent file is downloaded, it is used by a BitTorrent program which the user had previously installed. The .torrent file is the set of instructions the program needs to find the files referenced in the .torrent file. The file(s) is downloaded directly from the computer or computers sharing the file. The downloaded file is stored in the area previously designated by the user and/or the software. The downloaded file will remain until moved or deleted.

5) One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file.

6) A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location, making it possible for data to be transferred between computers.

7) The computer running the file sharing application, in this case a BitTorrent application has an IP address assigned to it while it is on the internet. Investigators are able to see the IP address of any computer system sharing files. Investigators can then search public records (ARIN) that are available on the internet to determine the internet service provider who has assigned that IP address. Based upon the IP address assigned to the computer sharing files, subscriber information can be obtained from the internet service provider.

8) On [redacted], your Affiant was aware that D/SGT. [redacted] of the Michigan State Police Computer Crimes Unit, was using a BitTorrent file sharing program, conducting undercover investigations into the internet sharing of child pornography. On the [redacted] discovered a computer sharing child pornography and was located on the BitTorrent file sharing network. The computer was utilizing the IP address of [redacted]

9) The following files of interest were downloaded by D/SGT. [redacted] between the dates and times of [redacted] at [redacted] EDT (UTC -4) and [redacted] at [redacted] EDT (UTC -4):

[redacted]

This affidavit consists of: 3 pages.

[redacted]
Affiant Detective [redacted]

Review on: _____
Date

By: _____
Prosecuting Official

Subscribed and sworn before me on: [redacted]
Date

[redacted]
Judge/Magistrate

STATE OF MICHIGAN 86th JUDICIAL DISTRICT	SEARCH WARRANT	CASE NO.

TO THE SHERIFF OR ANY PEACE OFFICER:

Police Agency: Michigan State Police Computer Crimes Unit

Report Number: CCU-[redacted]

Detective [redacted] has sworn to the attached affidavit regarding the following:

1. The **PERSON, PLACE, OR THING TO BE SEARCHED** is described as and is located at:

Charter Communications
12405 Powerscourt Drive
St. Louis, MO 63131
FAX: 314-909-0609

2. The **PROPERTY** to be searched for and seized, if found, is specifically described as:

Any and all records identifying the physical access point of the IP address [redacted] including subscriber information, physical home address, telephone numbers, billing history, credit card and or payment information, all email addresses, all Charter email content (Inbox, Outbox, Drafts, Saved, Any and all Folders, and Deleted), upload and download usage, logging information, modem device information and any other information maintained by or within the databases of Charter Communications.

IN THE NAME OF THE PEOPLE OF THE STATE OF MICHIGAN: I have found that probable cause exists and you are commanded to make the search and seize the described property. Leave a copy of this warrant with affidavit attached and tabulation (a written inventory) of all property taken with the person from whom the property was taken or at the premises. You are further commanded to promptly return this warrant and tabulation to the court.

IT IS FURTHER ORDERED that the account holder(s) not be notified of this request pursuant to MCL 780.654(3) for the term provided by law.

IT IS FURTHER ORDERED that since the stored electronic communications are being requested pursuant to a search warrant under 18 USC 2703(b)(1)(A) that the request is being made without notice to the account holder(s) and that the provider shall not disclose the nature or existence of the warrant or request.

IT IS FURTHER ORDERED that, to avoid prejudice to the Government's criminal investigation, Charter Communications and its agents and employees shall not disclose or cause a disclosure of this search warrant, court order or the request for information, facilities and assistance by the Michigan State Police, or the existence of the investigation to any person other than those of its agents and employees who require this information to accomplish the services hereby ordered. In particular, Charter Communications and its agents and employees shall not make such disclosure to any subscriber or any interceptee or participant in the intercepted communications.

Issued: [redacted]

Date

[redacted]

Judge/Magistrate

Bar no.

STATE OF MICHIGAN 86th JUDICIAL DISTRICT	SEARCH WARRANT	CASE NO.

TO THE SHERIFF OR ANY PEACE OFFICER:

Police Agency: Michigan State Police

Report Number: CCU-[redacted]

Detective [redacted] has sworn to the attached affidavit regarding the following:

1. The person, place, or thing to be searched is described as and is located at:

[redacted] State Of Michigan, [redacted]

Said address is more fully described as a two story residence, [redacted]

Any and all persons upon the listed property and all vehicles associated with the listed property.

This warrant to specifically to include a search of the digital contents of electronic devices located within the above described apartment and/or upon persons and vehicles.

2. The PROPERTY to be searched for and seized, if found, is specifically described as:

Any and all evidence of child sexually abusive activity or the production, distribution, or possession of child sexually abusive material as defined in MCL 750.145c et seq, including but not limited to:

1. Any and all Internet communication device(s) and storage medium(s) of all makes and kinds that are computer or Internet compatible and all their peripherals and attachments, whatever their function; this includes computers, laptops, phones, pads, gaming devices and all similarly Internet compatible devices;

2. This warrant to also specifically include the files within those devices, including but not limited to electronic or magnetic data files which contain nude, sexually suggestive, or sexually explicit images of minors, or of adults engaging in sexual activity with or in the presence of minors or the identity of the owner/user of these devices;

3. Electronic or magnetic data files which contain descriptions of or attempts to solicit child sexually abusive activity, and/or evidence of the distribution of child sexually abusive material, including but not

limited to e-mail messages and/or text files;

4. Any application software or other programs which could be used to facilitate the creation, transmission or storage of the described data files, including but not limited to photo editing software, e-mail applications, word processing software, and/or software used to access the Internet;

5. Any passwords or password files necessary to gain access to the files, software, or applications described above;

6. Copies of Internet web pages stored in the computer's memory which include images of the type described, or which describe, display, or promote child sexually abusive activity or child sexually abusive material;

7. Trace evidence of any of the above types of data files which may remain on the internal memory of any computer or digital camera, or on removable storage media, after files have been deleted.

8. Magazines, books, printed material, removable media including floppy disks, CD-Rom's, DVD's, zip disks, external drives, cell phones, contents of cell phones;

9. Computers, including personal computers, computer systems, central processing units, and computer peripheral devices, any electronic, magnetic, optical, electrochemical, or other high speed data processing and storage devices performing logical, arithmetic, or storage functions; data storage facilities (internal and/or peripheral) or media storage devices such as magnetic tape, hard disk drives, floppy disks, CD-ROM or scanner;

10. Data stored within computers or other processing and storage devices, to include computer applications, images, text, programs, encryption routines and algorithms, or other data that may be decoded, reconstituted, or otherwise manipulated to produce, utilize, transmit, receive, encrypt, encode, or display such images, text, programs, encryption routines, and algorithms.

11. Computer manuals, documents, logs and system documentation or instructional material including passwords, passphrases or other material whether handwritten, printed, or in book form, relating to such devices and printers.

12. Modems, communications facilities directly relating to or operating in conjunction with such device; devices for printing records of data and such records or data produced in various forms;

13. Electronic communications stored within computers or other processing and storage devices as e-mail. Such information and/or communications that may be in the form of electronic communications (such as e-mail) residing on any media (e.g., magnetic, optical or digital media). That information may include electronic communications held or maintained in electronic storage by an electronic communication service or remote computing service, as those services are defined within 18 U.S.C. 2703. These communications are referred to herein as "stored communications". These communications related to this case stored in the suspect's computer or other electronic devices as e-mail. That federal law, which is part of the Electronic Communications Privacy Act, allows interception of such electronic

STATE OF MICHIGAN 86th JUDICIAL DISTRICT	SEARCH WARRANT	CASE NO.

communication pursuant to a search warrant.

14. Printed copy(s) of electronic communications between suspect and conspirators, known or unknown.

15. Mail or any other documentation in any form or medium of the resident(s) of the address and/or the owner/users of the electronic/digital devices.

IN THE NAME OF THE PEOPLE OF THE STATE OF MICHIGAN: I have found that probable cause exists and you are commanded to make the search and seize the described property. Leave a copy of this warrant with affidavit attached and tabulation (a written inventory) of all property taken with the person from whom the property was taken or at the premises. You are further commanded to promptly return this warrant and tabulation to the court.

Issued _____
Date

[redacted]
Judge/Magistrate Bar no.

RETURN AND TABULATION

Search was made: _____ and the following property was seized:
Date

AG CASE

STATE OF MICHIGAN 86th JUDICIAL DISTRICT 13TH JUDICIAL CIRCUIT	**COMPLAINT** **FELONY**	DISTRICT: [redacted] CIRCUIT: [redacted] CTN: [redacted] MSP #: CCU [redacted]
District Court ORI: [redacted]	Circuit Court ORI: [redacted]	AG ORI: [redacted]

THE PEOPLE OF THE STATE OF MICHIGAN v [redacted]	Victim or complainant: STATE OF MICHIGAN Complaining Witness D/SPL. [redacted]
Co-defendant(s)	Date: On or about [redacted]
City/Twp./Village [redacted] / County in Michigan / Defendant SID	Defendant DOB [redacted]
Charge(s) See Below	Maximum Penalty See Below

PHILLIPS

STATE OF MICHIGAN, COUNTY OF GRAND TRAVERSE

The complaining witness says that on the date above and at/or in [redacted] MI, the defendant, contrary to law,

COUNT 1: CHILD SEXUALLY ABUSIVE MATERIAL - POSSESSION

did knowingly possess child sexually abusive material; contrary to MCL 750.145c(4). [750.145C4-A]

SORA NOTICE

This is a Tier I offense under the Sex Offender Registration Act (SORA). It is a Tier II offense if the defendant has a prior conviction for a Tier I offense. MCL 28.722(s) & (t). It is a Tier III offense if the defendant has a prior conviction for a Tier II offense. MCL 28.722(v).

FELONY: 4 Years and/or $10,000.00

COUNT 2: CHILD SEXUALLY ABUSIVE MATERIAL - POSSESSION

did knowingly possess child sexually abusive material; contrary to MCL 750.145c(4). [750.145C4-A]

SORA NOTICE

This is a Tier I offense under the Sex Offender Registration Act (SORA). It is a Tier II offense if the defendant has a prior conviction for a Tier I offense. MCL 28.722(s) & (t). It is a Tier III offense if the defendant has a prior conviction for a Tier II offense. MCL 28.722(v).

FELONY: 4 Years and/or $10,000.00

COUNT 3: CHILD SEXUALLY ABUSIVE MATERIAL - POSSESSION

did knowingly possess child sexually abusive material; contrary to MCL 750.145c(4). [750.145C4-A]

SORA NOTICE

This is a Tier I offense under the Sex Offender Registration Act (SORA). It is a Tier II offense if the defendant has a prior conviction for a Tier I offense. MCL 28.722(s) & (t). It is a Tier III offense if the defendant has a prior conviction for a Tier II offense. MCL 28.722(v).

FELONY: 4 Years and/or $10,000.00

COUNT 4: CHILD SEXUALLY ABUSIVE MATERIAL - POSSESSION

did knowingly possess child sexually abusive material; contrary to MCL 750.145c(4). [750.145C4-A]

SORA NOTICE

This is a Tier I offense under the Sex Offender Registration Act (SORA). It is a Tier II offense if the defendant has a prior conviction for a Tier I offense. MCL 28.722(s) & (t). It is a Tier III offense if the defendant has a prior conviction for a Tier II offense. MCL 28.722(v).

FELONY: 4 Years and/or $10,000.00

COUNT 5: CHILD SEXUALLY ABUSIVE MATERIAL - POSSESSION

did knowingly possess child sexually abusive material; contrary to MCL 750.145c(4). [750.145C4-A]

SORA NOTICE

This is a Tier I offense under the Sex Offender Registration Act (SORA). It is a Tier II offense if the defendant has a prior conviction for a Tier I offense. MCL 28.722(s) & (t). It is a Tier III offense if the defendant has a prior conviction for a Tier II offense. MCL 28.722(v).

FELONY: 4 Years and/or $10,000.00

COUNT 6: CHILD SEXUALLY ABUSIVE ACTIVITY- DISTRIBUTING OR PROMOTING

did distribute, promote, or finance the distribution or promotion of child sexually abusive activity or child sexually abusive material; contrary to MCL 750.145c(3). [750.145C3]

SORA NOTICE

This is a Tier II offense under the Sex Offender Registration Act (SORA). It is a Tier III offense if the defendant has a prior conviction for a Tier II offense. MCL 28.722(u) & (v).

FELONY: 7 Years and/or $50,000.00

COUNT 7: COMPUTERS - USING TO COMMIT A CRIME - MAXIMUM IMPRISONMENT OF 4 YEARS OR MORE BUT LESS THAN 10 YEARS

did use a computer program, computer, computer system, or computer network to commit, attempt to commit, conspire to commit, or solicit another to commit MCL 750.797(3)(D); contrary to MCL 752.796, and MCL 752.797(3)(d). [752.7973D]

FELONY: 7 Years and/or $5,000.00; reimburse government for expenses incurred in relation to violation in manner indicated by MCL 769.1f (see MCL 752.797(7))

Upon conviction of a felony or an attempted felony court shall order law enforcement to collect DNA identification profiling samples.

The complaining witness asks that defendant be apprehended and dealt with according to law.

[redacted]

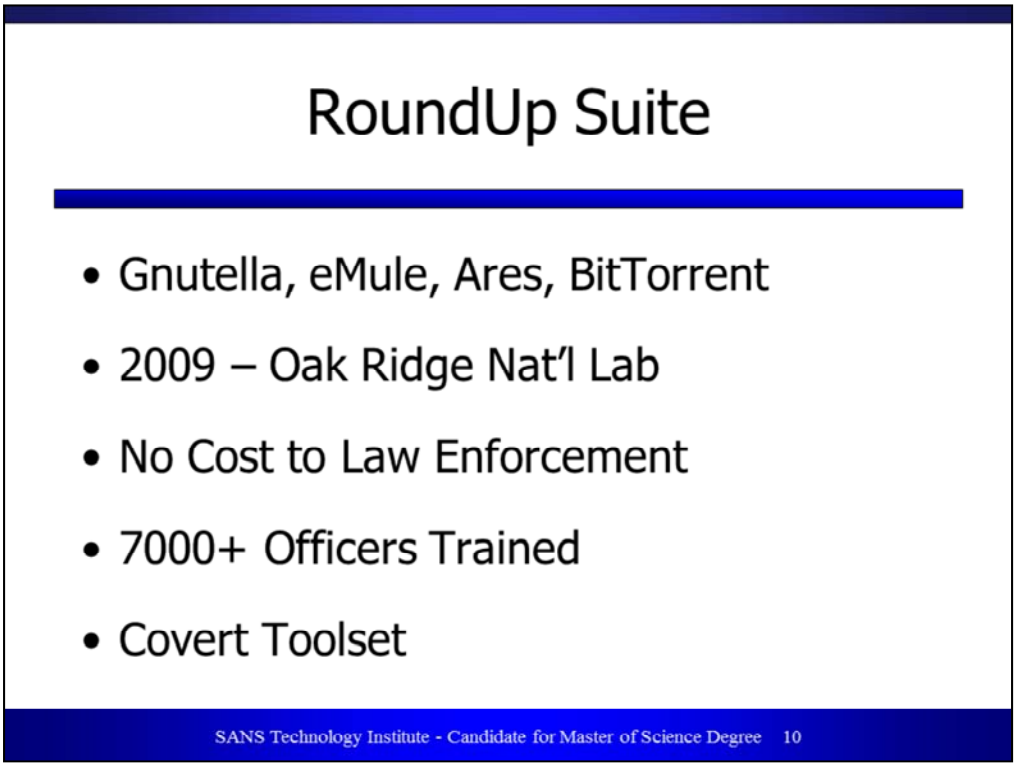
Complaining witness signature

Subscribed and sworn to before me on [redacted]

Date

[redacted]

Judge/Magistrate/Clerk Bar no.

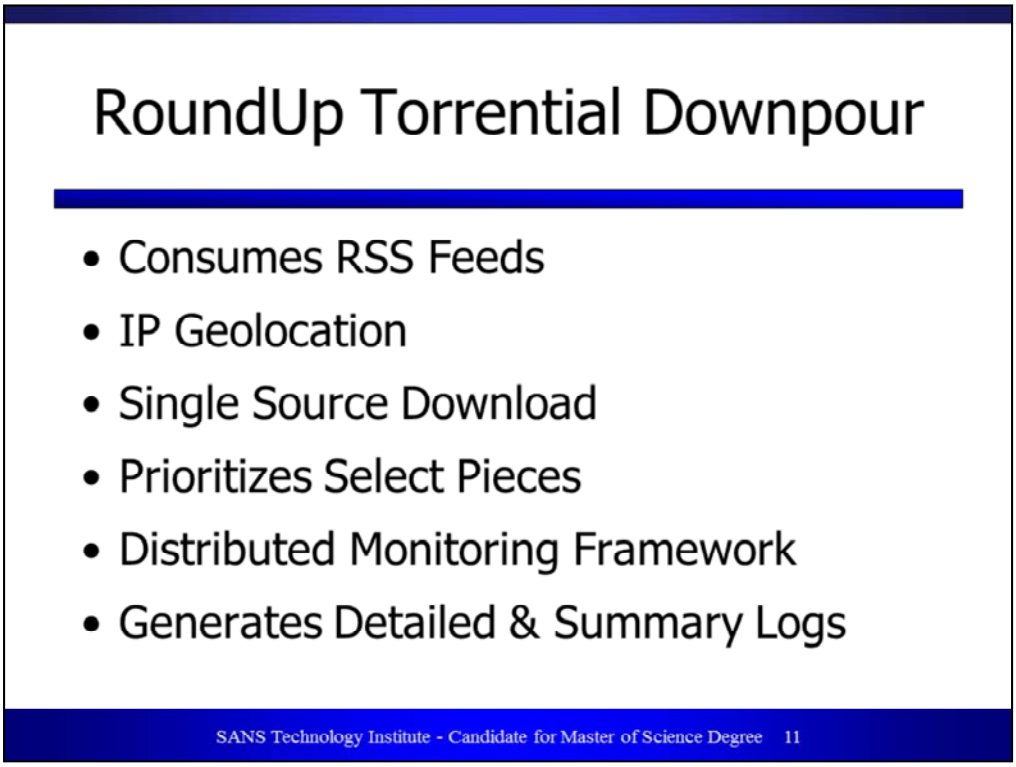


There are RoundUp tools for other P2P networks including Gnutella and eMule. The tool for BitTorrent is known as "RoundUp Torrential Downpour."

Used to identify 850 contact offenders that were sharing child pornography and to rescue 230 children. It has been used to generate over 10,300 search warrants

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. However, its existence has leaked out during the legal discovery process and one defendant even tried unsuccessfully to subpoena the source code for RoundUp-Gnutella.

The information that I am sharing with you today has been gleaned from the various research papers that the tool developers have published. Interestingly, for forensic investigative tools to be considered legally valid, they must be peer reviewed.



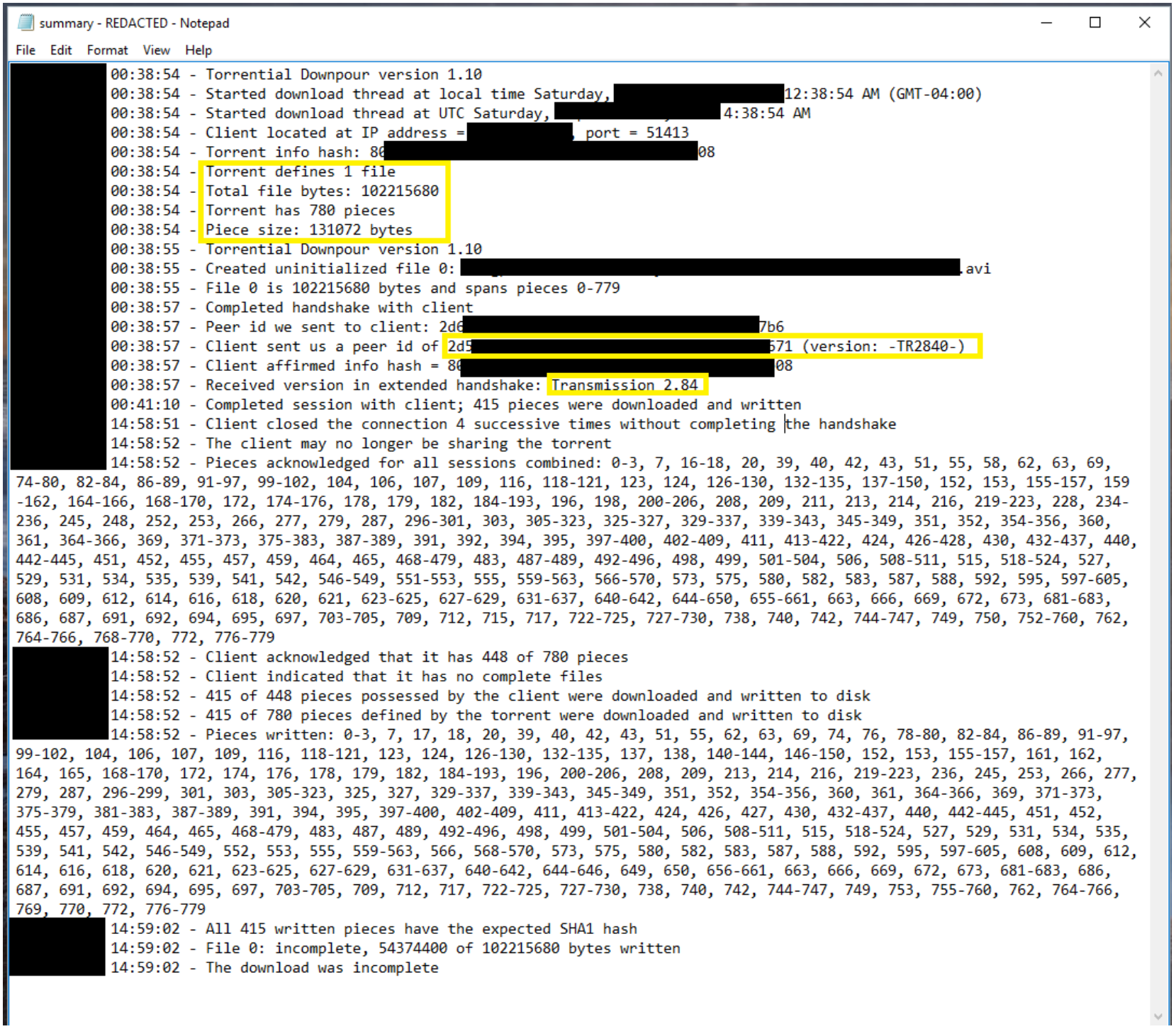
A 2011 press release stated that the software focuses on new torrent files announced in Really Simple Syndication protocol (RSS) feeds in addition to crawling the websites that index metainfo files, and it promptly investigates the Internet addresses of the peers in the swarm to create a list of suspects for further investigation. This list is partially based on the Geolocation of the IP address and the ISP that it belongs to.

The Roundup Torrential Downpour is apparently written in Java according to early published research papers on the software.

Instead of using the "Rarest-First" Piece selection algorithm defined by the protocol, RoundUp prioritizes select pieces of high evidentiary value in the event that it cannot download the entire torrent, due to the length of time it takes to perform a single source download by taking advantage of the periodic optimistic unchoke feature of the BitTorrent protocol.

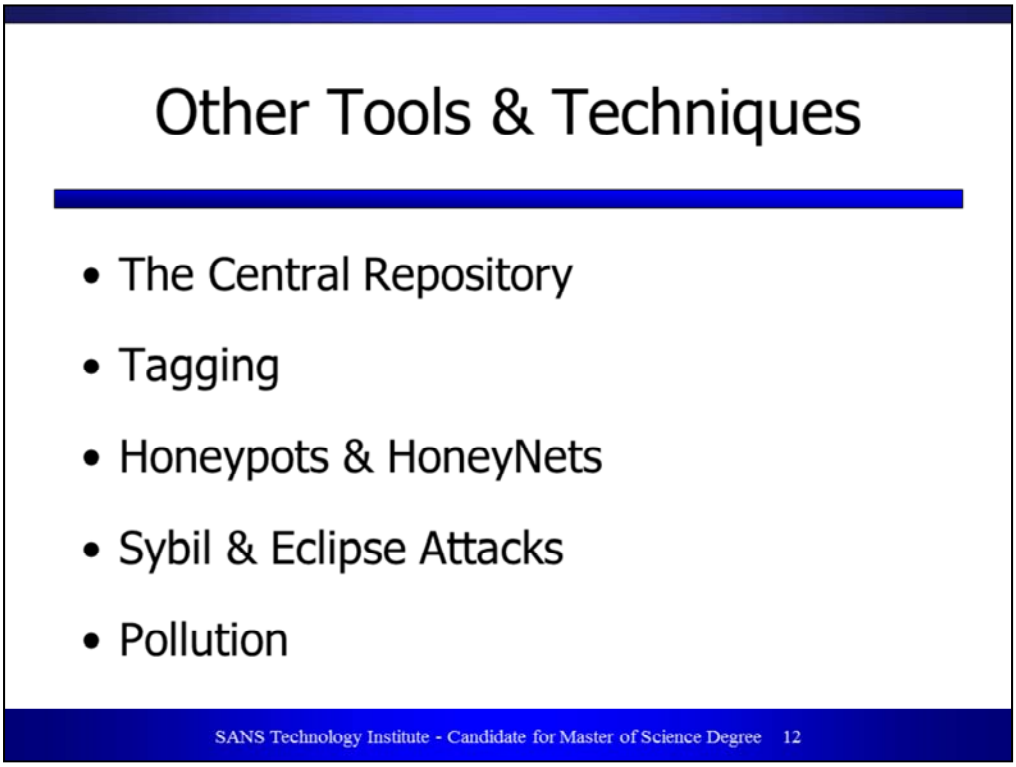
To operate covertly, it seems that the Roundup system includes a distributed monitoring framework, consisting of software agents that can participate as BitTorrent clients in swarms under investigation. These agents would operate from a variety of geographically disperse IP addresses with different Internet Service Providers.

The software that performs the single source download generates both a detailed and summary log that can be used as evidence.


summary - REDACTED - Notepad

File Edit Format View Help

[redacted] 00:38:54 - Torrential Downpour version 1.10
00:38:54 - Started download thread at local time Saturday, [redacted]12:38:54 AM (GMT-04:00)
00:38:54 - Started download thread at UTC Saturday, [redacted]4:38:54 AM
00:38:54 - Client located at IP address = [redacted], port = 51413
00:38:54 - Torrent info hash: 80[redacted]08
00:38:54 - Torrent defines 1 file
00:38:54 - Total file bytes: 102215680
00:38:54 - Torrent has 780 pieces
00:38:54 - Piece size: 131072 bytes
00:38:55 - Torrential Downpour version 1.10
00:38:55 - Created uninitialized file 0: [redacted].avi
00:38:55 - File 0 is 102215680 bytes and spans pieces 0-779
00:38:57 - Completed handshake with client
00:38:57 - Peer id we sent to client: 2d6[redacted]7b6
00:38:57 - Client sent us a peer id of 2d5[redacted]571 (version: -TR2840-)
00:38:57 - Client affirmed info hash = 80[redacted]08
00:38:57 - Received version in extended handshake: Transmission 2.84
00:41:10 - Completed session with client; 415 pieces were downloaded and written
14:58:51 - Client closed the connection 4 successive times without completing the handshake
14:58:52 - The client may no longer be sharing the torrent
14:58:52 - Pieces acknowledged for all sessions combined: 0-3, 7, 16-18, 20, 39, 40, 42, 43, 51, 55, 58, 62, 63, 69, 74-80, 82-84, 86-89, 91-97, 99-102, 104, 106, 107, 109, 116, 118-121, 123, 124, 126-130, 132-135, 137-150, 152, 153, 155-157, 159-162, 164-166, 168-170, 172, 174-176, 178, 179, 182, 184-193, 196, 198, 200-206, 208, 209, 211, 213, 214, 216, 219-223, 228, 234-236, 245, 248, 252, 253, 266, 277, 279, 287, 296-301, 303, 305-323, 325-327, 329-337, 339-343, 345-349, 351, 352, 354-356, 360, 361, 364-366, 369, 371-373, 375-383, 387-389, 391, 392, 394, 395, 397-400, 402-409, 411, 413-422, 424, 426-428, 430, 432-437, 440, 442-445, 451, 452, 455, 457, 459, 464, 465, 468-479, 483, 487-489, 492-496, 498, 499, 501-504, 506, 508-511, 515, 518-524, 527, 529, 531, 534, 535, 539, 541, 542, 546-549, 551-553, 555, 559-563, 566-570, 573, 575, 580, 582, 583, 587, 588, 592, 595, 597-605, 608, 609, 612, 614, 616, 618, 620, 621, 623-625, 627-629, 631-637, 640-642, 644-650, 655-661, 663, 666, 669, 672, 673, 681-683, 686, 687, 691, 692, 694, 695, 697, 703-705, 709, 712, 715, 717, 722-725, 727-730, 738, 740, 742, 744-747, 749, 750, 752-760, 762, 764-766, 768-770, 772, 776-779
[redacted] 14:58:52 - Client acknowledged that it has 448 of 780 pieces
14:58:52 - Client indicated that it has no complete files
14:58:52 - 415 of 448 pieces possessed by the client were downloaded and written to disk
14:58:52 - 415 of 780 pieces defined by the torrent were downloaded and written to disk
14:58:52 - Pieces written: 0-3, 7, 17, 18, 20, 39, 40, 42, 43, 51, 55, 62, 63, 69, 74, 76, 78-80, 82-84, 86-89, 91-97, 99-102, 104, 106, 107, 109, 116, 118-121, 123, 124, 126-130, 132-135, 137, 138, 140-144, 146-150, 152, 153, 155-157, 161, 162, 164, 165, 168-170, 172, 174, 176, 178, 179, 182, 184-193, 196, 200-206, 208, 209, 213, 214, 216, 219-223, 236, 245, 253, 266, 277, 279, 287, 296-299, 301, 303, 305-323, 325, 327, 329-337, 339-343, 345-349, 351, 352, 354-356, 360, 361, 364-366, 369, 371-373, 375-379, 381-383, 387-389, 391, 394, 395, 397-400, 402-409, 411, 413-422, 424, 426, 427, 430, 432-437, 440, 442-445, 451, 452, 455, 457, 459, 464, 465, 468-479, 483, 487, 489, 492-496, 498, 499, 501-504, 506, 508-511, 515, 518-524, 527, 529, 531, 534, 535, 539, 541, 542, 546-549, 552, 553, 555, 559-563, 566, 568-570, 573, 575, 580, 582, 583, 587, 588, 592, 595, 597-605, 608, 609, 612, 614, 616, 618, 620, 621, 623-625, 627-629, 631-637, 640-642, 644-646, 649, 650, 656-661, 663, 666, 669, 672, 673, 681-683, 686, 687, 691, 692, 694, 695, 697, 703-705, 709, 712, 717, 722-725, 727-730, 738, 740, 742, 744-747, 749, 753, 755-760, 762, 764-766, 769, 770, 772, 776-779
[redacted] 14:59:02 - All 415 written pieces have the expected SHA1 hash
14:59:02 - File 0: incomplete, 54374400 of 102215680 bytes written
14:59:02 - The download was incomplete



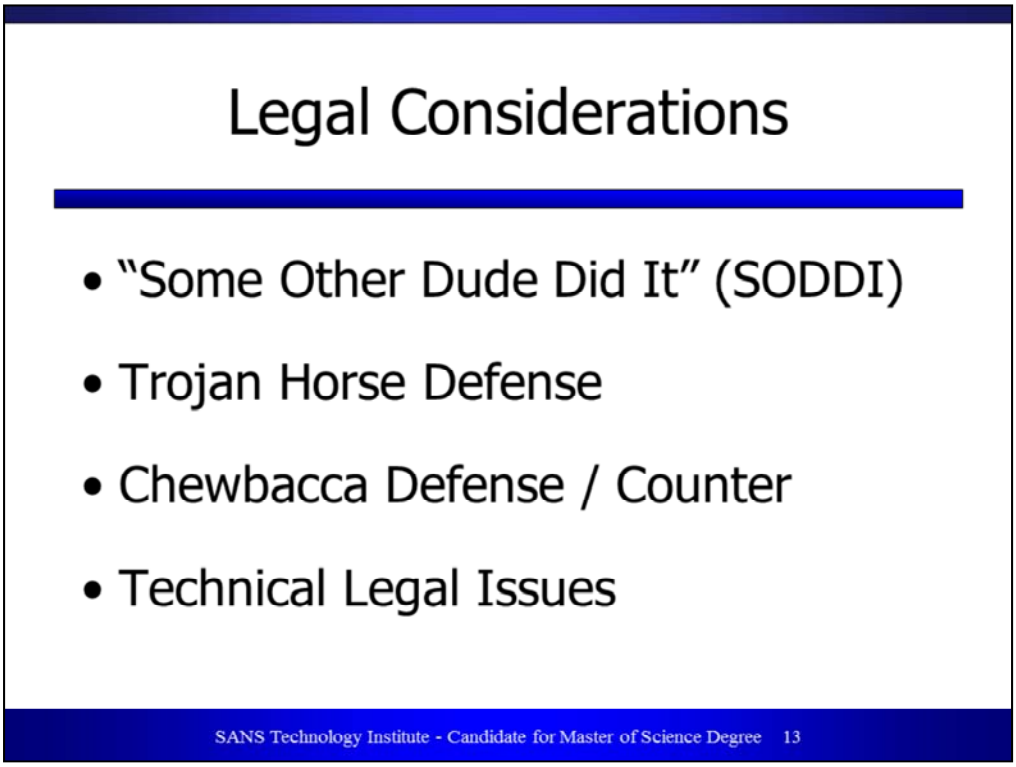
The **central database** coordinates the activities of investigators by allowing them to record the results of their investigations and to follow the progress of colleagues through a browser-based user interface.

Tagging - 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. Example tags in BitTorrent are the 20 byte peer ID and a cached reverse DNS lookup corresponding to the investigator's system.

Honeypots - 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.

In a **Sybil Attack**, a peer uses multiple identities to gain an advantage in a P2P file sharing network using a separate Peer ID with different ports and IP address combinations. 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.

Pollution 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.

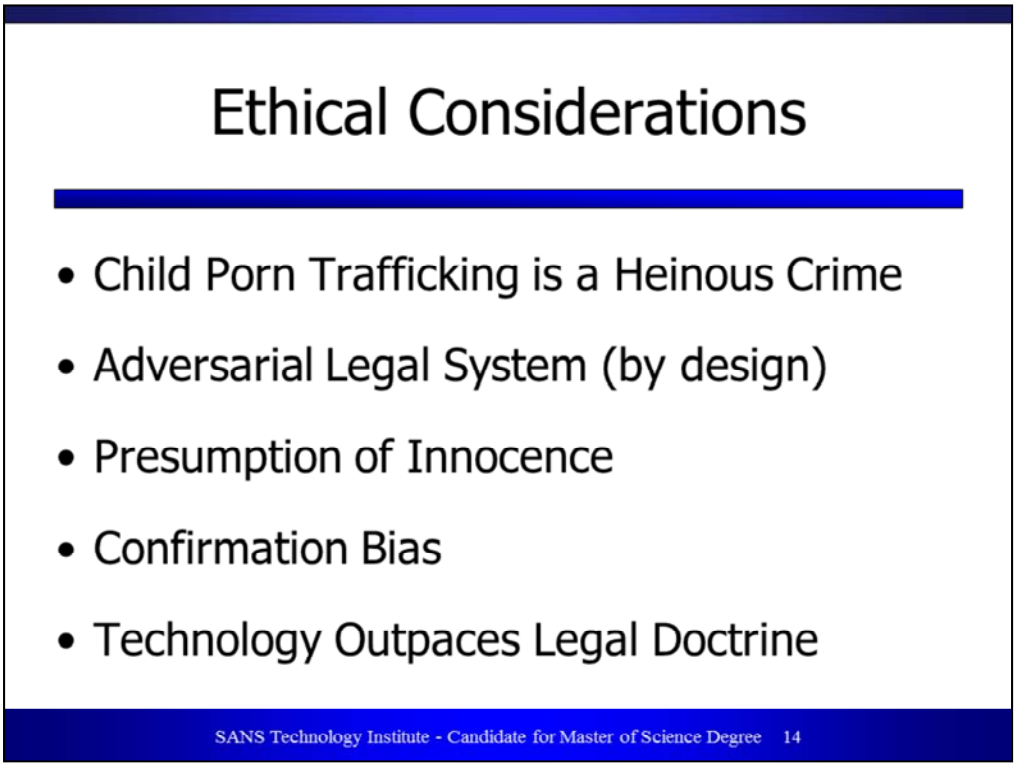


SODDI - Provides an alternate story that provides a plausible explanation for all of the evidence. Research has shown that a single, compelling alternative theory is more compelling than presenting several possibilities.

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.

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"

Legal Issues - Exactly when do digital bits become child pornography? What if a BT 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? What if the only CP found on the computer is in unallocated space?



In the US, we have an adversarial legal system, by design. This system allows the accused to confront their accusers. Another hallmark of our justice system is the presumption of innocence and that the accused must be proven guilty beyond a reasonable doubt.

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 effects on the investigator.

At various times CP has been used to frame an adversary, such as an ex-husband and a manager (as cited in my gold paper). I would argue that because of the very fact that CP is such a heinous crime, that investigators must guard against confirmation bias. Confirmation bias is the human tendency to look only for evidence that confirms a person's theory.

Legal scholars recognize that the law has not (and cannot) keep pace with the rapid change of technology. Nor can it anticipate every technical scenario where it will be applied. For this reason, the defense and not just the prosecution needs technical expertise.

This talk has just touched on the highlights of how law enforcement strives to police digital contraband in the BitTorrent ecosystem. The Gold Paper delves much deeper into the topic and is designed to be a resource for court cases involving this technology.

Child Pornography is a horrible crime, but what if your son was accused? Would you want him to have the best possible defense even if he was guilty of possession? Or what if your computer was found to have been used to traffic in CP and you knew you are innocent? Would you want an expert to examine the evidence and help your lawyer interpret it?

It is for this reason, that both the prosecution and the defense need expertise. Experts need not always testify. It is possible to keep your involvement in the case confidential as a requirement in the contract that you have with the attorney.

Lastly, I want to emphasize that Law Enforcement is performing society a very important service by innovatively trying to protect our children. These officers deserve our respect and appreciation.