1-1-2011

# An investigation into darknets and the content available via anonymous peer-to-peer file sharing

Symon Aked
*Edith Cowan University*



DOI: 10.4225/75/57b52857cd8b3
9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

# AN INVESTIGATION INTO DARKNETS AND THE CONTENT AVAILABLE VIA ANONYMOUS PEER-TO-PEER FILE SHARING

Symon Aked
School of Computer and Security Science
Edith Cowan University, Perth Western Australia
secau.2011@tanstaafl.com.au

## Abstract

*Media sites, both technical and non-technical, make references to Darknets as havens for clandestine file sharing. They are often given an aura of mystique; where content of any type is just a mouse click away. However, can Darknets really be easily accessed, and do they provide access to material that would otherwise be difficult to obtain? This paper investigates which Darknets are easily discovered, the technical designs and methods used to hide content on the networks, the tools needed to join, and ultimately what type and quantities of files can be found on anonymous peer-to-peer file sharing networks. This information was gathered by conducting weekly searches for specific file extensions on each Darknet over a 4 week period. It was found that connectivity to Darknets was easy to establish, and installing peer-to-peer file sharing applications was a simple process. The quantity of content found on Darknet peer-to-peer file sharing networks indicates that file sharing is rampant. Of particular concern was what appears to be a large quantity of child pornography made available.*

**Keywords**
Darknet, anonymous, p2p, peer-to-peer, file sharing

## INTRODUCTION

Peer-to-peer (also known as P2P) file sharing has been gaining in popularity since the days of Napster in 1999 (Riedel, 2006). Peer-to-peer file sharing accounts for around 18.8% of all North American, 18.0% of Latin American, and 30.1% of European fixed Internet access usage ("Sandvine Global Internet Report Spring 2011", 2011). This large amount of traffic shows that there is a high demand for the exchange of files between Internet users.

The types of file available on peer-to-peer file sharing networks are varied. The files available on BitTorrent can be broken down into seven categories (Sahi, 2010) (Table 1).

*Table 1 –claimed file types available on the BitTorrent peer-to-peer file sharing network*

| Movies and TV shows | Games and software | Pornography | Music | Books and guides | Images | Could not classify |
|---|---|---|---|---|---|---|
| 46% | 14% | 14% | 10% | 1% | 1% | 14% |

The files available via the eDonkey peer-to-peer file sharing network can also be categorised into seven types of content (Puig-Centelles, Ripolles & Chover, 2008) (Table 2).

*Table 2 – claimed file types available on the eDonkey peer-to-peer file sharing network*

| Video | Audio | Software | Images | Documents | Others | eMule Collection |
|---|---|---|---|---|---|---|
| 42% | 20% | 17% | 13% | 5% | 2% | 1% |

However these studies do not probe the types and quantities of content available on Darknets.

### What is a Darknet?

The term "Darknet" has no formal definition. It was popularised by the paper "The Darknet and the Future of Content Distribution" (Biddle, England, Peinado, & Willman, 2002), which defined a Darknet as "…a collection of networks and technologies used to share digital content.".

The usage of the term "Darknet" has evolved to refer collectively to all covert communications networks. Darknets are encrypted data networks that ensure data transmitted cannot be intercepted, changed, observed or read by an unauthorised party. Darknets may also be designed to allow participants to be anonymous, or obtain pseudo-anonymity where desired.

Darknets sit on "top" of the Internet, in an encrypted cloud that cannot be viewed without the required software. As the content and members of a Darknet are not publically viewable, their presence is easily overlooked.

Given the popularity of peer-to-peer file sharing systems that take few (if any) steps to preserve the anonymity of its users, what are the benefits in taking the extra steps required to join a Darknet and acquire content from it? Does being anonymous mean that different content is distributed and available to download? Can a person that is not technically sophisticated and looking to obtain content from a Darknet able to do so?

This paper examines the quantity and types of files available, based on their names and sizes, via easily discovered peer-to-peer file sharing applications running on their respective Darknets. A number of restrictions were placed on which Darknets were to be investigated to focus on those most likely to be encountered by someone not previously exposed to Darknets.

The first filter is to only examine those Darknets that run on Microsoft Windows. This is because with an approximate market share of 92% ("Desktop Operating System Market Share", 2011), it is likely that a Darknet novice is running Windows. This excluded Darknets such as Gnunet.

Peer-to-peer file sharing applications that require the user to go through a "vetting" process before being allowed access to content are also excluded from this investigation, as well as Darknets that have a friend-to-friend requirement (such as the Anonet 2). These are filtered as is quite likely that a person that has no experience connecting to Darknets would not have friends that can vouch for, or peer with them.

One of the most popular Darknets, TOR (The Onion Router), is also excluded. This is because peer-to-peer file sharing is highly discouraged on the network, due to the network not being designed to handle such traffic (Arma, 2010). This is also why there is no TOR-specific anonymous peer-to-peer sharing application. Also, BitTorrent is also known to not be secure over TOR (Arma, 2010).

*Table 3 – Darknets to be investigated*

| Darknet | URL | P2P protocols used | P2P applications used |
|---|---|---|---|
| I2P | http://www.i2p2.de | Gnutella, BitTorrent, eDonkey | I2Phex, I2PSnark, iMule |
| Freenet | https://freenetproject.org | Freenet | Frost |

The two Darknets that are to be investigated (Table 3) have quite different implementations of the way they encrypt, distribute content, and ensure users remain anonymous.

**I2P**

I2P (Invisible Internet Project) is an encrypted network layer that applications can use to transmit data. I2P uses four layers of encryption with both the source and destination IP addresses being hidden to each other and third parties. I2P is designed so that any application can send its data into the network via the client's I2P routing software, rather than requiring custom written applications. The advantage of this method is that open source peer-to-peer file sharing applications can be modified to function on I2P.

An I2P user communicates with other users by establishing a pool of inbound and outbound encrypted tunnels (Figure 1). When a client has data that has been requested by another client, it sends the data out of one of its outbound tunnels towards the target's inbound tunnel. The number of hops is determined by the client, trading latency for increased anonymity. Tunnels are torn down and re-created every 10 minutes to further enhance security.

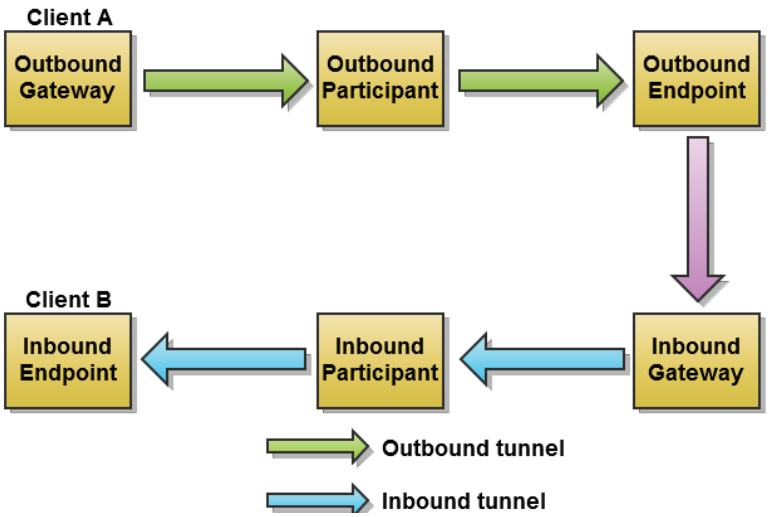


*Figure 1 – inbound and outbound tunnels in I2P*

I2P addresses can be identified by the ".i2p" TLD on website URLs. There are a number of Internet-to-I2P proxies that allow access to I2P websites, although being routed via the Internet removes the anonymity and encryption inherent in I2P.

I2P had an average of 6479 users connected to it in September ("One Month View for Total Routers", 2011). Usage of I2P was static at around 2500 users until May 2011, which saw the beginning of a greatly increased number of new users joining the network each month. This dramatic increase may be at least partially attributed to well publicised prosecution attempts of people downloading movies via BitTorrent such as The Expendables (Kravets, 2011) and The Hurt Locker (Williams, 2011).

The most popular protocols to share files on I2P are eDonkey, BitTorrent and Gnutella, accessed by the iMule, I2PSnark and I2Phex applications respectively. iMule is a modification of the popular aMule application, used to access the eDonkey network on the Internet. I2PSnark is built in to the I2P application and requires connectivity to a BitTorrent tracker, the most popular being "tracker2.postman.i2p". I2Phex is a modification of the Phex Gnutella client. The Gnutella network inside I2P has been decreasing in popularity due to issues connecting clients to the network.

**Freenet**

Freenet was initially released in March 2000 ("What is Freenet?", n.d.). It is a decentralised, distributed data store that affords users anonymity via multiple layers of encryption and routing.

The Freenet documentation states that it has a Darknet mode which requires that its friend-to-friend mode be engaged ("What is Freenet?", n.d.). For the purposes of this investigation the connection to Freenet will be in "Opennet" mode, as it fits the Darknet criteria of being encrypted and anonymous.

Freenet is unique in the way that it provides content to users. Instead of providing an encrypted tunnel into the network, which routes data to hosts that serve content in the traditional client-server manner, it instead allocates part of the user's secondary storage (typically a hard drive) for its use. Files stored on Freenet are encrypted and cut into chunks. These chunks of data are then stored on random Freenet user's secondary storage, replicated as required, to be made available to users that request content that comprises of these data chunks. As the chunks are encrypted, there is no way to determine what data is being stored in the Freenet storage area.

The network is designed so that the original provider of content to the network is not the sole source – once the content has been uploaded to Freenet, it remains there, regardless of the provider's Freenet connectivity. This negates the requirement for the original provider to stay connected to the network once the connected has been uploaded – instead the content is cut up, encrypted and replicated across Freenet. How popular the content is will dictate across how many nodes it gets replicated, so popular content is duplicated multiple times, and hence more readily available and quicker to download.

It is this same content distribution system that is used to publish websites. Instead of the traditional webserver hosting HTML pages, a website is instead distributed in the same way as other content on Freenet (encrypted and cut into chunks). The FBproxy application built in to Freenet is then used to access the content via a web browser. In this way websites can be published without requiring a dedicated server to host them.

Freenet has no central servers and is not under the jurisdiction of any individual or group. This makes Freenet a difficult target to take down, and is designed to be resilient against flooding, poisoned nodes and data tampering.

Each Freenet user not only acts as a data store, but also as a router. Each request for a data chunk may be served by a user, or the request forwarded on if it does not have the requested data. This method helps ensure the anonymity of users as an attacker cannot determine where data is being served from, or who the original requestor is.

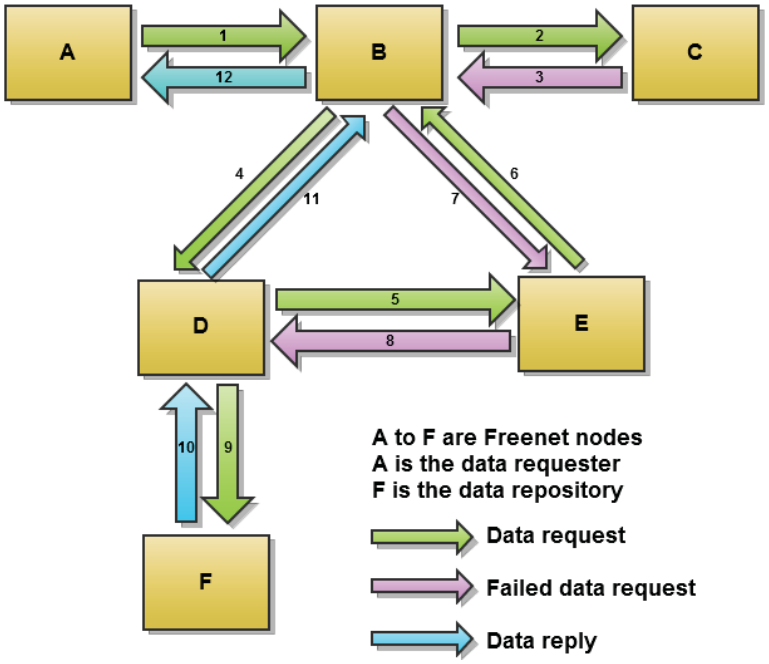


*Figure 2 – routing data in Freenet*

Figure 2 shows how data may be routed inside Freenet. Steps two and three show a data request that meets a dead end and gets routed back from whence it came. Steps four to eight show a routing loop, where the request is re-routed. Steps 10 to 12 show the requested data was located and distributed back to the requester.

In February 2010 Freenet had around 4500-7000 users connected to it at any one time ("Network Status and Network Statistics", 2011). This number has increased since then, but current figures are not available.

The most popular peer-to-peer file sharing application used on Freenet is Frost. This program is similar to a Usenet news reader in that there is a number of user created topics (or "boards") that users post messages to, either requesting content or supplying links to content inside Freenet.

## METHODOLOGY

To discover which Darknets are currently popular, simple Google searches were initiated on a newly formatted PC running Windows 7. The searches used a number of generic keywords that could be used by a person searching for Darknets, including "Darknet", "p2p" and "anonymous file sharing". Links were followed and a list of potential Darknets compiled. From the list, exclusions were applied to networks that did not fit the focus

criteria of this paper. Client software and peer-to-peer file sharing programs for each Darknet were then downloaded from official sites and installed.

Connectivity to each Darknet was established at approximately 15:00 each Sunday in September, 2011. Searches were conducted on each Darknet for predetermined file extensions to acquire file counts and content. Results were categorised manually based on the search result filenames and averaged over the four searches. Due to the differing natures of peer-to-peer file sharing applications, the search criteria used in each application varied.

It is important to note that at no time were any files ever downloaded, viewed or previewed. Due to the nature of the peer-to-peer file sharing applications, the only information that was exposed were file names and sizes, and only content titles and counts were gathered for analysis. As an extra precaution the file sharing applications were configured to download to a read-only file system, thereby negating the risk of accidently initiating a file transfer.

## RESULTS

### I2P

*Table 4 – eDonkey content via the iMule client*

| Claimed file content | File Extension | | | | | | Number of files |
|---|---|---|---|---|---|---|---|
| | **AVI** | **MKV** | **WMV** | **MPEG** | **MPG** | **MP4** | |
| Movies | 426 | 214 | 4 | 2 | 3 | 11 | 660 |
| Child pornography videos | 56 | 96 | 46 | 9 | 198 | 8 | 413 |
| Unknown | 3 | 4 | 219 | 31 | 81 | 38 | 376 |
| TV shows | 19 | 61 | 0 | 1 | 30 | 14 | 125 |
| Pornography videos | 15 | 6 | 71 | 9 | 6 | 0 | 107 |
| Music videos | 0 | 0 | 9 | 14 | 9 | 9 | 41 |
| | **MP3** | **FLAC** | **AAC** | **OGG** | **MP4** | | |
| Music | 316 | 57 | 28 | 61 | 36 | | 498 |
| | **ISO** | **EXE** | | | | | |
| Unknown | 8 | 73 | | | | | 81 |
| Operating systems | 26 | 0 | | | | | 26 |
| Games | 17 | 0 | | | | | 17 |
| Applications | 9 | 0 | | | | | 9 |
| Music | 5 | 0 | | | | | 5 |
| Movies | 3 | 0 | | | | | 3 |
| | **JPG** | **GIF** | **PNG** | **BMP** | | | |
| Images | 379 | 12 | 1 | 9 | | | 401 |
| | **DOC** | **DOCX** | **XLS** | **TXT** | **RTF** | | |
| Documents | 23 | 0 | 0 | 142 | 5 | | 170 |
| | **ZIP** | **RAR** | **ACE** | | | | |
| Archives | 128 | 269 | 20 | | | | 417 |

An average of 380 unique users was seen, sharing an average of 180,000 files.

*Table 5 - Gnutella content via the I2Phex client*

| Claimed file content | File Extension | | | | | | Number of files |
|---|---|---|---|---|---|---|---|
| | **AVI** | **MKV** | **WMV** | **MPEG** | **MPG** | **MP4** | |
| Pornography videos | 80 | 3 | 7 | 2 | 17 | 19 | 128 |
| TV shows | 60 | 0 | 0 | 0 | 0 | 0 | 60 |
| Movies | 45 | 0 | 0 | 0 | 0 | 0 | 45 |
| Music videos | 4 | 0 | 0 | 0 | 0 | 2 | 6 |
| Unknown | 2 | 0 | 0 | 0 | 0 | 1 | 3 |
| Child pornography videos | 1 | 0 | 0 | 0 | 1 | 0 | 2 |
| | **MP3** | **FLAC** | **AAC** | **OGG** | **MP4** | | |
| Music | 1 | 18 | 0 | 0 | 0 | | 19 |
| | **ISO** | **EXE** | | | | | |
| Applications | 0 | 0 | | | | | 0 |
| Operating systems | 0 | 0 | | | | | 0 |
| Games | 0 | 0 | | | | | 0 |
| Music | 0 | 0 | | | | | 0 |
| Movies | 0 | 0 | | | | | 0 |
| Unknown | 0 | 0 | | | | | 0 |
| | **JPG** | **GIF** | **PNG** | **BMP** | | | |
| Images | 4 | 0 | 2 | 0 | | | 6 |
| | **DOC** | **DOCX** | **XLS** | **TXT** | **RTF** | | |
| Documents | 0 | 0 | 0 | 2 | 0 | | 2 |
| | **ZIP** | **RAR** | **ACE** | | | | |
| Archives | 4 | 1 | 0 | | | | 5 |

An average of two unique users was seen, sharing an average of 277 files.

*Table 6 - BitTorrent content via the tracker2.postman.i2p I2P website*

| Claimed file content | Number of files |
|---|---|
| Movies | 667 |
| Music | 518 |
| TV shows | 400 |
| Books | 299 |
| Documentaries | 275 |
| Pornography | 203 |
| Leaked documents | 107 |
| Applications | 96 |
| Games | 66 |
| Audio books | 61 |
| Misc | 33 |
| Music videos | 17 |
| Pictures | 6 |

An average of 6900 unique users was seen, sharing an average of 2748 files.

**Freenet**

*Table 7 - Freenet content via the Frost client*

| Claimed board content | Thread count |
|---|---|
| Child pornography | 1433 |
| Miscellaneous | 449 |
| Unknown | 220 |
| Pornography | 45 |
| Anime | 34 |
| Music | 20 |
| Software | 4 |
| eBooks | 3 |

*An average of 430 unique users was seen across 2208 posts.*

## DISCUSSION OF RESULTS

**Ease of Connectivity**

I2P was one of the first Darknets to appear in the initial searches. Documentation for connection to the network was sufficient, with additional details provided post-installation via the I2P Router Console webpage. It took just over an hour between discovering I2P and having the iMule peer-to-peer file sharing application running. The most popular BitTorrent tracker was also documented in the I2P Router Console webpage, and so required just a few minutes to start searching for content. The I2Phex client proved more difficult to get connected. Downloading the client from the only known, trusted source took an hour, with a subsequent two hours spent getting it to connect to the Gnutella network. Its stability was poor, with frequent lockups that required restarting the application.

The Freenet Darknet was also a popular search result. The official webpage is very user friendly and it took about 20 minutes to download, install and connect to Freenet. Unlike I2P, the Freenet documentation is not detailed, so discovering and downloading the Frost peer-to-peer file sharing application took about an hour. Frost is unlike other peer-to-peer file sharing applications and so, after some more searching of forums, familiarity was gained in 30 minutes.

**Types and quantities of content discovered on the I2P eDonkey and Gnutella networks**

The quantity and variety of files available across the eDonkey and Gnutella networks appeared to be substantial (Table 4 and Table 5). The eDonkey network had a lot of content when compared to the Gnutella network, which is not surprising given the connectivity issues experienced with I2Phex. Based solely on the titles and sizes of files found on the network, the most popular content could be classified as:

- Movies
- Music
- Archives
- Child pornography videos
- Images

Given the popularity of copyrighted movies and music on Internet peer-to-peer file sharing sites, it is interesting to see that similar types of content are also popular on I2P, given the extra steps required to access it. A very confronting result of the content search was the large quantity of child pornography that was found on the I2P eDonkey network. Most videos were easy to classify due to obvious wording in the content title, but child pornography specific keywords were seen in many instances that aided in classification (Vehovar, Žiberna, Kovacic, Mrvar, & Douša, 2009).

**Types and quantities of content discovered on the I2P BitTorrent network**

Although the quantity of files offered via the primary I2P BitTorrent tracker are not as numerous as those offered via the eDonkey network, there was still a substantial amount of content available (Table 6). Based solely on the titles and sizes of files found on the network, the most popular content could be classified as:

- Movies
- Music
- TV shows
- Books
- Documentaries

The type of content available has many similarities to the content offered via Internet BitTorrent trackers. Although a detailed review of the files offered was not conducted, spot checks of file names and sizes indicated that current commercial movies, music and TV shows were the most popular files on offer.

**Types and quantities of content discovered on the Freenet Frost network**

Freenet's Frost peer-to-peer file sharing application does not offer a simple interface to determine filenames on offer, so instead topics of the Frost boards were used. The most popular board topics claimed they were focused on content that contained:

- Child pornography
- Miscellaneous
- Unknown
- Pornography
- Anime (Japanese cartoons)

By far the most popular topics of boards on Frost are those that are dedicated to the provision of child pornography (Table 7). Although a correlation between thread count and file count was not investigated, a brief survey of threads indicated that a great deal of content was on offer. As with the eDonkey network on I2P, it seems that the cover of anonymity is what draws people to offer content that would come with severe gaol terms should they be caught.

## LIMITATIONS

This study was limited in its scope to find Darknets that were easy to discover for an average Internet user, and offered anonymous peer-to-peer file sharing. In both the networks that were investigated, the assumption that filenames accurately reflected content was made. It is quite possible that the names of files offered greatly differed from the contents of the file, but without downloading a statistically significant amount of content, this assumption cannot be proven.

## CONCLUSION

From the results of this investigation, it appears that popular media sites are correct in stating that there is a large quantity of illegal content easily available on Darknets. The popularity of child pornography is particularly disturbing, and given the very nature of Darknets, it appears that the removal of content and prosecution of those offering such content would be very difficult.

It should be noted that the Darknets themselves do not offer content for others to download, nor do the creators of the peer-to-peer file sharing applications – that decision is down to the individuals participating on the networks. Darknets should not be seen as the source of content, but rather the conduit along which it travels.

Darknets are easy to connect to, and as they become more popular due to the barriers to entry shrinking, those that desire anonymity will be well served in the future. As well as those wishing to share copyrighted content while avoiding recent laws introduced to prohibit peer-to-peer file sharing (Anderson, 2011), Darknets have a political and human rights information distribution contribution to be made (ioerror, 2011).

The Australian High Tech Crime Centre identified that "Darknets…could potentially be abused by cybercriminals to distribute propaganda, images of child abuse, or copyrighted digital files in a secure manner to avoid the scrutiny of law enforcement agencies." ("Acquiring high tech crime tools", 2006). Judging by the results documented in this paper, this has certainly proven to be the case.

## REFERENCES

Anderson, N. [2011]. Guilty until proven innocent: New Zealand passes P2P bill. Retrieved September, 2011, from the Ars Technica website: http://arstechnica.com/tech-policy/news/2011/04/guilty-until-proven-innocent-new-zealand-rushes-ahead-with-p2p-bill.ars

Arma. [2010]. BitTorrent Over TOR Isn't A Good Idea. Retrieved September, 2011, from the TOR Project website: https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea

Acquiring high tech crime tools. [2006]. Retrieved September, 2011, from the Australian Institute of Criminology website: http://www.aic.gov.au/documents/A/B/C/%7BABCFCBC4-541A-4ED8-822E-3A0C3B082644%7Dhtcb013.pdf

Biddle, P., England, P., Peinado, M., Willman, B. [2002]. The Darknet and the Future of Content Distribution. Retrieved September, 2011, from the Stanford University website: http://crypto.stanford.edu/DRM2002/darknet5.doc

Bricklin, D. [2000]. Friend-to-Friend Networks. Retrieved September, 2011, from the Dan Bricklin website: http://www.bricklin.com/f2f.htm

Network Status and Network Statistics. [2011]. Retrieved September, 2011, from the Freenet Project website: https://freenetproject.org/news.html

What is Freenet?. [n.d.]. Retrieved September, 2011, from the Freenet Project website: https://freenetproject.org/whatis.html

Gnatek, T. [2005]. Darknets: Virtual Parties with a Select Group of Invitees. Retrieved September, 2011, from the New York Times website: http://www.nytimes.com/2005/10/05/technology/techspecial/05gnatek.html?scp=2&sq=darknet&st=cse

ioerror. [2011]. Recent events in Egypt. Retrieved September, 2011, from the TOR Project website: https://blog.torproject.org/blog/recent-events-egypt

Kravets, D. [2011]. Biggest BitTorrent Downloading Case in U.S. History Targets 23,000 Defendants. Retrieved September, 2011, from the Wired website: http://www.wired.com/threatlevel/2011/05/biggest-bittorrent-case

Desktop Operating System Market Share. [2011]. Retrieved September, 2011, from the Net Applications website: http://www.netmarketshare.com/report.aspx?qprid=8&qptimeframe=M&qpsp=152&qpcustomd=0

One Month View for Total Routers. [2011]. Retrieved September, 2011, from the stat.i2p.to website: http://stats.i2p.to/cgi-bin/total_routers_month.cgi

Puig-Centelles, A., Ripolles, O., & Chover, M. [2007]. P2P Traffic Measurements on the Emule System. Retrieved September, 2011, from the CiteSeer website: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.9594&rep=rep1&type=pdf

Riedel, S. [2006]. A Brief History of Filesharing: From Napster to Legal Music Downloads. Retrieved September, 2011, from the Associated Content website: http://www.associatedcontent.com/article/20644/a_brief_history_of_filesharing_from.html?cat=15

Sahi, S. [2010]. Census of Files Available via BitTorrent. Retrieved September, 2011, from the Freedom to Tinker website: https://freedom-to-tinker.com/blog/felten/census-files-available-bittorrent

Sandvine Global Internet Report Spring 2011. [2011]. Retrieved September, 2011, from the Wired website: http://www.wired.com/images_blogs/epicenter/2011/05/SandvineGlobalInternetSpringReport2011.pdf

Vehovar, V., Žiberna, A., Kovacic, M., Mrvar, A., & Douša, M. [2009]. An Empirical Investigation of Paedophile Keywords in eDonkey P2P Network. Retrieved September, 2011, from the Measurement and Analysis of P2P Activity Against Paedophile Content website: http://antipaedo.lip6.fr/T24/TR/keywords-vv.pdf

Williams, C. [2011]. Hurt Locker producers launch record-breaking copyright lawsuit. Retrieved September, 2011, from The Telegraph website: http://www.telegraph.co.uk/technology/8533042/Hurt-Locker-producers-launch-record-breaking-copyright-lawsuit.html