

SEALED

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
ABINGDON DIVISION

IN THE MATTER OF THE SEARCH OF :

RR 4 Box 531, Clintwood, VA 24228 :

Case No. 1:05mj00029

IN RE: ELITE TORRENTS ORGANIZATION :

USERNAME: "Duffman" :

FILED UNDER SEAL

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

I, Douglas W. Fender, being duly sworn, hereby depose and state as follows:

Introduction

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed for approximately fifteen years. I am assigned to the Richmond Division, Bristol Resident Agency. During my tenure as an FBI SA, I have had investigative assignments related to intellectual property rights, computer intrusions, and infrastructure protection. This affidavit is in support of an application for a search warrant in connection with an investigation into the activities of the Elite Torrents copyright piracy organization. As provided below, there is probable cause to believe that individuals associated with the Elite Torrents organization are operating throughout the United States and globally to reproduce and distribute copyrighted materials on a massive scale in violation of federal criminal conspiracy and copyright infringement statutes. Victims of this criminal organization include, but are not limited to, member companies of the following associations: the Motion Pictures Association of America

(MPAA); the Recording Industry of Association of America (RIAA); the Business Software Alliance (BSA); and, the Entertainment Software Alliance (ESA).

2. My experience as a FBI agent has included the investigation of cases involving the use of computers and the Internet to commit violations of fraud, intrusion and intellectual property laws. I hold a Master of Science degree in Criminal Justice. Prior to entering service with the FBI, I served as a Magistrate for the Commonwealth of Virginia for six years. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, intellectual property and other computer-based crimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures I have personally participated in the execution of search warrants involving the search and seizure of computer equipment.

3. I make this affidavit in support of an application by the United States of America for the issuance of a warrant to search RR 4 Box 531, Clintwood, VA 24228 ("the premises") for the items described in Attachment A, which constitute evidence, contraband, fruits, or instrumentalities of violations of the criminal conspiracy and copyright laws, namely Title 17, United States Code, Section 506(a), and Title 18, United States Code, Sections 371 and 2319. Title 17, United States Code, Section 506 provides, in pertinent part:

(a) **Criminal Infringement.** Any person who infringes a copyright willfully . . .
(2) 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 [shall be punished as provided under Section 2319 of Title 18, United States Code].

(b) **Forfeiture and Destruction.** When any person is convicted of any violation of subsection (a), the court, in its judgment of conviction shall, in addition to the penalty therein prescribed, order the forfeiture and destruction or other disposition of all infringing copies or phonorecords and all implements, devices, or equipment used in the manufacture of such infringing copies or phonorecords.

Title 18, United States Code, Section 2319(c) states, in pertinent part, that any person who violates 17 U.S.C. § 506(a)(2):

(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;

(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.

4. The facts set forth in this affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of a cooperating witness, as related to me by other law enforcement officers; my review of documents and computer records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

Summary of Relevant Computer and Internet Concepts

5. The Internet is a collection of computers and computer networks that are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information. Connections between Internet computers exist across state and international borders; therefore, information sent between two computers connected to the Internet frequently crosses state and international borders even where the two computers are located in the same state.

6. **Internet Service Providers (“ISPs”)**: Most individuals and businesses obtain access to the Internet through businesses known as Internet Service Providers (“ISPs”). AOL, Microsoft (“MSN”), and EarthLink are examples of some of the larger and better-known ISPs. Other Internet Service Providers include private entities such as corporations, universities and government agencies. Among other services, ISPs provide their customers with access to the Internet using telephone, cable, Digital Subscriber Line (“DSL”), or other types of telecommunications lines.

7. **Internet Protocol Address (“IP address”)**: An Internet Protocol (IP) Address is a unique numeric address used to identify computers on the Internet. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. Internet service providers (“ISPs”) assign IP addresses to their customers’ computers. An ISP might assign a different IP address to a customer each time the customer makes an internet connection (so-called “dynamic IP addressing”), or it might assign an IP address to a customer permanently or for a fixed period of time (so-called “static IP addressing”). Either way, the IP Address used by a computer attached to the Internet must be

unique for the duration of a particular session; that is, from connection to disconnection. ISPs typically log their customers' connection, which means the ISP can identify which of their customers was assigned a specific IP address during a particular session.

8. Domain Names: Numerical IP addresses generally have corresponding domain names. For instance, the IP address "149.101.10.40" resolves to the corresponding domain name "www.cybercrime.gov." The Domain Name System ("DNS") is an Internet service that associates each domain name with an IP address. This mapping function is performed by DNS servers located throughout the Internet. DNS allows a user knowing only a domain name to reach a computer without having to know its IP address. In general, a registered domain name should resolve to a numerical IP address.

9. Peer-to-Peer ("P2P") Networks: P2P file sharing networks allow a group of computer users with the same file sharing software program to connect with each other through the Internet and directly access files from one another's hard drives. Users of a P2P network are able to (1) find and download files located on another peer's hard drive, and (2) share with other peers files located on their own computers. Files are accessed by relaying a message throughout the members of the peer group until the object of the inquiry, e.g., a particular song or movie, is found or until it is determined that no member has that particular file. P2P file sharing networks are commonly used illegally to reproduce and distribute copyrighted material without authorization, the most common forms of which are sound recordings, motion pictures, software, and games. Additionally, in most instances download speed is significantly faster than upload speed for a given file transfer. As a result, downloading a file can take a long period of time.

Also, because files transferred through traditional P2P networks require a connection to a single peer, a break in that connection could require the user to start over.

BitTorrent Technology

10. BitTorrent is a newer generation of P2P file sharing technology. BitTorrent technology addresses the inefficiencies inherent in older P2P systems that require a one-to-one connection between peers to download a complete file. Files transferred using a BitTorrent-based P2P network are broken into smaller chunks of data that collectively comprise a complete file, copies of which may reside on numerous computers belonging to different network users. By breaking down files into smaller chunks of data, users can access and download files in pieces from multiple other users on the system instead of being dependent on a single peer. By default, BitTorrent file sharing software also requires that as soon as a user has downloaded a file chunk, that chunk be made available for uploading to others. The process of downloading pieces of a file from multiple users combined with immediately making those pieces available for others to download simultaneously, results in faster and more efficient downloads than competing peer-to-peer file transfer systems.

11. There are two types of programs that comprise the BitTorrent system: "clients" and "trackers." Clients are programs that users run to download and upload files. Trackers are programs that certain parties run to tell the clients where they can locate the files they want. This file-location service is critical to the functioning of the BitTorrent system. A tracker tracks clients and maintains a list, or index, of which clients are online sharing which files. Trackers do not store or relay the files themselves, but instead introduce clients to one another to make file sharing by individuals easier. A client communicates with a tracker to ask it for the Internet

Protocol (IP) addresses of clients sharing the file that the client wishes to download. The client then automatically communicates directly with those other clients to download the desired file from them.

12. The BitTorrent system enables users to download many types of files, including movies, music, television shows, and software, which are called "content" files. In order to download a content file with BitTorrent, a user must first find and download an associated "torrent" file. Torrent files contain the information BitTorrent clients need to download associated content files. A torrent file typically includes the address of a tracker, the name of a content file, the size of the content file, the size of the parts into which the file is divided, and unique file identifiers for each part. Torrent files are small files that essentially tell one computer where and how to get a content file directly from another computer.

13. The key philosophy of BitTorrent is that users should upload (transmit outbound) at the same time they are downloading (receiving inbound). In this manner, network bandwidth is utilized as efficiently as possible. BitTorrent is designed to work better as the number of people interested in a certain file increases, in contrast to other file transfer protocols. To date, it is the fastest way to download music and movies on the Internet.

Summary of Investigation

14. On March 1, 2005, the FBI received a complaint from the Motion Picture Association of America (MPAA) regarding the Elite Torrents ("ET") organization which maintains a website at <http://www.elitetorrents.org>. The MPAA informed the FBI that ET members have been reproducing and distributing copyrighted works without authorization. The MPAA provided to the FBI the log files of the ET website and server. These files were obtained

with the consent of the owners and system operators of the ET website and server who are cooperating in the MPAA and FBI investigations. Log files are computer-generated files containing information regarding the activities of computer users, processes running on a computer, and the activity of computer resources. The ET BitTorrent tracking server generated data transfer logs that captured information about each file transfer. These transfer logs include the date of transfer, name of the file transferred, direction of transfer (upload or download), the name or nickname of the individual accessing the computer, and the IP address of the computer sending or receiving the file.

15. Investigating the complaint, your affiant has confirmed that the P2P software program used on the ET network is based on BitTorrent technology. Members of ET have used ET's P2P software program to reproduce and distribute copyrighted works without authorization. For example, an ET member who wants to download the movie Spider-Man 2 will log onto the ET site and type the filename Spider-Man 2 into the search engine. The search engine will look for a "torrent file" associated with the specified content, in this example, Spiderman 2. The torrent file is a small "metadata" file received from the web server. "Metadata" means that the file contains information related to the data being transferred, but not the data itself. Assuming that the server locates a torrent file regarding Spider-Man 2, this torrent file will be transferred to the downloader's computer when s/he clicks on a link on the website to download Spider-Man 2. After the torrent file is downloaded, the member's BitTorrent client software communicates with the ET computer serving as a "tracker."

16. "Trackers" coordinate the actions of the BitTorrent clients. When the ET member clicks on the torrent file for Spider-Man 2, the member's BitTorrent software contacts the ET

tracker and accesses a list of the Internet Protocol addresses for members' computers that have the movie and have their connections open. The member will then begin to receive chunks of the Spider-Man 2 movie file from other members and also begin to share those chunks with other members also looking to download the file. Periodically, throughout the transfer, the user's machine will check with the tracker to obtain the upload and download status.

17. Membership in the ET network revolves around an upload/download ratio. If a member does not upload content to others on the network, the member is then restricted in the quantity of files s/he may download as well as the speed at which such files can be downloaded. Conversely, the more the member uploads onto the ET network, the more the member will be permitted to download and at faster rates. If a member's upload/download ratio falls too low, the member is eliminated from the site and his or her account is removed.

18. On March 17, 2005, the two original hard drives from the ET tracker were provided to the FBI. An analysis of the drives showed that the information provided to the MPAA and the FBI was consistent and accurate with the data located on the hard drive. Additionally, the owners allowed the tracker database to be downloaded directly several times from the web site, which in turn allowed investigators to obtain current database tracker information on the activity of ET's members. An analysis of the database showed that several individuals were using the same IP address on April 19, 2005 that they had been using on the original database tracker info obtained on February 12, 2005. Most of the remaining individuals were still accessing the ET website tracker from the same ISP, and their IP address was within their previous IP subnet range. This information was utilized for Federal Grand Jury Subpoenas to re-verify the identity of the members.

EliteTorrents Operational Structure And Its Member Classes

19. According to the most recent ET logs, there are 133,794 members of the ET organization. Each of these members has a unique Login ID and password. Each member is assigned to one of 12 different member classes identified on the ET site in increasing order of responsibility and privilege. These classes, from lowest to highest, include: (1) User, (2) Power User, (3) Extreme User, (4) Elite User, (5) VIP, (6) Support, (7) Uploader, (8) FMOD, (9) Moderator, (10) Administrator, (11) Sysop, and (12) Owner. There are two Sysops on the ET site who, as discussed in paragraph 14 above, are cooperating in this investigation. The next-highest class is Administrator. Administrators run the day-to-day operations of the ET site. There are six Administrators for the ET site all of whom have a high degree of control over the network. Three of these Administrators are located in the United States and are known by the following user names: (1) "sk0t;" (2) "prezto;" and, (3) "duffman."

20. Members who obtain original content for the ET organization are known as "Uploaders." Uploaders are responsible for supplying and uploading onto the network the first copy of a particular copyrighted movie or other content which is then made available to the entire network for downloading. Uploaders are an elite class on the site and are individually selected by the site administrators. In some cases, members have applied to one of the administrators to be an uploader, basing their application on their ability to obtain new releases and on having high bandwidth for uploading. Nine uploaders are believed to reside in the United States each of whom have originated ten or more copies of movies, television episodes and/or other copyrighted content without authorization to the ET network as of February 12, 2005.

21. The ET tracker keeps a log file or record of the uploader of each torrent file ("torrent") available on the ET site. On February 12, 2005, the tracker had tracked 1,830 torrents associated with content on the ET network. These 1,830 torrents had 376 different uploaders among them. The most active uploader was responsible for 208 torrents, the second most active was responsible for 84, and the third most active uploaded 83 torrents. The ten most active uploaders have IP addresses originating inside the United States. Two of these uploaders appear to be the same people as two of the three Administrators located in the United States. Specifically, Administrator "sk0t" appears to be the same individual as uploader "MindHunter," and Administrator "duffman" appears to be the same individual as uploader "McCalister." The other seven United States-based uploaders are known by the following user names: "r313007," "stonyvision," "cipher," "punker22," "neeksor," "G," and "bandwith."

22. In BitTorrent terminology, a "leech" is a member who is in the process of receiving and simultaneously sharing pieces of a movie or other type of content file, but does not yet have the complete file for that particular copyrighted work. A "seeder" is a member who shares a full copy of a content item. A "leech" becomes a seeder simply by downloading a full file and keeping his or her BitTorrent client open for some time afterwards to enable other ET members to obtain the file.

23. The ET server maintains a database, made available to the MPAA and the FBI, that makes it possible to determine which users are seeding the most files. That is, it is possible to determine which users are sharing the largest number of full files (as opposed to sharing only part of a file, which all users do while downloading files). Out of 133,794 users on record, 93,132 (70%) had uploaded content using the tracker's service as of February 12, 2005. Of that 70%,

the average amount of data uploaded was 22 gigabytes.¹ The largest uploader uploaded 28,000 gigabytes, or over 1,000 times the average. Out of the 133,794 members of the ET organization on February 12, 2005, 94,418 (71%) had downloaded content. Among that 71%, the average amount of data downloaded was 20 gigabytes.

Probable Cause To Believe That Administrator "duffman" Has Violated 18 U.S.C. 2319

24. A copy of the ET server database provided to the MPAA and to the FBI specifically identified an ET administrator with the username "duffman" and an IP address of 141.152.68.152. Using the publicly available search technologies on the Internet, a search for the IP address of 141.152.68.152 disclosed that it is owned by Verizon Internet Services, an Internet Service Provider located in San Angelo, Texas.

25. According to the ET data log files, "duffman" was added to the ET organization on August 30, 2004. He was promoted to Administrator status on September 12, 2004. He was promoted to Uploader status on two occasions: September 12, 2004 and November 4, 2004.

26. The ET data log files identified another user named "McCalister" as having the same IP address as "duffman." It is believed that "duffman" and "McCalister" are the same person. The ET server tracked "McCalister" as being a significant uploader within the ET organization.

27. A review of the ET data log files show that, using a computer assigned the IP address 141.152.68.152, a user with the screen name "McCalister" uploaded 1,105 gigabytes of content, and downloaded 182 gigabytes of content as of May 1, 2005.

¹Gigabyte is a term used to measure the amount of available computer storage space. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. 1,500 GB of data, if printed on 8.5" x 11" paper, would print out 750,000,000 pages of text. Infringing copies of movie found on the Internet are often about 1 gigabyte in size, and can be as large as 4.5 gigabytes.

28. "McCalister" also originated 31 movies and 5 television episodes for the ET organization each of which was downloaded hundreds or thousands of times by ET members. These movies include: *Collateral* (uploaded on November 27, 2004), subsequently downloaded 2,469 times; *Blade Trinity* (uploaded on December 9, 2004), subsequently downloaded 6,633 times; *The Incredibles* (uploaded on December 10, 2004), subsequently downloaded 3,418 times; *Garden State* (uploaded on December 14, 2004), subsequently downloaded 1,267 times; *Apollo 13* (uploaded on December 17, 2004), subsequently downloaded 1,388 times; *Team America* (uploaded on January 9, 2005), subsequently downloaded 4,573 times; *The Final Cut* (uploaded on January 17, 2005), subsequently downloaded 3,138 times. These movies are copyrighted and valued in excess of \$2,500.00.

29. In addition to uploading and downloading activity, an examination of comments posted by "McCalister" a/k/a "duffman" on the ET site, and reproduced below in part, demonstrates that "McCalister" was an active member of the ET network and was heavily involved in the operations of the group and its illegal activities:

- December 31, 2004
 "wow 201 snatches... 30 seeders....thanks guys. you know after this i feel less like upping anything again. there will be new rules implemented soon. people who are seen hitting and running torrents will be permanately(sic) banned."
- December 31, 2004
 "due to overwhelming number of hit and runners recently. i will be seeding excessively slow in order to force others to share. sorry for you people who share but im tired of spitting out 3mB/sec so some people can leech fast then leave. fuckin tired of it."
- January 5, 2005

“for those who want to know this is the explanation. NOX released this movie. CD2 audio was out of sync. it got nuked. so IATSE released their own. it was perfect. our first torrent up was missing many files. it was nuked and then "fixed". for some reason the fix still excluded 2 files from the torrent itself when created. still don't know why. but this is the 2 rars missing from the other one. NOW these two files were on the first IATSE upped by punker. so some of you who moved over from that torrent may not need these two files. however. if you started on the upload i did earlier then you will need these 2 files. hope this clears up the confusion.”

- January 27, 2005 (“McCalister” communicating with ET uploader “r313007” concerning recent account activity)

“don't take this as me coming down on u... you do a ton of damn tv shows.. it just looks more "scene" like.. when we leave the case the same as the scene released it; ;) thanks man.... great uploads btw.. you pretty much knock out the tv eps everynight. thanks again; well krylon set the minimum upload of 250kb/sec. its set that way so that when a torrent is upped your putting 250kb/sec into it. if your uploading 8 torrents at once and your max upload is 250kb/sec that doesnt work the speed is set that high because speed does matter. please don't think im like pinning you here. its just there is one set of rules. everyone follows the same rules. krylons rules are my rules and every uploader follows suit. conformity is a bitch but it helps keep the site from turning to supernova; honestly though your uploads are perfect. i don't grab much tv.. just so happened tonight 3 shows came up i wanted to grab. other then the lcase torrent names :) . i cant say enough how much your uploads are appreciated. don't let my bitching get to you i just have to say stuff. sorry i did realize also you might not know this is duffman. thanks for the american idol btw.. good stoner tv ;) the auditions anyways.”

- January 29, 2005

“if you drop off this torrent before your ratio for THIS torrent is 1:1.... be prepared for consequences... SEED.”

- January 29, 2005

“well im talking about when there is 3 seeders and 300 leechers.. someone finishes after downloading at their max connection.. then just drops off without uploading but maybe 10-20%.. thats a leech.. even if you're an extreme user. once you reach 1:1 you have given back what you took and are not taking download speed away from others...new torrents should remain seeded as long as possible.”

30. A review of ET data log files shows that an administrator with the screen name "duffman", using a computer assigned the IP address 141.152.68.152, accessed the ET network on February 11, 2005 at 05:01:12 GMT. A subpoena was served on Verizon Internet Services requesting subscriber and related account records for the subscriber assigned the IP address 141.152.68.152 that was used on February 11, 2005 at 05:01:12 GMT. Verizon Internet Services responded with records showing that this IP address was assigned to a subscriber named Brook Dove residing at RR 4 Box 531, Clintwood, VA 24228, telephone number (276) 926-5496. Verizon Internet Services further disclosed that this account provided DSL service to the same address at RR 4 Box 531, Clintwood, VA 24228.

31. A review of ET data log files shows that an administrator with the screen name "duffman", using a computer assigned the IP address 151.199.111.254, accessed the ET network on April 19, 2005 at 07:09:13 GMT. A subpoena was served on Verizon Internet Services requesting subscriber and related account records for the subscriber assigned the IP address 151.199.111.254 that was used on April 19, 2005 at 07:09:13 GMT. Verizon Internet Services responded with records showing that this IP address was assigned to a subscriber named Brook Dove residing at RR 4 Box 531, Clintwood, VA 24228, telephone number (276) 926-5496. Verizon Internet Services further disclosed that this account provided DSL service to the same address at RR 4 Box 531, Clintwood, VA 24228.

Other Information

32. I have personally viewed the premises to be searched, and confirm that the description set forth in the caption to this application is accurate. On May 18, 2005 I had the occasion to conduct a surveillance of the premises described as RR 4, Box 531, Clintwood,

Virginia, 24228. The residence is described as a two story red brick house located in the Town of Clintwood. (See Exhibit 1). A rural mail box is located on the street identified as Market Street in front of the premises. Displayed on the outside of the rural mailbox is "RR4, Box 531". On 05-19-2005, J.A. Green, who is a Captain with the Dickenson County Sheriff's Office advised me he made contact with the Water Department for Clintwood, VA.. Green advised me the Water Department stated to him the individual listed as the resident of RR4, Box 531, Clintwood, Virginia is identified as Daniel Dove. In addition, Green advised me a motor vehicle was parked in the driveway of RR4, Box 531, Clintwood, Virginia on May 19, 2005. (See Exhibit 1). Green advised the Virginia license tag on the vehicle is "JSG 9137". A query of the Virginia Department of Motor Vehicles records by Green revealed the license tag JSG9137 is registered to Daniel James Dove, RR 4, Box 531, Clintwood, Virginia 24228.

Evidence, Contraband, Fruits, and Instrumentalities of the Crime

33. Based on my experience and information that I have obtained from others experienced in such investigations, I have learned that members of copyright piracy organizations typically maintain at their residence, place of business, or other location at which they maintain their computer server, various pieces of computer hardware; computer software; computer storage media; computer records; paper and electronic notes regarding software piracy; and paper and electronic correspondence with others who engage in software piracy, within the meaning of Title 17, United States Code, Section 506(a), and Title 18, United States Code, Section 2319. All of these items constitute evidence, contraband, fruits, or instrumentalities of violations of Title 17, United States Code, Section 506(a), and Title 18, United States Code, Sections 371 and 2319.

34. I have also learned that individuals who participate in copyright infringement through the Internet often transfer or copy their illegally obtained computer software, games, and movies to computer storage media and other electronic systems that are not connected to the Internet. This is usually done to facilitate ease of use. Whether stored on a computer system connected to the Internet or on any other type of computer storage media, such illegally obtained movies, computer software, games and music are routinely kept and collected by the participants for many months or even years. This is often done because the participant wants to be able to reinstall the software or media whenever convenient, or because he or she wants to use those titles for his own use and benefit and to trade for other software and media. In addition, I have learned that, even if illegally obtained software is later deleted by a participant, the computer system that was previously used to store that software often retains evidence of the offense. This is because files deleted by the user may still remain (in whole or in part) on the storage media, as deletion of a file may not remove that data completely from the media.

35. Additionally, the aforementioned facts provide evidence of probable cause to believe that Brook Dove a/k/a "duffman" maintains and operates computer(s) and related equipment and media at RR 4 Box 531, Clintwood, VA 24228, which has/have been used to commit the offense of criminal copyright infringement; that is, to cause the unauthorized reproduction and distribution by electronic means during a 180-day period of one or more copies of copyrighted works having a total retail value exceeding \$2500. Therefore, the computer hardware, software, passwords, data security devices, digital storage media and computer data described in Attachment A constitute not only evidence, contraband, fruits, and instrumentalities of these offenses, but also constitute "implements, devices, or equipment used in the manufacture of"

infringing copies of copyrighted works, and are thereby subject to criminal forfeiture and destruction or other disposition pursuant to 17 U.S.C. § 506(b).

36. Based upon my knowledge, training, and experience, as well as 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 systems and storage devices. I also know that during the search of the premises it is rarely possible to complete on-site examination of computer equipment and storage devices 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 rarely possible 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. The analysis of computer systems and storage media often relies on rigorous procedures designed to maintain the integrity of the evidence and to recover "hidden," mislabeled, deceptively-named, erased, compressed, encrypted, or password-protected data while reducing the likelihood of inadvertent or intentional loss or modification of data. A controlled environment, such as a law enforcement laboratory, is typically required to conduct such an analysis properly.

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 physical search of the premises. The hard drives commonly included in mere desktop computers are capable of storing millions of pages of text.

37. Due to the volume of data at issue and the technical requirements set forth above, it may be necessary that the above-referenced equipment, software, data, and related instructions be seized and subsequently processed by a qualified computer specialist in a laboratory setting. Under the appropriate circumstances, some types of computer equipment can be more readily analyzed and pertinent data seized on-site, thus eliminating the need for its removal from the premises. One factor used in determining whether to analyze a computer on-site or to remove it from the premises is whether the computer constitutes an instrumentality of an offense and is thus subject to immediate seizure as such. Another determining factor is whether a particular device can be more readily, quickly, and thus less intrusively, analyzed off-site, with due considerations given to preserving the integrity of the evidence. This, in turn, is often dependent upon the amount of data and number of discrete files or file areas that must be analyzed, and this is frequently dependent upon the particular type of computer hardware involved. As a result, it is ordinarily impossible to appropriately analyze such material without removing it from the location where it is seized.

38. Based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in forensic examination of computers, I am aware that searches and seizures of evidence from computers taken from the premises commonly require agents to seize most or all of a computer system's input/output and peripheral devices, in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. Therefore, in those instances where computers are removed from the

premises, in order to fully retrieve data from a computer system, investigators must seize all the storage devices, as well as the central processing units (CPUs), and applicable keyboards and monitors which are an integral part of the processing unit. If, after inspecting the input/output devices, system software, and pertinent computer-related documentation, it becomes apparent that these items are no longer necessary to retrieve and preserve the data evidence, and are not otherwise seizable, such materials and/or equipment will be returned within a reasonable time.

Analysis of Electronic Data

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


Conclusion

40. Based on the information outlined above, the undersigned submits that there is probable cause to believe that the items identified in Attachment A have been used in the

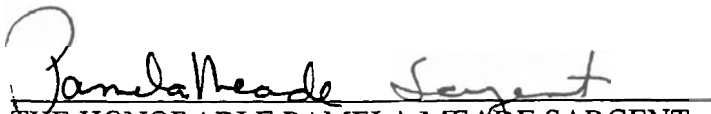
commission of a crime and constitute evidence, contraband, fruits, or instrumentalities of violations of Title 17, United States Code, Section 506(a), and Title 18, United States Code, Sections 371 and 2319, and will be found at the premises to be searched.

Request for Sealing

41. Because this is part of an ongoing investigation and based on the information set forth in this application, your affiant respectfully requests that the court seal the search warrant, application for search warrant and this affidavit.


Special Agent Douglas W. Fender
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence this 24th day of May, 2005.


THE HONORABLE PAMELA MEADE SARGENT
UNITED STATES MAGISTRATE JUDGE
WESTERN DISTRICT OF VIRGINIA