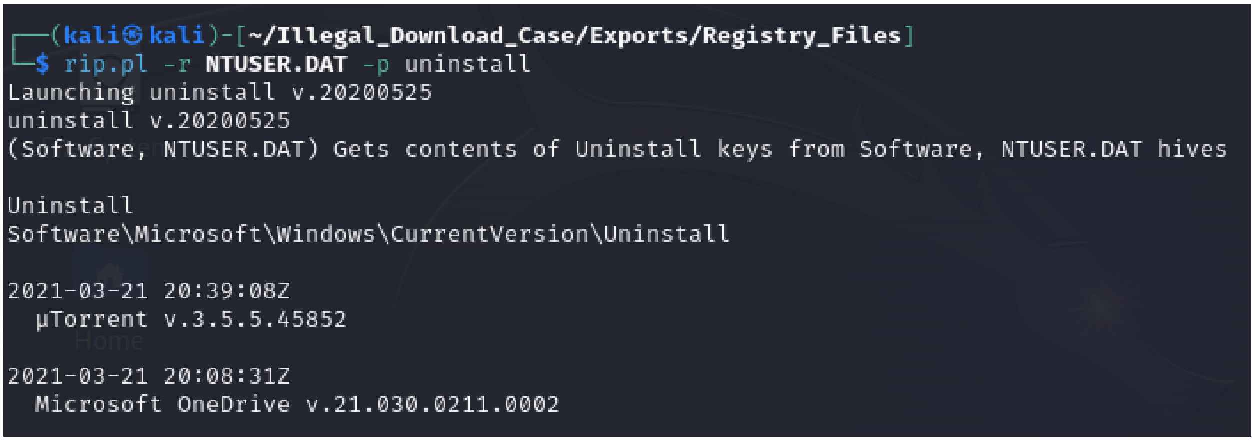
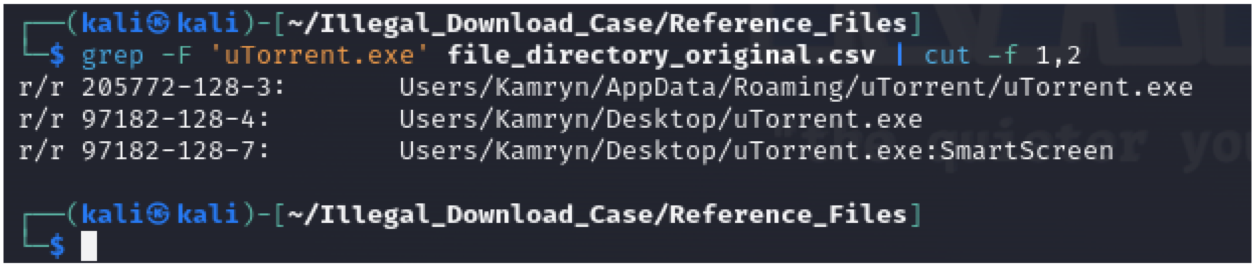
Daniella Boulos, Julianna Russo, Tyler Kaminer Oct 31, 2024
NIST Case: Torrent Logs Computer Forensics

User Regripper to find out when uTorrent could have been installed



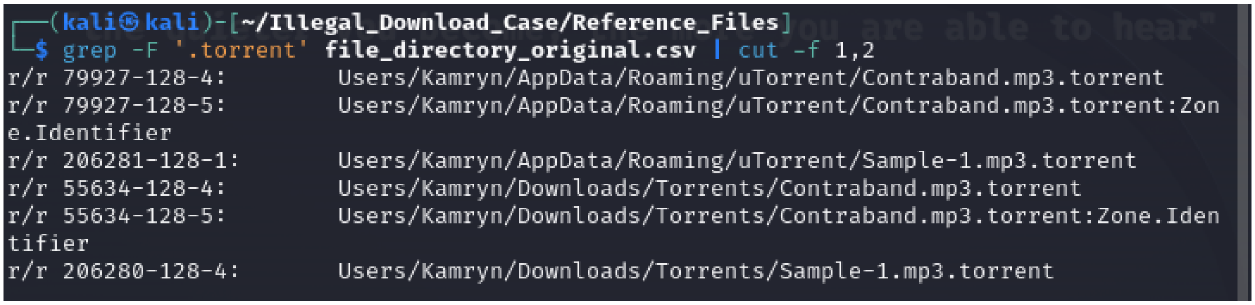
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ rip.pl -r NTUSER.DAT -p uninstall
Launching uninstall v.20200525
uninstall v.20200525
(Software, NTUSER.DAT) Gets contents of Uninstall keys from Software, NTUSER.DAT hives

Uninstall
Software\Microsoft\Windows\CurrentVersion\Uninstall

2021-03-21 20:39:08Z
  µTorrent v.3.5.5.45852

2021-03-21 20:08:31Z
  Microsoft OneDrive v.21.030.0211.0002
```

Use grep to get relevant file paths for uTorrent



```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ grep -F 'uTorrent.exe' file_directory_original.csv | cut -f 1,2
r/r 205772-128-3:       Users/Kamryn/AppData/Roaming/uTorrent/uTorrent.exe
r/r 97182-128-4:        Users/Kamryn/Desktop/uTorrent.exe
r/r 97182-128-7:        Users/Kamryn/Desktop/uTorrent.exe:SmartScreen

┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ █
```

Use grep to search for torrent files



```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ grep -F '.torrent' file_directory_original.csv | cut -f 1,2
r/r 79927-128-4:        Users/Kamryn/AppData/Roaming/uTorrent/Contraband.mp3.torrent
r/r 79927-128-5:        Users/Kamryn/AppData/Roaming/uTorrent/Contraband.mp3.torrent:Zon
e.Identifier
r/r 206281-128-1:       Users/Kamryn/AppData/Roaming/uTorrent/Sample-1.mp3.torrent
r/r 55634-128-4:        Users/Kamryn/Downloads/Torrents/Contraband.mp3.torrent
r/r 55634-128-5:        Users/Kamryn/Downloads/Torrents/Contraband.mp3.torrent:Zone.Iden
tifier
r/r 206280-128-4:       Users/Kamryn/Downloads/Torrents/Sample-1.mp3.torrent
```

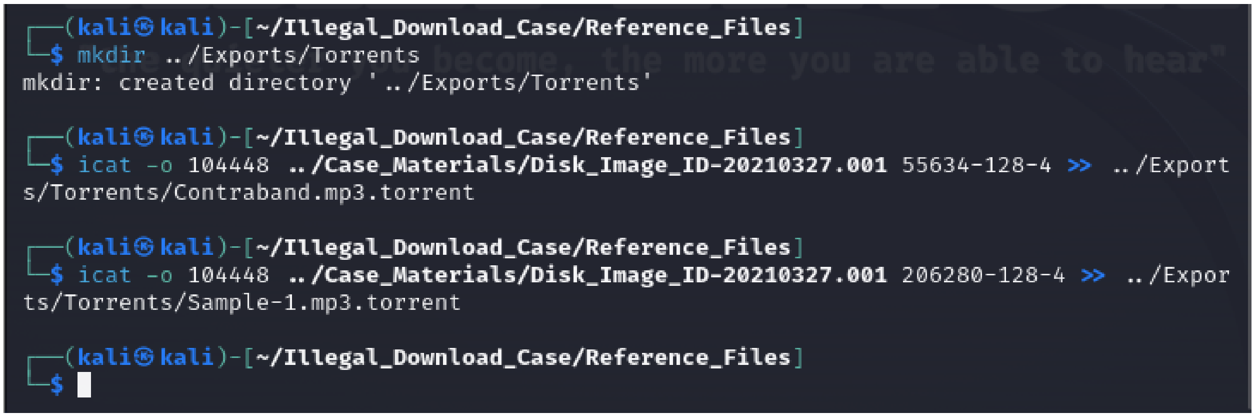
For torrent files on PC

a. **What was the original file?**
   i. Sample-1.mp3
   ii. Contraband.mp3
b. **What trackers are on the torrent file?**
   i. Udp
   ii. Http

c. **What torrent application created it?**
   i. uTorrent

d. **When was the torrent file created?**
   i. Contraband.mp3 file was created on 3/27/21 at 10:05:03 A.M.
   ii. Sample-1.mp3 was created on 3/21/21 at 4:42:39 P.M

Use icat to extract the torrent files



```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ mkdir ../Exports/Torrents
mkdir: created directory '../Exports/Torrents'

┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ icat -o 104448 ../Case_Materials/Disk_Image_ID-20210327.001 55634-128-4 >> ../Export
s/Torrents/Contraband.mp3.torrent

┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ icat -o 104448 ../Case_Materials/Disk_Image_ID-20210327.001 206280-128-4 >> ../Expor
ts/Torrents/Sample-1.mp3.torrent

┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ 
```

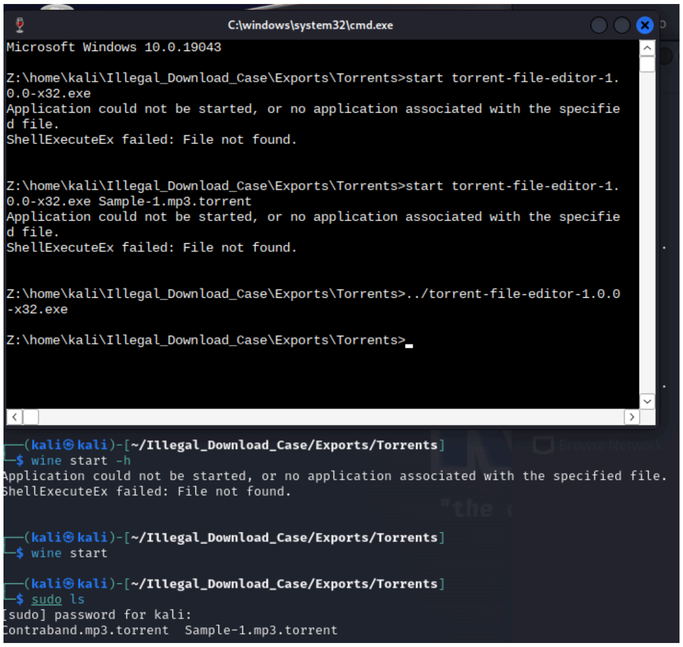
Verify that you have genuine copies:

Said to skip

Verify that extracted files are same as ones in Users/Kamryn/AppData/Roaming/uTorrent:

Said to skip

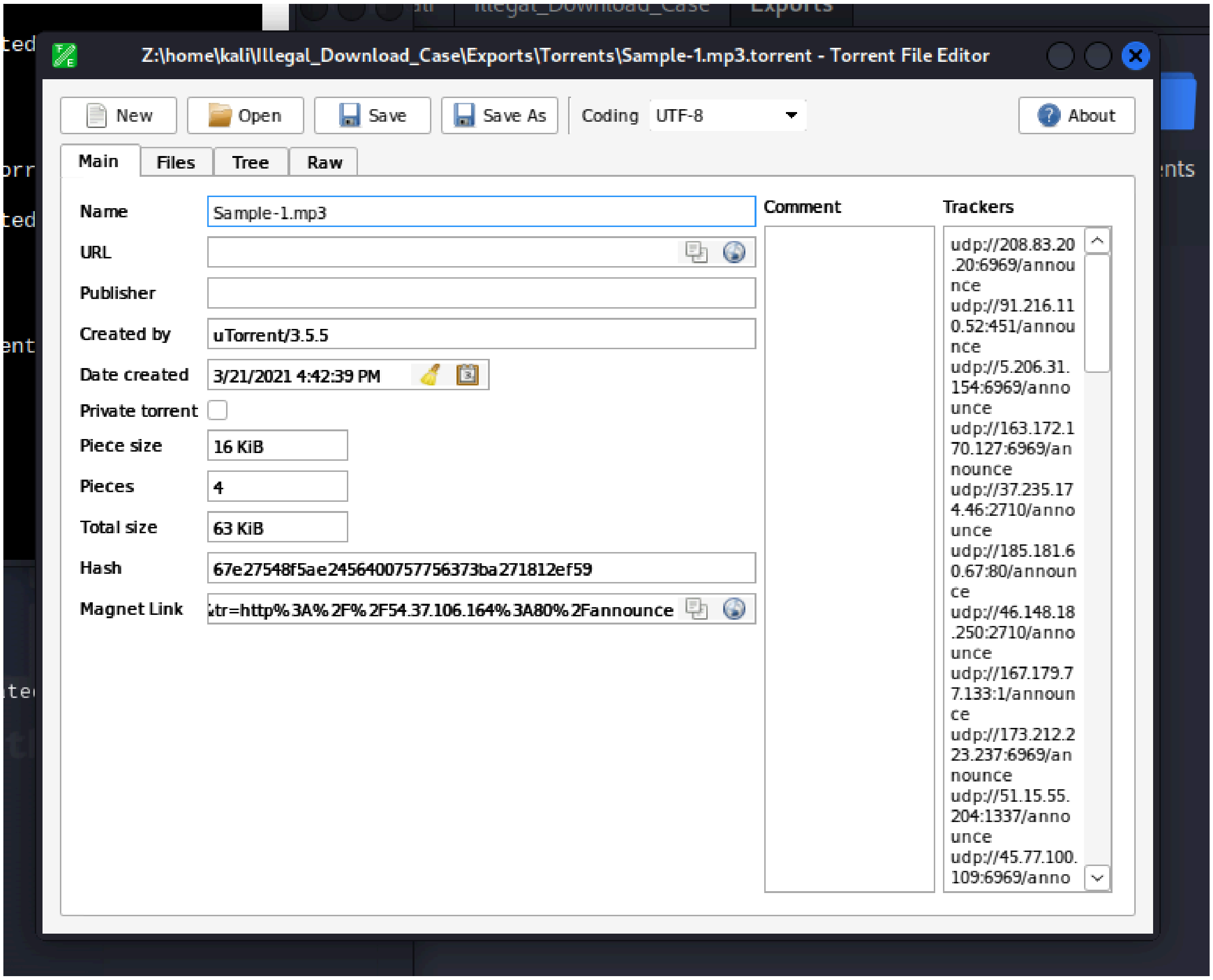
Use torrent file editor to analyze the torrent file Sample-1.mp3.torrent:



```
Microsoft Windows 10.0.19043

Z:\home\kali\Illegal_Download_Case\Exports\Torrents>start torrent-file-editor-1.
0.0-x32.exe
Application could not be started, or no application associated with the specifie
d file.
ShellExecuteEx failed: File not found.


Z:\home\kali\Illegal_Download_Case\Exports\Torrents>start torrent-file-editor-1.
0.0-x32.exe Sample-1.mp3.torrent
Application could not be started, or no application associated with the specifie
d file.
ShellExecuteEx failed: File not found.


Z:\home\kali\Illegal_Download_Case\Exports\Torrents>../torrent-file-editor-1.0.0
-x32.exe

Z:\home\kali\Illegal_Download_Case\Exports\Torrents>_
```

```
──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Torrents]
└─$ wine start -h
Application could not be started, or no application associated with the specified file.
ShellExecuteEx failed: File not found.


──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Torrents]
└─$ wine start

──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Torrents]
└─$ sudo ls
[sudo] password for kali:
Contraband.mp3.torrent  Sample-1.mp3.torrent
```

GUI will open, you should see:



Z:\home\kali\Illegal_Download_Case\Exports\Torrents\Sample-1.mp3.torrent - Torrent File Editor

Coding: UTF-8

Name	Sample-1.mp3
URL	
Publisher	
Created by	uTorrent/3.5.5
Date created	3/21/2021 4:42:39 PM
Private torrent	□
Piece size	16 KiB
Pieces	4
Total size	63 KiB
Hash	67e27548f5ae2456400757756373ba271812ef59
Magnet Link	&tr=http%3A%2F%2F54.37.106.164%3A80%2Fannounce

Comment

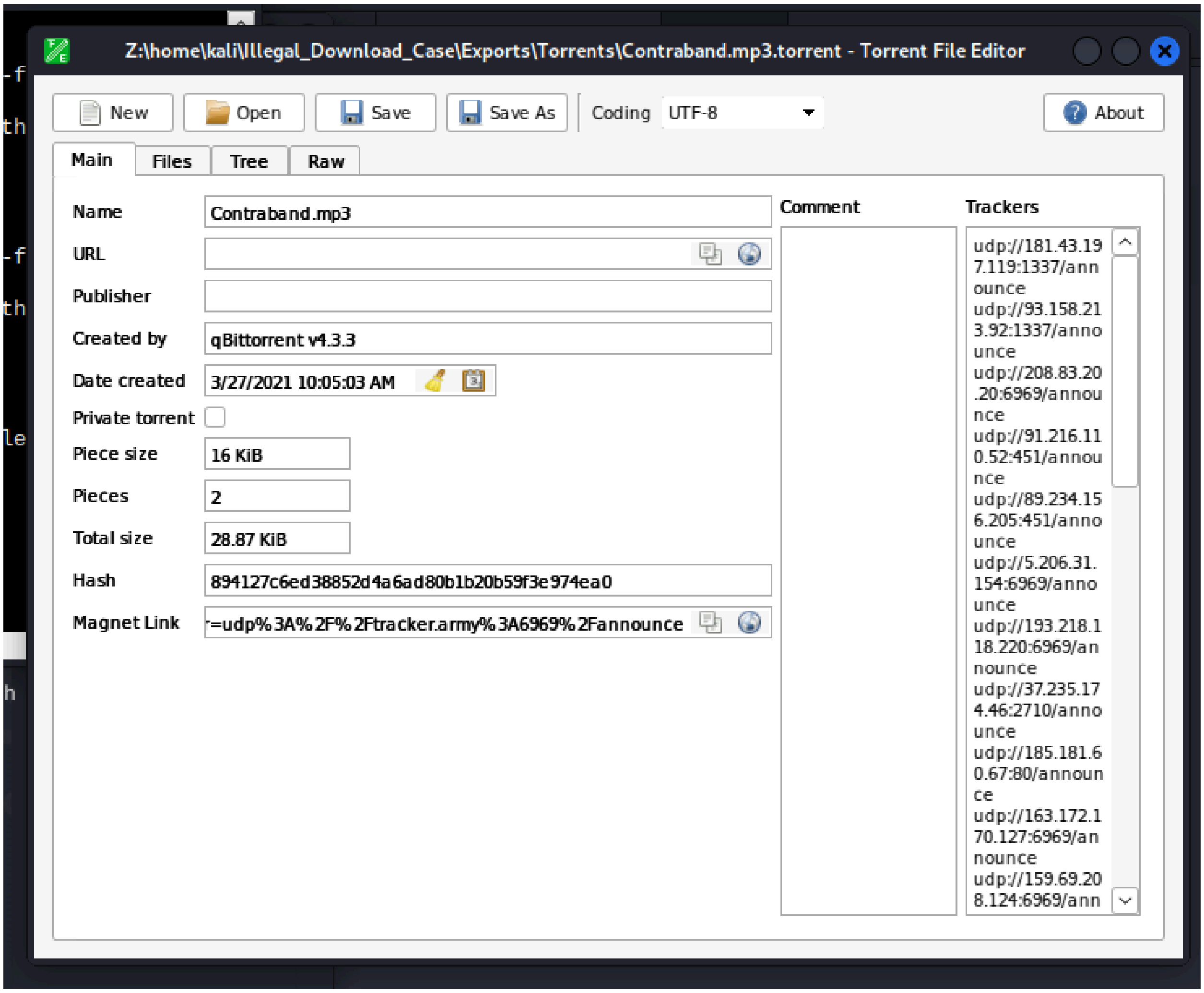
Trackers

```
udp://208.83.20.20:6969/announce
udp://91.216.110.52:451/announce
udp://5.206.31.154:6969/announce
udp://163.172.170.127:6969/announce
udp://37.235.174.46:2710/announce
udp://185.181.60.67:80/announce
udp://46.148.18.250:2710/announce
udp://167.179.77.133:1/announce
udp://173.212.223.237:6969/announce
udp://51.15.55.204:1337/announce
udp://45.77.100.109:6969/anno
```

Use Torrent File Editor to analyze the torrent file Contraband.mp3s:

See above

GUI will open, you should see:



Z:\home\kali\Illegal_Download_Case\Exports\Torrents\Contraband.mp3.torrent - Torrent File Editor

Coding: UTF-8

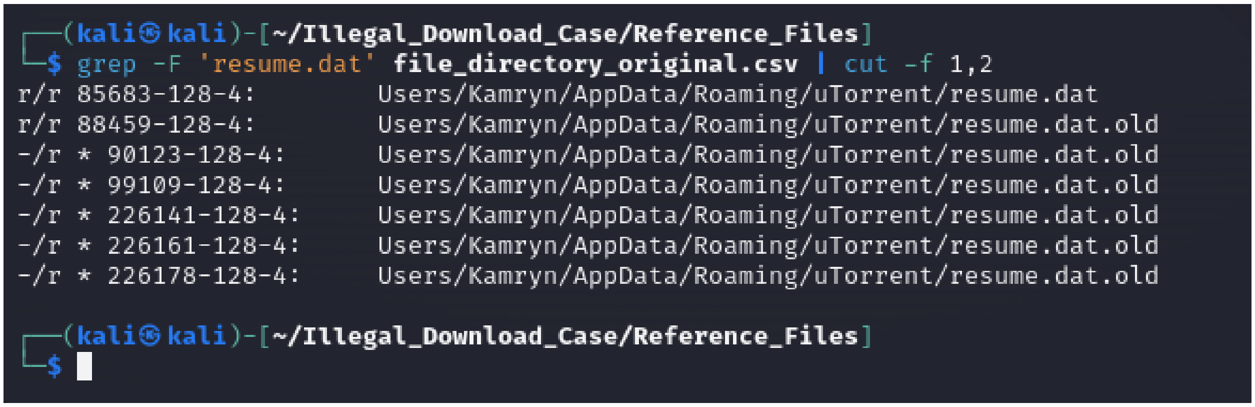
Name	Contraband.mp3
URL	
Publisher	
Created by	qBittorrent v4.3.3
Date created	3/27/2021 10:05:03 AM
Private torrent	□
Piece size	16 KiB
Pieces	2
Total size	28.87 KiB
Hash	894127c6ed38852d4a6ad80b1b20b59f3e974ea0
Magnet Link	=udp%3A%2F%2Ftracker.army%3A6969%2Fannounce

Comment

Trackers

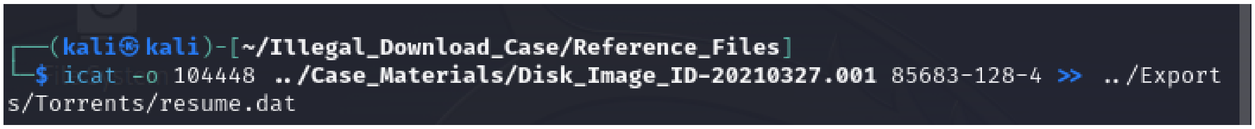
udp://181.43.197.119:1337/announce
udp://93.158.213.92:1337/announce
udp://208.83.20.20:6969/announce
udp://91.216.110.52:451/announce
udp://89.234.156.205:451/announce
udp://5.206.31.154:6969/announce
udp://193.218.118.220:6969/announce
udp://37.235.174.46:2710/announce
udp://185.181.60.67:80/announce
udp://163.172.170.127:6969/announce
udp://159.69.208.124:6969/ann

Use grep to find the log file:



```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ grep -F 'resume.dat' file_directory_original.csv | cut -f 1,2
r/r 85683-128-4:        Users/Kamryn/AppData/Roaming/uTorrent/resume.dat
r/r 88459-128-4:        Users/Kamryn/AppData/Roaming/uTorrent/resume.dat.old
-/r * 90123-128-4:      Users/Kamryn/AppData/Roaming/uTorrent/resume.dat.old
-/r * 99109-128-4:      Users/Kamryn/AppData/Roaming/uTorrent/resume.dat.old
-/r * 226141-128-4:     Users/Kamryn/AppData/Roaming/uTorrent/resume.dat.old
-/r * 226161-128-4:     Users/Kamryn/AppData/Roaming/uTorrent/resume.dat.old
-/r * 226178-128-4:     Users/Kamryn/AppData/Roaming/uTorrent/resume.dat.old

┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ 
```

Use icat to extract the log file:

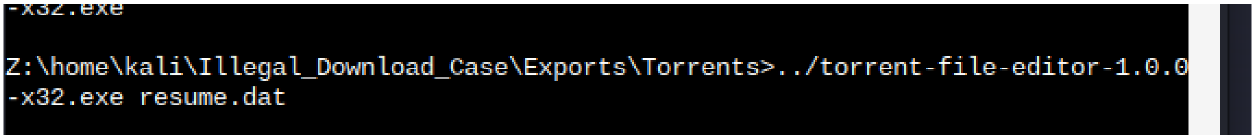


```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ icat -o 104448 ../Case_Materials/Disk_Image_ID-20210327.001 85683-128-4 >> ../Export
s/Torrents/resume.dat
```

Verify that you have a genuine copy:

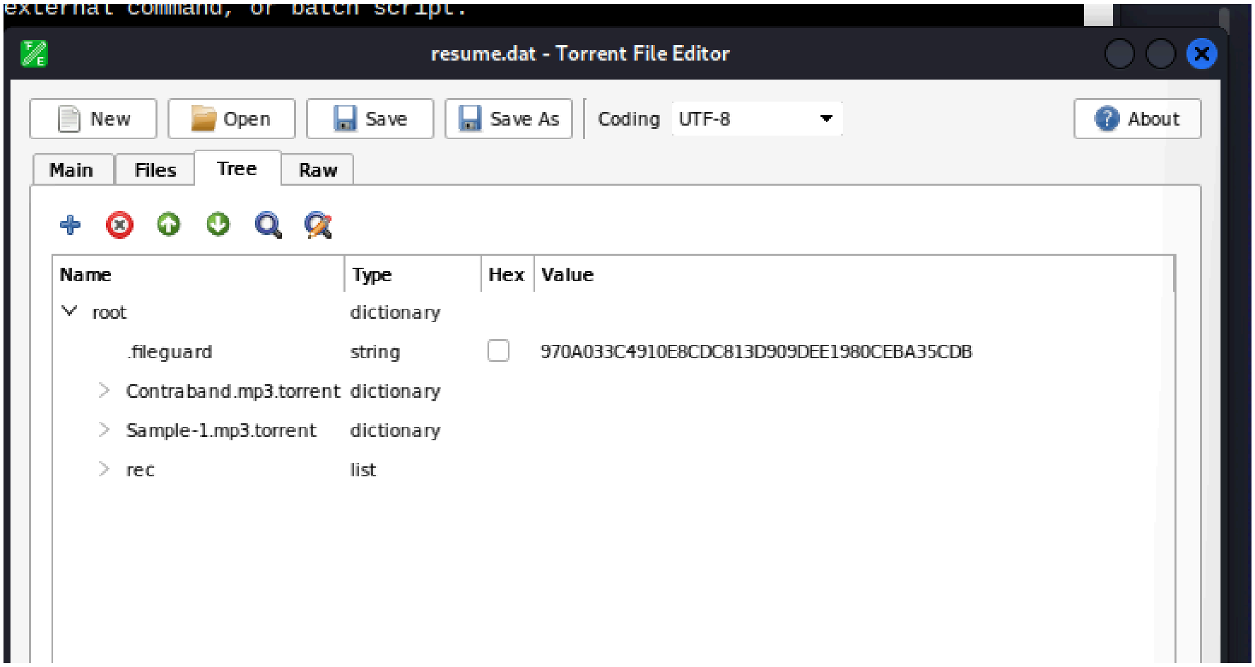
Said to skip

Use Torrent File Editor to analyze the log file:



```
-x32.exe

Z:\home\kali\Illegal_Download_Case\Exports\Torrents>../torrent-file-editor-1.0.0
-x32.exe resume.dat
```

Find out which torrent were added to uTorrent:



```
external command, or batch script.
```

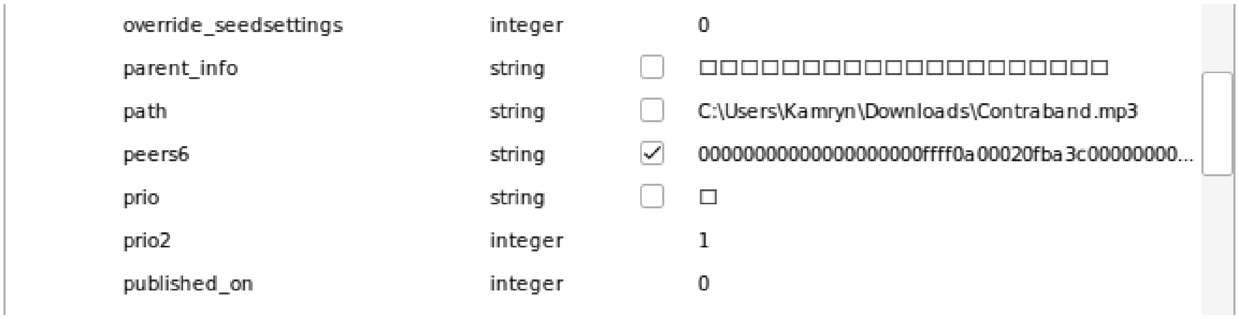
resume.dat - Torrent File Editor

Coding UTF-8

Name	Type	Hex	Value
root	dictionary		
.fileguard	string	□	970A033C4910E8CDC813D909DEE1980CEBA35CDB
Contraband.mp3.torrent	dictionary		
Sample-1.mp3.torrent	dictionary		
rec	list		

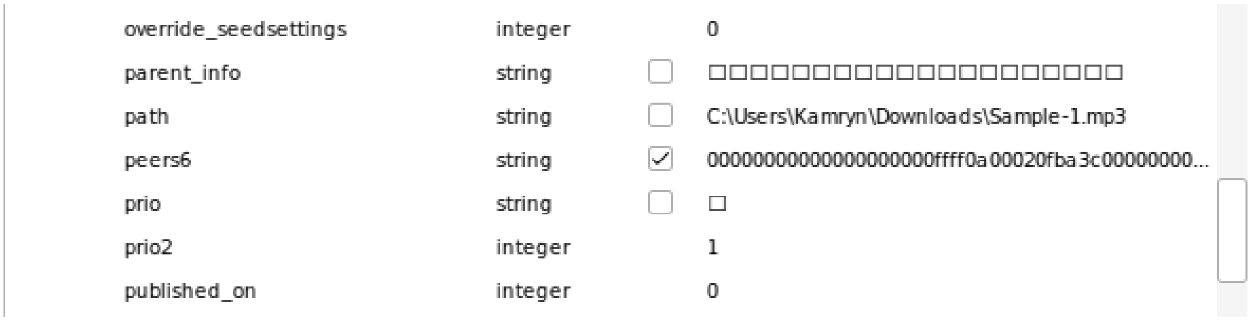
Locate the peer information for both torrents:

Contraband.mp3.torrent



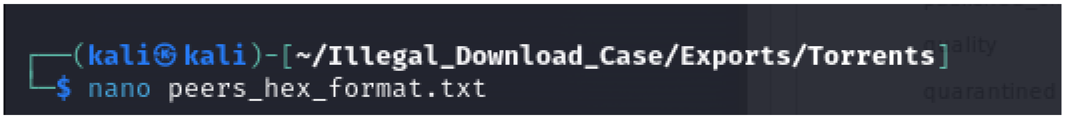
override_seedsettings	integer		0
parent_info	string	□	□□□□□□□□□□□□□□□□□□□□□□
path	string	□	C:\Users\Kamryn\Downloads\Contraband.mp3
peers6	string	☑	00000000000000000000ffff0a00020fba3c00000000...
prio	string	□	□
prio2	integer		1
published_on	integer		0

Sample-1.mp3.torrent



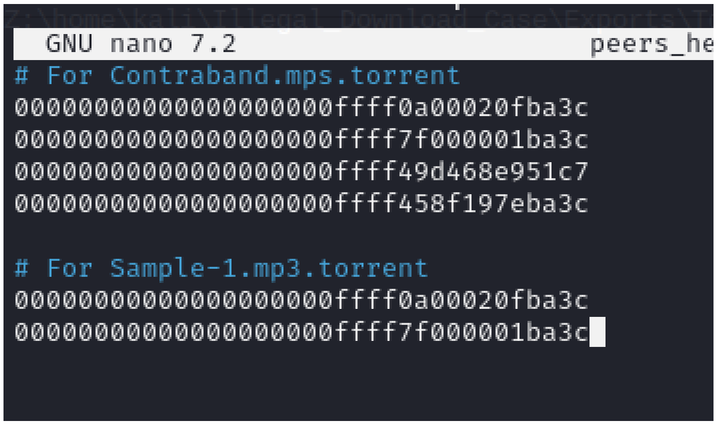
override_seedsettings	integer		0
parent_info	string	□	□□□□□□□□□□□□□□□□□□□□□□
path	string	□	C:\Users\Kamryn\Downloads\Sample-1.mp3
peers6	string	☑	00000000000000000000ffff0a00020fba3c00000000...
prio	string	□	□
prio2	integer		1
published_on	integer		0

Create a new text file to place the hex data in:



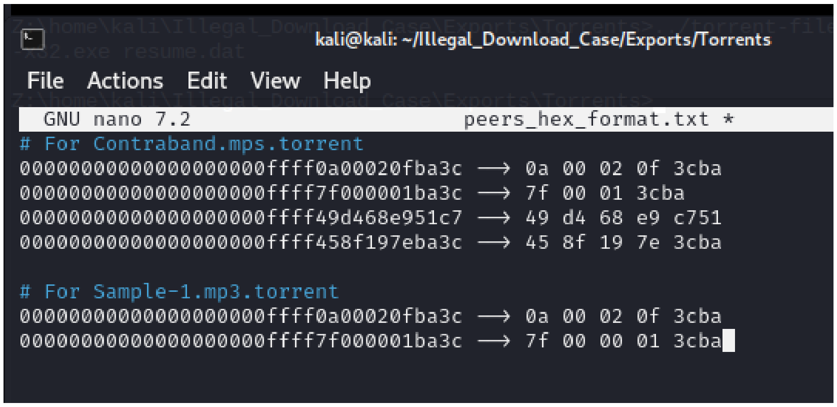
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Torrents]
└─$ nano peers_hex_format.txt
```

Paste the hex data in the new text file:



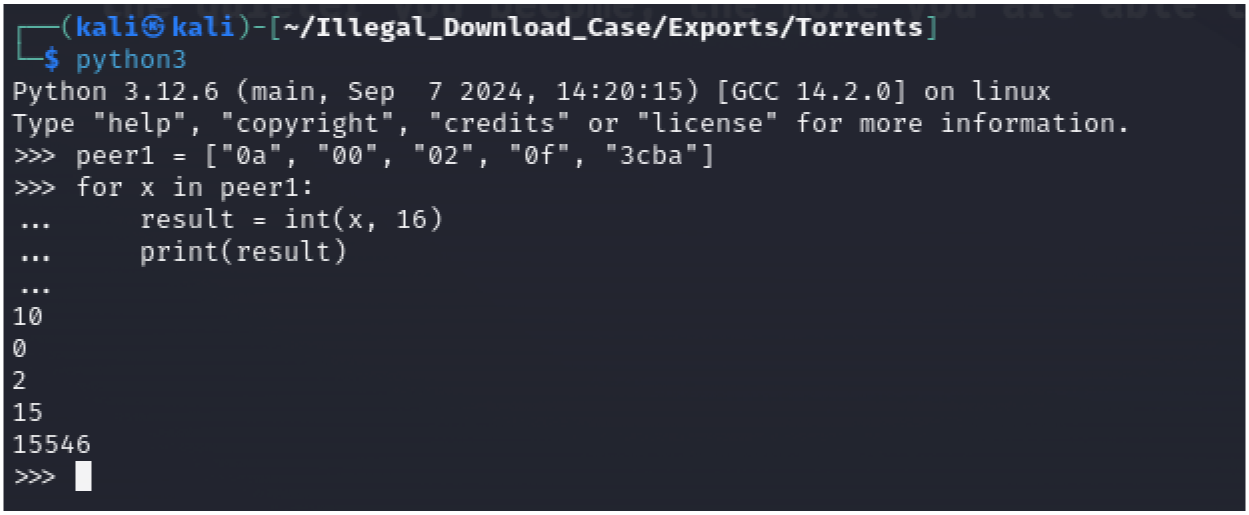
```
  GNU nano 7.2                     peers_he
# For Contraband.mps.torrent
00000000000000000000ffff0a00020fba3c
00000000000000000000ffff7f000001ba3c
00000000000000000000ffff49d468e951c7
00000000000000000000ffff458f197eba3c

# For Sample-1.mp3.torrent
00000000000000000000ffff0a00020fba3c
00000000000000000000ffff7f000001ba3c
```

You should have a text file with these entries:


kali@kali: ~/Illegal_Download_Case/Exports/Torrents
File Actions Edit View Help

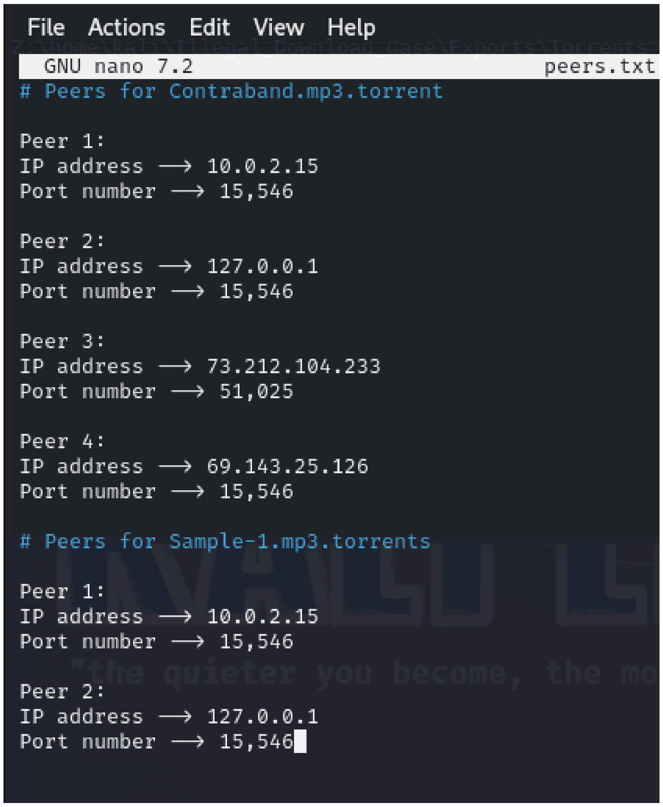
```
  GNU nano 7.2                                  peers_hex_format.txt *
# For Contraband.mps.torrent
00000000000000000000ffff0a00020fba3c ⟶ 0a 00 02 0f 3cba
00000000000000000000ffff7f000001ba3c ⟶ 7f 00 01 3cba
00000000000000000000ffff49d468e951c7 ⟶ 49 d4 68 e9 c751
00000000000000000000ffff458f197eba3c ⟶ 45 8f 19 7e 3cba

# For Sample-1.mp3.torrent
00000000000000000000ffff0a00020fba3c ⟶ 0a 00 02 0f 3cba
00000000000000000000ffff7f000001ba3c ⟶ 7f 00 00 01 3cba
```

Write a python script to convert from hex to decimal number:



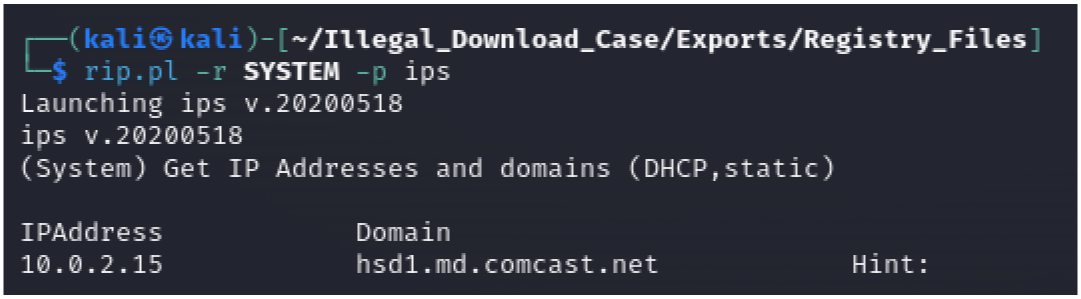
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Torrents]
└─$ python3
Python 3.12.6 (main, Sep  7 2024, 14:20:15) [GCC 14.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> peer1 = ["0a", "00", "02", "0f", "3cba"]
>>> for x in peer1:
...     result = int(x, 16)
...     print(result)
...
10
0
2
15
15546
>>> 
```

These are the IP addresses and port numbers for each peer:



```
 GNU nano 7.2                                      peers.txt
# Peers for Contraband.mp3.torrent

Peer 1:
IP address ⟶ 10.0.2.15
Port number ⟶ 15,546

Peer 2:
IP address ⟶ 127.0.0.1
Port number ⟶ 15,546

Peer 3:
IP address ⟶ 73.212.104.233
Port number ⟶ 51,025

Peer 4:
IP address ⟶ 69.143.25.126
Port number ⟶ 15,546

# Peers for Sample-1.mp3.torrents

Peer 1:
IP address ⟶ 10.0.2.15
Port number ⟶ 15,546

Peer 2:
IP address ⟶ 127.0.0.1
Port number ⟶ 15,546
```

Use Regripper to find the IP address of Kamryn’s system:



```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ rip.pl -r SYSTEM -p ips
Launching ips v.20200518
ips v.20200518
(System) Get IP Addresses and domains (DHCP,static)

IPAddress             Domain
10.0.2.15             hsd1.md.comcast.net            Hint:
```