Bittorrent over Tor: a bad idea? A scientific controversy revisited.

Camille Akmut

April 8, 2020

Abstract

Ten years ago "Bittorrent over Tor isn't a good idea" was published by the Tor Project. A technical discussion of Bittorrent over Tor is followed by a more general, philosophical one on privacy's goals.

Introduction

1

10 years ago, in April, Roger Dingledine under his pseudonym "arma" wrote *Bittorrent over Tor isn't a good idea* — an official Tor Project communication that would set the tone for an entire decade.

Researchers at INRIA had just published a paper on de-anynomyzing Tor and BitTorrent users : This would now serve as a scientific – not merely ethical – justification for discouraging such filesharing uses of the overlay network.

Matters related to these topics were now frowned upon, and this blog post and study were soon regularly referenced;

A scientific and social impermissible had been created.

2

It remains that questions that are not asked can not be answered; And, discussions that are never opened can not be closed.

Tor was a "privacy enhancing" technology, but not for all users, and not for all uses – this much became clear in these early stages.

3

In a first section, we offer a first, technical, but non-expert overview of Bittorrent over Tor.

We ask : Is Bittorrent over Tor possible? Is it secure?

We answer : Yes, and probably yes.

4

Extreme scarcity of resources or documentation, which in the view of this author can be directly traced back to the official position of the Tor project, made this project hard, and necessary.

Virtually every discussion on the topic encountered was abruptly ended by contributors relying on arguments of various nature.

5

"Noble" and "dirty" causes – this false dichotomy at the foundation of so many privacy activists' unthought thoughts – is the subject of section two.

Privacy's most important beneficiaries are average people, we argue.

"*the many who –though having a knowledge of their own abilities– accept the dominant system inside of their heads, and by their actions, reinforcing it, and indeed substantiating it.*"

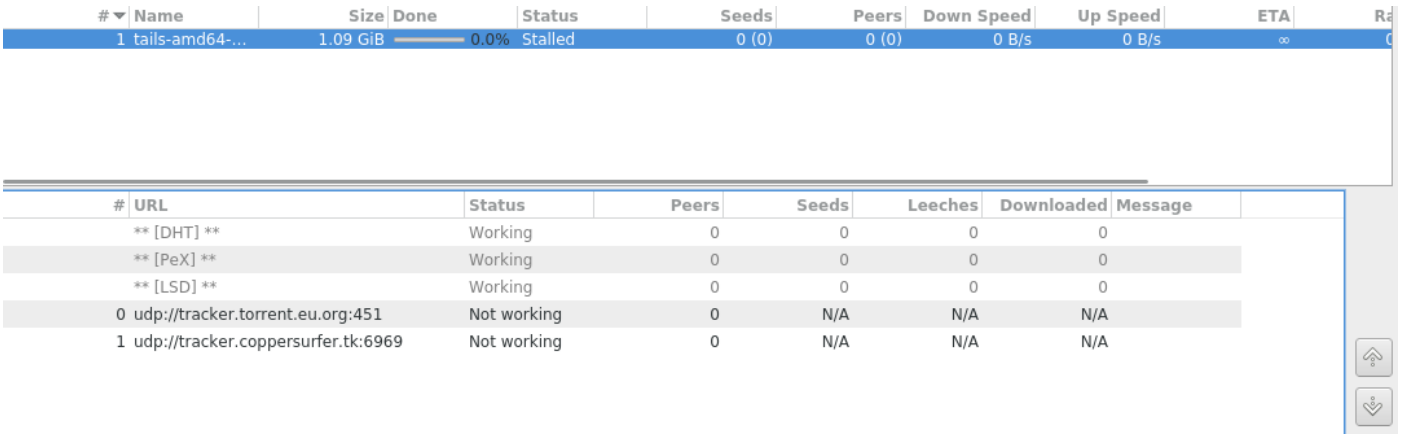
Effi Briest by Fassbinder, a (most likely) copyrighted film. Trans..

1. Conditions

In total, we experimented with BitTorrent over Tor on three different systems : 1. a standard Whonix installation, 2. Tails (running on a virtual machine) and 3. a standard Debian installation, with firewall (also).

An official Ubuntu image as well as a non-recent media, from a fairly mainstream torrent index, were downloaded — in order to make these experiments not only representative of average users and uses but also to enable reproducibility (the latter would ideally not have copyright holders).

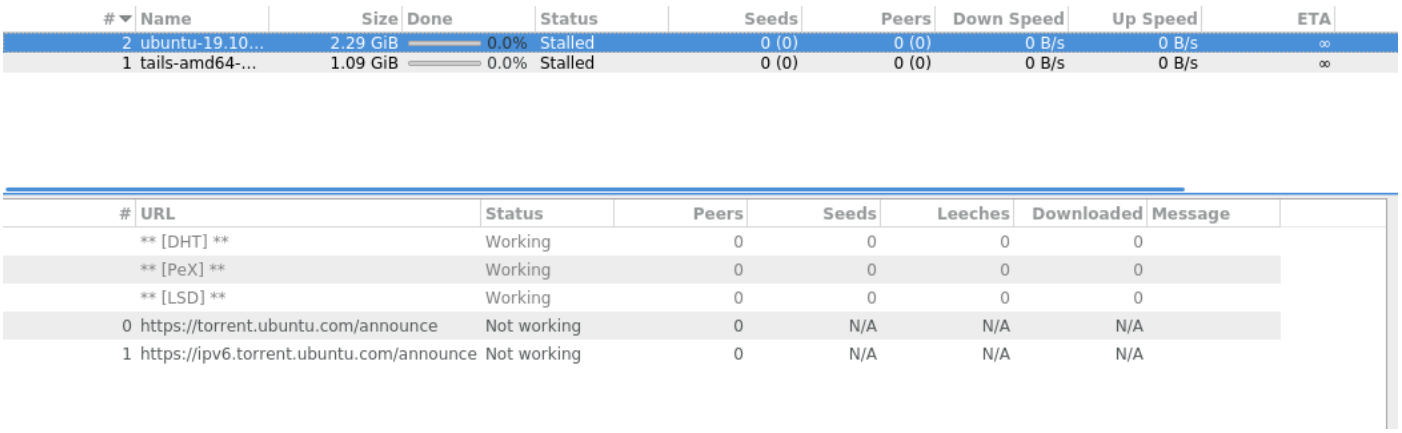
2. Tails



#	Name	Size	Done	Status	Seeds	Peers	Down Speed	Up Speed	ETA
1	tails-amd64-...	1.09 GiB	0.0%	Stalled	0 (0)	0 (0)	0 B/s	0 B/s	∞

#	URL	Status	Peers	Seeds	Leeches	Downloaded	Message
	** [DHT] **	Working	0	0	0	0	
	** [PeX] **	Working	0	0	0	0	
	** [LSD] **	Working	0	0	0	0	
0	udp://tracker.torrent.eu.org:451	Not working	0	N/A	N/A	N/A	
1	udp://tracker.coppersurfer.tk:6969	Not working	0	N/A	N/A	N/A	

Figure 1. Tails, and BitTorrent client not configured.



#	Name	Size	Done	Status	Seeds	Peers	Down Speed	Up Speed	ETA
2	ubuntu-19.10...	2.29 GiB	0.0%	Stalled	0 (0)	0 (0)	0 B/s	0 B/s	∞
1	tails-amd64-...	1.09 GiB	0.0%	Stalled	0 (0)	0 (0)	0 B/s	0 B/s	∞

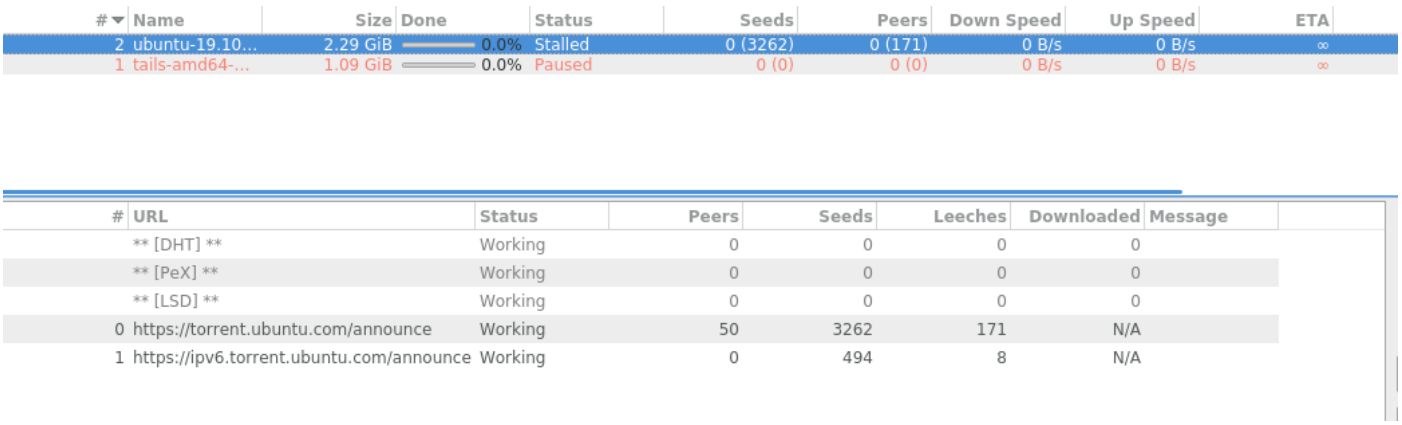
#	URL	Status	Peers	Seeds	Leeches	Downloaded	Message
	** [DHT] **	Working	0	0	0	0	
	** [PeX] **	Working	0	0	0	0	
	** [LSD] **	Working	0	0	0	0	
0	https://torrent.ubuntu.com/announce	Not working	0	N/A	N/A	N/A	
1	https://ipv6.torrent.ubuntu.com/announce	Not working	0	N/A	N/A	N/A	

Figure 2. … with HTTP trackers.

The above shows what a user of Tails upon installing a BitTorrent client with no further configuration would face.

The client can neither connect to trackers (“*Not working*“) nor has seeds/peers (as made clear by the notification “*0 (0)*“, in both cases).

In the next figure, we configure the BitTorrent client so as to use the tor proxy (127.0.0.1:9050).



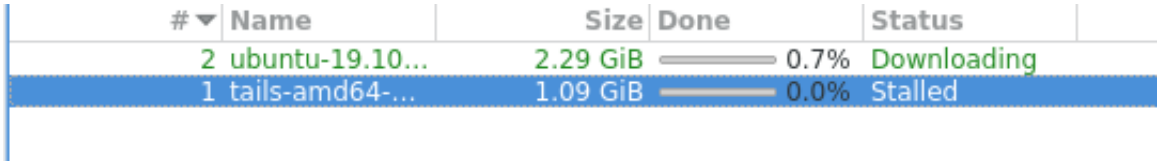
#	Name	Size	Done	Status	Seeds	Peers	Down Speed	Up Speed	ETA
2	ubuntu-19.10...	2.29 GiB	0.0%	Stalled	0 (3262)	0 (171)	0 B/s	0 B/s	∞
1	tails-amd64-...	1.09 GiB	0.0%	Paused	0 (0)	0 (0)	0 B/s	0 B/s	∞

#	URL	Status	Peers	Seeds	Leeches	Downloaded	Message
	** [DHT] **	Working	0	0	0	0	
	** [PeX] **	Working	0	0	0	0	
	** [LSD] **	Working	0	0	0	0	
0	https://torrent.ubuntu.com/announce	Working	50	3262	171	N/A	
1	https://ipv6.torrent.ubuntu.com/announce	Working	0	494	8	N/A	

Figure 3. Tails, BitTorrent client configured for tor proxy (trackers only).

This particular BitTorrent client has the quirk of only proxying trackers but not peer connections, by default, unless an additional option is checked - resulting in figure 4.

(This was what the first attack relied on, but this client blocked everything else because we enabled “Anonymous mode” : from the libtorrent mailing list, a library on which this client is based like many others, we knew that this enforced a strict mode on proxies.)



#	Name	Size	Done	Status
2	ubuntu-19.10...	2.29 GiB	0.7%	Downloading
1	tails-amd64-...	1.09 GiB	0.0%	Stalled

Figure 4. Tails, BitTorrent client configured for tor proxy (trackers + peer connections).

Note that here only the Ubuntu image is being downloaded, while the Tails image is stalled : we can conclude this is due to the sole presence of UDP trackers (while the former has http/s ones).

Tor is a TCP overlay network with limited capacities for UDP (for DNS management).

The qbittorrent logs showed not the actual IP as “External IP” but one of a Tor node.

The “Peers” swarm overview also did not contain the actual IP of the host.

Further, we did not notice any abnormal speeds.

However, under Tails’ “Onion Circuits” a very great number of circuits appeared continuously : a new one was created for every peer connection?

This might be worrying, and to our knowledge has already been reported once.

“tcpdump -n udp” revealed UDP network activity, but the IP’s involved appeared to be the internal ones used by the virtualization software (e.g. 10.0.2 …).

It is unclear to us whether this UDP traffic ever reached outside.

(Throughout these tests, we required encrypted traffic only. We make this annotation in case this has some relevancy.)

3. Whonix

Torrenting in Whonix functioned without any modification.

Neither the log's "External IP" entry nor the peer overview exposed the user's actual IP.

The maintainer has repeatedly claimed that torrenting on Whonix should be safe.

"*Whonix doesn't really care if DHT or whatever. DHT usually apparently is just UDP. If UDP / DHT leaked, we did something major wrong at Whonix.*"

(See also their documentation, e.g. the filesharing commentary.)

4. Debian with firewall

Lastly, we wanted to know if running a BitTorrent application without any UDP traffic would be possible (this would make it compatible with Tor's design);

We set up a firewall on a standard Debian system :

```
sudo ufw default deny outgoing
sudo ufw default deny incoming
sudo ufw allow 1:65535/tcp
```

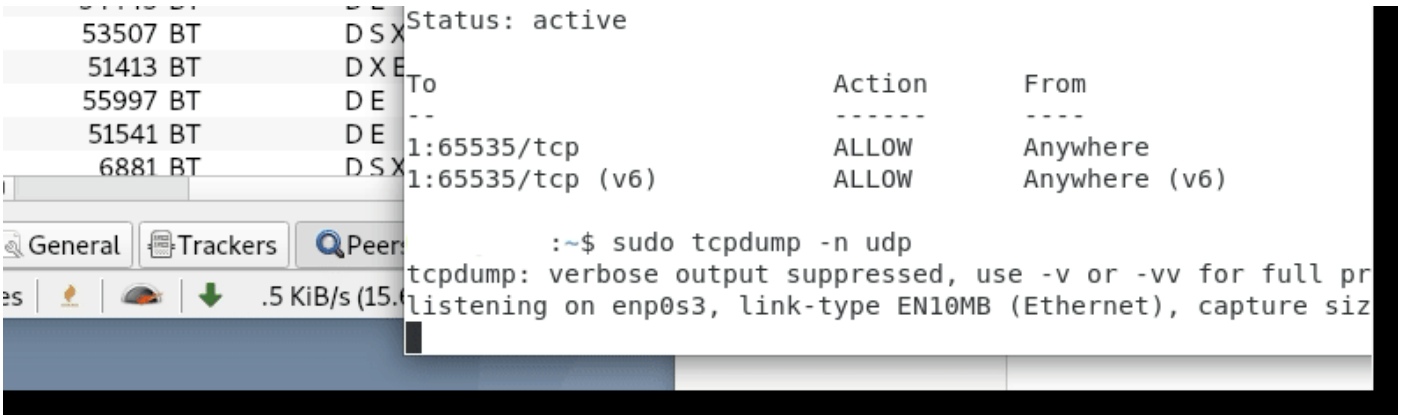


Figure 5. Debian with firewall allowing TCP only.

We let `tcmpdump` run for a few minutes (before the start of the application and while downloading) - with no messages.

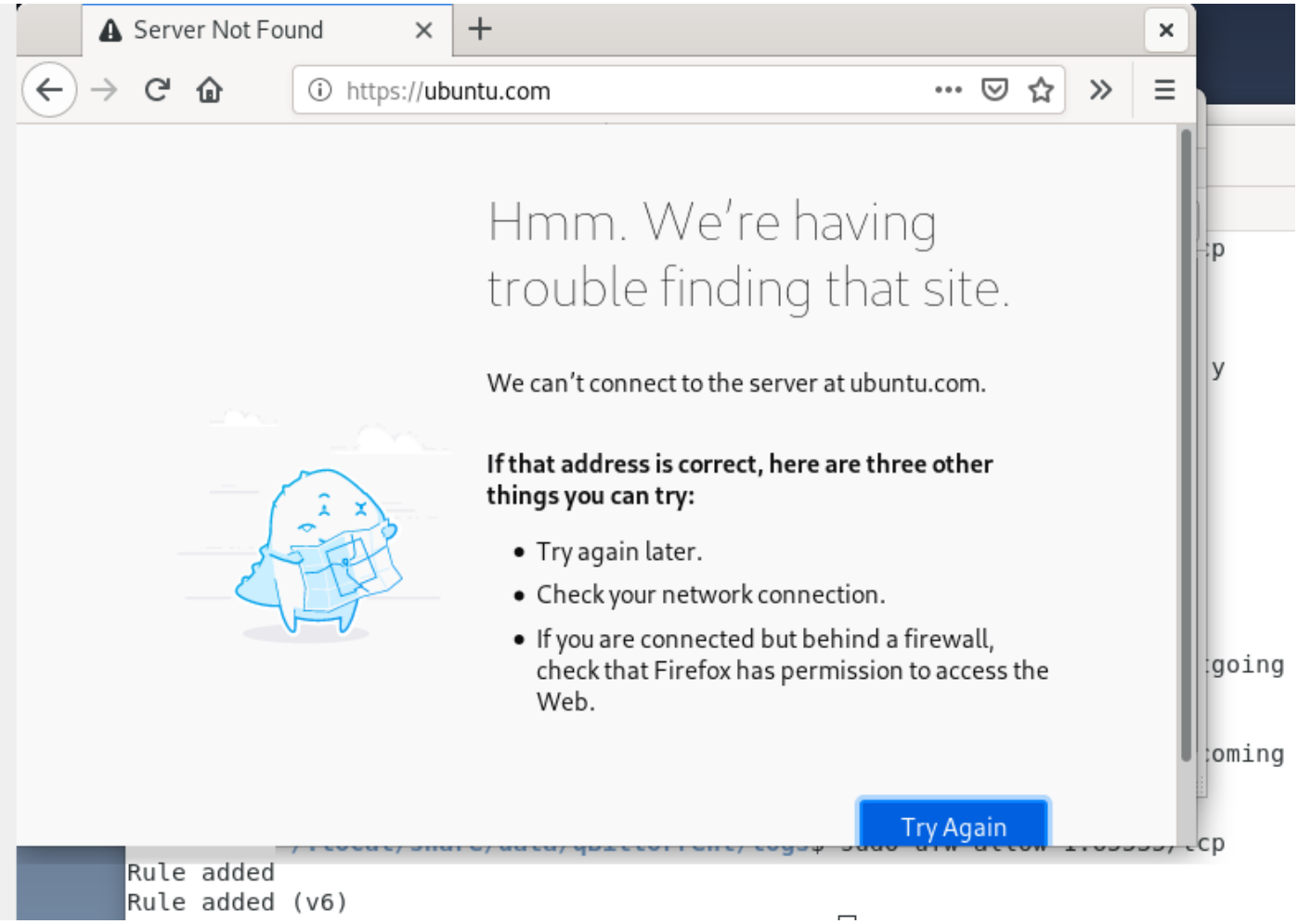


Figure 6. … Web browsing impossible.

Accessing websites was impossible just as was updating software (using http/s archives) during this time;

giving some confirmation that UDP traffic was blocked.

Here, too, the host's IP was not featured amongst peers while the logged "external IP" was from the Tor network.

```
~/.local/share/data/qBittorrent/logs$ ls
qbittorrent.log
```

(Another of many plaintext system files with highly sensitive data that should have never been enabled by default, as part of standard design.)

Conclusion

"BitTorrent over Tor is a bad idea" : This was the position of the Tor Project for the entirety of the previous decade.

This was re-iterated in a 2013 writing by its leader and remains a part of its current documentation.

200 Gbit/s go regularly unused on the Tor Network.

To give the reader some better understanding of this, it represents three times the traffic of a popular commercial VPN service (or 15,000-20,000 users).

BitTorrent over Tor is not only possible, but seems safe.

Without more research, we won't know definitely.

This study can be understood as a contribution towards that knowledge.

Privacy is most important for the average person :

For the downloader of pornography – so they may explore themselves.

For the watcher of Fassbinder films. He couldn't care less if his films were downloaded now, he died aged 37. In *Fox and his Friends* he mocked upper class gays in such brutal ways they never forgave him. In *Die dritte Generation* he mocked middle-class revolutionaries, who destroyed his films.

For the students in search of a complete edition of *The Critique of Pure Reason* (the first and second edition, the distinction is important).

Or, the one looking for Diogenes' *Lives of philosophers* in a recent translation (not the one by Hicks).

Or, the prosopography of the Roman Empire, whose volumes sell for 600 dollars!

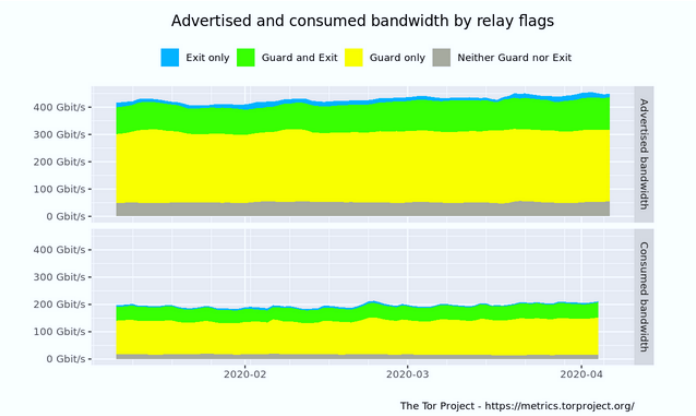
Or, the study by Panofsky of Early Netherlandish art.

It was there that this erudite scholar with a subversive mind told us that Bosch, the well-known painter of hell, was most likely one of those strict moralists who secretly delighted in seeing naked flesh.

This is because "noble causes" and lower ones, only exist in lower minds...

As absurd as anarchists insisting on rules (in their networks)...

REFERENCES



- Tor Project / arma. 04/2010. "Bittorrent over Tor isn't a good idea". https://blog.torproject.org/bittorrent-over-tor-isnt-good-idea

- Dingledine, Roger. 2013. Answer "How can BitTorrent traffic be anonymized with Tor?" https://tor.stackexchange.com/questions/64/how-can-bittorrent-traffic-be-anonymized-with-tor

- Schleizer, Patrick. 2017. Answer "DHT routed through Tor". https://tor.stackexchange.com/questions/14211/dht-routed-through-tor

- https://www.whonix.org/wiki/File_Sharing

- Norberg, Arvid. 2013. Answer "socks proxy obedience" https://sourceforge.net/p/libtorrent/mailman/message/31038818/

- https://metrics.torproject.org/bandwidth-flags.html