

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SEALED BY ORDER
OF THE COURT

UNITED STATES OF AMERICA

v.

WILLIAM VEYNA

WARRANT FOR ARREST

aka guyzzz, aka _ _ _ _ , aka pammy, aka 1010101, aka 5555, aka
i_love_dact, aka 8675309

CASE NUMBER:
05 70479 RS

YOU ARE HEREBY COMMANDED to arrest WILLIAM VEYNA
and bring him or her forthwith to the nearest magistrate to answer a(n)

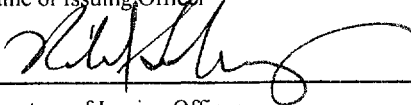
Indictment Information Complaint Order of court Violation Notice

charging him or her with (brief description of offenses)

Conspired to Commit Criminal Copyright Infringement and Circumvent Copyright Protection Systems, in violation of 18 U.S.C. § 371; Criminal Copyright Infringement and Aiding and Abetting, in violation of 17 U.S.C. § 506(a)(1), and 18 U.S.C. §§ 2, 2319; and Circumventing a Technological Measure that Protects a Copyright Work and Aiding and Abetting, in violation of 17 U.S.C. §§ 1201(a)(1)(A), 1204(a)(1), and Title 18 U.S.C. § 2.

Honorable Richard Seeborg

Name of Issuing Officer



Signature of Issuing Officer

United States Magistrate Judge

Title of Issuing Officer

June 28, 2005 San Jose, California

Date and Location

Bail fixed at \$ No Bail by Honorable Richard Seeborg

Name of Judicial Officer

RETURN

This warrant was received and executed with the arrest of the above-named defendant at

DATE RECEIVED	NAME AND TITLE OF ARRESTING OFFICER	SIGNATURE OF ARRESTING OFFICER
DATE OF ARREST		

ORIGINAL WARRANT HELD BY
U.S. MARSHAL & SA JESSIE
DO NOT MAKE REFERENCE TO THIS COURT
ANY ABOVE OFFICE FROM ANY

UNITED STATES DISTRICT COURT **ORIGINAL FILED**

NORTHERN DISTRICT OF CALIFORNIA JUN 28 2005

SEALED BY ORDER OF THE COURT

RICHARD W. WIEKING CLERK, U.S. DISTRICT COURT NORTHERN DISTRICT OF CALIFORNIA SAN JOSE

UNITED STATES OF AMERICA

v.

WILLIAM VEYNA

aka guyzzz, aka _-_-_, aka pammy, aka 1010101, aka 5555, aka i_love_dact, aka 8675309 9243 Johnell Road Chatworth, California 91311 (Name and Address of Defendant)

CRIMINAL COMPLAINT

CASE NUMBER:

05 70479 RS

I, the undersigned complainant, being duly sworn state the following is true and correct to the best of my knowledge and belief. Between in or about June 2003, to the present, in the Northern District of California and elsewhere, defendant(s) did, (Track Statutory Language of Offense)

See Attachment A, which is incorporated herein by reference, which alleges Conspiracy to Commit Criminal Copyright Infringement and Circumvent Copyright Protection Systems; Criminal Copyright Infringement and Aiding and Abetting; and Circumventing a Technological Measure that Protects a Copyright Work and Aiding and Abetting

in violation of Title 18, United States Code, § 2319 (criminal copyright infringement), Title 17, United States Code, § 506 (copyright infringement), § 1201 (Circumvention of copyright protection systems) and § 1204 (Criminal offenses and penalties), and Title 18, United States Code, § 371 (conspiracy) & § 2 (aiding and abetting). I further state that I am a Special Agent with the Federal Bureau of Investigation and that this complaint is based on the following facts:

- See Attached Affidavit in Support of Issuance of Criminal Complaint and Arrest Warrant

X Continued on the attached sheet and made a part hereof.

Approved as to form:

AUSA Mark L. Krotoski

Signature of Complainant Special Agent Julia Jolie Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence June 28, 2005

HON. RICHARD SEEBORG U.S. Magistrate Judge

Name and Title of Judicial Officer

at San Jose, California

Signature of Judicial Officer

**AFFIDAVIT IN SUPPORT OF ISSUANCE OF
CRIMINAL COMPLAINT AND ARREST WARRANT**

I, Julia B. Jolie, Special Agent of the Federal Bureau of Investigation (FBI), being duly sworn, depose, and state:

INTRODUCTION

1. I am an FBI Special Agent, currently assigned to the Oakland Resident Agency, San Francisco Division. I have been employed by the FBI since April 1995. As a Special Agent of the FBI, I am authorized to investigate violations of the laws of the United States, and I am a law enforcement officer with authority to execute arrest and search warrants under the authority of the United States. I have participated in a variety of criminal investigations, including criminal copyright infringement, Internet fraud, computer fraud, wire fraud, and mail fraud.

2. I make this affidavit in support of the issuance of a criminal complaint and arrest warrant against the following individual:

NAME: WILLIAM VEYNA
aka guyzzz, aka _-_-_, aka pammy, aka 1010101,
aka 5555, aka i_love_dact, aka 8675309
DOB: 8/20/1970
ADDRESS: 9243 Johnell Road
Chatworth, California 91311

3. As set forth more fully herein, there is probable cause to believe that the above defendant has committed violations of Title 18, United States Code, Section 2319 and Title 17, United States Code, Section 506(a)(1) (Criminal copyright infringement); Title 17 United States Code, Section 1201 (Circumvention of copyright protection systems) and Section 1204 (Criminal offenses and penalties); Title 18 United States Code, Section 371 (Conspiracy to commit the foregoing offenses), and Section 2 (Aiding and Abetting the foregoing offenses).

RELEVANT STATUTES

Criminal Copyright Infringement

4. Title 17, United States Code, Sections 506(a), (b) provide, in pertinent part:

(a) Criminal Infringement.—(1) In general.--Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed –

(A) for purposes of commercial advantage or private financial gain;

(B) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than \$1,000;

Penalties For Criminal Copyright Infringement

5. The penalties for violations of Title 17, United States Code, Sections 506, are set forth in Title 18, United States Code, Sections 2319(b), (c), (d), which provide in pertinent part:

(b) Any person who commits an offense under section 506(a)(1)(A) of title 17—

(1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than \$2,500;

(2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.

(c) Any person who commits an offense under section 506(a)(1)(B) of title 17, United States Code—

(1) shall be imprisoned not more than 3 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of \$2,500 or more;

(2) shall be imprisoned not more than 6 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than \$1,000.

Circumvention of Copyright Protection Systems

6. Title 17, United States Code, Section 1201, provides in pertinent part:

Section 1201. (a) Violations Regarding Circumvention of Technological Measures.—

(1) (A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.

...

(3) As used in this subsection—

(A) to “circumvent a technological measure” means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner; and

(B) a technological measure “effectively controls access to a work” if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

Penalties For Circumvention Of Copyright Protection Systems

7. The penalties for violations of Title 17, United States Code, Section 1201, are set forth in Title 17 U.S.C. Section 1204, which provides in pertinent part:

(a) In General - Any person who violates Section 1201 or 1202 willfully and for purposes of commercial advantage or private financial gain - (1) shall be fined not more than \$500,000 or imprisoned for not more than 5 years, or both, for the first offense; and (2) shall be fined not more than \$1,000,000 or imprisoned for not more than 10 years, or both, for any subsequent offense.

Conspiracy

8. Title 18 United States Code, Section 371 states, in pertinent part:

If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner of for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.

Aiding and Abetting

9. Title 18, United States Code, Section 2(a) states, in pertinent part:

(a) whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.

SOURCES OF INFORMATION USED IN THIS AFFIDAVIT

10. The facts set forth below are based upon my own personal observations, my own training and experience, reports, e-mails, on-line communications, other information provided to me by the undercover employee (UCE) conducting the undercover investigation, and from my conversations with other law enforcement agents knowledgeable in computer disciplines, and records I have obtained, and my conversations with other private companies who investigate copyright violations and have assisted in this investigation. This affidavit is intended to show that there is probable cause for the issuance of criminal complaints and arrest warrants, and does not purpose to set forth all of my knowledge of or investigation into this matter.

BACKGROUND CONCERNING WAREZ INVESTIGATION

11. In summary, this case involves an undercover investigation of organized groups of individuals and coconspirators – also known as "warez groups" or "warez coconspirators" – engaged in the illegal reproduction and distribution of copyright protected software over the Internet, including the illegal copying of movies, games, and software, in violation of federal copyright laws. The investigation stemmed from a Group II Undercover Operation (UCO) initiated in June 2003 by the Federal Bureau of Investigation (FBI), San Francisco Division and U.S. Attorney's Office, Northern District of California, San Jose Division. During the course of the investigation, investigators identified a number of large-scale software piracy groups, also known as "warez groups" or "warez coconspirators," engaged in the uploading, copying, duplication, reproduction, and distribution of copyright-protected computer software, games, and movies by way of the Internet, in violation of federal copyright and conspiracy laws.

Two Warez Sites: LAD and CHUD

12. During the undercover investigation, two warez sites were established in the Northern District of California, known as LAD and CHUD. The first was originally known as HOT and later named LAD. LAD was a smaller site (approximately 700 megabytes early on) and eventually became an archive site, holding older movies, games, and software (which is currently approximately 3.5 terabytes).¹ The second undercover warez site, CHUD, became an eleven terabyte site. In total, the two warez sites, combined with two servers (called VS and SNOWCAVE) which were provided by warez members, includes approximately 27 terabytes of pirated movies, games, and software, making this one of the largest undercover warez

¹ One terabyte equals approximately one trillion bytes, or approximately 700,000 3.5-inch floppy diskettes.

investigations. David Fish (aka x000x) and dact, among others, were instrumental in establishing CHUD. Acting as a siteop, David Fish, aka x000x agreed to script the site and dact would broker introductions with top warez groups.

13. Numerous warez groups and coconspirators came to the undercover sites to store a large number of movies, games, and software that could be uploaded and downloaded by hundreds of individuals. Warez leaders operated and controlled the sites and established terms of membership and conditions governing and restricting access. Some warez members were compensated under a credit ratio (also known as "ratio access") of one upload amount equal to three downloads (i.e. one gigabyte/three gigabytes) as a means of private financial gain. In other words, an individual who uploaded one movie could download three movies. In addition, other members paid money to other individuals suppliers to obtain early releases of movies, games, or software. Under this large conspiracy, involving multiple individuals and warez groups, hundreds of individuals obtained free, unauthorized access to pirated movies, games, and software. Investigators discovered numerous pre-released movies, which were placed onto the undercover warez site before the scheduled DVD release to the general public.

Distinct Conspiracy Roles

14. The success of any warez conspiracy depends on the roles and contributions of many coconspirators. Based on information obtained in the investigation, and based on my training and experience, I have formed the opinion that the Warez scheme and conspiracy were committed by individuals having distinct roles. While some members may handle multiple roles, other members may only be responsible for one role. Investigators learned that all members hold some responsibility in keeping their warez group and site up and running. In this investigation, the distinct roles have included but were not limited to: **Founders or Leaders** (originally formed the warez group and look for additional members who could provide something of value to the warez group); **Scriptors** (responsible for creating, programing, building the warez site); **Site Operators** (SiteOps) (site manager holding root access to the warez site); **Suppliers** (providing an unauthorized copyrighted movie, game or software); **Cammer** (uses an audiovisual recording device (such as a camcorder) to make an unauthorized copy of a motion picture or other audiovisual work that is protected by the copyright laws); **Equipment Suppliers** (provides hardware (such as hard drives, computer parts, and computer servers) to the warez site); **Brokers** (found groups to participate on the warez site); **Couriers** (charged with gathering computer software programs, games, and movies and uploading them to the warez site); **Encoder** (sometimes referred to as "ripper" and "cracker", is responsible for circumventing the technological measures and protections of copyrighted works on the DVDs to prevent unauthorized access and copying); **Leech** (a member based on friendship, not group affiliation with leech access to the movies, games, and software on the warez site); **Ratio** (a member who was required to fulfill a contribution requirement in order to download copyright works; e.g., the most common ratio is one upload to three downloads, permitting the warez member to download pirated material under a one to three ratio); **Affil** (a warez group that agreed to provide its' first release of movies, games, or software to a particular top site).

15. Warez members took numerous steps to conceal and protect the conspiracy to violate federal copyright laws. For example, the SiteOps group adopted security measures for the warez site; limited access to the warez site to specific members; established separate channels for private communications between members; and used a barter/credit system designed to reward members and provide access to the site based on the contributions of the members.

Nic Identification

16. In order to limit the number of members on the servers (and as an extra security feature), an individual must be invited to the site by a SiteOp. In order to gain access, the member will give his username, IP mask and password to the SiteOp. The username and password are given by the member (it is not issued). No two users can have the same FTP username. The IP mask acts as a filter, allowing the user to only use predetermined IPs to enter the site. The mask offers security for two reasons. First, only IPs that the SiteOp inputted will be able to access the system. Second, a user will not be able to log into the system using another users FTP user account name. When an individual invites himself into the IRC channel from the FTP server, a broadcast message is sent to the IRC channel that states the warez user invited himself and gives his IRC nic name. The IRC nic associated with the FTP user account is stored in a log file, allowing the association to be made between different FTP user accounts and IRC nic names. The UCE is then able to associate the different nics to FTP user accounts by checking the SysOp (system operation) logs.

Recent NDCA Search Warrants For E-Mail Accounts

17. On May 10, 2005, the Honorable Patricia V. Trumbull, Chief United Magistrate Judge, Northern District of California, signed search warrants for the e-mail accounts x000x@earthlink.net and davefish@gmail.com, both of which are known to be used by David Fish. The information obtained from the search warrants confirmed that David Fish had numerous warez communications with warez coconspirator Nate Lovell (aka Pest), a hardware supplier for the warez site, and warez coconspirator known as "Killiz420," who is one of the lead suppliers of movies, games and software to the warez site.

18. On June 2, 2005, the Honorable Richard Seeborg, United States Magistrate Judge, Northern District of California, signed a search warrant for the e-mail accounts of killaz420@hotmail.com, used account used by warez coconspirator known as "Killaz420." The results confirmed communications between Teves, Fish and others concerning the criminal infringement of copyrighted works on the warez sites. Based on online communications with the UCE, killaz420 has indicated that he has five or six sources for pirated DVDs. Killaz420 has provided several unauthorized copyrighted works to the warez sites during this investigation. Investigators learned that Killaz has listed in his address book the suppliers, and some warez members, including but not limited to: tonyd_12@hotmail.com, brando222@aol.com, and hunder.rodriguez@sbcglobal.net, and davefish@gmail.com.

Copyrighted Movies, Games And Software

19. Investigators compiled a directory list from the log of new movie titles that had been uploaded to CHUD and LAD as part of the warez conspiracy, and provided the list to the Motion Picture Association of America (MPAA) for analysis. MPAA confirmed in writing that its member organizations held copyrights to 766 of these movies. Many of these movies were uploaded to CHUD either before or at the time that the movie was being shown in U.S. theaters. As one recent example, the movie "Star Wars: Episode III - Revenge of the Sith (2005)" was placed on the warez site within hours of its theatrical release to the public. Some other examples of the infringed movie titles include Batman Begins (movie) uploaded on the UCO CHUD June 15, 2005 (released in the theaters on June 15, 2005) by an individual known as "OTR," Bewitched (movie) uploaded on the UCO CHUD June 26, 2005 (released in the theaters June 24, 2005) by an individual known as "c2".

20. Directory lists from the uploaded games to CHUD and LAD during the warez conspiracy were provided to the Entertainment Software Association (ESA) for confirmation that copyrights existed for the titled games. ESA confirmed in writing that its member organizations held copyrights to 1, 283 of the games, totaling approximately \$20,981.69. Some examples of the infringed game titles include, Air Force Delta Storm, American Chopper, Bionicle, Doom 3, among many more.

21. Directory lists of the logs of uploaded software to CHUD and LAD during the warez conspiracy were provided to the Business Software Alliance (BSA) for confirmation that copyrights existed for the titled software applications. BSA confirmed in writing that its member organizations held copyrights to 188 of the software applications, totaling approximately \$389,101.82. Some examples of the infringed software titles include Adobe Photoshop, Adobe Workshop CS2, ADOBE Creative Suite. Premium, Adobe Acrobat Professional V7, Autodesk Discreet 3D Studio.Mac.V7, Microsoft.Office.System Professional, Microsoft Office XP Professional SP3, Microsoft Windows XP x64 Pro, Apple.DVD.Studio.PRO.V4, Apple.soundtrack.pro.mac, Sony Vegas plus Dvd Production Suite, Norton 2005, VMware ESX Server, Autodesk Autocad mechanical V2006, Autodesk Revit Volume 7, Autodesk Autocad Volume 2006, ARCGIS Desktop Volume 9, Symantec Antivirus Corporate Edition, among many more.

Circumventing Technological Measures

22. Many new releases for movies, software and games include technological measures designed to protect or limit access to copyrighted materials. For example, many DVDs contain an access control and copy prevention system, including a "Content Scramble System" (CSS). CSS serves as a technological measure to protect the contents of a DVD from unauthorized access and copying, which are thwarted by a scrambled image. Some warez members have developed abilities to circumvent these technological measures protecting the copyrighted content on the DVDs. Once the technological measure is circumvented,

unauthorized access and copying can be permitted. For example, in this investigation the MPAA made a preliminary determination that circumvention tools were being used to bypass the technological measures designed to protect the copyrighted works, or movies. After conducting a preliminary analysis of some the products that had been placed on a server used by x000x that was located in the UCO ISP to encode movies and games, the MPAA confirmed that the following products enabled the circumvention of CSS, (a) AnyDVD; (b) Gordian Knot; (c) DVD2SVCD; (d) DVD Decrypter; (e) DVD Shrink; (f) DVD2AVI; and (g) VirtualDubMod.

DESCRIPTION OF CRIMINAL ACTIVITY

23. Investigators have concluded that WILLIAM VEYNA, aka guyzzz, aka _-_-_, aka pammy, aka 1010101, aka 5555, aka i_love_dact, aka 8675309, has been an active member on the undercover servers since January 9, 2005. VEYNA is the SiteOp on one of the undercover servers known as VS, allowing him to grant access to the server for warez groups and individuals.

24. As the SiteOp of the warez server VS, VEYNA is responsible for administering the site and controlling the daily operations of the server. By this conduct, VEYNA has aided and abetted numerous violations of the criminal copyright infringement laws. The UCE has learned from reviewing the warez site and in communications with VEYNA that he is a member of the warez groups CDZ and Gamerz (a Sony Playstation II, Sony Playstation Portable, Microsoft XBOX, and Nintendo Game Cube encoding and release group). In conversations with Veyna, the UCE discovered that Veyna was responsible for finding sites to affil with the warez groups CDZ and Gamerz. During these conversations with the UCE, VEYNA has admitted working with several warez groups, including TUN, Boozers, and Centropy, in attempting to affil them with VS.

25. A check of the SYSOP (System Operation) logs in combination with the undercover investigation revealed that an account exists for an individual using IP Mask 67.100.99.*, FTP user account names 1010101, aka 5555, aka i_love_dact, aka 8675309 which has access to download warez media from the site. An individual using the above listed FTP account usernames has used the following nicknames while on IRC: guyzzz, _-_-_, and pammy.

26. Through on-line IRC, e-mail conversations and face-to-face meetings with the person connected to the names guyzzz, aka _-_-_, aka pammy, aka 1010101, aka 5555, aka i_love_dact, aka 8675309, the UCE was able to identify the individual from a Department of Motor Vehicles photograph as being WILLIAM VENYA.

27. On or about April 7, 2005, the UCE received an e-mail from chatsworthlake@gmail.com. Attached to the e-mail was a scan of (2) Fry's Electronics receipts for Maxtor hard-drives. The receipts stated that the drives were charged to WILLIAM VEYNA. The e-mail was "signed" William.

28. On April 7, 2005, UCE received a package with return address WILLIAM VEYNA 9243 Johnell, Chatsworth, CA. The package contained 2 Maxtor hard-drives. On April 6, 2005, Venya stated to the UCE on IRC that "i think eveyrin wil be happy wwith the new 12 new drives added on" These drives were to be placed into the server VS.

29. On or about April 25, 2005, the UCE informed VEYNA, via chat and MSN Messenger that he was going to be in the Los Angeles area. Over the following days, UCE and VEYNA agreed that the UCE should pick VEYNA up at his place of business--S1, 8501 Falbrook, Chatsworth, CA. The following is a sample from the messages [VEYNA is zzz--- and AJ is the UCE]

• 4/26/2005 4:55:53 (co)zzz--- AJ veyna:how logn does it take to get form LAX wveyna: ot S1 aletaw: in traffic about one to one and one half hours

30. On April 29, 2005, the UCE met with the person who was identified as WILLIAM VEYNA based on his DMV photograph, at his place of business. The two had coffee at a Starbucks in Chatsworth, CA and discussed the addition of another warez group to the undercover servers. The UCE learned the following information from that meeting. VEYNA stated that the warez group Centropy was very security conscience, however it would be willing to use a private server that the UCE built and installed. VEYNA asked the UCE if he had a spare server VEYNA could use to crack and encode Playstation 2 and Playstation Portable games. VEYNA stated he would send the games to the UCE and the UCE would then install these into the server for VEYNA to crack and encode. VEYNA has two sources for getting pre-released games, one working for Sony, the other working for Activision. VEYNA has also brought in new members to his groups with access to many movies and games for encoding. VEYNA explains how he does this in this conversation on May 7, 2005, VEYNA told the UCE, "ftich is a CDZ new team member. were tring him out. he owns a video retnal store." As part of the conspiracy, it is necessary that warez members recruit individuals who are willing to provide media that would enable the group to continually acquire pre-releases for encoding.

31. According to the warez server logs, on or about the following dates, an individual using FTP user account names 1010101, 5555, and 8675309 downloaded the following media:

05/04/05	Symantec Norton.Ghost	\$ 69.95
05/04/05	ADOBE Photoshop	\$ 599.00
05/06/05	ADOBE Creative Suite.Premium Edition	\$1,199.00
05/15/05	XBox XBMC.Build.0515-RNSSUCKS	\$ 20.00
05/18/05	PS2 Motocross Mania 3	\$ 20.00
05/20/05	PS2 Outlaw Volleyball	\$ 20.00
05/23/05	XBox Madagascar	\$ 20.00
05/24/05	Hitch	\$ 20.00
05/25/05	Pariah	\$ 20.00
05/25/05	Great Battles of WWII	\$ 20.00
05/25/05	Close Combat	\$ 20.00

05/27/05	Adobe Workshop CS2	\$ 599.00
06/07/05	XBox Batman Begins	\$ 20.00
06/12/05	Because of Winn-Dixie	\$ 20.00
06/18/05	XBox Destroy All Humans	\$ 20.00
06/19/05	Batman Begins (movie)	\$ 20.00

The UCO server log files captured the IP address assigned to the computer from which the accounts downloaded files. On May 24, 2005, Covad advised subscriber information for the individual assigned the IP 67.100.99.99 was registered to WILLIAM VEYNA, 9243 Johnell Road, Chatsworth, CA 91311. Based on the foregoing copyright titles reproduced and distributed by WILLIAM VEYNA, he has infringed more than ten (10) copyrighted works, during a 180-day period, which have a total retail value of more than \$2,500.00, including by the reproduction or distribution via the Internet and for the purpose of commercial advantage or private financial gain, in violation of Title 18, United States Code, Section 2319 and Title 17, United States Code, Section 506(a)(1).

32. VEYNA is also responsible for assisting in maintaining the security of the warez servers. On the server logs, 1010101 is listed as a SiteOp on VS, and the Centropy server.

33. After a series of raids by the FBI, known as Operation Fastlink a national take-down of warez sites in April 2004, guyzzz stated the following:

24. 2004 Apr 21 12:52:05 <@guyzzz> prob cuz of all the Busts happnign here in the U.S.
25. 2004 Apr 21 12:52:25 <@guyzzz> i saw him msg chan to deluser himself and purge him
26. 2004 Apr 21 12:54:11 <@guyzzz> just bout every site is closing down for aweek
27. 2004 Apr 21 12:54:17 <@guyzzz> to see what happens
28. 2004 Apr 21 12:55:49 <@guyzzz> ifu want to know my opnion
29. 2004 Apr 21 12:55:53 <@guyzzz> id say SHUT the gl down
30. 2004 Apr 21 12:56:51 <@guyzzz> Sites confirmed busted -> Sites: APV DC FBI FS PI TLZ TB AF1 PI and the curry grp MOONSHINE
31. 2004 Apr 21 12:57:05 <@guyzzz> im pretty laiid back
32. 2004 Apr 21 12:57:11 <@guyzzz> but i shut down my gl sites
33. 2004 Apr 21 12:57:17 <@guyzzz> just to be safe
34. 2004 Apr 21 12:58:27 <@guyzzz> i couldl of let you know 5am pst

Shortly after this conversation, FTP account user names 1010101, aka 5555, aka i_love_dact, aka 8675309, using nickname guyzzz, _ _ _ _ returned to the warez site and has been active ever since.

34. Based on my training and experience, and based on information obtained during the course of the investigation, it can be concluded that guyzzz, using FTP user account names: 1010101, aka 5555, aka i_love_dact, aka 8675309 is a major participant in the warez scene.

VEYNA's ties to premier warez groups as well as his ability to recruit members for different aspects of the scene exemplifies his importance and his part in the warez conspiracy. Furthermore, VEYNA's security awareness confirms his knowledge that his actions are not legal. VEYNA continues to provide equipment to further aid the operation of the site, and receives financial gain by the continuance of his downloading copyrighted media from the site.

35. On May 2, 2005 the UCE placed an encoding server into the UCO that _ _ _ _ instructed him to do during a face-to-face meeting on April 29, 2005 so that _ _ _ _ could encode media, specifically Playstation 2, Playstation Portable (PSP), and movies. On June 24, 2005, the movie "Millions" was uploaded onto VS by 1010101. On June 24, 2005, the movie "Pacifier" was uploaded onto VS by 1010101. Based on my training and experience, and information obtained during the course of the investigation, this conversation indicates VEYNA's interest in circumventing technological measures designed to protect copyrighted works.

36. In furtherance of the conspiracy, and to effectuate its objects, WILLIAM VEYNA committed overt acts, in the Northern District of California, and elsewhere, including:

a. On or about June 22, 2005, defendant WILLIAM VEYNA accessed CHUD and uploaded one or more copyrighted works, including Be Cool, Coach Carter, Twisted, and FIFA Soccer USA (PSP game).

b. On or about June 9, 2005, defendant WILLIAM VEYNA accessed CHUD and downloaded one or more copyrighted works, including Area 51 (game) on June 9 and Battlefield 2 (game) on June 19, 2005.

c. On or about April 7, 2005, defendant WILLIAM VEYNA sent two (2) hard drives to the UCE so that they could be placed into the server VS.

d. On or about April 25, 2005, defendant WILLIAM VEYNA had a face-to-face meeting with the UCE to discuss issues concerning adding warez groups to the site as well as getting a spare server that VEYNA could use to crack and encode media.


37. Based on all of the facts and circumstances described above, I believe that probable cause exists that WILLIAM VEYNA, aka guyzzz, aka _ _ _ _ , aka pammy, aka 1010101, aka 5555, aka i_love_dact, aka 8675309, conspired to commit criminal copyright infringement and circumvent copyright protection systems, in violation of 18 U.S.C. § 371; committed criminal copyright infringement and aided and abetted criminal copyright infringement, in violation of 17 U.S.C. § 506(a)(1)(b), and title 18 U.S.C. §§ 2, 2319(c)(1); and circumvented a technological measure that protects a copyright work and aided and abetted such circumvention, in violation of 17 U.S.C. §§ 1201(a)(1)(A), 1204(a)(1), and Title 18 U.S.C. § 2.

38. Based on all of the facts and circumstances described above, I request the issuance of an arrest warrant for WILLIAM VEYNA, aka guyzzz, aka _ _ _ _ , aka pammy, aka 1010101,

aka 5555, aka i_love_dact, aka 8675309.

REQUEST FOR SEALING


39. The affiant respectfully requests that this affidavit be sealed until the first arrest of the defendant in this case or until such time as the Court directs. Disclosure of the affidavit in support of a complaint and arrest warrant at this time would seriously jeopardize the ongoing investigation, as such disclosure may provide an opportunity to destroy evidence, change patterns of behavior, notify any confederates, or allow the defendant or any confederates to flee or continue flight from prosecution. It may also take some time to locate the defendant prior to his arrest.



JULIA B. JOLIE
Federal Bureau of Investigation

SWORN AND SUBSCRIBED TO BEFORE ME

THIS 28th DAY OF June, 2005



RICHARD SEEBORG
United States Magistrate Judge

**CRIMINAL COMPLAINT
ATTACHMENT A**

18 U.S.C. § 371 - Conspiracy to Commit Criminal Copyright Infringement and Circumvent Copyright Protection Systems

Beginning at a time unknown, but not later than in or about March 2004, and continuing thereafter up to and including the present, in the Northern District of California, and elsewhere, the defendant, **WILLIAM VEYNA, aka guyzzz, aka -----, aka pammy, aka 1010101, aka 5555, aka i_love_dact, aka 8675309**, and others known and unknown, did knowingly agree, combine and conspire to commit offenses against the United States, that is:

- A. Criminal Infringement of a Copyright, by reproducing and distributing at least ten infringing copies of one or more copyrighted works, with a total retail value of more than \$2,500.00, during a 180-day period, for purposes of private financial gain, in violation of Title 17, United States Code, Section 506(a)(1)(A), and Title 18, United States Code, Section 2319(b)(1);
- B. Criminal Infringement of a Copyright, by reproducing and distributing, including by electronic means, at least ten infringing copies of one or more copyrighted works, with a total retail value of more than \$2,500.00, during a 180-day period, in violation of Title 17, United States Code, Section 506(a)(1)(B), and Title 18, United States Code, Section 2319(c)(1);
- C. Circumvent a Technological Measure that Protects a Copyright Work, by willfully, and for purposes of private financial gain, circumventing a technological measure that effectively controls access to a work protected under Title 17 of the United States Code, in violation of Title 17, United States Code, Sections 1201(a)(1)(A), and 1204(a)(1).

All in violation of Title 18, United States Code, Section 371.

17 U.S.C. § 506(a)(1)(B), and Title 18 U.S.C. §§ 2, 2319(c)(1) - Criminal Copyright Infringement and Aiding and Abetting

Between in or about January 2005 and June 2005, in the Northern District of California, and elsewhere, the defendant, **WILLIAM VEYNA, aka guyzzz, aka -----, aka pammy, aka 1010101, aka 5555, aka i_love_dact, aka 8675309**, did willfully, and for the purpose of private financial gain, infringe the copyrights of copyrighted works, that is, copyrighted movies, games and software, by reproducing and distributing via the Internet, ten (10) or more copies of one or more of the copyrighted works, during a 180-day period, which had a retail value of \$2,500 or more, all in violation of Title 17, United States Code, Section 506(a)(1)(B), and Title 18, United States Code, Sections 2, 2319(c)(1).

17 U.S.C. §§ 1201(a)(1)(A), 1204(a)(1), and Title 18 U.S.C. § 2 – Circumventing a Technological Measure that Protects a Copyright Work and Aiding and Abetting

Between in or about January 2005 and June 2005, in the Northern District of California, and elsewhere, the defendant, **WILLIAM VEYNA, aka guyzzz, aka ----, aka pammy, aka 1010101, aka 5555, aka i_love_dact, aka 8675309**, did willfully, and for purposes of private financial gain, circumvent a technological measure that effectively controls access to a work protected under Title 17 of the United States Code, all in violation of Title 17, United States Code, Sections 1201(a)(1)(A), and 1204(a)(1) and Title 18, United States Code, Section 2.

ORIGINAL FILED

JUN 28 2005

RICHARD W. WIEK
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE

1 KEVIN V. RYAN (CASBN 118321)
United States Attorney

2 EUMI L. CHOI (WVBN 0722)
3 Acting Chief, Criminal Division

4 MARK L. KROTOSKI (CASBN 138549)
Assistant United States Attorney

5 150 Almaden Boulevard, Suite 900
6 San Jose, California 95113
7 Telephone: (408) 535-5035
Facsimile: (408) 535-5066

SEALED BY ORDER
OF THE COURT

8 Attorneys for Plaintiff

9
10 UNITED STATES DISTRICT COURT
11 NORTHERN DISTRICT OF CALIFORNIA
12 SAN JOSE DIVISION


13 UNITED STATES OF AMERICA,)
14 Plaintiff,)
15 vs.)
16 WILLIAM VEYNA)
17 aka guyzzz, aka -----, aka pammy,)
18 aka 1010101, aka 5555,)
19 aka i_love_dact, aka 8675309,)
Defendant.)

NO 05-70479 RS
[Proposed]
ORDER GRANTING MOTION TO SEAL

20 Upon motion of the government, and good cause appearing,

21 IT IS HEREBY ORDERED that the complaint in this matter (including the affidavit in
22 support of the complaint and accompanying documents), the government's motion to seal, and
23 the declaration in support of the government's motion to seal, shall be sealed until the
24 defendant's initial appearance or further order of the Court.

25 DATED: June 28, 2005

26 
27 RICHARD SEEBORG
United States Magistrate Judge
28

ORIGINAL FILED

JUN 28 2005

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE
**SEALED BY ORDER
OF THE COURT**

1 KEVIN V. RYAN (CASBN 118321)
United States Attorney

2 EUMI L. CHOI (WVBN 0722)
3 Acting Chief, Criminal Division

4 MARK L. KROTOSKI (CASBN 138549)
Assistant United States Attorney

5 150 Almaden Boulevard, Suite 900
6 San Jose, California 95113
7 Telephone: (408) 535-5035
Facsimile: (408) 535-5066

8 Attorneys for Plaintiff

9 UNITED STATES DISTRICT COURT
10 NORTHERN DISTRICT OF CALIFORNIA
11 SAN JOSE DIVISION

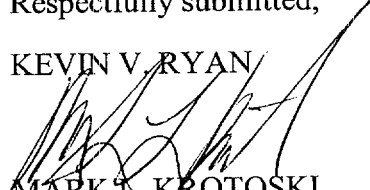
12 UNITED STATES OF AMERICA,)
13 Plaintiff,)
14 vs.)
15 WILLIAM VEYNA)
16 aka guyzzz, aka -----, aka pammy,)
17 aka 1010101, aka 5555,)
18 aka i_love_dact, aka 8675309,)
Defendant.)

~~NO. 05-70479~~ RS

MOTION TO SEAL

19 The United States of America respectfully requests the Court to seal the complaint,
20 (including the affidavit in support of the complaint and accompanying documents), and this
21 motion in the above-referenced case, until the defendant's initial appearance or further order of
22 the Court, for the reasons set forth in the Affidavit.

23 DATED: June 28, 2005

24 Respectfully submitted,
25 KEVIN V. RYAN
26 
27 MARK L. KROTOSKI
Assistant U.S. Attorney