IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 01-455-A
	)	
ZACARIAS MOUSSAOUI,	)	
Defendant	)	

GOVERNMENT'S OPPOSITION TO
STANDBY COUNSEL'S REPLY TO THE GOVERNMENT'S
RESPONSE TO COURT'S ORDER ON COMPUTER AND E-MAIL EVIDENCE

The United States respectfully responds to Standby Counsel's Reply to the Government's Response to the Court's Order on Computer and E-Mail Evidence (hereafter "Reply") as follows:

Authentication

The foundation of standby counsel's discovery requests regarding the computer and e-mail evidence rests upon their complaints regarding the "authentication" of 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 what the FBI originally acquired. As FBI Supervisory Special Agent Dara Sewell explains in her attached affidavit, the FBI uses three different methods to duplicate or image a hard drive:[1]

(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.

[1]In very simple terms, an "image" of a restored hard drive is to that restored hard drive what a negative is to a photograph.

(hereafter "Logicube").

Sewell Affidavit at 2. Standby counsel seek the "complete authentication information for all of the hard drives produced in discovery, particularly the information for Mr. Moussaoui's laptop, the University of Oklahoma system, and Mukkarum Ali's laptop." Reply at 8.

Before addressing the authentication for the four specific computers, an error in Mr. Allison's affidavit must be corrected. In his affidavit, Mr. Allison writes: "Many methods are available to create an exact duplicate; however, only one method – the GNU/Linux routine dd – has been approved by the National Institute of Standards and Technologies." Allison Affidavit at 3. This statement is simply wrong. The National Institute of Standards and Technologies (NIST) does not "approve" software, it merely tests it and then publishes the results of its tests. NIST did, indeed, test Linux dd and publish the results, which included some criticism. Sewell Affidavit at 3. Like Linux dd, Safeback has also been submitted to NIST for review and its final report was published on December 13, 2002. Sewell Affidavit at 3. NIST reported criticisms of Safeback comparable to those cited for GNU/Linux routine dd. Sewell Affidavit at 3-4.[2] Thus, for purposes of NIST, both Linux dd and Safeback are accurate imaging tools. With this in mind, the authentication of the four computers at issue follows.[3]

---

[2]None of the criticisms of Safeback or Linux dd have any apparent bearing on the issues in this case. Sewell Affidavit at 3-4.

[3]A detailed discussion for all 140 hard drives provided in discovery is not set forth because, to do so, would take extensive (and unnecessary) manpower. As stated below, the Government has provided the defense with a list of all hard drives and their source. All hard drives in this case were imaged by one of the three programs used by the FBI, all of which are recognized by the scientific community as reliable imaging programs. Thus, there should be no question about the authenticity of any of the hard drives. However, if the defense has additional questions about a specific hard drive other than the four at issue, the Government will answer

More important, the manufacturers of both Safeback and Logicube engaged in extensive self-testing of their programs before marketing them. Further, both contain verification programs\functions that ensure that the image\duplicate accurately reflects the data contained on the original. Sewell Affidavit at 4-5. Finally, FBI CART has validated the use of both Safeback and Logicube during their own use of the methods on hundreds of computers. Sewell affidavit at 4-5. Both Safeback and Logicube, like Linux dd, are methods that are accepted within the forensic computer community. Sewell Affidavit at 4-5.

Additionally, 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. However, as set forth in detail in SSA Sewell's affidavit, both Safeback and Logicube contain self-validating programs that ensure the image or copy process generates an exact duplicate of the original. Sewell Affidavit at 4-6. Therefore, the MD5 or SHA-1 programs only provide an additional layer of verification beyond the already proven reliability of the tool itself. Sewell Affidavit at 6.

Both defendant's and Mukkarum Ali's laptops were duplicated using the Safeback software. To eliminate any questions about authentication, the FBI employed the MD5 program suggested by Mr. Allison on both laptops. The program demonstrated that the images of both

---

those questions to the best of its ability.

laptops provided to the defense in discovery were accurate reproductions of the originals. Sewell Affidavit at 7-10. The significance of this point is two-fold. First, there can be no question that the defense has the exact same copy of the original that the Government has, so they can conduct any further investigation on their copy that they wish. Second, the results of the MD5 program as to these two laptops further demonstrate the reliability of the Safeback program.

Finally, standby counsel seek the BIOS (Basic Input/Output System) settings for defendant's laptop based upon the following assertion by Mr. Allison in his affidavit:

> The complete authentication information for Mr. Moussaoui's laptop is even more critical given the indication in the above documents, particularly Bates no. M-LBR-0002265, that the laptop had lost all power by the time of the government's CART examination on August 6, 2002. [Footnote omitted]. The loss of all power means that the original date and time settings cannot be retrieved, and that other settings, such as how the computer performed its boot sequence, the types of ports and peripherals enabled, and the settings regarding the hard disk and the controller, are all lost as well. All of this is essential information on how the laptop was set up.

Allison Declaration at 3-4. As SSA Sewell makes clear in her affidavit, however, the BIOS settings for defendant's laptop were recorded at the time that it was imaged, September 11, 2001, before any loss of power. The BIOS settings are set forth in SSA Sewell's affidavit. Sewell Affidavit at 11. Therefore, no authentication issues exist as to defendant's or Mukkarum Ali's laptops.[4]

Unlike the laptops, the two hard drives at the University of Oklahoma (known as "PC 11"

---

[4]In his Declaration, Mr. Allison requests the BIOS settings only for defendant's laptop because of the loss of power for this computer. Allison Declaration at 4. Standby counsel go much farther in their motion by requesting the BIOS settings for all four hard drives at issue. Reply at 8-9. Since the Government has demonstrated the authentication of all of the hard drives and only defendant's laptop lost power, there is no need for the BIOS settings for the other three hard drives.

and "PC 14") were never removed from the university and are not currently in the Government's possession. Due to the nature of the hard drives, the FBI used the Logicube hand-held disk duplicator to copy the drives and then imaged the duplicates with the Safeback program. Logicube was selected to duplicate the University of Oklahoma hard drives because of its portability. Sewell Affidavit at 3-5, 18. Like Safeback, Logicube has been verified by both its manufacturer and the FBI. Moreover, Logicube performs self-checking functions to ensure that the duplicate drive accurately reflects the contents of the original drive. Finally, although Logicube has not yet been reviewed by the NIST, hand-held disk-duplicators such as Logicube are widely accepted in the information and forensic communities. Sewell Affidavit at 5. Consequently, there can be no challenge to the authenticity of the duplicates of the University of Oklahoma hard drives.

The Request for a Chart for the Remaining Hard Drives

Standby counsel next seek a chart "for the approximately 140 remaining hard drives. At a minimum, the chart should include the origin/source for each drive and the significance of the drive to the case." Reply at 9.[5] On November 22, 2002, the Government supplied the defense with a chart listing each hard drive produced in discovery, when it was produced, and a detailed description of its source from which the defense can assess its significance. Further, in a letter dated December 18, 2002, the Government identified the computer evidence that it believes to be

[5]Paradoxically, in making this request, standby counsel concede that the Government has far exceeded its discovery responsibilities regarding the computer evidence, which this request only expands; yet, the defense has failed to provide the Government with the first piece of discovery. See Reply at 4 ("While we recognize that the Government may already have gone further with discovery in this area than would ordinarily be required . . . .").

relevant for this prosecution. Of course, the burden rests with the defense to determine the significance of a piece of evidence to their defense. Cf. United States v. Comosona, 848 F.2d 1110, 1115 (10th Cir. 1988) ("The Government has no obligation to disclose possible theories of the defense to a defendant. If a statement does not contain any expressly exculpatory material, the Government need not produce that statement to the defense. To hold otherwise would impose an insuperable burden on the Government to determine what facially non-exculpatory evidence might possibly be favorable to the accused by inferential reasoning."); United States v. Nachamie, 91 F. Supp. 2d 565, 569 (S.D.N.Y. 2000) ("The clear language of Rule 16(a)(1), however, does not require the Government to identify which documents fall in each category – it only requires the production of documents responsive to any category."); United States v. Greyling, 2002 WL 424655 at *3 (S.D.N.Y. 2002) ("Fed. R. Cr. P. 16(a)(1)(C) only requires that the Government afford defendants an opportunity to inspect the documents it intends to introduce at trial. It does not require the Government to *identify* which documents it intends to introduce.") (emphasis in original). Therefore, this request is now moot.

The University of Oklahoma Hard Drive

Standby counsel next request the Court to "[o]rder the Government to confirm that the UO hard drive produced in discovery has not been contaminated and explain why the 70 GB of unused storage space on that hard drive contains material that should not be there." Reply at 9. As the affidavit of SSA Sewell makes clear, the following answers Mr. Allison's concerns about University of Oklahoma PC 11. Approximately 9.537 gigabytes of information were duplicated from PC 11's hard drive by the Logicube program onto a 40 gigabyte drive. Thereafter, all data on the Logicube 40 gigabyte drive was imaged and later restored using the Safeback program

onto a 80 gigabyte hard drive, which was then turned over to the defense. The primary partition which exists on the defense 80 gigabyte duplicate hard drive accurately represents the approximately 9.529 gigabytes captured from the primary partition of PC 11 without contamination. The balance of the space on the 80 gigabyte hard drive provided to the defense contains the following:

(1) Approximately 7.26 megabytes of data of the 9.537 gigabytes of data captured from PC 11. This information actually appeared on PC 11 outside of the primary partition and was duplicated by Logicube. Therefore, this data previously existed on the PC 11 and did not result from the imaging/duplication process;

(2) Unused space which consists of a series of zeroes; and,

(3) Approximately 4 megabytes of repetition of the 9.537 gigabytes of information captured from PC 11, which was created by the Logicube tool when it first began to duplicate the material contained on PC 11.[6]

Sewell Affidavit at 19-20. All of this simply means that the first 9.537 gigabytes of 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 and was not "contaminated" by any outside data.

The Examination of Moussaoui's Laptop

Standby counsel's fourth request questions whether the defendant's laptop was imaged before it lost power. The defendant's laptop was imaged on September 11, 2001, before the

[6]In very simple terms, the Logicube tool essentially made sure it could duplicate the information contained on PC 11 before it began copying it. This "test information" appeared in the defense duplicate because the hard drive was much larger than the 9.5 gigabytes of information duplicated from the PC 11 by the Logicube program. Sewell Affidavit at 20 n. 3.

laptop lost power. Sewell Affidavit at 11. The BIOS settings for the laptop requested by standby counsel are set forth in SSA Sewell's affidavit. Sewell Affidavit at 11. Therefore, this request is now moot.

The xdesertman@hotmail Account and Other E-Mail Accounts

In their fifth request, standby counsel ask the Court to "[o]rder the Government to examine all of the temporary files of the computers Mr. Moussaoui used (those at UO, his laptop, and Mukkarum Ali's laptop) and determine whether information can be obtained from them concerning the xdesertman@hotmail.com account and the other email accounts listed in paragraph 33 of the Lawler Affidavit." Reply at 10. SSA Sewell's affidavit describes the unsuccessful searches of each hard drive conducted by FBI CART Field Examiner Thomas Lawler for the xdesertman@hotmail.com e-mail account as well as at least 27 variations of this account and other e-mail accounts associated with the investigation of this case. Sewell Affidavit at 15. Moreover, as previously demonstrated in the first section of this pleading addressing the authentication issues, the defense now has an exact copy of what the Government has. Therefore, there is no reason that the defense, including their computer expert, cannot conduct the same examinations of the four hard drives at issue as the Government. Consequently, this request should be denied.

Similarly, in their sixth request, standby counsel ask the Court to order the Government to conduct an investigation at their behest when they have the same ability to conduct the investigation. The defense possesses the same subpoena power as the Government and, if they wish to serve a subpoena on Hotmail, Microsoft, or any other company, they should do so. See Fed. R. Crim. P. 17(c); 18 U.S.C. § 3005. Moreover, the Group Manager for Policy Enforcement

for MSN Hotmail reports that a search as suggested by Mr. Allison in his Declaration (see Allison Declaration at 6) would have no success. Sewell Affidavit at 21-22. Therefore, this request should fail.

The Internet Provider Address for University of Oklahoma PC 11 Computer

Next, standby counsel ask the Court to "[o]rder the Government to (A) explain the reason for the discrepancy in IP addresses for the UO PC 11 computer, (B) confirm that the UO hard drive produced to the defense in discovery (129.15.110.31) comes from the computer used by Mr. Moussaoui at the University of Oklahoma, and (C) confirm that Mr. Moussaoui did not use any other UO computer." Reply at 11. Simply put, a typographical error exists in the Lawler Affidavit submitted by the Government. The correct internet provider address for University of Oklahoma PC 11 computer is 129.15.157.31. Sewell Affidavit at 18. As discussed in the first section of this pleading regarding authentication, a duplicate of the hard drive for PC 11 has been provided to the defense. As to whether Mr. Moussaoui used any other computer at the University of Oklahoma, only the defendant definitively knows the answer. The only evidence that the Government has regarding Mr. Moussaoui's computer use at the University of Oklahoma involves PC 11 and PC 14, copies of which have been provided to the defense in discovery.

The Kinko's in Eagan, Minnesota

In their eighth request, standby counsel seek "more information about the procedures used by Kinko's personnel and the steps they took to clean the Kinko's system and verify that no evidence of Mr. Moussaoui's communications via Kinko's internet access still remains on the Kinko's system." Reply at 11. SSA Sewell's affidavit describes in detail the procedures used by Kinko's to overwrite ("clean") their systems. The affidavit reveals that during the month

between the defendant's use of the computers at Kinko's on August 12, 2001, and September 11, 2001, Kinko's cleaned their machines at least one time and perhaps many more, since their policy was to re-image (clean) the computers weekly. Sewell Affidavit at 12. Since September 11, 2001, the computers have been re-imaged several times and Kinko's personnel adamantly state that they are unable to recover any pre-existing data from a work station hard drive after the re-imaging process. Sewell Affidavit at 13. Further supporting the inability to locate references to xdesertman@hotmail.com is the fact that FBI CART examiners searched all data related to this e-mail account on both defendant's and Mukkarum Ali's laptops as well as the University of Oklahoma computers, none of which were ever "cleansed" or overwritten, and no data was found collaborating even the existence of any such account, or its use by the defendant. Sewell Affidavit at 15-17. Thus, there is no reason to believe that a search of the Kinko's computers in Eagan, Minnesota, would recover any relevant information about the defendant's e-mail use on these computers. Sewell Affidavit at 17.[7]

The "File Slack" Portions of Mukkarum Ali's Laptop

Standby counsel next ask "the Government to confirm that the 'file slack' portions of Mukkarum Ali's computer do not contain relevant information about Mr. Moussaoui's use of the computer to send e-mails." Reply at 11. As previously stated in the first section of this pleading addressing authentication, the defense has an identical duplicate of what the Government has; therefore, they can search Mukkarum Ali's computer as they wish. Moreover, FBI Cart

[7]Kinko's management states that they will no longer grant access to their computers without a search warrant. Sewell Affidavit at 12. Since the Government does not believe that any evidence would be recovered from these computers, it lacks any basis to seek a search warrant for the Kinko's computers.

Examiner Thomas Lawler thoroughly reviewed Mukkarum Ali's computer, including the "file slack" portions, and found no relevant information. Sewell Affidavit at 15. Therefore, this request should be denied.

The "Ghosting" of the University of Oklahoma Computers

Standby counsel conclude their requests by asking "the Government to identify the procedures employed by UO personnel to 'ghost' the computer(s) allegedly used by Mr. Moussaoui and order the Government, despite the fact that it may be 'likely lost' (see Lawler Affidavit at ¶ 28), to retrieve any forensic evidence showing use of those computers by Mr. Moussaoui and what he did while using those computers." Reply at 11. Calvin Weeks, the technical security officer for the University of Oklahoma, told the FBI that the University of Oklahoma used the commercial software Norton Ghost to restore a previously recorded hard drive image. Sewell Affidavit at 21. As to the second part of standby counsel's request, the defense has in their possession a duplicate of University of Oklahoma PC 11 and PC 14; therefore, they can perform any investigation of these hard drives that the Government can. Therefore, this request should be denied.

Conclusion

The attached affidavit by SSA Sewell fully addresses the issues raised by standby counsel and demonstrates beyond question that the FBI properly and exhaustively examined all computer evidence in this case.

Respectfully Submitted,

PAUL J. McNULTY
UNITED STATES ATTORNEY

By: /s/
Robert A. Spencer
Kenneth M. Karas
David J. Novak
Assistant United States Attorneys

CERTIFICATE OF SERVICE

I certify that on the 30th day of December, 2002, a copy of the foregoing Government's Response was provided to defendant Zacarias Moussaoui through the U.S. Marshals Service and faxed and mailed to the following::

Edward B. MacMahon, Jr., Esquire
107 East Washington Street
P.O. Box 903
Middleburg, Virginia 20118
fax: (540) 687-6366

Frank W. Dunham, Jr., Esquire
Judy Clarke, Esquire
Public Defender's Office
Eastern District of Virginia
1650 King Street
Alexandria, Virginia 22314
Fax: (703) 600-0880

Gerald Zerkin, Esquire
Assistant Public Defender
One Capital Square
Eleventh Floor
830 East Main Street
Richmond, Virginia 23219
fax: (804) 648-5033

Alan H. Yamamoto, Esquire
108 N. Alfred Street
Alexandria, Virginia 22314
(703) 684-4700
fax: (703) 684-9700

/s/
David J. Novak
Assistant United States Attorney