

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----X  
:
  
GUCCI AMERICA, INC. :
  
:
  
Plaintiff, :
  
:
  
-against- :
  
:
  
FRONTLINE PROCESSING CORPORATION; :
  
WOODFOREST NATIONAL BANK; DURANGO :
  
MERCHANT SERVICES LLC d/b/a NATIONAL :
  
BANKCARD SYSTEMS OF DURANGO; ABC :
  
COMPANIES; and JOHN DOES, :
  
:
  
Defendants. :
  
:
  
:
  
:
  
:
  
:
  
:
  
:
  
:
  
-----X

09 Civ. 6925 (HB)

**DECLARATION OF SETH LEONE**

**I. Introduction**

1. I am an employee of Stroz Friedberg, LLC (“Stroz Friedberg”), which has been retained by Gibson, Dunn & Crutcher LLP (“Gibson Dunn”) and its client Gucci America, Inc. to provide forensic analysis and technical consulting services in connection with Gucci’s action against Durango Merchant Services, LLC, captioned above. I have personal knowledge of the facts set forth below, and if called upon to do so, could and would competently testify thereto.

2. This declaration addresses Stroz Friedberg’s forensic analysis of three forensic images or copies of hard drives used by Nathan Counley and William Demopolis.<sup>1</sup> As

---

<sup>1</sup> I submit this declaration for the limited purpose of describing Stroz Friedberg’s analysis to date related to the use of the Lavasoft File Shredder program on the three computers. Accordingly, my discussion does

discussed in greater detail herein, Stroz Friedberg determined that a data “wiping” program, Lavasoft File Shredder, was installed on all three computer hard drives. In addition, there is evidence that the File Shredder program was executed at least 28 times on the three computer hard drives between May 20, 2010 and June 28, 2010 for the purpose of securely deleting or “wiping”<sup>2</sup> data stored on these hard drives from areas including the Recycle Bin, temporary folders, and unallocated disk space.

## **II. Background**

3. Stroz Friedberg is a technical services and consulting firm that provides services in the areas of digital forensics; electronic data analysis, preservation, and production; computer crime and abuse investigation; and computer and infrastructure security. Founded in 2000, the company is managed by former federal prosecutors, former federal special agents, and local law enforcement officers with government and private sector experience in traditional and cyber-related investigations and prosecutions, complex civil litigation, computer forensics, data preservation and analysis, and infrastructure protection. Our staff of computer forensics examiners, electronic discovery specialists, and electronic security professionals joined Stroz Friedberg following careers in, among other places, law enforcement, Big Four consulting practices, the intelligence community, and academia.

4. I am an Assistant Director of Digital Forensics in Stroz Friedberg’s New York office. In my position, I assist in overseeing the firm’s forensic operations in New York,

---

not address all analyses that I have performed or may perform in the future related to Lavasoft or other investigations requested in connection with these computers.

<sup>2</sup> The terminology used by the Lavasoft File Shredder application is “shred”, although that term frequently is used interchangeably with “wipe” or “overwrite”.

assign projects to examiners, and perform forensic examinations. I have been employed by Stroz Friedberg since 2003. Prior to joining Stroz Friedberg, I worked since 1999 as a Security and Network Consultant for numerous public and private sector clients, where I led various projects from network design and implementation to intrusion detection and incident response. At Stroz Friedberg, I have conducted hundreds of forensic examinations and acquisitions, including examinations and acquisitions of laptop and desktop computers, and I have managed and led many large-scale electronic discovery and incident response matters. I am a Certified Information Systems and Security Professional (“CISSP”), an EnCase Certified Forensic Examiner (“EnCE”) and GIAC Certified Forensic Analyst (“GCFA”).

5. In the course of this engagement, Gibson Dunn requested that Stroz Friedberg perform forensic analyses of one computer hard drive used by William Demopolis and two computer hard drives used by Nathan Counley. We were asked to review forensic images of these hard drives for, among other things, evidence of the installation and/or use of a data wiping program, identified as Lavasoft File Shredder, to confirm that the software was installed, to determine if the program was executed and, if so, the number of times it was executed, and to identify or quantify, if possible, any data that may have been wiped from these computer hard drives.

6. Stroz Friedberg received three computer hard drives from other forensic firms retained by Gibson Dunn. These three drives were forensic images or copies of a computer hard drive used by William Demopolis and two computer hard drives used by Nathan Counley. In my review of these copies, I verified that the image of William Demopolis’s computer (hereinafter “the Demopolis Hard Drive”) is a true, accurate, and

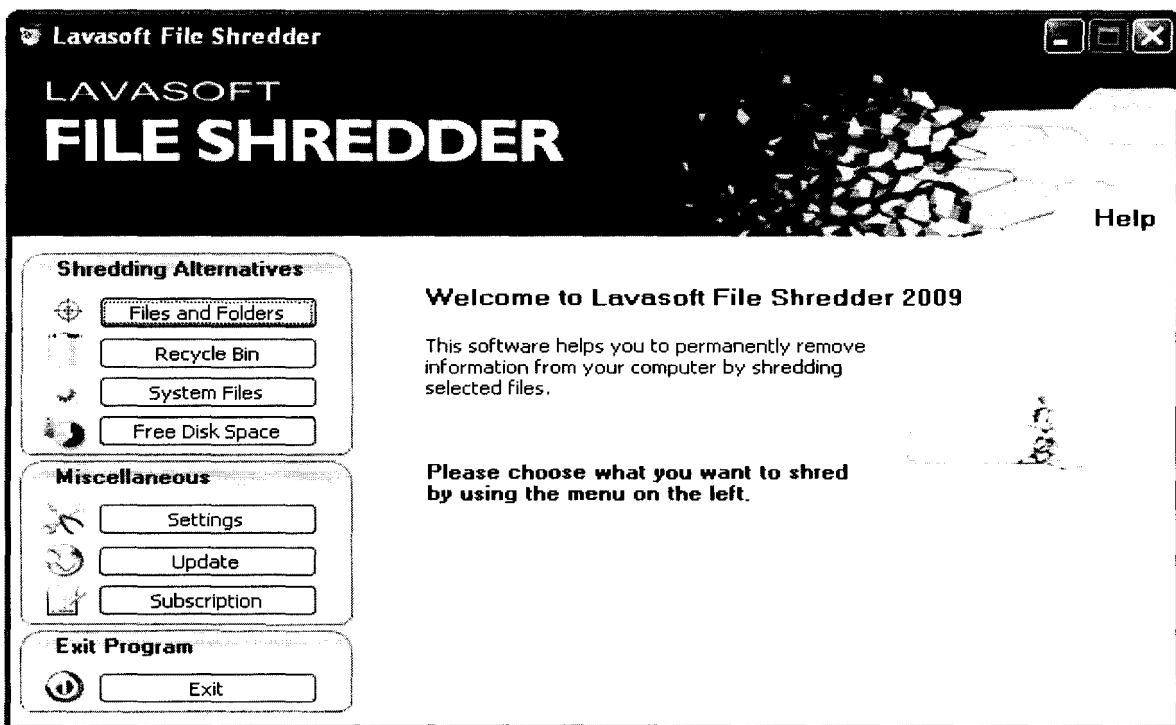
complete copy of all data that resided on the original Demopolis hard drive. Similarly, I verified that the two forensic copies I received of the hard drives used by Nathan Counley (hereinafter “Counley Toshiba Laptop” and “Counley Asus Laptop”) are true, accurate, and complete copies of the original hard drives.

### **III. Overview of Lavasoft File Shredder**

7. Lavasoft File Shredder is a data wiping program commercially available for purchase and download from the Internet. Generally, the function of a data wiping program is to “securely” delete or overwrite data on a hard drive so that the data is not recoverable through normal user actions or standard forensic recovery tools. By way of background, active files or folders are either user or system created files and folders that are accessible to a user on a computer hard drive. Those areas of the hard drive that do not contain active files or folders are commonly referred to as unallocated space or “free space” and can contain the contents of previously deleted files. When an active file is deleted, the location on the hard drive where that file resided is marked by the computer’s operating system as unallocated or in other words, available for use to store new data. The deleted data is not accessible to a user without the use of specialized software, but remains in unallocated space until such time as it is overwritten by new data. Once data is overwritten, whether through normal usage or through the use of a data elimination tool such as File Shredder, the original file’s content is not recoverable. Furthermore, the Recycle Bin is an area used by the Windows Operating System to temporarily store files that a user has selected to delete, such that a user could still recover those files. If the user were to then delete a file from the Recycle Bin or choose the option to “Empty the

Recycle Bin”, then that file is no longer accessible to the user without the use of specialized software.

8. As seen in Figure 1 below, when using Lavasoft File Shredder, the user is presented with several options of what to wipe, including files and folders, the recycle bin, system files, and free disk space. The user can only select one option at a time and would have to execute File Shredder repeatedly if the user wished to shred “Free Disk Space” and the “Recycle Bin.”



**Figure 1 - File Shredder Shredding Options**

9. By default, File Shredder creates a log file each time the program is run, which documents the settings selected by the user, including the “shredding alternatives” or hard drive locations selected to be wiped. These log files are saved with the naming format of “Month-Day-Year-Time.HTML” (for example, “08-01-2010-0930.html”) that records the month, day and year when the wiping action began as determined by the

computer's clock setting. The log files are created when the program commences the data wiping action and are stored in a subfolder called "Logs". Moreover, File Shredder log files contain information concerning the specific location(s) targeted for wiping, for example, a specific file or folder, the recycle bin or free space. Accordingly, the names of File Shredder log files offer evidence relating to each date and time the File Shredder program was executed and the option used to overwrite data on the hard drive.

10. File Shredder further provides users with an option to securely wipe the log created during each data wiping process. When files, folders, or free disk space have been successfully wiped, the application presents the user with a confirmation screen that includes a checkbox at the bottom to "Shred the created log file when closing." By default, File Shredder will retain logs of its use, but, if a user selects this checkbox, the program will thenceforth wipe the logs created during each subsequent wiping process.

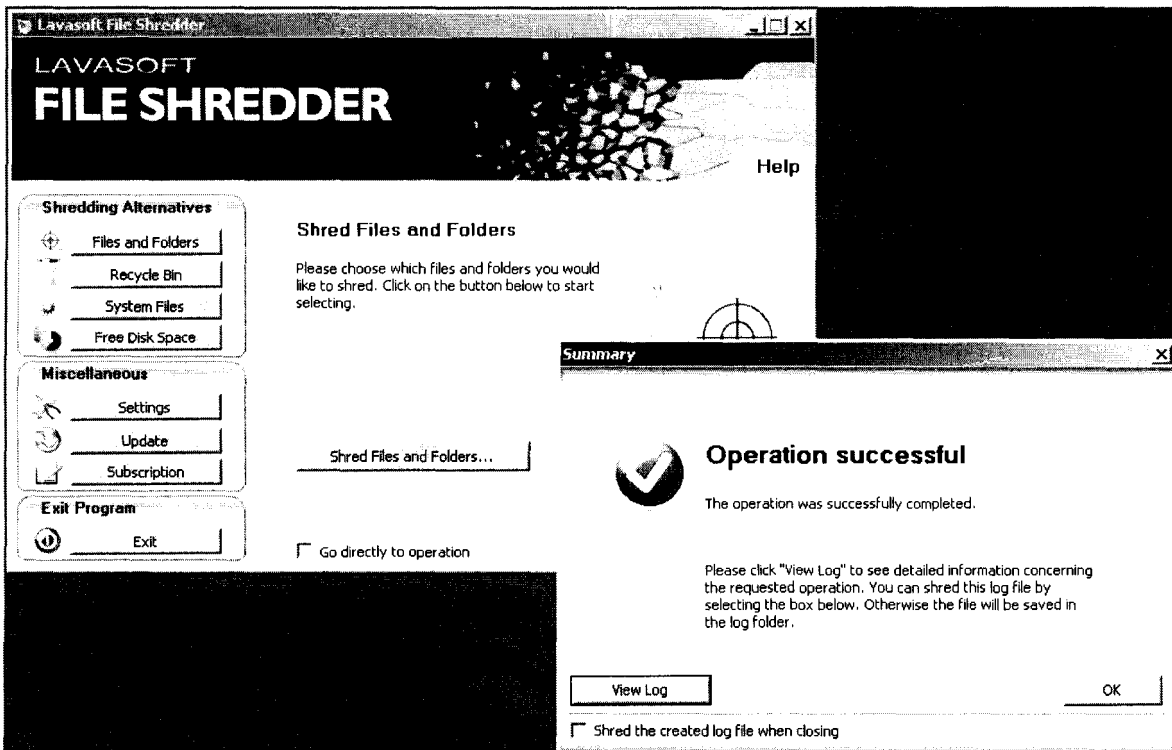


Figure 2: Option to shred the created log file

#### **IV. Demopolis Hard Drive**

11. I reviewed the forensic image of the Demopolis Hard Drive and identified that the Lavasoft File Shredder program was installed on this hard drive on May 20, 2010.

12. The File Shredder Logs folder on the Demopolis Hard Drive contained a single log file, named "06-13-2010-1711.html". The File Shredder Logs folder had a Creation Date of May 20, 2010. However, the Last Written date of the Logs folder is June 25, 2010, indicating that the contents of the Logs folder was modified on that date possibly by, the creation of new log files or the deletion of previously-created log files. As discussed in the following paragraphs, I determined through my forensic examination that there were additional File Shredder log files that were deleted sometime prior to the imaging of the Demopolis Hard Drive.

13. I executed a keyword search of the forensic image of the Demopolis Hard Drive for files matching the filename format of the File Shredder logs, to wit: "MM-DD-YY-HHMM.html" to determine if there was forensic evidence of additional log files that may have been created but stored in other areas of the drive or which were deleted but recoverable. My search revealed an additional 17 filenames that matched this file naming format. As discussed below, five of these files were recoverable and I confirmed that these files were File Shredder logs. Accordingly, based upon the naming convention and my examination, there is evidence indicating that that the File Shredder program was run at least 18 times on the Demopolis Hard Drive between May 20, 2010 and June 25, 2010.

14. The filename artifacts found in my searches were identified in an area of the hard drive used by a Windows 7 service called the Volume Shadow Services<sup>3</sup>. These 17 filenames were as follows:

- i. "05-20-2010-1831.html"
- ii. "05-20-2010-2228.html"
- iii. "05-20-2010-2229.html"
- iv. "05-26-2010-1319.html"
- v. "05-31-2010-1226.html"
- vi. "06-13-2010-1722.html"
- vii. "06-19-2010-1034.html"
- viii. "06-19-2010-1057.html"
- ix. "06-19-2010-1233.html"
- x. "06-19-2010-1240.html"
- xi. "06-19-2010-1243.html"
- xii. "06-21-2010-1650.html"
- xiii. "06-23-2010-1746.html"
- xiv. "06-24-2010-1118.html"
- xv. "06-24-2010-1131.html"
- xvi. "06-25-2010-1343.html"
- xvii. "06-25-2010-1502.html"

15. Of these 17 filenames, the following five File Shredder log files were forensically recovered during my analysis:

---

<sup>3</sup> Volume Shadow Services are a backup feature, enabled by default on all versions of Windows Vista and Windows 7 operating systems, that allows a user to revert a folder or file to a previous version.



- i. "05-20-2010-1831.html"
- ii. "05-20-2010-2228.html"
- iii. "05-20-2010-2229.html"
- iv. "05-26-2010-1319.html"
- v. "05-31-2010-1226.html"

16. I reviewed the data contained in the six available (the one active log file and the five deleted but recovered log files) File Shredder log files and identified the wiping options selected for each use. As shown in the following list, the user did not only chose the option to "Shred Free Space" but also deployed the options to "Shred Recycle Bin" and "Shred Files and Folders."

- i. "05-20-2010-1831.html" – "Shred Free Space"
- ii. "05-20-2010-2228.html" – "Shred Free Space"
- iii. "05-20-2010-2229.html" – "Shred Free Space"
- iv. "05-26-2010-1319.html" – "Shred Recycle Bin (1 file)"
- v. "05-31-2010-1226.html" – "Shred Free Space"
- vi. "06-13-2010-1722.html" – "Shred Files and Folders (1 folder, 0 files - c:\Users\WilliamDemopolis\Documents\Residuals)"

17. In my testing of the Lavasoft File Shredder program, I observed that when the Recycle Bin option is selected to be wiped, the entire contents of the Recycle Bin are wiped. Accordingly I believe that it is not possible to selectively wipe only one file from the Recycle Bin. Thus the one file listed in the recovered "05-26-2010-1319.html" log file indicates that at that time, there was only one file in the Recycle Bin.

18. I note that the 1 folder, 0 files entry listed in the “06-13-2010-1722.html” log file indicates that File Shredder was used to wipe one folder that had no files stored in it at the time of the wiping event.

19. In my examination of the Demopolis Hard Drive, I also reviewed the Internet Browser History, which revealed that the William Demopolis user profile accessed and opened the File Shredder log file “06-25-2010-1502.html” on June 25, 2010. Because this file is not recoverable and is not stored in the File Shredder Logs folder, I believe that the file was deleted or wiped from the File Shredder logs folder between June 25, 2010 and July 15, 2010, the date the hard drive was imaged.

#### **V. Counley Toshiba Hard Drive**

20. I reviewed the forensic image of the Counley Toshiba Hard Drive and identified that the Lavasoft File Shredder program was installed on this hard drive on September 3, 2009.

21. The File Shredder Logs folder on the Counley Toshiba hard drive contained no log files. However, the Last Written date of the Logs folder is June 28, 2010, indicating that data stored within the Logs folder was created, modified or deleted on that date.

22. I executed a keyword search on the Counley Toshiba Hard Drive for the filename format “MM-DD-YY-HHMM.html” to determine if there was any other forensic evidence of additional log files that may have been created but subsequently deleted. My search did not return any additional filename search hits matching the naming convention of the the File Shredder log files.

23. I performed additional examination in an effort to determine whether other evidence of the execution of the Lavasoft File Shredder program existed on the computer. In my analysis, I determined that additional artifacts related to the execution of the Lavasoft File Shredder program also are captured by the Windows operating systems. When a file is wiped by File Shredder, even though the data in the file has been overwritten such that the original content cannot be recovered, the metadata concerning the shredded file, which is maintained by the Windows file system, is changed in a characteristic way. Specifically, the filename is overwritten with the filename of “a”, and the “File Created”, “Last Written”, and “Last Accessed” timestamps of the overwritten files maintained by the operating system are changed in all circumstances to “12/31/79 06:00:00PM”. However, a fourth timestamp, the “Entry Modified” date and time, is updated with the date and time that the File Shredder overwriting action took place. Accordingly, it is possible to estimate the number of files and folders wiped by File Shredder by counting the number of entries with these characteristics.

24. In my examination of the Counley Toshiba Hard Drive, based upon the timestamp metadata characteristics described above, I identified evidence that indicates that File Shredder was run at least three times between June 12, 2010 and June 28, 2010. Specifically, as shown below, the available evidence shows that the user of the Counley Toshiba Hard Drive used File Shredder to shred the Recycle Bin, the “Temp” folder, and the “Temporary Internet Files” folder:

- i. on 6/12/2010, at least 563 items in the Recycle Bin were updated with the 12/31/79 metadata timestamp;
- ii. on 6/13/2010, at least 1,731 items in the Recycle Bin, “Temp” folder, and the “Temporary Internet Files” folder were updated with the 12/31/79 metadata timestamp; and

- iii. on 6/28/2010, at least one item in the Recycle Bin was updated with the 12/31/79 metadata timestamp.

## **VI. Counley Asus Hard Drive**

25. I reviewed the forensic image of the Counley Asus Hard Drive, and identified that the Lavasoft File Shredder program was installed on this hard drive on June 6, 2010.

However, there is evidence that the install file for Lavasoft File Shredder was “downloaded” from the Internet approximately two weeks earlier. Specifically, there is a file named “LavasoftFileShredder.exe” with a File Created date of May 20, 2010 in a folder called “Downloads”, which indicates that File Shredder was downloaded from the Internet on May 20, 2010 but not installed until June 6, 2010.

26. The File Shredder Logs folder on the Counley Asus Hard Drive contained three log files. Specifically,

- i. “06-13-2010-1147.html”
- ii. “06-13-2010-1150.html”
- iii. “06-13-2010-0343.html”

I noted that the Last Written date of the Logs folder is June 18, 2010, indicating that data stored within the Logs folder was either created, modified or deleted from this folder on that date.

27. I also executed a keyword search on the forensic image of Counley Asus Hard Drive for files with the filename format “MM-DD-YY-HHMM.html” to determine if there was forensic evidence of additional log files that may have been created but subsequently deleted. My search revealed an additional four filenames matching this

format, which indicates that the File Shredder program was executed at least seven times on this computer. These additional four filenames were as follows:

- i. "06-13-2010-0135.html"
- ii. "06-13-2010-0406.html"
- iii. "06-13-2010-0712.html"
- iv. "06-18-2010-1835.html"

None of these log files were recoverable.

28. I reviewed the data contained in available File Shredder log files and identified the locations selected for data wiping on each occasion, included the Recycle Bin, Free Space and System Files, as follows:

- i. "06-13-2010-1147.html" – "Shred Recycle Bin (131 files)"
- ii. "06-13-2010-1150.html" – "Shred Free Disk Space"
- iii. "06-13-2010-0343.html" – "Shred System Files (9,055 files)"

29. Through my testing, I observed that when a user chooses the File Shredder Option "Shred System Files", File Shredder overwrites data stored in temporary file storage locations created by the Windows operating system which may correspond to user activity on the computer. These temporary file storage locations include the Internet Browser history and cached files related to the opening and review of email attachments, where the attachments are not saved. The 9,055 files listed as wiped in the log file "06-13-2010-1147.html", correspond with these temporary files.

30. I set forth the following illustrative temporary files that were wiped through the use of File Shredder option "Shred System Files" by the Counley Asus Hard Drive user

on June 13, 2010. These temporary files had been created when the user was reviewing e-mail attachments on the Counley Asus Hard Drive:

- i. C:\Users\Nbot\AppData\Local\Microsoft\Windows\temporary internet files\Content.Outlook\Y5DM3EYS\Guide to Chargeback Fines.pdf
- ii. C:\Users\Nbot\AppData\Local\Microsoft\Windows\temporary internet files\Content.Outlook\Y5DM3EYS\last 2 years accounts.zip
- iii. C:\Users\Nbot\AppData\Local\Microsoft\Windows\temporary internet files\Content.Outlook\Y5DM3EYS\MC Rules Violated.pdf
- iv. C:\Users\Nbot\AppData\Local\Microsoft\Windows\temporary internet files\Content.Outlook\Y5DM3EYS\Merchant Application Portfolio - Durango.pdf “Merchant Application Portfolio – Durango.pdf”
- v. C:\Users\Nbot\AppData\Local\Microsoft\Windows\temporary internet files\Content.Outlook\Y5DM3EYS\Merchant Package.zip
- vi. C:\Users\Nbot\AppData\Local\Microsoft\Windows\temporary internet files\Content.Outlook\Y5DM3EYS\MerchDocsDurango.pdf.<sup>4</sup>

## **VII. Instant Messaging Log Findings**

31. Instant Messaging (“IM”) software allows two or more people to send direct, real-time messages to one another. IM software often provides for the creation of transcripts, commonly called chat logs, which may include the username, message content, and the date and time of the instant messages.

32. I identified an IM application, named Trillian, that was installed on all three hard drives. Trillian is an application that can connect to multiple platforms for IM, such as AOL Instant Messenger, Facebook, Gmail, and ICQ. In my review, I identified chat logs

---

<sup>4</sup> At the time of the filing of this declaration, Stroz Friedberg has not searched the Counley Asus Hard Drive or the other hard drives to determine whether these email attachments are available to the user of the computer or recoverable through forensic processes.

on all three hard drives that were responsive to keywords such as “delete”, “shred” or “lavasoft”.

33. Both the Demopolis Hard Drive and the Counley Asus Hard Drive contain in their chat log files a transcript of a conversation that occurred on May 20 and May 21, 2010. An excerpt of this conversation is attached as Exhibit A. In this conversation, on May 20, 2010 the user “nbot” (the username “nbot” has been identified as the chat display name of Nathan Counley), has sent the user “zeus” (based upon the available evidence we believe the username “zeus” is the chat display name of William Demopolis) an instant message that contains a URL link to download the File Shredder program from the Lavasoft webpage. As noted in my previous analysis, May 20, 2010 is the same date that the File Shredder software was installed on the Demopolis Hard Drive.

34. Further in the Exhibit A chat log, on May 21, 2010 between 10:14:02 am and 10:21:44 am Central Daylight Time, “nbot” and “zeus” discuss deletion of e-mail files and use of File Shredder.

35. The Demopolis hard drive also contained a chat log transcript of a conversation on June 16, 2010 between users “zeus” and “shaner” in which they discuss finding articles on the Internet about security policies and technologies relating to the protection of confidential or non public electronic information. An excerpt of this conversation is attached as Exhibit B.

## VIII. Conclusion


36. Based on my forensic review of the three provided hard drives and through my testing of how the File Shredder application works, available evidence indicates that File Shredder was installed on all three hard drives and was run:

- i. on the Demopolis Hard Drive at least 18 times between May 20, 2010 and June 25, 2010;
- ii. on the Counley Toshiba Hard Drive at least three times between June 12, 2010 and June 28, 2010; and
- iii. on the Counley Asus Hard Drive at least seven times between June 6, 2010 and June 18, 2010.

37. Recoverable File Shredder log files show that File Shredder was used to wipe not only free space, but system files and the contents of the Recycle Bin.

38. Forensic evidence has also shown that the majority of log files created by the File Shredder program subsequently were deleted from the File Shredder Logs folder.

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



8/3/2010

Seth Leone