IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Crim. No. 01-455-A
	)	Hon. Leonie M. Brinkema
ZACARIAS MOUSSAOUI	)	

GOVERNMENT'S RESPONSE TO COURT'S ORDER
ON COMPUTER AND EMAIL EVIDENCE

The United States respectfully submits the following response, and the attached affidavit of FBI Special Agent Bridget A. Lawler, to the Court's Order dated August 27, 2002.

Based on the attached affidavit of Special Agent Lawler, we submit the following points:

1. The United States was never aware of the "xdesertman@hotmail.com" account until July 2002, when the defendant listed it in one of his pleadings. That the "xdesertman" account was not discovered is explained primarily by understanding that Hotmail is a free email system that does not verify an account holder's identity and that Hotmail is unable to provide the account used by a particular user on a particular computer at a particular date and time.

2. That the xdesertman@hotmail.com address was not discovered by the FBI is further explained because it is extremely difficult, if not impossible, to find Hotmail account names from a forensically examined computer, unless the user downloaded account information to the computer or to electronic storage media. As far the United States can discern, Moussaoui did not download to computer or electronic storage media any data indicating the xdesertman@hotmail.com account name.

3. After September 11, 2001, the FBI learned that Moussaoui had used a computer at Kinko's, in Eagan, Minnesota, to connect to the internet. When the FBI learned that Moussaoui

had used a computer at Kinko's, the FBI investigated that Kinko's store and was informed that the Kinko's had since erased the data from its computers, as is Kinko's regular practice. Accordingly, the FBI did not seize the computers from Kinko's, Eagan, Minnesota. And, as noted above, even if such computers were seized, it is highly unlikely that evidence of the "xdesertman@hotmail.com" account would have been discovered.

4. The FBI seized and searched Mukkarum Ali's computer from the apartment that Ali and Moussaoui shared in Norman, Oklahoma, and the FBI searched a computer from the University of Oklahoma that Moussaoui claims to have used. Searches of these computers did not turn up the "xdesertman@hotmail.com" email account.

5. On August 16, 2001, when Moussaoui was arrested by the INS in Minnesota, his laptop computer and a floppy diskette were seized. On September 11, 2001, the FBI obtained and executed a search warrant for these items. Moussaoui had saved email activity from his "pilotz123@hotmail.com" account to the floppy diskette. The FBI also discovered that email account because Moussaoui used it to communicate with flight schools and aviation-related entities. The email from that diskette has been examined and will be used at trial; it has also been produced in discovery in this case.

6. A copy of Moussaoui's lap top was given to two other government agencies for their review, but the FBI has received no result from any analysis they may have done.

The FBI conducted an aggressive and responsible investigation into Moussaoui's computer and email activity, particularly given the great demands placed on the FBI's computer investigation capabilities in the wake of the September 11 terrorist attacks. The email activity recovered from Moussaoui's laptop computer and floppy diskette after September 11 will be

offered at trial. Unfortunately, Hotmail email accounts are extremely difficult to trace, and Moussaoui's use of Kinko's computers was not known until after September 11, when it was too late – literally and figuratively – to find the "xdesertman@hotmail.com" account.

The United States is, of course, ready to offer any additional information or explanation required by the Court.

Respectfully Submitted,

Paul J. McNulty
United States Attorney

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

AFFIDAVIT

I, Bridget A. Lawler, being duly sworn, depose and say:

1. I am a Special Agent with the Federal Bureau of Investigation. I have been a Special Agent with the FBI for four years. For three years, I had been assigned to investigate cybercrimes out of the FBI New York Field Office. My cases in the New York Field Office included denial of service attacks, computer hacking, extortion, and viruses (distribution of malicious code). In addition, I have participated in the following computer-related training classes at FBI: Network Investigations; UNIX; Cisco Routers; Advanced Network Investigation Techniques; and Basic Data Recovery.

2. Before I became an FBI Special Agent, I was employed by PriceWaterhouse as a management consultant. At Price Waterhouse, I specialized in implementing Oracle Financials, a financial computer program, for clients. I would typically assess a business's financial processes and systems and then develop and set up the optimum Oracle system for each particular business. I also wrote procedural manuals for the software designed specifically for each business. Before working for Price Waterhouse, I was employed as an auditor by Deloitte and Touche for two years. I also have an educational background in finance and accounting (I have a joint B.S./M.B.A. with a concentration in accounting from the University of Buffalo; I have passed the CPA exam but I currently hold inactive status).

3. In October 2001, I was assigned to the investigation of the terrorist attacks of September 11, 2001. Initially, I was assigned to investigate the financial aspect of the attacks, but in November 2001, I was assigned to investigate computers used by terrorists in conducting the September 11 attacks.

4. I am familiar with the investigation into Zacarias Moussaoui, and I have conducted many of the examinations of computer media that he used. In addition, I have communicated extensively with other FBI agents and laboratory examiners who have been involved in the computer-related examination of Moussaoui and the September 11 terror attacks, and I have knowledge of all of the Government investigation of computer media used by Moussaoui.

The xdesertman@hotmail.com account

5. In short, the FBI did not learn of the xdesertman@hotmail.com account until the defendant listed that account in one of his pleadings in July 2002. To understand how the FBI did not earlier discover the account, one must understand what a Hotmail account is and the differences between such an email account and the content of a computer. Without happening upon the name of such a Hotmail account (e.g., in the possession of a suspect), and unless a computer user downloaded email account content to his or her computer, it is extremely difficult to discover that users of particular computers used particular free email accounts.

6. The xdesertman@hotmail.com is a free Hotmail email account. Hotmail is owned by Microsoft and operated as a free email service. Any user can establish an account at Hotmail, using any available (i.e., not already in use) account name. Hotmail requires that any user provide a screen name and a password of his or her choosing. Hotmail requests certain subscriber information, but it makes no effort to verify it. Therefore, any user can provide fictitious subscriber information, and, in my experience, the subscriber information supplied to

free email services such as Hotmail is often fictitious or non-existent.[1] (In fact, two people can anonymously share information if they each know the Hotmail account name and the password, they can post and then independently read messages to each other.)

7. An investigator can subpoena from Hotmail account information in a particular name, but accounts registered to that name will only be given if the accounts were registered in that name. Accordingly, an investigator can find email accounts that are maintained at Hotmail only if the account holder has given true subscriber information. In my experience, this is a rare occurrence, particularly in the investigation into terrorism-related crimes after September 11.

8. During the course of our investigation, I and other agents investigated Hotmail, Yahoo, America On Line, Earth Link, and other major email service providers for accounts in the name of Zacarias Moussaoui and his known aliases. We discovered no accounts in those names.

9. Hotmail is not an internet service provider ("ISP"). One needs a computer connected to the internet to gain access to Hotmail. Hotmail does not maintain as much information about its users and their particular use of email or the internet as do internet service providers.

10. It is crucial to understand that unless a user proactively downloaded information from his or her Hotmail account, nearly all of the useful information about account activity of a Hotmail account is maintained at Hotmail and not on individual computers used by someone with access to the Hotmail account. The contents of the email account(s) reside on a computer owned by MSN Hotmail. When the email account is accessed, the user is able to view the

---

[1] For the "pilotz123@hotmail.com" account that we know Moussaoui used, he listed his name with Hotmail as "Zuluman Tangotango."

contents of the account, provided he or she gives the appropriate password for the account. The user would need to download the messages (copy the messages to the hard drive of the computer being used or to a floppy disk) to cause the messages to be on an individual computer used to gain access to the internet. By gaining access to an account and reading the messages the user is not copying them to the computer being used. For example, Moussaoui evidently used computers at the University of Oklahoma, owned by Mukkarum Ali, and at Kinko's to gain access to the internet. But, as far as we can determine, he did not download any information to these computers indicating that he had gained access to his "xdesertmen@hotmail.com" account.

11. An investigator could expect to find the following from a forensic examination of a computer used to gain access to a Hotmail email account:

a. Temporary internet cache files, which are files used to load the web page being accessed saved by the computer to enable quick access to information/data used frequently

b. bookmarks, with which a user can mark web pages visited while on the internet;

c. cookie files, which are files containing information sent to the internet user's computer from the computer hosting the web page; and

d. HTTP log (captures date, time, Uniform Resource Locator ("URL"), Internet Protocol ("IP") Address) which has information for each page hit while on the internet (sometimes called a road map for the internet sites visited from a particular computer).

12. From a computer's HTTP log (the information left on the computer used to access Hotmail account, where nothing is downloaded), an investigator can find the indication that the Hotmail web page had been visited. This shows, however, only that a user gained access to

Hotmail; it does not show which email account, or the name of email accounts, that were accessed at Hotmail.

13. Further, Hotmail policy states: “We cannot search for users with an IP only; the Hotmail account name must be listed." In approximately June 2002, during the course of our investigation, we learned from examining Kinko’s firewall logs, that Moussaoui used a Kinko’s computer in Eagan, Minnesota, on a particular date and time to connect to Hotmail. We discussed with Hotmail whether Hotmail could determine the Hotmail account that was visited by a particular computer (by IP address) at a particular date and time. We were informed (1) that Hotmail’s policy is as stated above – that Hotmail cannot search for account name from an IP address, and Hotmail referred investigators to Microsoft where it was discovered (2) that it is theoretically possible for Microsoft to determine an account name from an IP address, and a certain date and time of use, but that such a request must be made relatively quickly, and that in this case too much time had passed between Moussaoui’s use of the Kinko’s computer and our request to Microsoft.

14. With no email information downloaded (i.e., consciously or proactively saved either on the computer’s hard drive or on some electronic storage media), and without Hotmail being able to tell us account information based on the fact that a certain computer gained access to Hotmail at a particular date and time, to find which Hotmail account was accessed, a forensic computer examiner is left to the relatively small chance that a random remnant of memory still extant in a computer’s hard drive or a temporary file will include the Hotmail account name. In my experience, and based on discussions with other FBI computer experts, such a find is very, very rare.

15. In addition, a typical modern computer hard drive contains an enormous amount of information – so much that it is impossible for a forensic computer examiner to look at each piece of information on a hard drive. (If each piece of information that is on an average sized hard disk drive was printed out on a standard piece of paper, the result would be equal to five stacks of paper each as tall as the Washington monument.) Because of the vast amount of information to be reviewed, the FBI has developed lists of key words and phrases, which are run against the entire hard drive. The list used to forensically examine the computers in the Moussaoui and September 11 investigation was developed from information derived in this investigation. The process results in a list of all the files, which contain any of the key words. Each of these files is then reviewed for relevancy. We also review all of the web cache, email, document files, picture files, databases, spreadsheets, encrypted or password protected files and deleted files.

16. MSN Hotmail maintains the content of email accounts (as well as IP connection logs and subscriber/registration information) on its computers. Law enforcement authorities normally can get access to the content of unopened Hotmail email accounts only with a search warrant (and opened email can be obtained with a court order pursuant to 18 U.S.C. § 2703(d)). When an account is inactive for more than 30 days, however, Hotmail deletes the IP connection log and email content. Registration information is maintained by Hotmail for an additional 60 days, and then, if the additional 60 days passes with the account remaining inactive, then the registration information is deleted and the account name is made available to any new user. Once information has been deleted and removed from Hotmail's computers, it cannot be retrieved. Hotmail retains no archived record of this information.

17. The FBI first learned of the account name "xdesertman@hotmail.com" when Zacarias Moussaoui named it in one of his *pro se* pleadings in July 2002. Immediately upon receiving the name xdesertman@hotmail.com, I contacted Hotmail representatives who informed me that Hotmail had no record of the "xdesertman" account.

18. Other FBI agents and forensic computer examiners performed forensic examinations of computers we believe were used by Moussaoui to gain access to the internet. I have reviewed the results of all such forensic examinations. These computers are Mukkarum Ali's computer which he left in 209A Wadsack Drive, Norman, Oklahoma (the apartment he shared with Mr. Moussaoui in July 2001), and a computer at the University of Oklahoma computer lab. The timing and results of these searches are set forth below. The searches of these computers did not divulge the "xdesertman@hotmail.com" account name. For the reasons also set forth below, the FBI did not seize or search any computers from Kinko's, Eagan, Minnesota.

pilotz123@hotmail.com

19. Based on the results of a warrant-authorized search of Moussaoui's laptop computer and his possessions after September 11, the FBI learned that Moussaoui used the account name "pilotz123@hotmail.com." In addition, Moussaoui corresponded with Airman Flight School, Norman, Oklahoma, Pan Am International Flight Academy, and other aviation-related entities using the same email address. On September 12, 2001, the FBI obtained a search warrant for the content of that email and obtained such content from MSN Hotmail. In addition, Moussaoui had saved or downloaded the text of some of the email he sent or received using that account to a floppy diskette that was seized with his possessions. This diskette was searched by warrant after September 11, 2001, and the contents of the emails saved on that diskette were

discovered. I believe that the content of these emails has been produced to the defense as discovery in this case.

20. From a review of the Hotmail internet protocol address connection log for the pilotz123@hotmail.com account, agents were able to determine that Moussaoui connected to the internet to check his email from the following five separate computers/locations:

(1) Account created from IP 202.47.169.200 -- registered to HICOM, Shah Alam, Selangor, Malaysia (Internet Service Provider);

(2) Accessed from IP 164.58.10.124 (approximately 18 times) -- registered to ONENET;[2]

(3) Accessed from IP 129.15.157.166 (approximately 5 times) - - registered to the University of Oklahoma; A Domain Name Server query showed the IP address was registered to dyn157-166.kapts.ou.edu, which is the 209A Wadsack Drive address shared by Moussaoui and Mukkarum Ali; this IP address was traced to the Media Access Control address (a unique number assigned to the Network Interface Card (NIC) on every computer) on the NIC in Mukkarum Ali's computer;

(4) Accessed from IP 129.15.157.31 (approximately 1 time) -- Registered to the University of Oklahoma, and was assigned to PC 11, a computer located in a University computer lab; and

(5) Accessed from IP 204.120.50.1 (approximately 1 time) -- Registered to Kinko's to a computer located in Eagan, Minnesota.

---

[2] Further investigation by FBI agents revealed that there were no logs or records available from ONENET.

21. The FBI investigated Moussaoui's use of the domestic computers listed in the preceding paragraph to connect to the internet to check his email. The investigation of these computers failed to reveal the email account "xdesertman@hotmail.com."

Kinko's, Eagan, Minnesota

22. As do other internet cafes, Kinko's rents computers through which patrons can gain access to the internet. The FBI did not learn that Moussaoui had used Kinko's computers until September 11, 2001. The FBI learned of Moussaoui's use of Kinko's computers based on (1) the connection cited in paragraph 20 (5) above, and (2) the September 11, 2001, warrant-authorized search of Moussaoui's belongings seized from him when he was arrested earlier by the INS. During that search, agents discovered a Kinko's receipt in Moussaoui's possessions. The Kinko's receipt in question shows that Moussaoui was at the Kinko's, Eagan, Minnesota, on August 12, 2001.[3] On September 14, 2001, the lead FBI agent in Minnesota investigating Moussaoui set a lead to locate the Kinko's Computer and obtain the content of email and any additional email addresses that may have been used by Moussaoui. On September 22, 2001, FBI agents interviewed personnel at the Kinko's in Eagan, Minnesota. Kinko's personnel told the FBI that it was the policy of that Kinko's store to erase the data from the hard drives of the computers it rents to the general public every 24 hours.

23. The FBI expended significant investigative efforts and resources trying to discover evidence of Moussaoui's communication via Kinko's internet access. (This

[3] From this receipt, the FBI was able to find Moussaoui's use of the Kinko's computer on the firewall logs maintained by Kinko's. This led to our request to Microsoft to find the account name that Moussaoui used on August 12, 2001, as discussed above.

investigation included obtaining and examining the Kinko's firewall logs for the Kinko's in Eagan, Minnesota, and on a national scale.) This investigation showed an internet session by a user, in the Eagan Minnesota Store, on August 12, 2001, for approximately eight minutes connected to MSN/Hotmail. Through an interview of a Kinko's Eagan, Minnesota store employee and review of the receipt found in Moussaoui's possesion at the time of his arrest, it was determined that Moussaoui used a a Kinko's computer on August 12, 2001, in Eagan, Minnesota, for approximately eight minutes to connect to the internet, and paid for one black-and-white printout on a laser printer. During the course of this investigation, we discovered, unfortunately, that Kinko's frequently erases the data from the computers it rents out for internet access. FBI agents in Minnesota were informed by Kinko's personnel that Kinko's Eagan, Minnesota, store scrubs the data from its computers every day. Based on this information, approximately 44 days after Moussaoui used the computer at Kinko's in Eagan, Minnesota, FBI agents in Minnesota decided not to seize the computers from that Kinko's.

24. During the investigation of the September 11 terrorist attacks, the FBI has discovered that the 19 hijackers also made use of Kinko's computers in other cities to gain access to the internet. Accordingly, FBI agents contacted Kinko's stores in other cities and Kinko's headquarters in California. From these various contacts it appears that Kinko's stores erase data from, or re-image, the computers they rent to the public at varying times, from every 24 hours to every 30 days. For instance: Kinko's personnel in Salem, New Hampshire, and Orlando, Florida, told the FBI that they re-image their hard drives every seven days; and Kinko's headquarters in California told the FBI that the computers rented to the public must be re-imaged every 30 days. In any event, it is evident that we discovered Moussaoui's use of Kinko's in Eagan, Minnesota,

too late.

Mukkarum Ali's Computer

25. From approximately the beginning of July 2001 through August 10, 2001, Moussaoui lived with Mukkarum Ali, and one other man, in Apartment A, 209 Wadsack Drive, Norman, Oklahoma. The apartment was owned by the University of Oklahoma, which provided internet access. Ali kept a computer in the apartment, and, I believe, Moussaoui used that computer.

26. On September 15, 2001, the FBI, Oklahoma City, obtained and executed a search warrant for 209A Wadsack Drive, and Ali's computer was seized. On September 29, 2001, a Computer Analysis Response Team ("CART") Examiner, from the FBI's Oklahoma City Field Office, completed an examination of Ali's computer. The examination included creation of a forensically sound image of the laptop, a logical copy of the laptop, and the recovery of deleted files. On October 22 and 23, 2001, FBI agents reviewed the compact disks containing the logical files and recovered deleted files produced as a result of the CART examination. As a part of the review of the logical and recovered deleted files, the agents looked for all files created, modified, or deleted on the dates we suspected that Moussaoui used Ali's computer. Through investigation we had determined that Ali used a static IP address to connect to the Internet. Agents attempted to obtain from MSN Hotmail whether Hotmail could search records by IP address so that we could identify all user accounts accessed by the static IP address of Mukkaram Ali's computer. Hotmail indicated that it could not do so, citing their policy that they "cannot search for users with an IP only; the Hotmail account name must be listed." I and another FBI agent have also separately examined the information recovered from Mukkarum Ali's computer. We had no

success in identifying the "xdesertman@hotmail.com" address.

The University of Oklahoma Computer

27. From the results of the search of the "pilotz123@hotmail.com" account, we determined that Moussaoui had connected to that internet account from the IP address 129.15.110.31. In October 2001, further investigation revealed that that IP address was assigned to PC11, a lab computer on the campus of the University of Oklahoma, using Network Interface Card identified with MAC address 00:B0:D0:43:85:C8. On October 26, 2001, an FBI agent made a duplicate of the hard drive of PC 11. The FBI conducted a CART field examination of that hard drive, which examination included: identifying the computer and documenting the system parameters; making a logical copy of the Hard Drive; retrieving erased files. On November 21, 2001, an FBI agent reviewed the contents of 7 CD Roms containing the results of the CART Examination. (A copy of these CDs has been produced to the defense.) This review failed to turn up any internet activity or internet addresses by Moussaoui.

28. During the course of investigation of PC 11, FBI agents from Oklahoma interviewed computer staff at the University of Oklahoma. The computer staff told the FBI that on August 30, 2001, PC 11 was "ghosted" to prepare the for the new semester. The process of Ghosting a computer involves the use of a Norton Utility to wipe the computer hard drive clean. The ghosted set-up is installed on top of the old data. Thus, any forensic evidence showing use of that computer by Moussaoui, and what he did while using that computer, was likely lost during this ghosting process.

Moussaoui's Laptop Computer

29. On August 16, 2001, Zacarias Moussaoui was arrested by the INS in Eagan,

Minnesota. His laptop computer and a diskette was then seized from the Residence Inn, where he had been staying while attending the Pan Am International Flight Academy. On September 11, 2001, the FBI obtained a search warrant and conducted a search of that computer and diskette.

30. I have examined a mirror image of the data stored on Moussaoui's laptop computer and the diskette seized from him several times. A copy of that hard drive from Moussaoui's laptop, and the diskette recovered from Moussaoui, have been produced to the defense (and to Moussaoui in hard copy).

31. From the examination of Moussaoui's computer and the diskette in his possession, we recovered no evidence that Moussaoui had ever used that computer to connect to the internet, and we recovered no evidence of any email account other than "pilotz123@hotmail.com." That is, Moussaoui downloaded email he sent and received using the "pilotz123@hotmail.com" account to the floppy diskette that was seized from him; other than that, we found no email activity.

32. A mirror copy of the hard drive of Moussaoui's laptop computer was provided to two government agencies for their review. No results or information from any such review have been passed to me or the FBI Moussaoui investigation from either agency. Otherwise, no other government agency has been asked to review Moussaoui's computer or email use.

The Olimahammed2@hotmail.com account

33. The FBI was also not aware of the account "Olimahammed2@hotmail.com" until the defendant listed the account in his pleading dated August 15, 2002. The email address is mentioned a second time in a letter from the defendant to the prosecutors dated August 19, 2002,

where it is listed as "Alimohammed" or "Alimohammad" @Hotmail.com. Due to the hand writing of the defendant, I obtained a subpoena to Hotmail for information on the following variations of this account: olimahammed2, olimohammed2, alimahammed2, and alimohammed2@hotmail.com. After review of the August 19 letter, on August 22, 2002, I also obtained a subpoena to Hotmail for information on the following accounts: olimahammad, olimohammad, alimahammad, and alimohammad@hotmail.com. The results received from Hotmail to date revealed no records of accounts in the above-mentioned names.

Additional Investigation

34. During the course of this investigation, various possessions, including notebooks, were seized from Moussaoui and searched pursuant to warrant. Agents who reviewed these possessions have brought to my attention written words that resemble email account names. I have obtained subpoenas for multiple variations of approximately 6 email addresses. None of these addresses was "xdesertman@hotmail.com" or "Alimohhammed@hotmail.com" (or a variation on those names). The investigation into these apparent email addresses has yielded no

evidence suggesting another email account used by Moussaoui or with which Moussaoui corresponded.

_/s/_____
Bridget A. Lawler
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed
Before me this 4th day
of September 2002

/s/_____
Notary Public
Alexandria, Virginia