To: BM
Fax #: [Omitted]
From: Matthew McLaughlin, FBI Los Angeles
Phone #: (310) 996-3341
Return Fax #: (310) 996-3345
Re: Search warrant and affidavit
Date: 1/30/02
Pages: 29

Comments:

A093

SEARCH WARRANT ON WRITTEN AFFIDAVIT	
UNITED STATES DISTRICT COURT	DISTRICT CENTRAL DISTRICT OF CALIFORNIA
UNITED STATES OF AMERICA v. THE PREMISES KNOWN AS: [Address removed], Sherman Oaks, California	DOCKET NO. MAGISTRATE CASE NO. 02-0125M TO: ANY SPECIAL AGENT(S) WITH THE FEDERAL BUREAU OF INVESTIGATION OR ANY OTHER AUTHORIZED OFFICER

Affidavit(s) having been made before me by the below-named affiant that he/she has reason to believe that on the premises known as

SEE ATTACHMENT A

In the Central District of California there is now being concealed certain property, namely:

SEE ATTACHMENT B

and as I am satisfied that there is probable cause to believe that the property so described is being concealed on the person or premises above-described and the grounds for application for issuance of the search warrant exist as stated in the supporting affidavit.

YOU ARE HEREBY COMMANDED to search on or before ten (10) days (not to exceed 10 days) the person or place named above for the property specified, serving this warrant and making the search (in the daytime -- 6:00 A.M. to 10:00 P.M.) and if the property be found there to seize it, leaving a copy of this warrant and receipt for the property taken, and prepare a written inventory of the property seized and promptly return this warrant to the duty U.S. Magistrate judge as required by law.

NAME OF AFFIANT	SIGNATURE U.S. MAGISTRATE JUDGE **	DATE/TIME ISSUED
JOHN I. PI	JENNIFER T. LUM HONORABLE JENNIFER LUM	January 16, 2002 @8:49 am

* If a search is to be authorized "at any time in the day or night" pursuant to Federal Rules of Criminal Procedure Rule 41 (a), show reasonable cause therefor.
** United States Judge or Judge of a State Court of Record.

NK

ATTACHMENT A

PREMISES TO BE SEARCHED

[Address removed], SHERMAN OAKS, CALIFORNIA ("SUBJECT PREMISES") -- further described as follows: a single-story family residence, with white stucco sidings, a red brick front, and a light brown shingle roof. A detached car garage was located behind the house. The front of the residence faces east, has approximately three windows, a front door, and one large tree in the front yard of the house. The house was located in the southwest corner of the intersection of [Address removed].

ATTACHMENT B

ITEMS TO BE SEARCHED

A. Records, documents, programs, applications and materials which reflect malicious computer activity including copies of computer exploits, hacking tools and programs, lists of user names, passwords, credit card numbers, computerized logs, account names, personal telephone books, personal address books, exploits and other programs used

to obtain unauthorized access of computer systems or information or launch denial of service at acks on computer systems;

B. Records, documents, program applications and materials which reflect the identities and activities of UNDERGROUND COUNTERACTIVE ASSEMBLAGE UNIVERSAL NETWORK, UNDERGROUND CONFIDENTIAL ASSOCIATION/UNDERGROUND NETWORK, UCA, U.C.A., UCAUN, U.C.A.U.N, RAISE THE FIST, RAISETHEFIST, RTF, UNITED GRAFFITI FRONT, UGF, 2CP, TWOCP, 2-COOL PRODUCTIONS, Sherman Martin AUSTIN, Joseph PARKER, Josh PARKER, and [Name removed] including documentation, correspondence, notes, photographs, invoices, billing information, financial information, subscriber information, bulletin postings, Internet Relay Chat logs, electronic mails, Internet connection records, Internet activity logs, webpages, computer programs, computer code, and programming manuals.

C. Records, documents, programs, applications and materials regarding explosives, destructive devices, weapons of mass destruction, improvised explosive devices, NEW WORLD ORDER, NWO, INTERNATIONAL MONETARY FUND, IMF, WORLD ECONOMIC FORUM, WEF, and threats against the United States government, the President, and its officials including documentation, correspondence, notes, bulletin postings, Internet Relay Chat logs, electronic mails, webpages, computer program computer code, and programming manuals.

D. Records, documents, programs, applications and materials regarding SPEAKEASY.NET, AMERICA ONLINE (AOL), NETZERO.NET, WWW.RAISETHEFIST.COM, WWW.2CP.COM, 2CP.DYN.DHS.ORG, STEREOS2000.COM, ARMADASTYLE.COM, UNDERNET, and IMUSIC ARTIST DIRECT NETWORK including documentation, correspondence, notes, invoices, billing information, financial information, subscriber information, bulletin postings, Internet Relay Chat logs, electronic mails, Internet connection records, Internet activity logs, webpages, computer programs, computer code, and programming manuals.

E. Indicia, of occupancy including bills, letters, invoices, rental. agreements tending to show ownership, occupancy or control of the premises or the above-described items.

F. As used above, the terms records, documents, programs, applications or materials includes records, documents, programs, applications or materials created, modified or stored in any form.

G. In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:

i. Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial review of any computer equipment and storage devices to determine whether these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data.

ii. If the computer personnel determine it is not practical to perform an on-site search of the data within a reasonable amount of time, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. The computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

iii. Any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offense, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offense specified above. *[Cryptome would appreciate information on the legal basis for retaining seized data merely because it is encrypted and there is no proof that it fits any of these five characteristics. Send to jya@pipeline.com]*

iv. In searching the data, the computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data is within the items to be seized as set 25 forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.

v. If the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure, the government will return these items within a reasonable period of time not to exceed 60 days from the date of seizure unless further authorization is obtained from the Court.

H. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

i. Any computer equipment and storage device capable of being used to commit, further or store evidence, of the offense listed above;

ii. Any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;

iii. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

iv. Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software;

v. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

vi. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

AFFIDAVIT

I, JOHN I. PI, being duly sworn, hereby depose and state as follows:

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) currently assigned to the National Infrastructure Protection Squad of the Los Angeles Field Division. I have been a Special Agent with the FBI since 1997. Since 1997, I have conducted investigations involving computer intrusions, computer fraud, violent crimes; and weapons of mass destruction. Before joining the FBI, I received a bachelor of science degree in computer science from Columbia University School of Engineering in Now York, and I was employed as a computer engineer for IBM Inc. in Poughkeepsie, New York for approximately two years. I am currently the course instructor for a law enforcement training course, "Cyber Crime Investigation." I am a board certified Emergency Medicine physician with specialty interests in emergency services, toxicology, and trauma. I have worked with poison control centers and emergency services and have detected and treated numerous victim of biological and chemical poisoning as well as penetrating and blunt traumas. I have participated in weapons of mass destruction investigations, including the bombing of the United States Embassy in Tanzania, Atlantic Olympic bombing, and the latest New York City World Trade Center bombing. My current responsibilities include the investigation of computer intrusions and malicious computer activities on the Internet as well as investigation involving weapons of mass destruction.

2. This affidavit is made in support of an application for a search warrant for the residence of Sherman Martin AUSTIN (AUSTIN), date of birth April 10, 1983, located at [Address removed], Sherman Oaks, California, where I believe evidence of, as specifically set forth below, violations of Title 18, United State Code, Sections 1030

(computer f aud and abuse) and 842(p)(2) (distribution of information relating to explosives, destruc ive devices, and weapons of mass destruction), may be located. This affidavit is intended to show that there is probable cause for the search warrant and does not purport to set forth all of my knowledge of or investigation into this matter.

DEFINITIONS AND BACKGROUND INFORMATION

3. Internet, also known as the World Wide Web (WWW), refers to the global information system, which physically is comprised of individual computers linked together by telecommunication lines, based on Internet Protocol.

4. Internet Protocol (IP) specifies that each computer or system (computer) linked to the Internet has a globally unique address, known as the IP address, which identifies the computer at any given time.

5. A domain name is a text name equivalent of an IP address, which is consists of numbers only.

6. Digital Subscriber Lines, also known as DSL, is a form of telecommunication lines where computer and other digital data are transmitted. Each DSL line has a. physical installation address.

7. A webpage is a document on the Internet.

8. A website is an organized collection of webpages and is owned and organized by an individual, company, or organization. Each website and its webpages have their unique identifier, known as the Uniform Resource Locator (URL). WWW.RAISETHEFIST.COM and WWW.JRIFILMS.ORG/HOME.HTML are examples of URL's for a website and a webpage.

9. A domain server is an Internet computer where a website and its webpages are located.

10. A computer intrusion occurs when an unauthorized individual or entity breaks into or gain access to a computer of another individual or entity via a computer system vulnerability or security breach.

11. A website defacement occurs when an original webpage of an Internet website is replaced by another replacement webpage, which may contain substituted messages, content, links, and program codes.

12. A denial of service (DOS) attack occurs when a user, company, or organization is deprived of the services of a resource they would normally expect to have, such as a temporary loss of network connectivity, usually via a computer system vulnerability or security breach.

13. Port Scanning refers to the art of systematically scanning the ports of a computer. A port is a place where information is transmitted into and out of a computer. Port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks by system administrators; however, port scanning by computer intruders on victim computers is malicious in nature and is a way of looking for a weakened access point to enter the victim's computer.

14. Electronic mail, also known as Email, is a form of message transmission between two computers over communication networks.

15. Internet Relay Chat (IRC) is a form of real-time message transmission between two or more users across the Internet in a fashion similar to CB radio.

16. IRC channel, also known as a chat room, is where users may join to discuss a specific topic set for that channel. Each IRC channel has one or more operators who own and control the activities of that IRC channel, such as setting the topic of discussion.

17. Based on my previous experience in the investigation of computer intrusion matters, I learned that computer intruders frequently use fictitious names and contact information in order to avoid detection and identification by victims and law enforcement officers. I also learned that computer intruders frequently use unique aliases or nicknames to identify themselves with each other.

18. Based on my previous experience in the investigation of computer intrusion matters, I learned that computer intruders frequently communicate with each other via Internet webpages, Emails, electronic bulletin boards, news postings, and IRC channels, Topics communicated include methods of computer intrusions, plans of computer intrusions, system vulnerabilities, and credits of computer intrusion activities.

19. Based on my previous experience in the investigation of illegal Internet activities, I learned that illegal information may be transmitted, obtained, and propagated an the Internet.

20. Based on my previous experience in the investigation of computer intrusion matters, I learned that computer viruses and other unauthorized computer intrusion programs frequently had the appearance and disguise of legitimate computer programs but performed additional and/or covert tasks.

21. Title 18, United State Code, Section 1030 statute states "whoever knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value shall be punished."

22. Title 18, United State Code, Sections 842 (p) statute states that "it shall be unlawful for any person to teach or demonstrate the making or use of an explosive, a destructive device, or a weapon of mass destruction, or to distribute by any means information pertaining to, in whole or in part, the manufacture or use of an explosive, destructive device, or weapon of mass destruction, with the intent that the teaching demonstration, or information be used for, or in furtherance of, an activity that constitutes a Federal crime of violence.

23. Title 18, United State Code, Section 2101 statute states that "riots, whoever travels in interstate or foreign commerce or uses any facility of interstate or foreign commerce, including, but not limited to, the mail, telegraph, telephone, radio, or television, with intent to incite riot, or to organize, promote, encourage, participate in, or carry on riot or to commit any act of violence in furtherance of a riot or to aid or abet any person in inciting or participating in or carrying on a riot or committing any act of violence in furtherance of a riot."

PREMISES TO BE SEARCHED

24. The premises to be searched at [Address removed], SHERMAN OAKS, CALIFORNIA ("SUBJECT PREMISES") is further described as follows: a single-story family residence, with white stucco sidings, a red brick front and a light brown shingle roof. A detached car garage was located behind the house. The front of the residence faces east, has approximately three windows, a front door, and one large tree in the front yard of the house. The house was located in the southwest corner of the intersection of [Address removed].

SUMMARY OF INVESTIGATION

25. As set forth below, the FBI is currently investigating several computer intrusions on computer systems throughout the United States and the illegal distribution of information relating to explosives, destructive devices, and weapons of mass destruction. The computer intrusion activities have been launched against private commercial, government, and military computers. Some of these computer intrusion activities resulted in website defacement. Some of these computer intrusion activities resulted in the removal or destruction of proprietary information stored on private and military computer networks. In addition, the FBI is investigating the illegal distribution of

information elating to explosives, destructive devices, and weapons of mass destruction. The In erne website, WWW.RAISETHEFIST.COM (RAISETHEFIST.COM), contained information and instructions regarding the making and use of improvised explosive devises for illegal purposes.

26. The SUBJECT PREMISES is linked to the computer intrusions, website defacement and illegal distribution of information relating to explosives, destructive devices, and weapons of mass destruction based on, among other things, records and information obtained from the Internet website, RAISETHEFIST.COM, Internet Service Providers ("ISPs"), victim witnesses, cooperating witness, and public records on the Internet.

STATEMENT OF PROBABLE CAUSE

27. On May 1, 2001, the FBI initiated an investigation of a computer intrusion activity by an identity known as the UNDERGROUND COUNTERACTIVE ASSEMBLAGE/UNIVERSAL NETWORK (UCAUN), also known as UNDERGROUND CONFIDENTIAL ASSOCIATION/UNDERGROUND NETWORK, U.C.A., UCA, U.C.A.U.N., and UCAUN, based on the information provided by Guy TICHY (TICHY), of Streamwood, Illinois. TICHY frequently visited a website, WWW.JRIFILMS.ORG (JRIFILMS.ORG), of JAMES REDFORD INSTITUTE FOR TRANSPLANT AWARENESS of Los Angeles, California. This website was dedicated to organ transplantations. On or about January 2001, TICHY observed that the homepage, JRIFILMS.ORG/HOME.HTML, was defaced, and UCAUN claimed the responsibility for this computer intrusion and defacement activity. This defaced webpage contained anti-government and militant messages as well as a conspiracy theory of the New World Order.

28. On or about May 3, 2001, I reviewed the program coding of the above defaced webpage and determined the coding contained a link to another website, RAISETHEFIST.COM.

29. On or about May 3, 2001, I conducted a review of publicly available information on the Internet website RAISETHEFIST.COM and learned that it was an anarchist website, This website contained numerous organized webpages, which contained anti-government (primarily the United States), anti-capitalism, and militant messages that promoted communism and advocated violence. This website had a section for the UNITED GRAFFITI FRONT, also known as UGF, which had the motto, "spraypaint as weaponry against the corporate lies."

30. On or about May 3, 2001, I conducted a search of publicly available information on the Internet using the keywords, "UCA' and "UCAUN" and learned that approximately forty web sites had the above defacement webpage.

31. On or about May 3, 2001, I conducted a search of publicly available information on the Internet and learned that the administrative, billing, and technical contact for RAISETHEFIST.COM was Sherman AUSTIN of 2-COOL PRODUCTIONS, located at [Address removed], Sherman Oaks, California (SUBJECT PREMISES), telephone number [Telephone number removed], and an email address of UCA@NETZERO.NET. The domain server for RAISETHEFIST.COM was located at the Internet Protocol (IP) address of 64.81.234.187, also known as NS1.2CP,COM. Joseph PARKER, of 2871 King Avenue, Los Angeles, California 91423, was listed as the registrant for RAISETHEFIST.COM. Based on the Thomas Guide map of the Los Angeles County and public records on the Internet, I determined that the registrant information of RAISETHEFIST.COM was fictitious.

32. On or about May 1, 2001, I conducted a search of publicly available information on the Internet and learned that the domain name, 2CP.COM, was registered to 2-COOL PRODUCTIONS located at [Address removed], Sherman Oaks, California (SUBJECT PREMISES), telephone number [Telephone number removed], and an email address of UCA@NETZERO.NET. The domain server for 2CP.COM was located at the Internet Protocol (IP) address of 64.81.234.187, also known as NS1.2CP.COM.

33. On or about May 3, 2001, I conducted a review of the public telephone database, POWERFINDER 2000, FIRST EDITION, and learned that the telephone, number [Telephone number removed] was registered to Neil BLUMENKOPF, Sherman Oaks, California.

34. On or about May 3, 2001, I conducted a search of publicly available information on the Internet using the keyword "UCAUN" and learned the following:

a. A computer program with the name, TROOP.CGI was recovered from three websites.

b. TROOP.CGI was a computer program written in the computer language CGI, also known as the Common Gateway Interface, which is a standard way for an Internet computer to pass an Internet user's request to an application program and to return data back to the originating user.

c. At the beginning of TROOP.CGI program was the following comment:

"# Important security script from sysCheck Deamon
DO NOT DELETE! This script contains important data
in order for this machine to process information
correctly."

d. The body of TROOP.CGI program contained a program code designed to open the port 2001 of a computer operated by Belvoir Army Base, located at Fort Belvoir, Virginia. This program code checks for the keyword "Password:" on the above port and returns the message "found the shit" if the keyword matched the text returned from the above port.

e. The body of TROOP.CGI program contained a program code designed to return data back to another CGI script, /UCAUN/AUTOS/INDAINNAVY/COMMANDER.CGI, located at the IP address of 2CP.DYN.DHS.ORG, also known as 63.248.254.133. Based on the investigation of this case, I determined that the IP address 63.248.254.133 was a DSL line previously utilized by AUSTIN (details are provided in the following sections),

35. On or about June 11, 2001, I conducted a review of the Long Beach Police Department (LBPD) records and learned that AUSTIN was arrested on May 1, 2001 by LBPD in the violent demonstration at Long Beach, California. AUSTIN was charged by the State of California for the violation of California Penal Codes (PC) Sections 404(A) riot, 406 rout, 407 unlawful assembly, and 182(A)(1) conspire to commit a crime.

36. On or about June 24, 2001, I was notified by Intelligence Research Specialist Michael A. DORN of the Federal Bureau of Investigation that AUSTIN was cited by San Diego Police Department (SDPD) for a traffic violation, California Vehicle Codes Section 21456(8), "pedestrian crossing against a don't walk or wait sign" during a demonstration against the 2001 BIOTECHNOLOGY INDUSTRY ORGANIZATION INTERNATIONAL CONVENTION AND EXHIBIT event at San Diego, California.

37. On or about June 27, 2001, I conducted an interview of William DRAIN (DRAIN), of Edison, Texas. DRAIN provided the following information:

a. On or about November 2000, UCAUN intruded and defaced the computer of JOHNSTON PRINTING COMPANY (JOHNSTON) located at Edison, Texas.

b. DRAIN provided a copy of the defacement webpage by UCAUN to me. Upon the review of this webpage, I determined that this defacement webpage was the same one as the defacement webpage of JRIFILMS.ORG.

38. On September 10, 2001, I conducted a review of publicly available information on the Internet the website, RAISETHEFIST.COM, and learned that a main webpage, DC.RAISETHEFIST.COM had the title of "BREAK THE BANK!," which was a reference to the meeting of the WORLD BANK AND INTERNATIONAL MONETARY FUND (IMF) in Washington, D,C., which was scheduled to take place on or about September 29, 2001. This webpage included the following:

a. Links to information and instructions on transportation, housing, maps, guide, and outreach information for the protesters of this IMF event.

b Info mation on "police tactic[S] and how to defeat them," "unarresting comrades at a demons ration," "defensive weapons," and "de-bloc'ing."

c. The webpage, RAISETHEFIST.COM/EXIT/WEAPONS.HTML, had the title of "defensive weapons" and included the following information:

i. "In developing defensive-offense tactics, our bodies cant provide for everything we do in a battle. That is why we need to be prepared with the proper tools to execute our goal."

ii. "Many different weapons and tools can be used in street fighting. Make sure that you keep them clean of fingerprints, DNA fibers (hair follicles, etc.), especially explosives because they may not always ignite."

iii. "The following weapons are widely used and effective in executing the goal of the demonstration." This statement was followed by instruction on making and use of slings, slingshot, boomerangs, ninja stars, Molotov cocktails, smoke bombs, fuel-fertilizer explosives, pipe bombs, draino bomb, soda bottle bomb, and match head bomb.

iv. "Bust out Bart Simpson style and fire some tiny metal pellets at pigs. Very effective when used by large groups at once" was referenced under the use of slings.

v. "These easily available or homemade items are great when dealing with illegal situations. It can shield any media or police cameras from catching anyone on from participating in an illegal act. It can also disorient the police when they are advancing on the crowd" was referenced under the usage of smoke bombs.

vi. "Remember, be careful and responsible with these explosives. Don't blow yourself up, or any of your comrades! Don't get caught!"

d. Under the webpage, RAISETHEFIST.COM/EXIT/TACTICS.HTML, for "police tactics and how to defeat them" included the following information:

i. "One would attack the poorly defended positions by hurling rocks and firebombs. Since regular police could not sustain that for any longer period of time, the riot police would have to come to their aid. Then the second group of protesters would attack the now much weakened main objectives and possibly seize them."

ii. "If more aggressive approach was desired, one group of protesters would lead the police in a trap by making a quick assault and falling back immediately afterwards, as if fleeing the scene. The police would usually pursue them haphazardly, falling easy prey to a flanking attack of other protesters who would suddenly rush out from side streets."

iii. "Cars can be wonderful barricades and can be easily set on fire."

39. On November 7, 2001, I conducted an interview of Jeff Alan POWELL (POWELL) of Gulf Port, Mississippi who provided the following information:

a. POWELL is a web graphic design specialist.

b. POWELL had known AUSTIN via the Internet since approximately 1995.

c. AUSTIN used the nickname UCAUN on the Internet Relay Chat (IRC) channels on UNDERNet, an IRC network. POWELL provided fifteen logs of conversations on the IRC channel, #FREEDOMFIGHTERS, on UNDERNet, where AUSTIN used the nickname UCAUN and chatted with POWELL, who used the nickname, DRSKEET. On a log dated on January 28, 2000, POWELL stated that AUSTIN impersonated a police officer by stating his name to be Josh PARKER who was 26 years old and "worked with the Junior Police squad at the Los Angeles Police Academy,"

d. POWELL determined the true identity of UCAUN to be AUSTIN via the coding of webpages authored by AUSTIN and by the registrant information of the domain name, 2CP.COM which was registered to Sherman AUSTIN of 2-COOL PRODUCTIONS of [Address removed], Sherman Oaks, California and email address of UCA@NETZERO.NET.

e. AUSTIN was associated with the websites, 2CP.COM and 2CP.DYN.DHS.ORG.

f. In or about 2000, POWELL spoke to others on the Internet who stated that AUSTIN defaced numerous websites. POWELL provided two defacement webpages by AUSTIN, both of these webpages credited UCAUN for the defacement activities and had the same UCAUN "signatures."

g. AUSTIN with the IMUSIC user name of UCAUN, posted a user profile in the IMUSIC ARTIST DIRECT NETWORK, and it included the following information:

i. The IMUSIC username of UCAUN was registered to a male living in Los Angeles, California, with a date of birth of April 10, 1983.

ii. Under "My Bio," AUSTIN stated, "you fucking cops and feds better hide. The bullet is about to rikashade with a global uprise."

iii. AUSTIN listed RAISETHEFIST.COM as his Internet homepage.

40. On November 8, 2001, I conducted an interview of Neil D. BLUMENKOPF (BLUMENKOPF), of Encino, California, who provided the following information:

a. BLUMENKOPF is an attorney for the City of Los Angeles.

b. BLUMENKOPF has the home telephone number [Telephone number removed]. Based on previous investigation, I determined that this number was the same telephone number and fax number used in the subscriber's information for both website, RAISETHEFIST.COM and 2CP.COM. Furthermore, I determined that this telephone number differed from the home telephone number of AUSTIN, [Telephone number removed], by two numbers.

c. BLUMENKOPF denies any association with RAISETHEFIST.COM. 2CP.COM, and AUSTIN. BLUMENKOPF did not authorized AUSTIN to utilize his home telephone number [Telephone number removed].

d. BLUMENKOPF received numerous telephonic calls and faxes regarding the fraudulent Internet business activities of AUSTIN and 2CP.COM.

41. On November 9, 2001, Special Agent John W. DUNN of the Federal Bureau of Investigation and I conducted an interview of a cooperating witness (CW) who provided the following information:

a. CW positively identified a photograph of AUSTIN, which was provided by me. Subsequent to this identification, CW provided to me one computer image of AUSTIN and one computer image of his residence, which AUSTIN had previously provided to CW via the Internet.

b. CW had known AUSTIN since approximately 1997.

c AUSTIN had made comments about making bombs to get rid of "capitalist pigs." Aus in sta ed that he wanted to shut down the government system and that he would do whatever was necessary to take out the government.

d. AUSTIN told CW that AUSTIN personally designed and implemented RAISETHEFIST.COM. This website was hosted from the home computers of AUSTIN.

e. AUSTIN told CW that AUSTIN operated another website, 2CP.COM also 6 known as 2-COOL PRODUCTIONS, which advertised website designs and CGI programming.

f. On or about 1998 and 1999, AUSTIN was involved with the selling of stolen car stereos on the Internet via the website, STEREOS2000.COM, which the CW helped AUSTIN design.

g. AUSTIN was known to use the nicknames, UCA, UCAUN and RAISETHEFIST, on the Internet and was known to use the email address of RAISETHEFIST@AOL.COM.

h. AUSTIN told CW that AUSTIN participated in many protests and demonstrations. During these events, AUSTIN frequently wore a gas mask or a bandana to cover his face.

i. AUSTIN told CW that AUSTIN began hacking when he was about 13 years of age. AUSTIN had done numerous computer intrusion activities on the Internet, including intrusions into Department of Defense (DoD) computer networks. AUSTIN removed proprietary contents from these DoD computers.

j. CW identified the defaced webpage of JRIFILMS.ORG to be one of AUSTIN's defacement webpages via the unique "signature" of UCAUN.

42. On or about November 14, 2001, I conducted an interview of Kelley A. GRANDMAISON of Harmony, Maine who provided the following information:

a. GRANDMAISON is an Internet Information Specialist.

b. GRANDMAISON had known AUSTIN via the Internet since approximately 1997.

c. AUSTIN used the nickname UCAUN on the Internet Relay Chat (IRC) channel, #UFO, on UNDERNet, an IRC network. GRANDMAISON determined the true identity of UCAUN to be AUSTIN via the registrant information of 2CP.COM.

d. Via the Internet, GRANDMAISON was threatened and subjected to Denial of Service (DOS) Attacks by AUSTIN on numerous occasions after she expressed her disagreement with AUSTIN's militant view and his conspiracy theory. At one time, a DOS attack by AUSTIN caused a catastrophic crash of the harddrive of GRANDMAISON's computer. Via her computer activity log, GRANDMAISON determined that one of the DOS attacks originated from 2CP.COM.

e. GRANDMAISON provided a log of a conversation on the IRC channel, #FREEDOMGUARD, on UNDERNET, dated on July 11, 1999, where AUSTIN used the nickname UCAUN and the email address of 2CP@2CP.COM. AUSTIN was an operator for this IRC chat room, #FREEDOMGUARD. In this IRC log, AUSTIN chatted with approximately six other individuals about their New World Order conspiracy theory, and AUSTIN talked about his computer intrusion activities and attempted to recruit others to his militant activities. AUSTIN stated,the following:

i. "The U.C.A.U.N. hacks into thousands of websites, displaying the NWO message to the world ... on the hacked message, I should put like if you want to become a freedom fighter troop then please e-mail ..."

ii. "I have broken into .. HOW many Department of Defence Interest Computer Systems (DoDICS) tivek ?? I think 3 or 4 ..."

iii. "I have hundreds of US DoD Documents which I stole from hacking into US DoD computer systems, so everyone can see it."

iv. "I know we can. We have got to do it. We need guns and uniforms. We can do it and take it over, steal their technology, We have to do it, We must!!!!!!"

v. I can get people !! lots of people within weeks. I mean a whole freakin army and the, guns... Money is no problem here ... I can also get other people to invest in the opperation. We cab do it!!! I will start it tonight.. I still have thousands of websites to display the nwo message on.. etc.. and new ones every freakin day. Hundreds of thousands of people will be looking at it."

vi. "I will need you all first to just e-mail me: 2CP@2CP.COM with subject: NWO."

f. GRANDMAISON provided a defacement webpage by AUSTIN under the name f UCAUN. On the hacked message, AUSTIN stated the following:

i. "This server was hacked into so we could simply to get a warning message accross to the public."

ii. "The U. C, A, is currently seeking anyone who has at least 1 or more of the following qualifications: weapons training, inteligance in telecommunications, X-military/Navy Personal, Inteligence in computer hacking, financial support to help carry out this operation, ability to fly aircraft, ..., ability to provide uniforms... guns... etc..., the will to fight."

iii. "We are establishing UFF (UCAUN Freedom Fighter) troops into all major cities world wide. If you would like to become a UFF troop, then please e-mail: UCA@NETZERO.NET

iv. "We don't gather weapons, plan extreem opperations and risk our lives for nothing. This is REAL."

g. GRANDMAISON retrieved an AUTOMATED CREDIT-CARD HACKING SYSTEM from the website, 2CP.COM. The graphical user interface (GUI) of this credit card hacking system contained the line, "data fetched from Global-Track UCAUN software."

h. GRANDMAISON believed that AUSTIN conducted DOS attacks on GRANDMAISON's computer using a spoofed IP address, 192.31.75.202. which was registered to the ARMY ARTIFICIAL INTELLIGENCE CENTER, THE PENTAGON, Washington, D.C. GRANDMAISON observed DOS attacks from the above IP address immediately following arguments she had with AUSTIN on the Internet. These DOS attacks were similar in methodology to previous DOS attacks from AUSTIN.

43. on or about November 16, 2001, I received records from SPEAKEASY NETWORK (SPEAKEASY), located in Seattle, Washington, which hosted the IP address 64.81.234.187 where the websites, RAISETHEFIST.COM and 2CP.COM were located and learned the following:

a. The above IP address was assigned to a DSL connection installed at a residence located at [Address removed], Sherman Oaks, California (SUBJECT PREMISES).

b The DSL connection at [Address removed], Sherman Oaks, California, had been ac ive since March 14, 200 .

c. The name of the DSL subscriber was [Name removed].

d. The phone number for the DSL subscriber was [Telephone number removed].

e. [Name removed] stated in an Email to SPEAKEASY that she obtained this account "for my son Sherman's use."

f. Activity logs showed a webpage, at the above IP address and the domain name of ARMADASTYLE.COM which had the tide of ARMADA DESIGN, and it contained the logo, "copyright 1996-2000 by Sherman Austin - Armada Design and 2CP."

g. Activity logs showed an email from "TWOCP" with the email address of UCA@NETZERO.NET to SPEAKEASY.

h. Activity logs showed 14 complaints were filed against this IP address for port scanning activities since April 19, 2001. The complainants included private, commercial, university, and government entities, including the Civil Air Patrol (CAP. GOV).

i. Activity logs showed the previous DSL fine utilized by AUSTIN had the IP address of 63.248.254.133.

44. On or about December 10, 2001, I conducted a review of publicly available information on the Internet the website, RAISETHEFIST.COM and learned the following:

a. The webpage, DC.RAISETHEFIST.COM had been moved, modified and renamed to another web page, RAISETHEFIST.COM/EXIT/RECLAIM.HTML (RECLAIM.HTML).

b. RECLAIM and its links contained the same information and instruction about the making and use of improvised explosives as DC.RAISETHEFIST.COM.

c. The webpage, RAISETHEFIST.COM/EXIT/AGC/MAIN.HTML (AGC), listed an acknowledgement to "SHERMAN@RAISETHEFIST."

d. The webpage, RAISETHEFIST.COM/EXIT/INDEX.HTML, listed AGC as one of the sites that "I currently work on or am affiliated with in some way."

e. The webpage, RAISETHEFIST.COM/EXIT/INDEX.HTML, also listed RECLAIM.HTML as one of the sites that "I currently work on or am affiliated with in some way."

f. I also observed a graphical image of President George W. Bush with an overlay of a rifle scope sight centered on his face with the caption, "Bush Wanted! Dead or Alive!" on the webpage, www.raisethefist.com/news.cgi?artical=wire/9163wanted.gifIMG.article.

45. On or about January 8, 2002, I conducted a review of publicly available information on the Internet the website, RAISETHEFIST.COM and learned that a webpage, www.raisethefist.com/news.cgi?artica1=wire/83903t4a.article, included the following information:

a. "Shut down the WEF!" (WEF was an abbreviation for the World Economic Forum which was to be held on or about January 31 through February 4, 2002 in New York City.)

b. "Stop the WEF by any means necessary!"

c. "This.guide was developed as means to inspire and inform participants of the upcoming resistance in NY against the World Economic Forum. With this convergence comes the need to organize security, safety and direct action. The information within these pages is to hopefully strengthen these tactics amongst our resistance."

d. Links to same information on security culture, Black Bloc, defense weapons (including the use and making of improvised explosives and weapons of mass destruction), and shield constructions as the IMF webpage, DC.RAISETHEFIST.COM.

e. AUSTIN, using the nickname RTF, stated, "the reason why we feel the meetings need to be stopped by any means necessary is because of the police violence in the first place."

46. I know, based on my training and experience, that a computer is necessary to access the Internet through the use of a DSL connection, I also know, based on my training and experience, that it is likely that a computer located inside the SUBJECT PREMISES will contain evidence of a user's access and activities on the Internet.

COMPUTER DATA

47. Based upon my training, experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of system and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. Searching computer systems requires the use of precise scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the 4 physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing fifteen gigabytes of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 7.5 million pages of data, which, if printed out, would completely fill a 10' x 12' x 10' room to the ceiling.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in

an image file which cannot be viewed when the image file is opened. Therefore, a subs an ial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities, of a crime.

ITEMS TO BE SEIZED:

48. Based on the foregoing, I respectfully submit that there is probable cause to believe that the following items, which constitute evidence of violations of Title 18, United State Code, Sections 1030 (computer fraud and abuse) and 842(p)(2) (distribution of information relating to explosives, destructive devices, and weapons of mass destruction), will be found at the SUBJECT PREMISES:

a. Records, documents, programs, applications and materials which reflect malicious computer activity including copies of computer exploits, hacking tools and programs, lists of user names, passwords, credit card numbers, computerized logs, account names, personal telephone books, personal address books, exploits and other programs used to obtain unauthorized access of computer systems or information or launch denial of service attacks on computer systems;

b. Records, documents, programs, applications and materials which reflect the identities and activities of UNDERGROUND COUNTERACTIVE ASSEMBLAGE/UNIVERSAL NETWORK UNDERGROUND CONFIDENTIAL ASSOCIATION/UNDERGROUND NETWORK, UCA, U.C.A., UCAUN, U.C.A.U.N., RAISE THE FIST, RAISETHEFIST, RTF, UNITED GRAFFITI FRONT, UGF, 2CP, TWOCP, 2-COOL PRODUCTIONS. Sherman Martin AUSTIN, Joseph PARKER, Josh PARKER, and [Name removed] including documentation, correspondence, notes, photographs, invoices, billing information, financial information, subscriber information, bulletin postings, Internet Relay Chat logs, electronic mails, Internet connection records, Internet activity logs, webpages, computer programs. computer code, and programming manuals.

c. Records, documents, programs, applications and materials regarding explosives, destructive devices, weapons of mass destruction, improvised explosive devices, NEW WORLD ORDER, NWO, INTERNATIONAL MONETARY FUND, IMF, WORLD ECONOMIC FORUM, WEF, and threats against the United States government, the President, and its officials including documentation, correspondence, notes, bulletin postings, Internet Relay Chat logs, electronic mails, webpages, computer programs, computer code, and programming manuals.

d. Records, documents, program, applications and materials regarding SPEAKEASY.NET, AMERICA ONLINE (AOL), NETZERO.NET, WWW.RAISETHEFIST.COM, WWW.2CP.COM, 2CP.DYN.DHS.ORG, STEREOS2000.COM, ARMADASTYLE.COM, UNDERNET, and IMUSIC ARTIST DIRECT NETWORK including documentation, correspondence, notes, invoices, billing information, financial information, subscriber information, bulletin postings, Internet Relay Chat logs, electronic mails, Internet connection records, Internet activity logs, webpages, computer programs, computer code, and programming manuals,

e. Indicia of occupancy including bills, letters, invoices, rental agreements tending to show ownership, occupancy or control of the premises or the above-described items.

f. As used above, the terms records, documents, programs, applications or materials includes records, documents, programs, applications or materials created, modified or stored in any form.

g. In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:

i. Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the ("computer personnel") will make an initial review of any computer equipment and storage devices to determine whether these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data.

ii. If the computer personnel determine it is not practical to perform an on-site search of the data within a reasonable amount of time, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. The computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

iii. Any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offense, (2) fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offense specified above.

iv. In searching the data, the computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.

v. If the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41 (b), the government will return those items within a reasonable period of time not to exceed 60 days from the date of seizure unless further authorization is obtained from the Court.

h. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

i. Any computer equipment and storage device capable of being used to commit, further or store evidence of the offense listed above;

ii. Any computer.equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modem, docking stations, monitors, printers, plotters, encryption devices and optical scanners;

iii. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks and personal digital assistants;

iv. Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software.

v. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

vi. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

SUMMARY

49. There is probable cause to believe that AUSTIN had deliberately conducted computer in rusion activities into private, commercial, and possibly government computers in violation of Title 18, United State Code, Sections 1030 (computer fraud and abuse) based on the following facts:

a. AUSTIN was known as UCA, UCAUN, 2CP, and RAISETHEFIST on the Internet based on the witnesses, POWELL, GRANDMAISON, and CW.

b. The billing,, technical, and administrative contact for RAISETHEFIST.COM was Sherman AUSTIN of 2-COOL PRODUCTIONS located at SUBJECT PREMISES. The registrant of 2CP.COM was 2-COOL PRODUCTIONS located at SUBJECT PREMISES.

c. The defacement webpages of AUSTIN contained a link to RAISETHEFIST.COM and an Email address of UCA@NETZERO.NET, both of which were used by AUSTIN in the records provided by SPEAKEASY. Furthermore, UCA@NETZERO.NET was also the email address for the registrant of 2-COOL PRODUCTIONS.

d. All the defacement webpages of AUSTIN had the same signatures of UCAUN and the same anti-government and militant messages as well as a conspiracy theory of the New World Order.

e. On the IRC chat log, #FREEDOMGUARD, provided by GRANDMAISON, AUSTIN using the, nickname UCAUN claimed the responsibility of defacing websites and posting the New World Order message to the world, AUSTIN also claimed the responsibility of computer intrusion activities into three or four government DoD computer systems.

f. On the IMUSIC ARTIST DIRECT NETWORK user profile, provided by POWELL, AUSTIN had a username of UCAUN which was registered to a male living in Los Angeles, California, with a date of birth April 10, 1983, which was the date of birth of AUSTIN. AUSTIN also listed his Internet homepage to be RAISETHEFIST.COM.

g. The activity logs provided by SPEAKEASY showed at least fourteen complaints filed against the IP address of RAISETHEFIST.COM for port scanning activities since April 19, 2001. The complainants included private, commercial, university, and government entities, including Civil Air Patrol.

50. There is probable cause to believe that AUSTIN had violated Title 18, United States Code Section 842(p)(2) (distribution of information relating to explosives, destructive devices, and weapons mass destruction) in furtherance of riot based on the following facts;

a. AUSTIN posted on the website, RAISETHEFIST.COM, numerous webpages which contained explicit information and instructions on, the making and illegal use of improvised explosive devices and destructive weapons. AUSTIN stated, "make sure you keep them clean of fingerprints, DNA fibers (hair follicles, etc.), especially explosives because they may not always ignite and "these easily attainable or homemade items are great when dealing with illegal situations. It can shield any media or police cameras from catching anyone on film participating in an illegal act." On the webpage, RAISETHEFIST.COM/INDEX.HTML, AUSTIN stated that the above website was one of the projects that "I currently work on or am affiliated with in some way."

b. [Name removed], the mother of AUSTIN and subscriber of the above DSL line, stated in an Email to SPEAKEASY that she subscribed the DSL line of RAISETHEFIST.COM was for "my son Sherman's use."

c. AUSTIN stated to CW that AUSTIN personally designed and implemented RAISETHEFIST.COM, which was hosted from the home computers of AUSTIN.

d. AUSTIN had made comments to CW about making bombs and stated that he would do whatever was necessary to take out the government.

e. AUSTIN advocated violent radical anti-government and militant activities on his website, RAISETHEFIST.COM and defacement webpages. This was also documented on IRC chat log, #FREEDOMGUARD, provided by GRANDMAISON, where AUSTIN attempted to recruit others to join him in armed militant movements.

f. One of the defacement webpages of AUSTIN, provided by GRANDMAISON, attempted to recruit others with experiences in weapons training, computer hacking, ability to fly aircraft, and ability to provide uniforms and guns to join UFF, also known as UCAUN FREEDOM FIGHTER. AUSTIN used UCA@NETZERO.NET as his Email address for this defacement webpage.

51. There is probable cause to believe that items constituting evidence of violations of Title 18, United State Code, Sections 1030 (computer fraud and abuse) and 842(p)(2) (distribution of information relating to explosives, destructive devices, and weapons of mass destruction), as more specifically set forth above and in Attachment "A," will be found at [Address removed], Sherman Oaks, California based on the following:

a. The records of SPEAKEASY showed that the DSL line serving the IP address of RAISETHEFIST.COM and 2CP.COM was physically located at SUBJECT PREMISES.

b. The registration information of the domain name RAISETHEFIST.COM showed AUSTIN located at SUBJECT PREMISES as the administrative, billing, and technical contact.

c. The registration information of the domain name 2CP.COM showed AUSTIN located at SUBJECT PREMISES as the subscriber.

JOHN I. PI, Affiant
Special Agent, FBI

AFFIDAVIT subscribed and sworn to before me this 16th day of January, 2002.

JENNIFER T. LUM
UNITED STATES MAGISTRATE JUDGE

Transcription and HTML by Cryptome.