

# ICAC TASK FORCE

## Torrential Downpour / BitTorrent Investigations Update and Refresher

Presented by:

Detective Robert Erdely, Indiana County Detectives Bureau  
PA State Police (Retired)

March 10, 2016

# Webinar Information

---

This webinar is supported by grant 2013-MC-FX-K104, provided by the Office of Juvenile Justice and Delinquency Prevention (OJJDP), and is brought to you by the ICAC Training & Technical Assistance Program.

*Points of view or opinions expressed in this webinar are those of the presenter(s) and do not necessarily represent the official position or policies of OJJDP, the U.S. Department of Justice or Fox Valley Technical College.*

ICAC Training & Technical Assistance is a program of the Fox Valley Technical College-National Criminal Justice Training Center (NCJTC).

# During the Webinar

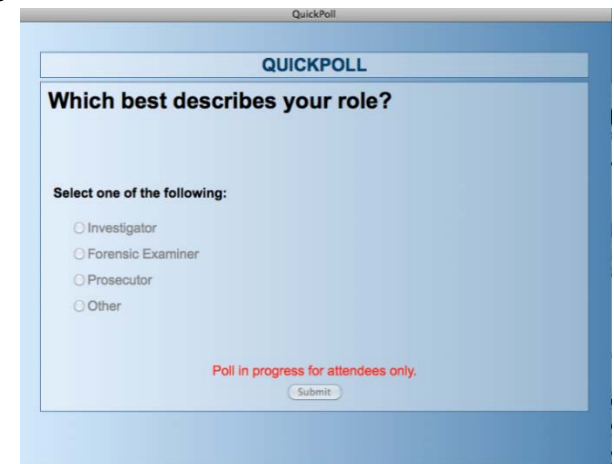
---

- All attendees will be muted.
- If you desire to ask a question, please use the questions section of the GoToWebinar dialogue box, typically on the right side of your screen.
- Please do not raise your hand for questions, we can not unmute you.
- Questions will either be answered directly by a panelist or asked to the presenter who will answer.

# Poll Questions

---

- Poll questions may be asked during the webinar. They are asked so we can better understand the audience and provide the most useful information to you.
- As they will only be open a short period of time, please respond promptly.



QuickPoll

**QUICKPOLL**

**Which best describes your role?**

Select one of the following:

- Investigator
- Forensic Examiner
- Prosecutor
- Other

Poll in progress for attendees only.

Submit

# Post Webinar Information

---

- At the conclusion of the webinar, a short survey will appear. We ask that you complete the survey in an effort to gather information to better serve the community in preparation for future webinars. Please complete it before signing off.
- You will receive a link to access our law enforcement only webinar library where you can view the recording and access related webinar material. Due to the sensitivity of some of the material you must be a registered law enforcement member of the *NCJTC.org* or *ICACTaskforce.org* websites. If you are not currently a member, you will need to register for access at [www.ncjtc.org](http://www.ncjtc.org).

# Additional Information

---

*Points of view or opinions expressed in this webinar are those of the presenter(s) and do not necessarily represent the official position or policies of OJJDP or the U.S. Department of Justice.*

# Poll Questions

---

# Investigative BitTorrent TD / TDR (Update)







[www.bittorrent.com](http://www.bittorrent.com)



## BitTorrent, Explained.

from **BitTorrent, Inc.** 2 years ago NOT YET RATED

Are you new to the world of BitTorrent? Have you been using BitTorrent for awhile, but you're curious about how it all works?

This video, produced by the team behind the popular BitTorrent and  $\mu$ Torrent software, includes an overview of the BitTorrent ecosystem and gives you great tips on how to leverage the products for your enjoyment.

# Torrential Downpour / Downpour Receptor

---

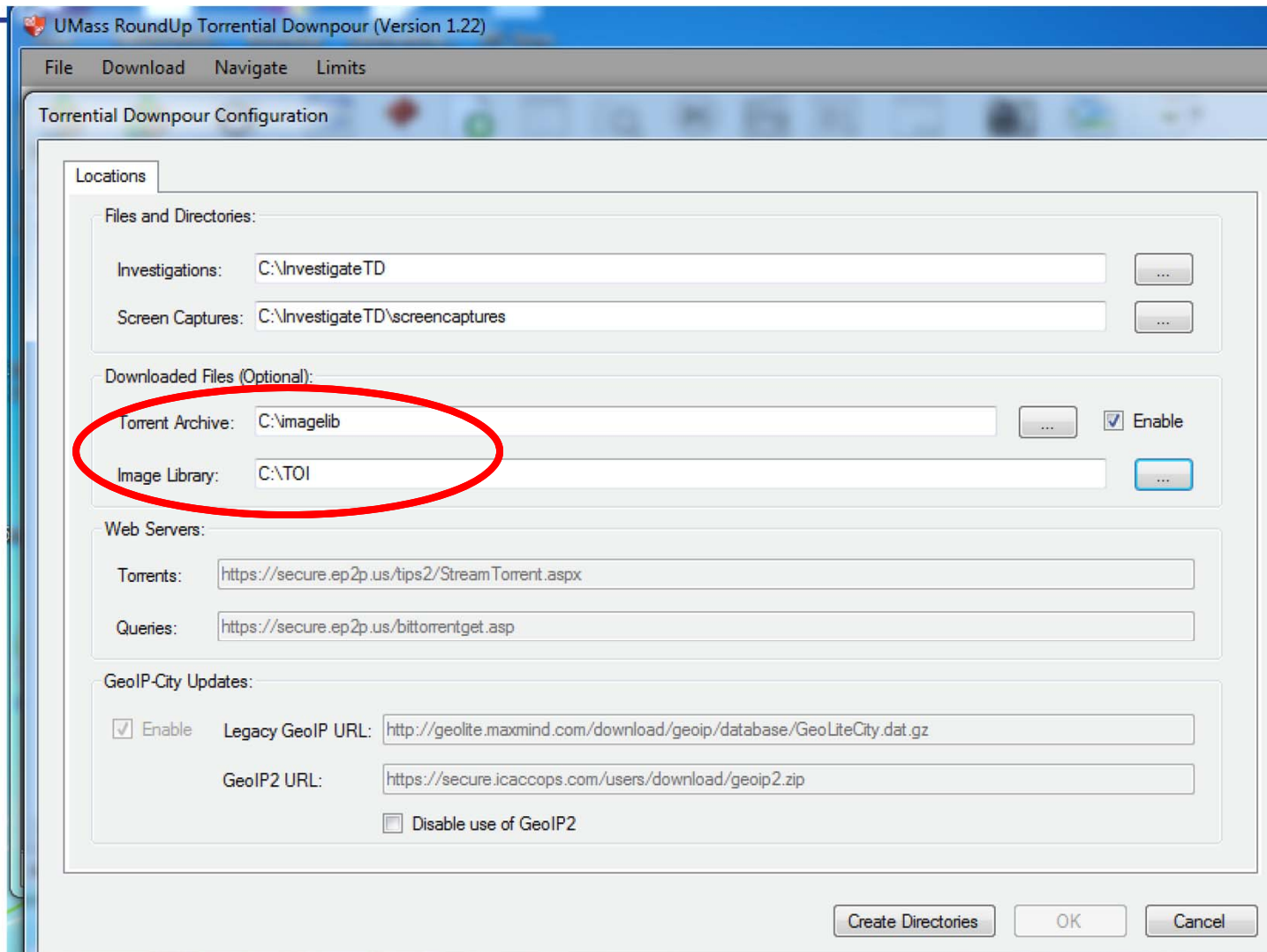
- Investigative Hurdles
  - Finding .torrent files
  - Analyzing .torrents
  - Torrents are shared in pieces
  - Knowing hash values of files
  - Finding .torrent on seized computer

# Torrential Downpour / Downpour Receptor

---

- Many new features
  - Download History
  - GeoIP2
  - Image Library
  - Ip Ranges
  - Filters
  - Weight
  - Military
  - Clean up

# Torrential Downpour



# Torrential Downpour

Torrential Downpour Configuration

Locations Options Investigator **Advanced**

TCP Listener:

TCP server Port:

Handshake Version:

Reschedule Downloads:

Hours after entire torrent  Hours after all possessed pieces

File System:

Maximum directory characters:  Maximum full path characters:

# .torrent weights

---

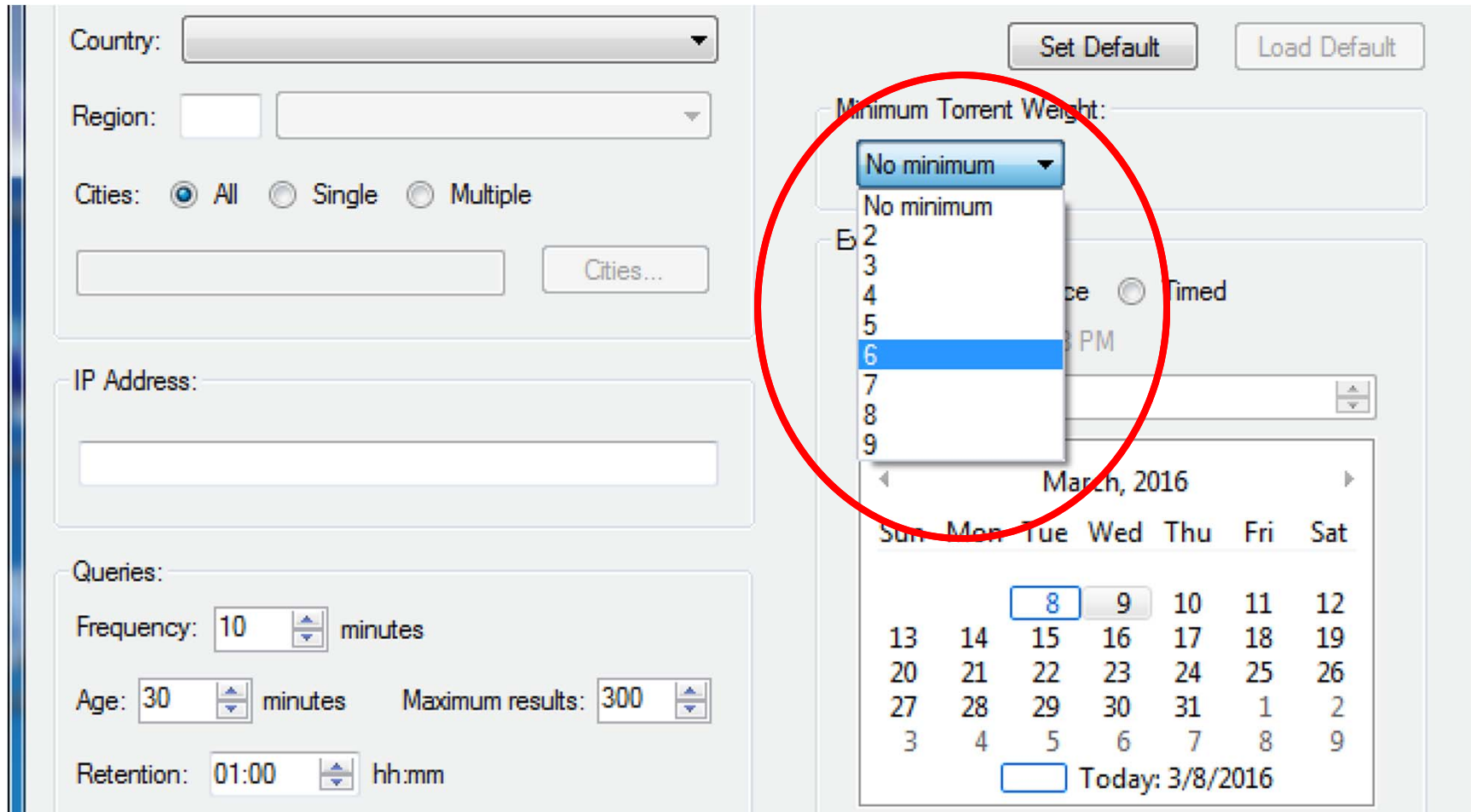
| Infohash or Weight <input type="text"/>                  |        |
|--|--------|
| Infohash   | Weight |
| <a href="#">817e0637dd4bdfdb4bc032408da650391d8fd609</a> | 9      |
| <a href="#">c8685605d51b4b7bdfeef9f441b93a16411be5bf</a> | 9      |
| <a href="#">0f8fc20786be858df001f93a34c8d49554e841c5</a> | 9      |
| <a href="#">8b687670eb33dbfd3f386a5f4466262477f7e22f</a> | 9      |
| <a href="#">3aeed2678db8a0494b7c4f21e2174cb21f510c60</a> | 9      |
|  |        |

# .torrent weights

---

- 9 – Worst of the Worst
- 5 – Default weight, not evaluated yet
- 1 – Clothed children, not illegal

# Torrential Downpour



Country:

Region:

Cities:  All  Single  Multiple

IP Address:

Queries:

Frequency:  minutes

Age:  minutes    Maximum results:

Retention:  hh:mm

Minimum Torrent Weight:

Immediate  Timed

March, 2016

| Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|-----|-----|-----|-----|-----|-----|-----|
|     |     | 8   | 9   | 10  | 11  | 12  |
| 13  | 14  | 15  | 16  | 17  | 18  | 19  |
| 20  | 21  | 22  | 23  | 24  | 25  | 26  |
| 27  | 28  | 29  | 30  | 31  | 1   | 2   |
| 3   | 4   | 5   | 6   | 7   | 8   | 9   |

Today: 3/8/2016





# Questions

# Torrential Downpour Receptor

Locations Options Investigator Advanced

Directories:

Investigations: C:\InvestTDRceptor

Downloaded Files (Optional):

Torrent Archive: C:\TOI Enable

Image Library: C:\imagelib

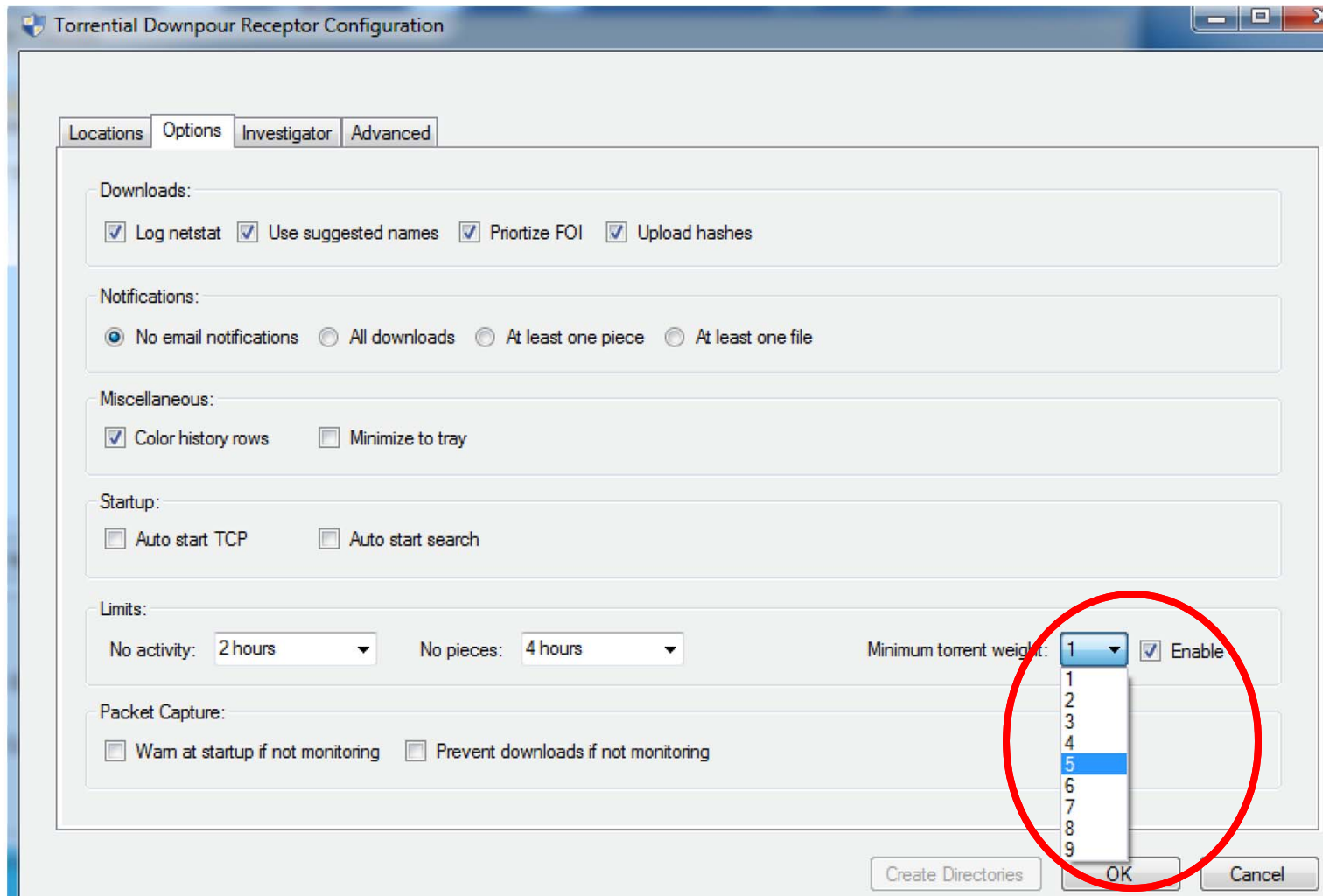
Law Enforcement Server:

Server: secure.ep2p.us

Ports:

TCP Port: 6881 DHT (UDP) Port: 21060 Enable DHT

# Torrential Downpour Receptor



# Torrential Downpour Receptor

Torrential Downpour Receptor Configuration

Locations Options Investigator Advanced

Identification:

Name:  Email:

License:

Mail Server (optional):

Host:  Port:   Use SSL

Login:  Password:  Confirm:

Alternate Email (optional):   Notify both addresses

# Torrential Downpour Receptor

Torrential Downpour Receptor Configuration

Locations Options Investigator Advanced

Identification:

Name:  Email:

License:

Mail Server (optional):

Host:  Port:   Use SSL

Login:  Password:  Confirm:

Alternate Email (optional):   Notify both addresses

# Torrential Downpour Receptor

Torrential Downpour Receptor Configuration

Locations Options Investigator **Advanced**

Handshake Version:

#0D40- (libTorrent 0.13.4)

GeoIP-City Updates:

Enable Legacy GeoIP URL:

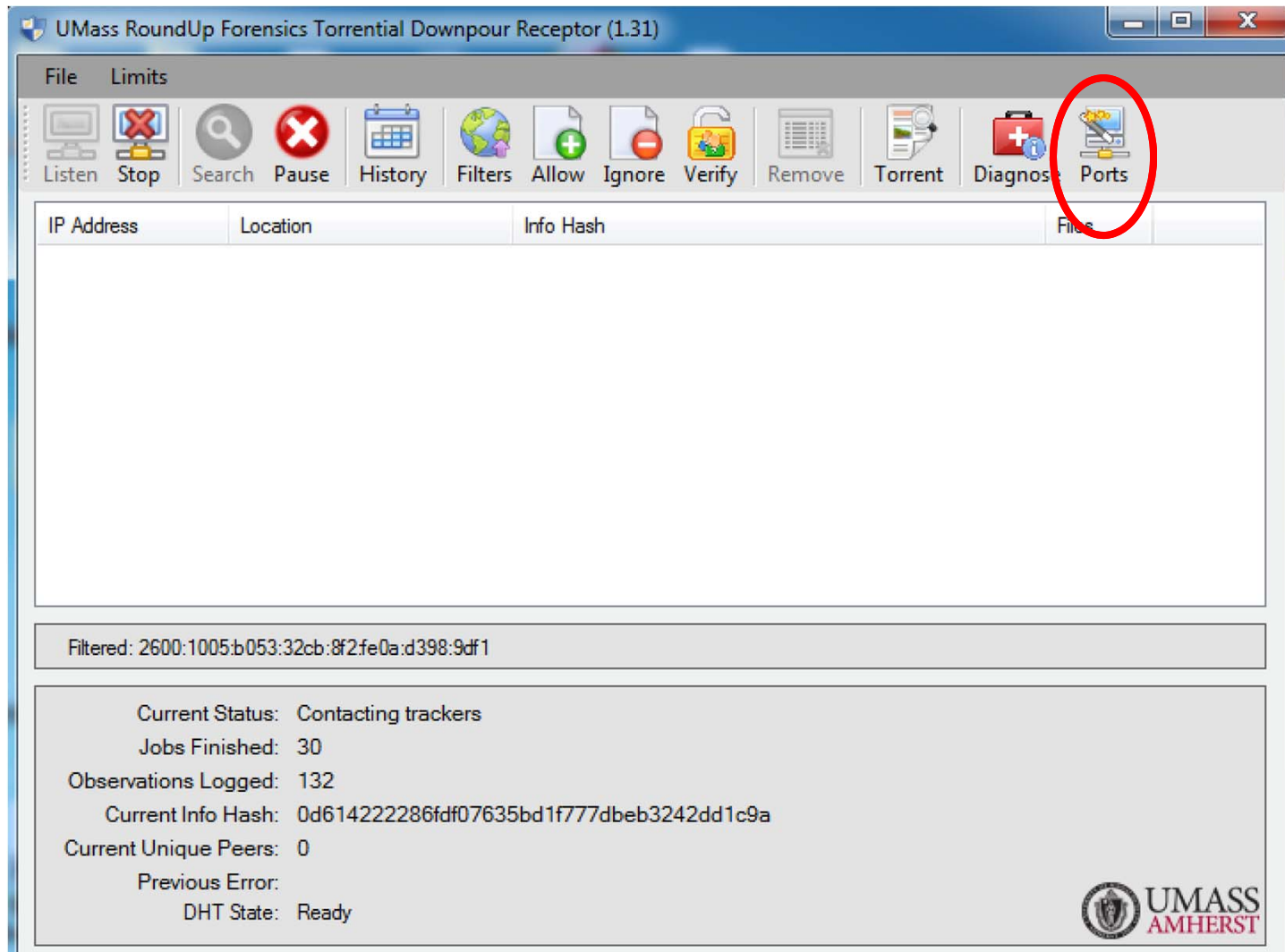
GeoIP2 URL:

Disable use of GeoIP2

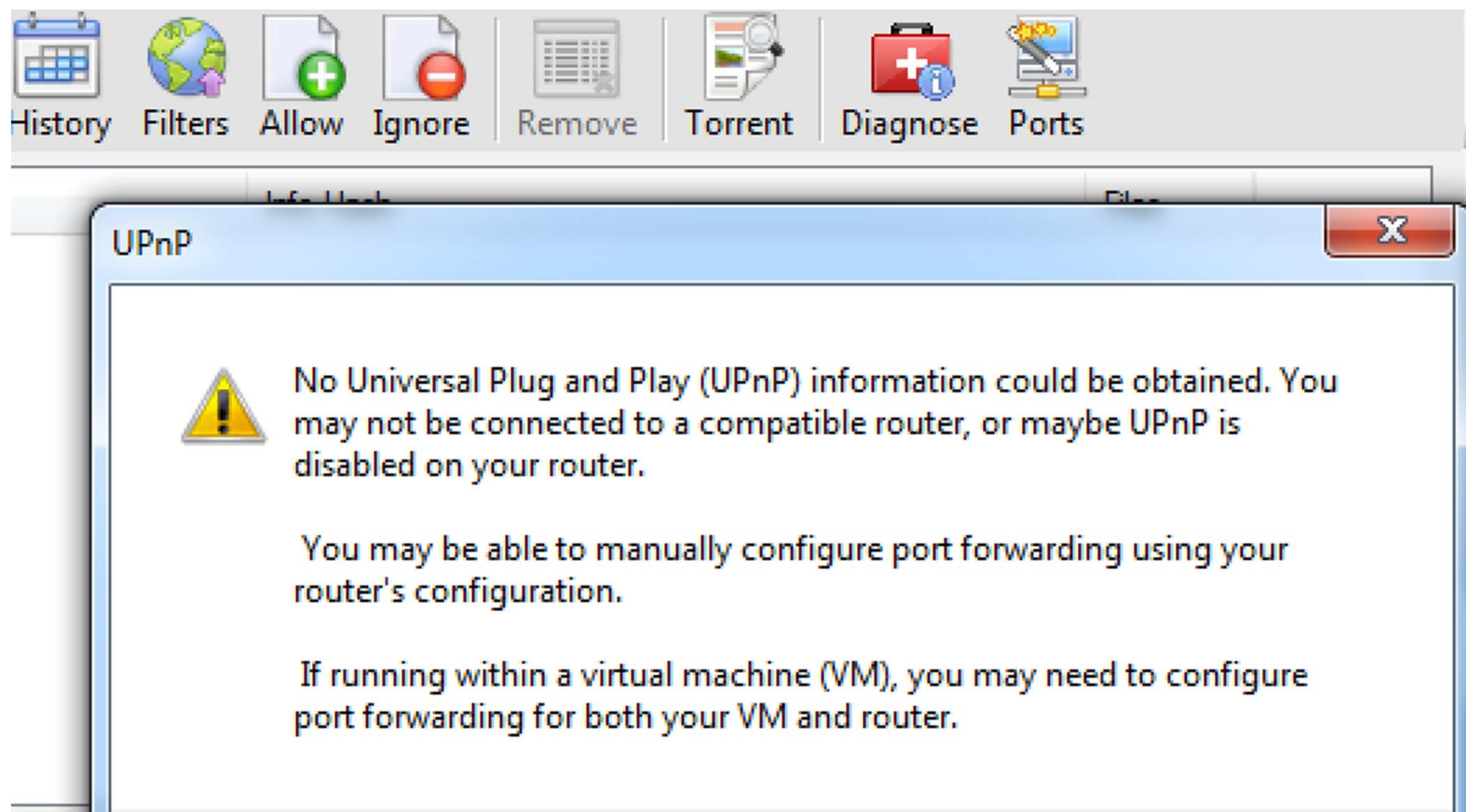
File System:

Maximum directory characters:  Maximum full path characters:

# Torrential Downpour Receptor

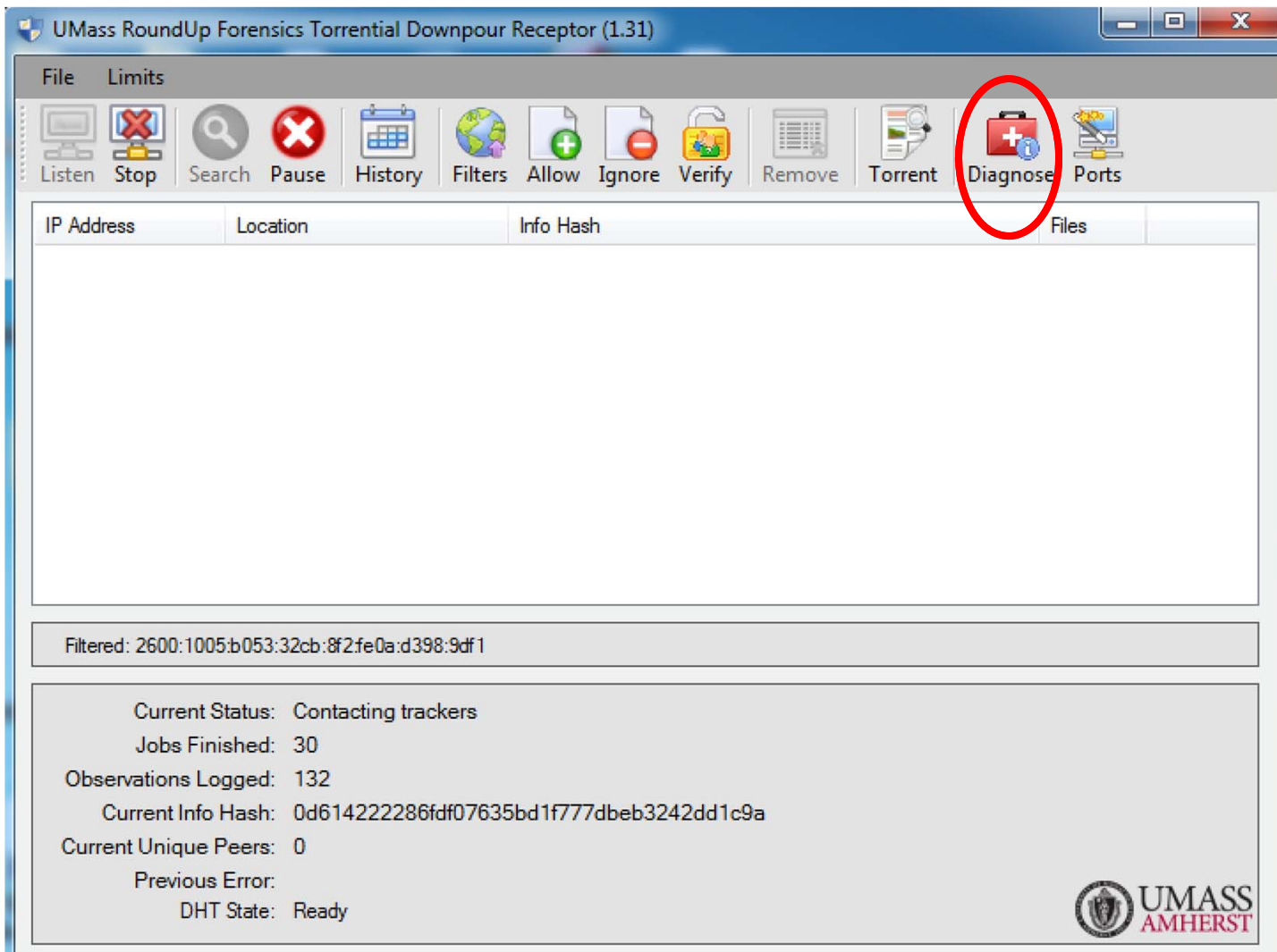


# Torrential Downpour Receptor



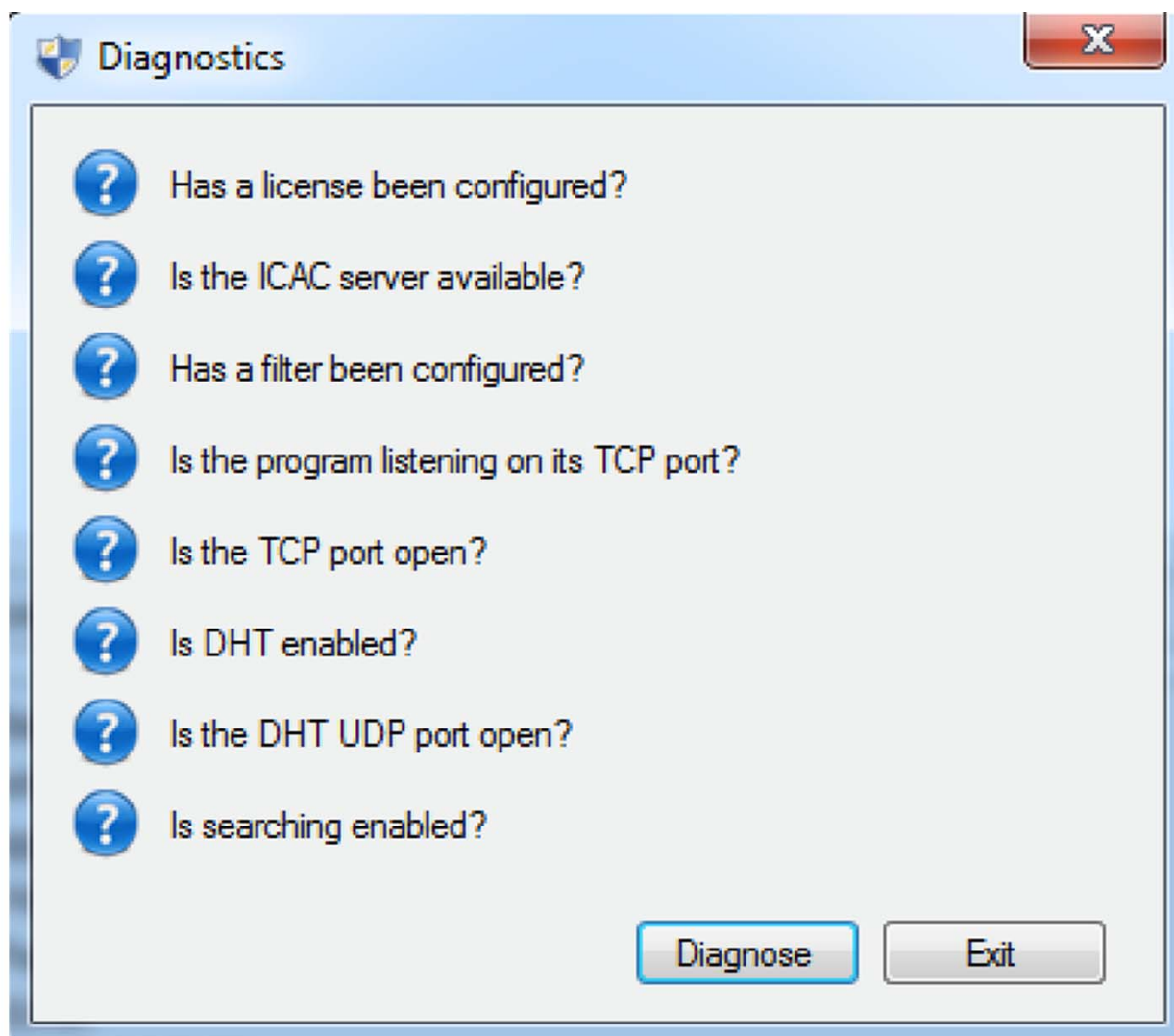


# Torrential Downpour Receptor

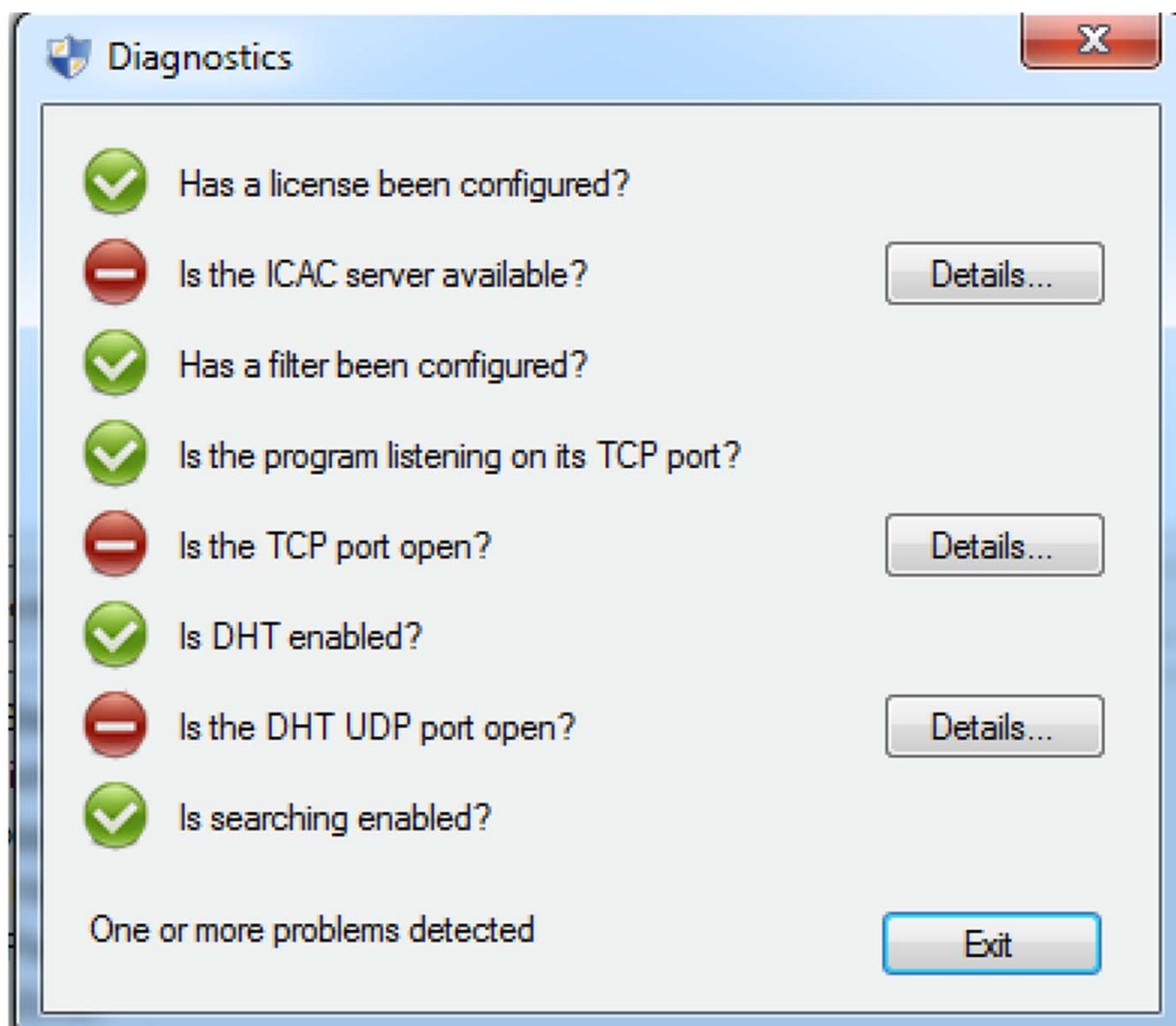


# Torrential Downpour Receptor

---



# Torrential Downpour Receptor





# Questions

# Torrential Downpour Receptor

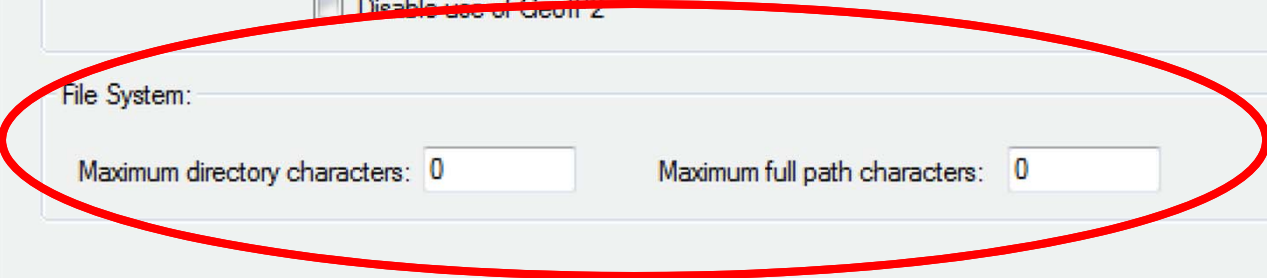
Torrential Downpour Receptor Configuration

Locations Options Investigator **Advanced**

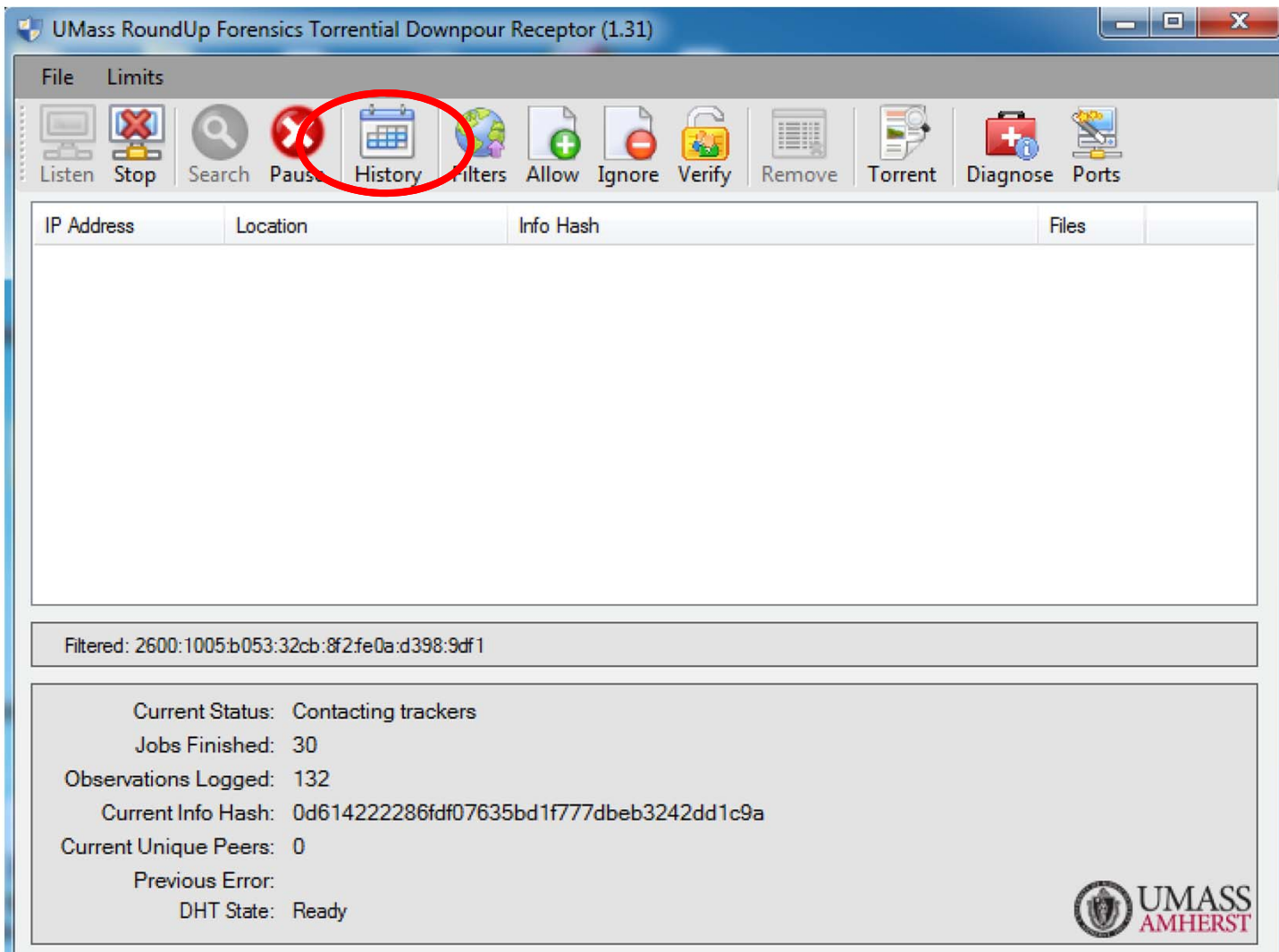
Handshake Version:  
 -t0D40- (libTorrent 0.13.4)

GeoIP-City Updates:  
 Enable Legacy GeoIP URL:   
GeoIP2 URL:   
 Disable use of GeoIP2

File System:  
Maximum directory characters:  Maximum full path characters:



# Torrential Downpour Receptor



# Torrential Downpour / Receptor

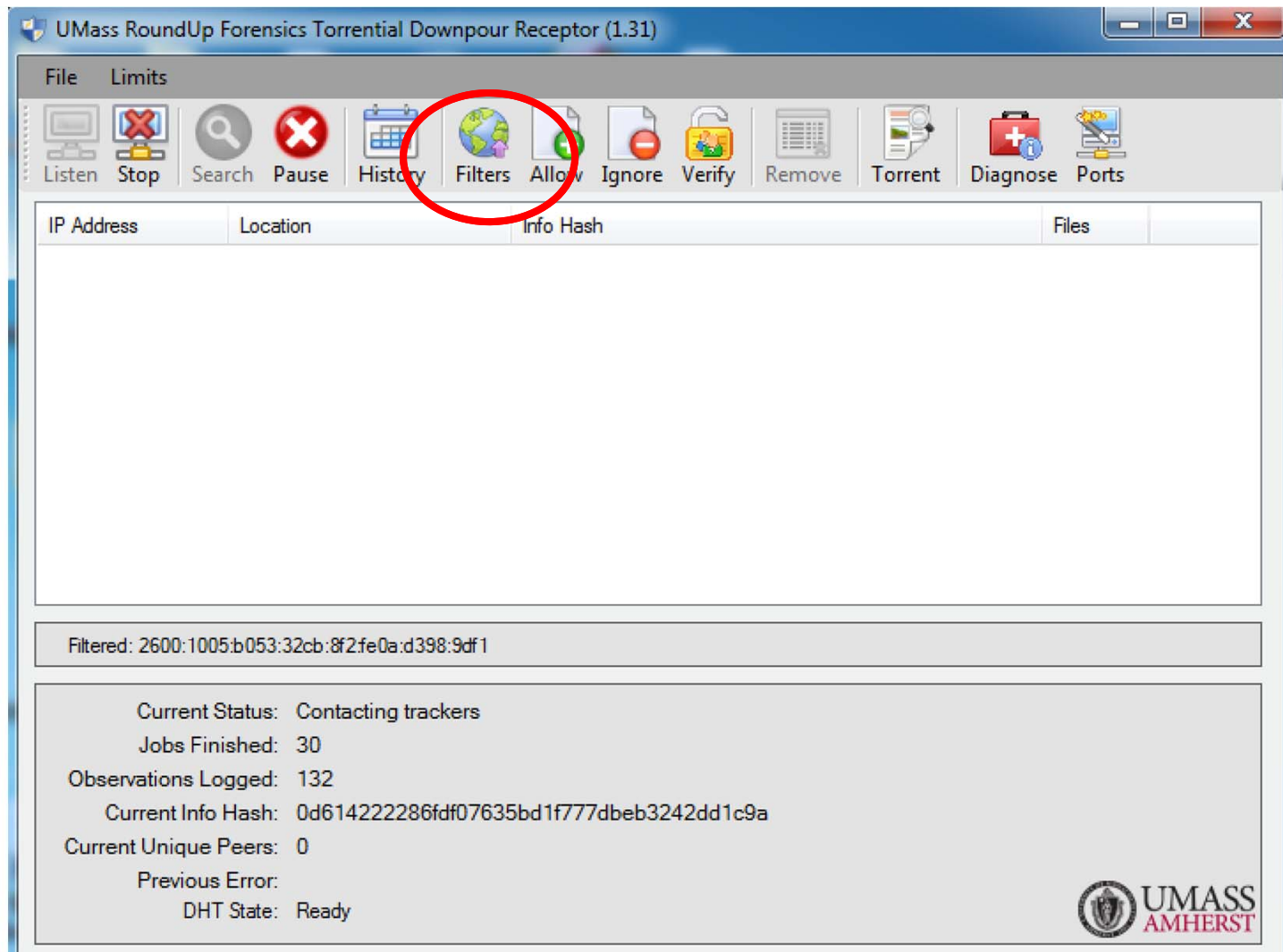
Download History (Last refreshed 3/9/2016 8:47:12 AM. Excludes current active and pending downloads.)

File Tools Search

Pittsburgh ✓

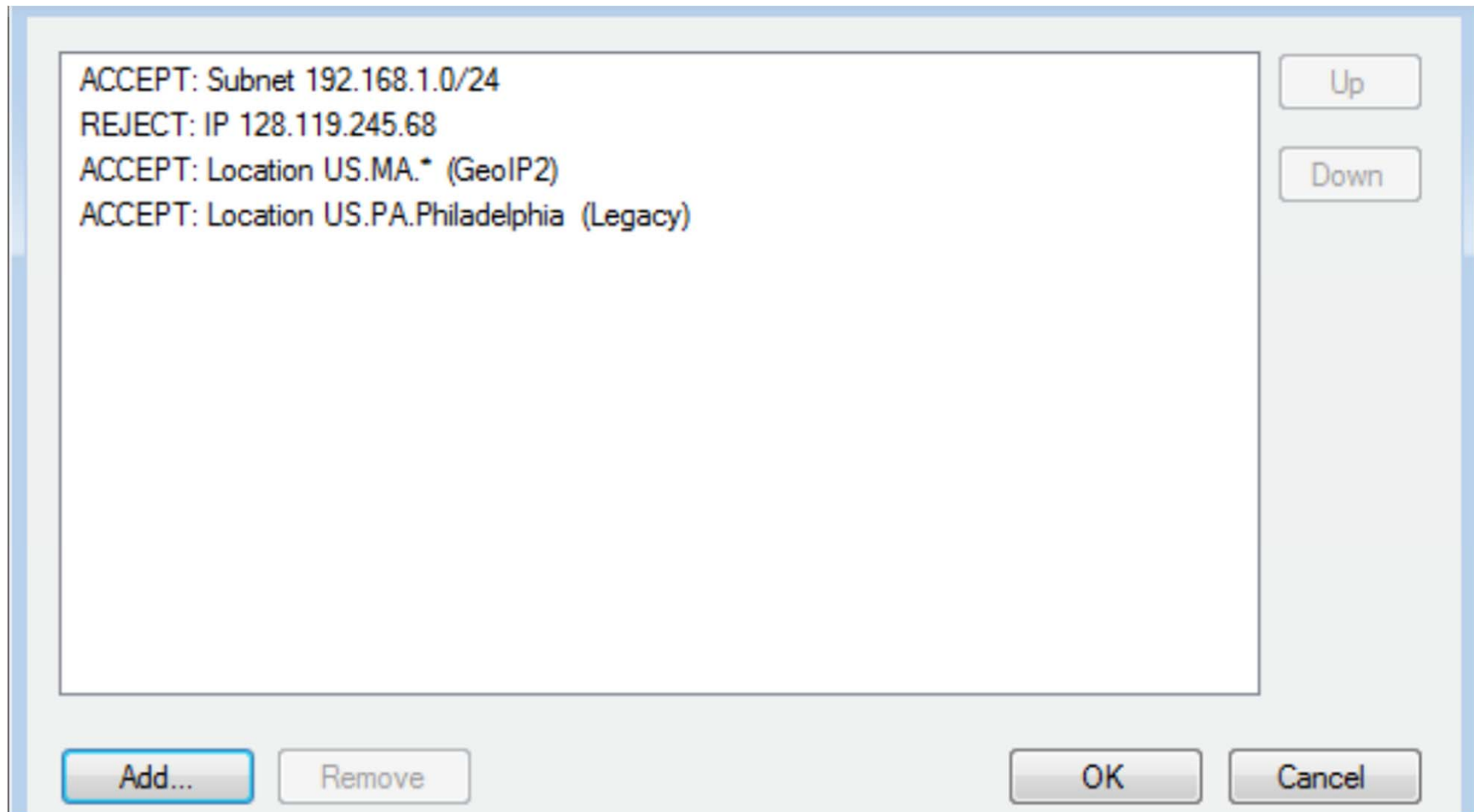
| Location         | Client               | Status   | Pieces | Acked | Written | Files | Completed | Started          | Stopped          |
|------------------|----------------------|----------|--------|-------|---------|-------|-----------|------------------|------------------|
| US.PA.Pittsburgh | 50.254.196.133:23874 | Finished | 248    | 248   | 248     | 9     | 9         | 2016-03-09 08:46 | 2016-03-09 08:46 |
|                  |                      |          |        |       |         |       |           |                  |                  |
|                  |                      |          |        |       |         |       |           |                  |                  |

# Torrential Downpour Receptor





# Torrential Downpour Receptor



# Torrential Downpour Receptor

**Add Filter**

**Location:**

Country:

Region:

Cities:  All  Single  Multiple

**Coordinates:**

Country:

Region:

Latitude:  Longitude:

Distance:   Miles  Kilometers

**Type:**

Location  Coordinates  Military

IP Address  Everything

**Geo Location Database:**

GeoIP2  GeoIP Legacy

**Action:**

Accept  Reject

**Notification:**

Send alert after handshake

# Torrential Downpour Receptor

www.latlong.net

To make a search, use the name of a place, city, state, or address, or click the lo

Place Name


Indiana, pa

Add the country code for better results. Ex: London, UK

Latitude

Longitude

Share On





# Questions

# Torrential Downpour Receptor

**Add Filter**

**Location:**  
Country:   
Region:   
Cities:  All  Single  Multiple

**Coordinates:**  
Country:   
Region:   
Latitude:  Longitude:   
Distance:   Miles  Kilometers

**Military:**  
Country:   
Region:   
Represented Country:

**Type:**  
 Location  Coordinates  Military  
 IP Address  Everything

**Geo Location Database:**  
 GeoIP2  GeoIP Legacy

**Action:**  
 Accept  Reject

**Notification:**  
 Send alert after handshake

# Torrential Downpour Receptor

---

Military:

Country: JP (Japan)

Region:

Represented Country: US (United States)

# Torrential Downpour Receptor

**Add Filter** [www.sitings.com](http://www.sitings.com)

**Location:**  
Country:   
Region:    
Cities:  All  Single  Multiple

**Coordinates:**  
Country:   
Region:    
Latitude:  Longitude:   
Distance:   Miles  Kilometers

**Military:**  
Country:   
Region:    
Represented Country:

**IP Address, Range, or IP Address / Subnet Bits (CIDR):**

**Type:**  
 Location  Coordinates  Military  
 IP Address  Everything

**Geo Location Database:**  
 GeoIP2  GeoIP Legacy

**Action:**  
 Accept  Reject

**Notification:**  
 Send alert after handshake

# Torrential Downpour Receptor

---

IP Address, Range, or IP Address / Subnet Bits (CIDR):

24.24.24.24 - 24.24.24.32



# Torrential Downpour Receptor

---

IP Address, Range, or IP Address / Subnet Bits (CIDR):

24.24.24.0/24|

# Torrential Downpour Receptor

---

## Inbound Connection Filters

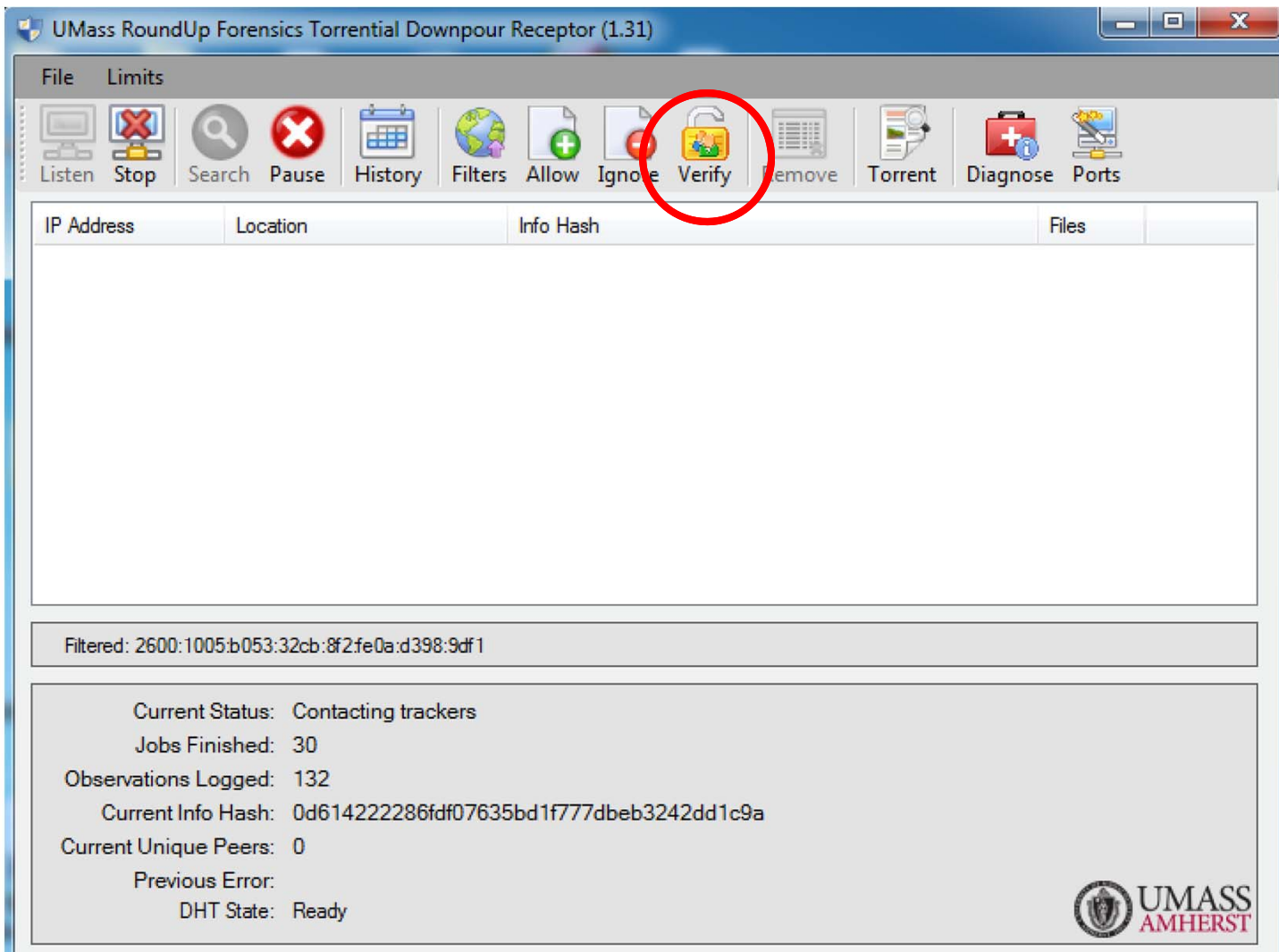
ACCEPT: Subnet 24.24.24.0/24

ACCEPT: Range 24.24.24.24 – 24.24.24.30

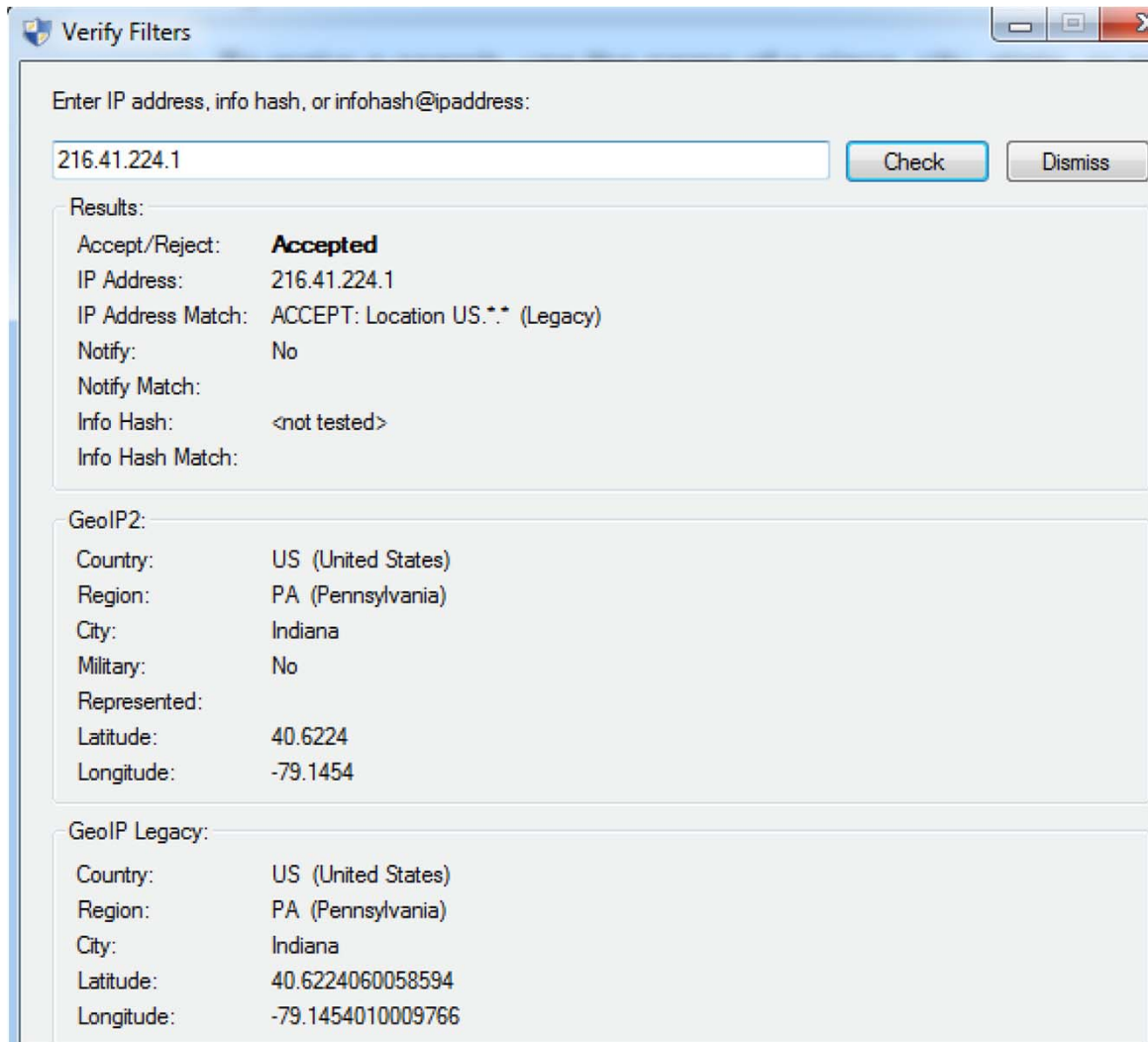
ACCEPT: IP 24.24.24.24

ACCEPT: Location US.\*.\* (Legacy)

# Torrential Downpour Receptor



# Torrential Downpour Receptor



Verify Filters

Enter IP address, info hash, or infohash@ipaddress:

216.41.224.1

Results:

|                   |                                |
|-------------------|--------------------------------|
| Accept/Reject:    | <b>Accepted</b>                |
| IP Address:       | 216.41.224.1                   |
| IP Address Match: | ACCEPT: Location US.* (Legacy) |
| Notify:           | No                             |
| Notify Match:     |                                |
| Info Hash:        | <not tested>                   |
| Info Hash Match:  |                                |

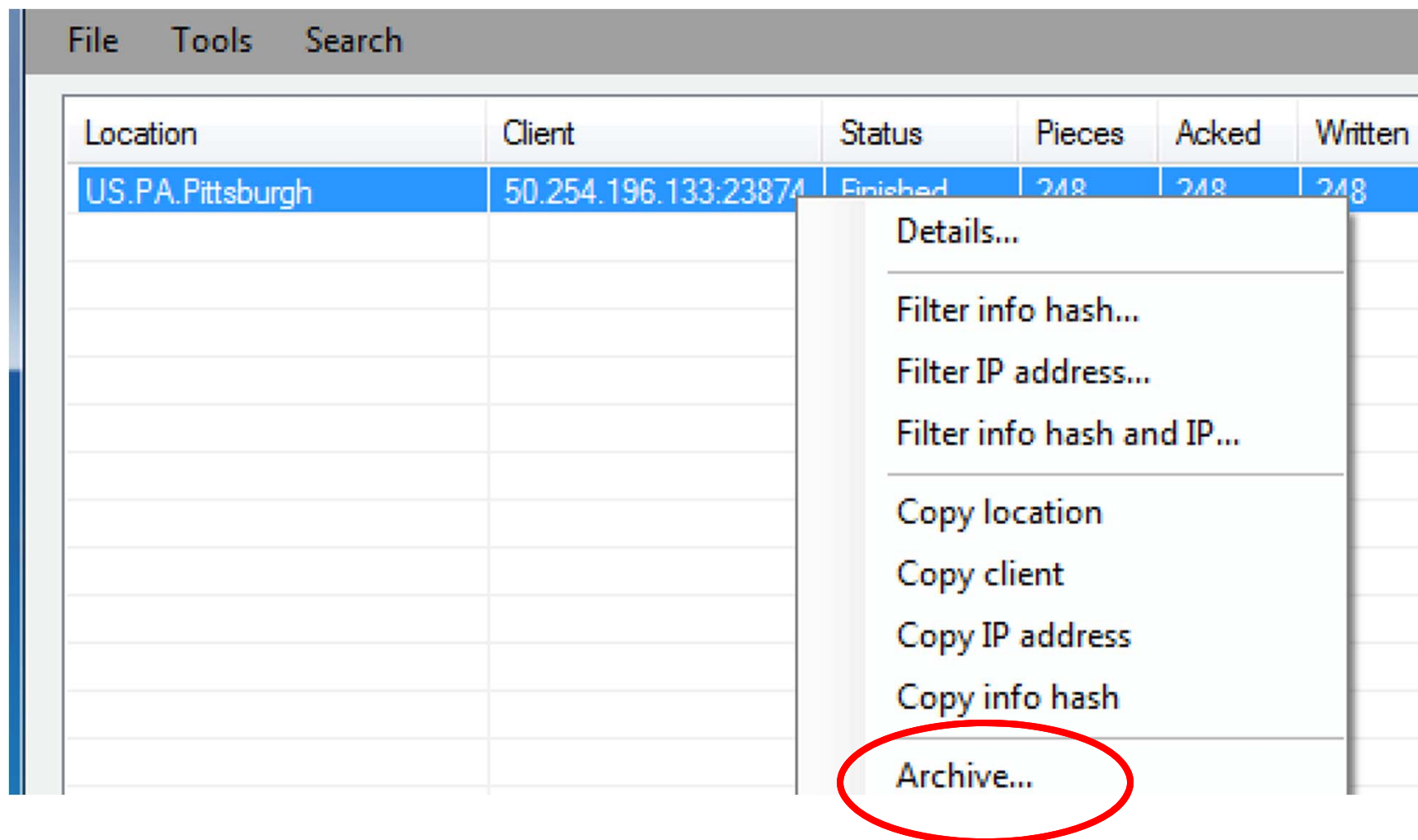
GeoIP2:

|              |                    |
|--------------|--------------------|
| Country:     | US (United States) |
| Region:      | PA (Pennsylvania)  |
| City:        | Indiana            |
| Military:    | No                 |
| Represented: |                    |
| Latitude:    | 40.6224            |
| Longitude:   | -79.1454           |

GeoIP Legacy:

|            |                    |
|------------|--------------------|
| Country:   | US (United States) |
| Region:    | PA (Pennsylvania)  |
| City:      | Indiana            |
| Latitude:  | 40.6224060058594   |
| Longitude: | -79.1454010009766  |

# Torrential Downpour / Receptor



| Location         | Client               | Status   | Pieces | Acked | Written |
|------------------|----------------------|----------|--------|-------|---------|
| US.PA.Pittsburgh | 50.254.196.133:23874 | Finished | 248    | 248   | 248     |
|                  |                      |          |        |       |         |
|                  |                      |          |        |       |         |
|                  |                      |          |        |       |         |
|                  |                      |          |        |       |         |
|                  |                      |          |        |       |         |
|                  |                      |          |        |       |         |
|                  |                      |          |        |       |         |
|                  |                      |          |        |       |         |
|                  |                      |          |        |       |         |
|                  |                      |          |        |       |         |

- Details...
- Filter info hash...
- Filter IP address...
- Filter info hash and IP...
- Copy location
- Copy client
- Copy IP address
- Copy info hash
- Archive...





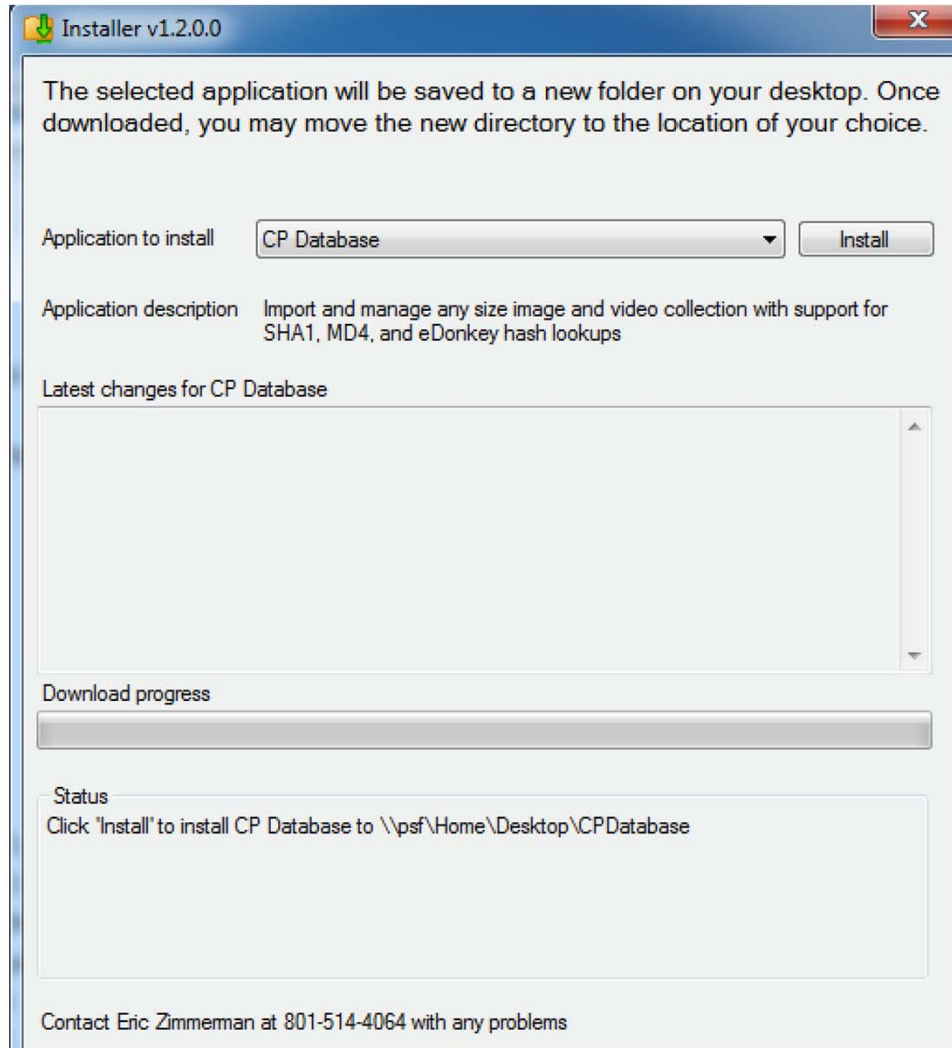
# Questions

# Image Library

The screenshot shows a web browser window with the address bar containing the URL <https://feeble-industries.com/forums/>. The browser's bookmark bar includes entries for "EZTV - TV Torrents", "Megan's Law Public", and "Tourist V". The main content area features a blue header with the phpBB logo and the text "FEEBLE Industries Anything but...". Below the header, there are navigation links for "Quick links" and "FAQ", and a "Board index" link with a home icon.

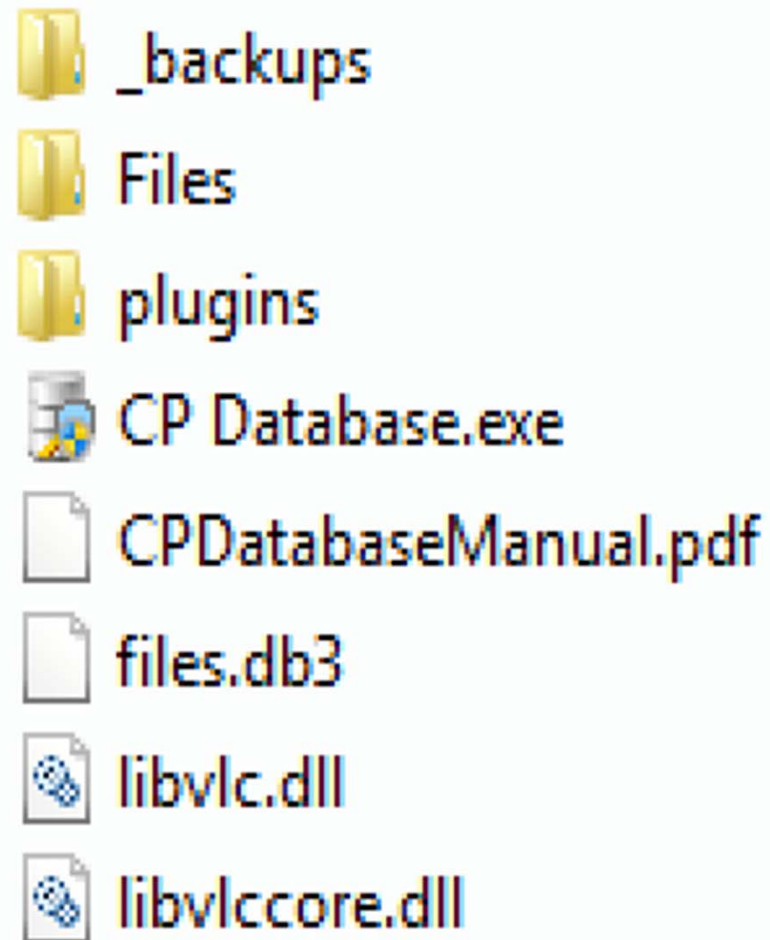


# Image Library

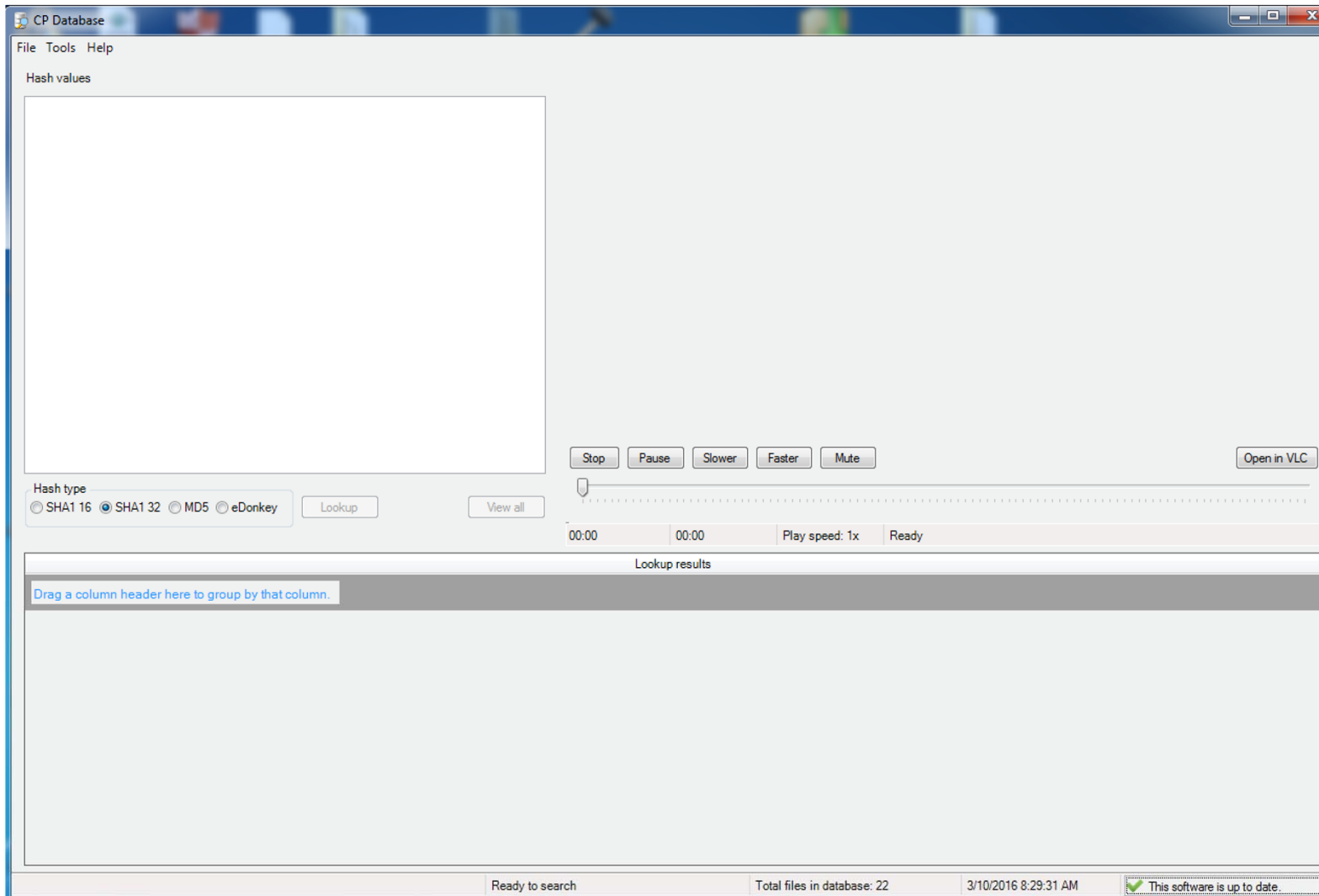


# Image Library

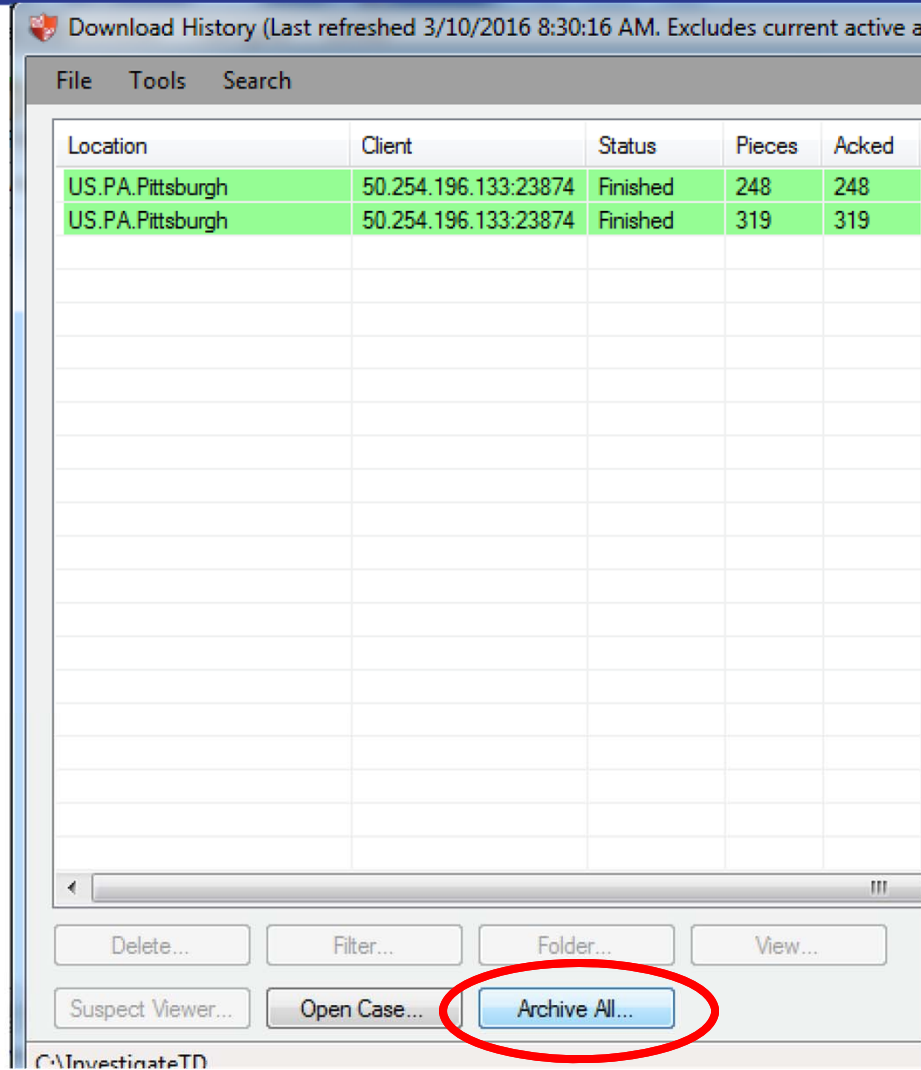
---



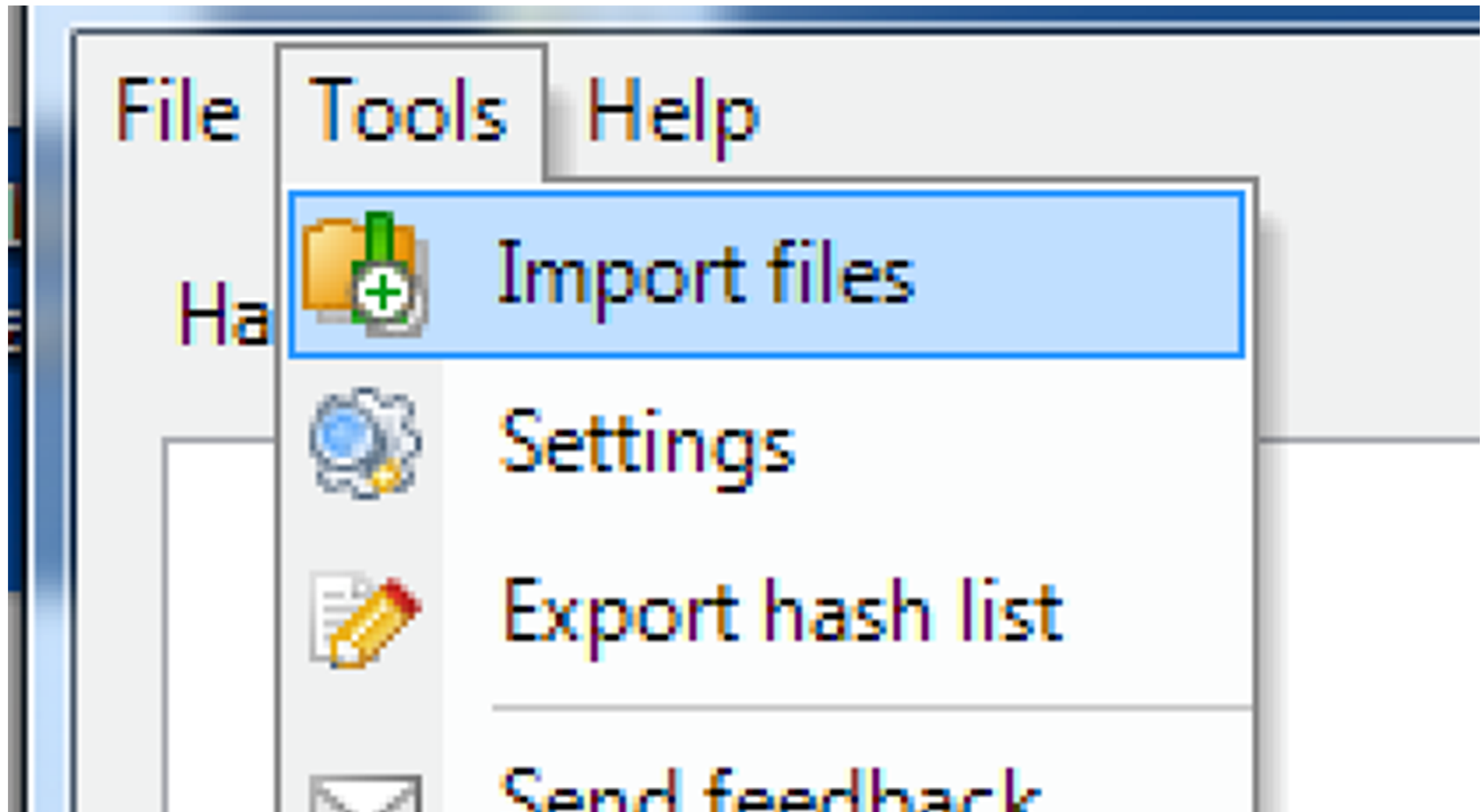
# Image Library



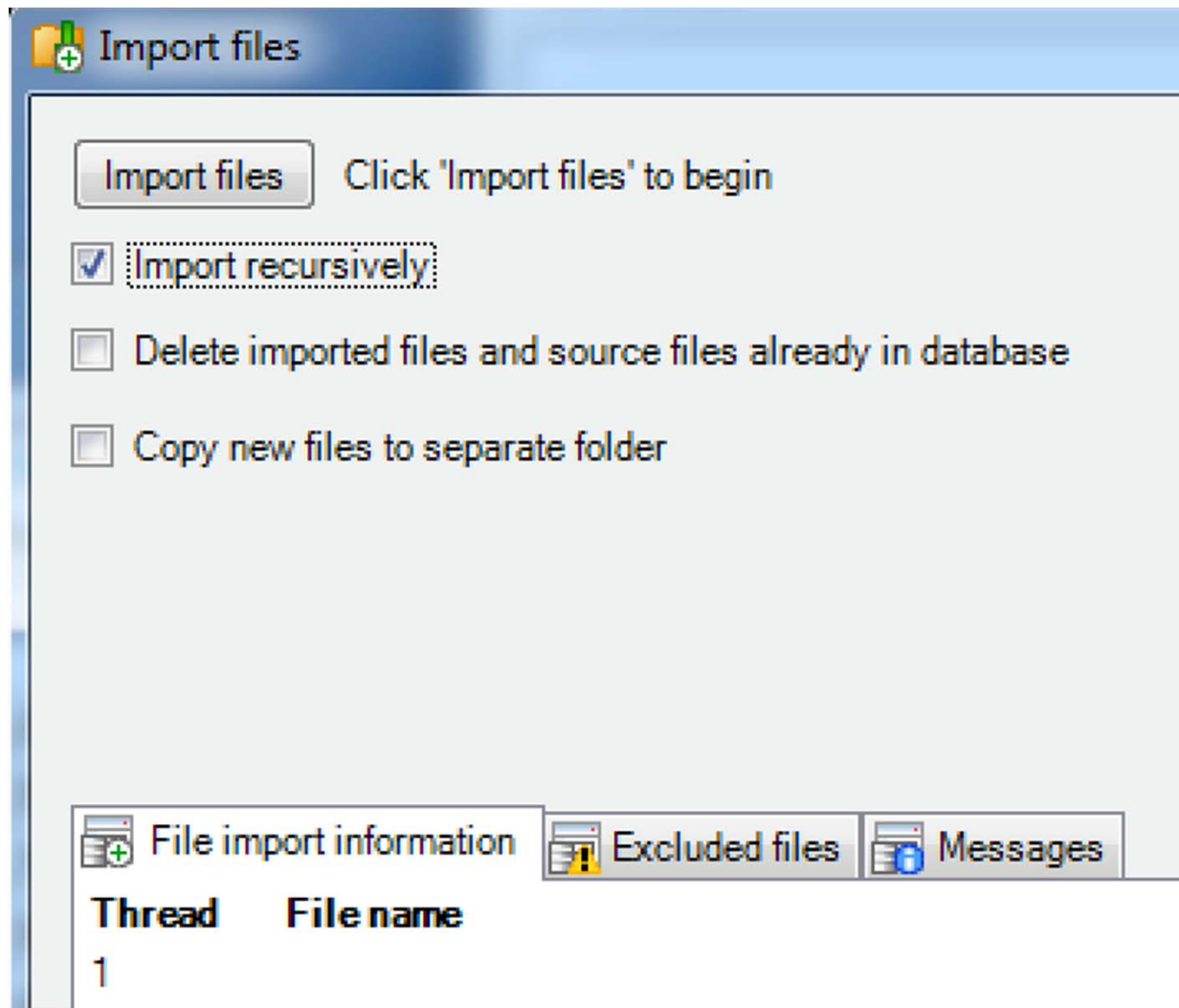
# Image Library



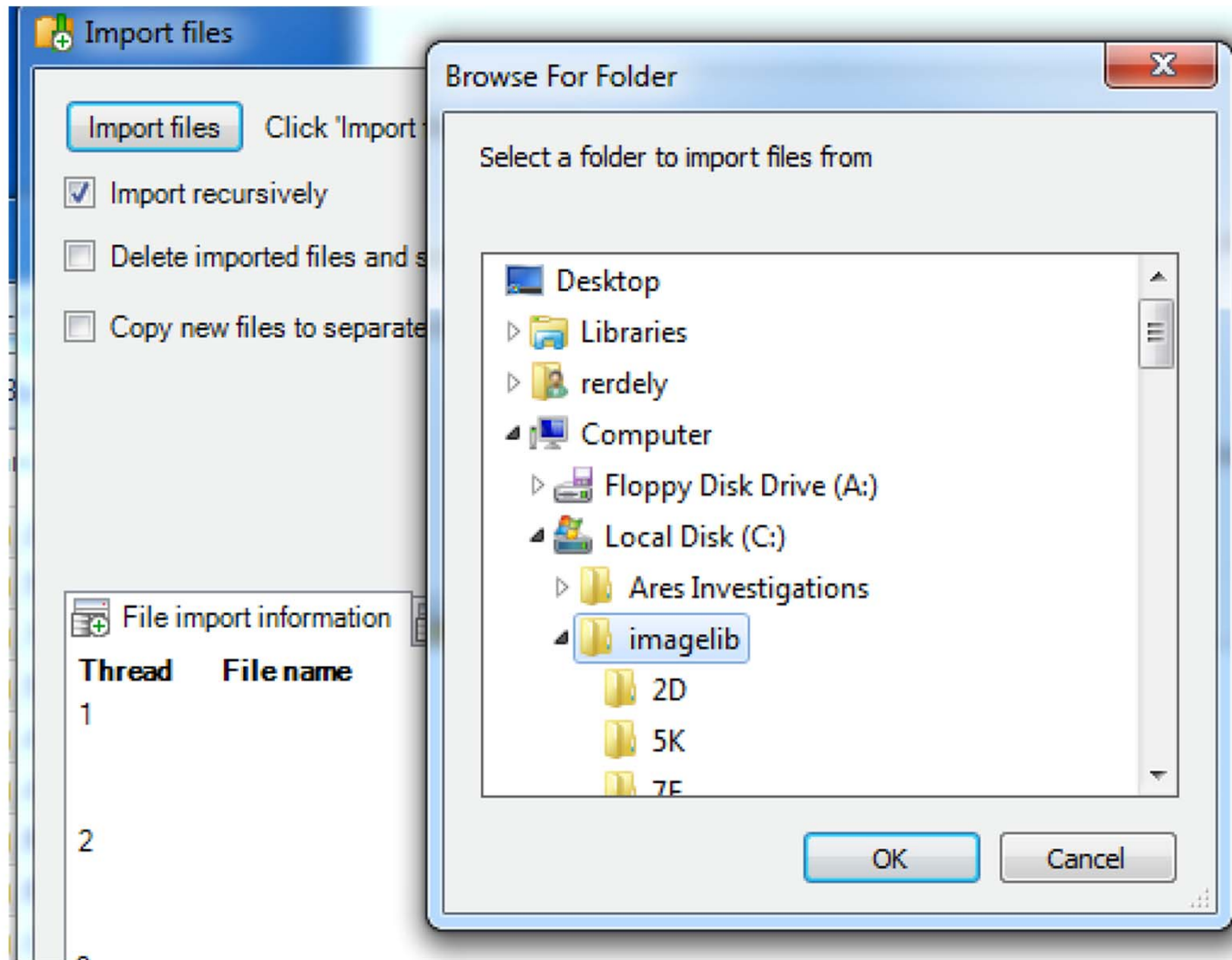
# Image Library



# Image Library



# Image Library



# Image Library

---



## Ready to import

Files found: 20

Total file size (MB): 9.06

The following settings will be used:

Recursive import: True

Delete existing and/or imported files: False

Copy new files to separate folder: False




# Image Library

Hash values

```
5KZE00EHYTVXYCT6VEKTM6ZLV75XM4KB  
2DSIQWUJINBKE7YG4BD75INSKGL3YID
```

Hash type  
 SHA1 16  SHA1 32  MD5  eDonkey



UNREGISTERED  
downloadhelper.net

Stop Pause Slower Faster Mute

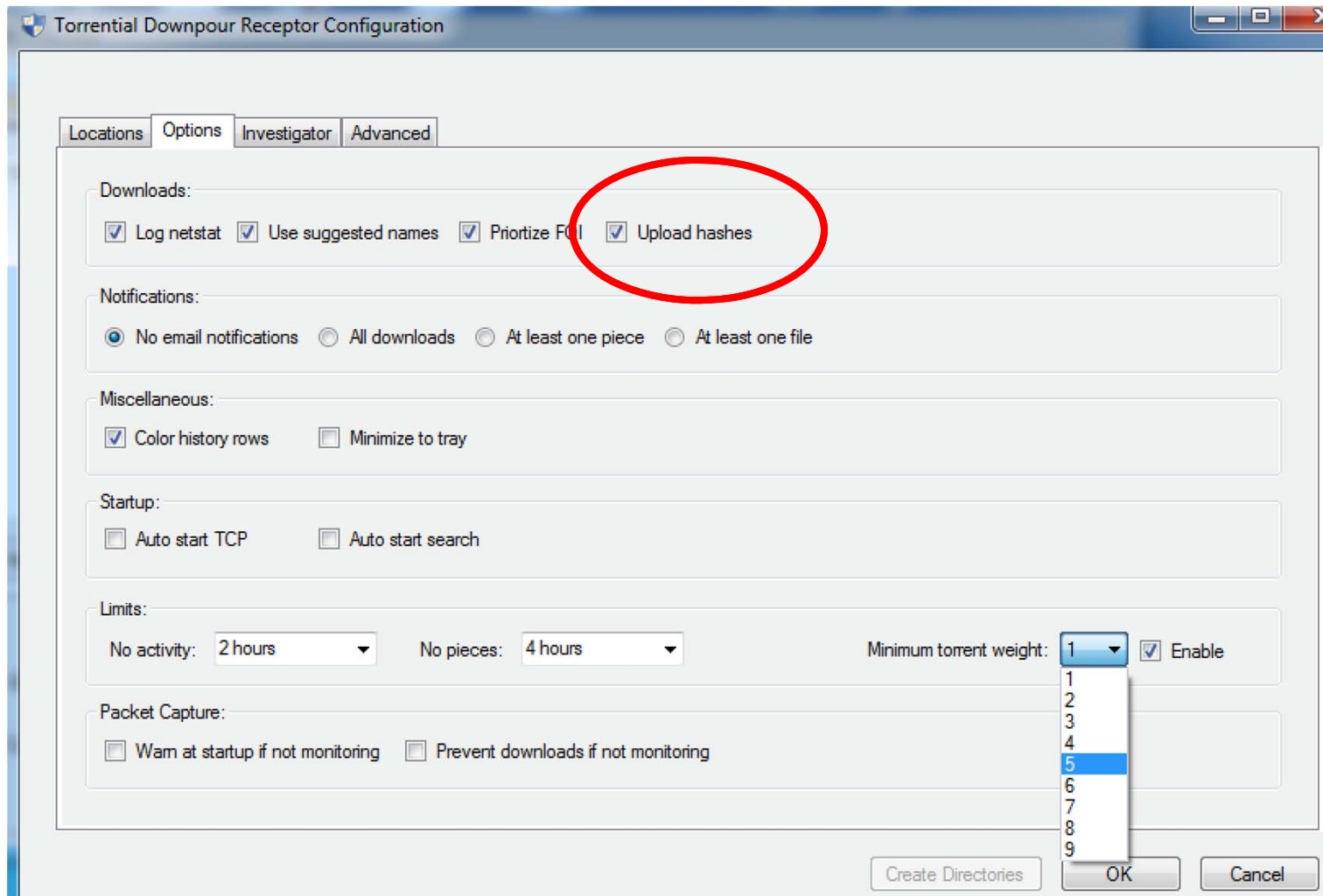
00:00:33 00:02:38 Play speed: 1x Playing

Lookup results

Drag a column header here to group by that column.

| SHA1 Base 16   | SHA1 Base 32  | eDonkey  | MD5  |
|--|---|--|--|
| <input type="checkbox"/> <input type="checkbox"/> EAB2A73287C4E87C0A7EA915367B2BAE8E767141 | <input type="checkbox"/> 5KZE00EHYTVXYCT6VEKTM6ZLV75XM4KB | <input type="checkbox"/> 1A18BEA87A0D26E8C41460C2589708B | <input type="checkbox"/> 5DE1029CD627AA2AAAC79751E0E2E2F |

# Torrential Downpour Receptor



# Torrential Downpour / Receptor

|                                   | FOI? | Sha1   | Md5       |
|-----------------------------------|------|--|-----------|
| Cunt (Pthc - 5m45s).mpg           | Yes  | 5a04dd7ed2ae730f715b269ff553b8dab21797b6                 | e19dc717  |
| e 6yo and dad.mpg                 | Yes  | <a href="#">4008122eea74c242bb977053f1df2a4c22805b8c</a> | 85329458  |
|                                   | Yes  | <a href="#">84473718fd96210136e5031bfeff8ea9ddc0c08e</a> | cc1faedbt |
| Sexed 2Yo Cums Hard With          | Yes  | <a href="#">6e24fd17667a4cd3e64a779fa38ab349065ad272</a> | 28a30f9f8 |
| Cum And Wants More {4.5           | Yes  |  |           |
|                                   | Yes  |  |           |
|                                   | No   |  |           |
| ter 2Yo Jenniefer Sofie Verm Suck | Yes  |  |           |

# Torrential Downpour / Receptor

## BitTorrent Downloads

Select Country:

Select Region:

Time Limit:

Select City:

IP Address

Case Opened Search Warrant Executed Arrest Made

= eMule F = Freenet GI = Giga G= Gnutela GB = Gnutella Browse

| nfohash                  | Files | IP Address | DL Date   | Software          | Region | City                      |
|--------------------------|-------|------------|-----------|-------------------|--------|---------------------------|
| <a href="#">cf546...</a> | 4     | 71.10      | 3/10/2016 | µTorrent 3.4.5    | PA     | <a href="#">Kingston</a>  |
| <a href="#">a41da...</a> | 4     | 24.13      | 3/9/2016  | BitLord 2.3.2-254 | PA     | <a href="#">Oil City</a>  |
| <a href="#">a41da...</a> | 3     | 24.13      | 3/9/2016  | BitLord 2.3.2-254 | PA     | <a href="#">Oil City</a>  |
| <a href="#">e48af...</a> | 1     | 74.99      | 3/9/2016  | BitTorrent 7.9.5  | PA     | <a href="#">Mechanic</a>  |
| <a href="#">e48af...</a> | 2     | 74.99      | 3/9/2016  | BitTorrent 7.9.5  | PA     | <a href="#">Mechanic</a>  |
| <a href="#">e48af...</a> | 1     | 74.99      | 3/9/2016  | BitTorrent 7.9.5  | PA     | <a href="#">Mechanic</a>  |
| <a href="#">d1ed7...</a> | 1     | 96.22      | 3/9/2016  | µTorrent 3.1.2    | PA     | <a href="#">Levittown</a> |
| <a href="#">b50c3...</a> | 1     | 96.22      | 3/9/2016  | µTorrent 3.1.2    | PA     | <a href="#">Levittown</a> |
| <a href="#">e7a0e...</a> | 1     | 96.22      | 3/9/2016  | µTorrent 3.1.2    | PA     | <a href="#">Levittown</a> |
| <a href="#">c47c0...</a> | 1     | 96.22      | 3/9/2016  | µTorrent 3.1.2    | PA     | <a href="#">Levittown</a> |

# Torrential Downpour / Receptor

---

| [Opt Out](#) (If you don't want your downloads in this list)

## BitTorrent Downloads

Select Country:

Select Region:

# Additional Information

---

*Points of view or opinions expressed in this webinar are those of the presenter(s) and do not necessarily represent the official position or policies of OJJDP or the U.S. Department of Justice.*