IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
V.	)	Crim. No. 01-455-A
	)	
ZACARIAS MOUSSAOUI	)	

AFFIDAVIT OF DARA K. SEWELL

I, Dara K. Sewell, being duly sworn, depose and say:

1. I am a Supervisory Special Agent with the Federal Bureau of Investigation. I have been a Special Agent for the FBI since 1996 and currently serve as the Computer Analysis Response Team (CART) Field Operations & Quality Program Manager. CART conducts forensic examinations of computers and other digital media evidence for the FBI, both at FBI Headquarters (HQ) and in 56 field divisions. In my current position, I am responsible for supervising field operations for 35 divisions and the development of CART procedures and practices as they relate to the forensic examination of computer evidence. I am knowledgeable in Macintosh, IBM Compatible, and UNIX platforms. I have completed CART forensic examiner training. As a CART Forensic Examiner, I have performed more than fifty (50) computer forensic examinations and assisted or supervised numerous others.

2. Prior to my current assignment, from 1996 to 2000, I was assigned to the FBI Pittsburgh Division as a Special Agent on the Regional White Collar Crime Squad and the High Technology Crime Task Force as an investigator and a CART Forensics Examiner. In 1999, I worked one-year as a full-time resident affiliate with the technical staff of Carnegie Mellon

University Software Engineering Institute internationally recognized Computer Emergency Response Team (CERT) Coordination Center as a visiting scientist. Prior to joining the FBI, I was employed as a Senior Electrical Design Engineer with the Westinghouse Defense Center (WDC) in Baltimore, Maryland. During my 17-year tenure at WDC, I participated in the design, manufacturing, testing and production of various radar systems and test equipment. I possess a Bachelor of Science Degree from the University of Maryland in Electrical and Mechanical Engineering.

3. I have reviewed the affidavit of Special Agent Bridget Lawler dated September 4, 2002, and the affidavit for the defense of Mr. Donald Eugene Allison dated September 20, 2002, as well as numerous reports and records relating to this investigation. The following addresses issues raised by Mr. Allison.

Imaging and Authentication of Computer Hard Drive or Data

4. Much of Mr. Allison's affidavit addresses authentication issues regarding the hard drives provided in discovery. "Authentication" in this context means the process of ensuring that the duplicate of the hard drive provided in discovery is an exact copy of that which the FBI originally acquired. The FBI uses three different methods to duplicate or image a hard drive:

(1) GNU/Linux routine dd command via Red Hat Linux 7.1 (hereafter "Linux dd");

(2) SafeBack version 2.18 imaging software by New Technologies (hereafter "SafeBack");

(3) Solitaire Forensics Kit, SFK-000A hand-held disk duplicator by Logicube, Inc. (hereafter "Logicube").

Generally speaking, FBI HQ CART procedures require, whenever possible, the use of computer

forensic software hardware or firmware (hardware with software-like operating instructions/protocols designed into the hardware) that have undergone validation testing by CART or a qualified third party recognized by CART. While Mr. Allison favors Linux dd, the FBI has completed a series of tests validating both SafeBack (as of July 2001) and Logicube (as of May 2001). SafeBack imaging software or the Linux dd command are typically used by CART examiners if they have unlimited access and control over an original subject computer hard drive. In circumstances where time, access or control are limited (as in instances where a computer hard drive may not be seized but must be examined on site), CART examiners will gravitate towards the use of the SFK-000A hand-held disk duplicator by Logicube due to its relative speed, ease of use, and portability.

5. As Mr. Allison states in his affidavit, "[m]any methods are available to create an exact duplicate [of computer data]." Allison Declaration at 3. However, Mr. Allison incorrectly asserts that "only one method - the GNU/Linux routine dd - has been approved by the National Institute of Standards and Technologies." Allison Declaration at 3 (emphasis added). The National Institute of Standards and Technology (NIST) does oversee the Computer Forensic Tool Testing Project (CFTT); however, contrary to Mr. Allison's assertions, NIST does not "approve" any computer forensic tools. Instead, it merely reports the results of its testing. Moreover, Mr. Allison wrongly identifies Linux dd as the "only one method . . . approved by [NIST]." Allison's Declaration at 3. First, the NIST report contained some criticisms of the Linux dd, none which have any bearing on this case.[1] Second, NIST also evaluated SafeBack and voted

[1] See "Test Results for Disk Imaging Tools: dd GNU fileutils 4.0.36, Provided with Red Hat Linux 7.1" which can be downloaded at www.ncjrs.org/pdffiles1/nij/196352.pdf.

to release its test results on December 13, 2002.[2] Like the NIST report regarding Linux dd, the NIST report for SafeBack contained some criticisms which also have no apparent impact on this case.

6. **SafeBack:** The computer forensic examiner executes SafeBack from a piece of removable media causing SafeBack to generate an "image" of the source digital media (e.g., hard drive) which then is saved to a digital medium, frequently Magneto-optical disks or digital tape (DAT tapes). Once the image is generated, the image may be verified. The image may later be "restored" to the same or a similar piece of media as the original source media (e.g., another hard drive). The restored image is the duplicate of the source hard drive's data -- an accurate reproduction of the original hard drive's data.

7. SafeBack imaging software has been utilized by computer forensic examiners in law enforcement for many years and the FBI has utilized it to successfully and accurately image hundreds, if not thousands, of computer hard drives. Moreover, the SafeBack software has been successfully validated by the FBI. In addition to FBI's testing, SafeBack's original producer, Sydex, Inc., as well as its current manufacturer, NTI, have completed extensive testing of SafeBack, which has consistently proven to accurately reproduce source data. Furthermore, SafeBack contains a self-verification program within the tool consisting of two write-error checking functions, which utilize hashes known as a cyclical redundancy checksum (CRC), to ensure that the SafeBack software is accurately duplicating a source hard drive bit by bit.

8. **Logicube:** Unlike SafeBack, the Logicube disk duplicator, is not software-based,

---

[2]The NIST SafeBack test report should be available at www.ojp.usdoj.gov/nij/sciencetech/ecrime.htm.

does not generate an image of a source data set (e.g., hard drive) and then require the "restoration" of the image to similar digital medium (e.g., another hard drive). Instead, the Logicube disk duplicator operates more like a high speed cassette duplicator, typically with the original source hard drive connected at one end of the hand-held Logicube device, and another destination hard drive connected at the other end of the device designated to receive the data of the source drive. But, not unlike SafeBack, the Logicube hand-held disk duplicator uses CRC verification techniques to ensure that the duplicate data set generated accurately reflects the source data set (the original source hard drive). Although Logicube has not been submitted to NIST for evaluation as of this writing, hand-held disk-duplicators such as Logicube are widely accepted in the information and forensic communities. Moreover, like SafeBack, the FBI has utilized Logicube to successfully and accurately image hundreds of computer hard drives for almost two years and has subjected Logicube to the FBI's own validation. Finally, the manufacturer of Logicube completed extensive testing of its product prior to marketing it to ensure that the tool accurately reproduces source data.

"Hash" Values and Their Use to Authenticate Hard Drive Duplicates

9. In his affidavit, Mr. Allison writes: "Further, once the duplicate has been created, a product such as the Message Digest version 5 (MD5) or the Secure Hash Algorithm version 1 (SHA-1) should be used to confirm that the duplication process has been done properly." Allison Affidavit at 3. Mr. Allison refers to programs that generate a unique value for both the data on the original hard drive and the data on a purported duplicate of that hard drive in order to further verify the results of the duplication process. These programs rely upon "hashes" to confirm that the duplication process has been done properly.

10. A "hash" is a colloquial reference to the number or value generated by the application of a mathematical formula to a specific data set (such as data in a computer file) in such a way so that it is extremely unlikely that the "hash value" represents any other data. In computer forensics, hashes may have many uses. A hash may be generated for a computer file prior to its duplication. After duplication, a hash may be generated on the duplicate. If the hash value of the original prior to duplication matches identically the hash value after the duplication, one may conclude that the duplicate file accurately reflects the data on the original file. The fact that the hash values match is typically more important than the hash values themselves.

11. There are a number of commonly accepted hash formulae and methods of "running" hashes in the computer forensic community, including the following: the Cyclical Redundancy Checksum (CRC), the Secure Hash Algorithm Version 1 (SHA-1), and the Message Digest Sum, Version 5 (MD5). Currently, CART techniques incorporate CRC and md5sum hashing methods.

12. Because SafeBack and the Logicube SFK-000A hand-held disk duplicator have been validated by CART as computer forensic imaging tools reliably capable of producing verifiable results, and because SafeBack and the Logicube SFK-000A incorporate reliable internal CRC verification techniques, CART procedures do not require examiners to generate separate MD5 or SH-1 hashes for computers imaged using SafeBack or Logicube SFK-000A disk duplicator. As such, absent a computer forensic examiner electing to generate such a hash on her own, there would not ordinarily be any MD5 or SH-1 hash values to disclose to the defense for any computer drives imaged with SafeBack or a Logicube disk duplicator.

CART Imaging Methods Used on Certain Computers of Interest

13. In the instant case, FBI reports indicate that the following computer hard drives were duplicated using the following approved methods:

(A) Zacarias Moussaoui's Toshiba Laptop, serial number 11552157G, was duplicated/imaged using SafeBack on September 11, 2001, by Minneapolis FBI CART Field Examiner Jerry Dewees with a CRC32 value of "63b56fef."

(B) Mukkarum Ali's Laptop, serial number 88914368A-1, was duplicated/imaged using SafeBack on September 16, 2001, by Oklahoma City FBI CART Field Examiner Timothy Ogiela with a CRC32 value of "d7dcad55."

(C) University of Oklahoma PC 11 was duplicated/imaged using Logicube's disk duplicator on October 26, 2001, by Oklahoma City FBI CART Field Examiner Jeffrey Blasnitz with a CRC32 value of "BABABD0A." Thereafter, the Logicube duplicate of PC 11 was imaged using SafeBack with a CRC value for the entire image of "7d235f08."

(D) University of Oklahoma PC 14, CPU serial number F6DM00B, was duplicated/imaged using Logicube's disk duplicator on October 26, 2001, by Oklahoma City FBI CART Field Examiner Timothy Ogiela with a CRC32 value of "D4E0014D." Thereafter, the Logicube duplicate of PC 14 was imaged using SafeBack with a CRC value for the entire image of "6e1f373."

14. **md5sum Hash Examination on Moussaoui's Laptop:** Notwithstanding CART's belief that its reliance upon SafeBack's CRC verification functions is reasonable, in order to demonstrate the point, on October 15, 2002, I requested that the FBI CART Lab at FBI

Headquarters do the following:

(A) Generate an md5sum hash on any partitions of the hard drive on Moussaoui's original laptop computer, serial number 11552157G;

(B) Restore the SafeBack image of the Moussaoui laptop to another drive (a duplicate) using the SafeBack image created by Minneapolis, MN FBI CART Field Examiner Jerry Dewees on September 11, 2001; and,

(C) Generate an md5sum hash on the primary partition of a restored SafeBack image of that hard drive (the duplicate) using the image generated by SA/FE DeWees on or about September 11, 2001.

15. On October 18, 2002, I was informed, in substance, by FBI HQ CART Examiner Lee Shepps of the following:

(A) On October 18, 2002, CART Examiner Shepps restored the SafeBack image made by SA/FE Jerry DeWees on September 11, 2001, of the hard drive of Mr. Moussaoui's Toshiba laptop, serial number 11552157G, to a hard drive;

(B) On October 18, 2002, CART Examiner Shepps examined the restored SafeBack image of the Moussaoui laptop using a Linux Boot CD and found it to have only one primary partition (one FAT 32 partition);

(C) On October 18, 2002, CART Examiner Shepps executed a md5sum command (-b /dev/hda1) to generate a value for the restored SafeBack image of the Moussaoui Toshiba laptop hard drive and noted the value to be "de12b076f9d6cc168fe3344dc1e07c58;"

(D) On October 18, 2002, CART Examiner Shepps examined the original hard drive of the Moussaoui Toshiba laptop, serial number 11552157G using a Linux Boot CD and found it contained only one FAT 32 partition; and,

(E) On October 18, 2002, CART Examiner Shepps executed a md5sum command (-b /dev/hda1) to generate a value for the hard drive of the Moussaoui Toshiba laptop, serial number 11552157G, and noted the value to be "de12b076f9d6cc168fe3344dc1e07c58."

Thus, even using the defense's preferred md5sum hashing standard, the hash values for the only FAT32 partition on the original Moussaoui Toshiba laptop hard drive and that of the corresponding partition from the SafeBack restored image of that Moussaoui Toshiba laptop hard drive were one in the same.

16. **md5sum Hash Examination on Mukkarum Ali's Laptop:** Similarly, on October 15, 2002, I also requested that the FBI CART Lab at FBI Headquarters do the following:

(A) Generate a md5sum hash on any partitions of Mukkarum Ali's original laptop computer, serial number 88914368A-1;

(B) Restore the SafeBack image of the Mukkarum Ali laptop to another drive (a duplicate) using the SafeBack image created by Minneapolis, MN FBI CART Field Examiner Timothy Ogiela on September 16, 2001; and

(C) Generate a md5sum hash on the primary partition of a restored SafeBack image of that hard drive using the image generated by SA/FE Ogiela on September 16, 2001.

17. On October 18, 2002, I was informed, in substance, by FBI HQ CART Examiner Lee

Shepps of the following:

(A) On October 18, 2002, CART Examiner Shepps restored the SafeBack image made by SA/FE Timothy Ogiela on September 16, 2001, of the hard drive of Mr. Mukkarum Ali's laptop, serial number 88914368A-1, to a hard drive;

(B) On October 18, 2002, CART Examiner Shepps examined the restored SafeBack image of the Ali laptop using a Linux Boot CD and found it to have only one FAT 32 partition;

(C) On October 18, 2002, CART Examiner Shepps executed a md5sum command (-b /dev/hda1) to generate a value for the restored SafeBack image of the Ali laptop and noted the value to be "a665ee60525f795bd99703cd0666937b;"

(D) On October 24, 2002, CART Examiner Shepps examined the original hard drive of the Ali laptop, serial number 88914368A-1, using a Linux Boot CD and found it contained one FAT32 partition; and,

(E) On October 24, 2002, CART Examiner Shepps executed a md5sum command (-b/dev/hda1) to generate a value for the hard drive of the Ali laptop, serial number 88914368A-1, and noted the value to be "a665ee60525f795bd99703cd0666937b."

Thus, even using the defense's preferred md5sum hashing standard, the hash values for the only FAT32 partition on the original Mukkarum Ali Toshiba laptop hard drive and that of the corresponding partition from the SafeBack restored image of that laptop hard drive were one in

the same.

Moussaoui Laptop BIOS Settings

18. Defense counsel seek the BIOS (Basic Input/Output System) settings for Mr. Moussaoui's laptop because the laptop had lost all power by the time of the Government's CART examination on August 6, 2002. A review of FBI records demonstrates that the Moussaoui Toshiba laptop, serial number 11552157G, was imaged by CART Field Examiner SA Jerry DeWees on September 11, 2001. At the time of generating the image, the Moussaoui Toshiba laptop did have power and SA DeWees made a record of the BIOS settings for the laptop. The BIOS settings for the Moussaoui Toshiba laptop were as follows:

Date per system: 9/11/2001

Actual date: 9/11/2001

Time per system: 5:17 p.m.

Actual time: 4:58 p.m. [local CT]

Boot CART Floppy (implying Boot sequence is to A).

The Eagan, Minnesota Kinko's Computers

19. **The Initial September 2001 Inquiry at the Eagan, MN Kinko's:** On October 17, 2002, I spoke with Minneapolis FBI Special Agent David Rapp. At that time, SA Rapp told me that, to the best of SA Rapp's unrefreshed recollection, on or about September 19, 2001, SA Rapp went to the Kinko's store in Eagan, Minnesota, to inquire about a receipt found on the person of Zacarias Moussaoui at the time of his arrest. At that time, SA Rapp met with a person who represented himself as a Kinko's employee responsible for managing and maintaining customer computer workstations. At that time, the Kinko's employee informed SA Rapp, in

substance, as follows:

(A) The Kinko's receipt did indicate that a computer workstation had been utilized;

(B) It could not be determined from the copy of the Moussaoui receipt alone which computer workstation was used;

(C) In response to SA Rapp's inquiry about the possibility of acquiring any information from the computer workstations regarding the use of the computers by Moussaoui, the Kinko's employee stated that, since the date of the receipt, all computers had been wiped clean/formatted and started with a fresh install; and,

(D) The computer workstations were generally wiped weekly or bi-weekly approximately, even though Kinko's policy called for weekly wipings. At a minimum, the Eagan Kinko's store wiped the computers at least once per month.

20. **Inquiries to Corporate Kinko's:** On October 11, 2002, I spoke with Timothy Cole, the Director of Loss Prevention for the Kinko's Corporation. Upon my inquiry about the possibility of obtaining hard drives (or images thereof) from the customer computer workstations in the Eagan Kinko's, Mr. Cole stated that Kinko's would not voluntarily comply with the request without a search warrant.

21. **Eagan Follow-up:** On October 11, 2002, I requested that the Minneapolis FBI Field Office contact Kinko's personnel at the Eagan store and determine if, as alleged by the defense, the Kinko's computer could still maintain evidence of defendant Zacarias Moussaoui's use from

August 2001. On or about October 15, 2002, Special Agents Brendan Hansen and Christopher Lester visited the Eagan Kinko's and interviewed Brian Fay, who, as of August 11, 2001, was one of two Kinko's employees who knew how to restore an image onto the six computers with internet access designated for customer use. Mr. Fay stated that the six computers presently at the store are the same computers (with the same hard drives) that were present in August of 2001. These six computers are leased and scheduled to be replaced at the end of this year. The computers are maintained by formatting the computers' hard drives and reloading an image using Norton Ghost whenever business is slow and time allows. There are no logs recording the dates or frequency of loading images on to the computers and Fay could not estimate how frequently they were imaged. Although Fay was not personally familiar with the exact details of the formatting and imaging process he administers to the computers, Fay had been advised by Kinko's that the formatting and restoration process destroyed all files associated with previous users.

22. **Kinko's Corporate Knowledge of its Internet Computer Maintenance Procedures:** On various dates in October, 2002, I communicated with various individuals who identified themselves as computer network and computer security personnel working for the nationwide corporate offices of Kinko's Copy Centers. Throughout all but the very last of these discussions (the last being with Michael Menard, which is discussed below), the reoccurring and unwavering assertion of Kinko's personnel was that data could not be recovered from Kinko's customer computer workstations after the Kinko's re-imaging process had been completed.

23. On October 18, 2002, I spoke with Michael Menard, Kinko's Security Network Engineer, Field Support Department, in Oxford, CA. At that time, Mr. Menard informed me that

Kinko's has a nationwide policy to re-image customer workstations, which he believed to be in effect in August 2001. The Kinko's re-imaging process consists of reinstalling baseline software to each customer workstation in the local branches using non-commercial compact disk read only memory (CD-ROM) disk sets custom-built by Kinko's engineers. Menard was not personally familiar with the exact details of the CD-ROM operations, but offered to contact Kinko's engineers.

24. On October 24, 2002, I again spoke with Mr. Michael Menard. At that time, he told me that, in August of 2001, Kinko's used a re-imaging baseline CD-ROM set version 8.3 in Eagan to re-image customer workstations. In March of 2002, Kinkos began using a new version CD-ROM set with updated software known as the Customer File Management Tool. The Customer File Management Tool runs automatically every four hours to delete temporary and cache files stored as a result of using internet browsers. The CD-ROM version 8.3 for Windows 95 system uses Symantec's Norton Ghost version 6.0 to transfer an image onto the customer workstation computer's hard drive. Menard spoke with the Kinko's engineer who devised the imaging process and he stated that there is no way to retrieve data from a drive after re-imaging by this process. Kinko's branch personnel are told during training that, after the Ghost process is completed, no data can be retrieved from the hard drives. Finally, in response to SSA Sewell's inquiry regarding the size of the computer hard drive and the image used by Ghost to overwrite a customer workstation, Menard was unable to identify the size of the replacement image or hard drive, but, after conferring off-line with an engineer, reiterated that, as a result of the re-formatting of the computer workstations' hard drives, and the resulting overwriting of the hard drive's partition tables, one would be unable to recover any pre-existing data from a workstation

hard drive after the re-imaging/reformatting process employed by Kinko's, except, perhaps, in a laboratory.

The Likelihood of Recovering xdesertman@hotmail.com References

25. **Results of Recent Search Efforts:** On October 20, 2002, I was informed by FBI CART Field Examiner Thomas Lawler that he conducted an examination of certain computer data to locate any reference to xdesertman@hotmail.com and other e-mail addresses allegedly used by Mr. Moussaoui. On October 15-18, 2002, SA Lawler restored images and/or duplicated copies of the following computer hard drives to individual hard drives:

(A) Zacarias Moussaoui's Toshiba Laptop, serial number 11552157G;

(B) Mukkarum Ali's Laptop, serial number 88914368A-1;

(C) University of Oklahoma PC 11; CPU serial number 27DM008; and,

(D) University of Oklahoma PC 14, CPU serial number F6DM00B.

Using the computer forensic software tool I-Look, SA Lawler ran a keyword text search of the data from each hard drive (which includes all file and unallocated space ("drive slack")) for xdesertman and as well as at least 27 variations of this account and other e-mail accounts associated with the investigation of this case. Keyword searches for all computers were negative.

26. **Present Likelihood of Recovery from Eagan Kinko's Computers:** Based upon my experience, education, training and study, in my opinion, the present likelihood of recovering

data attributable to Mr. Moussaoui's use of an Eagan Kinko's computer to allegedly view the xdesertman@hotmail.com e-mail account is extremely remote. I base this opinion, in significant part, upon the following factors:

(A) Regardless of whether the Kinko's imaging process wipes the customer computer workstation hard drives prior to overlaying a baseline image, the fact remains that the reformatting and re-imaging process does significantly reduce the chances of recovering internet browser cache or temporary files, not merely because their partition table is overwritten, but because subsequent users then refill those temporary files with the records of their own internet use. In the instant case, the evidence corroborates the fact that the Eagan Kinko's customer computer workstations had been reformatted and overwritten prior to the visit by FBI agents on September 19, 2001;

(B) All available evidence demonstrates that, since August 2001, the staff at the Eagan Kinko's Copy Center has reformatted and overwritten all customer computer workstations (which are the same which existed in August 2001) no less than once per month (an additional 13-14 times) with intervening use by customers during those periods, and potentially as often as once every week (potentially an additional 60 times). Moreover, since March of 2002, Kinko's began running software which is automatically scheduled every four (4) hours to delete all temporary and cache files generated by customer use;

(C) CART Forensic Examiner SA Thomas Lawler examined restored images of the Moussaoui laptop, the Mukkarum Ali laptop, and both University of

Oklahoma computers using keywords likely to recover any references to the e-mail addresses allegedly used by Mr. Moussaoui, including the xdesertman@hotmail.com address, and found no such references;

(D) In comparison, the Mukkarum Ali laptop computer, which was not, to the best of the FBI's knowledge, reformatted or overwritten and which was alleged by the defense to have been used by Mr. Moussaoui to also view the xdessertman@hotmail.com account, were, by Mr. Allison's own admission, not found to contain any reference to that use. See Allison Declaration at 6;

(E) Even, in the event that a random remnant reference to xdesertman@hotmail.com could be found, it would be unlikely that such a reference could be excluded as not having come from intervening news reports (including the web broadcast of official court records of this court at http://notablecases.vaed.uscourts.gov) relating to Mr. Moussaoui and xdesertman@hotmail.com. Indeed, in a recent search of the internet search engine at www.google.com, at least 212 internet links were found to reference "xdesertman" including commercial news web links;

(F) As alluded to by SA Bridget Lawler, in the context of examining a computer hard drive which had been reformatted and overwritten numerous times, and re-used potentially by countless individuals, the ability to recover a random remnant of memory (a reference not to saved cache files, but to file slack) attributable to Mr. Moussaoui's alleged use to view the xdesertman@hotmail.com account well over a year ago would, indeed, be a very rare find.

The University of Oklahoma PC 11 and IP address 129.15.157.31.

27. On October 9, 2002, I spoke with FBI SA Bridget Lawler, who told me that the discrepancy identified by Mr. Allison in his affidavit on page 7, paragraph 10(C), regarding the IP address assigned to PC 11 from the University of Oklahoma, was an error and should have read IP address 129.15.157.31. To the best of SA Lawler's knowledge, the duplicate computer drive provided to the defense in discovery for PC 11 was a duplicate of the correct computer hard drive corresponding to IP address 129.15.157.31 from the University of Oklahoma.

The Existence of Data outside the 10GB Partition on PC 11 from the Univ. of Oklahoma

28. The defense has expressed concern regarding the unexplained origin of extraneous data outside of the primary partition of the hard drive provided to them in discovery and represented to be a duplicate of the data on PC 11 from the University of Oklahoma. See Allison Declaration at 4. In order to properly answer these concerns, the defense returned their discovery copy of PC 11 to the Government. Based upon reports and conversations with Oklahoma City CART Field Examiner SA Jeffrey Blasnitz, FBI Field Examiner Thomas Lawler learned that, on or about October 24, 2001, SA Blasnitz generated a duplicate of a hard drive of PC 11 at the University of Oklahoma using a Solitaire SFK-000A Logicube disk-duplicator, version 1.15b. The Logicube duplicate hard drive receiving the duplicated data was approximately a 40 gigabyte (GB) (actually a 38.2 GB) hard drive. The Logicube SFK-000A duplicated 19, 999, 728 sectors. In generating the duplicate, SA Blasnitz declined the Logicube option to write zeros to the remaining target/destination drive space. Thereafter, SA Blasnitz generated a SafeBack image of the 40 GB Logicube duplicate of PC 11. On November 6, 2002, SA Lawler acquired the SafeBack image of PC 11 generated by SA Blasnitz, and restored it to a new, previously unused

40 GB hard drive (herein referred to as the "SafeBack Restored Image HD"). Beginning on November 6, 2002, SA Lawler examined the contents of Moussaoui PC 11 Discovery hard drive in comparison to the restored SafeBack image of PC 11 and found the following:

(A) The first 9.529 GB (out of the total 80 GBs) of the Moussaoui PC 11 Discovery hard drive is partition 0;

(B) The first 9.529 GB of the Moussaoui PC 11 Discovery HD is an exact copy of the data contained on the first 9.529 GBs of the restored SafeBack image of PC 11 (also in partition 0);

(C) On both the Moussaoui PC 11 Discovery hard drive and the SafeBack Restored Image, there begins at sector 19, 784, 836 of the drives a repeating pattern of 512 bytes of random data. That repeating pattern extended beyond the 9.529 GB partition 0 of both drives and continues for approximately 7.26 MB to end at sector 19, 999,728. [The exact number of sectors reported to have been duplicated by the Logicube SFK-000A from PC 11 produced by SA Blasnitz];

(D) Thereafter, on both the Moussaoui PC 11 Discovery hard drive and the SafeBack Restored Image there exists approximately 9.54 GBs of zeros (0) to end at sector 40,021,632 [the approximate middle of the 40 GB SafeBack Restored Image];

(E) Thereafter, on both the Moussaoui PC 11 Discovery hard drive and the SafeBack Restored Image, there exists 4 MB of data which is an exact duplicate of the first 4 MBs of data existing at the start of the hard drives (sectors 1 through

and including 8,192);[3]

(F) Thereafter, on both the Moussaoui PC 11 Discovery HD and the SafeBack Restored Image, there exists approximately 18.18 Gigabytes (GB) of zeros (0). [To the end of the 40 Gigabyte (GB) SafeBack Restored Image HD];

(G) Thereafter, on the 80 GB Moussaoui PC 11 Discovery hard drive (which was approximately twice the size of the 40 GB SafeBack Restored Image), there exists zeros to the end of the that 80 Gigabyte (GB) hard drive.

All of which demonstrates that the duplicate of PC 11 within the 80 gigabyte hard drive provided to the defense accurately contains all of the data that existed on PC 11 at the time of duplication

---

[3]**Logicube Integrity Checks.** On or about November 22, 2002, I spoke with Dr. Gideon Guy, the Technical Director for Logicube, Inc., and learned, in substance, the following: A) Dr. Guy has a doctorate in electrical engineering and has been involved in the field of computer hard drive imaging for 6-7 years. Dr. Guy has been with Logicube since March 1999; B) Designed into Logicube software v.1.15b was a standard unit integrity check which forced the Solitaire to verify the ability of the target hard drive (the drive onto which the duplicated data is to be placed) to read and write data (and therefore store data). This function occurred prior to Solitaire commencing the duplication process. The purpose of this function is twofold: 1) to assure that all cables are intact, all data bits have toggled at least once, and both drive interfaces are in good working order, and, 2) to determine the optimal speed to use with the subsequent duplication. The Logicube Solitaire would read the first 8,192 sectors (4 Megabytes) of the source drive (the original drive being copied) and write (duplicate) those sectors to the approximate middle of the target drive, then confirm that those sectors were properly written. This test function sequence always uses data obtained from the source drive and does not generate its own data for the test; C) Ordinarily, the integrity test data written to the target drive is overwritten by the ensuing duplicate image, or is overwritten by zeros when the Solitaire operator selects the option to write zeros to the end of the drive; D) If a source drive is substantially smaller than a target drive, and if the solitaire operator does not select the option to write zeros to the end of the target drive, some or all of the integrity test data may be observed on the target drive outside the partition which represents the duplicated data of the source drive; E) The existence of the integrity test data outside the partition on the target drive which represents the duplicated data of the source drive in no way undermines the accuracy of the duplicate data within the partition, and; F) In Logicube software version 1.17b and versions thereafter, the writability test sequence was altered to write the integrity test data to the first one quarter (1/4) of the target drive.

and was not contaminated by any outside data.

University of Oklahoma "Ghost" Imaging of PC 11 and PC 14

29. On December 17, 2002, Calvin Weeks, the technical security officer for the University of Oklahoma, advised me, in substance, that, during August of 2001, the University of Oklahoma used the commercial software Norton Ghost to restore a previously recorded hard drive image to the hard drives of the computers located in the computer laboratory, including PC 11 and PC 14.

Microsoft Hotmail and its Affiliates

30. In paragraph 10(B) on page 6 of his affidavit, Mr. Allison suggests that negative responses from hotmail regarding the existence of an xdesertman@hotmail.com e-mail account may not preclude the existence of such information in the records of affiliates of Hotmail or Microsoft. On November 22, 2002, I spoke with Tracy Ingle, Group Manager for Policy Enforcement for MSN Hotmail. Ms. Ingle was told of the nature of Mr. Allison's suggestion. In response, Ms. Ingle informed me that, MSN Hotmail subscriber information is not shared with other entities or third parties except as follows:

(A) Non-personally identifiable information (e.g., demographics information such as age, city, state and postal code) is shared with the MSN Hotmail marketing department;

(B) In 2001, account name, city, state and postal code were shared with INFOSPACE, a web-based publisher of an e-mail address directory, if, at the time of registering the account, the account subscriber did not elect to prohibit the sharing of this information;

(C) MSN Hotmail account e-mail is automatically deleted whenever the account subscriber fails to access the account for a period of thirty (30) days;

(D) A MSN Hotmail account is automatically deleted, and no record of it is thereafter maintained by MSN Hotmail, whenever the account subscriber fails to access the account for a period of 90 days;

(E) While, in theory, there could be references to a subsequently deleted hotmail e-mail account stored in data of other Microsoft services (e.g., a message posted to a MSN Group), such references would not be traceable to the registration information of that account holder as it would already have been deleted.

Moreover, according to Ms. Ingle, the search tools used by MSN Hotmail do not search such databases. A search for such information would require some degree of detailed information from the account holder to know what Microsoft services were actually used and when they were used in order to know where additional inquires could be made to possibly recover remnant references.

/s/
Dara K. Sewell
Supervisory Special Agent
Computer Analysis Response Team
Federal Bureau of Investigation

Sworn to and subscribed
Before me this 30th day
of December, 2002

/s/
Sharon Dibbley
Notary Public
Alexandria, Virginia
My Commission Expires: 10/31/03