

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

-----x
UMG RECORDINGS, INC., et al.,

05 CV 1095 (DGT)(RML)

Plaintiffs,

- against

MARIE LINDOR,

Defendant
-----x

DECLARATION OF DR. DOUG JACOBSON, Ph.D., CFCE

I, DR. DOUG JACOBSON, Ph.D., CFCE, declare:

1. I have been retained by the plaintiffs in this action, among other things, to review and provide my opinions regarding data and information contained on a disk drive image from defendant's computer that was provided to me. I have also previously provided an expert report regarding the initial detection of infringement on defendant's computer and the workings of Kazaa, among other things. I have personal knowledge of the facts set forth in this declaration except as where stated on information and belief. As to such facts, I believe them to be true.

2. My qualifications and prior testimony are as follows:

a. 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.

b. 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.

c. 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.

d. 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.

e. On September 9th 2003, I testified in front of the U.S. Senate Judiciary Committee on the uses of peer-to-peer protocols.

f. A true and correct copy of my Curriculum Vitae is attached as Exhibit A.

3. My prior relevant experience is as follows:

a. I have been teaching computer networking since 1986 and written papers and performed research on computer networks.

b. I have given over 50 presentations on computer security and networks at conferences, workshops, and various meetings.

c. 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.

d. 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.

e. 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.

4. In connection with my analysis, I have reviewed all of the underlying investigative data for this case, including all of the data supplied by MediaSentry. I have also reviewed the information supplied by defendant's Internet service provider, Verizon Internet Service. In particular, I considered the following:

- 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 Service subpoena response
- i. Disk drive image from defendant's computer

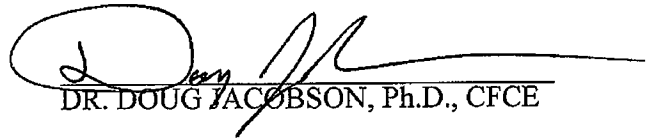
5. Based upon my review of the foregoing materials, as well as on my education and experience, it is my opinion and belief that defendant's computer had a public Internet Protocol ("IP") address and was not connected to the Internet via a wireless router. I base this on the data mentioned above, as well as on the registry entries recovered from the computer and the fact that there was no internal IP address here. Based on how IP addresses are assigned, it is not difficult to determine whether a computer was connected to the Internet via a wireless router. This computer was not.

6. In addition, it is my opinion and belief, based on my education and experience and on the data recovered from the hard drive that I reviewed, that this hard drive was not the same hard drive that was used to share copyrighted sound recordings as shown by the MediaSentry materials. A forensic inspection of a computer hard drive in a case like this one can provide significant information regarding the infringement alleged. For example, a forensic inspection would allow one to see, among other things, whether a file-sharing program was downloaded or installed and whether there is a share folder. It would also show whether the audio files, or any remnants or evidence thereof, that MediaSentry observed being distributed from defendant's IP address remained on defendant's computer. Finally, a forensic inspection can reveal whether a party attempted to delete file-sharing programs or other files. The MediaSentry data here showed that the computer connected to defendant's Internet account was running the Kazaa program. As such, a forensic inspection of that computer would have

revealed at least remnants of the Kazaa file-sharing service, as well as the existence of a share folder, or remnants of it, had someone attempted to delete it. The hard drive that was provided and that I inspected, showed little usage at all, as evidenced by the lack of user created files and e-mails, and did not reveal the evidence noted above, which I believe the correct hard drive would certainly have shown.

7. The hard drive that was provided did contain the resume of Gustave Lindor, Jr., and that document indicates that he was living and working in Brooklyn, New York during the dates that the copyrighted music was being shared.

Executed this 19th day of December, 2006, at Ames, Iowa.


DR. DOUG JACOBSON, Ph.D., CFCE