Computer Forensics LLC
1880 North Congress Ave, Suite 333
Boynton Beach, Florida 33426
Main: 561.404.3074

Summary of Experience

I have more than 25 years of law enforcement investigation experience, including more than 10 years as a computer crimes detective. I have performed computer forensic examinations for the Palm Beach County Sheriff's Office and surrounding cities of Palm Beach County FL, FBI, U.S. Customs, Florida Department of Law Enforcement, Secret Service, ATF, United States Military and was a member of the South Florida ICAC taskforce for 10 years. In 2009 I was assigned to supervise the law enforcement operations for the Palm Beach County Sexual Predator Enforcement (SPE) at the located in Boca Raton FL. I have extensive knowledge of undercover online investigations including online enticement and Peer-to-Peer networks. I have been involved with hundreds of cases and have testified in State, Federal, Appellate, and Military courts as a computer expert including testifying as an expert in the functionality of Encase® at a murder trial. I have many forensic certifications including EnCE, and SCERS, additionally I was an EnCase® certified instructor for Guidance Software and have taught many forensic analysts around the country. I have earned many awards including Detective of the Month, U.S. Customs Service Unit Commendation Citation Award for computer forensic work, and have twice earned the Outstanding Law Enforcement Officer of the Year citation awarded by the United States Justice Department.

Computer Expert Witness Experience

During my tenure as a law enforcement officer, I have been called to testify as an expert on numerous occasions in the field of computer forensics in Federal Courts in FL, CA, NJ, PA and NY, Appellate Courts, State Courts, and Military courts. The following is a list of some of the cases I have testified.

Malibu Media, LLC v. JOHN DOES 1, 6, 13, 14, and 16, U.S. District Court Eastern District of Pennsylvania, Civil Action No. 2012-2078 Consolidated from Cases: 2:12-cv-02078-MMB, 2:12-cv-02078-MMB, 5:12-cv-02088-MMB – June 10, 2013

Testimony: Expert testimony of my findings of the computers used by defendant Doe 16. Matters relating to the software used by IPP International, Germany to monitor and identify copyright infringers.

United States Court of Appeals, Eleventh Circuit. No. 02-16809
United States of America, Plaintiff-Appellee, v. Samuel Alan MORTON, Defendant-Appellant. - April 01, 2004

Testimony: "The government next called Patrick Paige, a detective with the Palm Beach County Sheriff's Office. Paige testified that he created a forensics report regarding the material on Morton's computer hard drive. Included in the report were downloaded movies that contained teen sex and a minor female and adult male engaged in sexual conduct. Paige also testified that he found approximately 30 images of minors. On re-direct Paige testified that Morton had approximately 50-100 images in his AOL account."

United States v. Kenneth WILK, U.S. District Court Southern District of Florida, Broward, Case No. 0:04-cr-60216-JIC – 2007. Capital Punishment Trail for Murder
Court: Testimony surrounding the intricate workings of Guidance's software EnCase®. EnCase is one of the top forensics software utilized by forensics analysts throughout the world.

United States Court of Appeals, Ninth Circuit. No. 07-10288.
United States of America, Plaintiff-Appellee, v. Walter M. SCHALES, Defendant-Appellant. - Argued April 15, 2008. - October 20, 2008

Testimony: "Detective Paige of the Palm Beach County Sheriff's Office also testified that he recognized images on the CD-ROM depicting a child and an adult male that he arrested. The minor female depicted was five years old at the time of the photograph."

Work Experience

Computer Forensics LLC **(2012 - Present)**

I'm currently a managing partner of this newly formed computer forensic company. The company is committed to providing top quality service and knowledge in the E-Discovery, Computer Forensics fields.

Guidance Software (Creators of EnCase® Software) **9 Years (2003 - 2012)**

During the years listed was employed as an Instructor with Guidance Software. Guidance Software is the world leader in providing computer and enterprise investigation solutions. Founded in 1997 and headquartered in Pasadena, CA, Guidance Software Inc., has offices and training facilities in California, Virginia, Texas and the United Kingdom. My duties as Instructor were to instruct students in the use of computer forensic software EnCase® made by Guidance Software. I also instruct students in other aspects of computer forensics like identifying and collecting computer evidence, how computers work, storage of electronic data and how files are deleted to name a few. Students who have attended classes I've taught include all branches of the military, local, state and federal officers. I have also assisted in the collection of data in the field for the Professional Division of Guidance Software who was contracted by the Department of Justice in the Sprint/Nextel merger in 2005.

Palm Beach County Sheriff's Office, Florida **21+ Years Employed (Ex: 1989 - 2011)**

Detective Computer Crimes Unit (2000 - 2011)

2000 to present, I've been assigned to the Computer Crimes Unit. During my current assignment to the Computer Crimes Unit I've investigated numerous Internet and computer related crimes. I've conducted many undercover online investigations resulting in the arrests of individuals around the United States. I have been involved in numerous search warrants involving online and child pornography investigations. I conduct computer forensic examinations for the Palm Beach County Sheriff's Office as well as local Law Enforcement. I've also done computer forensic examinations for the Broward County Sheriff's Office, FBI, U.S. Customs, FDLE, Secret Service, ATF and local cities. I have been a member of the South Florida ICAC (Internet Crimes Against Children) taskforce since January 2001. As the Senior Computer Forensic Examiner for the Sheriff's Office I was assigned to train new computer forensic examiners assigned to the unit. I served as point of contact for 2 known series of child pornography maintained by NCMEC (National Center for Missing and Exploited Children).

In 2009 I was assigned to supervise the law enforcement operations for the Palm Beach County Sexual Predator Enforcement (SPE) located in Boca Raton FL with offices provided by the TLO Corp. The TLO facility housed the computer servers used by law enforcement around the word to conduct P2P (Peer to peer) investigations. My assignments were as follows:

- Supervise the Detectives assigned to the unit which was consisted of 6 Online Investigators and 2 Computer Forensic Examiners.
- Conduct computer forensic analysis on computers seized by the unit and testify to the findings.
- Coordinate and supervise the execution of search warrants developed by Detectives assigned to the unit. Detectives assigned to the unit conducted undercover Online investigations and peer to peer investigation via commonly used file sharing programs like LimeWire, GigaTribe, eMule to name a few.
- Worked with TLO software engineers on developing and enhancing software tools used by law enforcement officers.
- Prepared weekly reports of statistics and arrests made by the unit which were distributed the local Chiefs of Police.
- Order and maintain computer forensic equipment, computers and software.
- Responsible for maintaining and tracking of all computer evidence seized for examination.

Detective Fraud Unit (1999)

This unit conducts investigations of criminal conduct in violation of Florida Laws concerning property crimes, fraud, forgery, and computer crimes. While I was assigned to this unit I was tasked with investigating cases connected with the Internet.

Agent Organized Crime Unit (1997 - 1999)

I was assigned to the Tactical Unit of the Palm Beach Sheriff's Office for two (2) years. During my assignment, I assisted in long term investigations, surveillances, dignitary protection and was assigned to aid the FBI, DEA, ATF and local law enforcement in investigations. I was also assigned to aid the Secret Service in the protection of heads of state, Vice President and President of the United States when they entered Palm Beach County FL.

Road Patrol Officer (1989 - 1997)

While assigned to the Road Patrol Division of the Palm Beach County Sheriff's Office, I developed a practical working knowledge of conducting investigations, evidence handling, and search and seizure laws. I also served as a FTO (Field Training Officer) for 3 years and was responsible for training over 35 new deputies hired by the Sheriff's Office.

ADVANCED LAW ENFORCEMENT & COMPUTER FORENSICS TRAINING

1. Seized Computer Evidence Recovery Specialist (SCERS) Federal Law Enforcement training Center in Glynco, GA 80HRS (2/2001)
2. Investigations of Computer Crimes (The International Association of Chiefs of Police) 40HRS
3. EnCase® Intermediate Analysis & Reporting course (Guidance Software Inc.) 32HRS
4. EnCase® Expert Series Internet & E-mail Examination course (Guidance Software Inc.) 32HRS
5. Conducting Online ICAC Investigations (Law Enforcement Against Child Harm Taskforce) 40HRS
6. Investigating Computer Use of the Internet by Child Sex Offenders (Institute of Child Advocacy)
7. Advanced Sex Crimes Investigations course (Palm Beach Community College) 40HRS
8. Organized Crimes Investigations course (Palm Beach Community College) 40HRS
9. Field Training Officer course (Palm Beach Community College) 40HRS
10. Advance Narcotics Identification (Palm Beach Community College) 40HRS
11. Dignitary Protection Operations (Tactical Response Training) 32HRS
12. Forensic Computer Examiner Training Program (International Association of Computer Investigation Specialists - IACIS) 80HRS (5/2004)
13. 17th Annual Crimes Against Children Conference (Dallas, TX) 20HRS August 15-18, 2005
(Conference courses attended: Forensics on Portable Devices, AOL & Yahoo investigations, Email Tracing and Techniques for Investigating Wireless Devices.)
14. 18th Annual Crimes Against Children Conference (Dallas, TX) 20HRS August 21-24, 2006
(Conference courses attended: Email and IP Tracing, Windows XP Forensic Gems, Digital Imaging Forensics and Investigating Wireless Devices.)
15. CEIC 2012 (Computer and Enterprise Investigations Conference) 4 days (Summerlin, Nevada) May 21-24 2012
(Conference courses attended: EnCase® version 7 training updates, Using cloud computing in forensics and electronic discovery, Embedded EnScripts®, Forensic tracking of USB devices, TD2, TD3 and the future of the forensic duplicator, exFat forensics and revealing Windows® 7 artifacts.)

AWARDS/CITATIONS

Delray Beach Police Department

3 – Patrol Division Commendations.
1987 – Rookie Officer of the year.
1988 – Police officer of the month for March and August.

Palm Beach County Sheriff's Office Florida

1991 – Deputy of the year awarded by the 100 Men's Club of Boca Raton & Rotary Club.
1997 – Deputy of the Month for June.
2001 – Detective of the Month for October.
2002 – Outstanding Law Enforcement Officer of the Year awarded by the United States Justice Department for work in the U.S. v Jerrold Levy case. News Articles
2003 – U.S. Customs Service Unit Commendation Citation Award for computer forensic work in Operation Hamlet. Operation Hamlet was one of the largest rings in U.S. Customs history of individuals who were molesting their own children, and transmitting the images and video via the Internet. News Articles 2005 – Detective of Month for December.
2007 – Outstanding Law Enforcement Officer of the Year awarded by the United States Justice Department for work in the U.S. v Jimmy Oliver case. Press Release

2008 – Letter of Commendation issued by the FBI for outstanding computer forensic work in the U.S. v Frank Grasso case. News Article

CERTIFICATIONS

EnCE – EnCase® Certified Examiner
Member of IACIS – International Association of Computer Investigative Specialists
CEECS – Certified Electronic Evidence Collection Specialist – IACIS
SCERS – Seized Computer Evidence Recovery Specialist – FLETC (Federal Law Enforcement Training Center in GA)
CFCE – Certified Forensic Computer Examiner – IACIS – CFCE from 2005 to 2008

COURSES TAUGHT FOR GUIDANCE SOFTWARE

1) Intermediate Analysis & Reporting – Sterling, VA December 2nd – 5th 2003 (32 hrs)
2) Introductory Computer Forensics – Sterling, VA August 12th – 15th 2003 (32 hrs)
3) Introductory Computer Forensics – Sterling, VA September 16th – 19th 2003 (32 hrs)
4) Incident Response, Forensic Analysis & Discovery – Sterling, VA September 29th – October 3rd 2003 (40 hrs)
5) Introductory Computer Forensics – Sterling, VA January 6th – 9th 2004 (32 hrs)
6) Introductory Computer Forensics – Sterling, VA August 10th – 13th 2004 (32 hrs)
7) Introductory Computer Forensics – Sterling, VA June 28th – July 1st 2005 (32 hrs)
8) Intermediate Analysis & Reporting (Special Class for U.S. Military) – Sterling, VA October 16th – 20th 2006 (40 hrs)
9) EnCase® Computer Forensics II – Sterling, VA January 29th – February 4th 2007 (32 hrs)
10) EnCase® Computer Forensics I – Sterling, VA April 23rd – April 29th 2007 (32 hrs)
11) EnCase® Computer Forensics I – Sterling, VA September 11th – September 14th 2007 (32 hrs)

COURES TAUGHT FOR PRIVATE SECTOR

1) Taught a specialized class on basic/intermediate computer forensic for Document Technologies, Inc. (DTI) in Atlanta, GA January 1st – 5th 2007 (40 Hrs.). The course covered topics relating to the seizure, handling and examination of digital evidence and the use of forensic software EnCase®, FTK and other various computer forensic examination software.

Testing Summary

The purpose of this report is to determine if the software being utilized by IPP Limited is able to accurately identify the IP address of a peer in a BitTorrent swarm. By way of, back ground the software named "International IPTracker" (IPT) owned and used by IPP Limited is used to identify individuals who are illegally downloading and trading and/or sharing copyrighted movies, images and software. For the purpose of this report we will be addressing the BitTorrent file distribution system. However this technology and similar investigative methods are being used by law enforcement officials when tracking individuals who transmit contraband files such as child pornography via the internet. I was employed in law enforcement for over 20 years and worked over 10 years in the computer crimes unit as a Detective. As a Computer Crimes Detective I was regularly involved in the investigation of P2P (peer 2 peer) networks and supervised the specialized unit that conducted those investigations. I was involved in the planning and execution of numerous search warrants involving P2P cases.

In this report, I will discuss the "real life" scenario where I put IPP's software and searching skills to the test in order to determine if the software works and if they were able to ascertain my location, identity and the "test" files I was sharing using BitTorrent. In order to understand the software and how or if it works, one must have a basic understanding on how data travels over the internet. Data travels across the internet in packets, or datagrams. The most common is the TCP/IP (Transmission Control Protocol/Internet Protocol) standard. Each packet is wrapped with a header and footer. The information contained in the wrapper tells computers what kind of data is in the packet, where the data came from, how it fits together with other data, and the data's final destination. When data is sent through the internet it is broken up into packets that travel across the network. Different packets from the same data do not have to follow the same path. Packets will travel from one machine to another until they reach their destination. As the packets arrive, the computer receiving the data assembles the packets like a puzzle, thus recreating the data. These data packets can be intercepted and their contents analyzed using various data packet analyzing software such as an open-source program called Wireshark. Wireshark software is designed to help understand the structure of different networking protocols. The program also allows you to capture data live from an active network connection. Later in this report we will discuss Wireshark and how it was utilized in the test.

Cryptographic Hash Function (SHA1, MD5 etc.) as defined by http://en.wikipedia.org

A cryptographic hash function is a hash function; that is, an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded are often called the "message," and the hash value is sometimes called the message digest or simply digest. Cryptographic hash functions were created by the United States National Security Agency for the purpose of acting as a unique finger print.

The ideal cryptographic hash function has four main properties:

- it is easy to compute the hash value for any given message
- it is infeasible to generate a message that has a given hash
- it is infeasible to modify a message without changing the hash
- it is infeasible to find two different messages with the same hash.

The main reason we need to understand this is because every network uses different hash algorithms for the purpose of ensuring the file requested is the file being downloaded as well as other data integrity uses.

We also need to have a basic understanding of IP (Internet Protocol) addresses. An IP address is a numerical value assigned to a computer or device that transmits and receives data via the internet. When a computer user accesses the internet they are assigned a unique IP address by their ISP (internet service provider). An IP address serves two principal functions, host or network interface identification and location addressing. Its role has been characterized as follows: A name indicates what we seek. An address indicates where it is. A route indicates how to get there.

Assessment

For the purpose of this test, I utilized 4 commonly used BitTorrent clients; (i.e., software applications) readily available on the internet. The software and the location on the internet I used for this test are listed below.

1. uTorrent install version 2.2 (Build 24683) located at http://www.utorrent.com
2. uTorrent install version 3.3 (Build 29126) located at http://www.utorrent.com
3. BitComet Install Version 1.34 located at http://www.BitComet.com
4. BitTorrent Install version 7.2 (Build 24441)

I Utilized GoDaddy's dedicated server service located at www.godaddy.com/hosting/dedicatedservers.aspx to setup 4 dedicated servers for this test. All four servers were setup identically and all were running Windows Server 2008R2 operating systems. The 4 BitTorrent software applications were downloaded and installed on each of the servers, one program to each server. Also installed on each of the test servers to monitor internet traffic to and from the servers was Wireshark Version 1.6.13 (SVN Rev 47347 from /trunk-1.6).

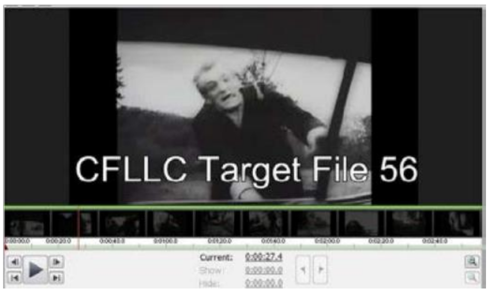
I then needed 4 "test" movies for this examination. I located 4 movies that were not copyrighted at http://archive.org/movies. Once the 4 movies were chosen and downloaded the original titles were renamed for testing purposes. Below are the 4 movies with their original titles along with their renamed titles.

Test Movie 1 - Night of the living dead was renamed to "EXOCannibalismFootage2012"
Test Movie 2 - MoviePowderPresentsPlan9FromOuterSpace was renamed to "alienhumanprobing"
Test Movie 3 - DiaryofaNudist_512kb was renamed to "2012nudestcamp"
Test Movie 4 - sex_madness_512kb was renamed to "Classichowtosex"

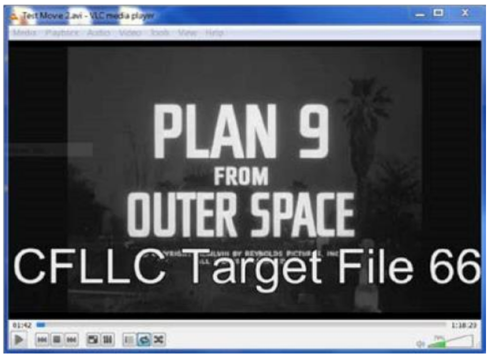
Using video editing software I encoded unique subtitles to each of the movies. The purpose of this is procedure is to insure that when the file is located and download by IPP Limited it can be readily identified as the file/movies I personally encoded. Below is a list of the test movies and the subtitle assigned to that file along with screen captures.

Test Movies & Encoded Titles

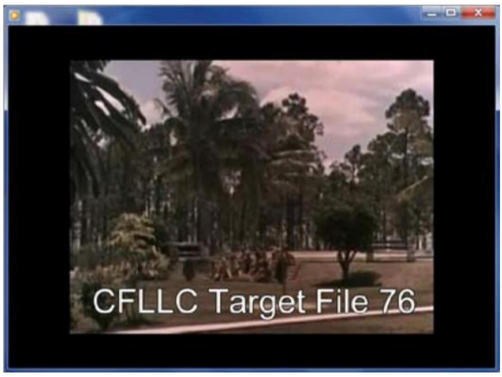
Test Movie 1 was encoded with "CFLLC Target File 56"



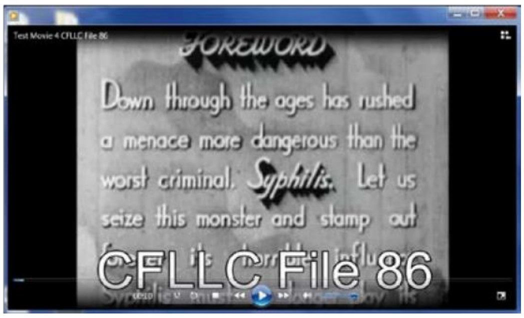
Test Movie 2 was encoded with "CFLLC Target File 66"


Test Movie 2.avi - VLC media player
Media Playback Audio Video Tools View Help
PLAN 9
FROM
OUTER SPACE
CFLLC Target File 66
01:42
1:18:23

Test Movie 3 was encoded with "CFLLC Target File 76"



Test Movie 4 was encoded with "CFLLC File 86"


Test Movie 4 CFLLC File 86
FOREWORD
Down through the ages has rushed
a menace more dangerous than the
worst criminal. Syphilis. Let us
seize this monster and stamp out
CFLLC File 86

Once the movies were encoded and the proper file sizes were obtained they were uploaded to each of the test servers on 2013 -03-09. I used one movie file for each of the servers used in the test. I Used AccessData's® software FTK® Imager version 2.9.0.138 5 100406 to create a digital finger print of my uploaded encoded movie files. Please note the part of the original IP address to the t est servers has been removed for confidentiality, but can be made available upon request.

Test Server 1(*.*.58.158) files name “EXOCannibalismFootage2012.wmv”

```
Information for C:\Upload\*.*.58.158-EXOCannibalismFootage2012.ad1:
[Custom Content Sources]
Torrent:C:\Torrent|*(Wildcard,Consider Case,Include Subdirectories)
[Computed Hashes]
MD5 checksum:   063d858ee9d5bda117bac19532313e73
SHA1 checksum:   0032cfa32eef081466e1b3945a49b38ecfda10ef
Image information:
Acquisition started:  Sat Mar 09 22:08:22 2013
Acquisition finished:  Sat Mar 09 22:09:26 2013 Segment list:
C:\Upload\*.*.58.158-EXOCannibalismFootage2012.ad1 Image Verification Results:
Verification started:  Sat Mar 09 22:09:26 2013
Verification finished: Sat Mar 09 22:09:32 2013
MD5 checksum:   063d858ee9d5bda117bac19532313e73 : verified
SHA1 checksum:   0032cfa32eef081466e1b3945a49b38ecfda10ef : verified
```

Test Server 2(*.*.184.230) file Name “alienhumanprobing.avi”

```
Information for C:\Upload\*.*.184.230-alienhumanprobing.ad1:
[Custom Content Sources]
 Torrent:C:\Torrent|*(Wildcard,Consider Case,Include Subdirectories)
[Computed Hashes]
MD5 checksum:   ffc7b83018808d63d57ca7a4fd7f3a77
SHA1 checksum:   eff97e8bc2c41bd00cc606969863e3b4023e3bad Image information:
Acquisition started:  Sat Mar 09 22:12:17 2013
Acquisition finished:  Sat Mar 09 22:15:16 2013
Segment list:
C:\Upload\*.*.184.230-alienhumanprobing.ad1 Image Verification Results:
Verification started:  Sat Mar 09 22:15:16 2013
Verification finished: Sat Mar 09 22:15:35 2013
MD5 checksum:   ffc7b83018808d63d57ca7a4fd7f3a77 : verified
SHA1 checksum:   eff97e8bc2c41bd00cc606969863e3b4023e3bad : verified
```

Test Server 3(*.*.176.61) file name “2012nudestcamp.mpg”

```
Information for C:\Upload\*.*.176.61-2012nudestcamp.ad1:
[Custom Content Sources]
Torrent:C:\Torrent|*(Wildcard,Consider Case,Include Subdirectories)
[Computed Hashes]
MD5 checksum:   7ec7d3718f92e1148aa1ebb9e666f075
SHA1 checksum:   6edca1382919d5eeb2014c316b023d3d541cc90e
Image information:
Acquisition started:  Sat Mar 09 22:31:23 2013
Acquisition finished:  Sat Mar 09 22:37:00 2013 Segment list:
C:\Upload\*.*.176.61-2012nudestcamp.ad1 Image Verification Results:
Verification started:  Sat Mar 09 22:37:00 2013
Verification finished: Sat Mar 09 22:37:16 2013
MD5 checksum:   7ec7d3718f92e1148aa1ebb9e666f075 : verified
SHA1 checksum:   6edca1382919d5eeb2014c316b023d3d541cc90e : verified
```

Test Server 4(*.*.188.154) file name "Classichowtosex.mov"

```
Information for C:\Upload\*.*.188.154-Classichowtosex.ad1:
[Custom Content Sources]
Torrent:C:\Torrent|*(Wildcard,Consider Case,Include Subdirectories)
[Computed Hashes]
MD5 checksum:   d2546b703d4f0451096bc50c01ec2390
SHA1 checksum:   8ed7013a04fb323db2280207273486b227d05d07 Image information:
Acquisition started:   Sat Mar 09 22:47:00 2013
Acquisition finished:  Sat Mar 09 22:49:16 2013 Segment list:
C:\Upload\*.*.188.154-Classichowtosex.ad1 Image Verification Results:
Verification started:  Sat Mar 09 22:49:16 2013
Verification finished: Sat Mar 09 22:49:28 2013
MD5 checksum:   d2546b703d4f0451096bc50c01ec2390 : verified
SHA1 checksum:   8ed7013a04fb323db2280207273486b227d05d07 : verified
```

Once each of the servers had one of the test movies uploaded to them I began the process of creating torrent files using the BitTorrent clients found on page 2. In order for computers to know how to put all the pieces back in the right order and use the content, BitTorrent clients requires a special reference file called a Torrent. The torrent is what you download from a website and load into µTo rrent or other BitTorrent software you are using at the time. All the computers and seeds (computers containing the entire file be ing shared), involved in the distribution of any given file have the matching torrent loaded into their client/software. In order to shar e your own content over the BitTorrent network you need to create a torrent for this content. Once each of the torrent files is created they were given the following names and a process known as seeding was started.

1. EXOCannibalismFootage2012.wmv.torrent
2. alienhumanprobing.avi.torrent
3. 2012nudestcamp.mpg.torrent
4. Classichowtosex.mov.torrent

The torrent files were created with the following BitTorrent trackers:

Trackers assigned to torrent files
udp://tracker.openbittorrent.com:80/announce udp://tracker.publicbt.com:80/announce
udp://tracker.ccc.de:80/announce udp://tracker.istole.it:6969
http://cpleft.com:2710/announce http://exodus.desync.com:6969/announce

The torrent tracker "keeps track" of which computers are currently sharing in the torrent and pass that information to the client. It may be noted that this is the only centralized part of a torrent.

On 2013-02-25 all 4 test servers were up and running with the BitTorrent and Wireshark software operational for the testing to begin. IPP Limited was only given the names of the 4 test movies listed in this report. No IP address or any other information was provided to IPP Limited. Within a 24 hour period IPP Limited had successfully downloaded and visually identified all four test movies. IPP Limited supplied log files that identified the 4 static IP addresses of all 4 test servers. I later logged onto each of the 4 test s ervers and reviewed the Wireshark "pcap" log files created on 2013-02-25. As discussed above Wireshark software is an OSS (open-source software). OSS is software that has made its software and source code open to the public. Wireshark is widely and commonly used by computer forensic examiners as well as law enforcement. I have used Wireshark software while in law enforcement to examine network traffic while investigating P2P cases. Wireshark software stores the collected network data in a log file commonly referred to as a "pcap" file. "Pcap" log files are also known as packet capture files. The pcap log files contain information on network traffic in and out of a client or host. The pcap log file contains but is not limited to times, dates, IP addresses and transmission protocol. The following activit y was noted using Wireshark software:

Test Server 1 recorded IPP Limited activity and IPT software was active on Test Server 1 from 2/25/2013 6:57 PM to 2/26/2013 1:17 PM.

Test Server 2 recorded IPP Limited activity and IPT software was active on Test Server 1 from 2/25/2013 6:52 PM to 2/26/2013 1:15 PM.

Test Server 3 recorded IPP Limited activity and IPT software was active on Test Server 1 from 2/25/2013 7:06 PM to 2/26/2013 1:15 PM

Test Server 4 recorded IPP Limited activity and IPT software was active on Test Server 1 from 2/25/2013 7:07 PM to 2/26/2013 2:21 PM.

IPP Limited provided Wireshark log information which corresponds to the above noted activity. IPP limit would not have known what Wireshark log information would correspond to the above note activity unless it had captured this information independently.

Based on the testing performed, IPP Limited successfully identified the test files produced by the name provided, downloaded and confirmed by message digest the files, and was able to accurately identify an IP address used to distribute data via the BitTorrent protocol through a forensically sound and verifiable method.

I **Patrick Paige** Declare That:

1. I understand that my duty in providing written reports and giving evidence is to help the Court, and that this duty overrides any obligation to the party by whom I am engaged or the person who has paid or is liable to pay me. I confirm that I have complied and will continue to comply with my duty.

2. I confirm that I have not entered into any arrangement where the amount or payment of my fees is in any way dependent on the outcome of the case.

3. I know of no conflict of interest of any kind, other than any which I have disclosed in my report.

4. I do not consider that any interest which I have disclosed affects my suitability as an expert witness on any issues on which I have given evidence.

5. I will advise the party by whom I am instructed if, between the date of my report and the trial, there is any change in circumstances which affect my answers to points 3 and 4 above.

6. I have shown the sources of all information I have used.

7. I have exercised reasonable care and skill in order to be accurate and complete in preparing this report.

8. I have endeavored to include in my report those matters, of which I have knowledge or of which I have been made aware, that might adversely affect the validity of my opinion. I have clearly stated any qualifications to my opinion.

9. I have not, without forming an independent view, included or excluded anything which has been suggested to me by others, including my instructing lawyers.

10. I will notify those instructing me immediately and confirm in writing if, for any reason, my existing report requires any correction or qualification

11. I understand that;

    11.1 My report will form the evidence to be given under oath or affirmation;

    11.2 Questions may be put to me in writing for the purposes of clarifying my report and that my answers shall be treated as part of my report and covered by my statement of truth;

11.3 The court may at any stage direct a discussion to take place between experts for the purpose of identifying and discussing the expert issues in the proceedings, where possible reaching an agreed opinion on those issues and identifying what action, if any, may be taken to resolve any of the outstanding issues between the parties;

11.4 The court may direct that following a discussion between the experts that a statement should be prepared showing those issues which are agreed, and those issues which are not agreed, together with a summary of the reasons for disagreeing;

11.5 I may be required to attend court to be cross-examined on my report by a cross-examiner assisted by an expert;

11.6 I am likely to be the subject of public adverse criticism by the judge if the Court concludes that I have not taken reasonable care in trying to meet the standards set out above.

12. I have read Part 35 of the Civil Procedure Rules and the accompanying practice direction and I have complied with their requirements.

13. I have read the "Protocol for Instruction of Experts to give Evidence in Civil Claims" and confirm that my report has been prepared in accordance with its requirements. I have acted in accordance with the Code of Practice or Experts

STATEMENT OF TRUTH

I confirm that I have made clear which facts and maters referred to in this report are within my own knowledge and which are not. Those that are within my own knowledge I confirm o be true. The opinions I have expressed represent my true and complete professional opinions on the maters to which they refer.

Respectfully Submitted,

Patrick Paige

Patrick Paige EnCE SCERS
Managing Partner
Computer Forensics LLC

Patrick Paige
Digitally signed by Patrick Paige
DN: cn=Patrick Paige, o=Computer Forensics LLC, ou, email=patrick@patrickpaige.com, c=US
Date: 2013.07.16 15:37:04 -04'00'