EXPERT DATA FORENSICS
INVESTIGATORS OF DIGITAL EVIDENCE

July 2014 eForensic Focus by: Leon Mare

Defending Internet Crimes Against Children

Technology continues to shape our culture – both to our benefit and detriment.

The Internet has blossomed as a global social town square and repository for much of the world's knowledge and wisdom, a modern-day Library of Alexandria.

The dark underside of the Internet, however, is the proliferation of child pornography and the exploitation of children, which has reached epidemic proportions.

Law enforcement has responded with initiatives such as the Internet Crimes Against Children (ICAC) Task Force Program, which allows local, state and federal law enforcement agencies to respond to cyber enticement and child pornography cases.

ICAC is a national network of 61 coordinated task forces representing more than 2,000 federal, state and local law enforcement and prosecutorial agencies.

Resources have been committed to forensic and investigative components, training and technical assistance, victim services and community education.

Defending those accused

Defending those accused of producing possessing or distributing child pornography has become a technical exercise in forensic investigation that now involves areas previously isolated to the world of information technology

Connect on Facebook

Follow on Twitter

Tel: (888) 355-3888

ExpertDataForensics.com

About the Expert

Leon Mare has testified as a Computer, Digital and Data Forensic Expert Witness in civil and criminal cases. He is one of a small number of examiners nationwide who is licensed as a private investigator and designated to provide expert witness services in Federal and State courts.

With his background in law enforcement, his expertise in computer network engineering and digital

professionals.

Defending those accused of child pornography crimes now involves an understanding of peer-to-peer file sharing software such as BitTorrent and eMule and the use of software such as Tor, which allows users access to a "dark net" area of the Internet where they can find anonymity to trade in explicit and illegal materials.

Tor is an "onion router," referring to the fact that a PC's net address is untraceable because data is encrypted in layers and sent through multiple relays before reaching its destination.

Tor was originally developed by the U.S. Navy and has been used by pro-democracy campaigns, whistle-blowers and journalists operating in oppressive regimes; all seeking anonymity.

Although Tor is popular for those seeking anonymity, the onion router has its limits. Though routed through multiple relays, Tor traffic eventually has to emerge from the dark net and enter the open Internet at exit nodes.

The node where traffic leaves Tor and enters the Internet can be monitored. If a user is accessing an encrypted website the exit node may be traceable. Someone who donates bandwidth by running an exit relay should understand that traffic exiting that relay could be traced to an IP address.

Defense attorneys should understand that a forensic data expert could trace exit nodes to determine if illegal activity was being piggybacked on a user's IP address.

Though criminals use these tools to violate the law, there are cases where innocent individuals find themselves wrongfully accused. Unprotected wireless networks, unrestricted access to personal computers and unsupervised home visitors has created legal challenges for the innocent.

Examples include the Buffalo, New York man who was raided by federal agents after a neighbor used his unprotected wireless router to download thousands of images of child pornography; or the Sarasota, Florida man who got a similar visit from the FBI last year after someone on a boat docked in a marina outside his

forensics and his vast experience as a Digital Forensic Expert Witness, Mr. Mare provides effective professional testimony. He has the ability to explain his findings and express the results in a clear and logical manner to the attorneys, judge and jury.

building used a potato chip can as an antenna to boost his wireless signal and download an astounding 10 million images of child porn.

Defense attorneys, using forensic data experts, can help answer the following questions:

- Did the accused unknowingly view images of minors?
- Were there links to illegal material found on the defendant's computer that were never opened?
- Could a peer-to-peer site have given a user the wrong download, leading to child pornography images showing up on the computer?
- Could another person have stolen a user ID and password to access pornographic images?
- Could the computer have been hacked, allowing an outsider to access illegal images without the owner’s consent?
- Did law enforcement use entrapment to lure the accused into an online chat room where illegal images were viewable?
- Are the images actively residing on the computer?
- Are the images cached and did the defendant view them?

Defense attorneys representing those accused of child pornography crimes should consult forensic data experts who can provide the following:

- Review protocols for seizing, storing and handling digital evidence
- Interview the accused to assist in the gathering of digital information
- Examine seized evidence for malware
- Examine settings that indicate which file-sharing protocol was used

Federal and state laws prohibit the production, possession, distribution or sale of pornographic materials

involving minors. Because of the severity of child pornography crimes, those accused are most often prosecuted to the full extent of the law. Since prosecutors are typically not lenient with sex offenders, people can receive severe sentences if they are convicted of child pornography crimes.

Outside of the legal arena, individuals facing child pornography charges often must deal with debilitating social consequences ranging from job loss to societal shunning and loss of familial and collegial interaction.

An individual accused of a child pornography offense who asserts his innocence must be prepared to meet the charges. For example, a person could face a false accusation if another downloaded child pornography onto his computer without his knowledge. He may become a suspect if he maintains an open wireless router and another piggybacks onto his Internet service to download and share illegal materials on a peer-to-peer network.

The accused individual's defense must be able explain how these processes work and the existence of other alternatives to a judge and jury. The defense attorney must be able to respond to the evidence presented by the government.

Leon Mare

Digital Forensic Investigator.

(Lic#1498)