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	)	

STANDBY COUNSEL'S REPLY TO THE GOVERNMENT'S RESPONSE TO COURT'S ORDER ON COMPUTER AND EMAIL EVIDENCE

On behalf of pro se defendant, Zacarias Moussaoui, standby counsel, submit the following reply, and the attached Declaration of computer forensics expert Donald Allison ("Allison Declaration"),[1] to the Government's Response to Court's Order on Computer and Email Evidence ("Government's Response").

On August 15, 19, 20, and 22, 2002, Mr. Moussaoui filed pro se motions seeking to discover the contents of his e-mail account, xdesertman@hotmail.com, that he had accessed from several computers, including Mukkarum Ali's laptop, and computers at Kinko's and the University of Oklahoma ("UO").[2] The Government filed a response to these requests that the Court deemed unsatisfactory in an order issued August 27, 2002. In that order the Court observed that "[g]iven the intense law enforcement attention focused on Mr. Moussaoui after September 11, 2001, we do not understand why an immediate and thorough investigation into the defendant's e-mail and computer

---

[1] Mr. Allison's Declaration is appended at Tab 1.

[2] *See* "Motion to Compel the FBI to Hand Over the Internet File on the Address Xdesertman@hotmail.com" (filed August 15, 2002); "Motion to Get Some Weapons to Combat the United Satan Secret Lies, Evidence and Cyberwar Machine" (filed August 19, 2002); "Motion to Get Xdesertman@hotmail.com File by Any Means Necessary From the United Satan Government" (filed August 20, 2002); and "Motion to Submit Ali Mukaram PCs, Kinkos Eagan PCs and Oklahoma University PCs to Forensic Examination" (filed August 22, 2002).

activities did not lead investigators to the xdesert@hotmail.com account, if it existed." Order at 2.

The scepticism expressed in the Court's order was shared by standby counsel who, for some time, have been concerned with the Government's approach to the computer evidence in this case. It was thus appropriate that the Court granted Mr. Moussaoui's motions and ordered the United States to "obtain an affidavit from the appropriate FBI official(s) explaining how and when, if at all, the FBI examined the contents of the defendant's computer, Ali Mukaram's computer, the University of Oklahoma computers, the Kinkos' computer and the xdesertman@hotmail.com e-mail account." Order at 2.

Counsel and their computer forensics expert have carefully reviewed the Government's Response to the Court's order, including the affidavit of FBI Special Agent Bridget A. Lawler (the "Lawler Affidavit"), and, unfortunately, find it lacking in several respects. These deficiencies heighten our ongoing concern with the handling and production of the computer evidence.

First, as a general matter, the Government has yet to identify and/or provide to defense counsel the complete authentication information for the computer hard drives that have been produced in discovery. Counsel requested this information for Mr. Moussaoui's laptop via a letter dated June 12, 2002.[3] On August 28, 2002, Counsel repeated this request and expanded it to include the authentication information for all of

[3] *See* letter to Kenneth Karas from Pamela Bishop dated June 12, 2002 at 1. A copy of this letter is appended at Tab 2.

the produced hard drives.[4] To date, the response to these requests is not acceptable from a technical standpoint.[5]

This authentication information is critical, both for the defense and the Government, to a thorough examination of the hard drives and the ultimate admissibility of any information derived from them. As the computer forensics expert for Mr. Moussaoui states in his Declaration,

> [The] authentication information (such as the MD5 message digest and other accepted computer forensic methods) is critical as without it, it is impossible to verify that the duplicate hard drives are an exact copy of those that exist on the original systems. Likewise, without such information it is impossible to determine if the material retrieved from the hard drives is accurate.

Allison Declaration at ¶ 6.

Second, although the Government has been forthcoming with the production of hard drives, it has not been forthcoming with information about those drives. Specifically, counsel have not been provided with the origin (source) or significance of

---

[4] *See* letter to Kenneth Karas and Robert Spencer from Frank Dunham dated August 28, 2002 at 2-3. A copy of this letter is appended at Tab 3.

[5] Counsel did receive a letter dated September 9, 2002 purporting to identify the authentication information for Mr. Moussaoui's laptop and stating that "some of the authenticating information you request . . . we have previously provided . . . in the form of the FBI 302s that describe the forensic analysis of each computer." *See* letter to Frank Dunham from Kenneth Karas dated Sept. 9, 2002 at 2 appended to the Allison Declaration at Tab 1. First, according to the defense expert, the identified authentication information pertaining to Mr. Moussaoui's computer is incomplete and "[does] not constitute sufficient authentication for the laptop." Allison Declaration at ¶ 7. Moreover, Mr. Karas' letter admits that only "some" of the authentication information has been produced, and that whatever has been produced is somewhere (he does not say where) in the approximately 160,000 FBI 302s that have been turned over. (Our search of the database for documents containing the critical "MD5" authentication did not produce any documents.) Obviously, this kind of response is inadequate to satisfy standby counsel's legitimate need for the complete computer authentication information in this case.

approximately 140 hard drives. While in the ordinary case such information may not be discoverable, particularly if the Government does not intend to use information from the hard drives in its case, this prosecution is far from the ordinary case.

Over 200 hard drives have been produced in discovery thus far. A thorough examination of a typical drive costs thousands of dollars and takes dozens of hours. A fortune of time and money will be consumed even if counsel had the resources (which it does not) to examine each and every one of the produced drives. Rather than undertake such a costly and potentially wasteful examination,[6] counsel would like to review only those hard drives that are of significance to the case. The Government can aid in this process, as it did on July 8, 2002 when it provided a chart of the origin and relevance of some of the computer media turned over in discovery,[7] by providing similar information for all of the remaining hard drives.[8] While we recognize that the Government may already have gone further with discovery in this area than would ordinarily be required, given that Mr. Moussaoui's case is overwhelming and unique on

---

[6] Some of this waste in resources can be attributed to the Government. *See* Allison Declaration at ¶ 9, n.3 (stating that the UO hard drive produced in discovery contains 80 gigabytes of storage area for approximately 10 gigabytes of data, forcing Mr. Allison "to examine 70 GB of unused storage space in addition to the 10 GB of relevant data").

[7] *See* letter (with attachment) to Frank Dunham from Robert Spencer dated July 8, 2002 appended at Tab 4.

[8] Counsel made a similar request on August 28, 2002. See August 28 letter *supra* note 4 at 3. In its response to that request the Government recently stated that "[w]e are not yet prepared to provide you with our view of the 'significance' of the remaining computers. If you have a view as to the 'significance' of any of these items, please so inform us." *See* letter to Frank Dunham from Kenneth Karas *supra* note 5 at 3.

so many levels (e.g., volume of discovery, subject matter/scope of the prosecution, defendant's pro se status), atypical solutions, such as complete information on the hard drives produced in discovery, is called for.

Third and finally, there are specific concerns with some of the representations made in the Lawler Affidavit. These concerns are:

- The University of Oklahoma hard drive produced to the defense in discovery may be contaminated. That drive contains 80 gigabytes of storage area. However, the data from the UO system only comprises approximately 10 GB of storage area. The remaining 70 GB of storage area should be empty, but it is not, indicating the possibility of contamination. *See* Allison Declaration at ¶ 9.
- Contrary to the representations of Special Agent Lawler (*see* Lawler Affidavit at ¶ 10), a computer user need not proactively download information from a Hotmail account in order for that information to be retained on the user's system. Information can be retrieved from a computer's "temporary files" that are created without the user proactively downloading any specific message information. *See* Allison Declaration at ¶ 10.A.
- It also is not "very, very rare" that "a random remnant of memory still extant in a computer's hard drive or temporary file" will contain relevant information. *See* Lawler Affidavit at ¶ 14. As noted above, temporary files are created on a hard drive even though the user has not proactively downloaded information from a Hotmail account. These temporary files

remain on the system until they are overwritten. Thus, "it is not rare, but very likely that information would be found in temporary files referring to email accounts." *See* Allison Declaration at ¶¶ 10.A., B.

- There also is no indication that the Government's search for the xdesertman and other e-mail accounts in Hotmail extended beyond Hotmail to organizations with which Hotmail shares information. Such organizations include divisions of Microsoft, of which Hotmail is a subsidiary, and third-party companies some of which automatically receive e-mail account information from Hotmail when a new account is opened. *See* Allison Declaration at ¶ 10.B.
- The internet protocol ("IP") address[9] of the UO computer (PC 11) examined by the Government is 129.15.110.31. *See* Lawler Affidavit at ¶ 27. That address does not match the IP address (129.15.157.31) of the UO computer that, according to Special Agent Lawler, Mr. Moussaoui used to connect to the internet to check his pilotz123@hotmail.com account. *See* Lawler Affidavit at ¶ 20(4). Thus, absent some other explanation, "it appears that the government obtained a hard drive other than the one used by Mr. Moussaoui at UO." *See* Allison Declaration at ¶ 10.C.
- Even though, as Special Agent Lawler indicates, the Kinko's system in Eagan, Minnesota appears to erase data from the computers every

[9] The IP address "is the primary identification address for that computer on the internet." *See* Allison Declaration at ¶ 10.C.

twenty-four hours (*see* Lawler Affidavit at ¶ 22), there is still a chance that temporary files still extant on the system may provide valuable information. This is because the local Kinko's staff may not use a process that wipes the *entire* hard drive clean. *See* Allison Declaration at ¶ 10.D. Without knowing more about the procedures used by Kinko's and the steps its staff took to clean its system, it is premature to conclude that the Government has satisfied its obligation "[to] indicate why investigators were unable to retrieve any information from MSN Hotmail and/or any other computers or accounts searched." Order dated August 27, 2002 at 2.

- Special Agent Lawler does not indicate whether the Government examined the "file slack" portions of Mukkarum Ali's computer. "These are files that have been partially overwritten by other information." *See* Allison Declaration at ¶ 10.E. Searching Mr. Ali's computer by the "dates we suspected that Moussaoui used Ali's computer," which is what Special Agent Lawler says was done (*see* Lawler Affidavit at ¶ 26), would not necessarily find relevant data on a file slack portion of the computer. This is because such files do not necessarily have dates associated with them. Thus, the Government may have missed relevant data if its examination was limited to a date search. *See* Allison Declaration at ¶ 10.E.
- It is possible that data from Mr. Moussaoui's use of the UO computer(s) is still retrievable, despite Special Agent Lawler's statement that such data

"was likely lost during the ghosting process." *See* Lawler Affidavit at ¶ 28. First, as noted above, given the mismatch in the IP addresses, there is a question whether the Government has examined the correct UO hard drive used by Mr. Moussaoui. Second, assuming the correct drive was examined, temporary files may still exist on that drive if the drive was not *entirely* wiped clean by the ghosting process. (In fact, our expert found temporary files on the UO hard drive that should not be there if the hard drive had been *entirely* wiped clean. *See* Allison Declaration at ¶ 10.F.) Thus, "it is critical to know the procedures employed by [the UO] personnel before the conclusion can be drawn that 'any forensic evidence showing use of that computer by Moussaoui . . . was likely lost during [the] ghosting process.'" Allison Declaration at ¶ 10.F. (quoting Lawler Affidavit at ¶ 28).

Relief Requested

Based upon the foregoing, standby counsel believe that the following relief is appropriate.

1. Order the Government to provide 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. This information should include confirmation of the use of accepted computer forensics methods for authentication of the produced hard drives produced in discovery as true and correct copies of the originals. *See* ¶¶ 6-7 of Allison Declaration. It also should include the BIOS information for each drive, including, for each drive the following

information:

- Seized system description
    - physical - make, model, serial number, diagrams, pictures, peripherals, additional media
    - logical - bios settings, operating system type, operating system settings
- Forensic method description
    - Imaging software and steps followed
    - Analysis software and steps followed
- Findings
    - Conclusion of analysis.

2. Order the Government to provide a chart, similar to the one provided to counsel on July 8, 2002,[10] 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.

3. Order 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. *See* Allison Declaration at ¶ 9.

4. Order the Government to indicate whether the CART examination conducted on August 6, 2002 on Mr. Moussaoui's laptop constitutes the only authentication information of the laptop, and if so, explain why such information was not

---

[10] *See* note 7 *supra*.

gathered until after a time when the laptop had lost all power. *See* Allison Declaration at ¶ 8, n.1.

Ref. xdesertman@hotmail.com Account and Other Email Accounts

5. Order 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.[11] *See* Allison Declaration at ¶¶ 10.A and B.

6. Order the Government to continue its search with Hotmail for records of the email accounts of xdesertman and the other email accounts listed in paragraph 33 of the Lawler Affidavit. Specifically, the Government should issue a subpoena to Hotmail for xdesertman account records (there is no indication in paragraph 17 of the Lawler Affidavit that this was done), and provide to the Court Hotmail's data retention policies to absolutely confirm that "[o]nce information has been deleted and removed from Hotmail's computers, it cannot be retrieved." *See* Lawler Affidavit at ¶ 16. Similarly, it is important to confirm the assertion that "Hotmail retains no archived record of [account] information." *Id*. Finally, the Government's search should extend beyond Hotmail to other Microsoft divisions and to third-party organizations with which Microsoft and Hotmail share account information. *See* Allison Declaration at ¶ 10.B.

---

[11] These are: Olimahammed2@hotmail.com, Alimohammed@hotmail.com, Alimohammad@hotmail.com, Olimohammed2@hotmail.com, Alimahammed2@hotmail.com, Alimohammed2@hotmail.com, Olimahammad@hotmail.com, Olimohammad@hotmail.com, Alimahammad@hotmail.com, and Alimohammad@hotmail.com.

Ref. Pilotz123@hotmail.com and the University of Oklahoma Computer

7. Order 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. *See* Allison Declaration at ¶ 10.C.

Ref. Kinko's, Eagan, Minnesota

8. Order the Government to provide 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. *See* Allison Declaration at ¶ 10.D.

Ref. Mukkarum Ali's Computer

9. Order 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. *See* Allison Declaration at ¶ 10.E.

Ref. the University of Oklahoma Computer

10. Order 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. *See* Allison Declaration at ¶ 10.F.

Conclusion

Many of the above tasks would be undertaken by standby counsel, but they lack the resources to do so. Many can be done only by the FBI because it has the original hard drives. Accordingly, for the foregoing reasons, standby counsel, on behalf of Zacarias Moussaoui, respectfully request that the Court grant the foregoing requested relief.

Respectfully submitted,

ZACARIAS MOUSSAOUI
By Standby Counsel

/S/
Frank W. Dunham, Jr.
Federal Public Defender
Eastern District of Virginia
1650 King Street, Suite 500
Alexandria, VA 22314
(703) 600-0808

/S/
Edward B. MacMahon, Jr.
107 East Washington Street
P.O. Box 903
Middleburg, VA 20117
(540) 687-3902

/S/
Alan Yamamoto
108 North Alfred Street
First Floor
Alexandria, VA 22134
(703) 684-4700

/S/
Judy Clarke
Federal Defenders of
Eastern Washington and Idaho
10 N. Post, Suite 700
Spokane, WA 99201
(703) 600-0855

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true copy of the foregoing Reply to the Government's Response to Court's Order on Computer and Email Evidence was served upon AUSA Robert A. Spencer, AUSA David Novak and AUSA Kenneth Karas, U.S. Attorney's Office, 2100 Jamieson Avenue, Alexandria, VA 22314, via facsimile and by placing a copy BY HAND in the box designated for the United States Attorney's Office in the Clerk's Office of the U.S. District Court for the Eastern District of Virginia and UPON APPROVAL FROM THE COURT SECURITY OFFICER via first class mail to Zacarias Moussaoui, c/o Alexandria Detention Center, 2001 Mill Road, Alexandria, VA 22314 this 20th day of September 2002.

/S/
Kenneth P. Troccoli