

UMG RECORDING INC., et al v. Lindor
ED - NY Case Number: 05-cv-1095

Supplemental Declaration and 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 an associate 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.

Prior Experience

- 6) I have been teaching computer networking since 1986 and written papers and performed research on computer networks.
- 7) I have given over 50 presentations on computer security and networks at conferences, workshops, and various meetings.

Dr. Doug Jacobson
2500 Woodview Dr, Ames, Iowa 50014
(515)-292-7239 dougj@iastate.edu

- 8) 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.
- 9) 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.
- 10) 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.
- 11) 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.

Hard Drive Forensics

- 12) 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.

- 13) 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 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. Once the media is delivered to the investigators, proper documentation is signed indicating the media transfer.

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

- 14) I have reviewed the underlining investigative data for the Lindor case. This includes all of the data supplied by MediaSentry. I also have reviewed information supplied by Defendant's Internet Service Provider (ISP) Verizon Internet Services. 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) Verizon Internet Services subpoena response
 - i) Disk drive image from defendant's computer

Conclusions

In addition to the conclusions contained in my report dated April 7th 2006 I have the following additional conclusions based on the additional information from the hard drive image.

- 15) I will testify to the procedures used and results obtained by MediaSentry coupled with the information supplied by Defendant's 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.
- 16) I will testify that based on the MediaSentry data mentioned above and registry entries recovered from the computer that the computer had a public IP address and was not connected to the Internet via a wireless router.
- 17) I will testify based on the forensics examination that the computer had three usernames of interest that were named Kathleen, Woody, and Yanick.
- 18) I will testify that I found very few user created files and saved emails on the hard I was provided to by the defendant.
- 19) I will testify that based on the data recovered from the hard drive provided by the defendant that the users Woody, Kathleen, and Yanick accessed the Internet using the computer.
- 20) I will testify that based on the data recovered from the hard drive that this hard drive does not appear to be the same hard drive that was used to share copyrighted songs as shown by the MediaSentry materials. I will testify based on the forensics examination of the hard drive that was copied from the computer owned by the defendant that the computer had no evidence of the KaZaA program nor was there any evidence of the KaZaA program ever being installed on the computer, although the MediaSentry data showed the computer connected to the defendant's Internet account was running the KaZaA program.

- 21) I will testify based on the data recovered from the hard drive produced by the defendant that the computer had a Western Digital 100 GB USB external hard drive connected to it and that the external hard drive was first connected on or before 7/8/2004. The external drive was not provided by the defendant.
- 22) The user Woody used Windows MediaPlayer to access songs and other files from a directory:
(F:\h\Documents and Settings\Yanick\My Documents\download\yayahq) located on the external hard drive.
- 23) I will testify that based on the data recovered from the hard drive that the user Woody was administer of the computer.
- 24) I will testify that based on the data recovered from the hard drive provided by the defendant that several email addresses were associated with users on the computer including: wraymond yanick_wright, kathleen, yayagq, yanick_ray.
- 25) I will testify that based on the data recovered from the hard drive provided by the defendant that the yahoo account jeanlindor was accessed using the computer.
- 26) I will testify that the computer contained the resume of Gustave Lindor, Jr and that the document indicates he was living and working in Brooklyn N.Y. and working at Long John Silver's during the dates that the copyrighted music was being shared.
- 27) 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.

Attachments:

Doug Jacobson – Curriculum Vitae – Exhibit (A)

I declare under penalty of perjury and the laws of the United States that foregoing is true and correct. Executed this 15 day of December, 2007, at 9:00am

A handwritten signature in black ink, appearing to read "Doug", is written over a horizontal line.

Dr. Doug Jacobson