Usenet Abuse Primer for Security and Law Enforcement Personnel

By: Mark Lachniet (mark@lachniet.com) and
Michael Harrington (linuxchimp@gmail.com)

Version 1.0 - Monday, January 08, 2007

1.0 Executive Summary

At the start of 2006, the use of Usenet as a means to anonymously transmit and receive illicit material such as pirated software, music, video and pornography is widespread. These same channels may be used for criminal purposes, such as the distribution of child pornography, malware and viruses, or possibly even steganographic[1] messages within covert channels. As we are not law enforcement officers who have specifically investigated these, we will not speculate as to how widespread the use of USENET is for these more villainous purposes. Rather, as a private-sector security consultant, we had thought to write up a high-level summary of how USENET works, and how it is being abused, for our peers in the security and law enforcement fields.

This document is not intended to give a thorough and detailed analysis of the topic, but rather to function as an introductory text on the topic. Specific examples, including URL's, software packages, and actual USENET content will be given. If you have questions, comments, or suggestions for improvements, please do not hesitate to contact the authors directly – we welcome your comments. This document was used as the basis for a couple of presentation at the 2006 International HTCIA conference that we put on.

Usenet is a particular problem for law enforcement because it is very difficult to investigate. First, because it is a store-and-forward technology, it is not always easy to identify the source of content on Usenet. At least with Peer-to-Peer investigations, it is usually possible to get the IP address of the naughty person using firewall logs or a protocol analyzer. Not so with Usenet – all connections are between a client and a Usenet server to upload or download content, and these servers then propagate the message amongst themselves. This difficulty is compounded by the fact that a large number of Usenet servers *do not keep any logs* of activity. Thus, it is not as simple as seizing equipment or getting a court order to turn over logs – there usually aren't any. In addition to this lack of logging, it is generally easy to spoof any information that goes into a Usenet posting, including the sender's from address. Further discussion of investigation will be discussed in a later section.

2.0 What is the Usenet?

The Wikipedia entry[2] about Usenet describes it as follows:

> *Usenet is a distributed Internet discussion system that evolved from a general purpose UUCP network of the same name. It was conceived by Duke University graduate students Tom Truscott and Jim Ellis in 1979. Users, sometimes called Usenetters, read and post email-like messages (called "articles") to a number of distributed newsgroups, categories that resemble bulletin board systems in most*

respects. The medium is sustained among a large number of servers, which store and forward messages to one another. Usenet is of significant cultural importance in the networked world, having given rise to, or popularized, many widely recognized concepts and terms such as "FAQ" and "spam".

…

Usenet is one of the oldest computer network communications systems still in widespread use. It was established in 1980 following experiments the previous year, over a decade before the World Wide Web was introduced and the general public was admitted to the Internet. It was originally conceived as a "poor man's ARPANET," employing UUCP to offer mail and file transfers, as well as announcements through the newly developed news software. This system, developed at University of North Carolina at Chapel Hill and Duke University, was called USENET to emphasize its creators' hope that the USENIX organization would take an active role in its operation (Daniel et al, 1980).

Today, almost all Usenet traffic is carried over the Internet. The current format and transmission of Usenet articles is very similar to that of Internet email messages. However, whereas email is usually used for one-to-one communication, Usenet is a one-to-many medium.

The articles that users post to Usenet are organized into topical categories called newsgroups, which are themselves logically organized into hierarchies of subjects. For instance, sci.math and sci.physics are within the sci hierarchy, for science. When a user subscribes to a newsgroup, the news client software keeps track of which articles that user has read.

When a user posts an article, it is initially only available on that user's news server. Each news server, however, talks to one or more other servers (its "newsfeeds") and exchanges articles with them. In this fashion, the article is copied from server to server and (if all goes well) eventually reaches every server in the network. The later peer-to-peer networks operate on a similar principle; but for Usenet it is normally the sender, rather than the receiver, who initiates transfers. Some have noted that this seems a monstrously inefficient protocol in the era of abundant high-speed network access. Usenet was designed for a time when networks were much slower, and not always available. Many sites on the original Usenet network would connect only once or twice a day to batch-transfer messages in and out.

Today, Usenet has diminished in importance with respect to mailing lists and weblogs. The difference from mailing lists, though, is that Usenet requires no personal registration with the group concerned (subscription is necessary only to keep track of which articles one has already read, and that information need not be stored on a remote server), that archives are always available, and that reading the messages requires no mail client, but a news client (included in most modern e-mail clients).

In my opinion, the author of this Wikipedia entry underestimates the importance of the Usenet for certain purposes, but the general description is accurate. Usenet *has* diminished in importance for the purpose of distributing messages – listserves are more convenient – but this is not why Usenet is currently popular, naughty content is.

Today, the size of Usenet is massive with gigabytes (perhaps terabytes?) of data transferred daily, with a large part of this content being binary content such as images or software. According to Wired Magazine[3] "more than 60 GB of complete DVD rips are now being posted each day."

3.0 How does Usenet work?

The following is my layman's interpretation of how Usenet works. If you want a technical description, please refer to RFC 0977[4] or RFC 1036[5]. The Usenet works as a store-and-forward system, and is very similar to e-mail. The key difference between e-mail and Usenet newsgroups is that with e-mail, a message is sent only to a specific recipient, while in Usenet, a message is sent to any peer that subscribes to the newsgroup in which a message was posted. This message can then be viewed by any client who has access to a participating Usenet server. Messages are stored for a while, but eventually cycled out of storage based on the retention policies of the server. Some servers store content for only a few days, while others store it for a few months or more – it all depends on the capabilities of the server.

3.1 An example Usenet Message

For example, the following is an example of a message posted to the Usenet:

```
Path:
border1.nntp.dca.giganews.com!nntp.giganews.com!feed2.newsreader.com!newsreader.com!npee
r.de.kpn-
eurorings.net!news.tele.dk!news.tele.dk!small.news.tele.dk!news.astraweb.com!newsrouter-
eu.astraweb.com!eweka!hq-
usenetpeers.eweka.nl!81.171.88.219.MISMATCH!newsreader30.eweka.nl!not-for-mail
From: "Apollo" <obscured@email.whatever>
Subject: were can i download the series?
Newsgroups: alt.binaries.battlestar-galactica
Date: Sun, 1 Jan 2006 16:47:29 +0100
Lines: 7
Message-ID: <43b7f8e3$0$1030$c807b3c@newsreader30.eweka.nl>
Organization: Eweka Internet Services
NNTP-Posting-Host: Eweka Internet Services
X-Trace: Posted by Eweka Internet Services, http://www.eweka.nl
X-Complaints-To: abuse@n-o-s-p-a-m.eweka.nl
Xref: number1.nntp.dca.giganews.com alt.binaries.battlestar-galactica:824361
```

In this example, you can see some similarities and differences from e-mail. For example, we have a **From** heading and a **Subject** as well as a **Date** and other similar looking headers. However, some key differences exist. For example, rather than a **To** field, we have a **Newsgroups** field. Some of the other fields may be optional.

A few notes about this. First, you can't really trust the **From** field to be an actual person – it is easy to spoof. Only a complete idiot would post illegal content with their real e-mail address. One thing you <u>can</u> probably trust is the **Message-ID** field. This field shows you what news server originally received the message. For the Usenet to work, this field has to be unique. Indeed, this is how messages are propagated between Usenet servers without creating redundant copies of the message.

3.2 Usenet Message Propagation

In layman's terms, Usenet propagation works something like the following:

1. A client with access to a Usenet server posts a message. This communication is between the client and the server directly, and usually takes place over TCP port 119. Let us suppose that the client had posted their message to alt.binaries.battlestar-galactica.

2. The server receives the message and assigns it a unique **Message-ID** field.

3. The server communicates with its Usenet peers (other Usenet servers). For each message that it has received locally, it checks with its peers to see if any of them subscribe to the alt.binaries.battlestar-galactica groups.

4. If the peer servers do subscribe, they communicate between themselves to see if they already have a copy of the message. This is based on the **Message-ID** field. If they subscribe to the newsgroup but do not have the specific message, it is transmitted to the peer. If the server already has the message, it ignores that message.

5. The message is propagated through the peer networks

6. A second client (the consumer) connects to their Usenet server (most likely a server in a completely different part of the world). The pull up a list of messages for the newsgroups for which they are subscribed, and the message in question is listed.

7. If the consumer client wishes to download the message, they do so, and the content is transferred to their computer.

3.3 Usenet binary content

The example I gave was of a text message, but it is entirely possible to send binary content that has been encoded into text, just like e-mail. Some methods to encode binary content include "BASE64, BinHex, UUencode, Quoted Printable" [6] and the Usenet-specific yEnc format. Indeed, this is the most common way that the Usenet is used for illegal purposes. A number of Usenet clients such as NewsReactor[7] and Forte Agent[8] have been developed that are specifically designed to facilitate the easy downloading of binary content.

In some cases, a binary file may fit within the limit of a single Usenet message. For example, small images and smaller files may be entirely self-contained. However, in the case of large files such as CD Images, video content, etc. the limit 10,000 lines of text is often exceeded. To accommodate this limitation, multi-part archive files are often used.

It is also interesting to note that each RAR file should have a copy of the information about which filenames were in the archive. For example, if you could only find one part of a 50 part multi-part RAR file, you still probably be able to identify what would have been in the archive by opening it and viewing the contents.

3.3.1 Multi-part Archive Files

The most common way to break a large file into several smaller chunks is to use a program such as WinRAR[9] to break the file into several smaller parts. See the demonstration section for an example of how these files work. In general, you will see a number of files that are denoted with part01.rar, part02.rar, etc. In some cases you may simply see numeric extensions. When you click on one of them, it will automatically load the other ones to get the needed content. When performing an investigation of a workstation, you need to be on the lookout for archive files, especially multi-part archive files, because the keywords and file headers that you are looking for might be compressed within an archive, or even split between archive files! Thus, it behooves a forensic investigator to identify all archive files and attempt to recreate the resultant file as part of the analysis.

An investigator may want to investigate the forensic validity of multi-part archive files. This article is intended to detail how Usenet (as a network protocol) is used, rather than the content that it delivers. It would be worthwhile to validate, for example, that a file that has been broken and then recreated has the same hash as the original. It should, but I would certainly try to prove that before you try to make your case.

3.3.2 Parity Files

Multi-part archive files are all well and good, but the Usenet (let alone the Internet!) is not a reliable medium for transmitting large amounts of data. In particular, with the

Usenet, it is common for some parts of a large archive file to be lost (generating a “fill” request for the poster to resend the missing parts). To accommodate this problem, enterprising software engineers came up with a way to create parity files for multi-part archives. This parity system is very similar to a RAID-5 disk array in the hardware world. The following description of how parity files works is from Wikipedia[10]:

> *Parchive (or parity volume set archive) is an error-correction system that can be applied to a collection of files to allow recovery when one or more of the files is lost. It was designed to be used on Usenet for transmission of large files such as movies. It is implemented using Reed-Solomon error correction.*
>
> *Files posted to Usenet newsgroups are broken into small parts and posted as text messages. Transmissions over Usenet are not guaranteed, so the larger the file posted, the more likely it is that some parts will become lost or corrupted along the way.*
>
> *There are incompatible versions 1 and 2 of the file format specification.*
>
> *For version 1, given files f1, f2, ..., fn, the Parchive consists of an index file (f.par) and a number of "parity volumes" (f.p01, f.p02, etc.) Given all of the original files except for one (for example, f2) it is possible to create the missing f2 given all of the other original files and any one of the parity volumes. Alternatively, it is possible to recreate two missing files from any two of the parity volumes and so forth.*
>
> *The index files (*.par in version 1 and *.par2 in version 2) are not needed to recover any data. The indexes consist solely of hashes to quickly identify the target files, and their content is duplicated in every parity volume. Index files are used to quickly check for errors to see if additional parity files are required. They were most useful in version 1 where the parity volumes were much larger than the short index.*
>
> *While Version 1 provided a great improvement in the way files were transmitted over Usenet, it was lacking in some respects, principally that if even 1% of a file was missing, Version 1 would require a whole recovery file to repair that 1% of a file. If 100 files were each missing only 1%, the missing data would total 1 file but Version 1 required 100 files to repair! Needless to say, this was tremendously inefficient.*
>
> *To improve on this situation, a second version of Parchive was released which in the worst case would work about as well as Version 1 but in the best case, would provide a great improvement. Version 2 allows files to be divided into blocks and then allows recovery files to be as small as one of these blocks. Thus, if a fraction of a file is missing, you'll only need to download a few extra recovery blocks rather than entire (full-sized) recovery files as was necessary with Version 1.*

The long and short of it is that with PAR and PAR2 software, it is possible to recreate complete archives, even if some portions of an archive are missing. If you understand RAID-5, you understand parity files. Here again, it behooves a forensic investigator to identify all parity files, as these may be necessary to recreate and identify suspicious content on a system. For an example of how this works, please view the demonstration section of this document.

4.0 Finding Usenet Content

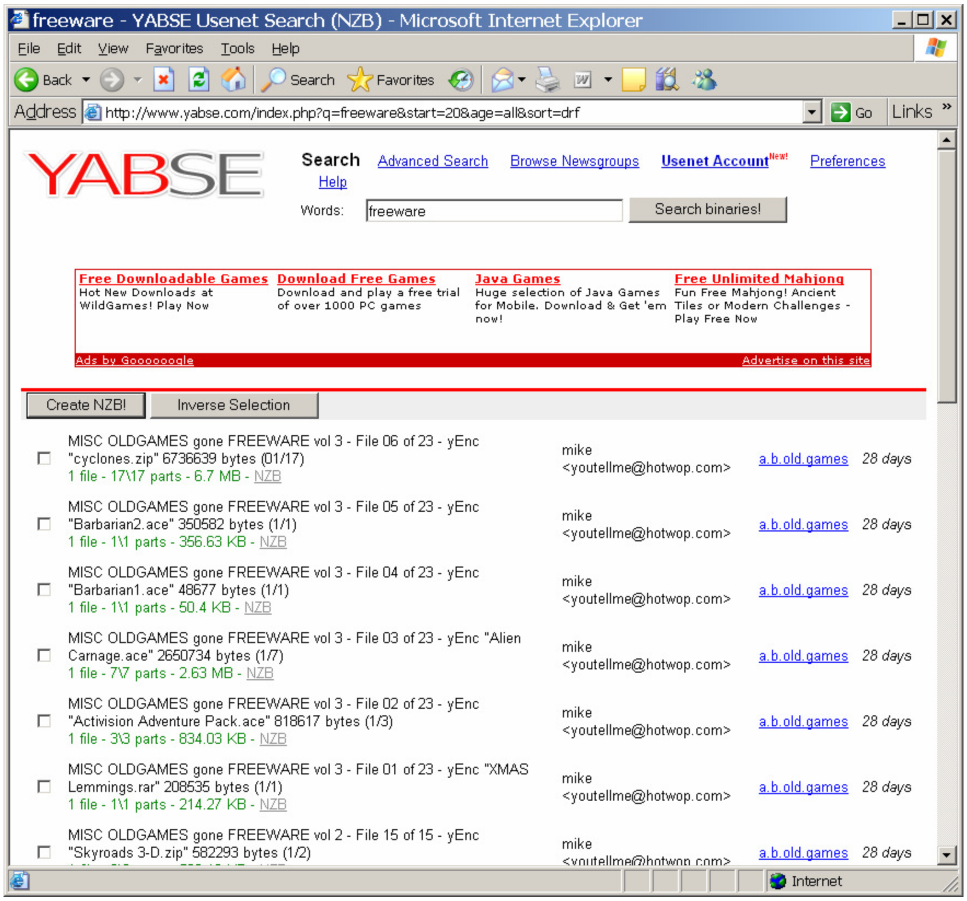
The Usenet is big, really big. It would take a very long time to poke through individual newsgroups looking for what you want. However, there are a number of search engines (and ever Usenet to binary download services) that you can use to make it easier. Let's look at a couple of ways to search the Usenet.

4.1 Looking for Text on the Usenet

If you were looking for information about a person that *wasn't* binary content, a good way to do this would be to search at http://groups.google.com. This type of search should be included in any "ego surfing" and background check activities, as it can turn up some juicy tidbits. While the Yahoo site has an extensive archive of historical data, there are several other search engines such as yabse.com[11] that track more current information. You can also find binary content this way, but it's not the most convenient.

4.2 Looking for binaries on the Usenet

There are also search engines for finding binaries on the Internet. A yabse search will turn up binaries. For example, if you were looking for Freeware, you could do a search such as: http://www.yabse.com/index.php?q=freeware which might turn up results such as the following:



Address: http://www.yabse.com/index.php?q=freeware&start=20&age=all&sort=drf

Words: freeware

□	MISC OLDGAMES gone FREEWARE vol 3 - File 06 of 23 - yEnc "cyclones.zip" 6736639 bytes (01/17) 1 file - 17\17 parts - 6.7 MB - NZB	mike <youtellme@hotwop.com>	a.b.old.games	28 days
□	MISC OLDGAMES gone FREEWARE vol 3 - File 05 of 23 - yEnc "Barbarian2.ace" 350582 bytes (1/1) 1 file - 1\1 parts - 356.63 KB - NZB	mike <youtellme@hotwop.com>	a.b.old.games	28 days
□	MISC OLDGAMES gone FREEWARE vol 3 - File 04 of 23 - yEnc "Barbarian1.ace" 48677 bytes (1/1) 1 file - 1\1 parts - 50.4 KB - NZB	mike <youtellme@hotwop.com>	a.b.old.games	28 days
□	MISC OLDGAMES gone FREEWARE vol 3 - File 03 of 23 - yEnc "Alien Carnage.ace" 2650734 bytes (1/7) 1 file - 7\7 parts - 2.63 MB - NZB	mike <youtellme@hotwop.com>	a.b.old.games	28 days
□	MISC OLDGAMES gone FREEWARE vol 3 - File 02 of 23 - yEnc "Activision Adventure Pack.ace" 818617 bytes (1/3) 1 file - 3\3 parts - 834.03 KB - NZB	mike <youtellme@hotwop.com>	a.b.old.games	28 days
□	MISC OLDGAMES gone FREEWARE vol 3 - File 01 of 23 - yEnc "XMAS Lemmings.rar" 208535 bytes (1/1) 1 file - 1\1 parts - 214.27 KB - NZB	mike <youtellme@hotwop.com>	a.b.old.games	28 days
□	MISC OLDGAMES gone FREEWARE vol 2 - File 15 of 15 - yEnc "Skyroads 3-D.zip" 582293 bytes (1/2)	mike <youtellme@hotwop.com>	a.b.old.games	28 days

From this, we can see the posting subject, the sender (probably spoofed) the newsgroup it was sent to, how many parts it has, and how long ago it was posted.

4.3 NZB Files

With yabse, and other programs, you have the option to create a NZB file. According to Wikipedia[12] NZB file is "a file format created by the owners of the internet site newzbin.com. The intention with NZB files is to create small header files for Usenet so that the user does not have to download the headers of an entire newsgroup in order to download the potentially few files that the user might want to download. This file simply makes the binary file easier and faster to download. In the example of the top listing "cyclones.zip" we can see that it is pretty large, and comes in 17 parts. If you click on the NZB link, it will create a file that newsreaders can use to immediately download the content. An example of a NZB file is as follows:

```
<?xml version="1.0" encoding="iso-8859-1" ?>
<!DOCTYPE nzb PUBLIC "-//newzBin//DTD NZB 1.0//EN" "http://www.newzbin.com/DTD/nzb/nzb-1.0.dtd">
<nzb xmlns="http://www.newzbin.com/DTD/2003/nzb">
<file poster="mike &lt;youtellme@hotwop.com&gt;" date="1135277730" subject="MISC OLDGAMES gone
FREEWARE vol 3 - File 06 of 23 - yEnc &quot;cyclones.zip&quot; 6736639 bytes (01/17)">
<groups>
<group>alt.binaries.old.games</group>
</groups>
```

```
<segments>
<segment bytes="416782" number="1">Xns9734CAA2DE2A8orisitdunnocom@194.152.65.251</segment>
<segment bytes="417226" number="2">Xns9734CAAE875D0orisitdunnocom@194.152.65.251</segment>
<segment bytes="416719" number="3">Xns9734CABA2DB36orisitdunnocom@194.152.65.251</segment>
<segment bytes="417547" number="4">Xns9734CAC6DA4B4orisitdunnocom@194.152.65.251</segment>
<segment bytes="418353" number="5">Xns9734CAEA7D81Aorisitdunnocom@194.152.65.251</segment>
<segment bytes="416432" number="6">Xns9734CAF5D96B0orisitdunnocom@194.152.65.251</segment>
<segment bytes="416716" number="7">Xns9734CB012548Corisitdunnocom@194.152.65.251</segment>
<segment bytes="416792" number="8">Xns9734CB10BF7E6orisitdunnocom@194.152.65.251</segment>
<segment bytes="416843" number="9">Xns9734CB1C23984orisitdunnocom@194.152.65.251</segment>
<segment bytes="416888" number="10">Xns9734CB2782A96orisitdunnocom@194.152.65.251</segment>
<segment bytes="416787" number="11">Xns9734CB3537B0Forisitdunnocom@194.152.65.251</segment>
<segment bytes="416984" number="12">Xns9734CB429BB9Aorisitdunnocom@194.152.65.251</segment>
<segment bytes="416935" number="13">Xns9734CB4DF5A45orisitdunnocom@194.152.65.251</segment>
<segment bytes="417771" number="14">Xns9734CB593CE68orisitdunnocom@194.152.65.251</segment>
<segment bytes="416982" number="15">Xns9734CB660E47Eorisitdunnocom@194.152.65.251</segment>
<segment bytes="416878" number="16">Xns9734CB714E266orisitdunnocom@194.152.65.251</segment>
<segment bytes="350296" number="17">Xns9734CB7C74014orisitdunnocom@194.152.65.251</segment>
</segments>
</file>
</nzb>
```

Here we can see all of the messages (noted by the unique **Message-ID** field and newsgroup) that are necessary to get the complete binary file.

You may also find .NFO files, which are simply text documents describing the content (such as the encoding format, the number of parts, etc). These should also be included in any forensic searches.

5.0 Usenet Anonymity

As mentioned previously, the headers of Usenet messages (other than the unique Message-ID) are pretty easy to forge, making it somewhat difficult to correlate a posting to a person. Indeed, there is a niche market that caters to Usenet downloaders who wish to be anonymous. Some Usenet service providers such as EasyNews intentionally do not log any activity, such that it would be very difficult to subpoena their records. Note their selling points from their web page[13]:

Privacy

- Easynews takes your privacy seriously. We have one of the most aggressive privacy policies in the industry.
- Easynews does not monitor or log downloads.
- No identifying information is placed in your Usenet posts. Your posts are virtually anonymous with all X-Headers removed.

At this time, I would like to point out that having an anonymous Usenet service is not, in and of itself, necessarily bad. There could be any number of reasons that a person might want to be anonymous, such as getting medical information on a private condition. There are many other providers who have the same policy, and I do not wish to single out Easynews in particular – they may be an excellent company, and entirely law abiding. I use their policy for demonstrative purposes only.

There are also gateways and proxies that can be used to anonymously transfer content from e-mail (such as listserves) to Usenet, and vice-versa. I have not personally investigated these, but they allegedly to exist, and could further complicate investigative efforts.

6.0 Demonstration

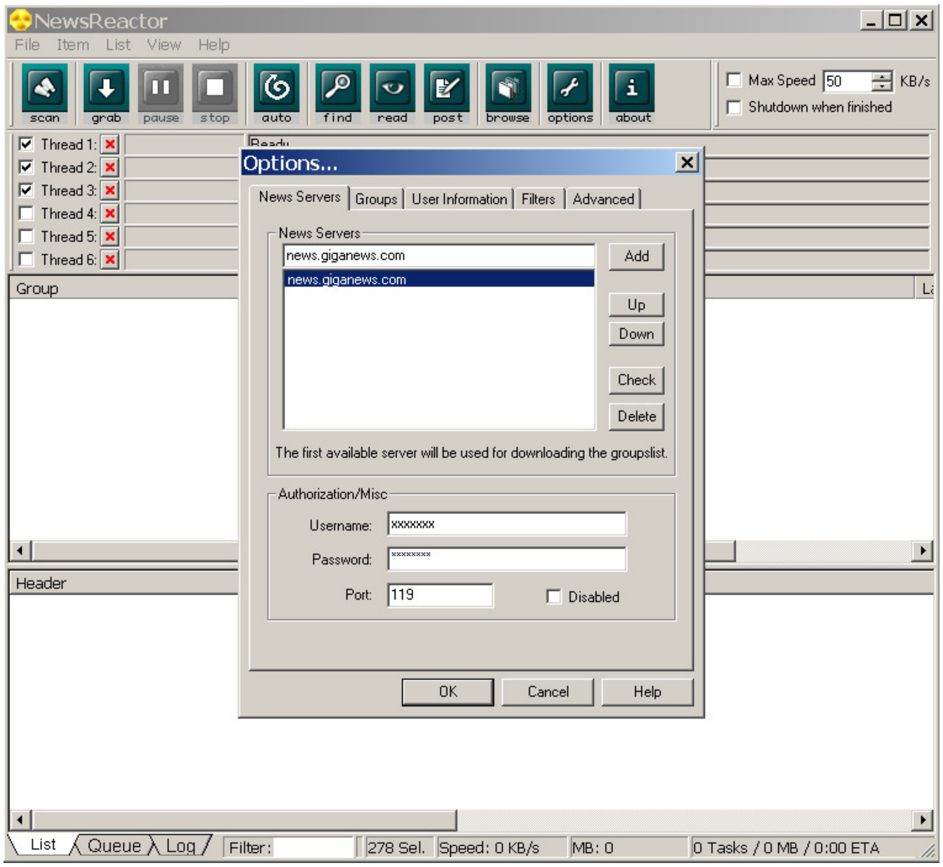
Now that we have a basic overview of how Usenet works, let’s go ahead and obtain some content. For our purposes, we’ll get something that is in the public domain, but obviously all you would need to do is change your searches to get to other binary content. To enhance readability, I will provide screen captures, where appropriate.

6.1 Obtain Usenet Access

The first thing you need to do is obtain access to a Usenet server. In our case, we’ll get a subscription to Giganews. They kindly provide a 3-day demonstration to try it out ☺ but they are also very well regarded as a service. You will then be provided with a username, password, and the IP addresses (or DNS names) of the Usenet servers.

6.2 Obtain a Newsreader

For our example, we’ll use the NewsReactor software. Download the software (please pay the author!) and install it. We’ll then configure NewsReactor to access Giganews. Go to File→options→and Add:



NewsReactor
File Item List View Help
scan grab pause stop auto find read post browse options about
Max Speed 50 KB/s
Shutdown when finished
Thread 1: Thread 2: Thread 3: Thread 4: Thread 5: Thread 6:
Ready
Group
Header
Options...
News Servers | Groups | User Information | Filters | Advanced
Add Up Down Check Delete
OK Cancel Help
List Queue Log Filter:
278 Sel. Speed: 0 KB/s MB: 0 0 Tasks / 0 MB / 0:00 ETA

News Servers

news.giganews.com

news.giganews.com

The first available server will be used for downloading the groupslist.

Authorization/Misc

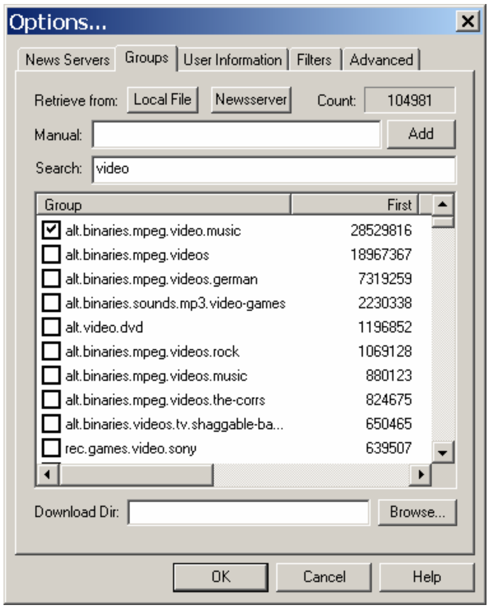
Username: xxxxxxx

Password: ********

Port: 119 □ Disabled

6.3 Finding a Download

Let's try to find a multipart program to download. To do this, we'll go to file→options→Groups and then retrieve the list of groups by clicking on the Newsserver button. I couldn't find any actual shareware or freeware to download on Giganews' groups, so we'll have to go with something as harmless as possible for our demonstration. You can either type in the group you are interested in manually, or do a keyword search of all groups. If you were looking for something specific, such as movies, xxx, etc. you would type it here. In our case, we'll look for music videos and subscribe to alt.binaries.mpeg.video.music. Note that you slide the bar to the right and then click on the header bar "count" to sort by the newsgroups with the most postings:



Retrieve from: Count: 104981

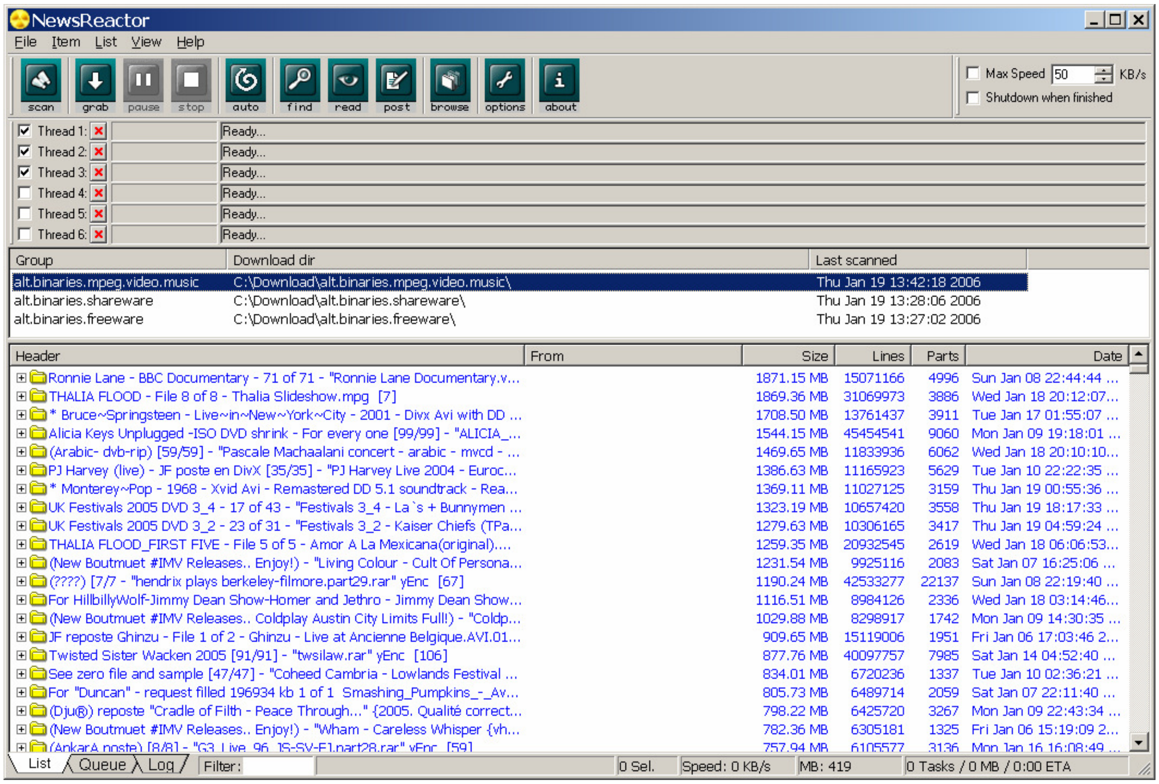
Manual:

Search: video

Group	First
☑ alt.binaries.mpeg.video.music	28529816
□ alt.binaries.mpeg.videos	18967367
□ alt.binaries.mpeg.videos.german	7319259
□ alt.binaries.sounds.mp3.video-games	2230338
□ alt.video.dvd	1196852
□ alt.binaries.mpeg.videos.rock	1069128
□ alt.binaries.mpeg.videos.music	880123
□ alt.binaries.mpeg.videos.the-corrs	824675
□ alt.binaries.videos.tv.shaggable-ba...	650465
□ rec.games.video.sony	639507

Download Dir:

We'll then click OK and then double-click on the newsgroup in the top window pane:



□ Max Speed 50 KB/s

□ Shutdown when finished

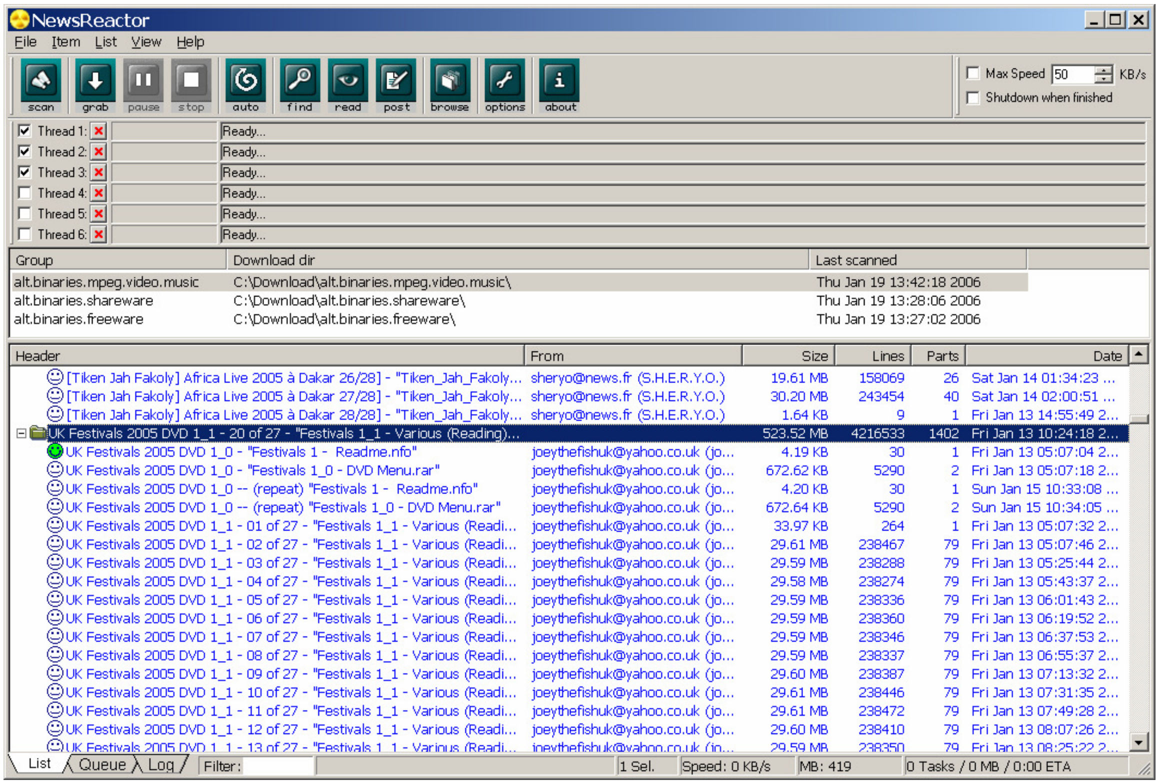
☑ Thread 1: Ready...
☑ Thread 2: Ready...
☑ Thread 3: Ready...
□ Thread 4: Ready...
□ Thread 5: Ready...
□ Thread 6: Ready...

Group	Download dir	Last scanned
alt.binaries.mpeg.video.music	C:\Download\alt.binaries.mpeg.video.music\	Thu Jan 19 13:42:18 2006
alt.binaries.shareware	C:\Download\alt.binaries.shareware\	Thu Jan 19 13:28:06 2006
alt.binaries.freeware	C:\Download\alt.binaries.freeware\	Thu Jan 19 13:27:02 2006

Header	From	Size	Lines	Parts	Date
⊞ Ronnie Lane - BBC Documentary - 71 of 71 - "Ronnie Lane Documentary.v...		1871.15 MB	15071166	4996	Sun Jan 08 22:44:44 ...
⊞ THALIA FLOOD - File 8 of 8 - Thalia Slideshow.mpg [7]		1869.36 MB	31069973	3886	Wed Jan 18 20:12:07...
⊞ * Bruce~Springsteen - Live~in~New~York~City - 2001 - Divx Avi with DD ...		1708.50 MB	13761437	3911	Tue Jan 17 01:55:07 ...
⊞ Alicia Keys Unplugged -ISO DVD shrink - For every one [99/99] - "ALICIA_...		1544.15 MB	45454541	9060	Mon Jan 09 19:18:01 ...
⊞ (Arabic- dvb-rip) [59/59] - "Pascale Machaalani concert - arabic - mvcd - ...		1469.65 MB	11833936	6062	Wed Jan 18 20:10:10...
⊞ PJ Harvey (live) - JF poste en DivX [35/35] - "PJ Harvey Live 2004 - Euroc...		1386.63 MB	11165923	5629	Tue Jan 10 22:22:35 ...
⊞ * Monterey~Pop - 1968 - Xvid Avi - Remastered DD 5.1 soundtrack - Rea...		1369.11 MB	11027125	3159	Thu Jan 19 00:55:36 ...
⊞ UK Festivals 2005 DVD 3_4 - 17 of 43 - "Festivals 3_4 - La`s + Bunnymen ...		1323.19 MB	10657420	3558	Thu Jan 19 18:17:33 ...
⊞ UK Festivals 2005 DVD 3_2 - 23 of 31 - "Festivals 3_2 - Kaiser Chiefs (TPa...		1279.63 MB	10306165	3417	Thu Jan 19 04:59:24 ...
⊞ THALIA FLOOD_FIRST FIVE - File 5 of 5 - Amor A La Mexicana(original)....		1259.35 MB	20932545	2619	Wed Jan 18 06:06:53...
⊞ (New Boutmuet #IMV Releases.. Enjoy!) - "Living Colour - Cult Of Persona...		1231.54 MB	9925116	2083	Sat Jan 07 16:25:06 ...
⊞ (????) [7/7 - "hendrix plays berkeley-filmore.part29.rar" yEnc [67]		1190.24 MB	42533277	22137	Sun Jan 08 22:19:40 ...
⊞ For HillbillyWolf-Jimmy Dean Show-Homer and Jethro - Jimmy Dean Show...		1116.51 MB	8984126	2336	Wed Jan 18 03:14:46...
⊞ (New Boutmuet #IMV Releases.. Coldplay Austin City Limits Full!) - "Coldp...		1029.88 MB	8298917	1742	Mon Jan 09 14:30:35 ...
⊞ JF reposte Ghinzu - File 1 of 2 - Ghinzu - Live at Ancienne Belgique.AVI.01...		909.65 MB	15119006	1951	Fri Jan 06 17:03:46 2...
⊞ Twisted Sister Wacken 2005 [91/91] - "twsilaw.rar" yEnc [106]		877.76 MB	40097757	7985	Sat Jan 14 04:52:40 ...
⊞ See zero file and sample [47/47] - "Coheed Cambria - Lowlands Festival ...		834.01 MB	6720236	1337	Tue Jan 10 02:36:21 ...
⊞ For "Duncan" - request filled 196934 kb 1 of 1 Smashing_Pumpkins_-_Av...		805.73 MB	6489714	2059	Sat Jan 07 22:11:40 ...
⊞ (Dju®) reposte "Cradle of Filth - Peace Through..." {2005. Qualité correct...		798.22 MB	6425720	3267	Mon Jan 09 22:43:34 ...
⊞ (New Boutmuet #IMV Releases.. Enjoy!) - "Wham - Careless Whisper {vh...		782.36 MB	6305181	1325	Fri Jan 06 15:19:09 2...
⊞ (AnkarA noste) [8/8] - "G3 Live 96 JS-SV-F1.part28.rar" yEnc [59]		757.94 MB	6105577	3136	Mon Jan 16 16:08:49 ...

Filter: 0 Sel. Speed: 0 KB/s MB: 419 0 Tasks / 0 MB / 0:00 ETA

Here we can see all of the messages that are posted. Click on the size header to sort by the largest, so you can find the ones that have actual content. You can do a keyword search if you like, and you can click on the + sign to expand out a selection, and see that there are in fact several messages. We'll use what appears to be home footage of a music festival (presumably public domain) from the UK for our example:



☐ Max Speed 50 KB/s
☐ Shutdown when finished

☑ Thread 1:	Ready...
☑ Thread 2:	Ready...
☑ Thread 3:	Ready...
☐ Thread 4:	Ready...
☐ Thread 5:	Ready...
☐ Thread 6:	Ready...

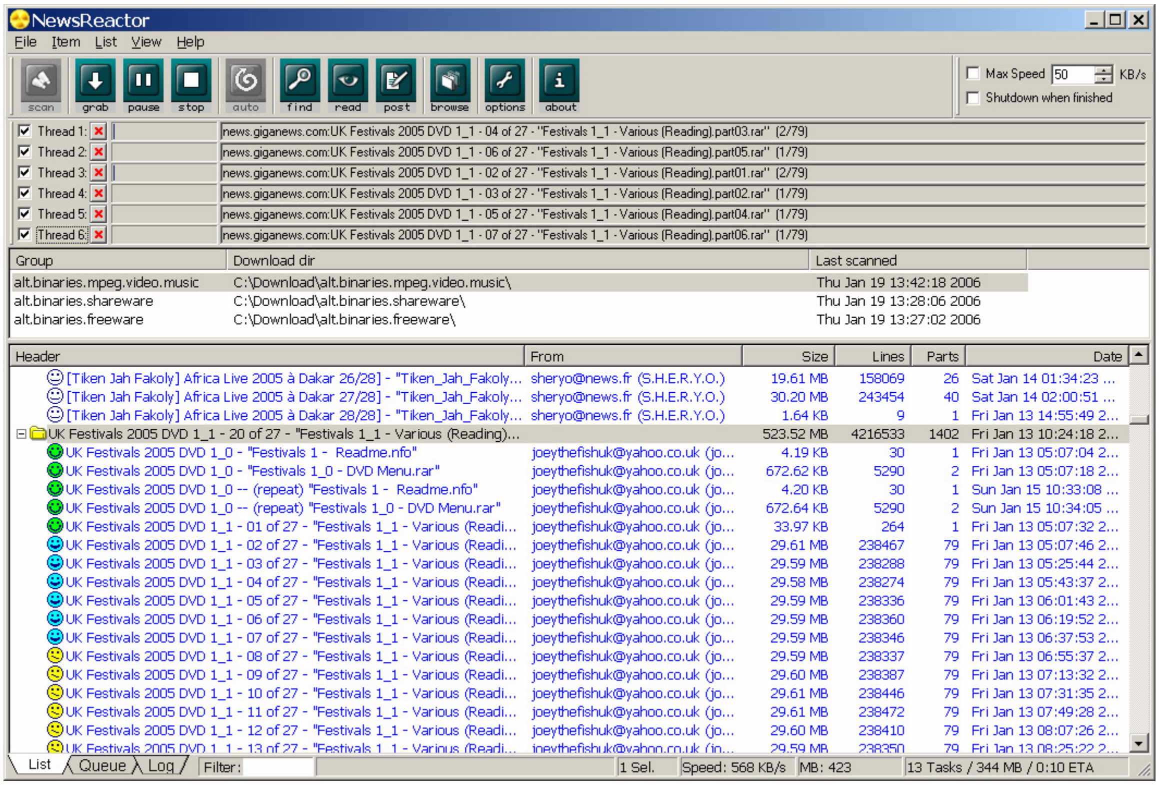
Group	Download dir	Last scanned
alt.binaries.mpeg.video.music	C:\Download\alt.binaries.mpeg.video.music\	Thu Jan 19 13:42:18 2006
alt.binaries.shareware	C:\Download\alt.binaries.shareware\	Thu Jan 19 13:28:06 2006
alt.binaries.freeware	C:\Download\alt.binaries.freeware\	Thu Jan 19 13:27:02 2006

Header	From	Size	Lines	Parts	Date
[Tiken Jah Fakoly] Africa Live 2005 à Dakar 26/28] - "Tiken_Jah_Fakoly...	sheryo@news.fr (S.H.E.R.Y.O.)	19.61 MB	158069	26	Sat Jan 14 01:34:23 ...
[Tiken Jah Fakoly] Africa Live 2005 à Dakar 27/28] - "Tiken_Jah_Fakoly...	sheryo@news.fr (S.H.E.R.Y.O.)	30.20 MB	243454	40	Sat Jan 14 02:00:51 ...
[Tiken Jah Fakoly] Africa Live 2005 à Dakar 28/28] - "Tiken_Jah_Fakoly...	sheryo@news.fr (S.H.E.R.Y.O.)	1.64 KB	9	1	Fri Jan 13 14:55:49 2...
⊟ UK Festivals 2005 DVD 1_1 - 20 of 27 - "Festivals 1_1 - Various (Reading)...		523.52 MB	4216533	1402	Fri Jan 13 10:24:18 2...
UK Festivals 2005 DVD 1_0 - "Festivals 1 - Readme.nfo"	joeythefishuk@yahoo.co.uk (jo...	4.19 KB	30	1	Fri Jan 13 05:07:04 2...
UK Festivals 2005 DVD 1_0 - "Festivals 1_0 - DVD Menu.rar"	joeythefishuk@yahoo.co.uk (jo...	672.62 KB	5290	2	Fri Jan 13 05:07:18 2...
UK Festivals 2005 DVD 1_0 -- (repeat) "Festivals 1 - Readme.nfo"	joeythefishuk@yahoo.co.uk (jo...	4.20 KB	30	1	Sun Jan 15 10:33:08 ...
UK Festivals 2005 DVD 1_0 -- (repeat) "Festivals 1_0 - DVD Menu.rar"	joeythefishuk@yahoo.co.uk (jo...	672.64 KB	5290	2	Sun Jan 15 10:34:05 ...
UK Festivals 2005 DVD 1_1 - 01 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	33.97 KB	264	1	Fri Jan 13 05:07:32 2...
UK Festivals 2005 DVD 1_1 - 02 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.61 MB	238467	79	Fri Jan 13 05:07:46 2...
UK Festivals 2005 DVD 1_1 - 03 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.59 MB	238288	79	Fri Jan 13 05:25:44 2...
UK Festivals 2005 DVD 1_1 - 04 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.58 MB	238274	79	Fri Jan 13 05:43:37 2...
UK Festivals 2005 DVD 1_1 - 05 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.59 MB	238336	79	Fri Jan 13 06:01:43 2...
UK Festivals 2005 DVD 1_1 - 06 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.59 MB	238360	79	Fri Jan 13 06:19:52 2...
UK Festivals 2005 DVD 1_1 - 07 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.59 MB	238346	79	Fri Jan 13 06:37:53 2...
UK Festivals 2005 DVD 1_1 - 08 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.59 MB	238337	79	Fri Jan 13 06:55:37 2...
UK Festivals 2005 DVD 1_1 - 09 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.60 MB	238387	79	Fri Jan 13 07:13:32 2...
UK Festivals 2005 DVD 1_1 - 10 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.61 MB	238446	79	Fri Jan 13 07:31:35 2...
UK Festivals 2005 DVD 1_1 - 11 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.61 MB	238472	79	Fri Jan 13 07:49:28 2...
UK Festivals 2005 DVD 1_1 - 12 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.60 MB	238410	79	Fri Jan 13 08:07:26 2...
UK Festivals 2005 DVD 1_1 - 13 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.59 MB	238350	79	Fri Jan 13 08:25:22 2...

Filter: | 1 Sel. | Speed: 0 KB/s | MB: 419 | 0 Tasks / 0 MB / 0:00 ETA

6.4 Downloading a file

Now we can see that there are multiple parts to the posting, including .rar and .nfo files. You could click on one of the sub-items, or you can click on the main header to download all of it. This time we'll download all of it, and we can now see it downloading the content:



☐ Max Speed 50 KB/s
☐ Shutdown when finished

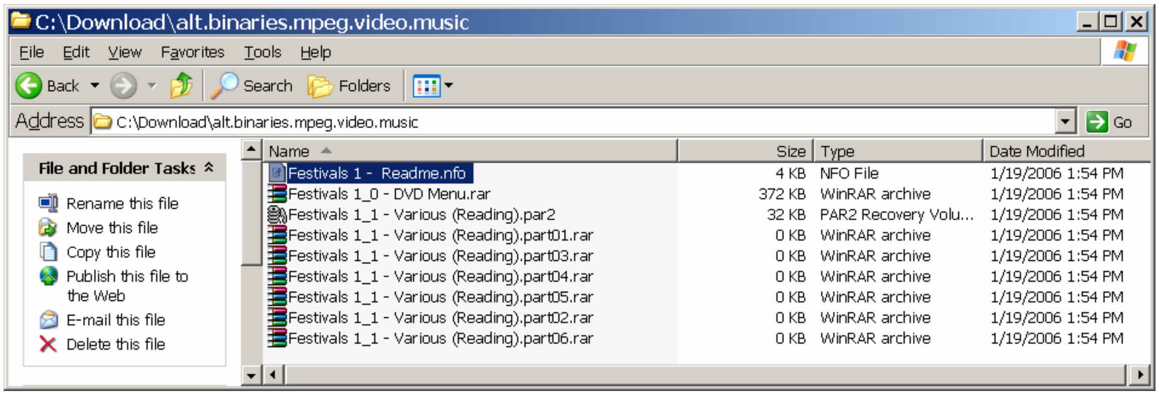
☑ Thread 1: news.giganews.com:UK Festivals 2005 DVD 1_1 - 04 of 27 - "Festivals 1_1 - Various (Reading).part03.rar" (2/79)
☑ Thread 2: news.giganews.com:UK Festivals 2005 DVD 1_1 - 06 of 27 - "Festivals 1_1 - Various (Reading).part05.rar" (1/79)
☑ Thread 3: news.giganews.com:UK Festivals 2005 DVD 1_1 - 02 of 27 - "Festivals 1_1 - Various (Reading).part01.rar" (2/79)
☑ Thread 4: news.giganews.com:UK Festivals 2005 DVD 1_1 - 03 of 27 - "Festivals 1_1 - Various (Reading).part02.rar" (1/79)
☑ Thread 5: news.giganews.com:UK Festivals 2005 DVD 1_1 - 05 of 27 - "Festivals 1_1 - Various (Reading).part04.rar" (1/79)
☑ Thread 6: news.giganews.com:UK Festivals 2005 DVD 1_1 - 07 of 27 - "Festivals 1_1 - Various (Reading).part06.rar" (1/79)

Group	Download dir	Last scanned
alt.binaries.mpeg.video.music	C:\Download\alt.binaries.mpeg.video.music\	Thu Jan 19 13:42:18 2006
alt.binaries.shareware	C:\Download\alt.binaries.shareware\	Thu Jan 19 13:28:06 2006
alt.binaries.freeware	C:\Download\alt.binaries.freeware\	Thu Jan 19 13:27:02 2006

Header	From	Size	Lines	Parts	Date
[Tiken Jah Fakoly] Africa Live 2005 à Dakar 26/28] - "Tiken_Jah_Fakoly...	sheryo@news.fr (S.H.E.R.Y.O.)	19.61 MB	158069	26	Sat Jan 14 01:34:23 ...
[Tiken Jah Fakoly] Africa Live 2005 à Dakar 27/28] - "Tiken_Jah_Fakoly...	sheryo@news.fr (S.H.E.R.Y.O.)	30.20 MB	243454	40	Sat Jan 14 02:00:51 ...
[Tiken Jah Fakoly] Africa Live 2005 à Dakar 28/28] - "Tiken_Jah_Fakoly...	sheryo@news.fr (S.H.E.R.Y.O.)	1.64 KB	9	1	Fri Jan 13 14:55:49 2...
UK Festivals 2005 DVD 1_1 - 20 of 27 - "Festivals 1_1 - Various (Reading)...		523.52 MB	4216533	1402	Fri Jan 13 10:24:18 2...
UK Festivals 2005 DVD 1_0 - "Festivals 1 - Readme.nfo"	joeythefishuk@yahoo.co.uk (jo...	4.19 KB	30	1	Fri Jan 13 05:07:04 2...
UK Festivals 2005 DVD 1_0 - "Festivals 1_0 - DVD Menu.rar"	joeythefishuk@yahoo.co.uk (jo...	672.62 KB	5290	2	Fri Jan 13 05:07:18 2...
UK Festivals 2005 DVD 1_0 -- (repeat) "Festivals 1 - Readme.nfo"	joeythefishuk@yahoo.co.uk (jo...	4.20 KB	30	1	Sun Jan 15 10:33:08 ...
UK Festivals 2005 DVD 1_0 -- (repeat) "Festivals 1_0 - DVD Menu.rar"	joeythefishuk@yahoo.co.uk (jo...	672.64 KB	5290	2	Sun Jan 15 10:34:05 ...
UK Festivals 2005 DVD 1_1 - 01 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	33.97 KB	264	1	Fri Jan 13 05:07:32 2...
UK Festivals 2005 DVD 1_1 - 02 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.61 MB	238467	79	Fri Jan 13 05:07:46 2...
UK Festivals 2005 DVD 1_1 - 03 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.59 MB	238288	79	Fri Jan 13 05:25:44 2...
UK Festivals 2005 DVD 1_1 - 04 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.58 MB	238274	79	Fri Jan 13 05:43:37 2...
UK Festivals 2005 DVD 1_1 - 05 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.59 MB	238336	79	Fri Jan 13 06:01:43 2...
UK Festivals 2005 DVD 1_1 - 06 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.59 MB	238360	79	Fri Jan 13 06:19:52 2...
UK Festivals 2005 DVD 1_1 - 07 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.59 MB	238346	79	Fri Jan 13 06:37:53 2...
UK Festivals 2005 DVD 1_1 - 08 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.59 MB	238337	79	Fri Jan 13 06:55:37 2...
UK Festivals 2005 DVD 1_1 - 09 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.60 MB	238387	79	Fri Jan 13 07:13:32 2...
UK Festivals 2005 DVD 1_1 - 10 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.61 MB	238446	79	Fri Jan 13 07:31:35 2...
UK Festivals 2005 DVD 1_1 - 11 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.61 MB	238472	79	Fri Jan 13 07:49:28 2...
UK Festivals 2005 DVD 1_1 - 12 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.60 MB	238410	79	Fri Jan 13 08:07:26 2...
UK Festivals 2005 DVD 1_1 - 13 of 27 - "Festivals 1_1 - Various (Readi...	joeythefishuk@yahoo.co.uk (jo...	29.59 MB	238350	79	Fri Jan 13 08:25:22 2...

Filter: | 1 Sel. | Speed: 568 KB/s | MB: 423 | 13 Tasks / 344 MB / 0:10 ETA

Once the download is complete, you can browse to the appropriate directory (C:\Download\alt.binaries.mpeg.video.music in a default installation) and view the resultant files:

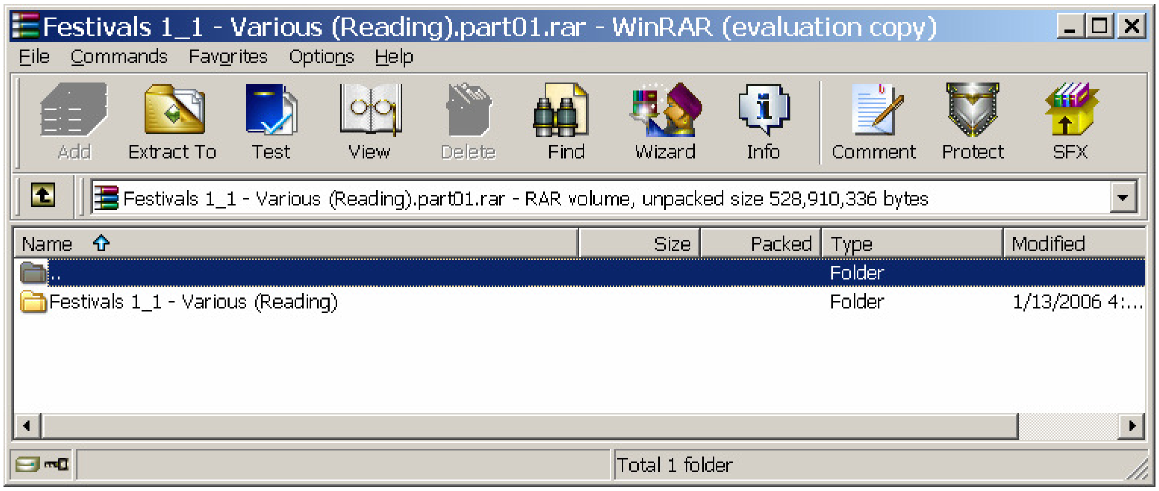


Address C:\Download\alt.binaries.mpeg.video.music

Name	Size	Type	Date Modified
Festivals 1 - Readme.nfo	4 KB	NFO File	1/19/2006 1:54 PM
Festivals 1_0 - DVD Menu.rar	372 KB	WinRAR archive	1/19/2006 1:54 PM
Festivals 1_1 - Various (Reading).par2	32 KB	PAR2 Recovery Volu...	1/19/2006 1:54 PM
Festivals 1_1 - Various (Reading).part01.rar	0 KB	WinRAR archive	1/19/2006 1:54 PM
Festivals 1_1 - Various (Reading).part03.rar	0 KB	WinRAR archive	1/19/2006 1:54 PM
Festivals 1_1 - Various (Reading).part04.rar	0 KB	WinRAR archive	1/19/2006 1:54 PM
Festivals 1_1 - Various (Reading).part05.rar	0 KB	WinRAR archive	1/19/2006 1:54 PM
Festivals 1_1 - Various (Reading).part02.rar	0 KB	WinRAR archive	1/19/2006 1:54 PM
Festivals 1_1 - Various (Reading).part06.rar	0 KB	WinRAR archive	1/19/2006 1:54 PM

6.5 Decompressing Files

At this point, you could load up one of the RAR files to decompress and extract your binary, run a PAR2 program to verify that you got all the pieces, or read the .nfo file. Ultimately, what you would end up with would be an MPEG file which you could then burn to DVD or view on a computer. Lets click on the part01.rar file, and fire up the WinRAR program:



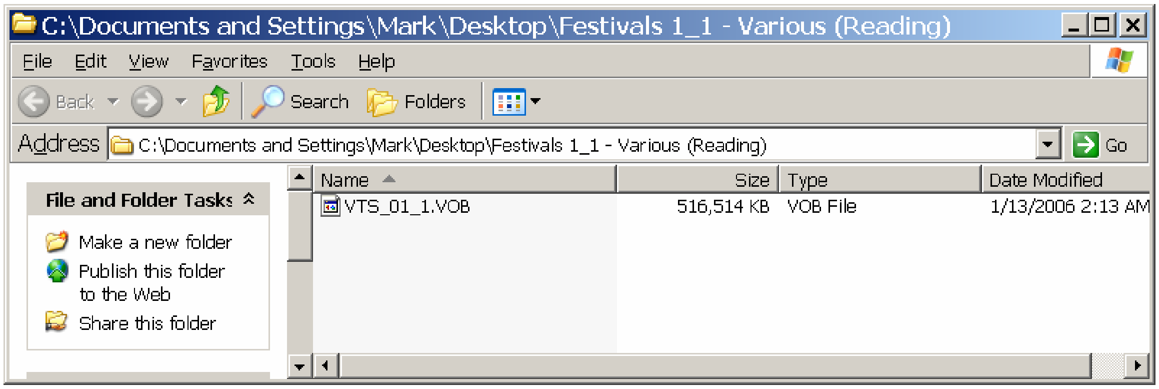
Festivals 1_1 - Various (Reading).part01.rar - WinRAR (evaluation copy)

Festivals 1_1 - Various (Reading).part01.rar - RAR volume, unpacked size 528,910,336 bytes

Name	Size	Packed	Type	Modified
..			Folder	
Festivals 1_1 - Various (Reading)			Folder	1/13/2006 4:...

Total 1 folder

We can now drag the folder to our desktop, and investigate the contents. Here we can see that we have a .VOB file (a MPEG-2 file used for DVD authoring)

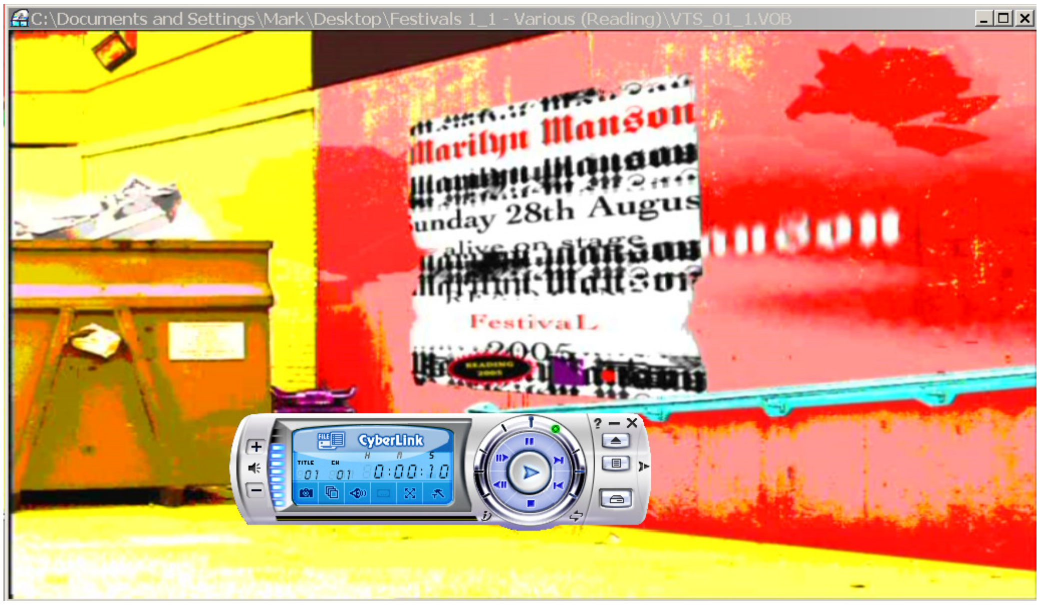


C:\Documents and Settings\Mark\Desktop\Festivals 1_1 - Various (Reading)

Address: C:\Documents and Settings\Mark\Desktop\Festivals 1_1 - Various (Reading)

Name	Size	Type	Date Modified
VTS_01_1.VOB	516,514 KB	VOB File	1/13/2006 2:13 AM

Using a DVD player program, we can open this VOB file and display it:



C:\Documents and Settings\Mark\Desktop\Festivals 1_1 - Various (Reading)\VTS_01_1.VOB

The same process works pretty much the same for other types of content. You'll obviously need an appropriate viewer to open it.

7.0 Legal Liability

What kind of liability do organizations have when it comes to Usenet postings? I am not a lawyer, and you should consult one for any reliable advice, but a few thoughts come to mind. First of all, it seems to me that being a Usenet provider is really not different from being an ISP – hence, I don't think that there is any real compulsion for providers to do any kind of filtering. Even if a legal entity did pass a law requiring (for example) logging of connections, users would just use an out-of-country server. However, there may be some implications for organizations that run their own severs internally. For example, if you work for a large corporation, and run a Usenet server that peers indiscriminately with other Usenet servers, you may be bringing in a lot of illegal material. Even if you don't make a conscious choice to allow pornography, for example, the act of not blocking it might be construed as promoting a sexually charged workplace or something similar. Similarly, you certainly wouldn't want to be on the receiving end of a Business Software Alliance audit, because a disgruntled employee turned you in.

8.0 Investigation

When it comes to investigating Usenet abuse, it's obviously not going to be that easy. Since there is no peer-to-peer connection, you have to rely on the information in the headers, some of which is forgeable. However, there are still some ways that you might be able to approach the problem.

8.1 On the Client

There may be traces of Usenet files on a workstation that you could turn up, either in allocated space, or in deleted / slack space. It would behoove a forensic investigator to include looking for evidence of Usenet abuse in their standard operating procedures.

Keyword searches might include:

- usenet
- nntp
- news
- binaries (or alt.binaries)
- known NNTP server names and IP addresses (you might find a personal firewall log or something with entries to a Usenet server, even if the program was deleted)

File searches might include:

- .RAR archive files
- .PAR and .PAR2 parity files
- .NFO description files
- .NZB batch files
- .ZIP files
- Known NNTP clients (in file space and the registry)

8.2 On the Network

If you had access to the network of either a suspect ISP or a suspect computer, you could use a protocol analyzer to identify suspicious activity. As previously noted, it is possible to get Usenet binaries entirely over web connections using gateways, as well as by watching for actual NNTP traffic. Using firewall logs, or a protocol analyzer such as Ethereal[14] you might look for connections such as:

- HTTP / HTTPS (TCP port 80 and 443) connections to known Usenet web servers such as Guba
- NNTP connections to any host on TCP port 119
- NNTP over SSL connections to any host on TCP or UDP port 563
- Traffic with a payload matching the keywords listed in 9.1

Of course, a crafty criminal will use the NNTP over SSL encryption option, or tunnel all of their connections through a SSH tunnel[15] or something.

8.3 At the Provider

Theoretically, you can get a Usenet provider to help you with a court order of some kind. However, as we noted previously, a lot of them don't keep any records at all, so this may be difficult. If you were looking for evidence of past wrongdoing, you are probably out of luck. However, if you have a suspect that you are watching over time, you might be able to get a court order to have them turn on logging, either at a server, or at the network level. I am interested in feedback from anyone who has tried to do this in an official capacity.

If you are going to get any information at all from a provider, you'll need to have that unique Message-ID field to work with. This may be your only way to figure out who posted a message. It is relatively certain that if you see a message with a Message-ID such as "Xns9734CAA2DE2A8orisitdunnocom@194.152.65.251" that the machine with the IP address of 194.152.65.251 was the one that originally took the posting. They *might* have some logs that could help you.

You might also look at the PATH header. For example, our previous example had a path of:

border1.nntp.dca.giganews.com!nntp.giganews.com!feed2.newsreader.com!newsreader.com!npeer.de.kpn-eurorings.net!news.tele.dk!news.tele.dk!small.news.tele.dk!news.astraweb.com!newsrouter-eu.astraweb.com!eweka!hq-usenetpeers.eweka.nl!81.171.88.219.MISMATCH!newsreader30.eweka.nl!not-for-mail

If it were possible for someone to spoof their Message-ID (and I assume it is) you might be able to determine what happened by contacting the next hop in the path, and querying their logs.

Regardless of how you look at it, this type of investigation could be very time consuming, not to mention cross a lot of jurisdictional lines. Good luck!

8.4 As a Sting

It's actually quite easy to set up your own Usenet server. In fact, a NNTP server is built into Windows Servers' IIS program[16]. You could set up your own private "invite only" Usenet server, and use some bait (over 18, not "jail bait") to lure people to your server. If they are using your own server, it would be very easy to log the connections, match it to an IP address, and then subpoena the records on that IP from the ISP. Of course, I'm not a cop or a lawyer, so I don't know the rules of engagement for this kind of thing (and especially what constitutes entrapment), but it's an idea.

9.0 Summary

I hope I have shown that there is a lot of activity (some of it illegal, but not all) on the Usenet. Due to the distributed nature of the service, and the lack of logging from service providers, it is also very difficult to trace activity on the Usenet. Given this, one wonders why any but the least technical of criminals would use anything but Usenet for their nefarious activities. Indeed, compared to Usenet, Peer to Peer file sharing is for chumps. It is also, alas, a huge blind spot (and pain to investigate!) for law enforcement. My concern is that this technology could be used for the exploitation of children, or possibly even passing covert messages to rogue actors on the international political scene.

Hopefully this document provided a cogent and understandable introduction to the topic. As I stated before, I welcome any questions, corrections or comments you might wish to offer on this document.

[1] (this has not been proven, but is entirely possible, see: http://niels.xtdnet.nl/stego/Usenet.php)

[2] http://en.wikipedia.org/wiki/Usenet

[3] http://www.wired.com/news/digiwood/0,1412,67588,00.html
[4] http://www.ietf.org/rfc/rfc0977.txt
[5] http://www.w3.org/Protocols/rfc1036/rfc1036.html
[6] http://www.yenc.org/whatis.htm
[7] http://www.daansystems.com/newsreactor/
[8] http://www.forteinc.com/agent/download.php
[9] http://www.rarlab.com/
[10] http://en.wikipedia.org/wiki/PAR2
[11] http://www.yabse.com/
[12] http://en.wikipedia.org/wiki/NZB
[13] http://easynews.com/
[14] http://ethereal.com/
[15] http://www.ssh.com/support/documentation/online/ssh/winhelp/32/Tunneling_Explained.html
[16] http://www.microsoft.com/mind/0100/NNTP/NNTP.asp