

Atlantic Recording, et al v. Howell
AZ Case Number: 06-cv-02076

Declaration and Supplemental Expert Report

Dr. Doug Jacobson, Ph.D., CFCE

Ph.D. Computer Engineering
Certified Forensic Computer Examiner
International Association of Computer Investigative Specialists

Qualifications & Prior Testimony

- 1) I am employed as a Professor of Electrical and Computer Engineering at Iowa State University and as the Director of the Iowa State University Information Assurance Center. I also have an appointment with the Iowa State University police department where I aid in computer forensics.
- 2) In addition, I am the Chief Technical Officer and founder of Palisade Systems, a high-tech computer security company that specializes in network monitoring and filtering technologies.
- 3) My employment with Iowa State University began in 1982 as a computer programmer. I completed my Ph.D. in Computer Engineering with a focus in computer networking in December 1985. In January 1986, I was hired by the Department of Electrical and Computer Engineering as an Assistant Professor to teach and research in the area of computer networks. Since that time, I have taught over 25 classes in computer networks at both the undergraduate and graduate level. I have received over 5 million dollars in funding for my research and have written several articles and made numerous presentations on the topic.
- 4) In 1995, I created and taught one of the first computer security classes at Iowa State University and in the country. Under my guidance, in 1999, Iowa State University was recognized by the National Security Agency as a center of excellence. And in 2000, the Iowa State University Information Assurance Center was created. I am its first and only director. I am a Certified Forensics Computer Examiner. My Curriculum Vitae is attached as Exhibit (A)
- 5) On September 9th 2003, I testified in front of the U.S. Senate Judiciary Committee on the uses of peer-to-peer protocols.
- 6) On February 23 2007, I gave a deposition in the case UMG Recordings v. Marie Lindor, Case No. 05-cv-1095 (E.D.N.Y.).
- 7) On October 1 & 2 2007, I testified at the trial in the case of Virgin Records v. Jammie Thomas, Case No. 06-cv-1497 (D. Minn.).

Prior Experience

- 8) I have been teaching computer networking since 1986 and written papers and performed research on computer networks.
- 9) I have given over 50 presentations on computer security and networks at conferences, workshops, and various meetings.
- 10) I hold two patents in the area of computer network security and have won two R&D 100 awards for technologies I developed at Palisade Systems. One of these technologies is designed to detect and block peer-to-peer network protocols in addition to over 100 other network protocols.
- 11) I have assisted the Iowa State University Police department on several computer cases including cases using peer-to-peer networks to distribute pirated software and child pornography.
- 12) One of my graduate students, under my supervision and guidance, developed a system that monitors peer-to-peer networks and other forms of file-sharing for child pornography.
- 13) My rate for analysis and testimony is \$200.00 per hour. Additional expenses relating to analysis, testimony, and travel are reimbursed at the incurred costs.

Description of Technologies Involved

- 14) This case involves copyright infringement using computers connected to the Internet and involves the identification of the computers using their IP addresses. How IP addresses are used in the Internet, how IP addresses are assigned within the Internet, and how IP addresses and computers are identified is described below.

The Internet and Addressing

The Internet is a collection of interconnected computers or network devices. In order to be able to deliver traffic from one computer or network device to another, each computer or network device must have a unique address within the Internet. The unique address is called the Internet Protocol (IP) address. This is analogous to the postal system where each mail drop has a unique address.

Each computer or network device is connected to a network which is administered by an organization like a business, internet service provider, college or university. Each network, in turn, is analogous to a zip code.

Information is transported through the Internet in small chunks called packets. Each packet traverses the Internet and is reassembled by the destination machine. Each packet contains both the source and destination IP addresses. The source address is analogous to the return address on a letter and the destination IP address is analogous to the send to address on a letter.

IP Address Assignment

Every computer or network device directly connected to the Internet must have a unique IP address. To ensure each IP address is unique, a block of IP addresses is allocated to an organization such as an Internet Service Provider, business, college or university. The IP address allocation is done in a highly structured manner with each set of IP addresses (a network) allocated by a single centralized authority. Each organization is then responsible for allocating the addresses to individual devices.

There are two allocation methods for the devices connected to the Internet. The first allocation method provides the device with a static IP address and requires the user of the device to provide the IP address to the device during configuration. The owner of the network typically will provide the user of the device with the address information. This method is often used in businesses and colleges or universities. Two devices cannot effectively function if they are directly connected to the Internet simultaneously with the same IP address.

The second method involves dynamic addressing. With this method the device asks the network provider for an IP address when it wishes to use the network. The device will send a request, and the network provider will respond back with a packet that contains an IP address. The IP address is often allocated for a short period of time, and the device must request a renewal from the network provider. This method is called DHCP and is commonly used by Internet Service Providers (ISPs). The network provider will maintain a log of address allocations. As in the static case, two devices cannot effectively function if they are directly connected to the Internet simultaneously with the same IP address.

- 15) This case involves illegal file distribution using peer-to-peer networks. Peer-to-peer networks are a method used to distribute files from a user's computer to other users on the internet. They can also be used to obtain files from other users. Peer-to-peer networks are often used to distribute copyrighted material like songs and movies. In addition, peer-to-peer networks are also used to distribute other files including pornography, child pornography, computer virus, and data files. A more detailed explanation of peer-to-peer network is included below.

Peer-to-Peer Networks

The basic idea behind peer-to-peer networks is to allow people to connect to each other and distribute files or other information. Unlike the World Wide Web (web sites) where data is stored on central web services and users connect to a central web server to download information from the web site, peer-to-peer networks allow users to connect to each other and transfer files directly from user to user. The users of peer-to-peer networks typically do not know each other nor do they have any relationship outside the peer-to-peer network. The users of the peer-to-peer network often think they are anonymous when they distribute files. In reality, they can be identified using the IP address. The IP address of the computer offering the files for distribution can be captured by a user during a

search or a file transfer. That IP address can be associated with an organization such as, an ISP, business, college or university which can identify the user by the IP address.

Peer-to-peer networks are designed to facilitate the searching and transfer of data. Two basic types of peer-to-peer networks are decentralized and semi-decentralized.

With the decentralized peer-to-peer network, every computer that is part of the network has its own list of files that are offered for distribution, and each computer is connected to a small number of other computers (neighbors). Each neighbor is connected to a small number of computers and so on. When a user wishes to search for a file, a request is sent to each neighbor and each neighbor sends the request to the next neighbor and so on. If a computer gets the request and has a match, it will send a message back to the requester telling them it has the file(s) and providing them with information about the file(s).

The semi-decentralized peer-to-peer network uses a central index server that contains an index of files that are offered for distribution by the users of the network. The files themselves are still stored on the user's computer and not on the central server. Files are transferred directly from one user to another user. In addition, users can connect directly to each other like in the decentralized peer-to-peer networks. The central server makes searching more efficient. The semi-decentralized model can have more than one central server interconnected in their own peer-to-peer network. Benefits of this model include speeding up searches and distributing the work load. This also provides redundancy so that if one server node quits, the other nodes can still function and the network is still usable.

KaZaA

KaZaA is one of the most popular semi-decentralized based peer-to-peer software programs in use today. KaZaA uses a protocol referred to as Fasttrack to create the semi-decentralized peer-to-peer network. When KaZaA is installed, it creates a folder called the "shared folder" on the user's computer that is used to store files that are downloaded from other users and for distribution to other users. By default this shared folder is located in the KaZaA program directory. KaZaA also provides the ability for the user to set up additional sharing folders that are used to share files with other KaZaA users. When a user starts KaZaA, they are connected to a central index server (super node) and KaZaA offers or advertises the files they have available for distribution.

Distributing files requires that the files must be in a shared folder. The distributing computer uploads information about the files it is distributing to the index server. Any changes to the list of files in the shared folder are reported by the distributing computer to the index server. The user of the sharing computer can disable the sharing function, which would prevent the sharing computer from

uploading the file list to the index server and would also prevent the distribution of files in the shared folder.

When files are distributed, there is a set of identifiers that are used to tie the files back to the user. These identifiers include the IP address of the client distributing the files, the name of the file, file size, the content hash, and the port information. In addition, there are file descriptors that provide information like the artist name, album name, and description field. This information is used in the search process. The description field is used to provide a description of the files and is part of the KaZaA system. This field is not part of the original data stored on a CD, but rather is generally added by users who rip the songs to the computer. This field is sometimes employed by the user who made the copy or "ripped" the original copyrighted material to brand the file with their name or handle (a fake name). The content hash is a mathematical function that is used to identify files that are the same. This allows the user to search for the file if the original download fails or to increase the transfer speed.

To find a file the user submits a query using the KaZaA application, which forwards the query to the super node. The super node looks in its database for the file(s) that match the search parameters. If one or more of the users connected to the super node has the files(s) that match the request, then the super node returns the IP address(s) and the file description(s) of all matches. Super nodes send queries between each other thus expanding the search capability. Users may also connect directly between each other, so if a user finds a file on another user's machine he or she may then query the machine directly to see what other files are offered for distribution.

Once a user has found the file they want to download they send a request to the computer sharing the file requesting a copy of the file. The sharing computer will copy the file from the shared folder(s), set up by the KaZaA user, into the computer's memory. The sharing computer then transmits the copy of the file contained in its memory to the computer that requested the file as a sequence of network packets. The network packets are transferred across the Internet. The requesting computer takes the packets it receives and places them into a file in the shared folder on the receiving computer.

KaZaA cannot be used to listen to music that is stored on another computer in the KaZaA network. In order to listen to or preview music that was stored on another computer, the file has to be downloaded to the user's computer. KaZaA will allow, however, a user to listen to small samples of music that can be purchased from the KaZaA web site.

In addition to KaZaA, there are several other applications that use the Fasttrack protocol. These applications include iMesh, Grokster, and iSwipe. These applications are available on computers using Microsoft Windows, Apple OS, and Linux. Since these applications use the Fasttrack protocol, users with

one application can share files with users using another application. The name KaZaA is often used to refer to the applications running the Fasttrack protocol.

Hard Drive Forensics

16) This case involved the examination of a hard drive. Several terms need to be defined relative to a hard drive examination.

Current Internet History – Internet history on the computer that has not been altered. This history can be tied to a specific user account on the computer, if the operating system permits it.

Forensically Sound – The preservation of evidence surrounding a case such that the evidence is kept exactly the way it was received. In computer terms, “forensically sound” relates to the preservation of the state of the data – no information has been added, edited or removed from the forensic media during the examination.

Initiating Party – The party that brings the forensic media in for analysis, and provides the scope of the investigation to the investigators.

Internet Cache – A location on a piece of media that contains downloaded images, movies, sounds and web pages of locations users have visited on the Internet. The Internet Cache is often cleared to make more space available on the media, and can be configured to be emptied when the user closes the Internet browser.

Investigators – Those performing the forensic analysis of the media for the specified parameters.

Media – The items that contain digital evidence, which are brought to the investigators for analysis. Media includes, but is not limited to, hard drives, USB devices, CD-ROM's, floppy discs, ZIP™ discs and DVD's.

Past/Removed Internet History – Internet history on the computer that had to be recovered from unallocated (deleted) file space.

Unallocated Space – When files are deleted from media, references to them are removed, but the actual data may still exist on the media. Unallocated space is the term used to describe any part on the media where a file may have existed. Since unallocated space is eventually overwritten, the usage of the computer dictates how long a deleted file will exist here.

17) The hard drive examination followed several steps as outlined below, which are consistent with the process outlined by the International Association of Computer Investigative Specialists.

Evidence Acquisition Phase

During the acquisition phase, the initiating party provides the investigators with all relevant media associated with the case. The initiating party also provides investigators with information surrounding the investigation that will be applied in the analysis stage.

Evidence Preservation Phase

During the preservation phase, an exact, forensically sound copy is made of each medium obtained in the acquisition phase. This ensures the original media is not tainted in any way. Further, hash values are created of the original media, and compared against the copies, to ensure that the copied data accurately represents the original media. This keeps the forensic process sound.

Analysis Stage

During the analysis stage, information that relates to the case is searched for over all the media obtained. This information is retrieved during the acquisition phase. This ensures that the investigators are only looking for information pertaining to this case. Investigations outside these parameters will not take place, unless otherwise explicitly stated by the initiating party.

Conclusion Stage

The conclusion stage will draw together everything analyzed in the analysis stage. Here, the investigator will review the recovered data, and provide explanations of why the data exists where it does, and how the data relates to the case.

Materials Considered

- 18) I have reviewed the underlining investigative data for the Howell case. This includes all of the data supplied by MediaSentry. I also have reviewed information supplied by Defendant's Internet Service Provider (ISP) Cox Communication. Below is a list of the materials I considered in developing my conclusions.
- a) MediaSentry Screenshots
 - b) MediaSentry Systemlog
 - c) MediaSentry UserLog (compressed)
 - d) MediaSentry UserLog
 - e) MediaSentry Download Logs
 - f) Certificate of Registration
 - g) MediaSentry Trace
 - h) Cox Communication subpoena response
 - i) Hard Drive submitted in the Howell Case
 - j) DVDs (labeled 1 through 10) submitted in the Howell Case

Conclusions

- 19) I will testify to the procedures used and results obtained by MediaSentry coupled with the information supplied by Defendants ISP, to demonstrate the Defendant's Internet account and computer were used to download and upload Copyrighted music from the Internet using the KaZaA peer-to-peer network.
- 20) I will testify that MediaSentry found over 4000 files shared on a computer using the KaZaA file sharing program based on the screenshots. The KaZaA user id is "jeepkiller@KaZaA"
- 21) I will testify that MediaSentry downloaded 12 songs as shown in Systemlog and the MediaSentry download logs and that many of these songs are copyrighted as shown in the Certificates of Registration.
- 22) I will testify that the information from MediaSentry (Systemlog, UserLog, UserLog (compressed), and the Download Logs) indicates that the computer with IP address 68.110.64.47 offered 2329 audio and music files, most of them are copyrighted music files, for distribution using the KaZaA program on 1/30/2006 starting at or around 1:30:42 AM EST through at least 2:09:06 AM EST.
- 23) I will testify that the information from MediaSentry provided in the MediaSentry trace shows that Cox Communication is the Internet provider for the computer with the IP address of 68.110.64.47 on 1/30/2006 starting at or around 1:30:42 AM EST through at least 2:09:06 AM EST, during which time the 2329 audio and music files were being distributed using the KaZaA program.
- 24) I will testify that the subpoena response from Cox Communication identifies Pamela Howell as the subscriber of record for the IP address 68.110.64.47 on 1/30/2006 at 1:52:28 AM EST. Cox Communications also identified the email address jeepkiller1@cox.net as belonging to the same subscriber.
- 25) I will testify, based on all of the information provided that the computer that had the IP address of 68.110.64.47 on 1/30/2006 starting at or around 1:30:42 AM EST

- through at least 2:09:06 AM EST was registered to the Defendant and that the said computer was used to distribute copyrighted music.
- 26) I will testify that, based on the MediaSentry UserLog, the music found on the Defendant's computer was downloaded from other users on the Internet.
 - 27) I will testify based on the hard drive supplied by Mr. Howell that the computer produced by Mr. Howell (the "Howell computer") had its operating system reinstalled on January 2, 2007 and that reinstalling the operating system on the hard drive will delete some of the files, but evidence of some of the files will still exist in the unallocated space on the hard drive.
 - 28) I will testify based on the hard drive supplied that the Howell computer had the peer-to-peer file sharing program KaZaA installed at one time. The KaZaA program was removed prior to the date of inspection.
 - 29) I will testify based on the hard drive supplied that the Howell computer had wiping software (Aevita wipedelete) installed on the computer and that the software was located in the "JH" folder on the Howell computer. Wiping software of this type is typically used to remove all evidence of certain files and or activity from the computer. It is not generally used for routine computer care and maintenance. The Aevita wiping software was downloaded in November of 2006 and appears to have been last used on March 20, 2007. It is not possible to determine what files or programs were wiped because no such logs of the Aevita wiping software's activity were kept.
 - 30) I will testify based on the hard drive supplied that the Howell computer had the username "jeepkiller1" appearing numerous times on the hard drive.
 - 31) I understand that Mr. Howell has claimed that the sharing of music files on 1/30/2006 was the result of a malfunction in the KaZaA software. In my review of the Howell computer I have found no evidence of a malfunction. In addition there is nothing abnormal in the MediaSentry data to indicate a malfunction in the KaZaA software.
 - 32) I understand that Mr. Howell has stated that the KaZaA program was sharing his entire hard drive on 1/30/2006. In my opinion this is not correct. The MediaSentry data showed just over 4000 files being shared. Examination of the Howell computer shows there are over 200,000 files on the hard drive. If Mr. Howell had shared his entire hard drive then MediaSentry's data would have shown over 200,000 files.
 - 33) I will testify based on the hard drive supplied that the Howell computer, in spite of the removal of the KaZaA program, contains evidence of the default KaZaA shared folder (c:\Program Files\Kazaa\My Shared Folder) in the unallocated space of the hard drive as shown in my Exhibit B. I will also testify that the shared folder contained MP3 files and one of these MP3 files matched a file found by MediaSentry on January 30, 2006.
 - 34) I will testify based on the hard drive supplied that the Howell computer had a "c:\My Music" folder which contained several thousand MP3 files as shown in my Exhibit C. The "c:\My Music" folder contains over 490 MP3 files which were placed in the folder on 11/05/2002 and over 120 MP3 files which were placed in the folder on 3/29/2006 and over 2200 MP3 files which were placed in the folder on 6/20/2006.

- 35) I will testify that none of the files from the "c:\My Music" folder were being shared by KaZaA on 1/30/2006. This testimony is based on the fact the entire contents of the "c:\My Music" folder that were created before 1/30/2006 did not appear in the MediaSentry capture. If the "c:\My Music" folder was being shared on 1/30/2006 then all of the files that were created before 1/30/2006 would have been captured MediaSentry. I have compared the list of MP3 files that MediaSentry found during their capture on 1/30/2006 with the list of MP3 files that existed in the "c:\My Music" folder on the Howell computer on 1/30/2006. The lists do not match.
- 36) I understand that Mr. Howell has said he used Roxio to automatically backup his "My Music" folder. I did find evidence on the Howell computer of the Roxio CD creator software, which is used to create audio and video CDs. I did not find any evidence on the Howell computer of any Roxio automatic backup software or any configuration of the Roxio software that would perform automatic backups.
- 37) I will testify based on the DVDs provided by Mr. Howell that DVD number 1 contains data files from the Windows operating system and that several of the data files were created in 2007 and one file was created in May 2008. It is my opinion that DVD number 1 either was not created in 2006 or has been altered. My analysis of the images of DVDs 2, 4, and 5 shows the data is not in a useful format and further investigation is needed.
- 38) My investigation of DVDs 3, 6, 7, 8, 9, and 10 shows these DVDs contain pornographic images and movies. Some of files correspond to the files being distributed as shown by the MediaSentry Userlog on 1/30/2006. Some of the files do not correspond to the files being distributed as shown by the MediaSentry Userlog on 1/30/2006. The number of pornographic images and movies found by MediaSentry on 1/30/2006 does not match the number of pornographic images and movies provided by Mr. Howell in the DVD images.
- 39) I will testify based on the DVD images provided by Mr. Howell that these DVDs contain copies of files from a computer and were not created as part of a normal windows backup process. Had the DVDs been created by a typical windows backup process they would have contained information about the file's original location and other information needed to restore the files to their original condition.
- 40) I reserve the right to review additional discovery materials, as they are made available for my review, and use any of the material considered as exhibits in my testimony. My investigation and forensics analysis of the hard drive and DVDs is not complete and I reserve the right supplement my report based upon further forensic examination and investigation.

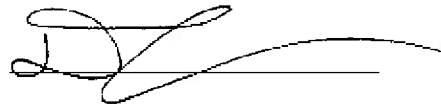
Attachments:

Doug Jacobson – Curriculum Vitae – Exhibit (A)

List of files found in "c:\Program Files\Kazaa\My Shared Folder" Exhibit (B)

List of files found in "c:\My Music" – Exhibit (C)

I declare under penalty of perjury and the laws of the United States that foregoing is true and correct. Executed this 8 day of July, 2008, at 4:20



Dr. Doug Jacobson