UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

MALIBU MEDIA, LLC, Plaintiff, vs. JOHN DOES 1-9, Defendants.	Civil Action No. 5:12-cv-04818

MOTION FOR LEAVE TO SERVE THIRD PARTY SUBPOENAS PRIOR TO A RULE 26(f) CONFERENCE

Pursuant to Fed. R. Civ. P. 26(d)(1), and upon the attached: (1) Memorandum of Law in support of this motion; and (2) Declaration of Tobias Fieser in support of this motion, Malibu Media, LLC. ("Plaintiff"), respectfully moves for entry of an order granting it leave to serve third party subpoenas prior to a Rule 26(f) conference (the "Motion"). A proposed order is attached for the Court's convenience.

Dated: August 22, 2012

Respectfully submitted,

FIORE & BARBER, LLC

By: _____

Christopher P. Fiore, Esquire
Aman M. Barber, III, Esquire
Attorneys for Plaintiff
425 Main Street, Suite 200
Harleysville, PA 19438
Tel: (215) 256-0205
Fax: (215) 256-9205
Email: cfiore@fiorebarber.com
ATTORNEYS FOR PLAINTIFF

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

MALIBU MEDIA, LLC, Plaintiff, vs. JOHN DOES 1-9, Defendants.	Civil Action No. 5:12-cv-04818

ORDER ON MOTION FOR LEAVE TO SERVE THIRD PARTY SUBPOENAS PRIOR TO A RULE 26(f) CONFERENCE

THIS CAUSE came before the Court upon Plaintiff's Motion for Leave to Serve Third Party Subpoenas Prior to a Rule 26(f) Conference (the "Motion"), and the Court being duly advised in the premises does hereby:

FIND, ORDER AND ADJUDGE:

1. Plaintiff established that "good cause" exists for it to serve third party subpoenas on the Internet Service Providers listed on Exhibit A to the Motion (the "ISPs"). See UMG Recording, Inc. v. Doe, 2008 WL 4104214, *4 (N.D. Cal. 2008); and Arista Records LLC v. Does 1-19, 551 F. Supp. 2d 1, 6-7 (D.D.C. 2008).

2. Plaintiff may serve each of the ISPs with a Rule 45 subpoena commanding each ISP to provide Plaintiff with the true name, address, telephone number, e-mail address and Media Access Control ("MAC") address of the Defendant to whom the ISP assigned an IP address as set forth on Exhibit A to the Motion. Plaintiff shall attach to any such subpoena a copy of this Order.

3. Plaintiff may also serve a Rule 45 subpoena in the same manner as above on any service provider that is identified in response to a subpoena as a provider of internet services to one of the Defendants.

4. Each of the ISPs that qualify as a "cable operator," as defined by 47 U.S.C. § 522(5), which states:

> the term "cable operator" means any person or group of persons
>
> (A) who provides cable service over a cable system and directly or through one or more affiliates owns a significant interest in such cable system, or
>
> (B) who otherwise controls or is responsible for, through any arrangement, the management and operation of such a cable system.

shall comply with 47 U.S.C. § 551(c)(2)(B), which states:

> A cable operator may disclose such [personal identifying] information if the disclosure is . . . made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed.

by sending a copy of this Order to the Defendant.

5. The subpoenaed ISPs shall not require Plaintiff to pay a fee in advance of providing the subpoenaed information; nor shall the subpoenaed ISPs require Plaintiff to pay a fee for an IP address that is not controlled by such ISP, or for duplicate IP addresses that resolve to the same individual, or for an IP address that does not provide the name of a unique individual, or for the ISP's internal costs to notify its customers. If necessary, the Court shall resolve any disputes between the ISPs and Plaintiff regarding the reasonableness of the amount proposed to be charged by the ISP after the subpoenaed information is provided to Plaintiff.

6. If any particular Doe Defendant has been voluntarily dismissed then any motion filed by said Defendant objecting to the disclosure of his or her identifying information is hereby denied as moot. Notwithstanding the foregoing, the applicable ISP shall withhold the moving

Defendant's identifying information from Plaintiff unless and until Plaintiff obtains a subsequent court order authorizing the disclosure.

7. Plaintiff may only use the information disclosed in response to a Rule 45 subpoena served on an ISP for the purpose of protecting and enforcing Plaintiff's rights as set forth in its Complaint.

DONE AND ORDERED this ___ day of _____, 2012.

By _____
UNITED STATES DISTRICT JUDGE

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

MALIBU MEDIA, LLC, Plaintiff, vs. JOHN DOES 1-9, Defendants.	Civil Action No. 5:12-cv-04818

MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO SERVE THIRD PARTY SUBPOENAS PRIOR TO A RULE 26(F) CONFERENCE

TABLE OF AUTHORITIES

MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO SERVE THIRD PARTY SUBPOENAS PRIOR TO A RULE 26(f) CONFERENCE

Pursuant to Fed. R. Civ. P. 26(d)(1), Plaintiff hereby respectfully submits this Memorandum in support of its Motion for Leave to serve third party subpoenas prior to a rule 26(f) conference.

I. INTRODUCTION

Plaintiff seeks leave to serve limited, immediate discovery on the Doe Defendants' Internet Service Providers ("ISPs") so that Plaintiff may learn Defendants' true identities. Plaintiff is suing each of the Defendants for using the Internet and the BitTorrent protocol to commit direct and contributory copyright infringement.

Since Defendants used the Internet to commit their infringement, Plaintiff only knows Defendants by their Internet Protocol ("IP") addresses. Defendants' IP addresses were assigned to the Defendants by their respective ISPs. Accordingly, the ISPs can use the IP addresses to identify the Defendants. Indeed, ISPs maintain internal logs, which record the date, time and customer identity for each IP address assignment made by that ISP. Significantly, the ISPs may maintain these logs for only a short period of time.

Plaintiff seeks leave of Court to serve a Rule 45 subpoena on the ISPs and any related intermediary ISPs. Any such subpoena will demand the true name, address, telephone number, e-mail address and Media Access Control ("MAC") address of the Defendant to whom the ISP issued an IP address.[1] Plaintiff will only use this information to prosecute the claims made in its Complaint. Without this information, Plaintiff cannot serve the Defendants nor pursue this lawsuit to protect its valuable copyrights.

[1] A MAC address is a number that identifies the specific computer used for the infringing activity.

II. ARGUMENT

Pursuant to Rule 26(d)(1), except for circumstances not applicable here, absent a court order, a party may not propound discovery in advance of a Rule 26(f) conference. Rule 26(b) provides courts with the authority to issue such an order: "[f]or good cause, the court may order discovery of any matter relevant to the subject matter involved in the action." In Internet infringement cases, courts routinely find good cause exists to issue a Rule 45 subpoena to discover a Doe defendant's identity, prior to a Rule 26(f) conference, where: (1) plaintiff makes a prima facie showing of a claim of copyright infringement, (2) plaintiff submits a specific discovery request, (3) there is an absence of alternative means to obtain the subpoenaed information, (4) there is a central need for the subpoenaed information, and (5) defendants have a minimal expectation of privacy. See Arista Records, LLC v. Doe 3, 604 F.3d 110 (2d Cir. 2010) (citing Sony Music Entm't v. Does 1-40, 326 F.Supp.2d 556, 564-65 (S.D.N.Y. 2004) (numbers added)); Elektra Entm't Group, Inc. v. Doe, No. 5:08-CV-115-FL, 2008 WL 5111886, at *4 (E.D.N.C. Dec. 4, 2008) (same); Warner Bros. Records, Inc. v. Doe, No. 5:08-CV-116-FL, 2008 WL 5111883, at *4 (E.D.N.C. Dec 4, 2008) (same); BMG Music v. Doe # 4, No. 1:08-CV-135, 2009 WL 2244108, at *3 (M.D.N.C. July 24, 2009) (same). See also, Arista Records LLC v. Does 1-19, 551 F. Supp. 2d 1, 6-7 (D.D.C. 2008), and the cases cited therein, noting the "overwhelming" number of cases where copyright infringement plaintiffs sought to identify "Doe" defendants and courts "routinely applied" the good cause standard to permit discovery. Here, Plaintiff easily satisfies all of these requirements. Accordingly, this Court should grant the Motion.

A. Circuit Courts Unanimously Permit Discovery to Identify John Doe Defendants

Federal Circuit Courts have unanimously approved the procedure of suing John Doe defendants and then using discovery to identify such defendants.

For example, the Second Circuit stated in Davis v. Kelly, 160 F.3d 917, 921 (2d Cir. 1998) that "courts have rejected the dismissal of suits against unnamed defendants . . . identified only as 'John Doe's . . . until the plaintiff has had some opportunity for discovery to learn the identities." See also, Penalbert-Rosa v. Fortuno-Burset, 631 F.3d 592 (1st Cir. 2011) ("A plaintiff who is unaware of the identity of the person who wronged her can . . . proceed against a 'John Doe' . . . when discovery is likely to reveal the identity of the correct defendant."). Accord Brown v. Owens Corning Inv. Review Comm., 622 F.3d 564, 572 (6th Cir. 2010); Blakeslee v. Clinton County, 336 Fed.Appx. 248, 250 (3d Cir. 2009); Young v. Transp. Deputy Sheriff I, 340 Fed.Appx. 368 (9th Cir. 2009); Green v. Doe, 260 Fed.Appx. 717, 719 (5th Cir. 2007); Krueger v. Doe, 162 F.3d 1173 (10th Cir. 1998); Dean v. Barber, 951 F.2d 1210, 1215 (11th Cir. 1992); Munz v. Parr, 758 F.2d 1254, 1257 (8th Cir. 1985); Maclin v. Paulson, 627 F.2d 83, 87 (7th Cir. 1980).

B. Good Cause Exists to Grant the Motion

1. Plaintiff Has a Prima Facie Claim for Copyright Infringement

A prima facie claim of copyright infringement consists of two elements: (1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original. Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., Inc., 499 U.S. 340, 361 (1991). Plaintiff satisfied the first good cause factor by properly pleading a cause of action for copyright infringement:

> 48. Plaintiff is the owner of the copyrights for the Works, each of which contains an original work of authorship.

> 49. By using the BitTorrent protocol and a BitTorrent Client and the processes described above, each Defendant copied the constituent elements of the Works that are original.
>
> 50. Plaintiff did not authorize, permit or consent to Defendants' copying of its Works.

Complaint at ¶¶ 48-50. See 17 U.S.C. §106; In re Aimster Copyright Litig., 334 F.3d 643, 645 (7th Cir. 2003), *cert. denied*, 124 S. Ct. 1069 (2004) ("Teenagers and young adults who have access to the Internet like to swap computer files containing popular music. If the music is copyrighted, such swapping, which involves making and transmitting a digital copy of the music, infringes copyright."); Elektra Entm't Group, Inc. v. Doe, No. 5:08-CV-115-FL, 2008 WL 5111886, at *4 (E.D.N.C. Dec. 4, 2008) ("[P]laintiffs have established a prima facie claim for copyright infringement, as they have sufficiently alleged both ownership of a valid copyright and encroachment upon at least one of the exclusive rights afforded by the copyright."); Warner Bros. Records, Inc. v. Doe, No. 5:08-CV-116-FL, 2008 WL 5111883, at *4 (E.D.N.C. Dec 4, 2008) (same). Further, Plaintiff's allegations of infringement are attested to by Plaintiff's investigator, IPP, Limited's employee, Tobias Fieser. See Declaration of Tobias Fieser in Support of Plaintiff's Motion For Leave to Serve Third Party Subpoenas Prior to a Rule 26(f) Conference ("Fieser Declaration") at ¶¶ 18 and 22, Exhibit A. Accordingly, Plaintiff has exceeded its obligation to plead a prima facie case.

2. Plaintiff Has Clearly Identified Specific Information It Seeks Through Discovery

Plaintiff seeks to discover from the Defendants' ISPs the true name, address, telephone number, e-mail address and Media Access Control ("MAC") address of the Defendants. This is all specific information that is in the possession of the Defendants' ISPs that will enable Plaintiff to serve process on Defendants. Since the requested discovery is limited and specific, Plaintiff

has satisfied the second good cause factor. Sony Music Entm't v. Does 1-40, 326 F.Supp.2d 556, 566 (S.D.N.Y. 2004); BMG Music v. Doe # 4, No. 1:08-CV-135, 2009 WL 2244108, at *3 (M.D.N.C. July 24, 2009) (finding under nearly identical circumstances that "the discovery request is sufficiently specific to establish a reasonable likelihood that the identity of Doe # 4 can be ascertained so that he or she can be properly served").

3. No Alternative Means Exist to Obtain Defendants' True Identities

Other than receiving the information from the Defendants' ISPs, there is no way to obtain Defendants' true identities because "[o]nly the ISP to whom a particular IP address has been assigned for use by its subscribers can correlate the IP address to a real person, the subscriber of the internet service." Fieser Declaration at ¶ 9. Indeed, "[o]nce provided with the IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and Media Access Control number of the subscriber [i.e., the Defendant]." Fieser Declaration at ¶ 23. Since there is no other way for Plaintiff to obtain Defendants' identities, except by serving a subpoena on Defendants' ISPs demanding it, Plaintiff has established the third good cause factor. See Columbia Ins. Co. v. Seescandy et al., 185 F.R.D. 573, 578-80 (N.D. Cal. 1999); Elektra Entm't Group, Inc. v. Doe, No. 5:08-CV-115-FL, 2008 WL 5111886, at *4 (E.D.N.C. Dec. 4, 2008) (finding that the feasibility of a suggested alternative method of determining defendants' identities by hiring a private investigator to observe downloading "is questionable at best"); Warner Bros. Records, Inc. v. Doe, No. 5:08-CV-116-FL, 2008 WL 5111883, at *4 (E.D.N.C. Dec 4, 2008) (same).

4. Plaintiff Needs the Subpoenaed Information to Advance the Asserted Claims

Obviously, without learning the Defendants' true identities, Plaintiff will not be able to serve the Defendants with process and proceed with this case. Plaintiff's important statutorily protected property rights are at issue in this suit and, therefore, the equities should weigh heavily in favor of preserving Plaintiff's rights. Since identifying the Defendants by name is necessary for Plaintiff to advance the asserted claims, Plaintiff has established the fourth good cause factor. Sony, 326 F.Supp. at 566; BMG Music v. Doe # 4, No. 1:08-CV-135, 2009 WL 2244108, at *3 (M.D.N.C. July 24, 2009) (finding under nearly identical circumstances that "[p]laintiffs have shown that the subpoenaed information—Doe # 4's identity—is centrally needed to advance Plaintiffs' copyright infringement claim").

5. Plaintiffs' Interest in Knowing Defendants' True Identities Outweighs Defendants' Interests in Remaining Anonymous

Plaintiff has a strong legitimate interest in protecting its copyrights. Defendants are all copyright infringers that have no legitimate expectation of privacy in the subscriber information they provided to the ISPs, much less in distributing the copyrighted work in question without permission. See Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) ("computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator"); BMG Music v. Doe # 4, No. 1:08-CV-135, 2009 WL 2244108, at *3 (M.D.N.C. July 24, 2009) (finding under nearly identical circumstances that "[p]laintiffs have shown that Defendant Doe # 4 has a minimal expectation of privacy in downloading and distributing copyrighted songs without permission"); Interscope Records v. Does 1-14, 558 F.Supp.2d 1176, 1178 (D. Kan. 2008) (a person using the Internet to distribute or download copyrighted music without authorization is not entitled to have their identity protected

from disclosure under the First Amendment); Sony, 326 F.Supp.2d at 566 ("defendants have little expectation of privacy in downloading and distributing copyrighted songs without permission"). Since Defendants do not have a legitimate interest in remaining anonymous, and since Plaintiff has a strong, statutorily recognized and protected interest in protecting its copyrights, Plaintiff has established the fifth good cause factor.

III. CONCLUSION

For the foregoing reasons, this Court should grant leave to Plaintiff to issue Rule 45 subpoenas to the ISPs.

Dated: August 22, 2012

Respectfully submitted,

FIORE & BARBER, LLC

By: _____

Christopher P. Fiore, Esquire
Aman M. Barber, III, Esquire
Attorneys for Plaintiff
425 Main Street, Suite 200
Harleysville, PA 19438
Tel: (215) 256-0205
Fax: (215) 256-9205
Email: cfiore@fiorebarber.com

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

MALIBU MEDIA, LLC. Plaintiff, vs. JOHN DOES 1-9, Defendants.	Civil Action No. _____

DECLARATION OF TOBIAS FIESER IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO SERVE THIRD PARTY SUBPOENAS PRIOR TO A RULE 26(f) CONFERENCE

I, TOBIAS FIESER, HEREBY DECLARE:

1. My name is Tobias Fieser.

2. I am over the age of 18 and am otherwise competent to make this declaration.

3. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

4. I am employed by IPP, Limited ("IPP"), a company organized and existing under the laws of Germany, in its litigation support department.

5. Among other things, IPP is in the business of providing forensic investigation services to copyright owners.

6. As part of my duties for IPP, I routinely identify the Internet Protocol ("IP") addresses that are being used by those people that are using the BitTorrent protocol to reproduce, distribute, display or perform copyrighted works.

7. An IP address is a unique numerical identifier that is automatically assigned to an

internet user by the user's Internet Service Provider ("ISP").

8. ISPs keep track of the IP addresses assigned to their subscribers.

9. Only the ISP to whom a particular IP address has been assigned for use by its subscriber can correlate the IP address to a real person, the subscriber of the internet service.

10. From time to time, a subscriber of internet services may be assigned different IP addresses from their ISP. Accordingly, to correlate a person with an IP address the ISP also needs to know when the IP address was being used.

11. Many ISPs only retain the information sufficient to correlate an IP address to a person at a given time for a very limited amount of time.

12. Plaintiff retained IPP to identify the IP addresses that are being used by those people that are using the BitTorrent protocol and the internet to reproduce, distribute, display or perform Plaintiffs' copyrighted works.

13. IPP tasked me with implementing, monitoring, analyzing, reviewing and attesting to the results of the investigation.

14. During the performance of my duties, I used forensic software named INTERNATIONAL IPTRACKER v1.2.1 and related technology enabling the scanning of peer-to-peer networks for the presence of infringing transactions. A summary of how the software works is attached as Exhibit A.

15. INTERNATIONAL IPTRACKER v1.2.1 was correctly installed and initiated on a server located in the United States of America.

16. I personally extracted the resulting data emanating from the investigation.

17. After reviewing the evidence logs, I isolated the transactions and the IP addresses being used on the BitTorrent peer-to-peer network to reproduce, distribute, display or perform

Plaintiffs' copyrighted works.

18. Through each of the transactions, the computers using the IP addresses identified on Exhibit B connected to the investigative server in order to transmit a full copy, or a portion thereof, of a digital media file identified by the hash value set forth on Exhibit B.

19. The IP addresses, hash values and hit dates contained on Exhibit B correctly reflect what is contained in the evidence logs.

20. The peers using the IP addresses set forth on Exhibit B were all part of a "swarm" of peers that were reproducing, distributing, displaying or performing the copyrighted work identified on Exhibit B.

21. Our software analyzed each BitTorrent "piece" distributed by each IP address listed on Exhibit B and verified that reassembling the pieces using a specialized BitTorrent Client results in a fully playable digital motion picture which has the same identical hash as on Exhibit B.

22. I was provided with a control copy of the copyrighted works identified on Exhibit B (the "Movies"). I viewed the Movies side-by-side with the digital media file identified by the hash value set forth on Exhibit B and determined that the digital media file contained movies that were identical, striking similar or substantially similar.

23. Once provided with the IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and Media Access Control number of the subscriber.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 16th day of August, 2012.

TOBIAS FIESER

By: _____

EXHIBIT A

TO: DECLARATION OF TOBIAS FIESER IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO A RULE 26(f) CONFERENCE

IPP international LTD.

FUNCTIONAL DESCRIPTION

IPP international IPTRACKER v1.2.1

Table of contents

1 Introduction

The following disquisition introduces the software IPP international IPTRACKER. The software was developed to determine copyright violations in peer-to-peer networks (called P2P networks) and to preserve evidences during illegal distribution of copyright protected material.

P2P allows spreading data of every kind (software, music, video etc.) via the Internet fast. The data is saved on the computers of the participants and is distributed by common P2P software products which are available on the Internet for free. The Data is usually copied from foreign computers (called download) while other data is sent at the same time (called upload). Every participant can release files on his computer and make it available to others, comparable to the file release function within a local network. The files are copied via direct connection between the computers. P2P networks have millions of users and offer an enormous variety of files.

The procedure itself is legal for data which is not under copyright.

A common description of the operation of most commonly used P2P peer-to-peer techniques used to exchange data on the Internet can be found in the addendum.

2 The program IPP international IPTRACKER v1.2.1

2.1 Description of Action

2.1.1 Filesearch

Once a file is downloaded, verified and definitely allocated to a Rights holder, the hash value is used to determine possible sources on the internet. Different servers, trackers and clients provide lists of IPs where the specific file could or still can be downloaded.

2.1.2 Summarization of the procedure

These lists are downloaded from the providing system and computed sequentially. Each IP found in these lists is requested using the common P2P protocol functions. If the requested P2P client confirms the existence of the file on the local hard disc (in the shared folders), the download is started.
If the part downloaded is sufficient to be verified and compared to the original, the IP address and exact time and date is stored in a secure database.
The download process is continued.

After completion of the download process and before the stored information is used for further steps the downloaded data is compared with the original (complete already downloaded and verified file) bit by bit.

2.1.3 Safety of IP and other connection data

A direct and continuous connection between the IPTRACKER-server and the uploader of the file is established and exists at least 10 seconds before, during and at least 10 seconds after the capture sequence i.e. during the whole download process.

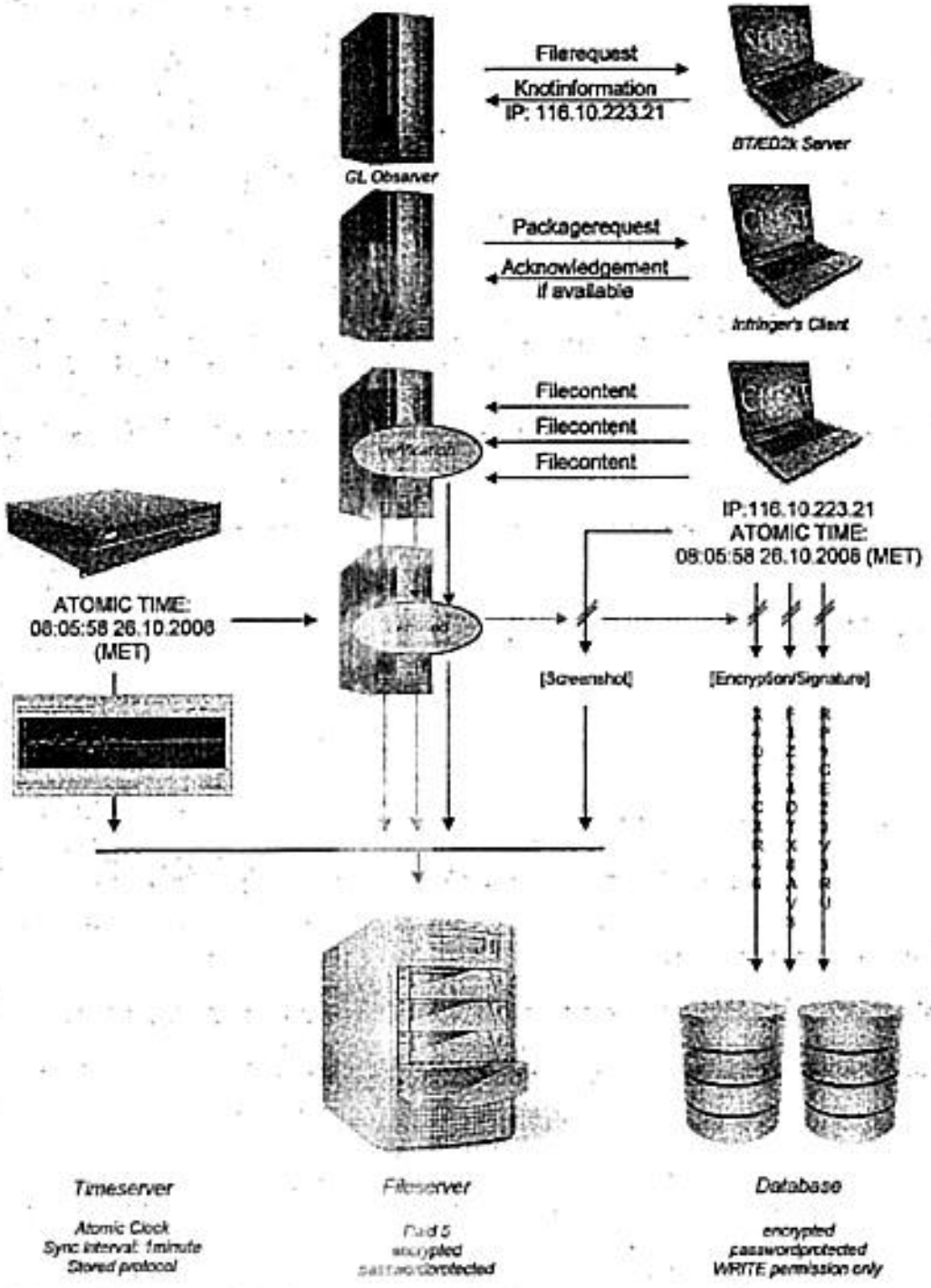
Optionally the screen can be capture automatically to backup another evidence.

2.1.4 The date and time

The (IPTRACKER-) server date and time is synchronised every minute via Network time protocol (NTP). This function is provided by an additional program (Dimension 4 v5.0 http://www.thinkman.com/dimension4).
The synchronization report is saved frequently and redundantly stored on a file server. The time is received from the Federal technological Institute in Brunswick (Physikalisch-Technische Bundesanstalt in Braunschweig) and has a maximum deviation of for 1/10 second (atomic clock).

Several other redundant institutes providing the exact time are stored in an internal database of the program: Dimension 4.

2.2 Visualisation of the process



2.3 Description of the most important program functions

The IPP international IPTRACKER is based on the hybrid Filesharing client Shareaza 2.4.0.0. All communication interfaces correspond to the specifications of the P2P protocols Bittorrent, Gnutella 1 and 2 as well as ED2k. These interfaces were left invariably in the filesharing client.

The function of the upload in addition was reduced to a minimum (handshaking).
The IPP international IPTRACKER merely stores the data of the hosts connected with, if the package verification succeeds.

- IP address
- port
- exact capture time
- name of the protocol
- filename
- file size
- hash values of the file (SHA1, ED2k, BitTH)
- GUID
- username
- clientname
- content downloaded

A screenshot of the host can be made by the IPTRACKER program. The host is marked automatically during the download phase to safeguard another evidence. Not relevant entries are masked. The name of the screenshot is also stored in the database.

To guarantee the immutability of the data, IP, date and time is signed with a private 4096 bit RSA key. The RSA key is included internally in the IPTRACKER program using a precompiled library and can be not read or used elsewhere.

RSA is a recognized asymmetrical encoding procedure which can be used both for the encoding and for the digital signature. It uses a key pair consisting of a private key which is used decode or sign data and a public key with which decoding or signature checks are made possible. Both keys are kept secret.

3 Logdata database

The data is stored in a MySQL database. The database server runs locally as a service on the respective server. The connection is established via ODBC driver: MyODBC-3.51.11. The query language is SQL. The IPTRACKER program accesses the database exclusively writing. The entries right-related cannot be changed.

The data is exclusively submitted as data sheets for the assertion of the injured rights.

3.1 Protection of data privacy and data security

The rack-servers are stored in a room which is locked and protected with most current security mechanisms.

The database is password protected and stored on an encoded hard disk. The hard disk is encoded with TrueCrypt 6.0 using AES encyption. The password is not saved on any computer, only known by two people and has more than 25 signs. It must be entered manually at every system startup. When the hard disk is removed from the computer or the power supply, it has to be mounted again using the password.

If the hard disk should be reached by unauthorized people, the data security is therefore ensured at any time.

To maximize data security, the IPTRACKER program offers an implemented program function which permits not only to sign but also to encode completely relevant data. So the data cannot be seen or changed even by persons with direct access to the server.

To create valid entries the secret key pair is necessary. It is not possibly to store data manually at any time.

Only the IPTRACKER program is able to create valid data.

The data can only be decoded and used by the responsible lawyer, only his software contains the deciphering method and this one in this case also secret (called "public") key.

4 Addendum

Basic Knowledge

P2P networks can be subdivided into several groups using their structure and operation.

Centralized P2P systems
These systems are using a central server to which all knots are connected. All search enquiries from the knots are processed by the server. The basis of P2P systems is the data transmission between the individual knots. A direct connection between the knots is established when the file is found on a specific knot.

The server is the bottle of the neck in this process.

Nowadays centralized P2P systems are of more minor importance.

Pure P2P systems without a central instance
There are networks without a central server which do not manage any central data stock (Gnutella1 and Gnutella2 network).

P2P-Filesharing networks via server client protocol
There are networks with one or several central servers which manage information about the users connected at present. This is provided by the Bittorrent and eDonkey network. With the installation of Emule the users receive a list of all users (file: servor.met) attached to a server and all released files. Bittorrent and eDonkey cover currently 95% of the exchange activity.

Gnutella

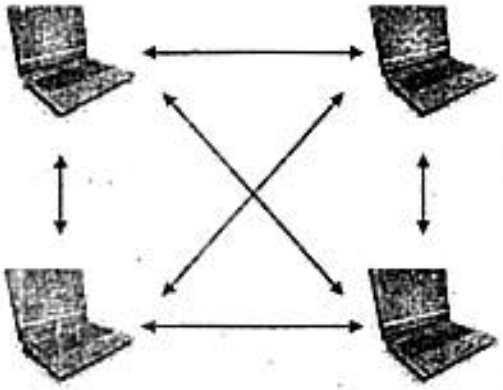
Gnutella is a P2P network decentralized completely which can be observed by the IPP international IPTRACKER software. "Decentralized" means that every knot uses a similar software and there are no central servers which process search enquiries.

A search query is passed to the neighbouring systems at first. These systems refer the query to their neighbours until the requested file was found. After that a direct connection for the data transmission can be established between searching and offering knot

Gnutella 2

Gnutella 2 works most largely like the original Gnutella network with a similar connection system but Unicode2 search function with extensive metadata, TigerTree Hashing, and generally faster link speed. A "Partial file Sharing" function was implemented which divides files into parts. It's possible to download these parts from different knots instead of downloading the whole file from one knot.

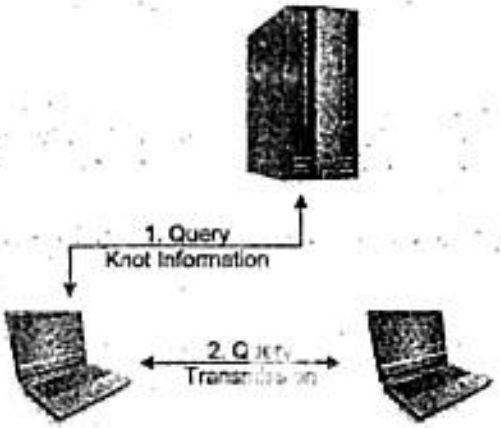
Some known Gnutella2 clients are:
Shareaza, Morpheus, Gnucleus, adagio, MLDonkey



eDonkey2000 (Ed2k)

The eDonkey2000 peer to peer network needs server to connect the knots. The server only provides lists of files which are available on the individual knots.

Some Edonkey2000 clients are: eMule, eMulePlus, aMule, xMule, MLDonkey, Lphant



Bittorrent (BT)

BitTorrent is used for the fast distribution of large amounts of data in which central servers are controlling the location of the files.

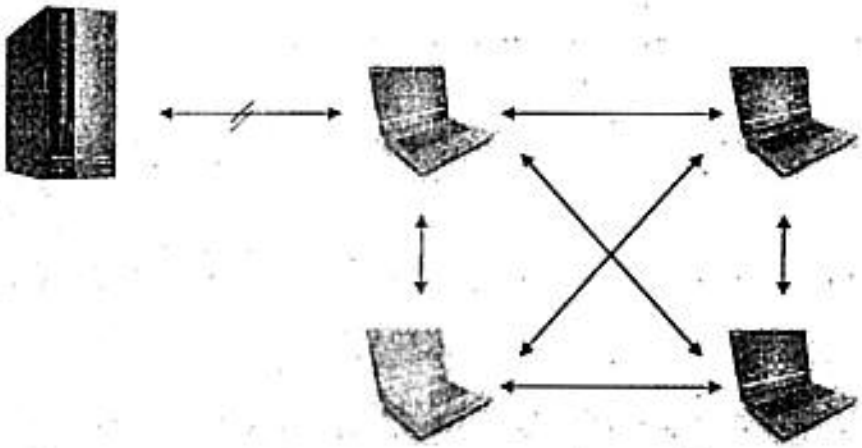
BitTorrent does not behave like a usual P2P network. There is no search function like it is available it at EDonkey or Gnutella clients.

To get all necessary information for a download, a .torrent file is downloaded (from another network or an internet page). It contains all information to start the download.

The Bittorrent participants connect with the so-called tracker of this file and with that with other users who also are interested in at this file. A private network is built.

Trackerless systems were developed in new versions. The tracker function is done by the client software. This avoids some of the previous problems (e.g. the missing failure safety of the trackers).

Some Bittorrent clients are: Shareaza, BitComet, Azureus



Globally Unique Identifier (GUID)

Every P2P user receives a unique identification which consists of a 32-digit hexadecimal number. The user receives the identification at the moment of the installation of the P2P program. The program generates the GUID from user-specific data. So it is possible that a user has several GUID identifications (e.g. he gets a new GUID at the installation of a network client), however, it is not possible that an allocated GUID is allocated to another user again.

The hash value

The hash value is necessary to identify a file.

A special advantage of Bittorrent, eDonkey and Gnutella networks is the fault-free data transmission between the users. Bigger files are subdivided into little packages. For every package a single identification value is generated using known algorithms. The hash value is frequently described as a fingerprint since it is unique similarly like a fingerprint.

i.e. each file exceeding the size of 2 megabytes owes more than one hash value - one for the whole file and one for each package.

Standard operation of common P2P-client programs during the filesharing process:

The client software must guarantee that the received content is always the queried one. Therefore only hash values are requested – filenames are unimportant during the transmission.

After a client received a data package the content has to be verified. Therefore the hash value of the package is generated by the client and compared to the hash value provided before. If the two keys are identical, the downloaded package is accepted. If there are deviations at the comparison, then the package is declined and requested again. The package can also be downloaded from another knot.

All mentioned programs are able to split bigger files into packages and to identify these using hash values independently which program is used for the data exchange. With this it is possible to assign small parts of a file to the original file. It is made sure that the part of the file always belongs to the requested file.

After the whole file is downloaded it will be verified on the whole before the download process is finished and the file is signed as "VERIFIED".

Every network uses different hash algorithms. Bittorrent the so-called "BITH", eDonkey this one "ED2K", and Gnutella the "SHA1" algorithm.

The IPP international IPTRACKER is able to generate and compare each hash algorithm listed above.

SHA-1 Hash: 5C30F05B0EF0F99BBF43E716A0EB53D31C179D7F **Title:** MaryJane Young Love
Rights Owner: Malibu Media

DOE#	IP	Hit date (UTC)	City	State	ISP	Network
1	174.60.64.189	6/26/2012 12:33	Reading	PA	Comcast Cable	BitTorrent
2	68.81.82.127	6/13/2012 22:25	Brookhaven	PA	Comcast Cable	BitTorrent
3	69.242.6.26	7/1/2012 22:01	Norristown	PA	Comcast Cable	BitTorrent
4	71.230.42.105	6/15/2012 23:34	Pottstown	PA	Comcast Cable	BitTorrent
5	68.238.195.233	8/4/2012 15:23	Allentown	PA	Verizon Internet Services	BitTorrent
6	71.175.140.161	7/24/2012 17:17	Philadelphia	PA	Verizon Internet Services	BitTorrent
7	71.175.185.128	6/2/2012 4:15	Fleetwood	PA	Verizon Internet Services	BitTorrent
8	71.175.78.237	6/27/2012 18:02	Jenkintown	PA	Verizon Internet Services	BitTorrent
9	98.114.230.81	7/30/2012 5:43	Southampton	PA	Verizon Internet Services	BitTorrent