

# EXHIBIT A

## PERCIPIENT WITNESS STATEMENT OF THOMAS SEHESTED

### **Professional Background and Experience**

I am the founder and Chief Executive Officer of DtecNet Software (“DtecNet”), a company with its principal offices at 9595 Wilshire Blvd, Beverly Hills, CA 90210 USA. DtecNet is a company that specializes in gathering evidence from the Internet.

Before the commencement of my employment with DtecNet in 2004, I held various senior level positions at companies that worked with and supplied Internet-based technologies. I have approximately 6 years of experience relating to the protocols, technical architecture, and operation of the Internet.

Within the last four years, I have testified as an expert at trial or deposition in the following cases: Arista Records LLC, et. al v. Usenet.com, Inc., Case No. 07-CV-08822 (S.D.N.Y.).

I have been retained by plaintiffs, through Munger, Tolles & Olson LLP, to provide testimony in the matter of Arista Records LLC et al. v. Lime Wire LLC et al., Case No. 06 CV 5936 (S.D.N.Y.).

Plaintiffs provided DtecNet with lists of sound recordings (the “Recordings”), and asked DtecNet to download copies of the Recordings from U.S.-based LimeWire users, and to gather and record information verifying the act of each download and the content of each download. I am the leader of the team of DtecNet employees engaged in this work.

DtecNet is being compensated \$26,000 for its work in connection with this project. In addition to this fee, I am being compensated for testimony during depositions and at trial at the rate of \$1,500 per day.

### **Overview of DtecNet LimeWire Download Project.**

Plaintiffs have retained DtecNet to download copies of the Recordings from U.S.-based LimeWire users, and to gather and record information verifying the act of each download and the content of each download. To perform this project plaintiffs provided DtecNet with lists containing artist and title information for the Recordings for the purpose of seeking and downloading each title from U.S.-based LimeWire users.

DtecNet successfully downloaded and verified a total of 10,341 files from LimeWire users on the Gnutella network located in the U.S. based on the title list provided by Plaintiffs. These files were downloaded on DtecNet’s U.S.-based servers, and were copied on a hard drive provided to Plaintiffs. The files verifying the act of each download are also included on this hard drive. I understand that Plaintiffs are providing to Defendants a copy of the files contained on this hard drive.

Below is a step by step account of how DtecNet has proceeded during the project.

### **Downloading**

First, DtecNet deployed its proprietary software (“Software”) to search on the Gnutella networks for U.S.-based LimeWire users sharing audio files matching the titles provided by Plaintiffs.

The Software connects to the Gnutella network using the communication protocol already made available to the public by the services operating on the P2P network. The Software connects to the P2P network in the same way as other publicly available P2P software clients and does not provide to DtecNet any information or data that would not be publicly available from the network if other publicly available software were used, such as the LimeWire client.

The evidence that DtecNet collected with respect to LimeWire users relates solely to titles that any other P2P user with a basic technical proficiency could search for and copy through other P2P software. DtecNet can only view and download files that the P2P users have chosen to distribute from the shared directory on their computers and DtecNet does not make any attempt to view or copy any other files on the users' computers.

When connected to the Gnutella P2P network the Software automatically began performing searches for titles based on the list of Recordings received from Plaintiffs. The matched results were then sent back to the Software for processing and to filter the results based on nationality, ISP and other relevant information.

Once a positive match for a file was established, the Software downloaded the file from the user. As part of this procedure the entire search and downloads process was closely monitored and recorded by the Software. This was done in order to deliver a complete and detailed evidence pack on each individual download. That information includes, among other things, the user's Internet Protocol ("IP") address and various log files to establish a 100% verification of the download as described below. As DtecNet was only instructed to search for users located within the U.S. all other users from other countries were automatically disregarded and therefore not investigated as part of this project.

### **Verification**

If the file completed a full download, each download was then processed through the audio fingerprinting software Audible Magic to verify the content as a matching title to the designated list.

If a file was verified, an evidence package was generated for each file which includes details such as the user's IP address, log files, packet capturing, and trace routing details. If a file was verified as "not matching," then the file was discarded and a reattempt was made on a different hash for the same title.

### **The Verification Evidence Package**

The verification evidence package for each downloaded track was included on the hard drive provided to Plaintiffs. The following is a summary of the verification evidence provided for each track.

### **Overview**

The first log file generated by the Software is a general summary of information related to the download conducted for each user. This includes key information about the download such as the IP Address of the uploader, the country and ISP information of the target user, and timestamps indicating when the investigation was initiated and completed.

This overview also shows what client the user was using while DtecNet was conducting the download, which in this case was Limewire 4.18.1.

[Overview](#)   [Activity Log](#)   [Communication Log](#)   [File List](#)   [Content Info](#)   [Traceroute](#)   [Print Page](#)

---

**Investigation details:**

<b>IP-Address</b>	12.158.149.32
<b>Country</b>	US
<b>Initiated</b>	06-07-2010 02:58:49.674 UTC
<b>Completed</b>	06-07-2010 03:02:44.904 UTC
<b>Protocol</b>	Gnutella
<hr/>	
<b>Target ISP</b>	AT&T WorldNet Services
<b>Target Port</b>	44810
<b>Target Hostname</b>	12.158.149.32
<hr/>	
<b>Server ISP</b>	Verizon Internet Services
<b>Server IP</b>	173.52.235.87
<b>Server Port</b>	13151
<b>Server Hostname</b>	pool-173-52-235-87.nycmny.fios.verizon.net
<b>Server Country</b>	US
<hr/>	
<b>Fingerprint</b>	77DEF69122A3DE3AFEFE53058053905C
<hr/>	
<b>Peer Client Info</b>	LimeWire/4.18.1

[»» View Packet Capture «« ««](#)   [View Downloaded Files «« ««](#)   [View Screen Shot Files «« ««](#)   [Export To Excel ««](#)

### Packet Capture.pcap

All network packets exchanged with the target machine are copied and stored using *WinPCap*, which is a widely used, professional packet capture library for Windows systems. The packets will be saved in trace files which can be viewed using *Ethereal*. Ethereal is a professional network traffic analyzer, supporting the WinPCap file format. All packets are stored in their original form, including a timestamp indicating when the packet was captured.

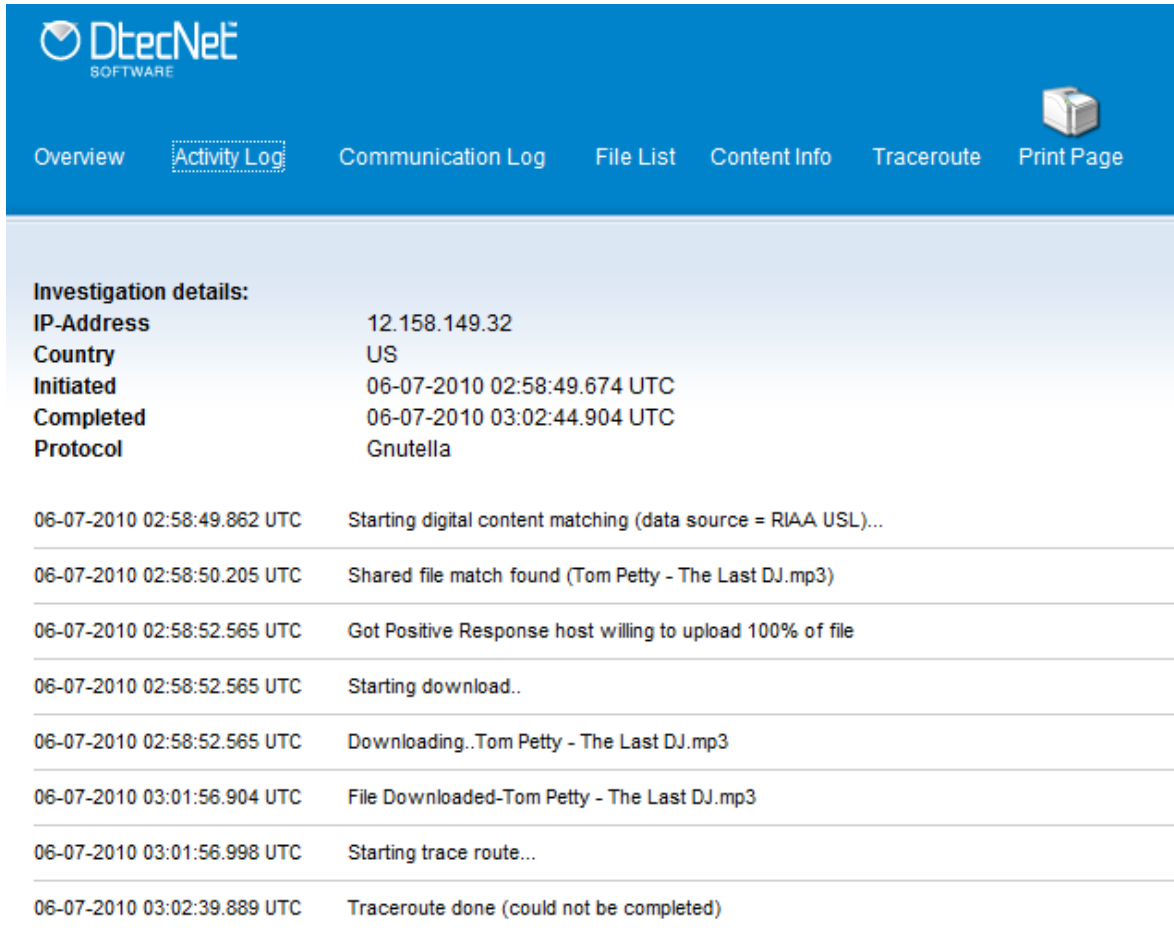
### Time Zone

All time stamps are in Coordinated Universal Time (UTC). This is a high-precision atomic time standard which replaced Greenwich Mean Time on 1 January 1972 as the basis for legal civil time all over the Earth. UTC has uniform seconds defined by International Atomic Time (TAI), with leap seconds announced at irregular intervals to compensate for the earth's slowing rotation, and other discrepancies. The leap seconds allow UTC to closely track Universal Time (UT), which is a time standard based on the earth's angular rotation, rather than a uniform passage of seconds.

### Activity Log

The activity log provides a general timeline for the entire download process and gives a summary of all the actions taken to secure evidence against the investigated user. Each activity logged will be accompanied by a timestamp indicating when the given event occurred.

The Activity Log for the case below breaks down each individual activity in detail from the moment of initiation to the moment of completion. Details such as what time the file was matched, if the user was willing to share with DtecNet the file, when the download began to the completion time of the download, and when the traceroute is conducted have all been preserved.



The screenshot shows the DtecNet Software interface. At the top, there is a navigation bar with the following tabs: Overview, Activity Log (which is highlighted with a dashed border), Communication Log, File List, Content Info, Traceroute, and Print Page. Below the navigation bar, the 'Investigation details' section is displayed, showing the following information:

<b>IP-Address</b>	12.158.149.32
<b>Country</b>	US
<b>Initiated</b>	06-07-2010 02:58:49.674 UTC
<b>Completed</b>	06-07-2010 03:02:44.904 UTC
<b>Protocol</b>	Gnutella

Below the investigation details, a list of activity log entries is shown, each with a timestamp and a description:

06-07-2010 02:58:49.862 UTC	Starting digital content matching (data source = RIAA USL)...
06-07-2010 02:58:50.205 UTC	Shared file match found (Tom Petty - The Last DJ.mp3)
06-07-2010 02:58:52.565 UTC	Got Positive Response host willing to upload 100% of file
06-07-2010 02:58:52.565 UTC	Starting download..
06-07-2010 02:58:52.565 UTC	Downloading..Tom Petty - The Last DJ.mp3
06-07-2010 03:01:56.904 UTC	File Downloaded-Tom Petty - The Last DJ.mp3
06-07-2010 03:01:56.998 UTC	Starting trace route...
06-07-2010 03:02:39.889 UTC	Traceroute done (could not be completed)

### Communication Log

File-sharing systems use a protocol, which defines a set of messages that enable clients to communicate with each other. The communication log will contain an entry for all protocol-related messages sent and received during the download. All entries will include a timestamp indicating when the message was sent or received.

The below Communication Log shows the active communication between DtecNet's monitoring agent and the uploader. Within the communication's log, the uploader shares details of the filename, the file hash, and the client application being used.

Overview
Activity Log
Communication Log
File List
Content Info
Traceroute
Print Page

**Investigation details:**

<b>IP-Address</b>	12.158.149.32
<b>Country</b>	US
<b>Initiated</b>	06-07-2010 02:58:49.674 UTC
<b>Completed</b>	06-07-2010 03:02:44.904 UTC
<b>Protocol</b>	Gnutella

06-07-2010 02:58:52.565 UTC <--

```

HTTP/1.1 200 OK Date: Tue, 6 Jul 2010 02:58:38 GMT Content-Disposition: attachment;
filename="Tom%20Petty%20-%20The%20Last%20DJ.mp3" Content-Range: bytes 0-3685981/3685982 X-Gnutella-
Content-URN: urn:sha1:T54DFDBBRFH4X7FW2E5SRGORZURD656C X-Create-Time: 795672412000 X-Features:
chat/0.1,browse/1.0,fwalt/0.1 X-Thex-URI: /uri-res
/N2X?urn:sha1:T54DFDBBRFH4X7FW2E5SRGORZURD656C;PJHR2VEPXZ4AGRQJFIOCKWQRWBONOOM5AJP6ABY
Server: LimeWire/4.18.1 Content-Length: 3685982 Content-Type: application/binary Connection: Keep-Alive
            
```

### Content Info

The Content Info section contains key details regarding the file such as the file name, file size, the percentage of the file that is being shared, the percentage of the file in which we were able to download, the hash value, the artist name, and the title of the content. In the case below, DtecNet was able to complete the download of the Tom Petty song The Last DJ from the uploader who had the full 3.52MB of the file.

Overview
Activity Log
Communication Log
File List
Content Info
Traceroute
Print Page

**Investigation details:**


<b>IP-Address</b>	12.158.149.32
<b>Country</b>	US
<b>Initiated</b>	06-07-2010 02:58:49.674 UTC
<b>Completed</b>	06-07-2010 03:02:44.904 UTC
<b>Protocol</b>	Gnutella


---

<b>File Name</b>	Tom Petty - The Last DJ.mp3
<b>File Size</b>	3.52 MB
<b>Shared</b>	3.52 MB (100 %)
<b>Downloaded</b>	3.52 MB (100 %)
<b>Verified</b>	N/A
<b>Hash Value</b>	T54DFDBBRFH4X7FW2E5SRGORZURD656C
<b>Match Database</b>	RIAA USL
<b>Artist</b>	Tom Petty
<b>Title</b>	The Last DJ

### Traceroute.xml

A trace route of the investigated user's IP address is performed. This estimates the route that network packets travel to reach the investigated user's machine. DNS lookups are performed on all machines encountered.



 [Print Page](#)

[Overview](#)
[Activity Log](#)
[Communication Log](#)
[File List](#)
[Content Info](#)
[Traceroute](#)
[Print Page](#)

**Investigation details:**

<b>IP-Address</b>	12.158.149.32
<b>Country</b>	US
<b>Initiated</b>	06-07-2010 02:58:49.674 UTC
<b>Completed</b>	06-07-2010 03:02:44.904 UTC
<b>Protocol</b>	Gnutella

<b>Traceroute Initiated</b>	06-07-2010 03:01:57.014 UTC
<b>Traceroute Completed</b>	06-07-2010 03:02:39.889 UTC

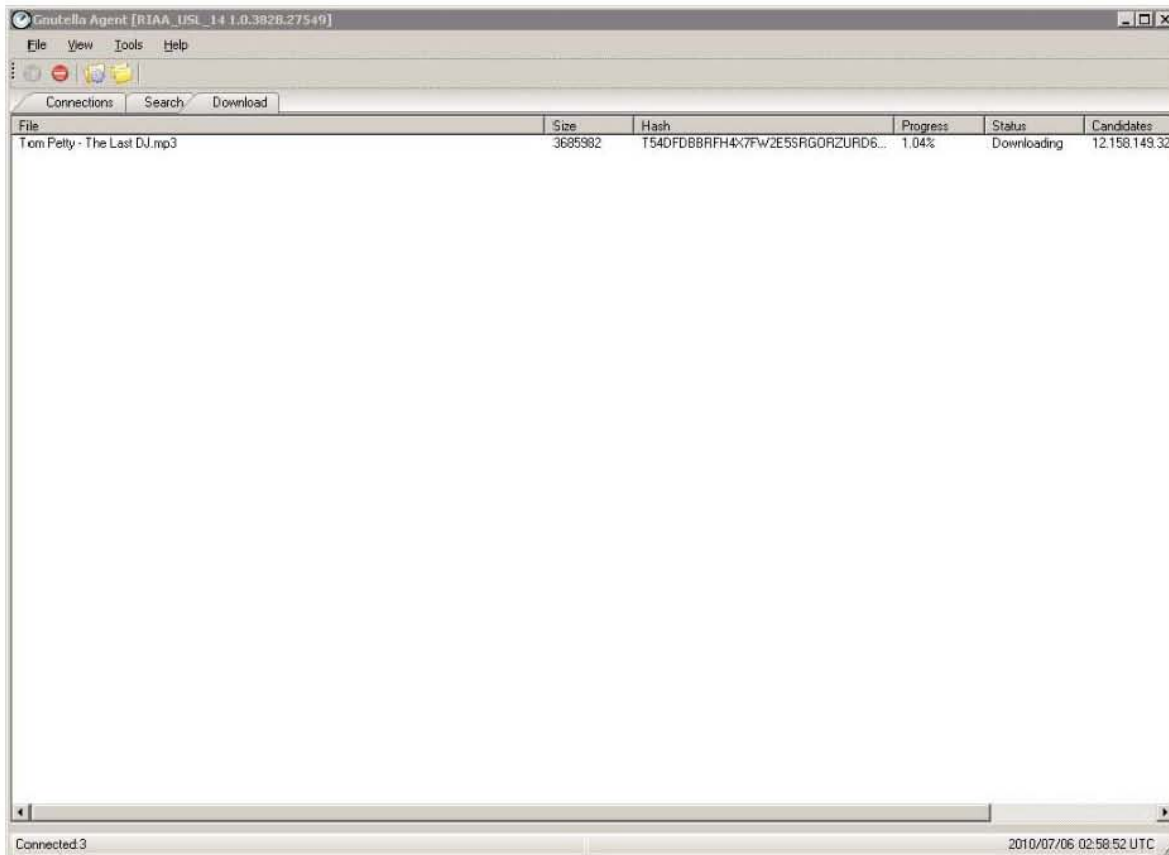
#	Time	RTT	IP	AS	Name
1	3ms	0ms	74.55.38.89	US	THEPLANET.COM INTERNET SERVICES
2	0ms	0ms	207.218.245.21	US	THEPLANET.COM INTERNET SERVICES
3	0ms	0ms	207.218.223.37	US	THEPLANET.COM INTERNET SERVICES
4	0ms	0ms	70.87.253.154	US	THEPLANET.COM INTERNET SERVICES
5	5ms	5ms	12.88.102.229	US	AT&T WorldNet Services
6	16ms	16ms	12.122.147.138	US	AT&T WorldNet Services
7	16ms	16ms	12.122.28.157	US	AT&T WorldNet Services
8	16ms	16ms	12.122.28.86	US	AT&T WorldNet Services
9	15ms	15ms	12.123.130.89	US	AT&T WorldNet Services
10	33ms	33ms	12.88.71.234	US	AT&T WorldNet Services
11	34ms	34ms	76.77.218.18	US	Carson Communications, LLC
12	34ms	34ms	68.234.96.65	US	Blue Valley Tele-communications
13	37ms	36ms	169.254.10.249	Unknown	Local Area Network
14	-1ms	-1ms			
15	-1ms	-1ms			
16	-1ms	-1ms			

<b>DNS Lookup(12.158.149.32)</b>	<b>12.158.149.32</b>
----------------------------------	----------------------

### Screen Prints

The screen prints below show the Software downloading the specific file from the user as well as the completion of the full download.





File	Size	Path	Ping(s)	State	Location
Test File - The Last Of Us	309180	15014659746107-2510-40202104	100	Connected	12.90.18.10

September 30, 2010

Thomas Sehested