

United States District Court

EASTERN DISTRICT OF

LOUISIANA

In the Matter of the Search of

(Name, address or brief description of person, property or premises to be searched)

4811 W. Metairie Avenue
Metairie, Louisiana 70001

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: 03 MAG 12/4-1

I, Special Agent Sung-Ki Lim being duly sworn depose and say:

I am a(n) Special Agent with the Federal Bureau of Investigation and have reason to believe
Official Title

that on the person of or on the property or premises known as (name, description and/or location)
4811 W. Metairie Avenue, Metairie, Louisiana 70001

in the Eastern District of Louisiana

there is now concealed a certain person or property, namely (describe the person or property to be seized)

See Attachment B.

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

concerning a violation of Title 18 United States code, Section(s) 1030(a)(5)(B)(iv)

The facts to support a finding of Probable Cause are as follows:

See Attached Affidavit.

Continued on the attached sheet and made a part hereof.

Yes No

S-K Lim
Signature of Affiant

Sworn to before me, and subscribed in my presence

December 04, 2003
Date

at New Orleans, Louisiana
City and State

Louis Moore, Jr., United States Magistrate Judge
Name and Title of Judicial Officer

Louis Moore, Jr.
Signature of Judicial Officer

**AFFIDAVIT OF SUNG-KI LIM IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT**

I, Sung-Ki Lim, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), San Francisco Division, San Francisco, California, being duly sworn, depose and state as follows:

A. Introduction and Agent Background

1. This Affidavit is in support of a search warrant application for a search warrant for evidence and instrumentalities of criminal activity conducted at **4811 W. Metairie Avenue, Metairie, Louisiana 70001** (the premises), the home of **DAVID JEANSONNE**, further described in Attachment A. As set forth herein, there is probable cause to believe that on the premises there exist evidence and instrumentalities of violations of Title 18, United States Code, Sections 1030(a)(5)(B)(iv) (intentionally causing a threat to public health or safety by transmission of program, code or command).

2. I have been a Special Agent of the FBI since April 2002 and am currently assigned to the Hayward Resident Agency at San Francisco, California. Since joining the FBI, I have investigated violations of federal law in computer-related crimes, and currently investigate federal violations concerning computer intrusions. I have gained experience through previous work experience, classes, and everyday work related to conducting these types of investigations. Prior to joining the FBI, I was an electrical engineer for seven years.

3. As a Federal Agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

4. The statements contained in this Affidavit are based on my experience and background as a Special Agent and on information provided by other agents of the FBI.

B. Sources of Information Used in this Affidavit

5. The facts set forth below are based upon my own personal observations, my own training and experience, reports and information provided to me by the victim entities, information obtained from my conversations with other law enforcement agents knowledgeable in computer disciplines, and records I have obtained. Since this affidavit is being submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause that evidence and instrumentalities of violations of the statutes listed in this affidavit will be found at the premises to be searched.

C. Background Regarding Computers, the Internet and E-Mail

6. Based on my knowledge, training, and experience, and the experience of other law enforcement officers, I have knowledge of the Internet and how it operates. I know that the Internet is a worldwide computer network which connects computers and allows communications and transfer of information and data across state and national boundaries. Individuals who utilize the Internet can communicate by using electronic mail (hereinafter "e-mail"). The following paragraphs describe some of the functions and features of the Internet as it relates to the subject of this search warrant.

7. Internet Service Providers ("ISPs"): Individuals who have an Internet account and an Internet based e-mail address must have a subscription, membership, or affiliation with an

organization or commercial service which provides access to the Internet through its servers. A provider of Internet access and services is referred to as an Internet Service Provider or "ISP."

8. Electronic Mail ("E-Mail"): E-mail is an electronic form of communication which usually contains written correspondence. It is similar to conventional paper mail in that it is addressed from one individual to another and is usually considered private. An e-mail usually contains a message "header" which generally displays the sender's e-mail address, the recipient's e-mail address, and the date and time of the e-mail transmission. If a sender chooses to do so, he or she can type a subject line into the header. E-mail message "headers" usually contain information, such as identification of the sender's ISP and Internet Protocol (IP) address, which enables law enforcement officers to trace the message back to the original sender. In order to do so, information must be obtained from the sender's ISP through a Grand Jury subpoena.

An IP address is a unique code given to a computer when connected to the Internet through an ISP. The IP address is assigned to an end user by an ISP. The IP address, along with the date and time, usually allows the ISP to identify the location of the end user and/or subscriber.

9. WebTV: Based on my training and experience and interviews with Julie Pearl, Security Program Manager at Microsoft (MS) Corporation, I have learned the following about WebTV:

a. WebTV is a product offered by MS that allows users to connect to the Internet through a standard television. WebTV users can also send and receive e-mail once connected to the Internet. In order for customers to utilize the product, they must purchase hardware and a service plan from WebTV. The hardware consists of a WebTV box, which acts as a computer, a

keyboard, and various interface wires. The WebTV box connects to the Internet through a modem connected to the user's standard phone line. When users sign-on, the WebTV box dials a local number through its internal modem and connects to Internet through the WebTV servers.

b. MS is the ISP for consumers who have purchased the WebTV product and service plan.

c. Older versions of the WebTV box incorporated a hard disk drive, while more recent versions contain some form of storage media within the box. The information stored on the media consists of "cookies," which reveal recently visited web sites.

10. The term "computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such devices."

D. Applicable Law Relating to Computer Offenses

11. Title 18, United States Code, Section 1030 prohibits the following conduct:

(a)(5)(A)(i) Whoever knowingly causes the transmission of a program, information, code or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

* * *

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if complete, have caused) –

(iv) a threat to public health or safety;

12. Section 1030(e)(2)(B) defines "protected computer" as a computer "which is used in interstate or foreign commerce or communication" MS' WebTV computer servers are

located in Santa Clara, California, which communicate via the Internet to the WebTV boxes. Those WebTV boxes are located in users' homes across the United States.

E. Facts Supporting Probable Cause

13. In an interview on December 23, 2002 and in subsequent followup interviews, Julie Pearl, Security Program Manager at Microsoft (MS) Corporation, informed me of the following:

a. On or shortly after July 14, 2002, twenty-one WebTV customers received an e-mail from an unknown individual which contained an attached program. The message purported the attachment was a harmless program that when executed, changed the user's display colors. In fact, however, the attachment contained a malicious script that was concealed within the code of the program. The malicious script executed four specific commands, unbeknownst to the victim:

- i) Reset the modem dial-in number to "9-1-1."
- ii) Copied the victim's website history and stored it to a location on the Internet at "<http://ykladmfp.netfirms.com/cgi-bin/h11.txt>." The victim's website history is a list of all the websites recently visited.
- iii) E-mailed the victim's WebTV unique serial ID number to the e-mail account "timmy@postmark.net."
- iv) Forwarded the original e-mail containing the malicious script to eighteen specified WebTV e-mail addresses.

As a result of the script commands, the next time the user attempted to log in to Web TV, the WebTV box dialed 9-1-1 instead of the local modem telephone number. For those users who did not attempt to log in for the rest of the day, the WebTV box is programmed to log into the main

center at midnight everyday. Therefore, for some users the WebTV box attempted to call 9-1-1 at midnight. Of the twenty-one victims, ten reported to MS' customer service that the local police either called or visited their residence in response to the 9-1-1 call. The twenty-one victims were located throughout the country from Rochester, New York to San Diego, California.

b. Pursuant to an order issued under 18 U.S.C. § 2703(d), MS provided the results of its investigation to the FBI. MS' investigation showed that the malicious e-mail was sent from an ISP located in the United Kingdom. The malicious e-mail was sent from a website that allowed users to send e-mails with attachments anonymously. This feature is not a regular service provided by the website and was disabled shortly after the incident. The website, www.airportgarage.co.uk, appears to be a legitimate site that offers information on used vehicles for sale in the county of Suffolk, England.

c. MS searched their logs for all incoming e-mails to WebTV users from timmy@postmark.net around the time of the incident. MS discovered that a WebTV user, exdrinker@webtv.net, received two e-mails from timmy@postmark.net a day before the incident, on July 13, 2002. The two e-mails contained code that was very similar to, and in many cases exactly the same as, the code in the malicious script sent out the next day on July 14, 2002.

d. The e-mail address exdrinker@webtv.net was registered to DAVID JEANSONNE at 4811 W. Metairie Avenue, Metairie, Louisiana 70001. Further investigations by MS into e-mails sent to and from exdrinker@webtv.net revealed that JEANSONNE received several more e-mails that contained code that was similar to that of the malicious script prior to the day of the incident, July 14, 2002. The e-mails were sent from either himself or an anonymous e-mail account.

e. MS also provided e-mails between exdrinker@webtv.net and another WebTV user, CHRISTOPHER FISH, using the e-mail accounts tyhart@webtv.net and tyhart@angelfire.com. Those e-mails implicate JEANSONNE as the individual behind the malicious script. The following excerpts are from those e-mails:

Sun, 14 Jul 2002 15:36:19 -0700 (PDT)

From: tyhart@webtv.net

To: ExDrinker@webtv.net (Me)

Subject: Re: HAHA

I just checked and see what you mean. I gotta laff at them with the police coming over... but please now just lie real low... stay real out of sight for some time.

Mon, 22 Jul 2002 19:44:36 -0700 (PDT)

To: exdrinker@webtv.net

From: "Christopher Fish" <tyhart@angelfire.com>

Reply-To: tyhart@angelfire.com

Hi Dave - Thank you for the script info. But, as you can imagine, that has not been what I think of when I think of you lately. How are you? Any problems? As much as I value your friendship and appreciate your support, I wish you had not done that... at least not the "9 you know what" aspect. It could have caused terrible trouble for you, and has been stressful for me because a cloud of suspicion has settled over me due to the target. Please only email me to this service. And please provide a web-based email addy [address] I can reach you at.... Chris

Sat, 10 Aug 2002 08:22:13 -0700 (PDT)

From: ExDrinker@webtv.net (Me)

To: tyhart@webtv.net

...I recently had to hack into <http://DNetworks.net> to get their attention concerning my attachment mailer, <http://dnetworks.net/Tools/att4.cgi>. Seems they thought it was OK to say they created the tool. They soon discovered the hard way (BASICII WAS HERE!!) it was not. There is a thread in rotatory77's ng [newsgroup] about it.

news.alt.discuss.clubs.public.internet.misc.rotatory77

If you didn't notice, taxx's addy was changed to taxx1.cgi...had to reconfigure it's output to octet-stream rather than text/html. MsnTV killed the latter since the 911 Bug made headlines. Touche'!

They say they patched the 911 exploit, but they only patched one possible syntax of the phone-setup url...it is easily enabled using a variety of combinations of arguments. Maybe we'll let them discover that out without any help...

Sat, 10 Aug 2002 08:47:35 -0700 (PDT)

From: tyhart@webtv.net

To: ExDrinker@webtv.net (Me)

...I notice that the 911 historic episode seems to have had a sobering affect on the ty_sux original regulars. MrsV and some others, who started this current assault on me, were not around the hate group at the time of 911.

Yes, I read the thread about BasicII in Rotatory. Very respectful :-)
It's a damn shame some people are not respectful without being shaken by the collar.

..You live in new Orleans... what an awesome place to be. I never knew anyone from there... except Jamester :(

...Have a great weekend, and thanks for answering.... Chris

f Pursuant to a Federal Grand Jury Subpoena served on June 2, 2003, Jeremy Abraham, Network Abuse Specialist at Lycos Incorporated, provided that the e-mail account, tyhart@angelfire.com, was registered to CHRISTOPHER FISH at 1390 Main Street, Osterville, Massachusetts. Pursuant to a Federal Grand Jury Subpoena served on July 17, 2003, Catherine Taelor, MS compliance Manager, provided that the e-mail account tyhart@webtv.net is registered to CHRIS FISH at 1390 Main Street, Osterville, Massachusetts.

g. Based on my investigation, I believe that JEANSONNE and FISH are friends who communicate only through the Internet. Furthermore, I believe that in the past, FISH, using his tyhart@webtv.net account, was disliked by some WebTV users. The last communication highlighted above between JEANSONNE and FISH indicate that those account holders who disliked FISH were specifically targeted by JEANSONNE. I believe that JEANSONNE wanted to ensure that eighteen specific individuals received the malicious e-mail. This was done by programming the script to resend the same malicious e-mail to eighteen specific e-mail addresses each time the program was executed. Since the script was hidden, some of the victims forwarded the e-mail with the attachment to other friends. As a result, there was a total of twenty-one victims

h. MS discovered a link between exdrinker@webtv.net and a previous WebTV user, basicii@webtv.net. One example, in the last communication highlighted above mentions an on-line discussion about BasicII. Both accounts registered the name DAVID or DONNA JEANSONNE as the user. The account associated with exdrinker@webtv.net registered an alternate credit card number that was the same as the primary credit card number associated with basicii@webtv.net.

i. MS' records also showed that the basicii@webtv.net account registered an address located at 4723 W. Metairie Avenue, Metairie, Louisiana, while the exdrinker@webtv.net account registered an address located in the same proximity at 4811 W. Metairie, Metairie, Louisiana.

j. MS has informed me that Basiciii@webtv.net was a well-known hacker among the WebTV community who was subsequently banned from WebTV for his behavior. WebTV terminated the Basiciii@webtv.net account for unauthorized activity a total of 17 times from

December 2000 to November 2002. Some of the unauthorized activity involved hacking, creating hacking methods, impersonating other users, and repeatedly setting up new accounts after being banned from WebTV.

k. Furthermore, the following e-mails between tyhart@webtv.net and exdrinker@webtv.net support the conclusion that exdrinker and basicii are the same individual, and that that person's name is Dave (or David):

Mon, 1 Jul 2002 05:49:12 -0700 (PDT)
From: tyhart@webtv.net
To: exdrinker@webtv.net

Hi Dave -

...Also, since that is so similar to your last "post on the fly" trick, it would immediately ID ExDrinker as BASICII. You would get reported to Donnelly and TOSed [Donnelly is a MS employee, TOSed is a termination of service] in a heartbeat... and your host sites would be jeopardized.

I hope you understand my concerns, Dave. Let's keep you around for awhile, OK :-)

Chris

Mon, 1 Jul 2002 06:24:08 -0700 (PDT)
From: tyhart@webtv.net
To: exdrinker@webtv.net

Hi again Dave ...

I been trying to think what I would do if i were in your position. I would want to have fun and amaze people or why bother with webtv. So I would set up a persona that was unrelated to BASICII. I would adopt the type of email address and handle using alt characters that teenagers use: script4z@webtv.net (d4=A7killz)... that sort of thing.

Then I would create a sig with a grad table, maybe a scope and a name logo. And also post with RAM every time...

Like a lot of the posters and posts here:

news:alt.discuss.clubs.public.internet.misc.rotatory77

Then I would post in that group to introduce myself. I would be inarticulate and brief in the posts/... like a 17 year old would be. I would use swears as parts of speech here and there.

I would just post generally with meaningless posts to threads (as they do in the younger "scriptahz" groups) for a few weeks.

I would post everyday how I am studying perl and cgi and ask some simple pl and cgi questions.

After a about a month, I would start with the tricks... "hey look what I can do now".

The point is to establish a persona, style, and behavior pattern that is unrelated to BASICII. I know it is a lot of work to set up with the name and sig, and posting nothing amazing for a month or so.

But I think you must set up a solid anonymous base before just coming out with amazing tricks. Because when someone no one ever heard of, like exdrinker, just appears out of the blue one day and posts an amazing trick, anybody with a brain instantly knows who it is.

Chris

1 MS routinely monitors newsgroups relating to WebTV topics. From various newsgroups postings, MS' impression of JEANSONNE's background is that he is married with children.

14. WebTV e-mail has limited access outside of the user's home. WebTV e-mail can be accessed on external computers that are connected to the Internet. However, this feature must first be set within the WebTV servers by the user. When this feature is set, the WebTV server acts as a Post Office Protocol (POP) server, which essentially holds inbound e-mails until they are retrieved by the account holder. During the investigation by MS shortly after the incident, exdrinker@webtv.net's account did not have this feature enabled. Therefore, the e-mail account could only be accessed from the WebTV box located at JEANSONNE's residence.

15. On March 18, 2003, a Grand Jury Subpoena was issued on the credit card

account number that was registered to both exdrinker@webtv.net and basicii@webtv.net. The credit card account belonged to DONNA H. JEANSONNE, 4811 W. Metairie Avenue, Metairie, Louisiana (LA) 70001.

16. On November 17, 2003, SA Gary Elmore, New Orleans FBI, confirmed that a 1999 Mitsubishi Mirage parked at 4811 W. Metairie Avenue, Metairie, LA, was registered to DAVID and DONNA JEANSONNE. Under the vehicle's registration, the address for JEANSONNE was 4723 W. Metairie Avenue, Metairie, LA 70001.

17. Further criminal history searches revealed that DAVID JEANSONNE was arrested seven times for alcohol-related offenses and four times for property-related offences. The addresses documented in the criminal history report included both 4723 W. Metairie Avenue, Metairie, LA and 4811 W. Metairie Avenue, Metairie, LA 70001. Based on my investigation, I believe that JEANSONNE moved from 4723 W. Metairie to 4811 W. Metairie, and is currently residing at the latter address.

F. Premises to be Searched

18. 4811 W. Metairie Avenue, Metairie, LA 70001 is more fully described in Attachment A - Premises to be Searched. Attachment A is incorporated by reference into this Affidavit for Search Warrant.

19. Based upon my knowledge, training and experience, and consultations with Julie Pearl, Security Program Manager at Microsoft Corporation, and SA Charles Esposito, an experienced FBI SA assigned to the San Francisco, CA Division and who is specially trained in computer search and seizure and is certified by the FBI as a member of the Computer Analysis Response Team (CART), I believe it is common for individuals who commit computer crimes of this nature to maintain electronic evidence relating to their crimes for an indefinite period of time on their WebTV box and computer systems. I know that electronic information can remain

on the WebTV box and in computer storage media, such as hard drives, for an indefinite period of time. Even when a computer user attempts to delete records from a computer storage medium, the records may still exist and can be recovered through computer forensic techniques. Based on the above and my knowledge, training and experience, I also believe that it is common for individuals who commit computer crimes who move their residence to also move their computer systems with them, thus maintaining electronic evidence relating to their crimes for an indefinite period of time on their computer systems at their new residences.

G. Items to Be Seized

20. Based on all the facts and information described in this affidavit for a search warrant, along with my training, experience, and consultations with others, I believe that there is probable cause to believe that the items described in Attachment B (attached hereto and incorporated herein by reference) are currently located at the premises commonly known as 4811 W. Metairie Avenue, Metairie, Louisiana 70001, and that those items constitute evidence and instrumentalities of JEANSONNE's violation of 18 U.S.C. § 1030(a)(5)(B)(iv). I know that the WebTV box and service does not offer the capability of creating and saving text documents and/or programs or scripts. Because the WebTV box and service does not support word processing, programs like that of the malicious script used in this case would most likely have been created on a computer. Furthermore, based on my training and experience, my conversations with other agents who have training and experience in this area, and my conversations with MS employees, I believe that individuals who have the capability of creating a malicious script and have computer software programming knowledge (such as here), also commonly use and own a computer at their residence. Therefore, I believe that JEANSONNE is an individual who owns a computer and has used that computer to create the aforementioned malicious script. Therefore, any WebTV box and/or computers discovered on the premises is

considered an instrumentality of the violation, and therefore will be seized indefinitely.

21. The terms "records," "document," and "materials," include all of the foregoing items of evidence in whatever form and by whatever means such as records, documents, or materials, their drafts, or their modifications may have been created or stored, including (but not limited to) any handmade form (such as writing, drawing, sketching, with any implement on any surface directly or indirectly), any mechanical form (such as printing or typing), and any electrical, electronic, or magnetic form (such as computer or digital information on an electronic or magnetic storage device, such as floppy diskettes, hard disks, backup tapes, CD-ROMs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as printouts or readouts from any magnetic storage device).

22. The terms "hardware," "software," "documentation," and "passwords" and "data security devices" include the following:

a Hardware: Consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes any data processing devices (such as central processing units (CPUs), memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disks drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be

used to restrict access to computer hardware (such as physical keys and locks).

b. Software: Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word-processing), utilities, compilers, interpreters, and communications programs.

c. Documentation: Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use the computer hardware, software, or other related items.

d. Passwords and Data Security Devices: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

H. The Propriety of the FBI Maintaining Custody of Evidence.

23. Based on my knowledge, training and experience, and consultations with SA Esposito, I know that to completely and accurately retrieve data maintained in computer hardware or on computer software, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary to remove some computer equipment, attached

equipment (peripherals), related instructions (in the form of manuals and notes), as well as the software necessary to operate the computer from its original location and subsequently process the items in a laboratory setting with the assistance of a qualified computer specialist. This is true for the following reasons:

a. Volume of Data Stored: Computer storage devices (like hard disks, diskettes, tapes, laser disks, cartridge drives, optical drives) can store the equivalent of thousands of pages of information. Additionally, a user may try to conceal criminal evidence by storing it in random order with deceptive file names. This may therefore require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

b. Technical Requirements: Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. Data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis. Based on my training and experience I know that computer users sometimes encrypt files, and that such users may keep the encryption passwords or encryption keys separately written in their residences or on a separate computer file.

24. It is therefore requested that agents executing this search warrant be allowed to employ the following procedure upon execution of this search warrant:

a. Initial Review: Upon securing the premises, an FBI CART specialist will make an initial review of any computer equipment or computer peripherals capable of storing or creating information in an electronic format to determine whether it is possible to search these items during the execution of the search of the subject premises in a reasonable amount of time and without jeopardizing our ability to preserve any information stored in an electronic format.

b. Back Up Copy or Seizure: If it is not reasonable to search the equipment on site, a back-up copy will be made of all electronic data including software programs used to create/read the data. If it is not possible to make a back-up copy of these materials, any computer equipment, or computer peripherals will be seized and transported to an appropriate law enforcement laboratory for review.

c. Review Off Premises: Any back-up copies or computer equipment or computer peripherals which are seized for review off the premises, shall be reviewed by appropriately trained personnel to seize any information or data that falls within the list of items to be seized as set forth in Attachment B to this search warrant. Once such a review and seizure has been made of electronic information, any computer equipment taken from the premises shall be returned within a reasonable period of time. This time period may vary depending upon the volume of electronically stored information to be reviewed, and the need for specialized equipment and/or expertise to conduct the review.

25. Due to the characteristics of the WebTV box, "micro" computers or "personal" computers, physical removal of the items is often the more practical alternative, and is often less intrusive than requiring federal agents to remain at the premises for the amount of time

reasonably required to review, analyze, and copy pertinent data. Thus, a presumption exists that such computers may need to be seized and subsequently processed by a qualified computer specialist in a laboratory setting for reasons set forth above.

26. Based upon my knowledge, training, and experience, and the experience of other law enforcement personnel with whom I have conferred, I know that searches and seizures of evidence from computers taken during a search commonly require agents to seize most or all of a computer system's input/output peripheral devices for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. Therefore, in those instances where computers are removed from the premises, to fully retrieve data from a computer system, investigators must seize all magnetic storage devices as well as the central processing units (CPUs).

I. Analysis of Electronic Data

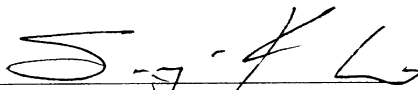
27. The analysis of electronically stored data, whether performed on-site or in a laboratory or other controlled environment, may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); "opening" or reading the first few "pages" of such files to determine their contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; or performing electronic "key-word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

28. A Special Agent of the FBI specially trained in computer evidence recovery will supervise the retrieval of digitally based evidence from the seized computers. Based upon the

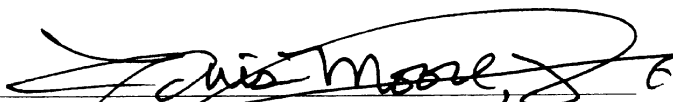
nature of the alleged criminal activity, it is common for incriminating evidence of computer fraud and abuse to be secreted or deleted on a subject's computer system.

J. Request for Sealing

29. Since this investigation is continuing, disclosure of the search warrant, affidavit and application, and the attachments thereto will jeopardize the progress of the investigation. Accordingly, I request that the Court issue an order that the search warrant, this affidavit in support of application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.


Special Agent Sung-Ki Lim
Federal Bureau of Investigation


Subscribed to and sworn before me this 14th day of December, 2003.


THE HONORABLE LOUIS MOORE, JR.
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched is **4811 W. Metairie Avenue, Metairie, LA 70001**. It is further described as a two story duplex located on the 4800 block of W. Metairie Avenue, approximately 75 yards west of the intersection of Zinnia Avenue and W. Metairie Avenue. The duplex is on the north side of W. Metairie Avenue facing south. The exterior color of the house is light blue. There is a two car driveway leading up to an exposed car port and a covered front porch at ground level. The adjacent duplex, 4809 W. Metairie Avenue is the mirror image of 4811. The address, 4811, is clearly marked on the face of the covered front porch facing the street. The duplex is only accessible from the west bound street of W. Metairie. The main entrance is believed to be at the front porch.


LOUIS MOORE, JR.
UNITED STATES MAGISTRATE JUDGE
1204-03

ATTACHMENT B

ITEMS TO BE SEIZED

1. All WebTV boxes
2. All computer hardware, software, documentation, passwords, and data security devices belonging to DAVID JEANSONNE that constitute or contain evidence or fruits of, or that were instrumentalities of, violations of 18 U.S.C. § 1030(a)(5)(B)(iv)
3. Any and all items and documentation relating to WebTV or Microsoft (MS) Internet security.
4. Any records, documents, and materials containing communication in any form describing WebTV, computer hacking techniques and/or hacking activity between "basicil," "exdrinker," or DAVID JEANSONNE and any other persons.
5. Any and all notes, items, documentation, and correspondence, in physical, digital, or any form referring to, or relating to any hacking activities, to include hacking tools and training/how-to manuals;
6. Any and all notes, documents, correspondence, monthly statements and other records, in physical, digital, or any other form, relating to ownership, payments, and/or responsibility for Internet connectivity by or on behalf of DAVID JEANSONNE, computers used or owned by DAVID JEANSONNE, or any other persons or computers to or from which communications were sent or received by DAVID JEANSONNE, or computers used or owned by DAVID JEANSONNE in the course of planning for or effecting the distribution of the malicious script in July 2002.
7. Any records, documents, and materials which refer to WebTV and an event involving a "9-1-1" incident.

The terms "records," "document," and "materials," include all of the foregoing items of evidence in whatever form and by whatever means such as records, documents, or materials, their drafts, or their modifications may have been created or stored, including (but not limited to) any handmade form (such as writing, drawing, sketching, with any implement on any surface directly or indirectly), any mechanical form (such as printing or typing), and any electrical, electronic, or magnetic form (such as computer or digital information on an electronic or magnetic storage device, such as floppy diskettes, hard disks, backup tapes, CD-ROMs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as printouts or readouts from any magnetic storage device).

The terms "hardware," "software," "documentation," "passwords" and "data security devices" include the following:


a. **Hardware:** Consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes any data processing devices (such as central processing units (CPUs), memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disks drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

b. **Software:** Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word-processing), utilities, compilers, interpreters, and communications programs.

c. **Documentation:** Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use the computer hardware, software, or other related items.

d. **Passwords and Data Security Devices:** Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

An FBI Special Agent specially trained in computer evidence recovery shall supervise the retrieval of digital evidence from the computers and related storage devices and materials at the premises to be searched.


LOUIS MOORE, JR.
UNITED STATES MAGISTRATE JUDGE
12-04-03

UNITED STATES DISTRICT COURT

EASTERN

DISTRICT OF

LOUISIANA

In the Matter of the Search of

(Name, address or brief description of person or property to be searched)

4811 W. Metairie Avenue
Metairie, Louisiana 70001

SEARCH WARRANT

CASE NUMBER: 03 MAG 1214-1

TO: Special Agent Sung-Ki Lim - Federal Bureau of Investigation and any Authorized Officer of the United States

Affidavit(s) having been made before me by Special Agent - Sung-Ki Lim who has reason to believe that

Affiant

on the person of or on the premises known as (name, description and/or location)

4811 W. Metairie Avenue, Metairie, Louisiana 70001

in the Eastern District of Louisiana there is now concealed a certain person or property, namely (describe the person or property)

See Attachment A.

I am satisfied that the affidavit(s) and any record testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before

December 14, 2003
Date

not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search (in the daytime -- 6:00 A.M. to 10:00 P.M.) (at any time in the day or night as I find reasonable cause ~~has been established~~) and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to

U.S. Magistrate Judge Louis Moore, Jr.

as required by law.

U.S. ~~Judge or~~ Magistrate Judge

12-04-03 - 9:45 A.M.
Date and Time Issued

at New Orleans, Louisiana
City and State


Louis Moore, Jr.
U.S. Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched is **4811 W. Metairie Avenue, Metairie, LA 70001**. It is further described as a two story duplex located on the 4800 block of W. Metairie Avenue, approximately 75 yards west of the intersection of Zinnia Avenue and W. Metairie Avenue. The duplex is on the north side of W. Metairie Avenue facing south. The exterior color of the house is light blue. There is a two car driveway leading up to an exposed car port and a covered front porch at ground level. The adjacent duplex, 4809 W. Metairie Avenue is the mirror image of 4811. The address, 4811, is clearly marked on the face of the covered front porch facing the street. The duplex is only accessible from the west bound street of W. Metairie. The main entrance is believed to be at the front porch.


LOUIS MOORE, JR.
UNITED STATES MAGISTRATE JUDGE
12-04-03

ATTACHMENT B

ITEMS TO BE SEIZED

1. All WebTV boxes.
2. All computer hardware, software, documentation, passwords, and data security devices belonging to DAVID JEANSONNE that constitute or contain evidence or fruits of, or that were instrumentalities of, violations of 18 U.S.C. § 1030(a)(5)(B)(iv).
3. Any and all items and documentation relating to WebTV or Microsoft (MS) Internet security.
4. Any records, documents, and materials containing communication in any form describing WebTV, computer hacking techniques and/or hacking activity between "basicii," "exdrinker," or DAVID JEANSONNE and any other persons.
5. Any and all notes, items, documentation, and correspondence, in physical, digital, or any form referring to, or relating to any hacking activities, to include hacking tools and training/how-to manuals;
6. Any and all notes, documents, correspondence, monthly statements and other records, in physical, digital, or any other form, relating to ownership, payments, and/or responsibility for Internet connectivity by or on behalf of DAVID JEANSONNE, computers used or owned by DAVID JEANSONNE, or any other persons or computers to or from which communications were sent or received by DAVID JEANSONNE, or computers used or owned by DAVID JEANSONNE in the course of planning for or effecting the distribution of the malicious script in July 2002.
7. Any records, documents, and materials which refer to WebTV and an event involving a "9-1-1" incident.

The terms "records," "document," and "materials," include all of the foregoing items of evidence in whatever form and by whatever means such as records, documents, or materials, their drafts, or their modifications may have been created or stored, including (but not limited to) any handmade form (such as writing, drawing, sketching, with any implement on any surface directly or indirectly), any mechanical form (such as printing or typing), and any electrical, electronic, or magnetic form (such as computer or digital information on an electronic or magnetic storage device, such as floppy diskettes, hard disks, backup tapes, CD-ROMs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as printouts or readouts from any magnetic storage device).

The terms "hardware," "software," "documentation," "passwords" and "data security devices" include the following:


LOUIS MOORE, JR.
UNITED STATES MAGISTRATE JUDGE

12-04-02


a. Hardware: Consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes any data processing devices (such as central processing units (CPUs), memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disks drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

b. Software: Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word-processing), utilities, compilers, interpreters, and communications programs.

c. Documentation: Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use the computer hardware, software, or other related items.

d. Passwords and Data Security Devices: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

An FBI Special Agent specially trained in computer evidence recovery shall supervise the retrieval of digital evidence from the computers and related storage devices and materials at the premises to be searched.


LOUIS MOORE, JR.
UNITED STATES MAGISTRATE JUDGE
12-04-03