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.

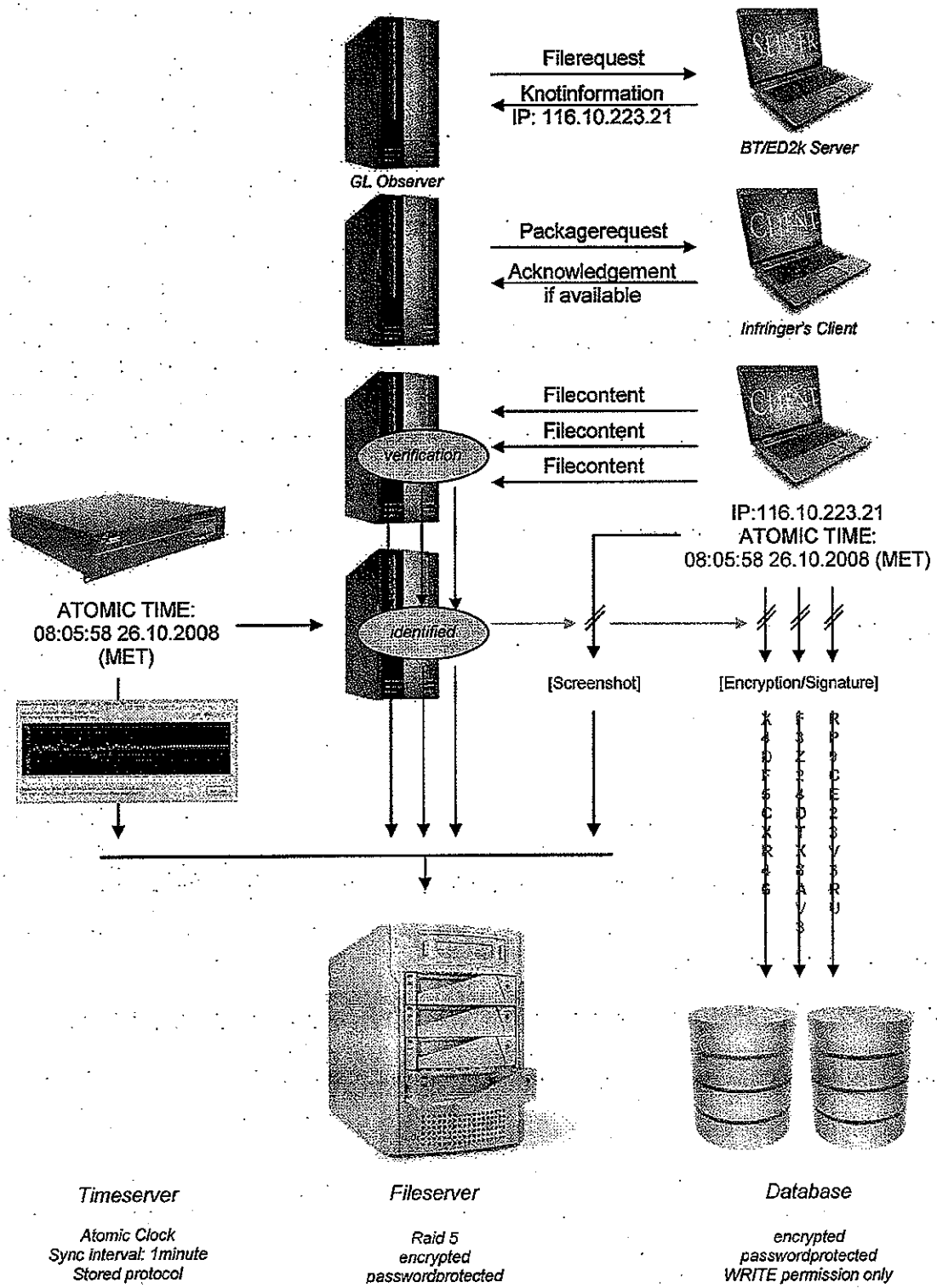
Optionally the screen can be capture automatically to backup another evidence.

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, BiTH)
- 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: server.met) attached to a server and all released files. Bittorrent and eDonkey cover currently 95% of the exchange activity.

Gnutella

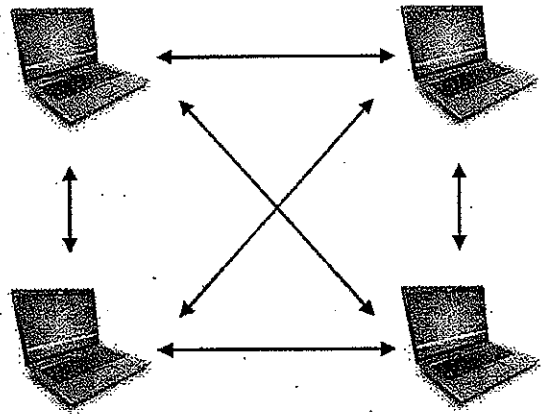
Gnutella is a P2P network decentralized completely which can be observed by the IPP international IPTRACKER software. "Decentralized" means that every knot uses a similar software and there are no central servers which process search enquiries.

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.

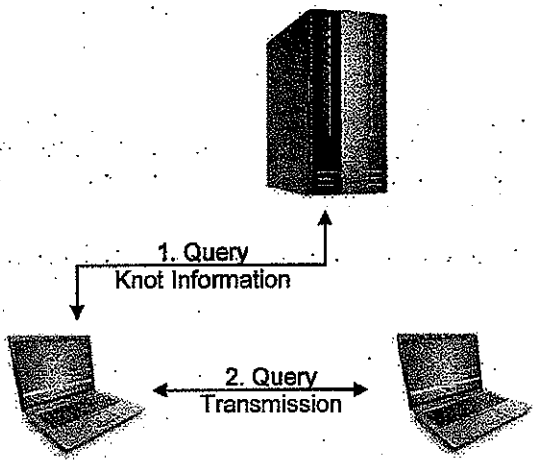
Some known Gnutella2 clients are:
Shareaza, Morpheus, Gnucleus, adagio, MLDonkey



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.

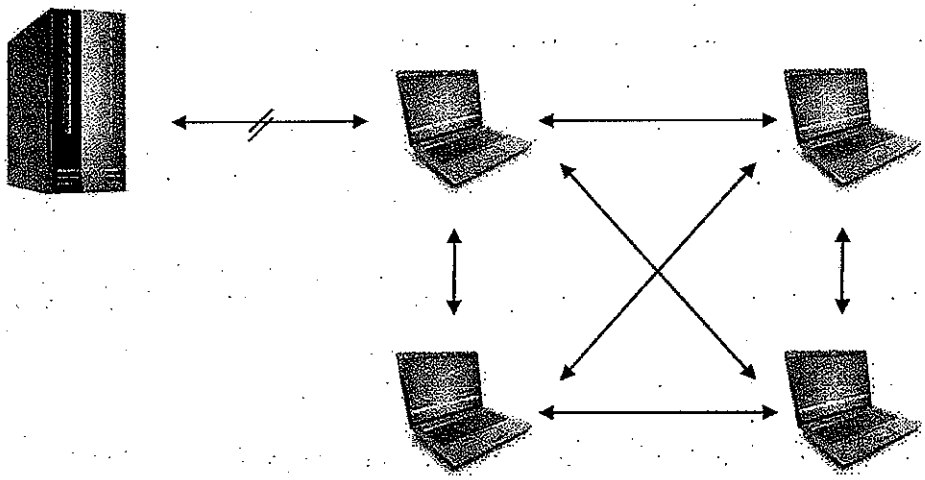
BitTorrent does not behave like a usual P2P network. There is no search function like it is available it at EDonkey or Gnutella clients.

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.