Honorable Thomas S. Zilly

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

VENICE PI, LLC, Plaintiff, v. SEAN O'LEARY JR., et al. Defendants.	Civil Action No. 17-cv-988TSZ
VENICE PI, LLC, Plaintiff, v. JONATHAN DUTCZAK, et al. Defendants.	Civil Action No. 17-cv-990TSZ
VENICE PI, LLC, Plaintiff, v. MARTIN RAWLS, et al. Defendants.	Civil Action No. 17-cv-991TSZ
VENICE PI, LLC, Plaintiff, v. INA SICOTORSCHI, et al. Defendants.	Civil Action No. 17-cv-1074TSZ

LOWE GRAHAM JONES PLLC
701 Fifth Avenue, Suite 4800
Seattle, Washington 98104
206.381.3300 • F: 206.381.3301

VENICE PI, LLC, Plaintiff, v. GREGORY SCOTT, et al. Defendants.	Civil Action No. 17-cv-1075TSZ
VENICE PI, LLC, Plaintiff, v. YELENA TKACHENKO, et al. Defendants.	Civil Action No. 17-cv-1076TSZ
VENICE PI, LLC, Plaintiff, v. CELINA POTTER, et al. Defendants.	Civil Action No. 17-cv-1160TSZ
VENICE PI, LLC, Plaintiff, v. TONJA LAIBLE, et al. Defendants.	Civil Action No. 17-cv-1163TSZ
VENICE PI, LLC, Plaintiff, v. VICTOR TADURAN, et al. Defendants.	Civil Action No. 17-cv-1164TSZ

LOWE GRAHAM JONES PLLC
701 Fifth Avenue, Suite 4800
Seattle, Washington 98104
206.381.3300 • F: 206.381.3301

VENICE PI, LLC, Plaintiff, v. JESSE COOPER, et al. Defendants.	Civil Action No. 17-cv-1211TSZ
VENICE PI, LLC, Plaintiff, v. JASMINE PATTERSON, et al. Defendants.	Civil Action No. 17-cv-1219TSZ
VENICE PI, LLC, Plaintiff, v. DAVID MEINERT, et al. Defendants.	Civil Action No. 17-cv-1403TSZ

LOWE GRAHAM JONES PLLC
701 Fifth Avenue, Suite 4800
Seattle, Washington 98104
206.381.3300 • F: 206.381.3301

Bunting Digital Forensics, LLC
33579 Blue Heron Drive
Lewes, DE 19958
Phone: +1.302.260.2633
www.BuntingDigitalForensics.us

Expert Report – Testing of GuardaLey LTD's MaverickEye UB (MEU) Copyright Infringement Detection System

Prepared by: Stephen M. Bunting, EnCE, CCFT
CEO / Senior Forensic Consultant
Bunting Digital Forensics, LLC

DECLARATION OF STEPHEN M. BUNTING

I, STEPHEN M. BUNTING, DO HEREBY DECLARE:

1. My name is Stephen Michael Bunting. I am over the age of twenty-one (21), and I am competent to make this Declaration. I make this Declaration voluntarily and the facts stated herein are based on my personal knowledge and information.

2. I currently work as Director of Services for SUMURI, LLC and as independent forensic consultant as owner of Bunting Digital Forensics, LLC. Prior to that, I was a police officer from 1980 until 2009 with the University of Delaware Police from which I retired as a Captain. During the last ten years with the University of Delaware Police, I was in charge of the digital forensics and cyber investigations unit, that I founded. From 2009 until early 2013, I was a Senior Forensic Consultant with Forward Discovery, LLC, which in late 2012 was acquired by Alvarez and Marsal (NY) where I was a manager in the digital forensics division. I founded Bunting Digital Forensics, LLC in early 2013.

3. I have taken hundreds of hours of training in digital forensics, network forensics, and cyber investigations. I have provided training in the same topic areas, from beginner to expert levels, to members of various local, state, and federal law enforcement agencies and private sector examiners. I have trained like personnel internationally in over twenty-one (21) different countries. I have provided training, as either a part-time employee or contractor, for Guidance Software, Magnet Forensics, MicroSystemation, A.B., Organization of American States, and the U.S. Department of State Anti-Terrorism Assistance Program (Cyber Division). I have developed digital forensic or cyber training programs for several government and private entities.

4. I hold several industry-related certifications. I was the recipient of the 2002 Guidance Software Certified Examiner Award of Excellence for receiving the test score on my certification examinations. Among my varied certifications I am an EnCase Certified Examiner EnCE (Guidance Software), an AccessData Certified Examiner (ACE), Certified Computer Forensics Technician (HTCN), and a Certified XRY Instructor.

5. I am the principle author of *EnCase Computer Forensics - The Official EnCE: EnCase Certified Examiner Study Guide, 3rd Edition,* the co-author *Mastering Windows Network Forensics and Investigation, the author of EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide, 2nd Edition,* the co-author *Mastering Windows Network Forensics and Investigation 2nd Edition, the author of EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide, 3rd Edition* (all published by Wiley).

6. I have written numerous articles in the field of digital forensics over my career. Most recently I published two articles regarding spoliation examinations in which several peer-to-peer cases on which I have consulted were referenced in a hypothetical context:

Forensic Analysis of Spoliation and Other Discovery Violations - Part 2 of a 2-Part Series - Windows Examinations - eForensics Magazine - December 2016

Forensic Analysis of Spoliation and Other Discovery Violations - Part 1 of 2-Part Series - Macintosh Examinations - eForensics Magazine - October 2016

7. I have testified as a fact and expert witness numerous times in the field of computer forensics before state and federal courts in Delaware and New Jersey. I have submitted affidavits, as an expert in digital forensics, on many matters in several states, including Delaware, Georgia, and South Carolina.

8. No court has ever refused nor has any attorney ever challenged to accept my testimony on the basis that I was not an expert or not qualified in the field of computer forensics.

9. As a digital forensics examiner I have acquired and examined hundreds of computer systems and mobile devices for various local, state, and federal agencies, in addition to scores of private clients. The types of cases or examinations include: homicide, child-exploitation, fraud, Medicaid fraud, unlawful intrusion into computer systems (hacking), intellectual property theft, research fraud, email forgery, criminal impersonation, forgery, sexual harassment, peer-to-peer, and spoliation. I have acquired computer systems of many types, including servers, virtual servers, desktops, and laptops. I have acquired hundreds of mobile devices (feature phones and smart phones), both logically and physically. I also have acquired smart phones using JTAG and chip-off techniques, both of which require disassembly and working with the printed circuit boards inside a smart phone.

10. I have considerable experience with network-related cases, such as unlawful intrusions and peer-to-peer cases. I have investigated or provided digital forensics support to several unlawful intrusion incidents in both a law enforcement and a private sector capacity.

11. As a police officer I received specialized training in conducting peer-to-peer investigations by S.A. Flint Waters with the Wyoming Internet Crimes Against Children (ICAC) Task Force. S.A. Waters developed the Wyoming Toolkit, a customized version of Phex, a peer-to-peer client on the Gnutella network. I participated with members of the State of Delaware ICAC in this training program and afterwards in a task force conducting peer-to-peer investigations. Using the Wyoming Toolkit, we searched for child sexual exploitation images and movies on the peer-to-peer networks. When images were found, the software identified offending computers by their IP addresses [Note 1].

> Note 1: A public or internet routable IP address is a router or computer's address on the internet at a specific time. IP addresses uniquely identify a computer, as no two computers can have the same exact public, internet routable, IP address at the same time. If the address is that of a router, the computer typically has a private address

behind the router. In a typical home network, the ISP provides a 'box', which is often both a modem and a router / firewall / DHCP server. The router has a public or internet facing IP address assigned to it. On the back side of the router, several devices (computers, smart phones, etc) are connected using private addresses. Thus several devices in a home network share the public internet routable address assigned to the ISP's box (router). Other computers on the internet, including peer-to-peer software, see and use the public facing IP address assigned to the customer's router. The router routes network traffic for specific devices on the private side or behind the router using a protocol called NAT (Network Address Translation), thus assuring network traffic is sent to the correct computer.

IP addresses, as mentioned, are often time specific. These IP addresses are called dynamic IP addresses. They are assigned for certain periods of time, called leases. There is great variability in how often dynamic IP addresses change, but because they can and do change, the specific time of the offense is necessary to determine which subscriber was assigned a specific IP address at a specific time. ISP's maintain connection logs that record to whom a specific IP address is assigned and exactly when. By contrast, an IP address can be a fixed IP address. Even they can change and, as an investigator, you do not know which type a subscriber has and thus the exact time is always obtained and submitted to an ISP when requesting subscriber information.

The IP addresses hosting the illegal images are parsed by the toolkit using an IP geolocation database by which offending IP's are isolated or filtered to only those within our police jurisdiction. Once offending IP's were found in Delaware, we would request that the Attorney General's office submit subpoenas to the ISP (Internet Service Provider) for specific customer information and address of the offending IP address. As IP addresses are often time-specific, we submitted the exact date / time (along with time zone offset) for the offending IP address. The ISP would return to us the customer or subscriber information (name, address, account information,

etc.) for the ISP in question. We would investigate further and obtain a search warrant for the premises at which the IP was hosted. The search warrant would permit us to seize all media and electronic devices capable of holding digital media, as we did not know specifically which device behind the router was the offending device. The IP address detected by the peer-to-peer software was the public facing internet addressable IP address of the router, which is associated with the subscriber and their residence and not to a specific computer in the residence. Because it was a criminal investigation, we requested that the subscriber not be notified of the subpoena so that digital evidence would not be destroyed. Thus, in nearly all cases, the offending subscribers were surprised by the execution of the search warrant. In all the times that we did so, not once did the IP address lead to an innocent person's residence. Rather, we always found evidence therein of child sexual exploitation media on the computer system(s) therein.

12. I have found that the Wyoming Toolkit was a most reliable tool for identifying the IP addresses for peer-to-peer clients that were hosting child sexual exploiting images and video.

13. In my experience, the IP address's subscriber, or a family member thereof, is likely the offending party.

14. I have been involved in a case where the owner of the computer and charged party was professing his innocence, claiming someone else must have used his wireless network, citing a neighbor who reportedly engages in photography of a questionable nature. However, the evidence on his computer suggests otherwise. The software used by the investigators detected the name and version of the peer-to-peer software client involved, which happened to match the one found on his machine. Further, the same exact images detected by the investigative software were found on his machine. His claims were without merit and in direct contradiction to the overwhelming digital evidence found on his computer.

15. Unsecured wireless routers in homes used to be commonplace 15 years ago. In recent years, however, Internet Service Providers (ISP's) have undertaken great effort to provide and deploy secured wireless systems. Most "internet interface boxes" (combination modem / router / firewall / DHCP server) are preconfigured to operate with WPA2 security with a complex password already set. These devices are secure out of the box with strong encryption and complex passwords that are lengthy alpha numeric passphrases. Thus, valid claims of compromised home wireless systems today are, in my experience, rare compared to 15 years ago.

16. In the past, I have consulted with Computer Forensics, LLC in copyright infringement cases where spoliation was an issue. I'm familiar with the technology that was used in those cases to detect the copyright infringement offenders.

17. I have been retained by Voltage Pictures, LLC to provide digital forensic services and consulting in matters of copyright infringement. In anticipation of potential testimony in that regard, I have undertaken tests of the infringement detection software used, which is MaverickEye UB (MEU). This software and hardware platform is owned and run by GuardaLey, LTD, a German company located in Eggenstein, Germany. The CEO and Senior Developer at GuardaLey is Benjamin Perino.

18. Mr. Perino has written an export report describing the features and functions of this proprietary software, MaverickEye UB, or MEU, in detail. I have read that report in its entirety.

19. The manner in which MaverickEye works and the manner in which the software that I have used in my law enforcement capacity (Wyoming Toolkit) work to connect a peer-to-peer violation with an IP and subsequently with a subscriber are quite similar. In fact, MaverickEye UB, in my opinion, is much better with greater integrity features. Based on having read Mr. Perino's expert report on the function and features of the MaverickEye UB system, I note that the MaverickEye UB system is better because of the following: The law enforcement software

does not capture or retain any network packets, whereas MEU does. The law enforcement software does not use a WORM drive to store evidence, whereas MEU does. The law enforcement software is not housed or run in an ISO/IEC 270001:2013 compliant datacenter nor does it comply with PCI security specification, whereas MEU does.

20. I constructed and then conducted a test to determine the accuracy of the MaverickEye software as to its ability to detect an infringing party's IP address, identifying metadata (client software and version used by infringer), and identifying the known test files distributed on the torrent network.

21. To test the MaverickEye software, I created four video files, ones I created and owned from my archives. They were short clips of nature scenes, contained no people, and ones I could readily identify on site as being unique and ones I had in fact created. I embedded identifying metadata into these files, specifically my name, a description of the content, the data, and a statement that was placing them into the public domain. I also created MD5 and SHA1 hashes of each of the four files. A hash is an algorithm that produces a value that is best described as an electronic fingerprint. Files that are identical will have the same MD5 each time it is hashed. The slightest change by so little as one bit will produce a dramatically different hash value. Using this method, file integrity can be assured. Using two different hash algorithms eliminates any possible claims of hash value collisions.

22. I configured four different computers each with a different operating system and each with a different bit torrent client software. Bit torrent client software is used to share files over the bit torrent network using the bit torrent protocol. The below matrix, Table 1 below, shows the test configurations:

Computer	Operating System	Bit Torrent Client

Dell Laptop E6510	Linux Ubuntu 16.04 LTS	KTorrrent 4.3.1
Dell Laptop E5500	Windows 7 Professional	BitTorrent 7.10
HP Laptop Envy	Windows 10 Enterprise	uTorrent 3.5.1
MacBook Pro 15" 2016 Touch Bar	High Sierra OS X 10.13.2	Transmission 2.9.2

Table 1- The four test computers, their installed operating systems, and their installed bit torrent clients.

23. After configuring the above laptops, I installed and tested the latest version of Wireshark on each laptop. Wireshark is a software tool that captures the network packets that traverse or are transmitted over any particular network interface on the host computer. Thus, it is a means of recording the traffic over the network. I have used Wireshark and its predecessor, Ethereal, for many years in both my law enforcement and private sector careers. I have also trained others to use it.

24. On a fifth machine, not part of the test, I created torrents of the test or known movie files and allowed them to 'seed,' which means to share them on the torrent network and make them available for others to download. I took the four torrent files and physically placed them on the four test laptops, one unique file to each laptop. I started Wireshark on each test machine to capture the download and loaded the torrent files in each laptop's client software. In short order, each torrent file was able to locate the file and download it from the source machine that was initially sharing all four files. In so doing, the client software on each test machine was found to be working as designed. On each test machine, the newly downloaded movie file appeared to be identical to the original known files, as created. Each was found to contain the embedded metadata, including my name. To be absolutely certain the downloaded files were identical to the source files, each file was hashed and the hashes were found to be identical to those hashes the original files. The results are shown below:

Computer	File Name	MD5 Hash Original	MD5 Hash Downloaded onto Test Machines
Dell Laptop E6510	01CanadianGooseHenonNest.m4v	a13a318a02c32b0d1a8e276ae92227d8	a13a318a02c32b0d1a8e276ae92227d8
Dell Laptop E5500	02GeeseHonkingOK.m4v	6cdca839624df3e7c202766964394069	6cdca839624df3e7c202766964394069
HP Laptop Envy	03StripersJumpingOK.m4v	5ae4fbf8a2b73e131e3f8030ad99242c	5ae4fbf8a2b73e131e3f8030ad99242c
MacBook Pro 15" TouchBar	04WinterWetlandsOK.m4v	36c24f6d10c86df4994e435b055d01f9	36c24f6d10c86df4994e435b055d01f9

Table 2 - Test computers, the test or known file shared by each, and their hash values

25. At this point in the test, the only sources for these four files anywhere were the four test machines and the source machine on which they were created. The source machine torrent client (Transmission) was stopped, making the four test machines now the only sources. The HP Laptop and the MacBook Pro was shut down for the first phase of the test, leaving the two Dell laptops the only sources for the first two files in the list. At this point, I provided the four torrent files to Mr. Perino in Germany. He loaded the torrent files onto the MaverickEye UB system so that the system could attempt to locate the known test files on the torrent network, download them, and identify the IP address of the device responsible for distributing the files.

26. For the first phase of the test, the two Dell laptops were behind a firewall / DHCP server / router and would share the same public facing, internet-routable IP address. They could be distinguished by their port number for the connection, as well as by their bit torrent client and version number. The time was synchronized with a time server and the public, internet-routable address was checked and noted.

27. Once I was informed that the MaverickEye system (MEU) had been loaded with the torrent files, I took the third laptop (HP Envy) to another location to use a different network configuration. The laptop was connected to a network at which I had an account and was configured directly with a public internet-routable IP address, such that the IP address of the laptop itself would be exposed directly to the internet. The time was synchronized with a time server and the public, internet-routable address was checked and noted. After running the test for a little more

than an hour, I was informed that the MEU system had detected all three files thus far placed into the torrent network. I shutdown the HP Envy laptop and returned to my original location where the first two laptops were still running the torrent clients.

28. I connected the fourth laptop to the original network, adding a third machine to the public IP address shared by the first two laptops. The fourth laptop was a MacBook Pro and was sharing the fourth file. The time was synchronized with a time server and the public, internet-routable address was checked and noted. Late in the afternoon, I was notified that all four files had been detected by the MEU system and that the test was concluded.

29. Mr. Perino sent me, via email, a copy of the network packet [Note 2] captures (PCAP files) and a spreadsheet summarizing the captures. In addition, he sent me copies of the four files that the MEU downloaded based on the torrent files that I send to him.

[Note 2] – Information sent over a network travels in packets. Each packet contains, among other data, a destination IP address, a destination port, a source IP address, and a source port. Thus, every packet contains what amounts to a delivery address and a return address, to make this somewhat analogous to the postal system by which mail travels. A stream of packets constituting a bit torrent download will often contain thousands of packets, each and every one of them containing source and destination IP addresses. As those packets also contain the file data of the bit torrent file, the source IP address for packets containing the file data itself is demonstrable evidence of the source of the file captured by the MEU system. A bit torrent network shares files on a peer-to-peer basis, meaning the two computers actually connect to each other. Hence the destination and source IP's represent the two computers involved in this file sharing. Further, these packets travel via a TCP protocol, which is a guaranteed delivery system. If a packet sent is not acknowledged as received, it is sent again and again, until it either is acknowledged or times out and fails.

30. For all four files, the MEU system captured the public, internet-routable IP address for the source of the test or known files that I was sharing on the bit torrent network. I knew exactly what the IP addresses were, as I had recorded them before and after the downloads. The IP addresses involved were dynamic IP addresses and thus time sensitive. The ISP's for those IP addresses maintain logs that record which subscriber or user is assigned a particular IP address at a particular time. Had a subpoena been served on either of the two different ISP's used in this test, I would have been correctly identified as the responsible subscriber / user at those exact times for those involved IP addresses.

31. Further, the MEU correctly captured the exact name of the bit torrent client and version numbers that were in use by each test computer. This capture is possible because when the MEU first connects to the computer hosting a file to be shared on the bit torrent network, a handshake occurs. Each machine's bit torrent client sends a packet to the other stating, among other things, their peer ID. Part of the peer ID is the name of the bit torrent client followed by its version number. Table 3, below, is a copy of Table 1, above, with an added column at the right showing the Bit Torrent client and version number as it was exchanged in the handshake. You can see that they were correctly identified in each instance.

Computer	**Operating System**	**Bit Torrent Client**	Bit Torrent Client Captured by MEU
Dell Laptop E6510	Linux Ubuntu 16.04 LTS	KTorrrent 4.3.1	KT4310
Dell Laptop E5500	Windows 7 Professional	BitTorrent 7.10	BT71000
HP Laptop Envy	Windows 10 Enterprise	uTorrent 3.5.1	UT351S
MacBook Pro 15" 2016 Touch Bar	High Sierra OS X 10.13.2	Transmission 2.9.2	TR2920

Table 3 - The 4th column shows the bit torrent client and version number, as captured in the handshake, which

corresponds currently with the installed client.

32. As previously mentioned, the MEU captures the source port number in addition to the source IP address, as they are parts of the 'address' of each packet. I confirmed that the port numbers captured by the MEU system were accurate. I did this by spot checking packet captures on both systems. By that, I mean that packets sent and received from a test machine are captured as they are sent. Simultaneously, packets sent and received on the MEU system are likewise captured. As the two machines are connected, peer-to-peer, and the MEU is downloading a file from the test machine, the packets sent and received between the machines are the same packets of data and are being captured simultaneously. Thus, one can examine packets from both machines and can identify them as one and the same. I did this with several packets and this confirms positively that the MEU is accurately reporting the source IP address and other metadata (port numbers, client name, & client version). While making these packet comparisons, I examined the TCP (Transmission Control Protocol) layer of the packets, wherein the port numbers are found and noted that the port numbers are being correctly reported. Figure 1, below, shows the TCP layer information. The top one is from a packet captured on the MEU system, showing the Destination Port for this packet as 54702. The bottom one is from a packet captured on the Windows 10 test laptop (HP Envy). The Destination Port for this packet is also 54702.

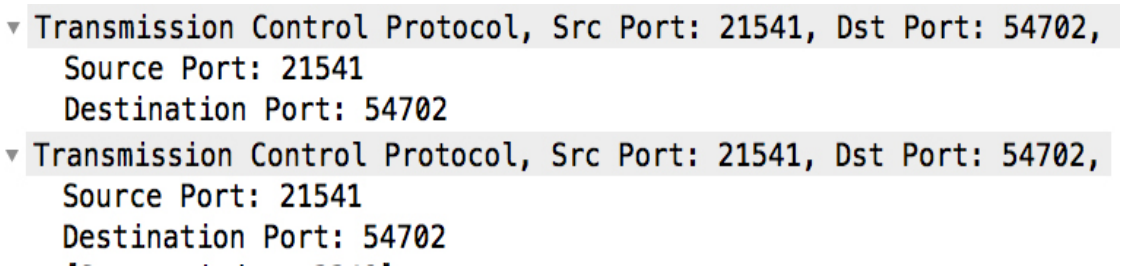


Figure 1 - TCP layers from MEU on top and Windows 10 test machine on bottom. Port numbers match and are being correctly reported by MEU

They are identical and should be for the connection to have been successful. Packets are sent back and forth during a file sharing exchange, regardless of which party is downloading. In this case, the MEU is requesting a segment of the file that is being shared by this machine and identifies it by an index number. The Windows 10 test laptop (HP Envy) machine is using port 54702 for its client (UTorrent) to share files. So, when the MEU sends the request to the Windows 10 test machine, the destination port is 54702. When the Windows 10 test machine sends a packet to the MEU, the Windows 10 machine then becomes the source for the packet and thus the port would be listed as the source port. Thus, the MEU network packet captures are correctly reporting the port on the computer hosting the shared file that is also being identified by its IP address. As the MEU system is obtaining the port information from the network packets and, since the packets are reporting correctly (matching on both sides of the transmission), the summary report from Mr. Perino is listing port 54702 for this particular download is, as to be expected, correct and accurate.

33. Whenever the MEU was connected to my torrent clients to download from them, never did I see it offer any portion of the file to share. At all times it listed it as 0% available when using the inspector to look at connected peers. At one point after the regular test was concluded, I allowed one test machine to download all four files so they could be shared and subsequently detected by the MEU again, this time via a VPN. At that point, minimally, those four files were present on the one source machine on my network and also on the MEU, as all four had been detected and downloaded onto the MEU software. Since I was requesting those same files, were the MEU sharing files it has downloading, it would have responded as a normal torrent client would have responded and allowed my client to download them. The MEU did not connect and provide any download to my test laptop that was seeking those four files for download. Rather, they were downloaded only from sources within my local network of test machines. Thus, based

on the observation I made during a test, I agree with Mr. Perino's description of the MaverickEye software in that it only downloads from clients offering files to share and does not share any files in return.

34. To protect my privacy and to preserve the integrity and confidentiality of the MEU system, no IP addresses for those systems are being specified in this declaration nor are any screen captures of those IP addresses by shown.

35. As previously stated, Mr. Perino provided copies of the test or known files that were downloaded from the test machines by the MEU system. I examined those files and, on visual inspection, I identified them as the same files that I had prepared for this test. I looked inside the files and noted that the metadata was still present exactly as I had inserted the data, including my name. Next, I hashed the known or test files provided by Mr. Perino using both MD5 and SHA1 hashing algorithms. I compared the hashes from the MEU download to the hashes in the original set and found them to be identical. Thus, the files downloaded by the MEU from the test machines, via the bit torrent (peer-to-peer) network were identical, bit-for-bit copies of the original source test or known files.

36. I have concluded, based on this test, that the MaverickEye UB (MEU) infringement detection software works and accurately identifies the IP address of the device responsible for sharing of a particular file on the bit torrent network and the exact time of the violation. The MEU connects to the computer hosting a file that is being shared, peer-to-peer (computer-to-computer). The MEU downloads that file or portions of that file. In our test case, it downloaded the entire file from the test machines, as they existed nowhere else. The files downloaded by the MEU from the test machines were identical in all regards. The hash values matched, proving they were bit-for-bit, identical copies. The MEU captures and retains the network packets involved in the file sharing process, as such network packet captures were made and provided to me as part of the test. Those

network packets contain, among other data, the actual data (shared file content) from the machine that is sharing the file, along with the IP address of the computer sharing that data. MEU will, in fact, often capture hundreds or thousands of packets of data, with each and every packet identified by and containing the violator's IP address, bit torrent sharing port, bit torrent client, and bit torrent client version. Each packet captured will contain the exact time that the packet was transmitted. Per Mr. Perino's expert report, MEU's time is being synchronized with an atomic clock for accuracy. The MEU will not capture every file being shared on the bit torrent network, but for those it is configured to monitor and does capture, that data capture will, in my opinion and based on my testing, accurately identify the public facing, internet-routable IP address of the device sharing that file, as well as the exact time the file was shared. Likewise, it will, in my opinion and based on my testing, also identify the port used by the bit torrent client on the internet facing device if not the computer itself, the actual name of the bit torrent, and the version number of that bit torrent software. Furthermore, based on my testing, the MEU performed accurately regardless of the operating system or the torrent client being used.

37. Based on a combination of my testing and of my understanding of the features and function of the MEU system, having read Mr. Perino's expert report on the MEU system, I am of the opinion that it was designed to maintain the accuracy and integrity of the evidence throughout. For example, as per Mr. Perion's export report, the MEU:

- Captures and retains the actual network packets whereby a file is downloaded from a copyright infringement violator. As noted previously each and every one of those packets identifies the source IP address of the violator and the exact time.
- Said captures are stored on a WORM drive. A WORM drive is a Write Once, Read Many drive, meaning once the evidentiary network packets are written to the drive, they cannot be altered, thus maintaining evidentiary integrity.

- WORM drives containing evidence are stored in a vault
- A log is automatically maintained of each copyright infringement violating download that occurs
- Time accuracy is maintained by synchronization with an atomic clock
- MEU is housed in an ISO/IEC 270001:2013 compliant datacenter
- MEU complies with the PCI security specification

38. As to the possibility of the MEU yielding false positive, I have read Mr. Perino's expert report, specifically section B, items 26, 27, 28, and 29, which deal with "TCP/IP Connections cannot be spoofed and cannot yield false positives." I concur with his statements in 26, 27, 28, and 29.

39. With regard to item 26, it is important to understand that the bit torrent protocol is a peer-to-peer file sharing protocol. Peer-to-peer means just that, a computer-to-computer connection. This means that files or portions of files are shared by direct connections between computers. When a direct connection occurs and packets are exchanged, the destination and source IP addresses of the two connected computers are found in the packets that are exchanged. They must be for the connection to be established and the stream of packets containing the file segments to transmit. Each and every packet contains the IP address of the sender and receiver (source and destination) and this goes for every packet involved in the transaction, not just those containing data. The TCP protocol is, as previously mentioned, an assured delivery system in that packets sent must be acknowledged as received. All the traffic associated with that acknowledgement process also must contain the IP addresses of the sender and receiver.

40. With regard to item 27, IP spoofing can be done by an experienced network specialist. Specially crafted network packets can be used to create denial of service attacks, but these packets are small and usually involve repeatedly sending the same small crafted packet over

and over again, creating a flood of messages that results in a denial of service attack. Creating a few small, specially crafted packets that are sent repeatedly is a completely different task than trying to do so for a bit torrent stream, where tens of thousands of packets, mostly all different, are involved.

41. With regard to item 28, Mr. Perino is accurate in his assessment of complexities and enormity of the task that would be involved in trying to do an IP spoof of a bit torrent stream. In a practical sense, a very technically adept person would have to know a victim's IP address. This person would have to physically connect a computer into the same network segment as the intended victim in order to intercept the network traffic involved. Doing so would involve considerable knowledge and skills, in and of itself, and could involve illegal access to a building or ISP network equipment. The person would need to have the file in question on their computer, be sharing it using bit torrent software, and have some software or code capable of or rewriting tens of thousands of bit torrent packets on the fly, as any delay could cause a time-out. While many things are theoretically possible, I am unaware of any such software being available. Such an endeavor would involve tremendous effort and resources. In addition, the person would have to know that a particular file was being monitored for copyright infringement downloading. And finally, such a person would have to have a very strong motivation to undertake such a task and to target a particular person and/or IP address. Considering all that would be involved in such an endeavor, it is so unlikely to occur as to be nearly impossible, as Mr. Perino states.

42. With regard to item 29, often IP spoofing, as described above, is interpreted or confused by many, including Google's search engine, with IP address hiding. If you search for "IP spoofing software," you will find most of the hits will involve VPN (Virtual Private Network) software. VPN software allows the user of a computer to create an encrypted tunnel to a VPN server from which the internet traffic emerges unencrypted. The VPN server's internet facing IP

address also becomes the user's public internet-routable IP address. It acts as a proxy and is your frontend IP or point of presence IP on the internet. All network traffic between the user and the VPN server is encrypted. VPN's are intended for privacy of a user's internet traffic and also for protecting the identity of their IP address. A proxy server is similar in function to a VPN server. The major difference is that there is no encrypted tunnel between the user and the proxy server. The proxy server still serves, however, as the user's frontend IP or point of presence IP on the internet. A proxy server is not as secure as a VPN server because there is no encrypted tunnel. A proxy server is, however, faster than a VPN server because encryption requires time resources to achieve and results in slower network speeds, all other things being equal. If a VPN or a proxy server is used to engage in bit torrent file sharing, the MEU will see the source IP of the infringer as the public facing, internet routable IP address that of the VPN or proxy server, as that is the user's IP address, by proxy. This is not a false positive by any definition. Rather, the MEU is capturing packets that contain the source IP for the file as that of the VPN or proxy. When a VPN or proxy is being used, MEU can only trace the connection to the front-end or public-facing, internet routable IP address, which is accurate to that point. To obtain the IP of the user behind the VPN or proxy who is responsible for download, the VPN or proxy server owner or manager would have to be contacted. If they maintain logs, and many quite intentionally do not, the connection to the source can then be identified through the subpoena process. Because the front-end interface to the MEU used by plaintiff's counsel only has filters for known ISP's (Comcast, Verizon, AT&T, etc), IP addresses for VPN's and Proxy services are not in those filtered groups and will not be visible.

43. With regard to item 29, I conducted a separate test, after concluding the one described above whereby I configured one laptop (MacBook Pro – High Sierra) with a VPN service. With the VPN enabled, I launched Transmission (bit torrent client) and shared all four test

or known files. I noted the public, internet-routable, frontend IP address in use by the test computer. After running this bit torrent configuration overnight using the VPN service, Mr. Perino reported to me that the MEU captured and downloaded the known or test files from the IP address that I had recorded for the computer. It was, as expected, the IP address of the VPN server. Thus a test of the scenario, as described by Mr. Perino in item 29, it absolutely correctly stated and accurate.

44. When a user adds a torrent file for a file that they want to download, the "Trackers" that are included in the torrent file actively work to connect torrent clients that have either all or parts of a requested file with those seeking those files. In doing so, the IP addresses and port numbers, along with other metadata are shared, visible, and otherwise made public within that 'swarm' of torrent users. It is by this mechanism of identifying each computer in the swarm by its IP address and port number that computers in the swarm can connect directly to one another and share parts of the file. It is also by this mechanism that MEU system can see the public IP addresses and port numbers of copyright infringers and connect directly with them to download files and capture evidence of copyright infringement. Such a process is akin to going to a coffee shop and asking if anyone in the room has sugar on their table, as you do not. Perhaps you want 6 packets of sugar and you need a a packet or two from several tables to get your 6 packets. The conversations that take place during this discovery and sharing process are very much out in the public for all in the coffee shop to hear. There is no expectation of privacy when such a request is made. Anyone in the coffee shop can see who you are and hear what it is that you are requesting. The swarm works much the same way. Once you announce that you want a file, the trackers in that torrent file being asking other users if they have that file, sharing your IP and port, and thereby facilitating the download of segments of the requested file from many users in the swarm. It matters not where the various torrent clients are located, as the internet is global and crosses nearly all country boundaries. In this case, the MEU happens to be in Germany, but could be anywhere. The simple

fact is that if you wish to join a peer-to-peer, file-sharing network, you have to share your IP address and port with those in that public pool of persons doing likewise. You are agreeing to and consenting to allowing others to connect to your computer in order that you can exchange files. As with asking for a packet of sugar in a crowded coffee shop, those in a swarm will hear your request and know who you are by your public routable IP address.

45. In Mr. Perino's expert report, in number 44, he defines what Bitfield is within the context of the bit torrent network. Each shared file is divided into 16 KB segments or blocks and is shared in increments of 16 KB segments. If a file consists of 5,000 segments and a user had 2,500 segments, that user has 50% of the file and would show a Bitfield value of 50%. When I conducted the test, each of the four laptops had one of each of the four files in its entirety (100%) on each of the laptops. The summary report provided by Mr. Perino after the test showed that the MEU system accurately detected that each of the four files had a Bitfield value of 100%, meaning each laptop had the entire test or known file.

46. Attached hereto as Declaration Exhibit 1 is a true and accurate copy of my Curriculum Vitae which truly and accurately represents my relevant employment history, training, experience, certifications, and expert-witness experience.

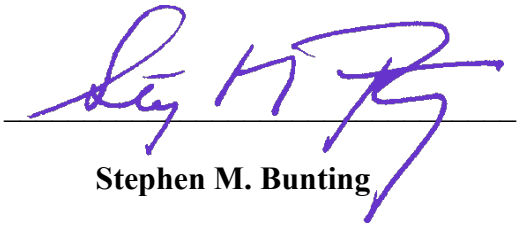
47. I am paid on an hourly basis by Voltage Pictures, LLC at the rate of $250 / hour for my digital forensics services.

FURTHER DECLARANT SAYETH NAUGHT

DECLARATION

PURSUANT TO 28 U.S.C SS 1746, I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed February 2, 2018.

By: 

Stephen M. Bunting

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document has been served to all counsel or parties of record who are deemed to have consented to electronic service via the Court's CM/ECF system, and to all Defendants at their last known address via U.S. mail.

s/ David A. Lowe

LOWE GRAHAM JONES PLLC
701 Fifth Avenue, Suite 4800
Seattle, Washington 98104
206.381.3300 • F: 206.381.3301