

United States District Court

NORTHERN DISTRICT OF INDIANA

FILED

UNITED STATES OF AMERICA

v.

CRIMINAL COMPLAINT

APR 13 2006

Vikram S. Buddhi
208 Airport Road - Apt. 2
West Lafayette, Indiana

CASE NO. 2:06MJ
ANDREW P. RODOVICH
UNITED STATES MAGISTRATE
U. S. DISTRICT COURT
NORTHERN DISTRICT OF INDIANA

I, Eric Dickey, the undersigned complainant, being duly sworn state the following is true and correct to the best of my knowledge and belief. On or about December 2005 through January 2006 in Tippecanoe County, in the Northern District of Indiana defendant(s) did;

- Threaten the President of the United States;
- Threaten an immediate family member of the President of the United States;
- Threaten the Vice President of the United States;
- Threaten an immediate family member of the Vice-President of the United States;
- Threaten by means an explosive to kill, injure, or intimidate an individual; and
- Threaten by means an explosive to damage and destroy buildings and real or personal property of another;

in violation of Title 18, United States Code Section 871(a), 879(a) and 844(e).

I further state that I am a(n) Federal Bureau of Investigation Special Agent and that this complaint is based on the following facts:

SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof.

(X) Yes () No

Signature of Complainant
Eric Dickey
United States Secret Service

Sworn to before me, and subscribed in my presence

April 13, 2006 at HAMMOND, INDIANA
Date

ANDREW P. RODOVICH
UNITED STATES MAGISTRATE JUDGE
Name and Title of Judicial Officer
AUSA PHILIP C. BENSON

1st Andrew P. Rodovich
Signature of Judicial Officer

AFFIDAVIT

I, ERIC DICKEY, having been duly sworn according to law, depose and state as follows:

1. I am a Special Agent of the United States Secret Service (USSS), and have been employed by the Secret Service since 2001. I am currently assigned to the Chicago, Illinois Field Office. My duties include the investigation of counterfeiting, financial fraud and threats against the President, Vice President and their families. I have been involved with investigations involving the use of computers to make threats against public officials. Based upon my training and experience, I know that the use of computers and related storage media is common in the commission of threatening the President or other public officials. Information relevant to the investigation of these crimes (internet transactions, e-mails, customer databases, web site development and source objects) is often stored in electronic media and can be retrieved. Relevant and probative information is often contained on the hard drive of the computer, computer diskettes and other computer equipment.

2. The information contained in this affidavit is based upon information obtained directly from USSS Special Agent Wayne Gault of the Indianapolis Field Division Office and others who assisted SA Gault in his investigation of this matter. My conclusions also rely on the internal investigation by the Purdue University Police Department and Scott Ksander, the Senior Inforensics Analyst for Purdue University's Information Technology Department within the Department of Computer Technology.

3. Based on my training and experience, a search of the information associated with computers necessarily requires agents to seize electronic storage devices so that these devices may be examined later by a qualified forensic analyst in a laboratory or other controlled

environment. I know that computer hardware, software, electronic files, documentation, passwords, and data security devices may be important to a criminal investigation in at least two respects: (1) the objects themselves may be instrumentalities, fruits of a crime, or evidence of a crime, and/or (2) the objects may have been used to collect and store information about crimes (in the form of electronic data).

Applicable Statutes

4. Title 18, United States Code, Section 871(a) provides that any person knowingly and willfully makes any threat to take the life of, to kidnap, or to inflict bodily harm upon the President of the United States, the President-elect, the Vice President or other officer next in the order of succession to the office of President of the United States, or the Vice President-elect, shall be subject to a fine, imprisonment, or both. In addition, Title 18, United Code, Section 879(a) provides that whoever knowingly and willfully threatens to kill, kidnap, or inflict bodily harm upon a former President or a member of the immediate family of a former President; a member of the immediate family of the President, the President-elect, the Vice President, or the Vice President-elect; a major candidate for the office of President or Vice President, or a member of the immediate family of such candidate; or a person protected by the Secret Service under section 3056 (a)(6), shall be subject to a fine, imprisonment, or both.

5. Title 18 United States Code Section 844(e) states in relevant parts as follows: "Whoever, through the use of (an) instrument of interstate commerce ... or in or affecting interstate commerce ... willfully makes any threat or conveys false information knowing the same to be false, concerning an attempt or alleged attempt being made, or to be made, to kill, injure, or intimidate any individual, or unlawfully damage or destroy any building, vehicle, or

other real or personal property by means of fire or an explosive” shall be fined or imprisoned, or both.

Applicable Definitions

6. I know, based upon my training and experience, the following:

7. Internet Protocol address: An Internet protocol address, also known simply as "IP" address, is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178).

Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most Internet service providers control a range of IP addresses.

8. Static IP address: A static IP address is an IP address that is assigned permanently to a given user or computer on a network. A customer of an ISP that assigns static IP addresses will have the same IP address every time the user connects to the internet. Computers connected to the internet through Digital Subscriber Lines "DSL" or cable modems are often assigned a static IP address.

9. Uniform Resource Locator (URL): A URL is the global address of a document or other web-based resource. The first part of the URL indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located. For example, the two URLs below point to two different files at the domain "sample-domain.com". The first specifies an executable file that should be fetched using the FTP protocol; the second specifies a Web page that should be fetched using the HTTP protocol:

ftp://www.sample-domain.com/stuff.exe

http://www.sample-domain.com/index.html

10. Log File: A log file is a file that lists actions that have occurred. For example, Web servers maintain log files listing every request made to the server. With log file analysis tools, it's possible to get a good idea of where visitors are coming from, how often they return, and how they navigate through a site.

11. Media Access Control (MAC) Address: The unique serial number burned into Ethernet adapters that identifies that network card from all others.

12. Address Resolution Protocol (ARP): A protocol used to convert an IP address into a physical address, such as an Ethernet address. A user wishing to obtain a physical address broadcasts an "ARP request" onto the network. The host on the network that has the address in the request then replies with its physical hardware address. ARP requests follow a simple protocol:

- An ARP Request: Computer A asks the network, "Who has this IP address?"

- An ARP Reply: Computer B tells Computer A, "I have that IP. My MAC address is [whatever it is]."

13. ARP Table: Network devices have an ARP table, a short-term memory of all the IP addresses and MAC addresses the device has already matched together. The ARP table ensures that the device doesn't have to repeat ARP Requests for devices it has already communicated with. It is possible for the ARP table to be "poisoned". In the above listed example, this poisoning could occur if, when Computer A asked the network, "Who has this IP address?", Computer C answered "I have that IP. My MAC address is [whatever it is]."

However, Computer C does not have that IP address, since it belongs to Computer B. Computer A now believes that Computer C is actually Computer B and will send all of its internet traffic intended for Computer B to Computer C. This is often done in an attempt to conceal the identity of Computer C.

Description of Criminal Activity

14. On 12/13/05, a concerned citizen contacted Secret Service's Dallas Field Office to report a subject, using the screen name "extertriemist_bush", posted a threatening message directed towards President George W. Bush, Vice President Richard B. Cheney, First Lady Laura Bush, Second Lady Lynne Cheney, and Secretary of Defense Donald Rumsfeld on a Yahoo! Finance message board dedicated to Sirius Satellite radio (URL: <http://finance.yahoo.com/q/mb?s=SIRI>). The subject's message was titled, "CALL FOR ASSASSINATION OF GW BUSH". The content of the message in part, stated as follows, "...GO IRAQIS!...RAPE AND KILL THE ANGLOSAXONS...NO MERCY....KILL GW BUSH...RAPE AND KILL LAURA BUSH...KILL DICK CHENEY THE WHITE FAT PIG...RAPE AND KILL LYNNE CHENEY...KILL DONALD RUMSFELD THE OLD GEEZER CROOK...RAPE AND KILL THE ANGLOSAXON REPUBLICANS..."

15. On 12/16/05, a subject using screen name "exsteimist_bush" posted two messages on the internet. These new messages were posted on a Yahoo! Finance message board associated with JDSU (URL: <http://finance.yahoo.com/q/mb?s=JDSU>). JDSU is the stock market ticker symbol for JDS Uniphase, a publicly traded company. The messages were titled "CALL FOR ASSASSINATION OF GW BUSH" and "BOMB KEY SITES IN US:IT'S LEGAL 4 ARABS". The content of the messages was identical to the one posted by extertriemist_bush" on 12/13/05.

16. On 12/21/06, a subject using screen name "extreriemist_bush", posted a message on the internet. This message was posted to the same Yahoo! Finance message board associated with JDSU (URL: <http://finance.yahoo.com/q/mb?s=JDSU>), as the two messages posted on 12/16/05, by the subject using screen name "exsteimist_bush." The message was titled "ASSASSINATION OF GW BUSH SOON". The content of the message in part stated, "IT IS NOW LEGAL UNDER INTERNATIONAL LAW TO BOMB KEY SITES IN THE USA. IRAQIS! GIVE ANGLOSAXONS THE TIT REACTION FOR THE TAT ACTION OF BUSH AND REPUBLICANS...KILL THE WHITE ANGLOSAXN AMERICAN BRITISH BASTARDS...FULLY JUSTIFIED IN LIGHT OF THESE WHITE EVIL DOERS ACTIONS".

17. On 1/17/06, a subject using screen name "exxtremist_bush", posted a message on the internet. This message was posted to a Yahoo! Finance message board associated with General Motors. The message was titled "CALL FOR ASSASSINATION OF GW BUSH." This is the exact same title as used on 12/16/05, by subject using screen name "exsteimist_bush" in the posting referenced in paragraph 17 of this affidavit and the posting on 12/13/05, by the subject, using the screen name "extertriemist_bush" and referenced in paragraph 16 of this affidavit. The content of the message on 1/17/06, in part stated "ENOUGH OF SHIT FROM ANGLOSAXONS. SEEK THEM OUT WHERE EVER THEY ARE ON THIS EARTH, RAPE THEIR WOMEN, KILL THEIR MEN, CUTOUT THEIR VAGINAS, CUT OUT THEIR PENISES, CHOP OFF THEIR HEAD, SHOVE THEIR CHOPPED VAGINA AND PENISES DOWN THEIR BEHEADED-NECK-STUMP-HOLES. THIS IS THE ONLY AND LEGAL WAY TO DEAL WITH ANGLOSAXONS...." The second paragraph continued on stating "BOMB ALL FACILITIES SETUP BY ANGLOSAXONS, BOMB ALL TRADE AND

COMMERCE SETUP BY ANGLOSAXONS IN ASIA, AND BUILD YOUR OWN FACILITIES THAT EXCLUDES THE ANGLSAXONS. THIS IS THE ONLY WAY TO DEAL WITH ANGLOSAXONS.” The third paragraph stated “BOMB AND DESTROY ANGLOSAXON POWERPLANTS, ROADS, BRIDGES, NUCLEAR PLANTS, WATER SUPPLY, COMMERCE BUILDINGS, OIL LINES ‘OWNED’ BY ANGLOSAXON REPUBLICANS, DENY THEM THEIR LOOTING WAY OF LIFE. THIS IS THE ONLY JUST AND LEGAL WAY TO DEAL WITH ANGLOSAXONS. BOMB KEY FACILITIES IN THE USA AND BRITAIN...FULLY JUSTIFIED IN THE LIGHT OF THE LOOTING AND KILLING WAY OF LIFE OF THE ANGLOSAXONS. KILLING ANGLOSAXONS AND BOMBING THEIR WAY OF LIFE IS LEGAL AND JUSTIFIED...”

18. On 12/21/05, the United States Attorney of the Northern District of California issued a Grand Jury Subpoena to Yahoo! Inc., located at 701 First Avenue, Sunnyvale, California, requesting any and all information associated with the Yahoo screen name: “extertriemist_bush”.

19. On 1/5/06, Yahoo! responded to the above mentioned subpoena. The results showed that the screen name “extertriemist_bush” was listed as an “Other Identity” for login name “lallynino106”. The full name listed for the account was Mr. John Foster, with a Zip Code of 13432. A search of the United States Postal Service website shows that Zip Code 13432 is not a valid Zip Code. The account for “lallynino106” was created on Sunday, May 15, 2005 at 06:06:03 (PST) and was registered from IP address 128.211.252.161.

20. On 1/13/06, the United States Attorney of the Northern District of California issued a Grand Jury Subpoena to Yahoo! Inc., located at 701 First Avenue, Sunnyvale,

California, requesting any and all information associated with the Yahoo screen name:

“exsteimist_bush”.

21. On 1/25/06, Yahoo! responded to the above mentioned subpoena. The results showed that the screen name “exsteimist_bush” was listed as an “Other Identity” for login name “lallynino105”. The full name listed for the account was Mr. John Foster, with a Zip Code of 13432. A search of the United States Postal Service website shows that Zip Code 13432 is not a valid Zip Code. The account for “lallynino105” was created on Sunday, May 15, 2005 at 06:05:47 (PST) and was registered from IP address 128.211.252.161.

22. A search of the American Registry of Internet Numbers (ARIN) shows that IP address 128.211.252.161 is registered to Purdue University in West Lafayette, Indiana.

23. The subpoena results also included a list of logins for login names “lallynino106” and “lallynino105” from 11/20/05 through 12/14/05. These logins were completed from four different IP addresses within subnet 128.211.252.XX. According to Scott Ksander, Senior Inforensic Analyst\Engineer in the Computer Forensic Department of Purdue University, all IP addresses within this subnet are static and assigned to a physical location at Purdue University within their computer network.

24. On 1/12/06, Special Agent Lawrence Brown and I met with Scott Ksander, Purdue University. Ksander stated he reviewed the entries in the ARP table for the IP addresses within subnet 128.211.252.XX that were listed in the Yahoo! subpoena returns. Each entry in the ARP table lists an IP address and the MAC which it is linked to. Ksander reviewed the ARP table entries for each time when Yahoo! user “lallynino106” logged in and for the times associated with each of the threatening messages referenced above which were posted on Yahoo!. He stated

the IP addresses listed in the Yahoo! subpoena return (128.211.252.64, 128.211.252.68, 128.211.252.47 and 128.211.252.70) are all associated in the ARP table with MAC address 00:0A:E6:EB:14:10. Ksander stated that these facts, one MAC address associated with numerous IP addresses, would result from that MAC address poisoning the ARP table and misrepresenting itself as those other IP addresses.

25. Ksander stated that he then searched Purdue University computer records for the first instance of MAC address 00:0A:E6:EB:14:10. He stated that on-campus residents are required to register their MAC address when they initially establish their internet connection to the University network. He stated that the MAC address 00:0A:E6:EB:14:10 was listed as the registration MAC address for the account assigned to Vikram Subbarao Buddhi.

26. Ksander also searched Purdue University computer records for the most consistent uses associated with this MAC address. He stated that this MAC address was frequently listed as the MAC address associated with log-ins to the e-mail account assigned to Vikram Subbarao Buddhi.

27. Scott Ksander advised that by using the information supplied by the Yahoo subpoena mentioned above he was able to determine that the person using the screen name "extertrimist_bush" was using multiple IP addresses belonging to other students at Purdue University to post the threatening messages.

28. On 1/18/06, SA Lawrence Brown and I interviewed Vikram Subbarao Buddhi (DOB 5/10/71) at the Purdue University Police Department. Buddhi admitted to posting the threatening messages on Yahoo! message boards on 12/13/05 under user name "extertriemist_bush". Buddhi also admitted to deliberately using the IP addresses other than his

own in an attempt to conceal his identity. Buddhi admitted to having a computer in his residence.

29. Buddhi claimed not to use illegal or prescription drugs, alcohol and not to be suffering from any mental illnesses. He claimed not to be under the influence of any foreign substance at the time he posted the threatening messages.

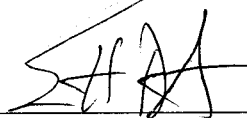
30. Information from the Department of Homeland Security / Immigration Customs Enforcement (DHS/ICE) intelligence office revealed that Buddhi came to the United States on an F1 Student visa in 1996 to pursue a doctorate degree in mathematics. Buddhi extended this visa every year since 1996 through the filing on an I-20 extension form with DHS/ICE. In 2004, Buddhi's I-20 extension form filed by Purdue University indicated that Buddhi was now pursuing a masters degree in industrial engineering. Conversations with Purdue University officials revealed that Buddhi was originally a teaching assistant in the mathematics department but was removed from that position and in now a teaching assistant in the industrial engineering department.

31. A records check revealed that as of 4/13/06, Buddhi still resided at the location commonly known as: Purdue Village - 208 Airport Road, Apartment #2, West Lafayette, Indiana.

Conclusion

32. I respectfully submit there is probable cause to believe that Vikram Subbarao Buddhi has violated Title 18, United States Code, Section 871(a) and 879(a), and 844(e).

FURTHER YOUR AFFIANT SAITH NOT



ERIC DICKEY
Special Agent
United States Secret Service

Subscribed and sworn before me the 13 day of April, 2006.



ANDREW P. RODOVICH
United States Magistrate Judge
Northern District of Indiana