

**MOTION PICTURE ASSOCIATION OF AMERICA, INC.**

15503 VENTURA BOULEVARD  
ENCINO, CALIFORNIA 91436



JAMES W. SPERTUS  
Vice President and Director  
United States Anti-Piracy Operations

PHONE: (818) 995-6600  
FAX: (818) 382-1797  
E-MAIL: jim.spertus@mpaa.org

DATE PRINTED

December 20, 2007

Special Agent Kiffa Shirley  
Special Agent Lori Jensen  
Federal Bureau of Investigation  
9797 Aero Drive  
Sand Diego, CA 92123

Re: EliteTorrents BitTorrent Tracker

Dear Agents Shirley and Jensen,

I am the Director of United States Anti-Piracy Operations for the Motion Picture Association of America (MPAA)<sup>1</sup> and I write to refer for investigation and possible prosecution members of a massive piracy ring operating in the Southern District of California and elsewhere in the United States. The members of this piracy ring are stealing copyrighted materials on a massive scale in violation of the criminal copyright statutes: Title 17, United States Code, Section 506, and Title 18, United States Code, Section 2319. In addition, the agreement between these subjects to help each other steal copyrighted works is itself a violation of Title 18, United States Code, Section 371 (conspiracy). We hope that you will investigate this piracy ring and bring the most culpable members of the organization to justice.

The piracy ring that is the subject of this referral is a criminal organization called "EliteTorrents." EliteTorrents is an organization dedicated to helping its members steal copyrighted works, and the members are, in fact, rewarded for being the first to make copyrighted works available to the other members of the organization. As of February 12, 2005, there were 133,794 members of the EliteTorrents organization, a wide majority of which had a record of exchanging copyrighted material over the Internet. There are many members of the EliteTorrents organization residing within the Southern District of California, and other members, including some of the most culpable, are scattered throughout the United States. EliteTorrents maintains a web site at <http://www.elitetorrents.org>.

As a preliminary matter, you should know that the MPAA has never before made a criminal referral of this type. Although we actively investigate many cases of online piracy, we routinely pursue our own civil remedies in these matters rather than burden

<sup>1</sup> The Motion Picture Association of America is a trade association representing the interests of Columbia Pictures Industries, Inc., Disney Enterprises, Inc., Metro-Goldwyn-Mayer Studios Inc., Paramount Pictures Corporation, TriStar Pictures, Inc., Twentieth Century Fox Film Corporation, United Artists Pictures, Inc., United Artists Corporation, Universal City Studios LLLP, Universal City Studios Productions LLLP, and Warner Bros Entertainment Inc.

criminal investigators with our complaints. However, the Administrators and Originators for the EliteTorrents organization are some of the most significant and egregious online pirates in the world, and there simply is no adequate civil remedy that would adequately punish these offenders and deter them and others from engaging in piracy on a massive scale. EliteTorrents is world renowned among online pirate communities, and an investigation and prosecution of these criminals by the United States Government would deter millions of similarly situated individuals who engage in large-scale piracy everyday.

The MPAA has been investigating the EliteTorrents organization since August 2004. In late 2004 and early 2005, individuals claiming to run the EliteTorrents site contacted the MPAA to offer a rare opportunity to investigate the EliteTorrents organization from the inside. The two individuals offering this opportunity run the EliteTorrents system by directing two EliteTorrents "System Operators," the individuals with the highest level of technical privileges and access on the system. They directed the System Operators to configure the EliteTorrents servers to log everything occurring on the servers. This wealth of information provided an extremely rare opportunity for the MPAA to investigate the site from the inside, and the scale of piracy we've observed on the site is staggering. The piracy covers not only movies but also television content, software, and music.

In order to evaluate the offer of cooperation from the EliteTorrents directors, the MPAA requested a complete copy of all data contained on the EliteTorrents servers so that the MPAA could evaluate the data. The directors provided the MPAA with a complete copy of all data from the EliteTorrents server as of February 12, 2005, and the MPAA has had that data analyzed and it was genuine. With this data, we have been able to identify and investigate some of the largest scale pirates in the world. This referral focuses on the most culpable leaders and contributors of the EliteTorrents organization.

#### **APPLICABLE STATUTES**

The members of the EliteTorrents organization are stealing copyrighted materials in violation of 18 USC 2319 and 17 U.S.C. 506. These criminal statutes provide as follows:

1. **Title 18, United States Code, Section 2319: Criminal Copyright Infringement.**

(a) Whoever violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsections (b) and (c) of this section and such penalties shall be in addition to any other provisions of title 17 or any other law.

(b) Any person who commits an offense under section 506 (a)(1) 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. . . .

2. Title 17, United States Code, Section 506:

(a) Criminal Infringement— Any person who infringes a copyright willfully either—

(1) for purposes of commercial advantage or private financial gain, . . .

shall be punished as provided under section 2319 of title 18, United States Code.

**OVERVIEW OF THE ELITETORRENTS FILE SHARING NETWORK**

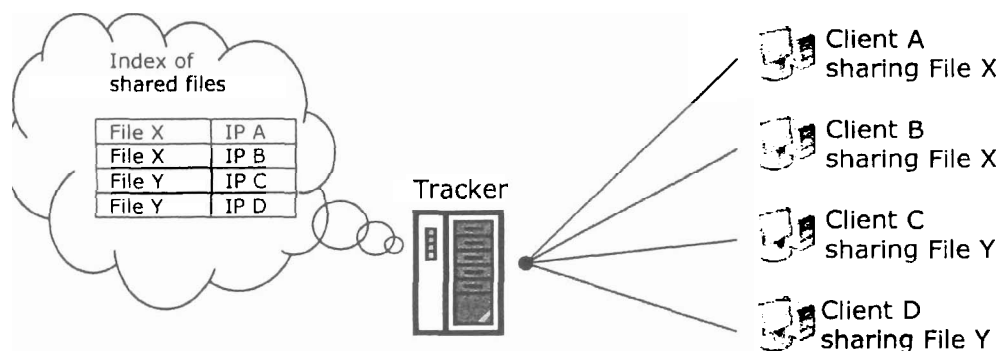
The MPAA has a close working relationship with Dr. Kelly Truelove, PhD, a computer scientist who frequently consults with the MPAA on the MPAA's most important peer-to-peer investigations. Dr. Truelove earned his Ph.D. in physics in 1997 from the University of California, Berkeley, where his research focused on complex computer simulations. He started working on Internet end-user applications immediately thereafter, first as a consultant and then as a venture-capital-backed entrepreneur. Dr. Truelove began technical studies of peer-to-peer systems on behalf of his investors in early 2000, and he wrote and spoke publicly about the technology during that work. Since late 2001, Dr. Truelove has served as an independent consultant to the MPAA, the Recording Industry Association of America, and the National Music Publishers' Association in support of their most important peer-to-peer litigation and related investigations. In this role, Dr. Truelove maintains a detailed familiarity with peer-to-peer technology and piracy, including the BitTorrent system and sites that put that system to an infringing use.

I and other employees at the MPAA directed Dr. Truelove to examine the data from EliteTorrents that had been provided to the MPAA as described above, and to opine on the authenticity of that data. Dr. Truelove found that the data correspond both broadly and specifically with data publicly accessible on the EliteTorrents site, and that the data appear to be the authentic data of a functioning BitTorrent system. Dr. Truelove noted that, although it is technically possible the directors or operators removed some data from the copy produced to the MPAA, it does not seem likely that the data produced was fabricated. I have had many discussions with Dr. Truelove about the EliteTorrents data and during those discussions I learned the following:

1. The technology used by EliteTorrents is called BitTorrent. BitTorrent is a system for locating and transferring files between computers on the Internet. Mechanically, files shared over a BitTorrent system are broken down into separate parts that are separately shared. A user downloading over a BitTorrent network will begin sharing the parts of a file as he acquires them, which is even before he or she has

acquired all of the parts of the larger file. The BitTorrent system is designed so that users will obtain the missing parts of the files they are acquiring faster if they upload the parts they acquire as they acquire them. This combination of partial-sharing and tit-for-tat techniques generally results, especially for larger files such as movies, in BitTorrent providing faster downloads than competing peer-to-peer file transfer systems.

2. There are two sorts 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 motivated 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. The figure below shows the architecture of a BitTorrent system.

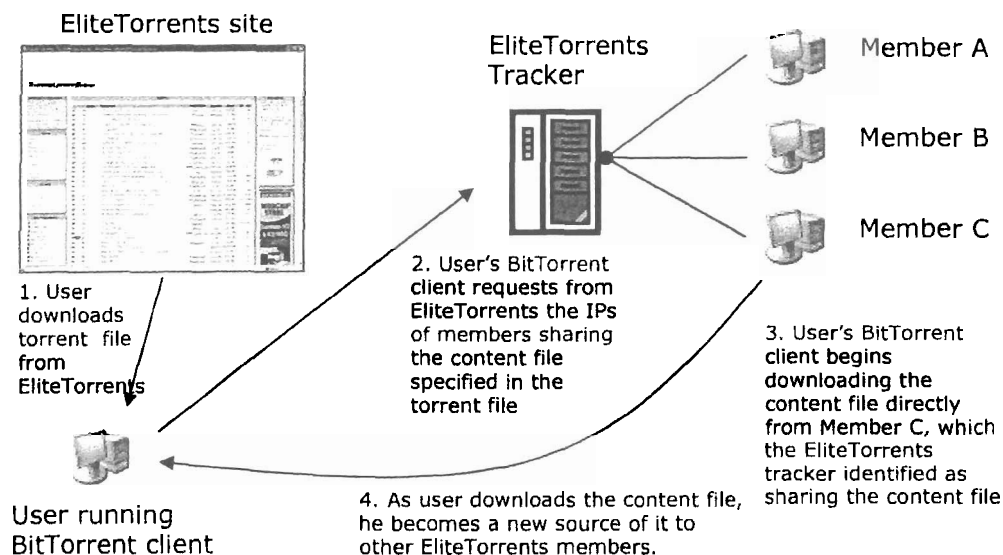


3. The BitTorrent system enables users to download many types of files, including movies, music, and software files, which are called "content" files. In order to download a content file with BitTorrent, a user must first find and download an associated "torrent" file. The EliteTorrents organization operates its own torrent site and its own tracker. Torrent files contain the information BitTorrent clients need to download associated content files. Namely, a torrent file 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.

4. Applying this technology to the case at hand, members of EliteTorrents use this technology to trade copyrighted works. For example, an EliteTorrents member who wants to download the movie Spider-Man 2 will log onto the EliteTorrents torrent site and type the filename Spider-Man 2 into the search engine. The appropriate torrent file will be located and the member clicks on the name to download the file. After the

torrent file is downloaded, the member's BitTorrent software communicates with the tracker, learns the Internet Protocol (IP) addresses of other EliteTorrents members who have the movie file, and the member will begin to receive the movie file from the other EliteTorrents members.<sup>2</sup>

5. The details of this process are largely invisible to the user. From an EliteTorrents member's perspective, he or she merely clicked on a Spider-Man 2 link on a website and, with no further action, found a copy of the movie on his computer some time later. From the user's perspective, it is as though the EliteTorrents site itself supplied the movie. The figure below illustrates the process of downloading a file using BitTorrent and the EliteTorrents site.



### **ELITETORRENTS OPERATIONAL STRUCTURE AND ITS MEMBER CLASSES**

6. There are 133,794 members of the EliteTorrents organization, and each of these members has a unique Login ID and password. Every username is unique and

<sup>2</sup> An IP Address is a unique numeric address used by computers to communicate on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned a unique IP Address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP Address acts much like a home or business street address for Internet communications, and enables Internet routers to properly route traffic to each other so that communications reach the intended destination computers. There are two types of IP Addresses, dynamic and static. To assign dynamic IP Addresses, the ISP randomly assigns one of the available IP Addresses in the range of IP Addresses controlled by the provider each time a customer dials in or connects to the provider in order to connect to the Internet. The customer's computer retains that IP Address for the duration of that session (i.e., until the user disconnects), and the IP Address cannot be assigned to another user during that period. Once the user disconnects, however, that IP Address becomes available to other customers who dial in at a later time. Thus, an individual customer's dynamic IP Address may, and almost always will, differ each time he dials into or connects to the ISP. To designate static IP Addresses, the ISP assigns the customer a permanent IP Address. The customer's computer would then be configured with this IP Address every time he or she dials in or connects to the Internet.



constant, and only an individual with the password associated with a particular username can log onto the site as that user. Each user is assigned to a class, and there are 12 different user classes on the EliteTorrents site: (1) Leech, (2) User, (3) Power User, (4) Extreme User, (5) Elite User, (6) VIP, (7) Support, (8) Uploader, (9) FMOD, (10) Moderator, (11) Administrator, and (12) Sysop. The lowest class with the least amount of privilege is the "Leech" class, and the highest class with the most amount of privilege is the "Sysop" class. There are two Sysops on the EliteTorrents site, and these were the two individuals working under the direction of the two individuals who provided the data from the EliteTorrents servers as described above. The highest class other than the Sysops is Administrator, and the Administrators run the day-to-day operations of the EliteTorrents site. There are six Administrators for the site, and all of them have a high degree of control over the site. Three of these Administrators are located in the United States, and these three administrators use the following three usernames: (1) sk0t, (2) prezto, and (3) duffman. All three of the U.S.-based Administrators are being referred to you, each under separate cover. These three Administrators are the most culpable leaders of the EliteTorrents organization that we could identify and refer.

7. The individuals who obtain original content for the EliteTorrents organization are members that we term the "Originators." Originators are an elite class (class "Uploader" from the paragraph above) on the site which are individually selected by the site administrators. In some cases, members had to apply to one of the administrators to be an originator, advising of their capability of getting new releases and having high bandwidth for uploading. Twelve Originators believed to reside in the United States originated 10 or more movies and television episodes to the EliteTorrents organization, which means they were the very first individuals to supply a particular title to the EliteTorrents organization. In our opinion, these Originators are the second most culpable class of individuals in the EliteTorrents organization who have most damaged the movie industry. The EliteTorrents tracker keeps a record of the Originator of each torrent file available on the EliteTorrents site. On February 12, 2005, there were 1,830 torrent files associated with content tracked by the EliteTorrents site. In BitTorrent lingo, the tracker was tracking 1,830 torrents. These 1,830 torrents had 376 different originators between them. The biggest originator was responsible for 208 torrents, the second-biggest was responsible for 84, and the third-biggest, 83. The twelve Originators whose IPs indicate US locations, and who have originated the most movies and television episodes are being referred to you as appendices attached to this document. Interestingly, two of these Originators appear to be the same people as two of the four U.S. Administrators. Specifically, Administrator "sk0t" appears to be the same individual as Originator "MindHunter," and Administrator "duffman" appears to be the same individual as Originator "McCalister." The other 11 U.S.-based Originators that are being referred are usernames "r313007," "stonyvision," "mattb," "cipher," "punker22," "neeksor," "Nick4753," "G," "StanTek," and "bandwidth."

8. Dr. Truelove also explained to me the role of seeders on the EliteTorrents site. A "seeder" is a user who shares a full copy of a content item (the item may consist of many different files). A user can become a seeder simply by downloading a full file and keeping his BitTorrent client open for some time afterwards to enable other EliteTorrents member to obtain the file from him or her. EliteTorrents maintains a

database 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 services as of February 12, 2005. Among that 70%, the average amount of data uploaded was 22 gigabytes.<sup>3</sup> The largest Uploader uploaded 28,000 gigabytes, or over 1,000 times the average. Out of the 133,794 members of the EliteTorrents organization on February 12, 2005, 94,418 (71%) had downloaded content. Among that 71%, the average amount of data downloaded was 20 gigabytes.

9. The appendices that follow were written using data extracted from the EliteTorrents database. Appendix 1 is a full template for the administrator registered as Sk0t. Appendices 2-11 cover the probable cause sections for ten additional originators. Full templates for each individual were omitted to prevent redundancy. We will provide additional appendices as they become available or necessary.

Sincerely,

James W. Spertus  
Vice President and Director  
United States Anti-Piracy Operations  
Motion Picture Association of America

---

<sup>3</sup> 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 in 750,000,000 pages of text. Infringing copies of movies found on the Internet are often about 1 gigabyte in size.

g. Scott McCausland,  
4134 Hoyt St.  
Erie, PA 16510  
US  
Phone: (814) 824-6521  
Email: webmaster@sk0t.com

h. I believe this is sk0t's real name and address. The domain registration company Register.com that is the registrar for this name likely has customer data for the registrant of the sk0t.com domain.

i. According to the Google PhoneBook service on February 21, 2005, this phone number belongs to "Russell Mccausland" at the above address.

j. According to Erie County Tax & Assessment records (<http://www.eriepa.us>) as of February 21, 2005, this address corresponds to a residence.

k. On the site <http://forums.elitetorrents.com>, which is a message board for EliteTorrents members, the user profile for sk0t, as reviewed on February 21, 2005, stated his "AOL Messenger Screen Name" was "PleesDontCutMe," the same as in the EliteTorrents database user record for MindHunter, further evidencing they are one individual.

l. The message board user profile also states sk0t is a male with a birthdate of August 17, 1982.

13. If you were to serve a grand jury subpoena on Road Runner Communications for the subscriber information pertaining IP address 24.160.220.217 on February 11, 2005, at 04:41 server time, when Sk0t accessed EliteTorrents, the subscriber for the IP address at that date and time would likely be the true name for sk0t, and the subscriber address sk0t's address.

14. If you were to serve a grand jury subpoena on Road Runner Communications for the subscriber information pertaining IP address 24.160.220.217 on February 10, 2005, at 16:18 server time, when MindHunter accessed EliteTorrents, the subscriber for the IP address at that date and time would likely be the true name for MindHunter, and the subscriber address MindHunter's address.

15. You will likely learn that sk0t and MindHunter are the same people, both located in Erie, Pennsylvania.

16. If you were to review Pennsylvania Department of Motor Vehicle records, you may determine that the true name for sk0t and MindHunter is registered with the Department of Motor vehicles at the same address as the subscriber to IP address 24.160.220.217 both on February 11, 2005, at 04:41 server time, and on February 10, 2005, at 16:18 server time.

17. If you were to check with the Postmaster at the Post Office responsible for the residence address for the Road Runner IP Address subscriber associated with sk0t and MindHunter, you may find that the individual has not changed his or her address.

**AN ONSITE REVIEW OF COMPUTER EVIDENCE WILL LIKELY NOT BE POSSIBLE**



18. Based upon my training and experience, I know that individuals involved in the operation of BitTorrent servers such as EliteTorrents invest a great deal of time and effort in developing these networks and administering them. These individuals are likely to keep evidence of their activities in their homes and on their computers for an extended period of time.

19. Based upon my training, experience I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that computer evidence must typically be analyzed in a laboratory 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 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 substantial 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:**

20. Based on the foregoing, I respectfully submit that there is probable cause to believe that the following items, which constitute evidence of violations of 18 U.S.C. 2319 and 17 U.S.C. 506, will be found at the Subject Premises:

- a. A large number of computers and computer storage devices containing copyrighted content such as movies and television content.
- b. Videotaped, recorded, or digitized movies and television programming, or any other form of motion picture on tape, compact disc, hard disk, DVD, diskette, or any other media.
- c. Records, documents, programs, applications and materials relating to the recording, distributing or selling of unauthorized copyrighted motion pictures or television content;
- d. Records, documents, programs, applications and materials relating to the online piracy organization named EliteTorrents;
- e. Accounting and financial records, sales and shipping records, copies of tax returns both personal, business and corporate, federal and state (including schedules, Forms 1099, correspondence, memoranda and another records used in the preparation of the tax returns), general ledgers, cash disbursement and receipt journals, check registers, bank statements, money market funds, investment accounts, cashier's checks (including purchaser copies), cancelled checks, deposited items, deposit tickets, telephone records, rental agreements for self storage units, opened and unopened e-mails, correspondence;
- f. Indicia of occupancy, including: invoices, letters, bills, personal effects, and mortgage and loan agreements tending to show ownership, occupancy, or control of the premises or the above described items;
- g. Diaries, appointment books, calendars, day planners, address and telephone books that reflect scheduled meetings and dates;
- h. Videotapes, DVDs, VCD, materials or copyrighted works belonging to any motion picture studio or authorized distributor;
- i. Video editing and transferring equipment, Digital Video editing kits, FireWire devices, and video/graphics cards;
- j. Machines capable of reproducing copyrighted items, such as DVD's and CD's, as well as materials used in the packaging, reproduction, or distribution of motion pictures in any format, including labels, videotape boxes, CD-ROM/DVD boxes, covers, or shipping materials.

k. 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.

21. In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing a search warrant may wish to employ the following procedures:

a. 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.

b. 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.

c. 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.

d. If the computer personnel determine that the data does not fall within any of the items to be seized pursuant to this warrant, that the seized computer equipment was not used as an instrumentality of a crime or is not otherwise legally seized, the government will return these items.

22. 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:

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

b. 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;

c. 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;

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

e. 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;

f. 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

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

23. Based upon the facts as set forth above, and upon my training and experience, I believe there is probable cause to believe that sk0t's residence will contain fruits, evidence and instrumentalities of violations of Title 17, United States Code Section 506, Title 18, United States Code Section 2319 and Title 18, United States Code Section 371.

Sincerely,

James W. Spertus  
Vice President and Director  
United States Anti-Piracy Operations  
Motion Picture Association of America