Expert Report of Benjamin Perino

Benjamin Perino
November 23, 2017
GuardaLey LTD
Daimlerstr.9, 76344 Eggenstein
Phone Number: +49 (0) 721 / 97 79 57 4

EXPERT REPORT OF BENJAMIN PERINO

I, Benjamin Perino, declare as follows:

1. My name is Ben Perino.

2. I am over the age of 18 and am otherwise competent to make this declaration. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

3. I am currently the Chief Executive Officer and a Senior Developer at GuardaLey, LTD ("GuardaLey"), a German company located at Daimlerstr.9, 76344 Eggenstein, Phone Number: +49 (0) 721 / 97 79 57 4.

4. Most of the information contained in this report provides GuardaLey with a competitive advantage and is not generally known to the public. I therefore respectfully request that this report be filed and kept under seal.

5. I implemented, maintain and monitor GuardaLey's data collection system used to track and identify the IP addresses used by people to commit copyright infringement via the BitTorrent protocol. GuardaLey licenses this infringement detection system to MaverickEye UG ("MEU").

6. I went to Carl Engler Technical High school in Germany and graduated from there in 1999.

7. I have worked in the Information Technology business since 2001. I am a Senior Developer and System Architect with nearly 20 years of experience.

8. Between 2001 and 2010, I worked for Siemens AG in Germany. Initially, I began as a Developer and IT Specialist in Research and Development. In this role, I was in charge of the development of Optical Identification Systems for 2D matrix codes for process automation. I developed observing mechanisms for optical sensors that are used in any kind of automated assembly lines.

9. Thereafter, at Siemens, I secured the role of Senior Developer and was charged with the development of Industrial Ethernet Bus Analysis Software BANY.NET / PNIO Time and

telegram analysis on real-time Ethernet. This software is described in detail at the following website: http://www.industry.siemens.com/datapool/industry/industrysolutions/services/en/Bany-pnio-en.pdf. BANY PNIO records non-reactively data traffic up to 1 Gbps with a resolution of 10 nanoseconds. The software engages in timestamping, and the data is backed up in a format readable with Wireshark. The software is an equivalent of Wireshark but designed for industrial purposes with higher accuracy. It is used to observe and identify network traffic. It enables the user to inspect relevant packets sent over the networks. Decoding network packets and writing function that do this was my main focus.

10. Around 2007, I worked at a department at Siemens where I was responsible for the quality assurance for the automation development process of SIMATIC PCS 7 PDM section maintenance and field device monitoring. The key part of this job was to pass new features developed for Siemens' proprietary Monitoring software used to observe the correct functionality of power plant automation and process automation systems.

11. In 2008, I founded GuardaLey LTD and designed GuardaLey's entire infringement detection system which is now licensed to MEU, and which MEU uses to track and identify the IP addresses using the BitTorrent protocol. At GuardaLey, I plan and design software, I maintain the server infrastructure to add new products, new services, new infrastructures, and I run and monitor the software on our servers. Specifically, I programmed the BitTorrent tracking software which MEU uses.

12. I am not paid by Venice PI, LLC for my testimony in this matter. However, MEU pays me an hourly rate of $250 per hour for preparation of this report. However, if required to testify at any trial or deposition, MEU will compensate me a daily rate of $2500.

13. Attached as Exhibit "A," is a list of all cases in the last four years wherein I was subpoenaed to testify either at a deposition or at trial. I did not have to appear in all cases since some of them were canceled/settled before I had to appear. I cannot reproduce exactly which ones were cancelled. *See* List of Perino's Testimony, Exhibit "A."

A. THE INFRINGEMENT DETECTION SYSTEM ACCURATELY RECORDS EVIDENCE OF INFRINGEMENT OF WORKS THROUGH THE BITTORRENT PROTOCOL

14. MEU is in the business of providing forensic investigation services to copyright owners around the world.[1] Specifically, MEU uses GuardaLey's backend software and servers to run the infringement detection system to track digital content and record the online downloading and distribution of Plaintiff's copyrighted works through the BitTorrent file distribution network, and subsequently identifies the Internet Protocol ("IP") addresses that are being used by infringers to distribute these copyrighted works without authorization.

15. The data collection system provided to MEU has the following components:

a. a proprietary BitTorrent Client that analyzes the Bittorrent traffic and writes infringing transactions to a database;

b. servers running a MySQL database cluster which log verified infringing transactions;

c. packet analyzers, also known as packet sniffers, which create and analyze PCAPs;

d. servers that run the proprietary BitTorrent Client and record PCAPs;

e. servers that run BitTorrent Clients to download a reference copy of each version of the work.

f. WORM ("Write Once Read Many") tape drives for storing the PCAPs and torrent data;

g. a program to synchronize the servers' clocks with an atom clock;

h. a proprietary program which checks the content downloaded against the reference files.

i. a proprietary program to transmit the data

j. a proprietary program which checks the information contained in an Excel Spreadsheet against what is in MySQL server's log files.

---

[1] This is based on my review of the Declaration of Daniel Arheidt's in Support of Plaintiff's *Ex Parte* Motion for Expedited Discovery.

16. This infringement detection system accurately collected and recorded evidence proving that the IP addresses in this case infringed Plaintiff's copyrighted work(s). *See* List of Cases, Relevant IP Addresses, and BitField Values attached hereto as Exhibit "B."[2]

17. The infringement detection system uses a proprietary BitTorrent client to connect to the swarm of infringers unlawfully sharing Plaintiff's copyrighted movie. Once it has joined the swarm, the infringement detection system connects to infringing peers using a TCP/IP connection, and begins to download the unauthorized files from the IP addresses. Each of these infringing transactions is also recorded in the form of a PCAP.

18. Data sent through the Internet is delivered in the form of "packets" of information. A PCAP is a computer file containing captured or recorded data transmitted between two computers. PCAP stands for "Packet Capture." To provide evidence of infringement, the system records each infringing transaction in the form of a PCAP.

19. The PCAPs are then stored on WORM tapes. "WORM" stands for "write-once-read-many." The reason we use WORM tapes are because once information is written thereon, it cannot be modified. This feature provides assurance that the data cannot be manipulated or altered once it is written to the WORM tape. Each of the WORM tape drives is electronically stamped with a German government issued time stamp at least every twenty-four hours.

20. The WORM tapes are then stored in a vault. The infringement detection system and infrastructure fulfills the standards of the PCI security specifications, which is one of the highest security standards required by credit card processing companies. Additionally, the datacenter where all collected data is stored is certified ISO/IEC 270001:2013.

21. The infringement detection system uses a proprietary packet analyzer and TCPDump (a free open-source packet analyzer) to record the infringing transactions in PCAPs. TCPDump is widely used and is capable of accurately recording network traffic.

---

[2] The case numbers pertaining to each IP address were provided by Plaintiff's counsel, David Lowe.

22. Here, the PCAPs are recordings of numerous BitTorrent computer transactions during which the IP Addresses listed on Exhibit B sent pieces of an infringing computer file (which contain an unlawful copy of Plaintiff's movie) to the servers. Each infringing transaction is also recorded on a log. *See* Infringement Capture Logs for Relevant IP Addresses attached hereto as Exhibit "C."[3] Each entry in the log file correlates to a specific PCAP file.

23. The infringement detection system ***does not*** upload or distribute content; it was created such that it is incapable of doing so. It only downloads the content from infringing IP addresses.

24. The system also engages in enhanced surveillance to discover other digital media files distributed by Defendant over the BitTorrent Protocol. *See* Additional Evidence Logs for Relevant IP Addresses attached hereto as Exhibit "D."[4] To compile the Additional Evidence, a separate surveillance system records IP addresses listed in a BitTorrent swarm's directory (Tracker and DHT data) known to participate in sharing each of the third-party works. Thereafter, the surveillance system only records the title, hash values, date, and time of the IP address's participation within the third-party swarms. Unlike the TCP/IP connection MEU establishes with respect to IP addresses distributing Plaintiff's movies, the surveillance system ***does not*** establish a direct TCP/IP connection nor does it transact with IP Addresses concerning third-party works listed on the additional evidence.

25. GuadaLey is required, by German Highcourts, to provide expert witness reports for its system on an annual basis, and its system has been successfully audited and tested by independent expert witnesses in several countries. For example, Dr. Simone Richter and Robert D. Young each reviewed the system separately and both determined that it accurately identified IP addresses distributing works via the BitTorrent network and that the PCAPs accurately reflect the data associated with the transactions. The result of each examination is listed in more detail within

---

[3] The Infringement Capture Logs only includes log entries for the motion picture at issue in this case.

[4] As a precautionary measure, I have asked Plaintiff's counsel to file the exhibit under seal since many of these logs contain adult content titles.

their respective expert reports. *See* Dr. Simone Richter's Expert Report attached hereto as Exhibit "E;" *see also* Robert D. Young's Expert Report is attached here to as Exhibit "F."

B. TCP/IP CONNECTIONS CANNOT BE SPOOFED AND CANNOT YIELD FALSE POSITIVES

26. As previously stated, the infringement detection system connects to the infringing peers using a TCP/IP connection. Often times in BitTorrent copyright infringement cases, defendants claim that their IP address was spoofed. It is self-explanatory that IP spoofing cannot be used in this scenario when you understand what spoofing is.

27. With IP spoofing a very experienced network specialist (initiator) can send messages to an IP (recipient) pretending that this message was sent from another IP (fake sender / victim). The recipient's computer then automatically answers this message and sends the answer back to the fake sender / victim. This is usually used for DDOS attacks (denial of service), where the fake sender / victim is flooded with hundreds of thousands of messages at the same time. This can only be achieved by using a lot of computers (recipients) at the same time, attacking one machine.

28. To use this method to really receive usable packets, like in BitTorrent where the content is used to put together the whole file, the Initiator would have to catch the packets coming from the recipient before they reach the victims computer to be able to fake the whole continuous communication. Not only can this not be done by an average user, the effort to setup all of this just to download a movie is far too burdensome. You need to be a very experienced tech-savvy person with a large skillset in network techniques and you would have to be located in the same (local) network to catch the packets. Accordingly, it is next to impossible that a party would use spoofing in their use of BitTorrent.

29. With respect to the use of VPN where users are enabled to hide their IP address by using another IP address as a frontend, the infringement detection system would capture the infringement from the frontend IP address. But such IP addresses would then belong to a professional VPN service and would not belong to Comcast.

C. WHAT WAS DETECTED?

30. The infringement detection system establishes a direct TCP/IP connection to the IP addresses and downloads 16KB blocks which are verified to the original torrent via hash comparison. The significance of this direct connection is that the detection system can prove that the IP address provided illegal content at an exact time.

31. Once this direct connection is established, the system begins the process of downloading a piece or pieces of the infringing computer file from the device connected to the internet through the IP address. As previously stated, the entire process and all of the transactions are recorded and stored in a database and evidenced by stored PCAPs.

32. MEU tasked me with effectuating, analyzing, reviewing and attesting to the results of the investigation for the relevant IP addresses.

33. Upon review of the forensic activity logs for the relevant IP addresses, I determined that the forensic servers were connected to electronic devices using the relevant IP Addresses. Consequent to this connection, the relevant IP addresses were documented as distributing to the servers, multiple pieces of Plaintiff's copyrighted movie titled *Once Upon A Time in Venice*. The foregoing activity is listed by IP Address in Exhibit C.

34. A digital file can be identified by what is called a "Cryptographic Hash Value". This concept was developed by the United States National Security Agency. The infringement detection system determined that the file being distributed by the relevant IP Addresses have unique Cryptographic Hash as listed on Exhibit C.

35. Full copies of the digital files identified by the different Hashes were downloaded by the system, and MEU confirmed these files are of the digital movie *Once Upon a Time in Venice*. MEU further viewed this file and determined it was substantially similar to Venice LLC's copyrighted movie titled *Once Upon a Time in Venice* [5].

---

[5] All statements made within this report regarding the verification and comparison of the hashes between the unauthorized copy of *Once Upon a Time in Venice* and an authorized copy of Plaintiff's *Once Upon a Time in Venice* is based on my review of the Declaration of Daniel Arheidt filed in support of Plaintiff's *Ex Parte* Motion for Expedited Discovery.

36. In addition to the correct IP, the validation of the content transferred and the reference file that was manually and audiovisually compared to the original movie the exact time at which the infringement was captured is of importance. We are able to provide synchronization protocols to prove that the servers collecting the data were accurate and in sync with atom clocks i.a. provided by the physical-technical federal institute Brunswick, Germany. Each capture is covered by two protocols from two independent timeservers.

37. For these reasons, the infringement detection system cannot yield a false positive. Indeed, the TCP/IP connection actually occurred. In making this direct peer-to-peer connection, the infringement detection system shows, through a confirmed transaction, that an IP address is actively broadcasting Plaintiff's copyrighted movie. The system also verifies the file downloaded is an infringing copy of Plaintiff's movie, and records the exact time of the direct peer-to-peer transaction. Thus, concerns about reassigned IP addresses, and false positives are overcome because the infringer's IP address are time-specific, and verified as being received and acknowledged by both parties. Furthermore, the connection is established 5 seconds before the actual transmission and is kept upright at least 5 seconds after the transaction. Most of the time the systems are connected over multiple minutes. An IP address change would interrupt and terminate this connection.

D. THE INFRINGEMENT CAPTURE LOG AND ADDITIONAL EVIDENCE LOGS CAN PRESENT PROOF THAT EACH IP ADDRESS ENGAGED IN COPYRIGHT INFRINGEMENT

38. As previously discussed, the system engages in enhanced surveillance using a BitTorrent swarm's directory (Tracker and DHT data). This provides MEU with the titles of other digital media files distributed by the relevant IP addresses over the BitTorrent Protocol. *See* Additional Evidence Logs for Relevant IP Addresses attached hereto as Exhibit "D."

39. Tracker and DHT data is generally accurate since participants regularly announce themselves in the BitTorrent swarms. The Additional Evidence can be used to support or enhance the infringement information captured as explained below:

a. The Additional Evidence Log can potentially provide an infringer's viewing habits and interests and may be used to identify the actual infringer within a household. Indeed, it is possible to correlate these works with a list of a defendant's publicly displayed interest on social media.

b. A subscriber may claim that the infringer was a weekend guest. However, the Additional Evidence Log (and even the Infringement Capture Log) may reflect an IP address engaging in constant and continual BitTorrent use over a period of weeks or months.

c. The Additional Evidence Log (and even the Infringement Capture Log) can establish that when a defendant left on a trip, infringement abruptly stopped. And when the infringer returned from his trip, activities continue.

d. The Additional Evidence Log can show downloading of extensive files in a particular language, which can help the parties determine the identity of the infringer by determining the individual who speaks that particular language within the household.

40. Accidental behavior becomes extremely unlikely when the Additional Evidence Log lists thematically consistent records over an extended period of time (e.g., when the defendant is an established photographer, and the Additional Evidence shows a multitude of photography software downloaded over a period of a year). Simply put, the data (as a thematic whole) can provide evidence of infringing activity tied to a specific IP address.

41. Similar to the Additional Evidence Logs, Infringement Capture Logs also establish a time line (supported by direct TCP/IP connections and PCAPs). In addition, upon request, we can provide the name of the BitTorrent Protocol the Infringer used in each infringing transaction. This can be critical information because often times the infringer will use the exact same BitTorrent Protocol over an extended amount of time and can even upgrade to a newer version of the same BitTorrent Protocol as it became available. This type of record supports the argument that the infringer is an individual with regular access to the IP address rather than a one-time interloper or weekend guest. The parties can also compare a defendant's work or school schedule with the timeline provided.

E. IT IS HIGHLY UNLIKELY THAT THE ELECTRONIC DEVICE USING THE RELEVANT IP ADDRESSES DID NOT DOWNLOAD PLAINTIFF'S COPYRIGHTED WORK TO COMPLETION

42. The Court has asked that Plaintiff produce expert testimony and evidence regarding the likelihood that the infringer has a "playable" and actionable segment of the copyrighted work at issue in this case.

43. Individuals are actively initiating the download of a file over the BitTorrent network with the intention to download an exact copy of the whole work. The reason why BitTorrent was created, was to distribute and obtain large computer files as fast as possible with the least network load. BitTorrent downloads can therewith sometimes be faster than downloads from single servers. With today's bandwidth and internet speeds, an infringer can download an average movie file in less than 20 minutes, and sometimes even in less than 5 minutes. Most often files are downloaded quickly and remain available to others so that the amount of possible download sources increase.

44. The infringement detection system protocols the "BitField" value which is also contained in the PCAPs and in the Infringement Log Files in Exhibit "C." The "BitField" is data which is exchanged during the handshake (and it also increases as the user continues to obtain more bits of the works) between the infringer and another peer. It informs the peer about the pieces available for download and therefore the total amount of the torrent file that the infringer ***has already downloaded*** and which the infringer is able to distribute to another peer upon request. In other words, this broadcasted value provides other peers with the percentage of the file which the infringer possesses. Here, the BitField values for the relevant IP addresses all range, and the majority are as high as 100%. *See* List of Cases, Relevant IP Addresses, and BitField Values attached hereto as Exhibit "B." In addition, Exhibit B also includes the total number of minutes of the infringing copy which each BitField value represents.

45. Lastly, the infringement detection system documents copyright infringement in BitTorrent networks, which would include a partial upload of copyrighted content to the system from an IP address at a specific proven point in time. Thus, even without a complete copy of the

material, the infringer is still distributing copyrighted content to potentially thousands of other infringers world-wide and actively helping them to put together the complete movie file. Even if each peer would only provide a specific portion of the movie. A combination of a few peers working together are enough to provide the full file to everyone, while none of them may have a complete copy.

I declare under penalty of perjury of the laws of the United States of America that the foregoing is true and correct.

EXECUTED the 23rd day of November, 2017.

Ben Perino