UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

MALIBU MEDIA, LLC,	:	
	:	Civil Action No. 2012-2078
Plaintiff,	:	
	:	Consolidated from Cases:
vs.	:	2:12-cv-02078-MMB
	:	2:12-cv-02084-MMB
JOHN DOES 1, 6, 13, 14, and 16,	:	5:12-cv-02088-MMB
	:	
Defendants.	:	

DECLARATION OF PATRICK PAIGE

I, PATRICK PAIGE, DO HEREBY DECLARE:

1. I am a founding member of Computer Forensics, LLC. A copy of my CV is attached hereto as Exhibit A.

2. I am over the age of 18 and am otherwise competent to testify.

3. I received a hard drive from Lipscomb, Eisenberg and Baker, PL ("LEB"). The hard drive was marked with a note stating Doe 16 Atty Ronald Smith. In this declaration, I refer to this hard drive as the "First Hard Drive."

4. The First Hard Drive is a three terabyte hard drive manufactured by Seagate and is marked by the manufacturer with the following serial number: W1F1GX0Q. It is enclosed in a Thermaltake external USB3 hard drive enclosure.

5. I connected the First Hard Drive to a Tableau TD3 forensic device. TD3 forensic devices are widely used by computer forensic experts. TD3 forensic devices support collecting data in a forensically sound (a.k.a. "write-blocked") manner.

6. The TD3 forensic device created a forensically sound copy of the First Hard Drive. All work which was performed on the First Hard Drive was done on the forensically sound copy. A forensically copy is one that has an identical Hash Value to the original.

7. EnCase Forensic software is widely used by computer forensic experts who need to conduct efficient, forensically sound data collection and investigations using a repeatable and defensible process.

8. EnCase Forensic has the ability to open and analyze a broad range of operating systems and file system artifacts including but not limited to Windows, Linux, Solaris, AIX and OSX operating systems (OSX is used by Apple computers).

9. In short, EnCase Forensic is able to open and analyze almost every type of operating system used to run a personal computer.

10. I used the EnCase Forensic software to attempt to open and analyze the First Hard Drive.

11. EnCase Forensic software was unable to open or read the First Hard Drive.

12. Subsequently, I used a software program called Active Partition Recovery. Active Partition Recovery is a program used by computer forensic professionals to recover data from a hard drive that is not formatted or partitioned correctly.

13. Through the use of Active Partition Recovery, I was able to see that the First Hard Drive contains images of three computers, among other files. And, that the images of the three computers were made between December 16, 2012 and December 22, 2012.

14. Active Partition Recovery did not, however, enable me to open or read the images of the computers. Instead, the report generated by Active Partition Recovery indicated that there were a large number of “poor” partitions. When a hard drive has “poor” partitions, the files on it

are usually not recoverable. Active Partition Recovery did recover some files. However, the files that Active Partition Recovery did recover would not open and were corrupted.

15. Ultimately, in late April 2013, I concluded that the First Hard Drive was completely or very nearly completely unreadable because it was not partitioned correctly.

16. Between May 6 and May 7, 2013 (it took 15 hours and twenty minutes), I calculated the SHA-1 Hash value of the First Hard Drive. The SHA-1 Hash Value of the First Hard Drive is: SHA-1: 81712cce5f9fea430367367797f2c871e4a609a7. Simultaneously, I created another forensically sound copy of the First Hard Drive. The Hash Value of that copy is: SHA-1: 81712cce5f9fea430367367797f2c871e4a609a7.

17. Hash Values are often analogized to a finger print for a piece of data. Each unique piece of data has an unique Hash Value; and, identical copies of a unique piece of data will have the same Hash Value.

18. Since the SHA-1 Hash Value of Hard Drive One and the SHA-1 Hash Value of the copy are identical, I can conclusively state that the original and copy are identical.

19. On May 9, 2013, via Federal Express, I sent the original First Hard Drive to:

Ronald A. Smith, Esq.
1617 John F. Kennedy Blvd.
Suite 355
Philadelphia, PA 19103

20. On May 9, 2013, I received a second three terabyte hard drive from LEB (the "Second Hard Drive.")

21. The Second Hard Drive is a three terabyte hard drive manufactured by Seagate and is marked by the manufacturer with the following serial number: W1F0XKSK. It was enclosed in the original box with matching serial number.

22. Upon receiving the Second Hard Drive, I connected it to the Tableau TD3 forensic device.

23. I created a forensically sound copy of the Second Hard Drive by using the TD3 forensic device. All work which was performed on the second hare drive was done on the forensically sound copy.

24. The Second Hard Drive contains the following files and folders:

Name
FILE desktop-1tb.img
FILE desktop-1tb.img.zip
FILE desktop-240gb.img
FILE desktop-240gb.img.zip
FILE external.img
FILE external.img.zip
FILE img-sha512-sums
FILE One.zip
FILE pi.img.zip
FILE sq-laptop.img
FILE sq-laptop.img.zip
FILE work-mac.img
FILE work-mac.zip
FILE work-thumb.img
FILE work-thumb.img.zip
FILE zip-sha512-sums
FOLDER J:\.Trash-999\
FOLDER J:\One\
FOLDER J:\pi.image\

25. The Second Hard Drive is not a copy of the First Hard Drive.

26. Indeed, the SHA-1 Hash Value of the Second Hard Drive is: 1c8b557c1c78008b7e0ea60fdc7ad5207cd7b18c which does not correspond to the SHA-1 Hash Value of the First Hard Drive. The difference in the SHA-1 Hash Values conclusively establishes that the Second Hard Drive is not a copy of the First Hard Drive.

27. The images listed in paragraph 24 described as:

(a) Desktop-240gb.im and Desktop-240gb.img.zip

(b) Sq-laptop.img and Sq-laptop.img.zip

(b) Work-mac.img and Work-mac.zip

contain images of what appear to be a working computer systems based on their file structures.

28. LEB informed me that John Doe 16 testified that he built a computer with a 1 Terabyte Hard Drive. Further, that among other things, that he plays computer games on that machine. And, that the 1 Terabyte computer is a stationary computer located in an office in his home.

29. The images titled desktop-1tb.img and desktop-1tb.img.zip do not contain a copy of a working computer system. The image desktop-1tb.img.zip is a copy of desktop-1tb.img that has been compressed.

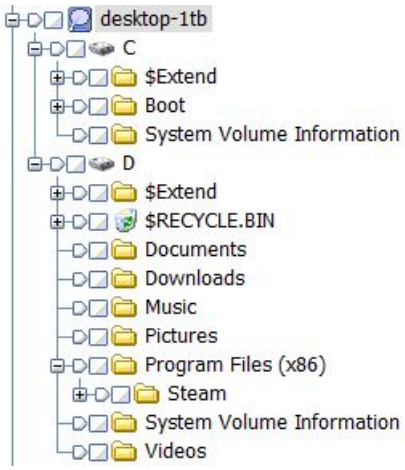
30. The only images of a computer with a one terabyte hard drive on Hard Drive Two are desktop-1tb.img and desktop-1tb.img.zip. Since they are the same, for the remainder of this declaration, I will refer to the images of these two drives as the "1 Terabyte Hard Drive."

31. After analyzing the 1 Terabyte Hard Drive, I can state with one hundred percent (100%) certainty that it has so many files and folders missing from it that if it was installed into John Doe 16's physical computer it would not boot up. Instead, one would only see a blank screen.

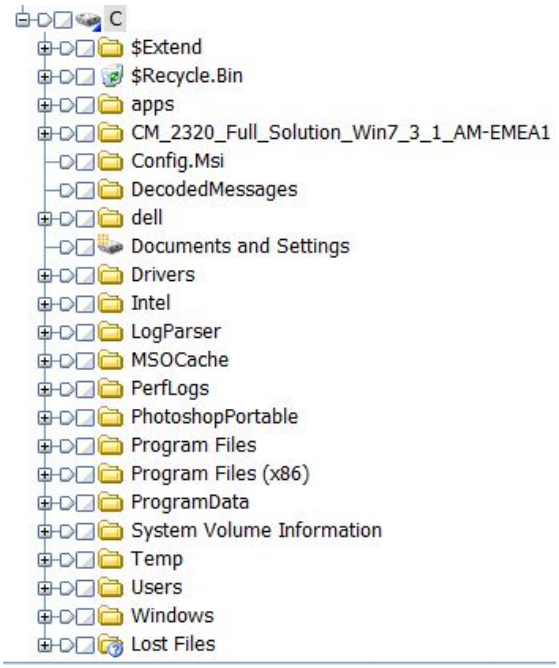
[Remainder of page left intentionally blank.]

32. This is because the 1 Terabyte Hard Drive is missing all of the files for Windows and all of the Program Files and User folders. See:

The 1 Terabyte Hard Drive



Normal Hard Drive



33. As you can see, a normal hard drive has a Windows folder. The Windows folder is not on 1 Terabyte Hard Drive. I know Windows was installed on the 1 Terabyte Hard Drive at some point because it has the core system files that correlate to Windows.

34. Windows is an operating system. Without an operating system, a computer will not function. The 1 Terabyte Hard Drive does not have ANY operating system.

35. When Windows is first installed on a hard drive it installs the core system files needed to run the operating system. The core system files are hidden system files.

[Remainder of page left intentional blank.]

36. The file creation date of the core system files including the Master File Table (MFT) indicate the First Hard Drive was formatted and first put into use on November 11, 2012. See:

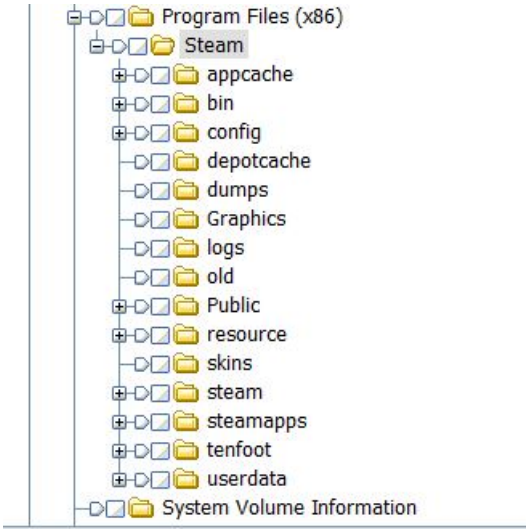
	Name	File Created
7	MFT Allocation Bitmap	
8	Volume Slack	
9	$RECYCLE.BIN	11/11/12 09:38:41AM
10	Program Files (x86)	11/11/12 11:17:20AM
11	Downloads	11/11/12 11:29:30AM
12	Documents	11/11/12 11:29:53AM
13	Music	11/11/12 11:30:28AM
14	Videos	11/11/12 11:30:39AM
15	Pictures	11/11/12 11:32:49AM
16	$AttrDef	11/11/12 12:03:41PM
17	$Boot	11/11/12 12:03:41PM
18	$BadClus	11/11/12 12:03:41PM
19	$LogFile	11/11/12 12:03:41PM
20	$Secure	11/11/12 12:03:41PM
21	$MFTMirr	11/11/12 12:03:41PM
22	$MFT	11/11/12 12:03:41PM
23	$Bitmap	11/11/12 12:03:41PM
24	$UpCase	11/11/12 12:03:41PM
25	$Volume	11/11/12 12:03:41PM
26	$Extend	11/11/12 12:03:41PM
27	System Volume Informat...	11/11/12 12:22:25PM

37. LEB informed me that Plaintiff propounded a request for production of documents on November 8, 2012 seeking John Doe 16's hard drive.

38. Based upon the foregoing, I can state with 100% certainty: (a) the 1 Terabyte Hard drive was not in use prior to November 11, 2012; or (b) all of the data that had previously been on the 1 Terabyte Hard Drive had been erased prior to November 11, 2012. Put another way, the 1 Terabyte Hard Drive was either new or reconditioned to a like new state.

[Remainder of page left intentional blank.]

39. The only program that was installed on the 1 Terabyte Hard Drive is called Steam. See:



40. Steam is a program used for on-line gaming.

41. The only way Defendant could have used Steam is if he had the 1 Terabyte Drive connected to another computer that had a functioning operating system.

42. When data is deleted from a computer running a Windows operating system, the data remains on the hard drive until the operating system overwrites that area. The deleted data will then reside in an area of the hard drive commonly referred to as unallocated space.

43. Approximately ninety-nine percent (99%) of the unallocated space on desktop-1tb.img contains zeros, i.e. no data. After reviewing the legible data in the unallocated space, all of it appears to relate to Steam.

44. In a normal computer, the unallocated space would have deletions from search engines, such as Google, Bing, Ask Jeeves, etc., emails, Word documents, Window system file updates, pictures, etc. In short, in would be filled with all the data a normal computer user routinely deletes. The 1 Terabyte Hard Drive does not have any of this expected data.

45. A typical computer which has been in use by a typical computer user for any substantial length of time would have much more than 1% of the unallocated space filled up by deleted data.

FURTHER DECLARANT SAYTH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 17th day of May 2013.

By: Patrick Paige Digitally signed by Patrick Paige DN: cn=Patrick Paige, o=Computer Forensics LLC, ou, email=patrick@patrickpaige.com, c=US Date: 2013.05.17 12:36:23 -04'00'

PATRICK PAIGE