Case Analysis
Kevin Rex West

- **NC State Bureau of Investigation Computer Crimes Unit / ICAC Commander - Special Agent in Charge (Retired)**
- **Detective Cary Police Department**

Analysis: Cowlitz County P2P Case
Michael W. Hart
CPS (Child Protections System Data - Child Pornography Case
Re: IP Address: 24.20.137.22 and 98.232.158.142

BACKGROUND ON PEER TO PEER INVESTIGATIONS

Detective West knows from training and experience that child pornography comes from many sources. Computers have revolutionized the way in which those sources and users interact. Computers have also revolutionized the way in which collectors and users of child pornography can keep their collections. The development of computers and the Internet has greatly changed and added to the way in which child pornography is disseminated, collected, and viewed.

Computers have facilitated the ability of child pornography collectors and traders to keep their collections hidden. Photographs and videos that were previously stored in boxes are now traded and collected as digital images that can be stored and maintained on electronic media, such as a digital storage device called a "Micro Secure Digital Card", that is smaller than a postage stamp. Computers and the Internet now aid and serve in the production of child pornography, the distribution of child pornography, the viewing of child pornography, the storage of child pornography and communication between child pornography traders.

One of the fast growing areas that facilitates and is used by child pornography collectors and traders is the P2P networks like FastTrack, ARES, EDonkey, Bittorrent and the Gnutella Networks. The Peer-to-peer (P2P) Networks have become ideal for traders to openly exchange collections and share those collections. The P2P network has provided a way for traders to have what they feel is an open and anonymous distribution and trading network. These networks enables trading on a world-wide basis and with upload and download speeds as if the trader was next door.

Detective West has personally worked undercover P2P investigations and worked on the beginning phases (starting in December of 2003) of the current largest national P2P undercover initiative targeting those sharing files on the Gnutella Network. Detective West has served on the National ICAC Task Force Technology Committee with former Special Agent Flint Waters, of the Wyoming ICAC Task Force. Detective West has discussed with Flint Waters P2P investigations and the work being conducted across the country into investigations of P2P child pornography file sharing. Flint Waters is the original programmer/developer of the current Peer to Peer undercover initiative nationally. Those officers doing undercover ultimately use either software and/or techniques developed by him or something spawned off a development conceptualized by him. Detective West has also spent countless hours reading, studying and

trying the various eDonkey and Gnutella Client software programs in an effort to learn research and understand the P2P system of file sharing and am currently an Instructor in the P2P Undercover program nationwide.

Detective West is currently working with and continues to work with the National Undercover training initiatives for P2P to ensure a cohesive and proper use of the protocols and programs written for the National Undercover operation for the investigation of child pornography shared on the P2P Networks. Detective West knows from training, research, personal experience in undercover investigations involving P2P networks, and by personal participation in the undercover program the following information.

Detective West personally researched the Gnutella Network, eDonkey Network and other P2P networks used by those individuals to distribute and share child pornography on the Internet. Investigators nationwide use software that interfaces with information publicly available on the file sharing (Gnutella) network as well as other “open source” information available on the Internet. Using that software Detective West has conducted and continues to conduct investigations on the P2P Networks. Detective West has received training and since has provided training in numerous venues to the National ICAC Investigators, to State ICAC Investigators and to Foreign Officers out of country in the investigation of Child Pornography trading on the P2P Networks.

Detective West knows that computers on the eDonkey and Gnutella networks have software installed on them that facilitate the trading of images. The software, when installed, allows the user to search for pictures, movies and other digital files by entering text as search terms. Some names of the software used include, but are not limited to, ARES, eMule, eDonkey, BearShare, Frostwire, LimeWire, Shareaza, Morpheus, Gnucleus, Phex and other software clients. Those are software programs that interface with the Gnutella Network, the ARES Network and the eDonkey network.

HOW SEARCHES ON THE GNUTELLA P2P NETWORK WORKS

A user obtains files by conducting keyword searches of the P2P network. When a user initially logs onto the P2P network, information about the files that the user is sharing is transmitted to the network Ultrapeers that the user connects to. The P2P software (through search terms) then matches files in these file lists to keyword search requests from other users. Detective West knows that P2P users can find images and movies of child pornography by using search terms. Some examples of search terms that locate files containing child pornography are "PTHC" (which stands for "Pre-Teen Hard Core"), "babyj", “pedo”, “kiddie”, “underage”, and various terms relating to ages such as “10yo”, etc. These search terms typically results in the user being presented with a list of files that include movie and image files that when downloaded and viewed contain child pornography illegal in all states.

Detective West knows that when a user sends search terms out looking for a file in the Gnutella Network that the search terms are sent to an Ultrapeer that the users is connected to. Ultrapeers are other computer users on the Gnutella Network that have an elevated status because of their connectivity that make them an indexing peer. They maintain data about what each user they are

(5) Next, during installation users must elect or choose to change certain settings or to take the recommended default settings. Defaults don't just happen on their own but happen because a user makes that selection. Alternately, the user can read the selections and make informed choices during the installation procedure. All users must at least click through "next" buttons after being presented with choices.
(6) After installation the user must learn something about the program by hit and miss experimentation or reading on-line documentation on how to actually use the program.
(7) With P2P programs, the user must make choices again on configuration the first time they run the program. Initially, in some P2P programs, the user must also select a server to connect to.
(8) The user must make some type of decision as to what search term to use. Search terms are always selected based on what the user wants to find. File results do not magically jump onto the search results page but happen because of a process of selection of a search term in the mind of the user and the user then transmits the words the users selects to search on.
(9) When search term results come back based on what peers are saying they have with the term in their file name, the user must either select individual results and start a download request or select everything in a group and start a download request. There are no P2P programs that Detective West has ever seen or experimented with that make files start downloading without a positive action and decision on the part of the user.
(10) There is no function or button or language protocol inside the P2P programs that will allow anyone to randomly send anyone else a file unasked for. The protocols and language all require a positive action on the part of a user in making a request for a file.
11) After the user starts downloads at some point the user must decide on what files they like and what files to keep and what files to discard. Use of a P2P program will fill a users hard drive in a short period of time if there are no files selected to discard.
12) In addition to discarding files users must make a selection to either keep all the files they like in the shared folder or to move them to some area for storage.
13) Many users elect to view the files they download, get their gratification and then delete the files. Users who do this have either decided to do this out of fear of being caught by their significant other or out of a simple though process they the files are out there and they can re-download them at anytime they want to get their next gratification. Some users feel guilty about their habits and discard all files and then when their need for gratification surpasses their guilt they download again.
14) At any rate each and every daily log of a file in the CPS database reflect this decision tree or process.

DOWNLOADS

A user looking to download files simply conducts a keyword search. The results of the keyword search are displayed and the user then purposefully selects file(s)which he/she wants to download. There is no accidental download process. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) hosting the file. Once a file has been downloaded, it is stored in the area previously designated by the user and will remain there usually as a shared file until moved or deleted. Most of the P2P software applications keep logs of each download event. Frequently, a computer forensic examiner, using

Kevin Rex West
4016 Forty Niners Road Clayton NC 27520 919-550-4725
Consultant – Kevin West Consulting
Detective - Cary Police Department
120 Wilkinson Ave, Cary, NC 27513 919-801-3257 (cell)

EMPLOYMENT

Kevin West Consulting **(January 2009 – Present)**

Conduct Training and Consultation Nation wide and world wide in Internet Crimes Against Children Investigation and On-Line Undercover issues. Training has been for Wake Technical Community College, Nash Community College, Randolph Community College, TLO Inc., Australian National Police, Queensland Australia Police, Brazilian National Police, Canadian Police College, Southern Virginia ICAC, Northern Virginia ICAC, New Jersey ICAC, Georgia ICAC, Los Angeles CA ICAC, South Florida ICAC, Idaho ICAC, Washington ICAC, Montana ICAC, NC ICAC, Maryland ICAC, Hawaii ICAC, Illinois ICAC, and many, many others.

Detective Cary Police Department (Reserve Officer) **Years Employed (July 2009 – Present)**
CARY POLICE DEPARTMENT CARY, NORTH CAROLINA
COMPUTER CRIMES INVESTIGATIONS Unit

Work as a Sworn-Detective on a part time basis in Criminal Investigations (Computer Crime Unit) working undercover on-line child exploitation cases: including Peer-To-Peer Investigations, Chat Investigations, and Sexual Exploitation cases. (20 hours a week average).

Special Agent In Charge **Years Employed (Nov 2003 – January 2009)**
NORTH CAROLINA STATE BUREAU OF INVESTIGATION RALEIGH, NORTH CAROLINA
COMPUTER CRIMES INVESTIGATIONS Unit

Supervised a staff of fifteen Special Agents of the North Carolina State Bureau of Investigation assigned to conduct computer and Internet investigations and forensic examinations in the field. These agents are trained in forensic accounting and computer forensics and investigation. Maintained oversight and case management of all cases investigated statewide by the N. C. State Bureau of Investigation involving computer crime and the use of the Internet in the commission of crimes. Managed, supervised, and commanded the NC ICAC (Internet Crimes Against Children) Task Force Unit, consisting at the time of over 70 officers statewide.

Special Agent In Charge **Years Employed (1998 - 2003)**
NORTH CAROLINA STATE BUREAU OF INVESTIGATION TRAINING SECTION RALEIGH, NORTH CAROLINA

Management of All SBI Training Programs, all SBI Trainees, all Personnel in SBI Training Section, and all Academies, Basic Law Enforcement Programs, In-Service, Firearms, Investigative Training, Computer Training Programs, Computer Investigations Training, Child Sex Abuse Investigations, Homicide, Arson, and other training programs. Management of 51+ employees during an academy, but it ranged down to 14 full time when an academy was not in session. Management of Agents who came to all training programs while in the training environment. Management and decisions on all training for the SBI. Coordination and management of Initiatives on Computer Crimes Training in conjunction with NC Justice Academy and Financial Crimes. Conducted computer training for the SBI including an initiative on laptops where I wrote and conducted the training on Internet connections and laptop uses when laptops were issued to all agents.

Assistant Special Agent In Charge **Years Employed (1998 - 2003)**
NORTH CAROLINA STATE BUREAU OF INVESTIGATION RALEIGH, NORTH CAROLINA
INTELLIGENCE AND TECHNICAL SERVICES SECTION, NC STATE BUREAU OF INVESTIGATION

Assistant Supervisor over Intelligence Analysts, liaison for Intelligence Section for Field Agents, Undercover Internet Investigations of Terrorist Groups, Surveillance and Tracking of Terrorist Groups, Undercover Membership in KKK, Militia, and Terrorist Groups via Internet, Liaison for Computer Investigations on the Internet, Computer Assistance in Intelligence Section, Management of Computerized Databases and Intelligence while in Intelligence Section, State INTERPOL liaison, organized, conducted, and managed as well as wrote the code for the first SBI Internet Homepage, Management of computer leads coming in through the Internet, Management of the SBI Most Wanted and Unsolved Cases programs on the Internet and via television broadcast.

Special Agent **Years Employed (1987 - 1994)**

NORTH CAROLINA STATE BUREAU OF INVESTIGATION — RALEIGH, NORTH CAROLINA
FIELD INVESTIGATIONS / CRIMINAL AGENT / DRUG AGENT

Conducted criminal investigations into alleged violations of State and Federal law, and provided assistance to local and federal law enforcement agencies as requested. Investigations included Homicide, Fraud, Child Sexual Exploitation, Embezzlement, Corruption, Computer Crimes, and Narcotics. Specialized duties as Western District Computer Crimes Investigation Agent, Specialized duties as Western District Child Sex Abuse Investigations Agent.

Detective — **Years Employed (1984 - 1987)**
GUILFORD COUNTY SHERIFF'S DEPARTMENT — GREENSBORO, NORTH CAROLINA
DETECTIVES DIVISION – NARCOTICS
Detective assigned to work Narcotics cases and Drug Interdiction cases

Deputy Sheriff — **Years Employed (1979 - 1984)**
GUILFORD COUNTY SHERIFF'S DEPARTMENT — GREENSBORO, NORTH CAROLINA
PATROL DIVISION
Criminal Patrol Division - Deputy Sheriff

EDUCATION

Bachelor of Science in Criminal Justice — **Years Attended (1977-1979)**
BRIGHAM YOUNG UNIVERSITY — PROVO, UTAH

Rick's College (Now Called BYU-Idaho Campus) — **Years Attended (1973-1974)**
REXBURG, IDAHO

Administrative Officers Management Program — **Year Attended (1996)**
NORTH CAROLINA STATE UNIVERSITY — RALEIGH, NORTH CAROLINA

FBI National Academy (197th Session) — **Year Attended (1998)**
FEDERAL BUREAU OF INVESTIGATION — QUANTICO, VIRGINIA

- Over 1,000+ hours of Computer Crime, Internet Investigation and Computer Forensics training from SEARCH, National Center for Missing & Exploited Children, FBI-Computer Crime Training, Unisys Unix Training, NCJA, EnCase, AccessData, NW3C and other agencies. First computer crimes courses 1991.
- Over 384 hours of training in the management of training and law enforcement related training issues.
- Over 235 hours of training directly related to child abuse and child sex abuse investigation, forensic child interviewing and suspect interrogation.
- Over 219 hours of training directly related to homicide and crimes scenes.
- Over 2000 additional hours of training in various law enforcement related subjects including the North Carolina State Bureau of Investigation Academy.
- Full Transcript of training while with the NC SBI available on request and need.

SKILLS

- Completed Basic Law Enforcement 1980.
- Completed N. C. State Bureau of Investigation Basic Academy 1987
- State Certified Law Enforcement Instructor.
- State Certified School Director for 6 years.
- Formerly State Certified Firearms Instructor.
- Taught in about every law enforcement topic, both Basic and Advanced and including Internet Investigations across the State.
- Attended numerous symposiums, conferences (too many to count – yearly since 2003) and seminars regarding on-line investigations involving child pornography, and Internet crimes against children.
- Awarded North Carolina Basic, Intermediate & Advanced Law Enforcement Certificates
- Served as a Commissioner for three years on North Carolina Criminal Justice Education Training and Standards Commission.
- Teach in the NC Community College System for Wake Technical Community College, Nash Technical Community College, Johnston Community College, Randolph Community College, and have taught for Guilford Technical Community College also teach for Canadian Police College-Internet Forensics Course.
- Have taught Nationally for the ICAC program at ICAC Schools and Conferences.

Published

- Google Hello Investigation and Forensics "White Paper" for the National ICAC Task Forces 2007.
- eDonkey Peer to Peer Investigations and Forensics "White Paper" for the Peer to Peer Undercover Investigators and the National ICAC Task Forces 2011.

Computer Court Testimony

- May 2007 Federal Court Middle District of North Carolina – Charles Childers. Testified in a Bond Revocation Hearing as an expert on how Yahoo Chat works. Bond was revoked for the defendant based on the fact that he had been accessing Yahoo with his cell phone in violation of his release agreement.
- May 2009 – Fort Bragg Military Court – Testified as an expert witness in Peer-to-Peer Investigation in a case against a man who had been charged based on Peer-to-Peer downloading. (Cannot recall the man's name)(Prosecutor was Captain Paul Dubbling).
- May 2007. Wayne County Superior Court – Thomas Edward Anderson. Testified as expert about P2P Investigations P2P Software and P2P usage.
- Expert Witness December 2012 Lagrange GA - Peter Mallory Case

Teaching - Computer Crimes

- Wake County Technical Community College – 2009, 2010, 2011, 2012, 2013 (Twice each semester each class)
  - Investigation of Social Networking (1 day)
  - Internet Crimes Against Children Basic Investigation (3 days)
  - Computer Crime Scene First Response Forensics Triage (2 days)
  - Undercover Online Investigations (3 days)
  - Wireless Investigations (2 days)
  - P2P Undercover Investigations (3 days)
  - Gigatribe Investigations (1 day)

- Randolph County Technical Community College –2011, 2012, 2013 (Twice each semester each class)
  - Investigation of Social Networking (1 day)
  - Internet Crimes Against Children Basic Investigation (3 days)
  - Computer Crime Scene First Response Forensics Triage (2 days)
  - Undercover Online Investigations (3 days)
  - P2P Undercover Investigations (3 days)
  - Gigatribe Investigations (1 day)

- Johnston County Technical Community College – 2009, 2010, 2011, 2012, 2013 (Twice each semester each class)
  - Investigation of Social Networking (1 day)
  - Internet Crimes Against Children Basic Investigation (2 days)
  - Computer Crime Scene First Response Forensics Triage (1 days)
  - Undercover Online Investigations (2 days)

- North Carolina State Bureau of Investigation ICAC Program (Teach each class 2-4 times per year depending on the need)
  - Internet Crimes Against Children Basic Investigation (4.5 days)
  - P2P and Gigatribe Undercover Investigations (4.5 days)

***Over the past years I have taught P2P Undercover Investigations on a regular basis in the following locations: Australia, Brazil, Florida, Georgia, Hawaii, Virginia, Maryland, New Jersey, Illinois, California, Idaho, Kansas, North Dakota, Washington, Missouri, and many other locations.

***My latest class was in Internet Online Undercover Investigation December 2014 for the NC ICAC, and Latest Peer To Peer Undercover was April 2015.

My Background

I graduated from Brigham Young University in 1979. I have been a sworn law enforcement officer in the State of North Carolina since 1979. I graduated from Basic Law Enforcement Training in 1980. I began with Guilford County Sheriff's Department as a Patrol Deputy and moved to the vice and narcotics section in 1984. I have attended numerous schools in investigation prior to leaving the Guilford County Sheriff's Office. I left Guilford County in 1987 and became a Special Agent with the North Carolina State Bureau of Investigation. 1987, I graduated from the SBI Academy. Since that time I have attended literally thousands of hours of training in a wide variety of Investigations Training including; Homicide Investigations, Arson Investigations, Crime Scene Investigations, Interrogation, Interview, Drug Investigations, Child Sex Abuse Investigations, Child Interviewing, Child Abuse Issues, Search and Seizure, Search Warrant Preparations, Computer Forensics, Internet Crimes and many other Criminal issues. I was assigned to General Criminal Investigations from 1987 to 1994 in Jackson and Swain Counties. While in that assignment I worked homicides, rapes, robberies, drug cases and numerous child sex abuse cases. During that tenure I was also assigned to handle computer related cases. I was assigned to the SBI Intelligence Section from 1994 thru 1997 and worked as an Intelligence Coordinator tracking criminal and terrorism groups in North Carolina. During this period I conducted undercover operations and research on the various criminal, militia and terrorism groups by using the evolving Internet. From 1997 to 2003 I was assigned as the Special Agent in Charge of the Training Section for the State Bureau of Investigation. In November of 2003, I was appointed as the Special Agent in Charge of a newly formed Computer Crimes Investigation Unit made up of seasoned investigators with skills and abilities in Computer Forensics and Computer Investigations and placed in charge of the Internet Crimes Against Children Task Force in NC. In January of 2009 I retired from the State with 30 Years of service. In March of 2009 I was hired by the Cary Police Department to be a Police Detective and am currently assigned to assist in the Investigation of Internet Crimes Against Children.

Specifically related to computer training I attended my first Computer Crime Investigations classes in the early 1990s. During the ensuing years I have attended numerous Internet and Computer Investigation related classes and conferences. I wrote and developed the NC State Bureau of Investigations' first On-Line Internet Web Page. I have researched the Internet and its many facets in order to teach and investigate crimes committed on the Internet. I have had training in Computer Forensics, Internet Investigations, Undercover Internet Investigations, Internet Crimes Against Children Issues, Wireless Hacking, Internet Fraud, Computer Networks and other Computer related issues. I have had training in the current and past Internet Crimes Against Children Task Force Peer-to-Peer (P2P) operations. I have served in various capacities as a trainer in the past P2P operations and have been trained and have conducted training all over the country and overseas in the current P2P operation. I have also taken the FBI P2P training called e-P2P. I have written numerous lesson plans and have taught various aspects of Internet Crimes Investigations since working in the Intelligence Section in 1994. Over the years I have taught Internet-related investigations classes all over the State for Law Enforcement Officers at community colleges, the North Carolina Justice Academy, the NC State Bureau of Investigation Academy, the Georgia Bureau of Investigation, the Virginia State Police, the Idaho State Police, the Washington State Police, the Orange County California District Attorney's Office, the Queensland Australia State Police, and Project Safe Childhood-- a US Attorney initiative. I have received computer training in Basic Data Recovery and Acquisition, computer previews using Knoppix software, Access Data Forensic Tool Kit, EnCase Forensic software, computer peer-to-peer investigations, Bit-Torrent investigations, undercover on-line operations, computer investigative utilities, and various other subjects through the National Internet Crimes Against Children (ICAC) Task Force, National White Collar Crime Center, and other training organizations.

I have served as a member of the NC Criminal Justice Education Training and Standards Commission. I have received my Basic, Intermediate and Advance Law Enforcement Certificates from both the North Carolina Criminal Justice Education Training and Standards Commission and North Carolina Sheriff's Training and Standards Commission. I am a graduate of the FBI National Academy and the North Carolina State Administrative Officers Management Program. I have served in the past on the National Internet Crime's Against Children Task Force Working Group and have served as a member of the Technical Committee and as a member of the Legal Committee for the National ICAC Task Forces. I served in the past as the co-chair of the Technical Committee to the National Internet Crimes Against Children Task Forces and currently serve as a technical advisor to the Internet Crimes Against Children Task Force Undercover On-Line Training program.

I know from training and experience that child pornography comes from many sources. Computers have revolutionized the way in which those sources and users interact. Computers have also revolutionized the way in which collectors and users of child pornography can keep their collections. The development of computers and the

Internet has greatly changed and added to the way in which child pornography is disseminated, collected, and viewed. Computers have facilitated the ability of child pornography collectors and traders to keep their collections hidden. Photographs and videos that were previously stored in boxes are now traded and collected as digital images that can be stored and maintained on electronic media, such as a digital storage device called a "Micro Secure Digital Card", that is smaller than a postage stamp. Computers and the Internet now aid and serve in the production of child pornography, the distribution of child pornography, the viewing of child pornography, the storage of child pornography and communication between child pornography traders.

One of the fast-growing areas that facilitates and is used by child pornography collectors and traders is the P2P networks like FastTrack, EDonkey, Bittorrent and the Gnutella Networks. The Peer-to-peer (P2P) Networks have become ideal for traders to openly exchange collections and share those collections. The P2P network has provided a way for traders to have what they feel is an open and anonymous distribution and trading network. This network enables trading on a world-wide basis and with upload and download speeds as if the trader was next door.

I have personally worked many undercover P2P investigations and worked on the beginning phases of the current largest national P2P undercover initiative that began in 2003 and 2004 targeting those sharing files on the Gnutella Network. I have spent countless hours reading, studying, and trying the various Gnutella Client software programs in an effort to learn research and understand the P2P system of file sharing and am currently an instructor in the P2P Undercover program nationwide.

I have in the past served on the National ICAC Task Force Technology Committee with former Special Agent Flint Waters, of the Wyoming ICAC Task Force, who was the driving force and programmer behind the current methodologies in investigating Peer-to-Peer networks. During numerous ICAC board meetings, and in subsequent conversations and training situations, I have discussed with Flint Waters P2P investigations and the work being conducted across the country into investigations of P2P child pornography file sharing. Flint Waters is the original programmer/developer of the current Peer to Peer undercover initiative nationally. Those officers doing undercover ultimately use either software and/or techniques developed by him or something spawned off a development conceptualized by him. I am currently working with and continue to work with the National Undercover called "Beyond Operation Fairplay" training initiative for P2P to ensure a cohesive and proper use of the protocols and programs written for the National Undercover operation for the investigation of child pornography shared on the Gnutella Network. I know from training, research, personal experience in undercover investigations involving P2P networks, and by personal participation in the ICAC Task Force Board meetings the following information.