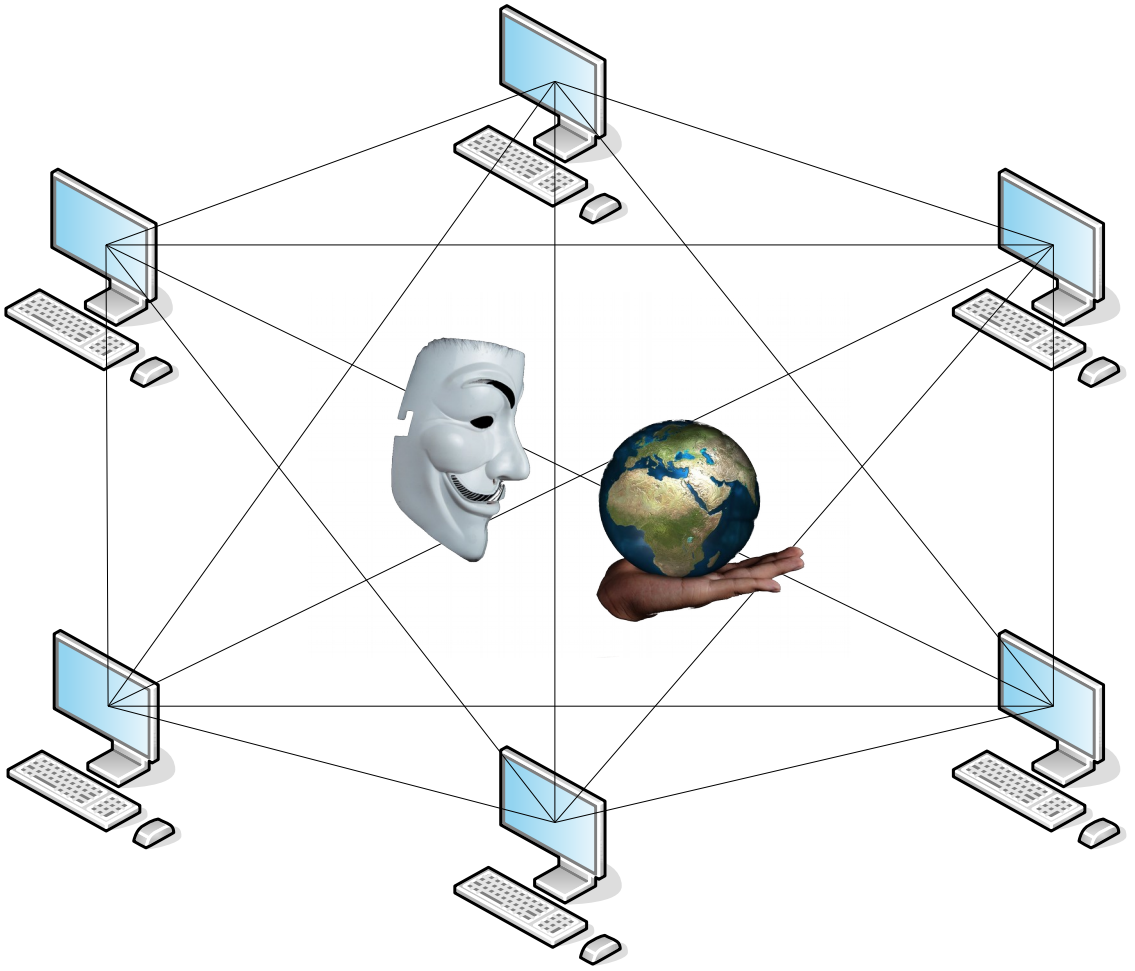
Ограничение использования файлообменных сетей P2P на примере протокола BitTorrent



Об авторе

- Антон Тарасов, г. Алматы, Казахстан
- Сертификаты MikroTik: MTCNA, MTCRE, MTCWE, MTCTCE
- Сертифицированный тренер MikroTik TR0416
- WWW: http://routeros.kz
- Skype: a_tarassov
- E-mail: a.tarassov@gmail.com

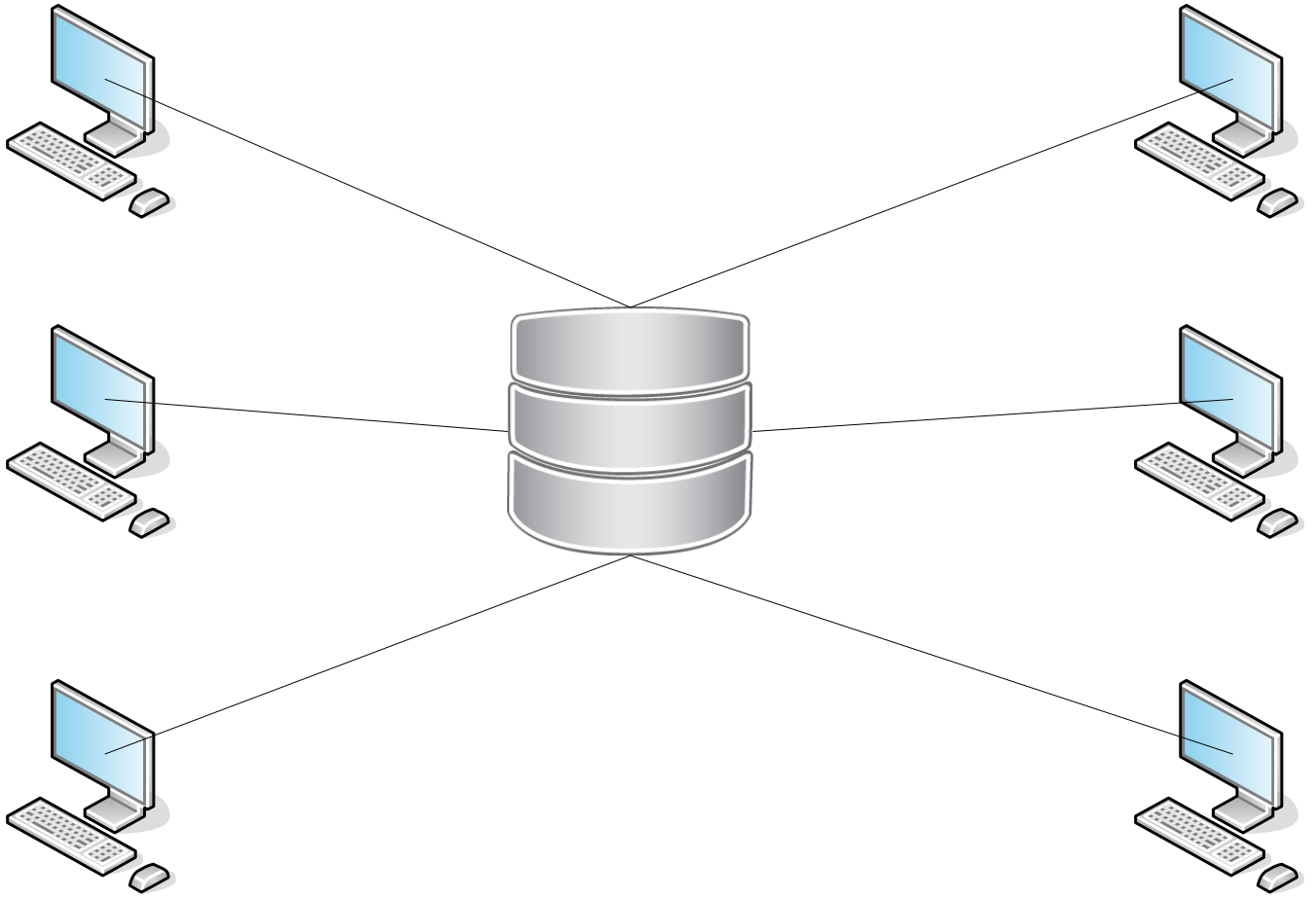
Цель презентации

- Исследовать протокол BitTorrent и его расширения согласно официальной документации и при помощи Wireshark
- Показать возможности использования Layer7 фильтров на RouterOS
- Ограничить скорость скачивания файлов из сети BitTorrent
- Реальный опыт эксплуатации

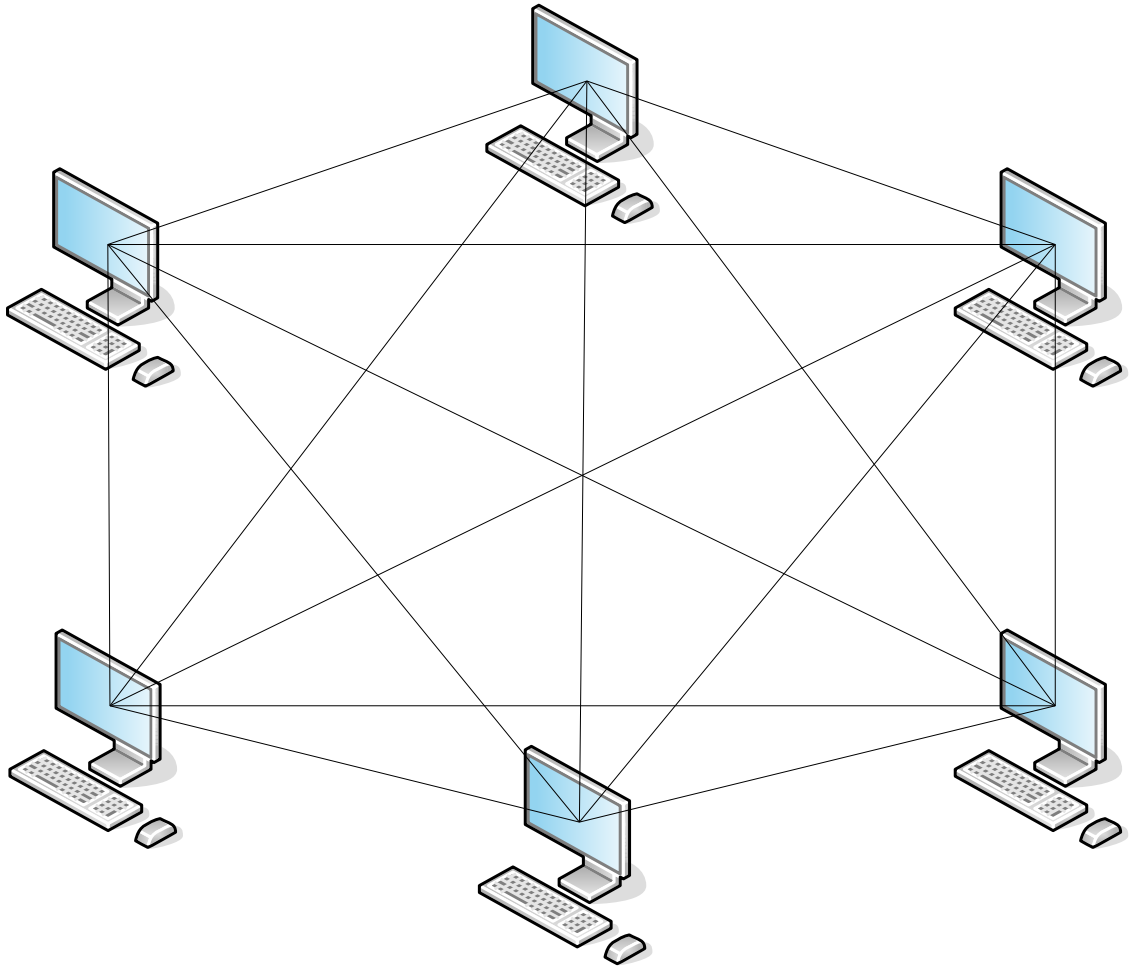
Основная задача

- НЕ запретить, НО ограничить

Модель сети «клиент-сервер»



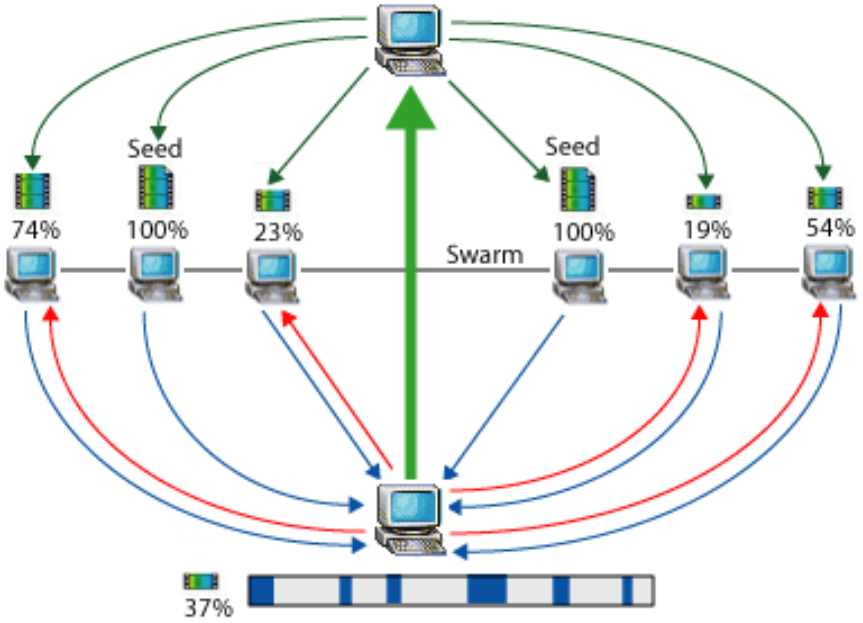
Одноранговая или пиринговая сеть



Пиринговая (P2P) сеть

- BitTorrent - P2P-протокол, предназначенный для обмена файлами через Интернет
- Торрент-трекер координирует действия скачивающего и раздающих (сидеров)

BitTorrent-трекер идентифицирует рой и сопровождает обмен файлами



Компьютер при помощи BitTorrent-клиента одновременно получает и отправляет множество частей файлов

Плюсы и минусы P2P сетей

Плюсы:

- отсутствие очередей на закачку
- высокая скорость (чем больше раздающих, тем выше скорость)
- докачка файлов (в любое время можно продолжить загрузку)
- много трекеров без регистрации

Минусы:

- не слабо загружает канал, если не ограничивать, иногда даже страничку открыть сложно
- требуется установка сторонней программы (bittorrent, utorrent, transmission и т. д.)

Политики разрешения

Запрещено все, что не разрешено:

- Обычно применяется в корпоративных сетях
- Большой набор разрешающих правил
- Более высокая нагрузка на CPU

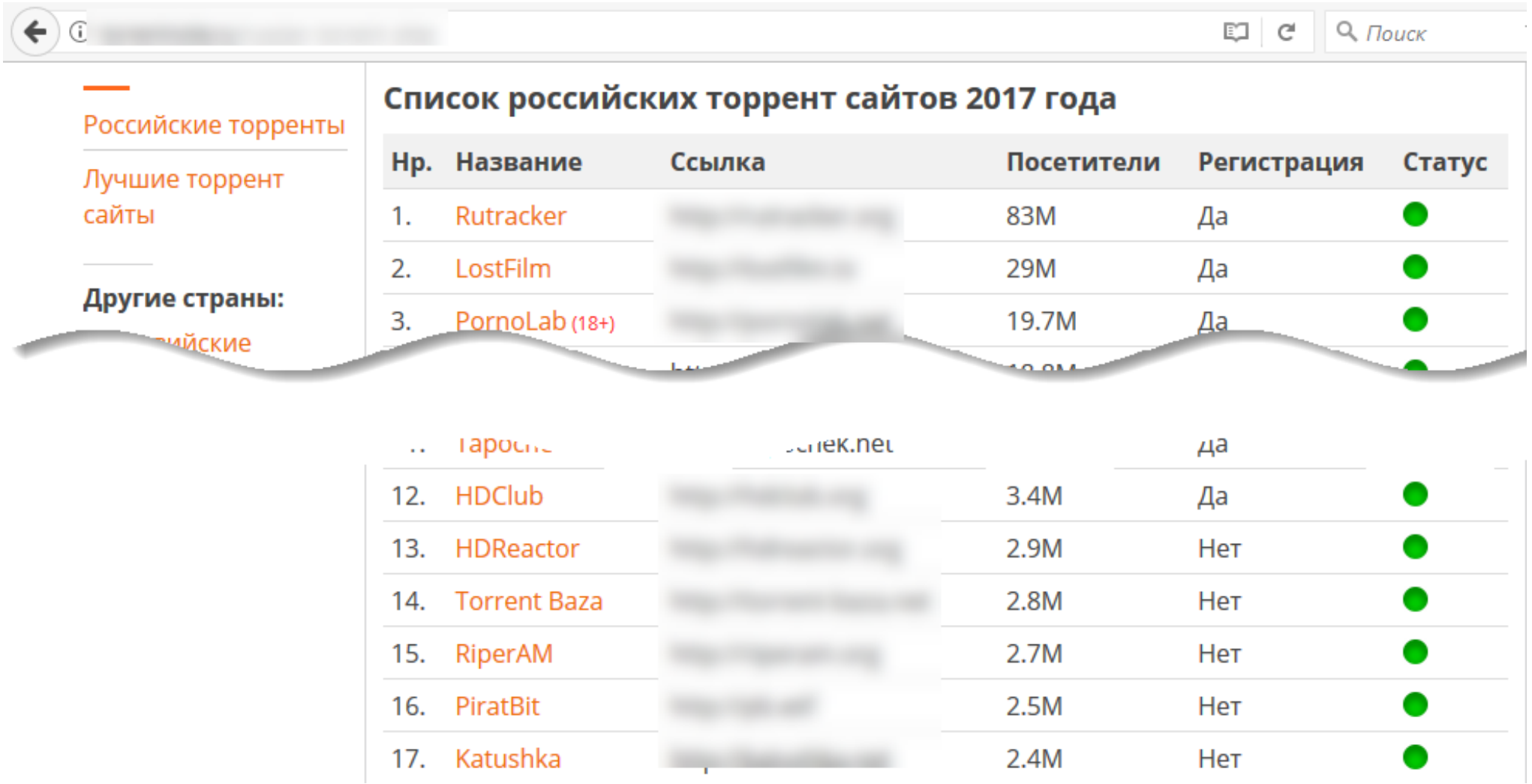
Разрешено все, что не запрещено:

- Обычно применяется в сетях сервис провайдера при пропуске трафика к абонентам
- Несколько запрещающих правил
- Менее высокая нагрузка на CPU

Порядок определения и ограничения P2P трафика

- Создание адресного листа (/ip firewall address-list), для хранения IP адресов раздающих – „p2p-seeds“
- Добавление FQDN трекеров в адресный лист – „p2p-seeds“
- Создание списка Layer7 протоколов (/ip firewall layer7-protocol)
- Создание правил обнаружения P2P соединений
- Добавление обнаруженных IP адресов в адресный лист
- Маркировка соединений и пакетов с IP адресами из адресного листа
- Ограничение скорости (/simple queues или /queue tree)

Создание адресного листа и добавление FQDN трекеров



Создание адресного листа и добавление FQDN трекеров

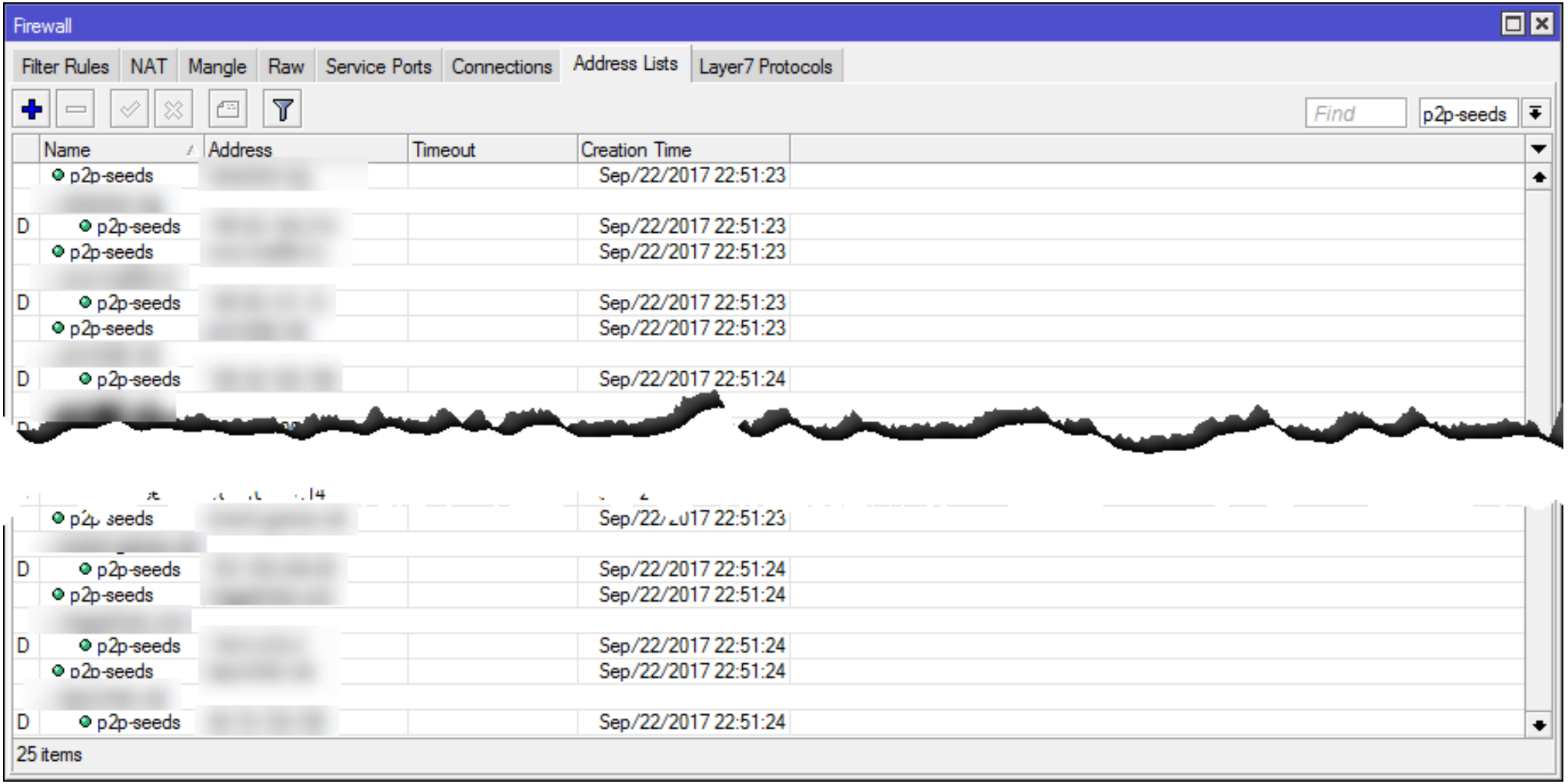
v6.36 changes

...

*) firewall - allow to add domain name to address-lists (dynamic entries for resolved addresses will be added to specified list);

...

Создание адресного листа и добавление FQDN трекеров



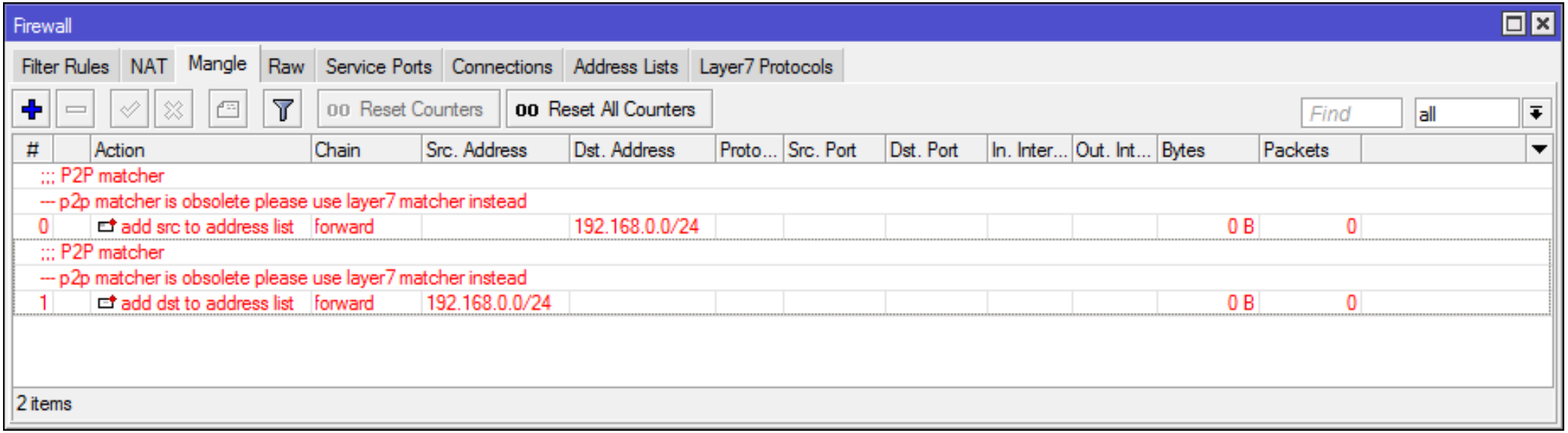
Встроенный P2P matcher

v6.39 changes

...

!) firewall - discontinued support for p2p matcher (old rules will become invalid);

...

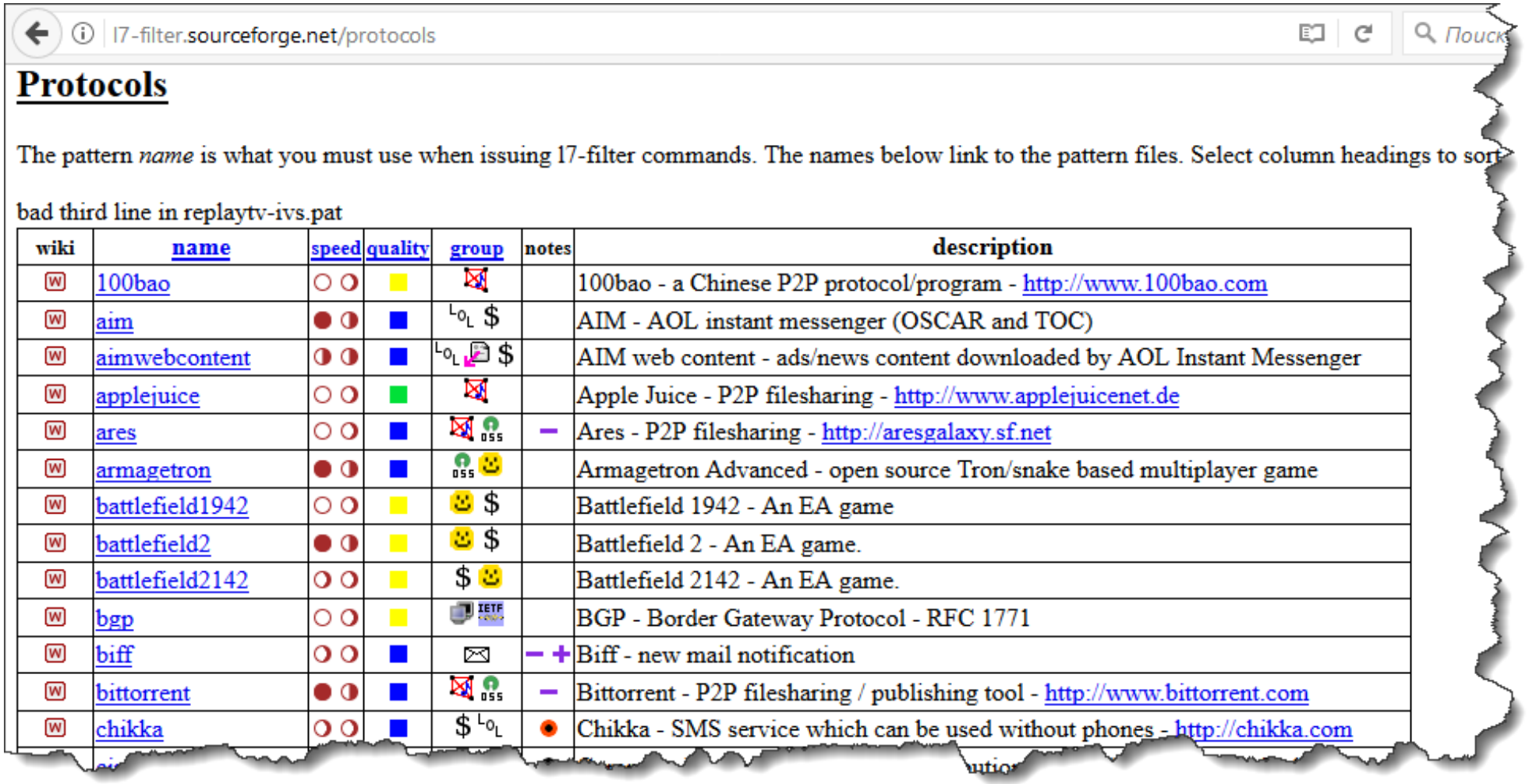


RouterOS Layer7

- Метод поиска данных по шаблону в ICMP/TCP/UDP потоках
- L7 matcher анализирует первые 10 пакетов или первые 2КБ соединения
- L7 matcher должен видеть и входящий и исходящий трафик, т. е. находиться в цепочке forward, или обязательно в prerouting+postrouting
- L7 это ресурсоемкий процесс
- L7 шаблоны независимы от регистра

RouterOS Layer7

- RouterOS L7 шаблоны совместимы с шаблонами проекта L7-filter



l7-filter.sourceforge.net/protocols

Protocols

The pattern *name* is what you must use when issuing l7-filter commands. The names below link to the pattern files. Select column headings to sort

bad third line in replaytv-ivs.pat

wiki	name	speed	quality	group	notes	description
W	100bao	○ ◑	■			100bao - a Chinese P2P protocol/program - http://www.100bao.com
W	aim	● ◑	■	L7 $		AIM - AOL instant messenger (OSCAR and TOC)
W	aimwebcontent	◑ ◑	■	L7 $		AIM web content - ads/news content downloaded by AOL Instant Messenger
W	applejuice	○ ◑	■			Apple Juice - P2P filesharing - http://www.applejuicenet.de
W	ares	○ ◑	■	OSS	−	Ares - P2P filesharing - http://aresgalaxy.sf.net
W	armagetron	● ◑	■	OSS		Armagetron Advanced - open source Tron/snake based multiplayer game
W	battlefield1942	○ ◑	■	$		Battlefield 1942 - An EA game
W	battlefield2	● ◑	■	$		Battlefield 2 - An EA game.
W	battlefield2142	◑ ◑	■	$		Battlefield 2142 - An EA game.
W	bgp	○ ◑	■	IETF		BGP - Border Gateway Protocol - RFC 1771
W	biff	◑ ◑	■		− +	Biff - new mail notification
W	bittorrent	● ◑	■	OSS	−	Bittorrent - P2P filesharing / publishing tool - http://www.bittorrent.com
W	chikka	◑ ◑	■	$ L7	●	Chikka - SMS service which can be used without phones - http://chikka.com

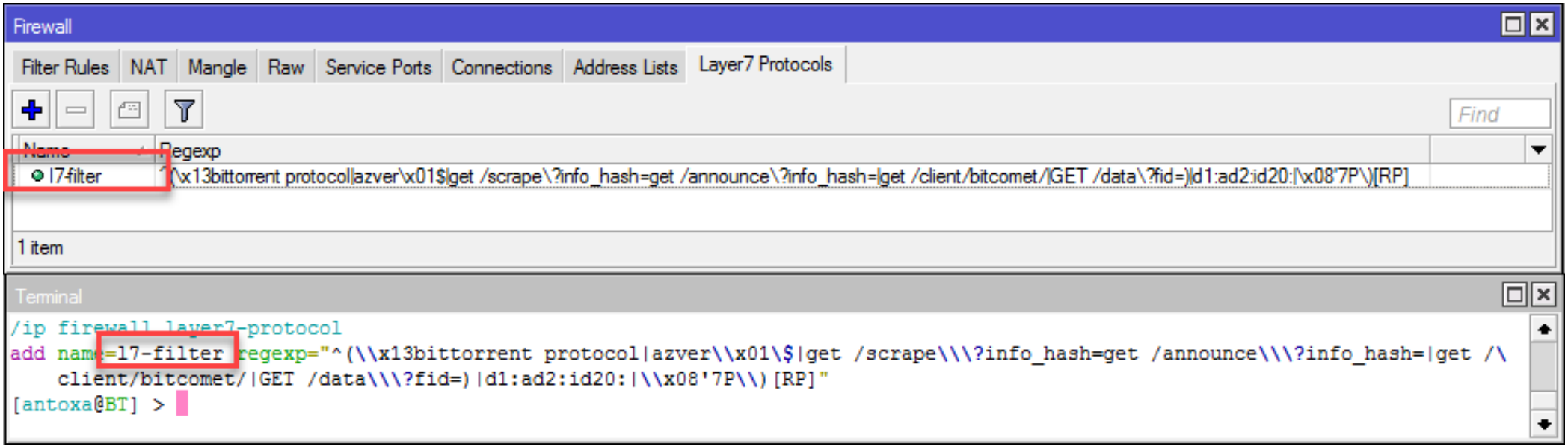
RouterOS Layer7

l7-filter.sourceforge.net/layer7-protocols/protocols/bittorren

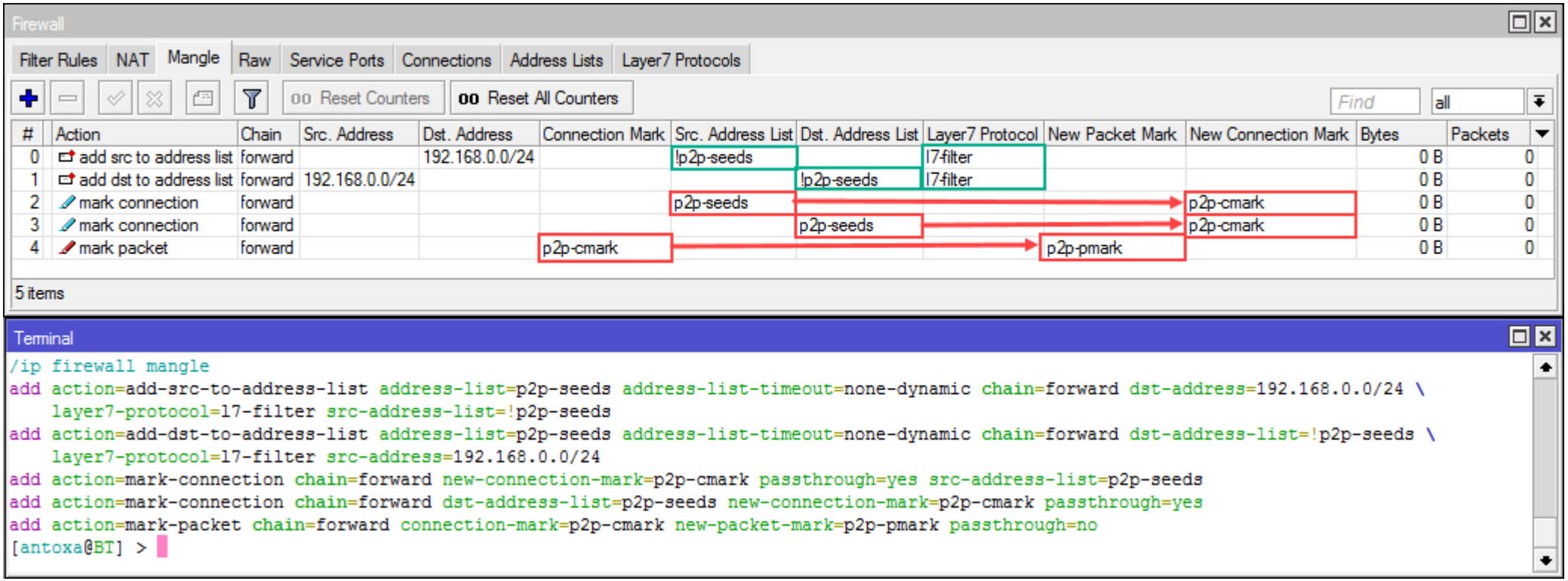
Поиск

```
# Bittorrent - P2P filesharing / publishing tool - http://www.bittorrent.com
# Pattern attributes: good slow notsofast undermatch
# Protocol groups: p2p open_source
# Wiki: http://www.protocolinfo.org/wiki/Bittorrent
# Copyright (C) 2008 Matthew Strait, Ethan Sommer; See ../LICENSE
#
# This pattern has been tested and is believed to work well.
# It will, however, not work on bittorrent streams that are encrypted, since
# it's impossible to match (well) encrypted data.

bittorrent

# Does not attempt to match the HTTP download of the tracker
# 0x13 is the length of "bittorrent protocol"
# Second two bits match UDP wierdness
# Next bit matches something Azureus does
# Ditto on the next bit.  Could also match on "user-agent: azureus", but that's in the next
# packet and perhaps this will match multiple clients.
# bitcomet-specific strings contributed by liangjun.

# This is not a valid GNU basic regular expression (but that's ok).
^(\x13bittorrent protocol|azver\x01$|get /scrape\?info_hash=get /announce\?info_hash=|get /client/bitcomet/|GET
/data\?fid=)|d1:ad2:id20:|\x08'7P\)[RP]

# This pattern is "fast", but won't catch as much
#^(\x13bittorrent protocol|azver\x01$|get /scrape\?info_hash=)
```

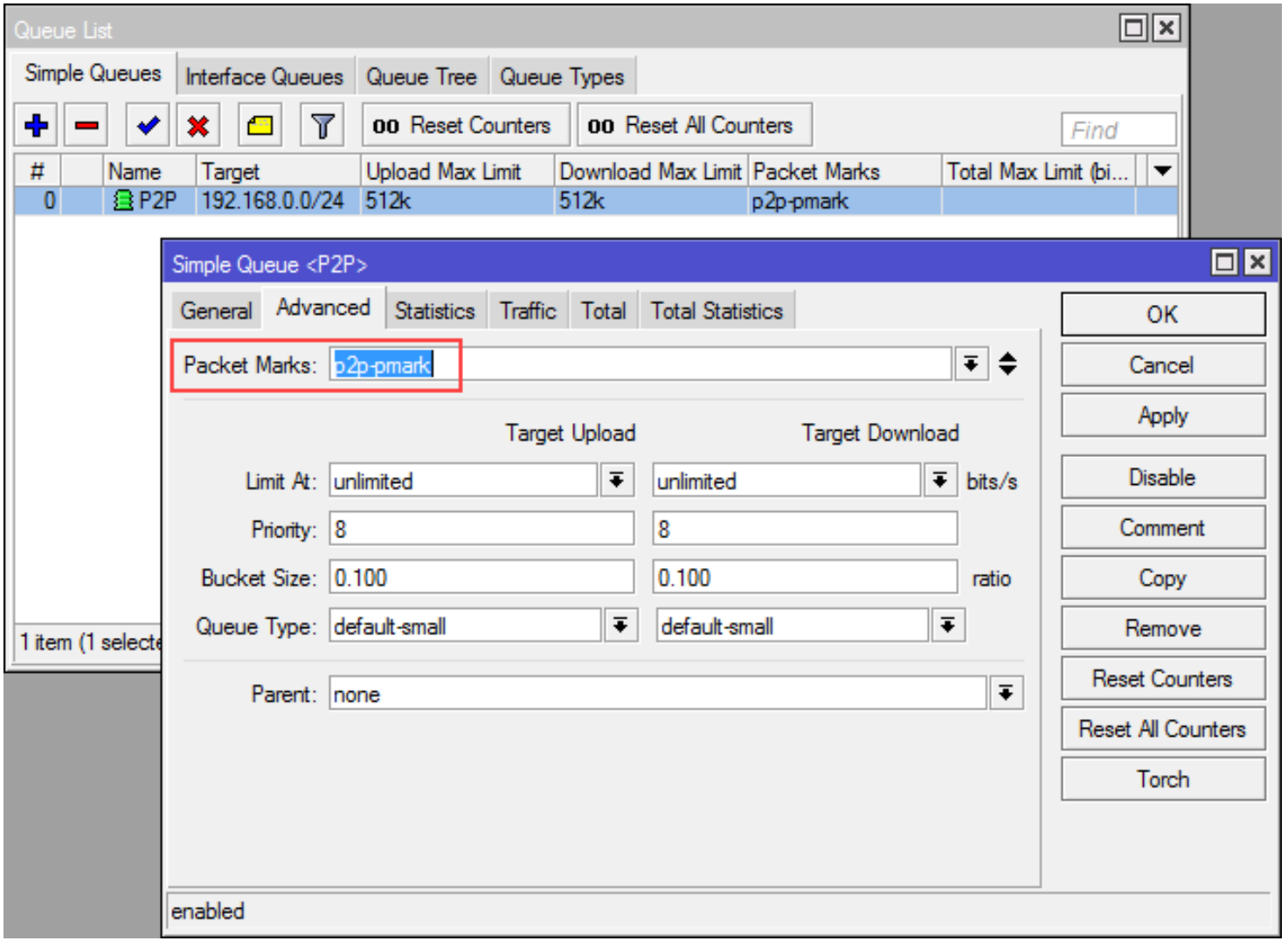
RouterOS Layer7



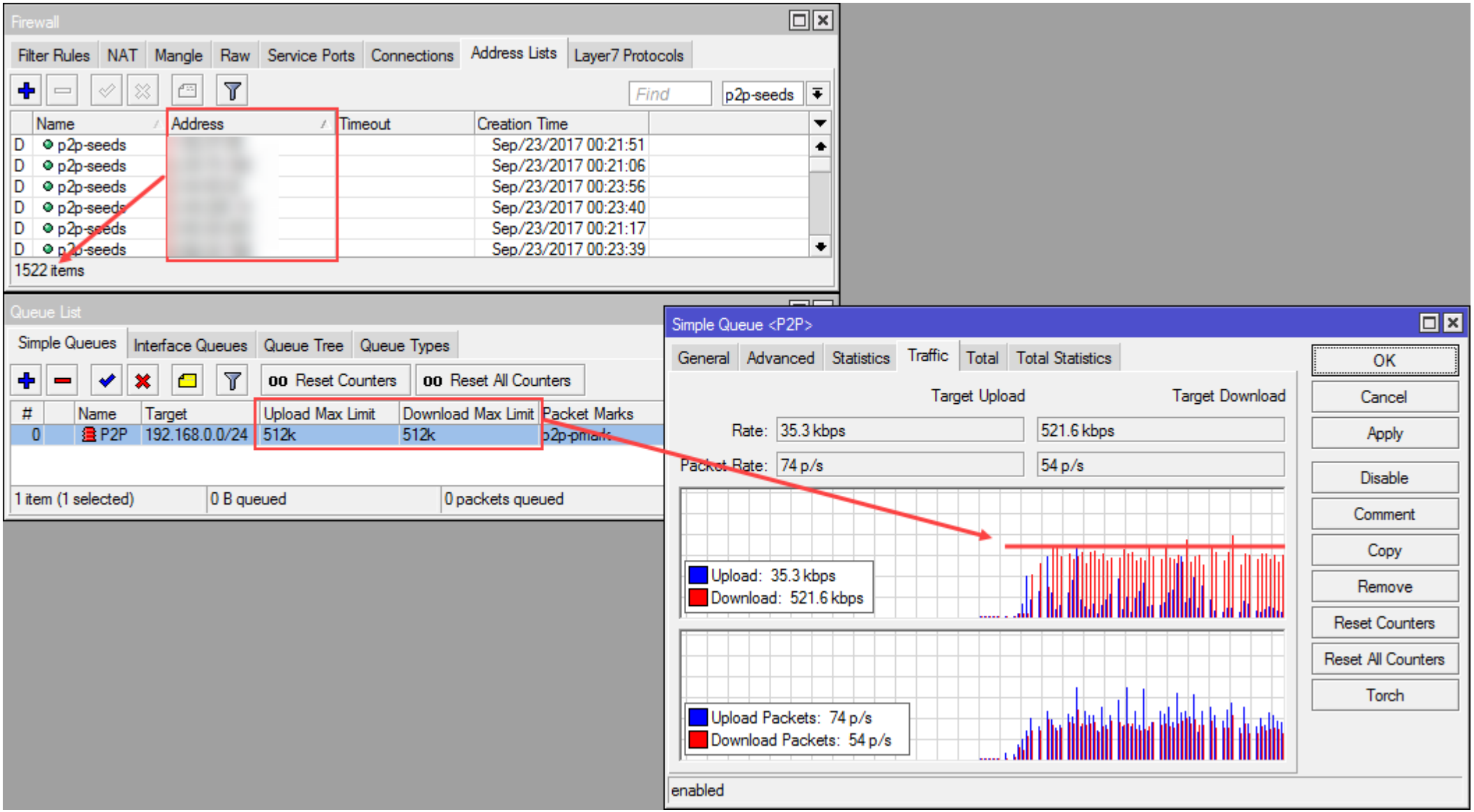
Определение P2P соединений и маркировка пакетов



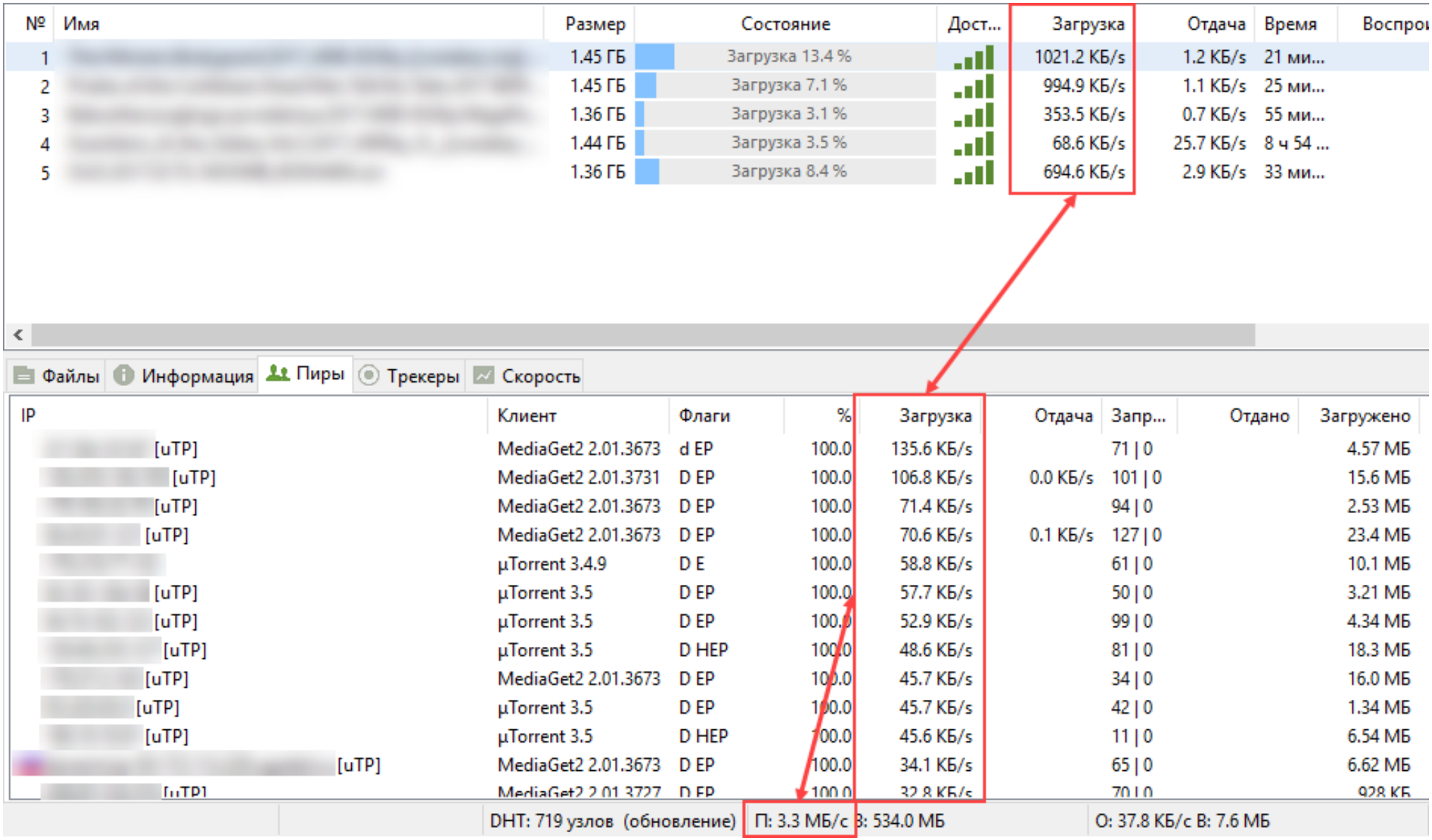
Ограничение скорости P2P



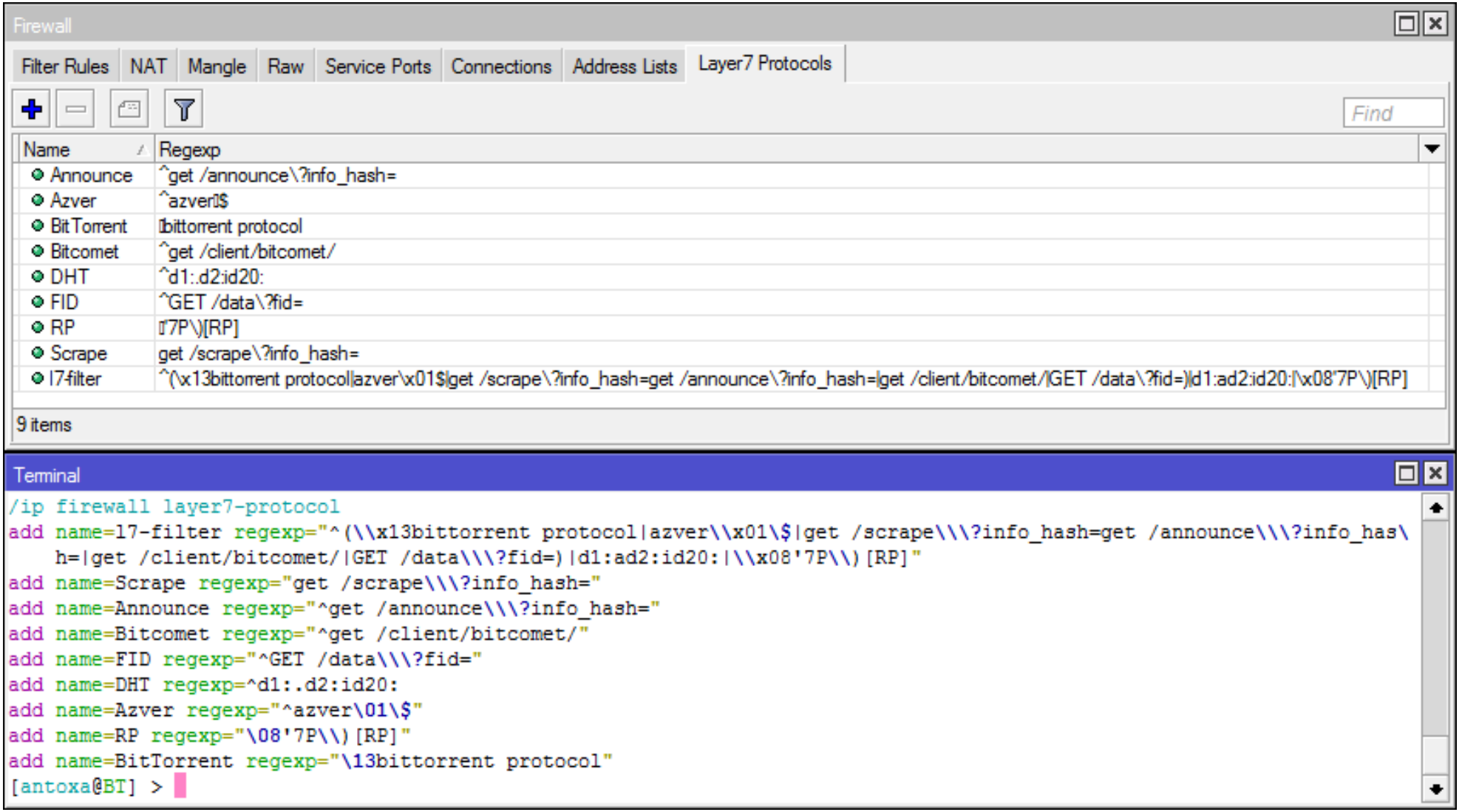
Тестирование конфигурации



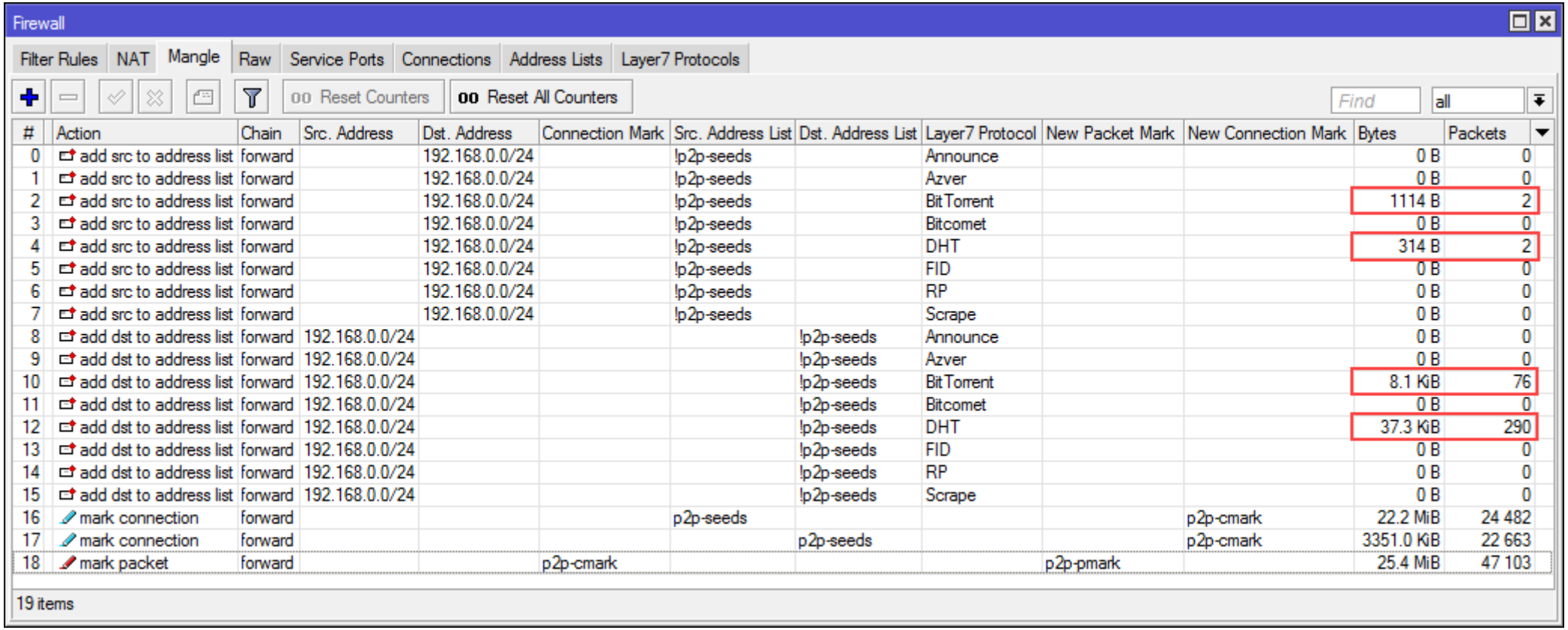
Тестирование конфигурации



RouterOS Layer7



Определение P2P соединений и маркировка пакетов



Firewall

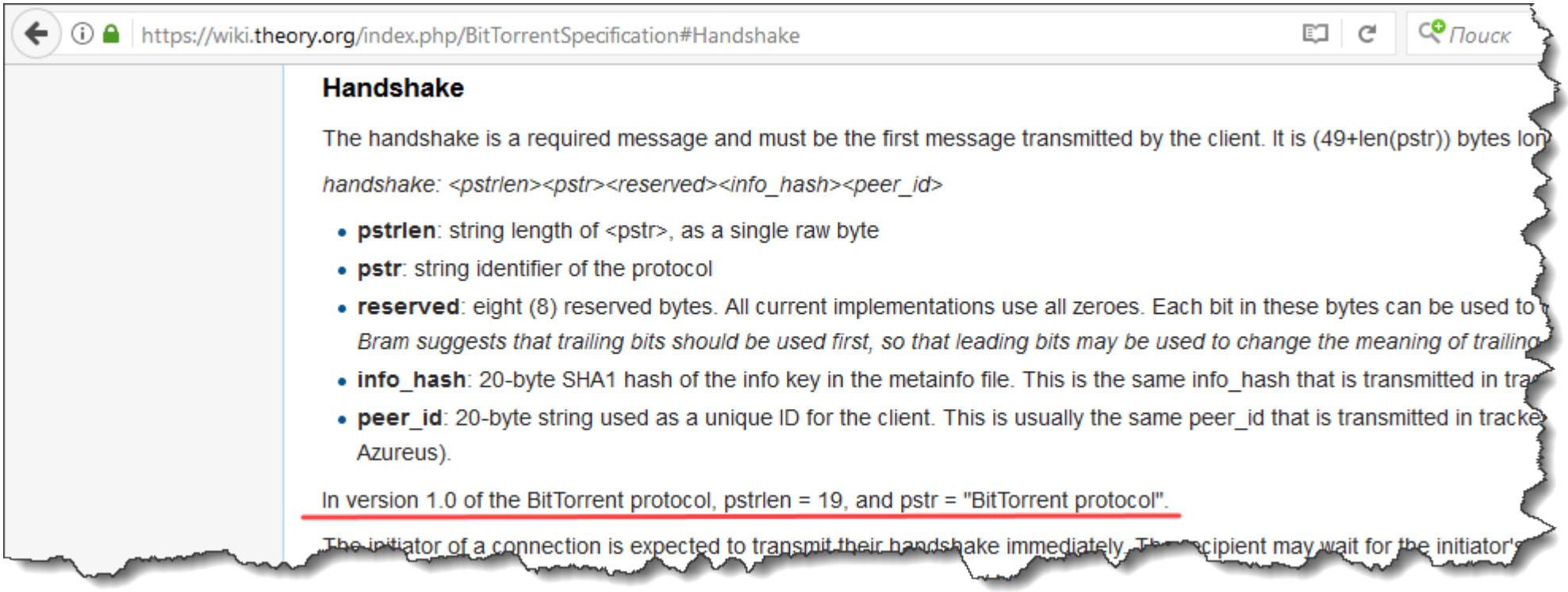
Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

oo Reset Counters | oo Reset All Counters | Find | all

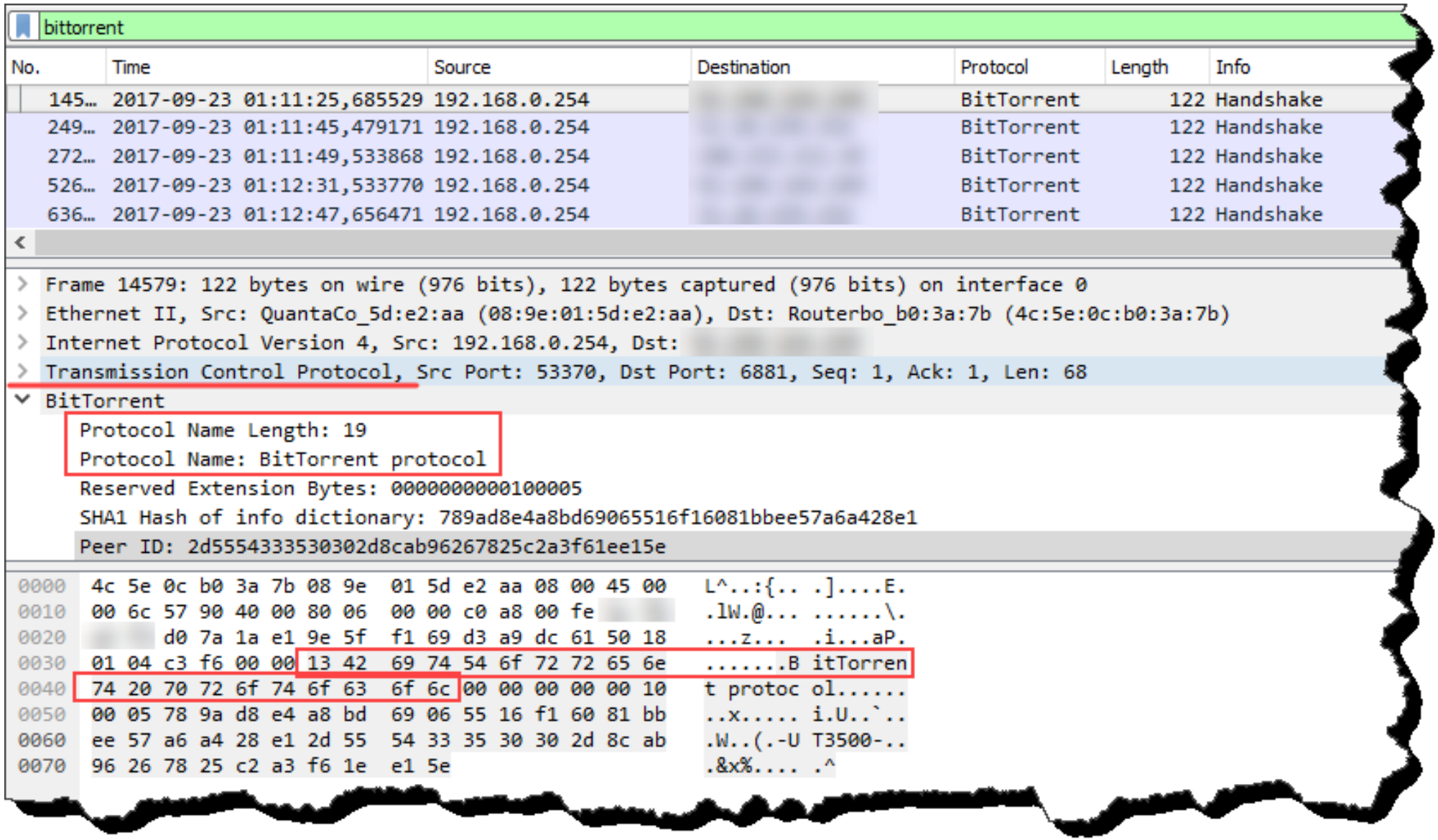
#	Action	Chain	Src. Address	Dst. Address	Connection Mark	Src. Address List	Dst. Address List	Layer7 Protocol	New Packet Mark	New Connection Mark	Bytes	Packets
0	add src to address list	forward		192.168.0.0/24		!p2p-seeds		Announce			0 B	0
1	add src to address list	forward		192.168.0.0/24		!p2p-seeds		Azver			0 B	0
2	add src to address list	forward		192.168.0.0/24		!p2p-seeds		BitTorrent			1114 B	2
3	add src to address list	forward		192.168.0.0/24		!p2p-seeds		Bitcomet			0 B	0
4	add src to address list	forward		192.168.0.0/24		!p2p-seeds		DHT			314 B	2
5	add src to address list	forward		192.168.0.0/24		!p2p-seeds		FID			0 B	0
6	add src to address list	forward		192.168.0.0/24		!p2p-seeds		RP			0 B	0
7	add src to address list	forward		192.168.0.0/24		!p2p-seeds		Scrape			0 B	0
8	add dst to address list	forward	192.168.0.0/24				!p2p-seeds	Announce			0 B	0
9	add dst to address list	forward	192.168.0.0/24				!p2p-seeds	Azver			0 B	0
10	add dst to address list	forward	192.168.0.0/24				!p2p-seeds	BitTorrent			8.1 KiB	76
11	add dst to address list	forward	192.168.0.0/24				!p2p-seeds	Bitcomet			0 B	0
12	add dst to address list	forward	192.168.0.0/24				!p2p-seeds	DHT			37.3 KiB	290
13	add dst to address list	forward	192.168.0.0/24				!p2p-seeds	FID			0 B	0
14	add dst to address list	forward	192.168.0.0/24				!p2p-seeds	RP			0 B	0
15	add dst to address list	forward	192.168.0.0/24				!p2p-seeds	Scrape			0 B	0
16	mark connection	forward				p2p-seeds				p2p-cmark	22.2 MiB	24 482
17	mark connection	forward					p2p-seeds			p2p-cmark	3351.0 KiB	22 663
18	mark packet	forward			p2p-cmark				p2p-pmark		25.4 MiB	47 103

19 items

Спецификация BitTorrent



Wireshark BitTorrent



DHT

- DHT (Distributed hash table – распределенная хэш-таблица) – это протокол, позволяющий битторрент-клиентам находить друг друга без использования трекера
- Клиенты с поддержкой DHT образуют общую DHT-сеть и помогают друг другу найти участников одних и тех же раздач

Спецификация DHT

- DHT запросы (Queries)
  - ping
  - find_node
  - get_peers
  - announce_peer

http://www.bittorrent.org/beps/bep_0005.html

Спецификация DHT

ping

The most basic query is a ping. "q" = "ping" A ping query has a single argument, "id" the value is a 20-byte string containing the senders node ID in network byte order. The appropriate response to a ping has a single key "id" containing the node ID of the responding node.

```
arguments:  {"id" : "<querying nodes id>"}

response: {"id" : "<queried nodes id>"}
```

Example Packets

```
ping Query = {"t":"aa", "y":"q", "q":"ping", "a":{"id":"abcdefghij0123456789"}}
bencoded = d1:ad2:id20:abcdefghij0123456789e1:q4:ping1:t2:aa1:y1:qe

Response = {"t":"aa", "y":"r", "r": {"id":"mnopqrstuvwxyz123456"}}
bencoded = d1:rd2:id20:mnopqrstuvwxyz123456e1:t2:aa1:y1:re
```

Спецификация DHT

find_node

Find node is used to find the contact information for a node given its ID. "q" == "find_node" A find_node query has two arguments, "id" containing the node ID of the querying node, and "target" containing the ID of the node sought by the queryer. When a node receives a find_node query, it should respond with a key "nodes" and value of a string containing the compact node info for the target node or the K (8) closest good nodes in its own routing table.

```
arguments:  {"id" : "<querying nodes id>", "target" : "<id of target node>"}

response: {"id" : "<queried nodes id>", "nodes" : "<compact node info>"}
```

Example Packets

```
find_node Query = {"t":"aa", "y":"q", "q":"find_node", "a": {"id":"abcdefghij0123456789", "target":"mnopqrstuvwxyz1234
bencoded = d1:ad2:id20:abcdefghij01234567896:target20:mnopqrstuvwxyz123456e1:q9:find_node1:t2:aa1:y1:qe

Response = {"t":"aa", "y":"r", "r": {"id":"0123456789abcdefghij", "nodes": "def456..."}}
bencoded = d1:rd2:id20:0123456789abcdefghij5:nodes9:def456...e1:t2:aa1:y1:re
```

get_peers

Спецификация DHT

get_peers

Get peers associated with a torrent infohash. "q" = "get_peers" A get_peers query has two arguments, "id" containing the node ID of the querying node, and "info_hash" containing the infohash of the torrent. If the queried node has peers for the infohash, they are returned in a key "values" as a list of strings. Each string containing "compact" format peer information for a single peer. If the queried node has no peers for the infohash, a key "nodes" is returned containing the K nodes in the queried nodes routing table closest to the infohash supplied in the query. In either case a "token" key is also included in the return value. The token value is a required argument for a future announce_peer query. The token value should be a short binary string.

```
arguments:  {"id" : "<querying nodes id>", "info_hash" : "<20-byte infohash of target torrent>"}

response: {"id" : "<queried nodes id>", "token" :"<opaque write token>", "values" : ["<peer 1 info string>", "<peer 2 i

or: {"id" : "<queried nodes id>", "token" :"<opaque write token>", "nodes" : "<compact node info>"}
```

Example Packets:

```
get_peers Query = {"t":"aa", "y":"q", "q":"get_peers", "a": {"id":"abcdefghij0123456789", "info_hash":"mnopqrstuvwxyz12
bencoded = d1:ad2:id20:abcdefghij01234567899:info_hash20:mnopqrstuvwxyz123456e1:q9:get_peers1:t2:aa1:y1:qe

Response with peers = {"t":"aa", "y":"r", "r": {"id":"abcdefghij0123456789", "token":"aoeusnth", "values": ["axje.u",
bencoded = d1:rd2:id20:abcdefghij01234567895:token8:aoeusnth6:values16:axje.u6:idhtnmee1:t2:aa1:y1:re

Response with closest nodes = {"t":"aa", "y":"r", "r": {"id":"abcdefghij0123456789", "token":"aoeusnth", "nodes": "def4
bencoded = d1:rd2:id20:abcdefghij01234567895:nodes9:def456...5:token8:aoeusnthe1:t2:aa1:y1:re
```

Спецификация DHT

announce_peer

Announce that the peer, controlling the querying node, is downloading a torrent on a port. announce_peer has four arguments: "id" containing the node ID of the querying node, "info_hash" containing the infohash of the torrent, "port" containing the port as an integer, and the "token" received in response to a previous get_peers query. The queried

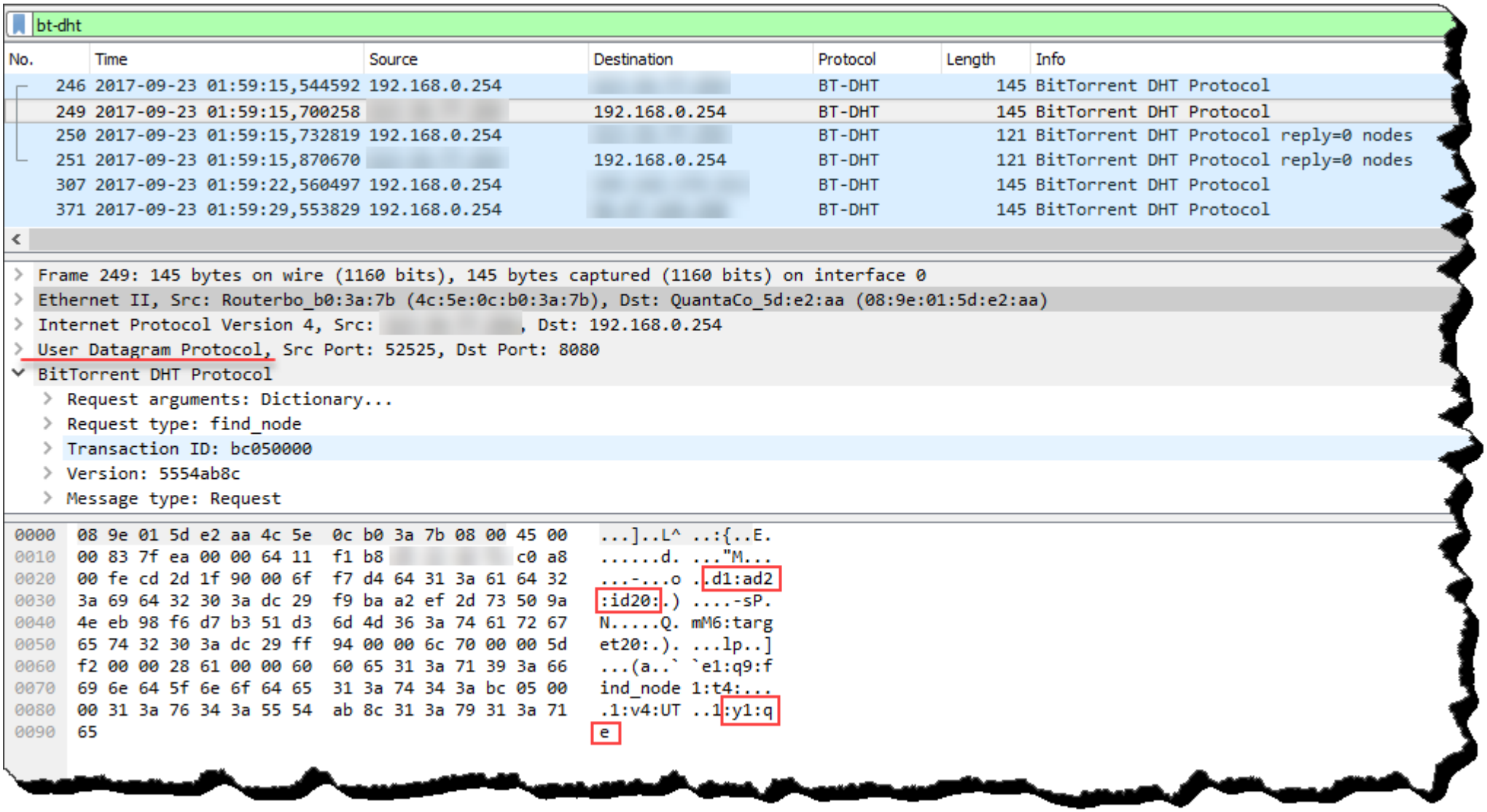
port argument should be ignored and the source port of the UDP packet should be used as the peer port instead. This is useful for peers behind a NAT that may not know their external port, and supporting uTP, they accept incoming connections on the same port as the DHT port.

```
arguments:  {"id" : "<querying nodes id>",
  "implied_port": <0 or 1>,
  "info_hash" : "<20-byte infohash of target torrent>",
  "port" : <port number>,
  "token" : "<opaque token>"}

response: {"id" : "<queried nodes id>"}
```

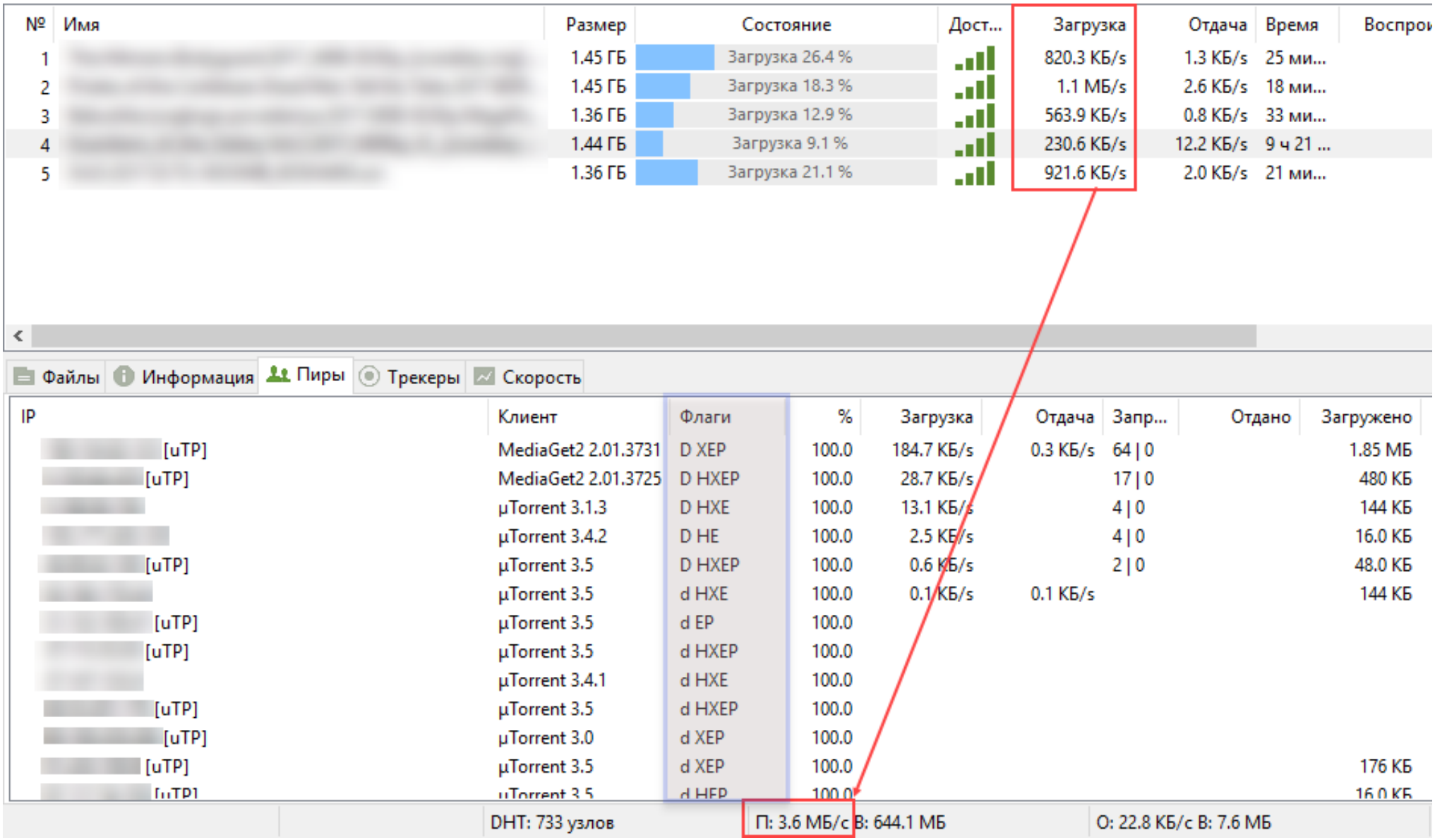
Example Packets:

```
announce_peers Query = {"t":"aa", "y":"q", "q":"announce_peer", "a": {"id":"abcdefghij0123456789", "implied_port": 1
bencoded = d1:ad2:id20:abcdefghij01234567899:info_hash20:<br />
mnopqrstuvwxyz1234564:porti6881e5:token8:aoeusnthe1:q13:announce_peer1:t2:aa1:y1:qe

Response = {"t":"aa", "y":"r", "r": {"id":"mnopqrstuvwxyz123456"}}
bencoded = d1:rd2:id20:mnopqrstuvwxyz123456e1:t2:aa1:y1:re
```

Wireshark DHT



Тестирование конфигурации



№	Имя	Размер	Состояние	Дост...	Загрузка	Отдача	Время	Воспрои
1		1.45 ГБ	Загрузка 26.4 %		820.3 КБ/s	1.3 КБ/s	25 ми...	
2		1.45 ГБ	Загрузка 18.3 %		1.1 МБ/s	2.6 КБ/s	18 ми...	
3		1.36 ГБ	Загрузка 12.9 %		563.9 КБ/s	0.8 КБ/s	33 ми...	
4		1.44 ГБ	Загрузка 9.1 %		230.6 КБ/s	12.2 КБ/s	9 ч 21 ...	
5		1.36 ГБ	Загрузка 21.1 %		921.6 КБ/s	2.0 КБ/s	21 ми...	

Файлы | Информация | Пиры | Трекеры | Скорость

IP	Клиент	Флаги	%	Загрузка	Отдача	Запр...	Отдано	Загружено
[uTP]	MediaGet2 2.01.3731	D XEP	100.0	184.7 КБ/s	0.3 КБ/s	64 | 0		1.85 МБ
[uTP]	MediaGet2 2.01.3725	D HXEP	100.0	28.7 КБ/s		17 | 0		480 КБ
	µTorrent 3.1.3	D HXE	100.0	13.1 КБ/s		4 | 0		144 КБ
	µTorrent 3.4.2	D HE	100.0	2.5 КБ/s		4 | 0		16.0 КБ
[uTP]	µTorrent 3.5	D HXEP	100.0	0.6 КБ/s		2 | 0		48.0 КБ
	µTorrent 3.5	d HXE	100.0	0.1 КБ/s	0.1 КБ/s			144 КБ
[uTP]	µTorrent 3.5	d EP	100.0					
[uTP]	µTorrent 3.5	d HXEP	100.0					
	µTorrent 3.4.1	d HXE	100.0					
[uTP]	µTorrent 3.5	d HXEP	100.0					
[uTP]	µTorrent 3.0	d XEP	100.0					
[uTP]	µTorrent 3.5	d XEP	100.0					176 КБ
[uTP]	µTorrent 3.5	d HEP	100.0					16.0 КБ

DHT: 733 узлов | П: 3.6 МБ/с В: 644.1 МБ | О: 22.8 КБ/с В: 7.6 МБ

Флаги µTorrent

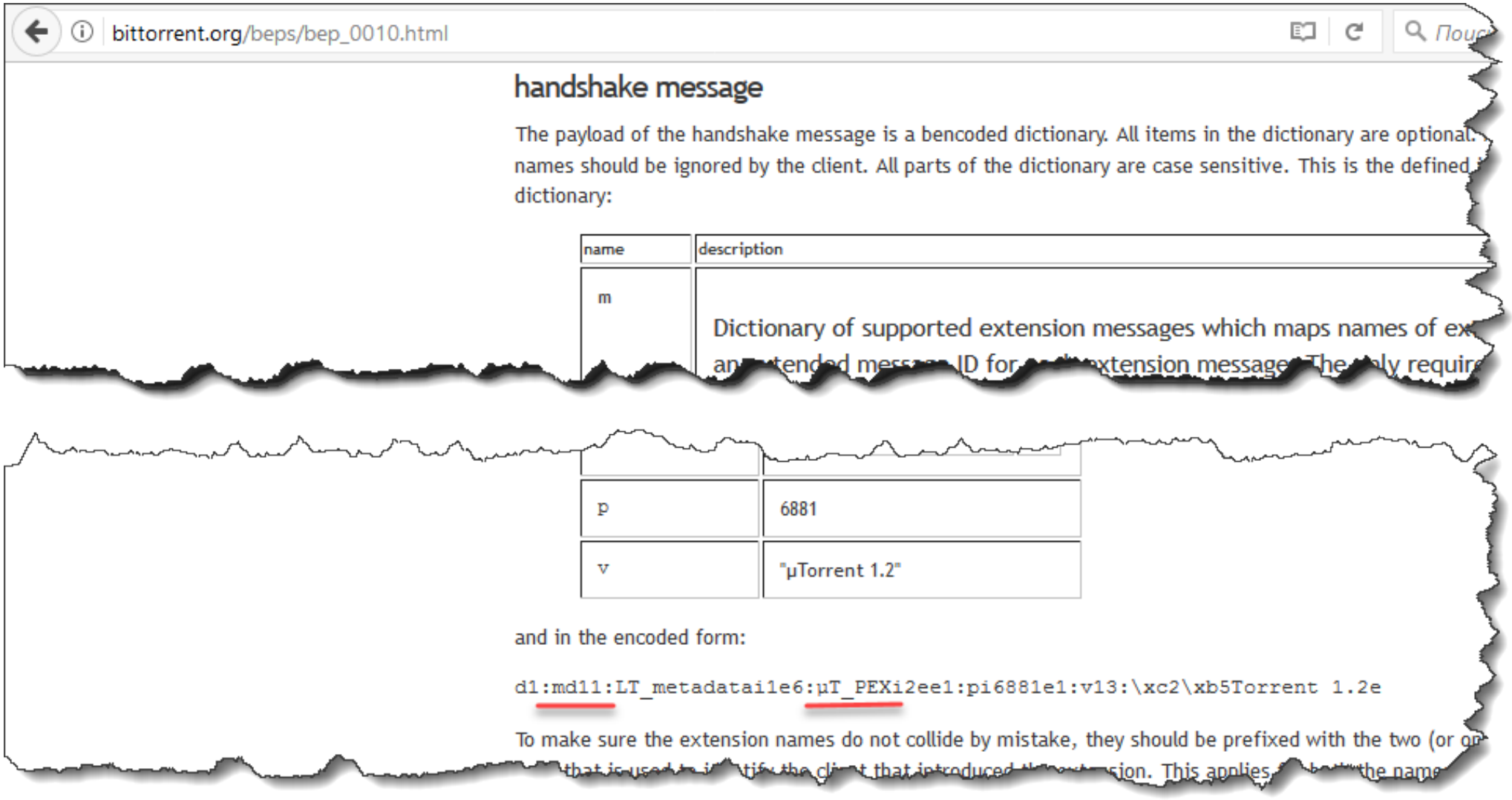
- D – В данный момент скачивается (заинтересован и доступен)
- d – Ваш клиент хочет скачать, но пир не хочет отдавать (заинтересован, но занят)
- U – В данный момент отдается (заинтересован и доступен)
- u – Пир хочет у Вас скачать, но Вы еще не отдаете (заинтересован, но занят)
- E – Пир использует шифрование протокола (весь трафик)
- e – Пир использует шифрование протокола (при соединении)
- **X** – Пир был добавлен через обмен пирами (Peer Exchange, PEX)
- **H** – Пир был добавлен через DHT-сеть
- h – Пир подключился с использованием UDP-hole punching
- **P** – Пир подключился через uTP
- I – Входящее подключение
- S – Пир "уснул" (нулевая активность)
- O – Пир освобождается и скоро будет готов раздавать
- K – Пир хочет Вам отдать, но Вы не хотите скачивать
- ? – Ваш клиент готов отдать, но пир не хочет получать
- L – Локальный пир (был найден через "Поиск локальных пиров")
- F – Пир был замечен в передаче "битого" куска (не обязательно плохой пир, просто был вовлечен)

BEP – BitTorrent Enhancement Proposal

- DHT – Distributed Hash Table – распределённая хеш-таблица
- PEX – Peer EXchange – расширение BitTorrent-протокола для обмена списками участников
- µTP – Micro Transport Protocol – транспортный протокол с контролем доставки (подобно TCP) на основе протокола UDP

http://www.bittorrent.org/beps/bep_0000.html

Спецификация PEX



bittorrent.org/beps/bep_0010.html

handshake message

The payload of the handshake message is a bencoded dictionary. All items in the dictionary are optional. names should be ignored by the client. All parts of the dictionary are case sensitive. This is the defined dictionary:

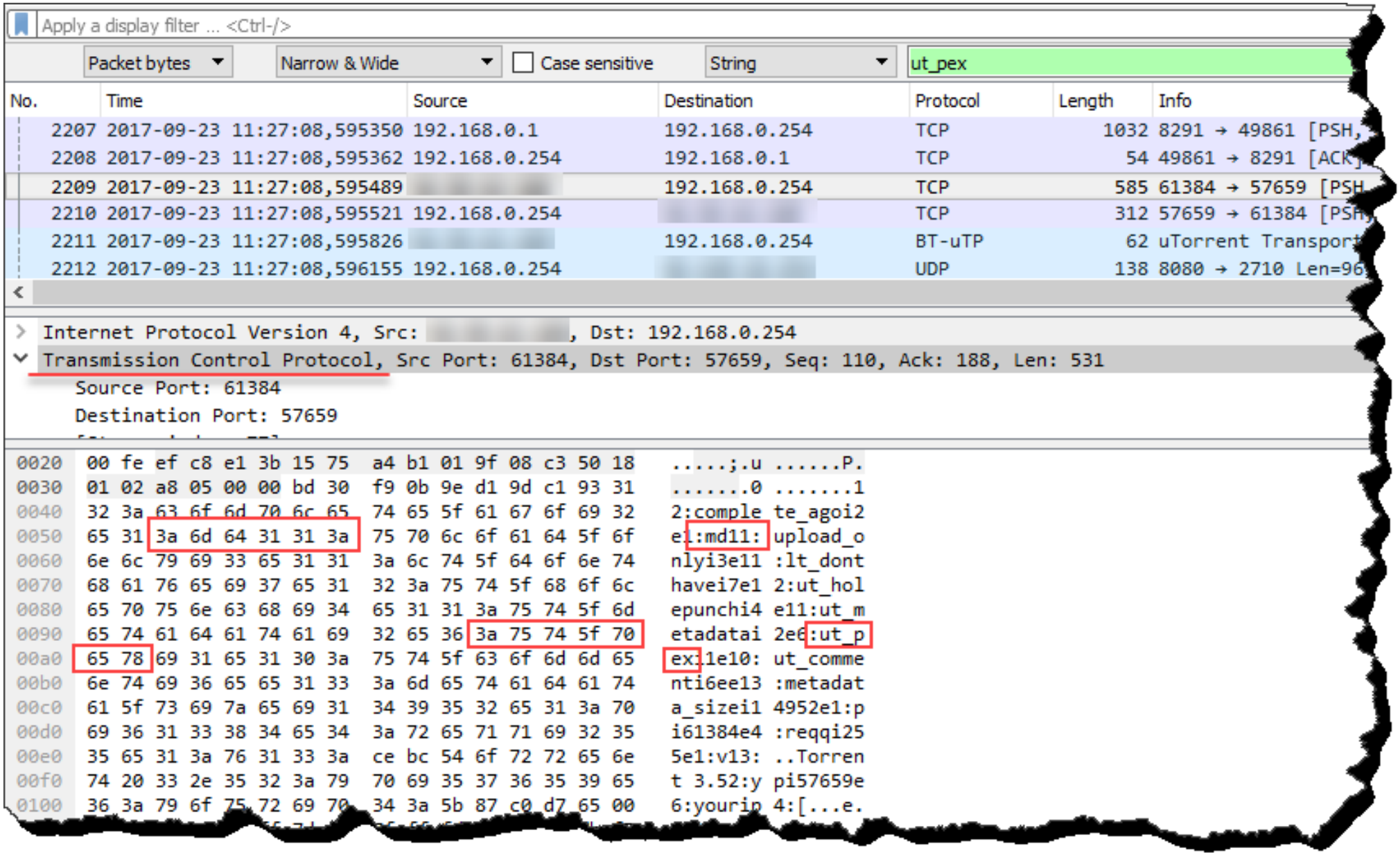
name	description
m	Dictionary of supported extension messages which maps names of ex... an extended message ID for ... extension message. The only requir...
p	6881
v	"µTorrent 1.2"

and in the encoded form:

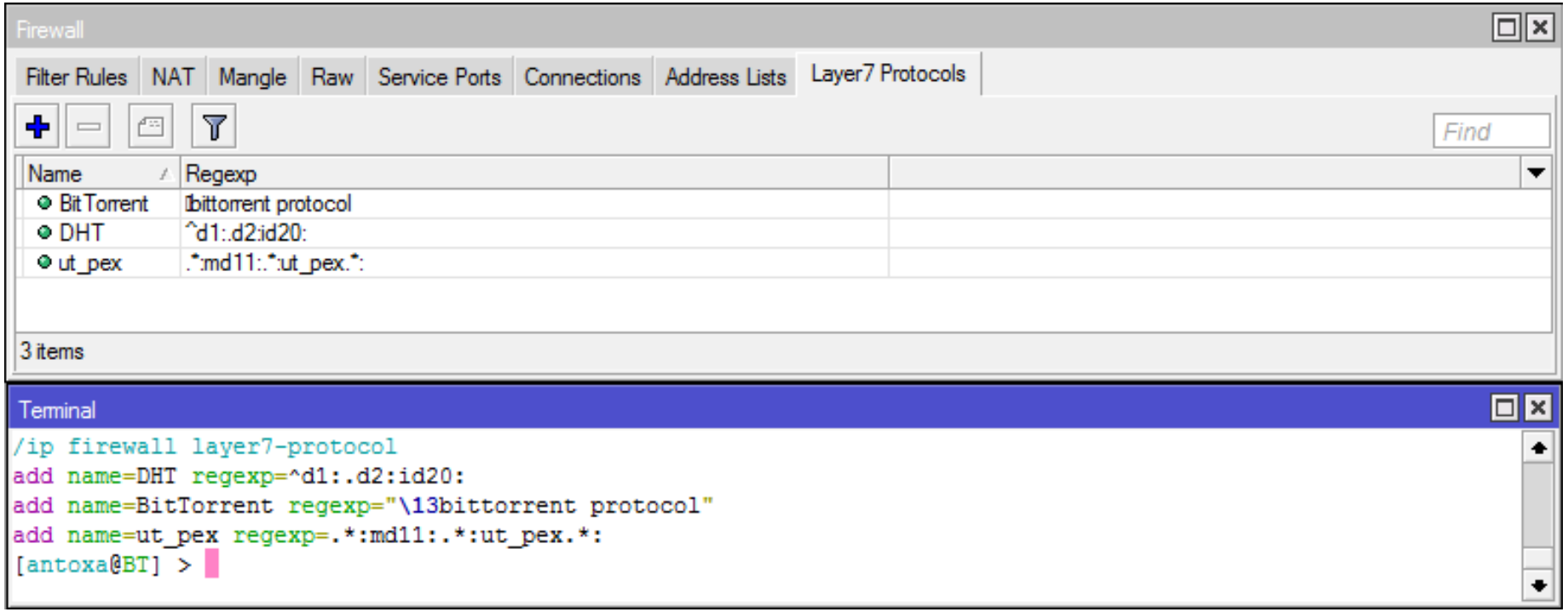
```
d1:md11:LT_metadatai1e6:µT_PEXi2ee1:pi6881e1:v13:\xc2\xb5Torrent 1.2e
```

To make sure the extension names do not collide by mistake, they should be prefixed with the two (or on... that is used to identify the client that introduced the extension. This applies ... the name...

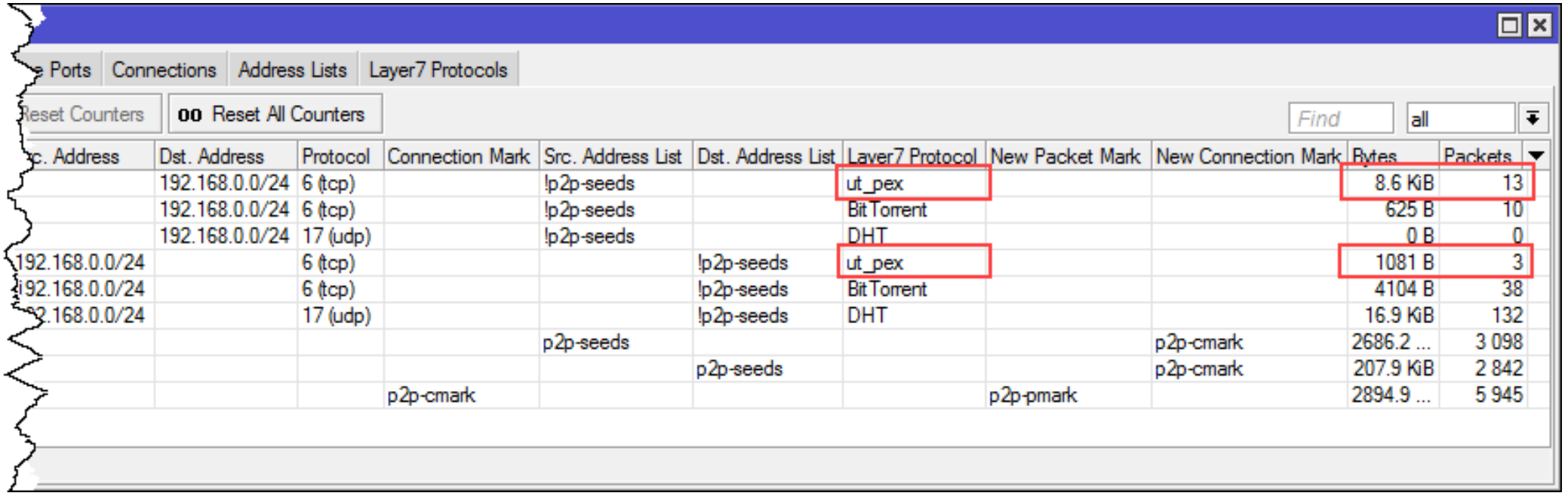
Wireshark PEX



RouterOS Layer7



Определение P2P соединений и маркировка пакетов

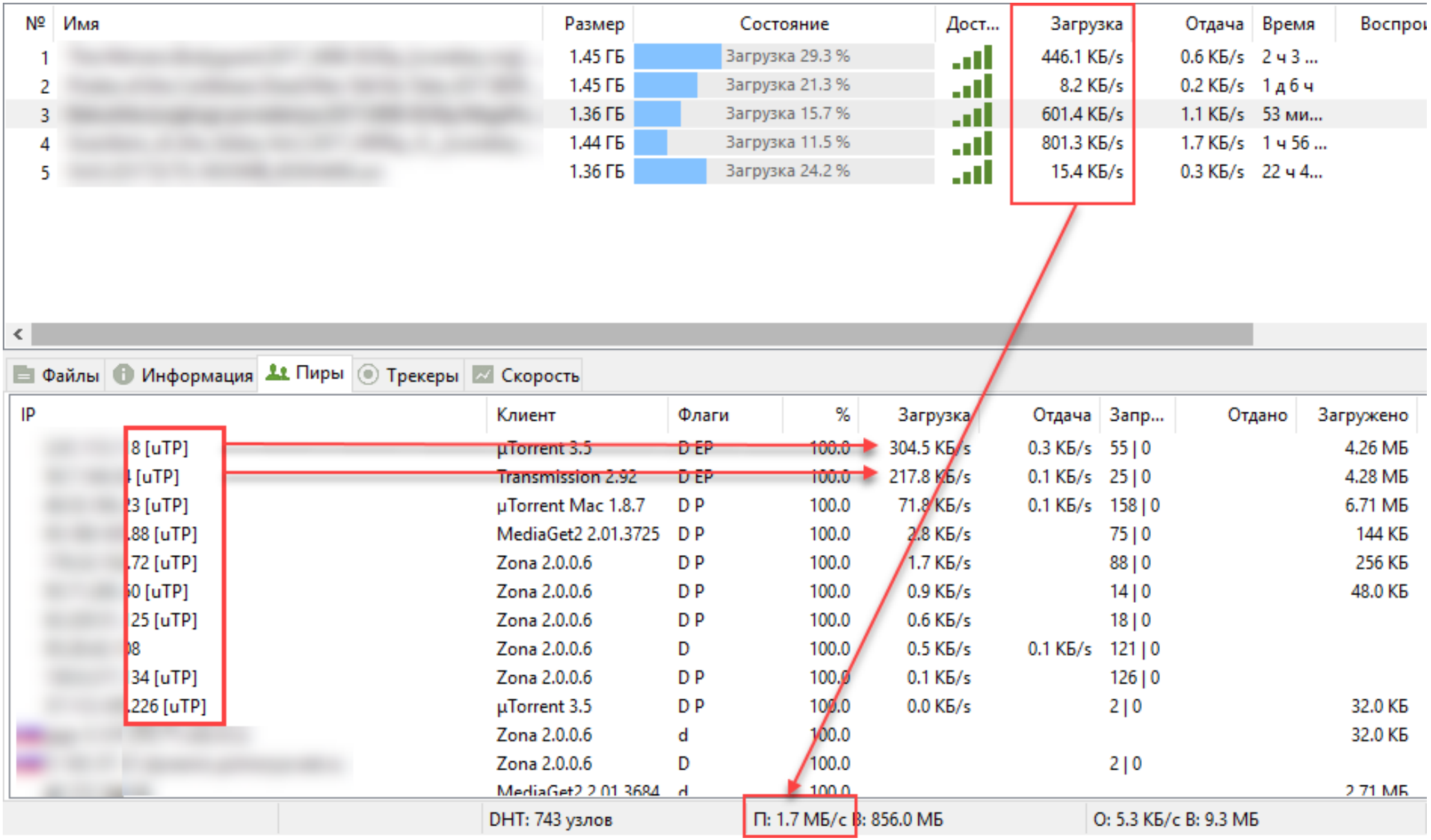


Ports | Connections | Address Lists | Layer7 Protocols

Reset Counters | 00 Reset All Counters | Find | all

c. Address	Dst. Address	Protocol	Connection Mark	Src. Address List	Dst. Address List	Layer7 Protocol	New Packet Mark	New Connection Mark	Bytes	Packets
	192.168.0.0/24	6 (tcp)		!p2p-seeds		ut_pex			8.6 KiB	13
	192.168.0.0/24	6 (tcp)		!p2p-seeds		BitTorrent			625 B	10
	192.168.0.0/24	17 (udp)		!p2p-seeds		DHT			0 B	0
192.168.0.0/24		6 (tcp)			!p2p-seeds	ut_pex			1081 B	3
192.168.0.0/24		6 (tcp)			!p2p-seeds	BitTorrent			4104 B	38
2.168.0.0/24		17 (udp)			!p2p-seeds	DHT			16.9 KiB	132
				p2p-seeds				p2p-cmark	2686.2 ...	3 098
					p2p-seeds			p2p-cmark	207.9 KiB	2 842
			p2p-cmark				p2p-pmark		2894.9 ...	5 945

Тестирование конфигурации



№	Имя	Размер	Состояние	Дост...	Загрузка	Отдача	Время	Воспрои
1		1.45 ГБ	Загрузка 29.3 %		446.1 КБ/s	0.6 КБ/s	2 ч 3 ...	
2		1.45 ГБ	Загрузка 21.3 %		8.2 КБ/s	0.2 КБ/s	1 д 6 ч	
3		1.36 ГБ	Загрузка 15.7 %		601.4 КБ/s	1.1 КБ/s	53 ми...	
4		1.44 ГБ	Загрузка 11.5 %		801.3 КБ/s	1.7 КБ/s	1 ч 56 ...	
5		1.36 ГБ	Загрузка 24.2 %		15.4 КБ/s	0.3 КБ/s	22 ч 4...	

Файлы | Информация | Пиры | Трекеры | Скорость

IP	Клиент	Флаги	%	Загрузка	Отдача	Запр...	Отдано	Загружено
8 [uTP]	µTorrent 3.5	D EP	100.0	304.5 КБ/s	0.3 КБ/s	55 | 0		4.26 МБ
[uTP]	Transmission 2.92	D EP	100.0	217.8 КБ/s	0.1 КБ/s	25 | 0		4.28 МБ
3 [uTP]	µTorrent Mac 1.8.7	D P	100.0	71.8 КБ/s	0.1 КБ/s	158 | 0		6.71 МБ
.88 [uTP]	MediaGet2 2.01.3725	D P	100.0	2.8 КБ/s		75 | 0		144 КБ
.72 [uTP]	Zona 2.0.0.6	D P	100.0	1.7 КБ/s		88 | 0		256 КБ
0 [uTP]	Zona 2.0.0.6	D P	100.0	0.9 КБ/s		14 | 0		48.0 КБ
25 [uTP]	Zona 2.0.0.6	D P	100.0	0.6 КБ/s		18 | 0		
8	Zona 2.0.0.6	D	100.0	0.5 КБ/s	0.1 КБ/s	121 | 0		
34 [uTP]	Zona 2.0.0.6	D P	100.0	0.1 КБ/s		126 | 0		
.226 [uTP]	µTorrent 3.5	D P	100.0	0.0 КБ/s		2 | 0		32.0 КБ
	Zona 2.0.0.6	d	100.0					32.0 КБ
	Zona 2.0.0.6	D	100.0			2 | 0		
	MediaGet2 2.01.3684	d	100.0					2.71 МБ

DHT: 743 узлов | П: 1.7 МБ/с В: 856.0 МБ | О: 5.3 КБ/с В: 9.3 МБ

µTP – Micro Transport Protocol

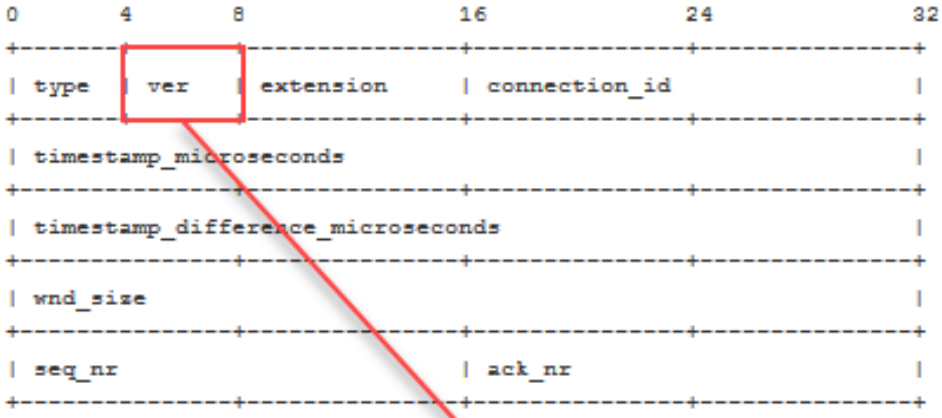
- транспортный протокол с контролем доставки (подобно TCP) на основе протокола UDP
- предназначен для более быстрого скачивания, так как работает по протоколу UDP
- ускорение достигается за счёт того, что торрент-клиент берёт на себя выполнение нужных функций, отсутствующих в UDP, например, клиент перепроверяет целостность данных и, если блок неверен, скачивает его заново

Спецификация µTP

bittorrent.org/beps/bep_0029.html

header format

version 1 header:



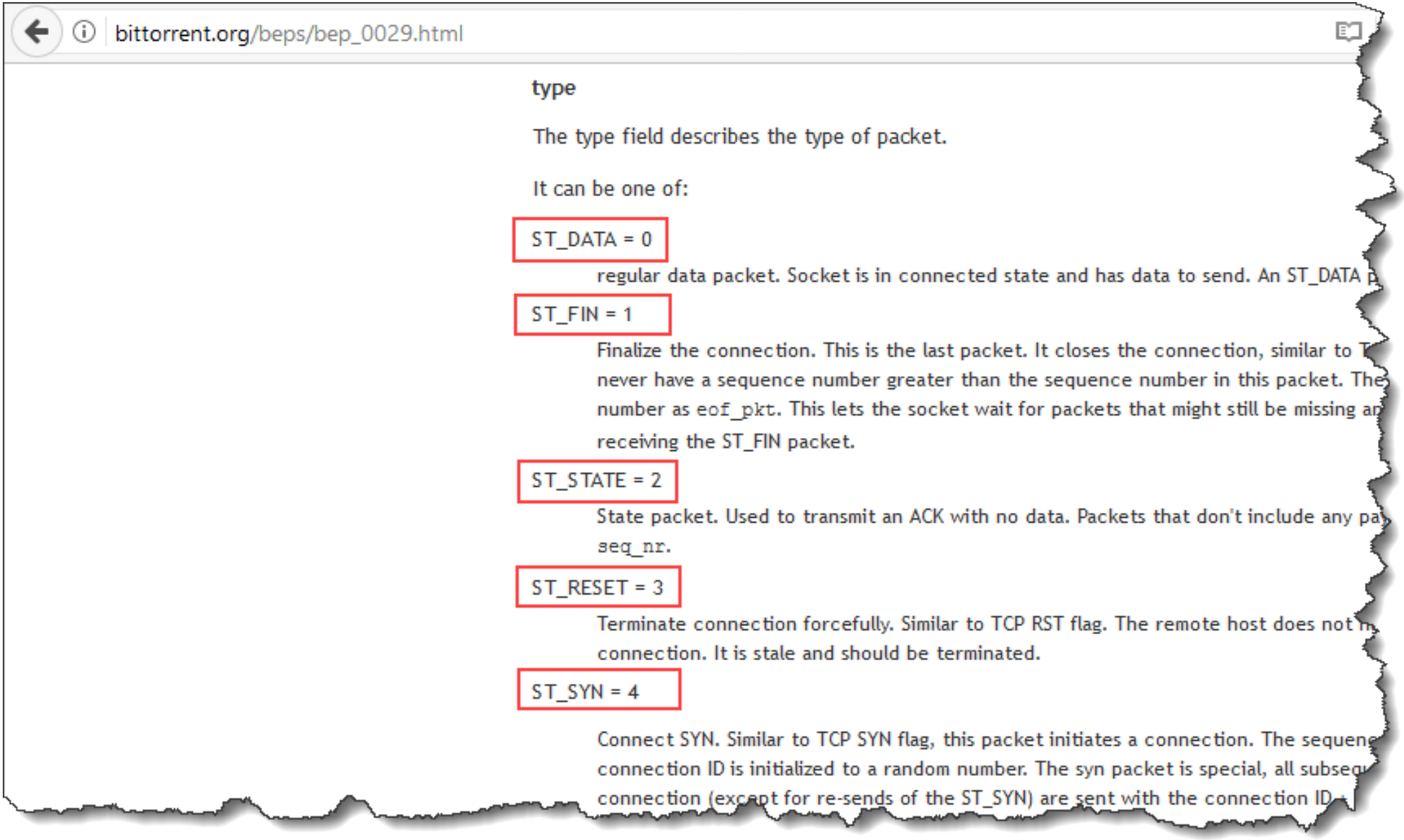
All fields are in network byte order (big endian).

version

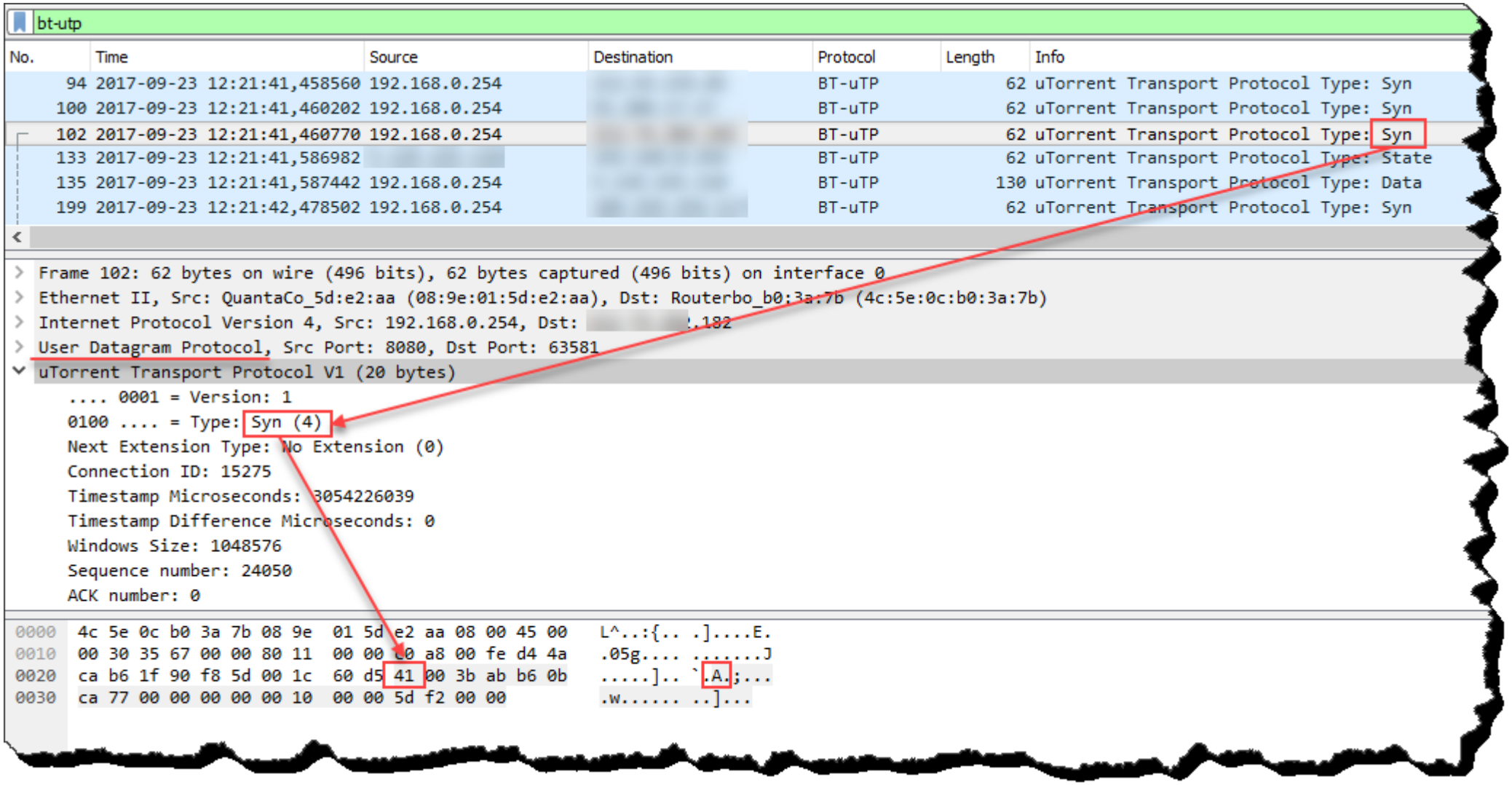
This is the protocol version. The current version is 1.

connection_id

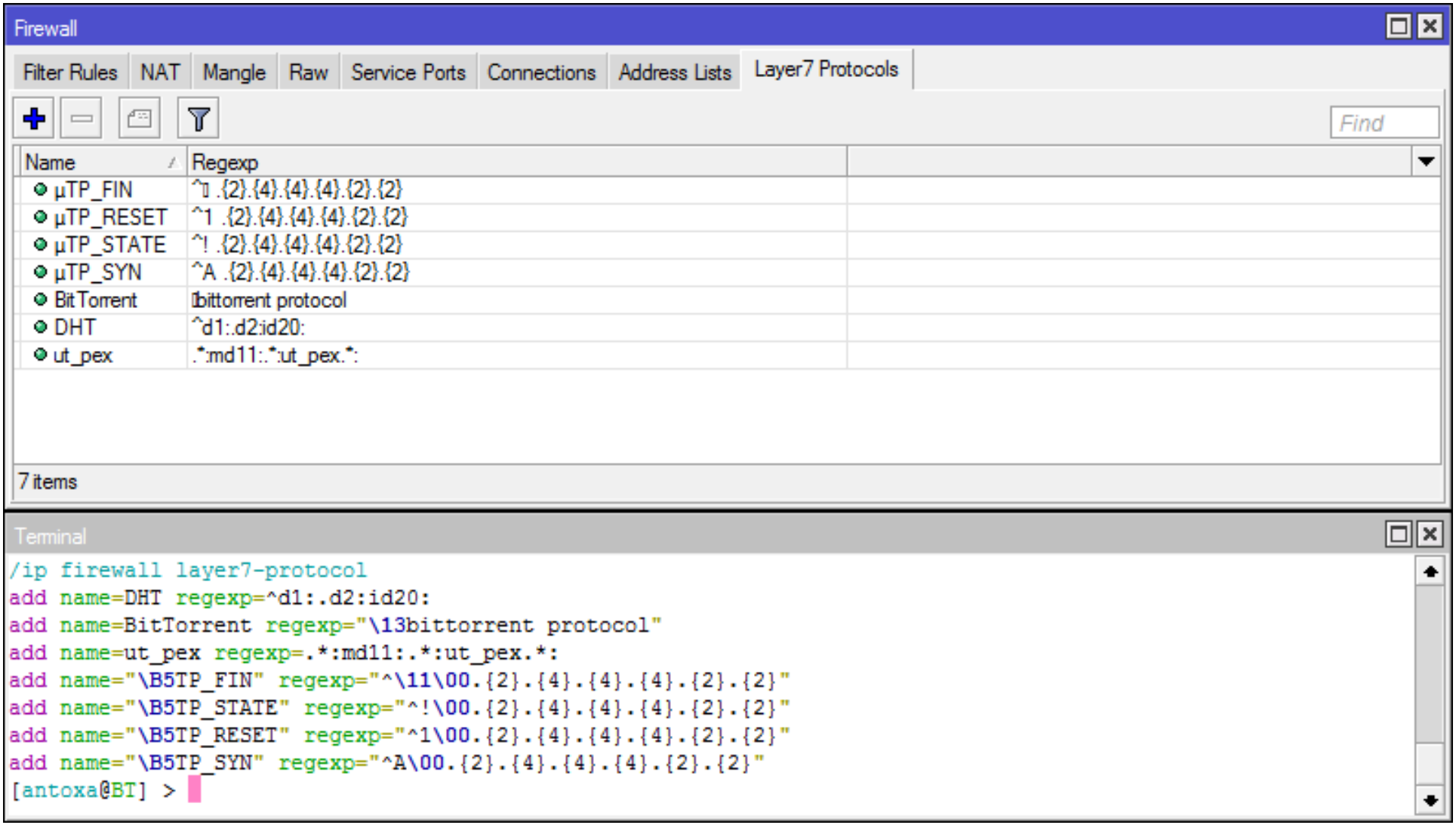
Спецификация µTP



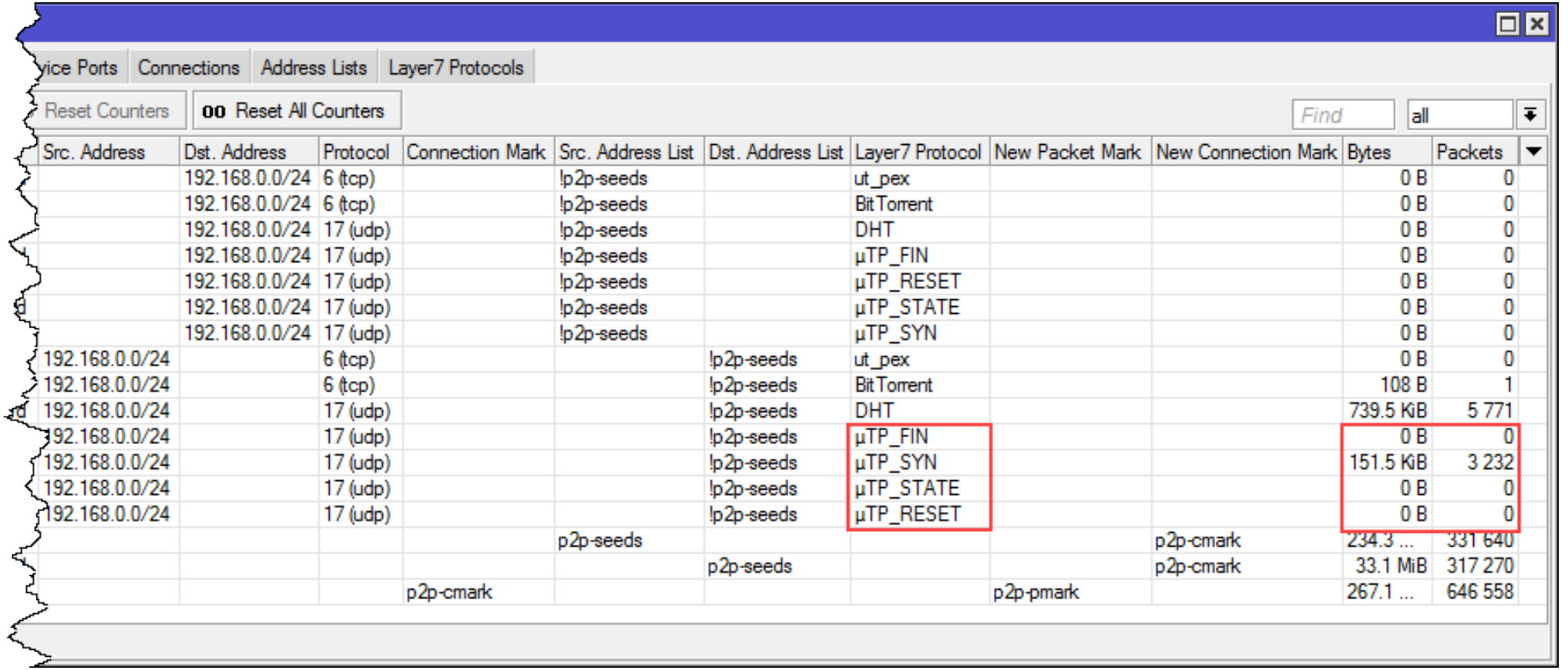
Wireshark µTP



RouterOS Layer7



Определение P2P соединений и маркировка пакетов

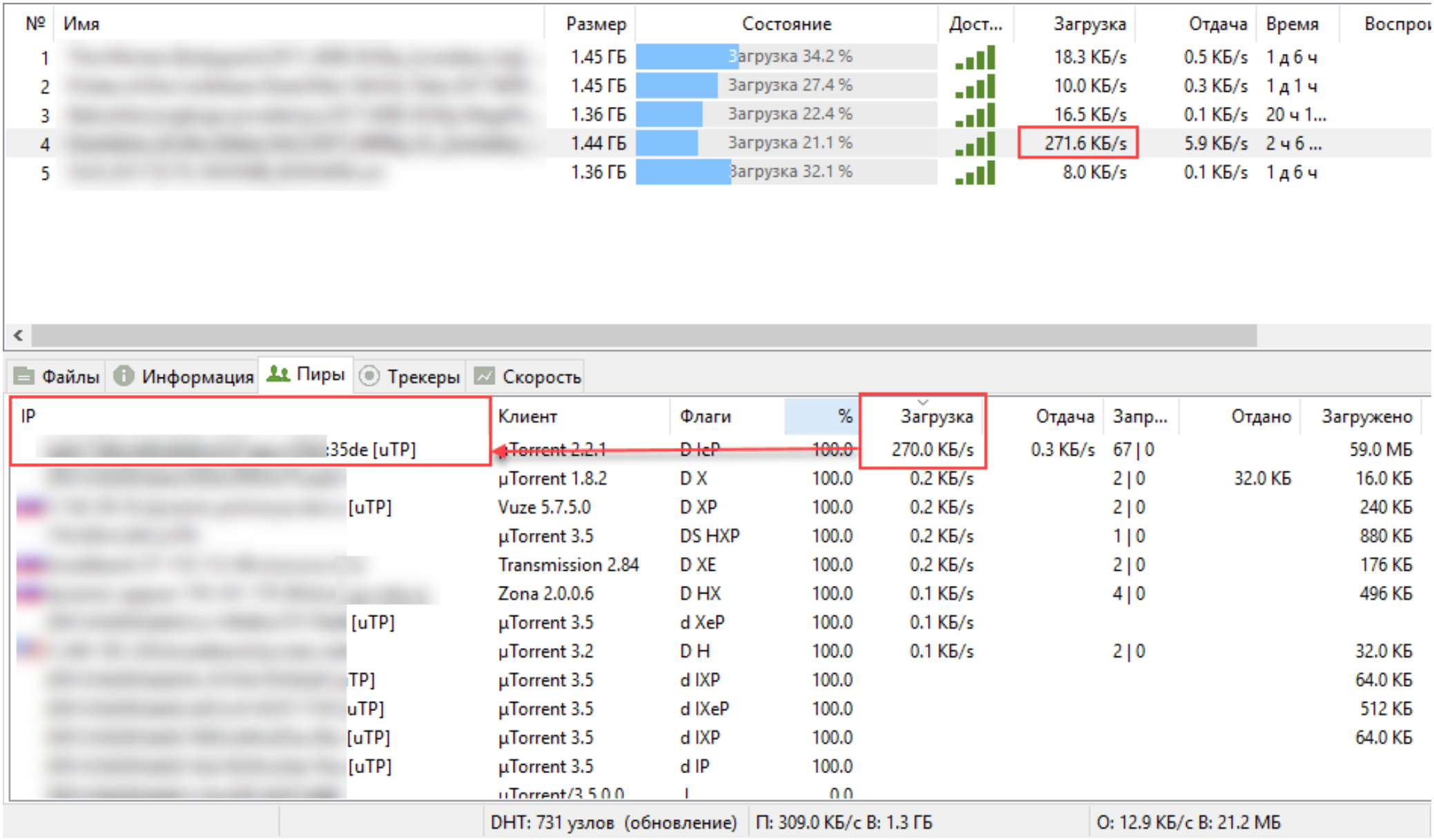


vice Ports | Connections | Address Lists | Layer7 Protocols

Reset Counters | oo Reset All Counters | Find | all

Src. Address	Dst. Address	Protocol	Connection Mark	Src. Address List	Dst. Address List	Layer7 Protocol	New Packet Mark	New Connection Mark	Bytes	Packets
	192.168.0.0/24	6 (tcp)		!p2p-seeds		ut_pex			0 B	0
	192.168.0.0/24	6 (tcp)		!p2p-seeds		BitTorrent			0 B	0
	192.168.0.0/24	17 (udp)		!p2p-seeds		DHT			0 B	0
	192.168.0.0/24	17 (udp)		!p2p-seeds		µTP_FIN			0 B	0
	192.168.0.0/24	17 (udp)		!p2p-seeds		µTP_RESET			0 B	0
	192.168.0.0/24	17 (udp)		!p2p-seeds		µTP_STATE			0 B	0
	192.168.0.0/24	17 (udp)		!p2p-seeds		µTP_SYN			0 B	0
192.168.0.0/24		6 (tcp)			!p2p-seeds	ut_pex			0 B	0
192.168.0.0/24		6 (tcp)			!p2p-seeds	BitTorrent			108 B	1
192.168.0.0/24		17 (udp)			!p2p-seeds	DHT			739.5 KiB	5 771
192.168.0.0/24		17 (udp)			!p2p-seeds	µTP_FIN			0 B	0
192.168.0.0/24		17 (udp)			!p2p-seeds	µTP_SYN			151.5 KiB	3 232
192.168.0.0/24		17 (udp)			!p2p-seeds	µTP_STATE			0 B	0
192.168.0.0/24		17 (udp)			!p2p-seeds	µTP_RESET			0 B	0
				p2p-seeds				p2p-cmark	234.3 ...	331 640
					p2p-seeds			p2p-cmark	33.1 MiB	317 270
			p2p-cmark				p2p-pmark		267.1 ...	646 558

Тестирование конфигурации



№	Имя	Размер	Состояние	Дост...	Загрузка	Отдача	Время	Воспрои
1		1.45 ГБ	Загрузка 34.2 %		18.3 КБ/s	0.5 КБ/s	1 д 6 ч	
2		1.45 ГБ	Загрузка 27.4 %		10.0 КБ/s	0.3 КБ/s	1 д 1 ч	
3		1.36 ГБ	Загрузка 22.4 %		16.5 КБ/s	0.1 КБ/s	20 ч 1...	
4		1.44 ГБ	Загрузка 21.1 %		271.6 КБ/s	5.9 КБ/s	2 ч 6 ...	
5		1.36 ГБ	Загрузка 32.1 %		8.0 КБ/s	0.1 КБ/s	1 д 6 ч	

Файлы | Информация | Пиры | Трекеры | Скорость

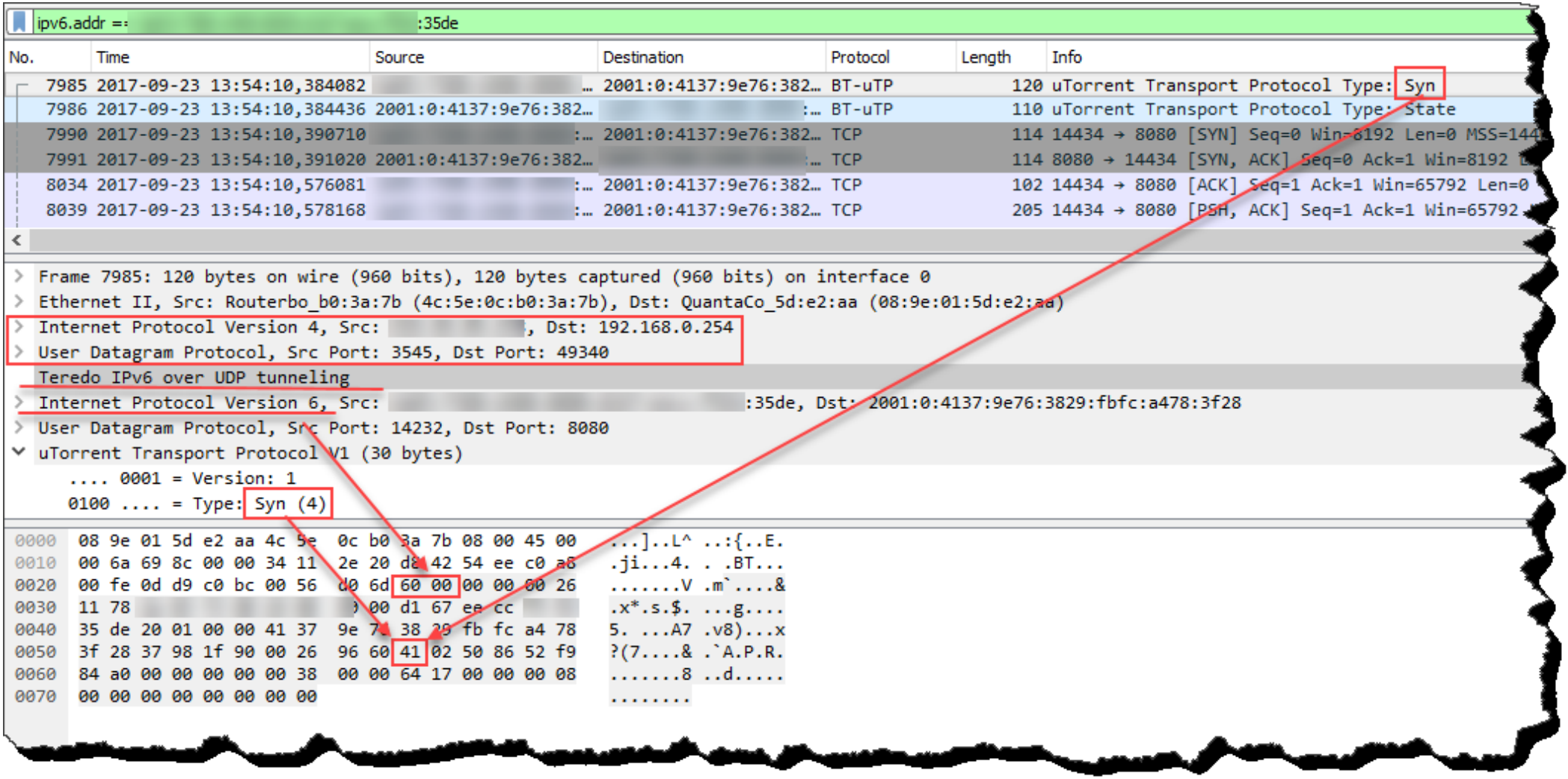
IP	Клиент	Флаги	%	Загрузка	Отдача	Запр...	Отдано	Загружено
:35de [uTP]	µTorrent 2.2.1	D IcP	100.0	270.0 КБ/s	0.3 КБ/s	67 | 0		59.0 МБ
	µTorrent 1.8.2	D X	100.0	0.2 КБ/s		2 | 0	32.0 КБ	16.0 КБ
[uTP]	Vuze 5.7.5.0	D XP	100.0	0.2 КБ/s		2 | 0		240 КБ
	µTorrent 3.5	DS HXP	100.0	0.2 КБ/s		1 | 0		880 КБ
	Transmission 2.84	D XE	100.0	0.2 КБ/s		2 | 0		176 КБ
	Zona 2.0.0.6	D HX	100.0	0.1 КБ/s		4 | 0		496 КБ
[uTP]	µTorrent 3.5	d XeP	100.0	0.1 КБ/s				
	µTorrent 3.2	D H	100.0	0.1 КБ/s		2 | 0		32.0 КБ
TP]	µTorrent 3.5	d IXP	100.0					64.0 КБ
uTP]	µTorrent 3.5	d IXeP	100.0					512 КБ
[uTP]	µTorrent 3.5	d IXP	100.0					64.0 КБ
[uTP]	µTorrent 3.5	d IP	100.0					
	µTorrent/3.5.0.0	I	0.0					

DHT: 731 узлов (обновление) | П: 309.0 КБ/с В: 1.3 ГБ | О: 12.9 КБ/с В: 21.2 МБ

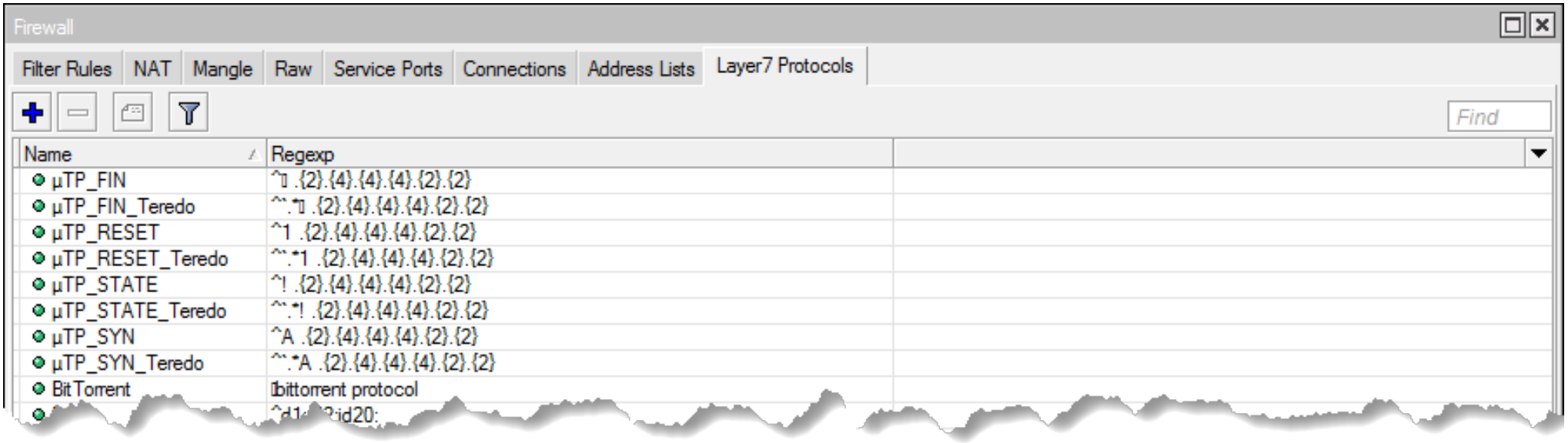
Teredo

- Teredo – сетевой протокол, предназначенный для передачи IPv6 пакетов через сети IPv4, путём их инкапсуляции в UDP-дейтаграммы
- Использует UDP порт 3544

Wireshark Teredo

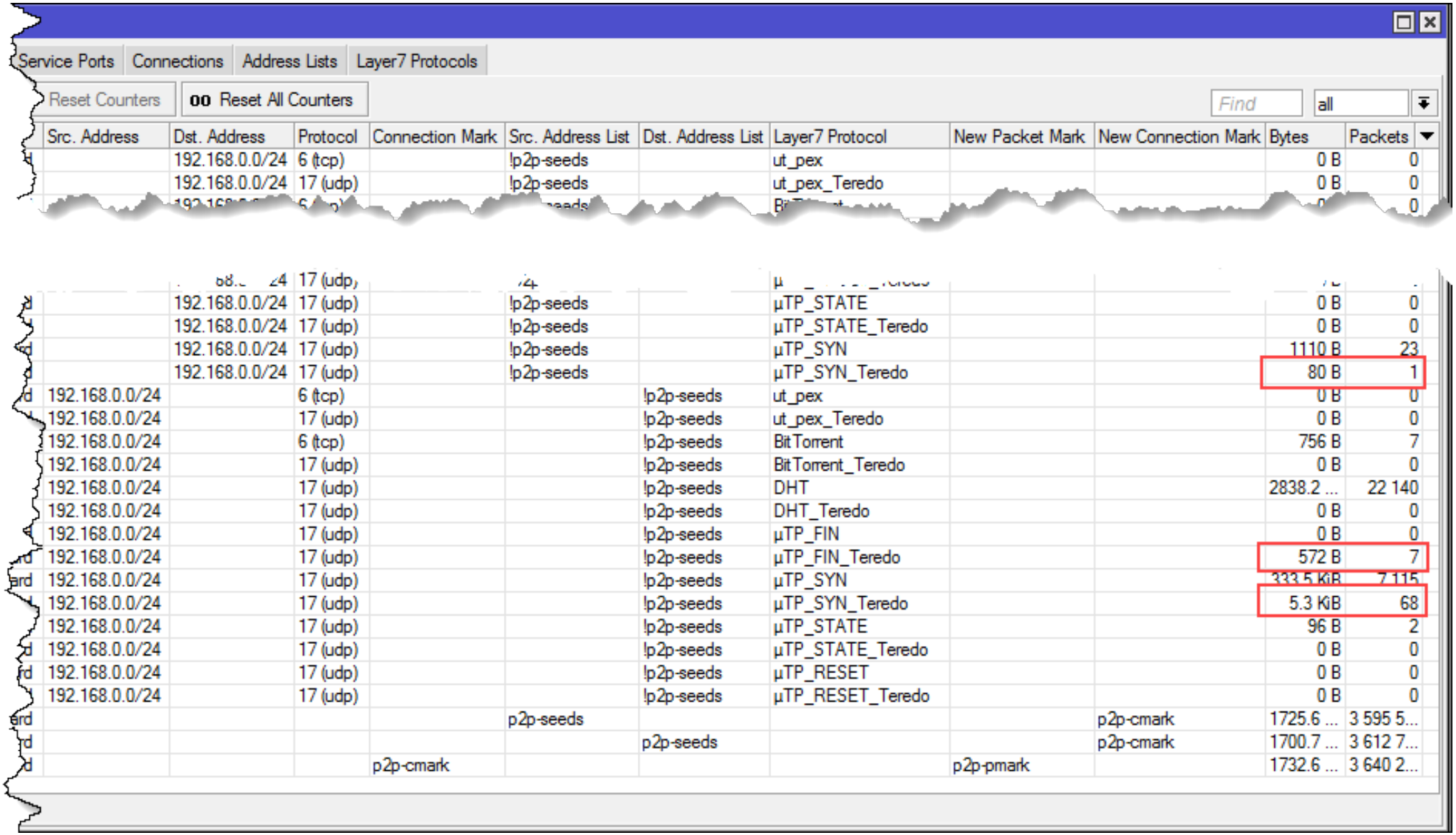


RouterOS Layer7




```
# serial number = 522604A2270A
/ip firewall layer7-protocol
add name=DHT regexp=^d1:.d2:id20:
add name=BitTorrent regexp="\13bittorrent protocol"
add name=ut_pex regexp=.*:md11:.*:ut_pex.*:
add name="\B5TP_FIN" regexp="^\11\00.{2}.{4}.{4}.{4}.{2}.{2}"
add name="\B5TP_STATE" regexp="^!\00.{2}.{4}.{4}.{4}.{2}.{2}"
add name="\B5TP_RESET" regexp="^1\00.{2}.{4}.{4}.{4}.{2}.{2}"
add name="\B5TP_SYN" regexp="^A\00.{2}.{4}.{4}.{4}.{2}.{2}"
add name=bittorrent_Teredo regexp="^`.*\13bittorrent protocol"
add name=DHT_Teredo regexp="^`.*d1:[a|r]d2:id20:.*y1:[q|r]e"
add name=ut_pex_Teredo regexp="^`.*:md11:.*:ut_pex.*"
add name="\B5TP_SYN_Teredo" regexp="^`.*A\00.{2}.{4}.{4}.{4}.{2}.{2}"
add name="\B5TP_STATE_Teredo" regexp="^`.*!\00.{2}.{4}.{4}.{4}.{2}.{2}"
add name="\B5TP_RESET_Teredo" regexp="^`.*1\00.{2}.{4}.{4}.{4}.{2}.{2}"
add name="\B5TP_FIN_Teredo" regexp="^`.*\11\00.{2}.{4}.{4}.{4}.{2}.{2}"
[antoxa@BT] >
```

Определение P2P соединений и маркировка пакетов

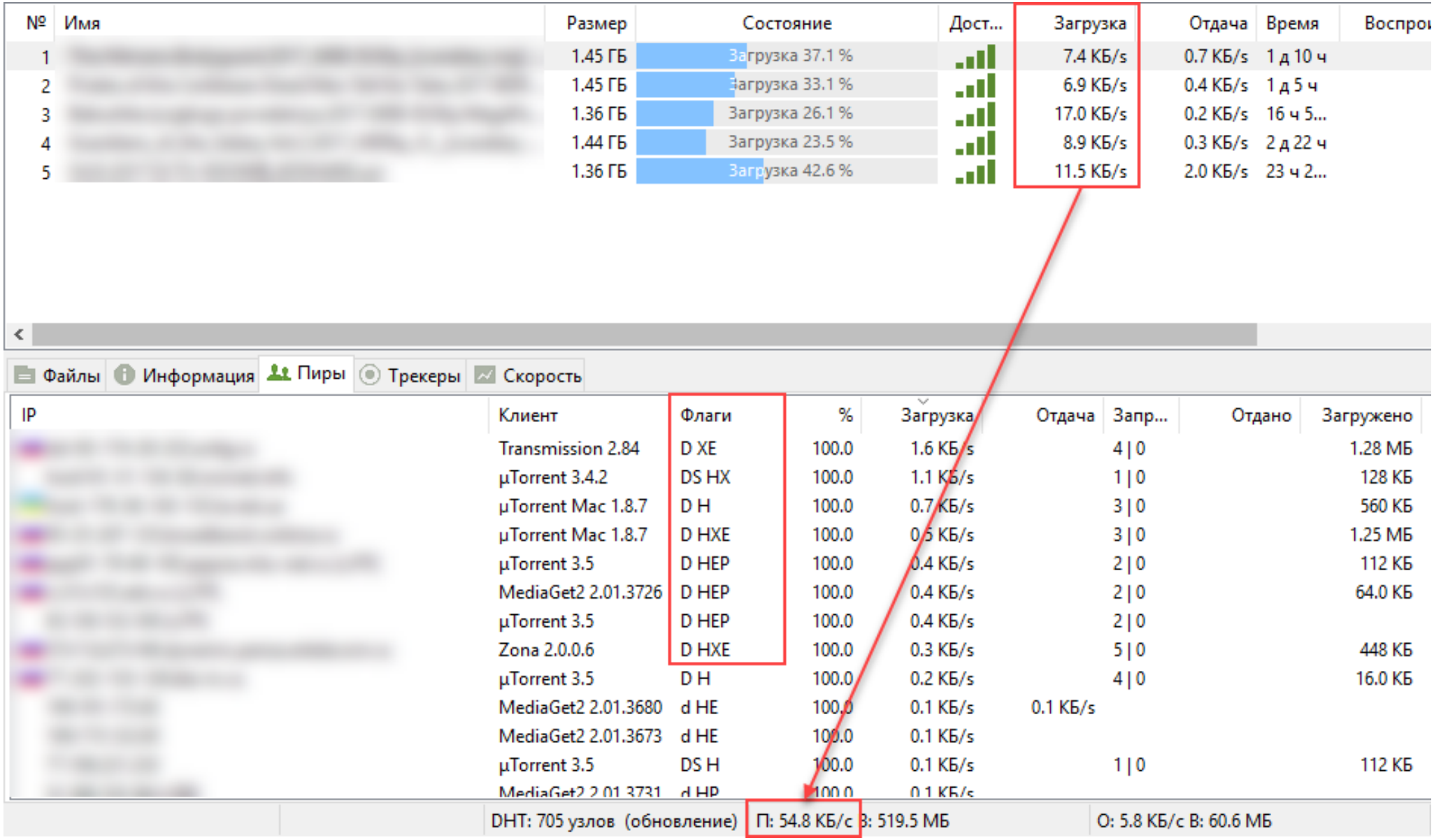


Service Ports | Connections | Address Lists | Layer7 Protocols

Reset Counters | 00 Reset All Counters | Find | all

Src. Address	Dst. Address	Protocol	Connection Mark	Src. Address List	Dst. Address List	Layer7 Protocol	New Packet Mark	New Connection Mark	Bytes	Packets
	192.168.0.0/24	6 (tcp)		!p2p-seeds		ut_pex			0 B	0
	192.168.0.0/24	17 (udp)		!p2p-seeds		ut_pex_Teredo			0 B	0
		17 (udp)								
	192.168.0.0/24	17 (udp)		!p2p-seeds		µTP_STATE			0 B	0
	192.168.0.0/24	17 (udp)		!p2p-seeds		µTP_STATE_Teredo			0 B	0
	192.168.0.0/24	17 (udp)		!p2p-seeds		µTP_SYN			1110 B	23
	192.168.0.0/24	17 (udp)		!p2p-seeds		µTP_SYN_Teredo			80 B	1
192.168.0.0/24		6 (tcp)			!p2p-seeds	ut_pex			0 B	0
192.168.0.0/24		17 (udp)			!p2p-seeds	ut_pex_Teredo			0 B	0
192.168.0.0/24		6 (tcp)			!p2p-seeds	BitTorrent			756 B	7
192.168.0.0/24		17 (udp)			!p2p-seeds	BitTorrent_Teredo			0 B	0
192.168.0.0/24		17 (udp)			!p2p-seeds	DHT			2838.2 ...	22 140
192.168.0.0/24		17 (udp)			!p2p-seeds	DHT_Teredo			0 B	0
192.168.0.0/24		17 (udp)			!p2p-seeds	µTP_FIN			0 B	0
192.168.0.0/24		17 (udp)			!p2p-seeds	µTP_FIN_Teredo			572 B	7
192.168.0.0/24		17 (udp)			!p2p-seeds	µTP_SYN			333.5 KiB	7 115
192.168.0.0/24		17 (udp)			!p2p-seeds	µTP_SYN_Teredo			5.3 KiB	68
192.168.0.0/24		17 (udp)			!p2p-seeds	µTP_STATE			96 B	2
192.168.0.0/24		17 (udp)			!p2p-seeds	µTP_STATE_Teredo			0 B	0
192.168.0.0/24		17 (udp)			!p2p-seeds	µTP_RESET			0 B	0
192.168.0.0/24		17 (udp)			!p2p-seeds	µTP_RESET_Teredo			0 B	0
				p2p-seeds				p2p-cmark	1725.6 ...	3 595 5...
					p2p-seeds			p2p-cmark	1700.7 ...	3 612 7...
			p2p-cmark				p2p-pmark		1732.6 ...	3 640 2...

Тестирование конфигурации



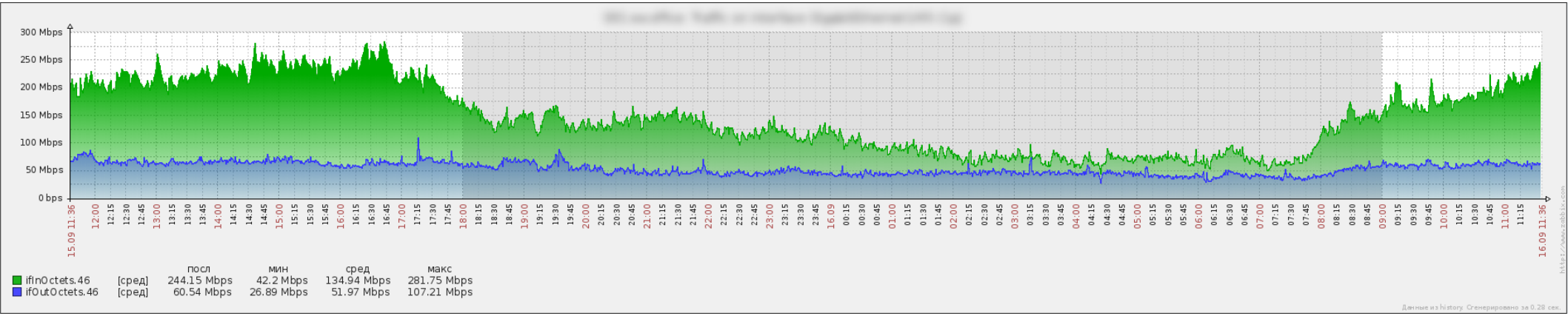
№	Имя	Размер	Состояние	Дост...	Загрузка	Отдача	Время	Воспрои
1		1.45 ГБ	Загрузка 37.1 %		7.4 КБ/s	0.7 КБ/s	1 д 10 ч	
2		1.45 ГБ	Загрузка 33.1 %		6.9 КБ/s	0.4 КБ/s	1 д 5 ч	
3		1.36 ГБ	Загрузка 26.1 %		17.0 КБ/s	0.2 КБ/s	16 ч 5...	
4		1.44 ГБ	Загрузка 23.5 %		8.9 КБ/s	0.3 КБ/s	2 д 22 ч	
5		1.36 ГБ	Загрузка 42.6 %		11.5 КБ/s	2.0 КБ/s	23 ч 2...	

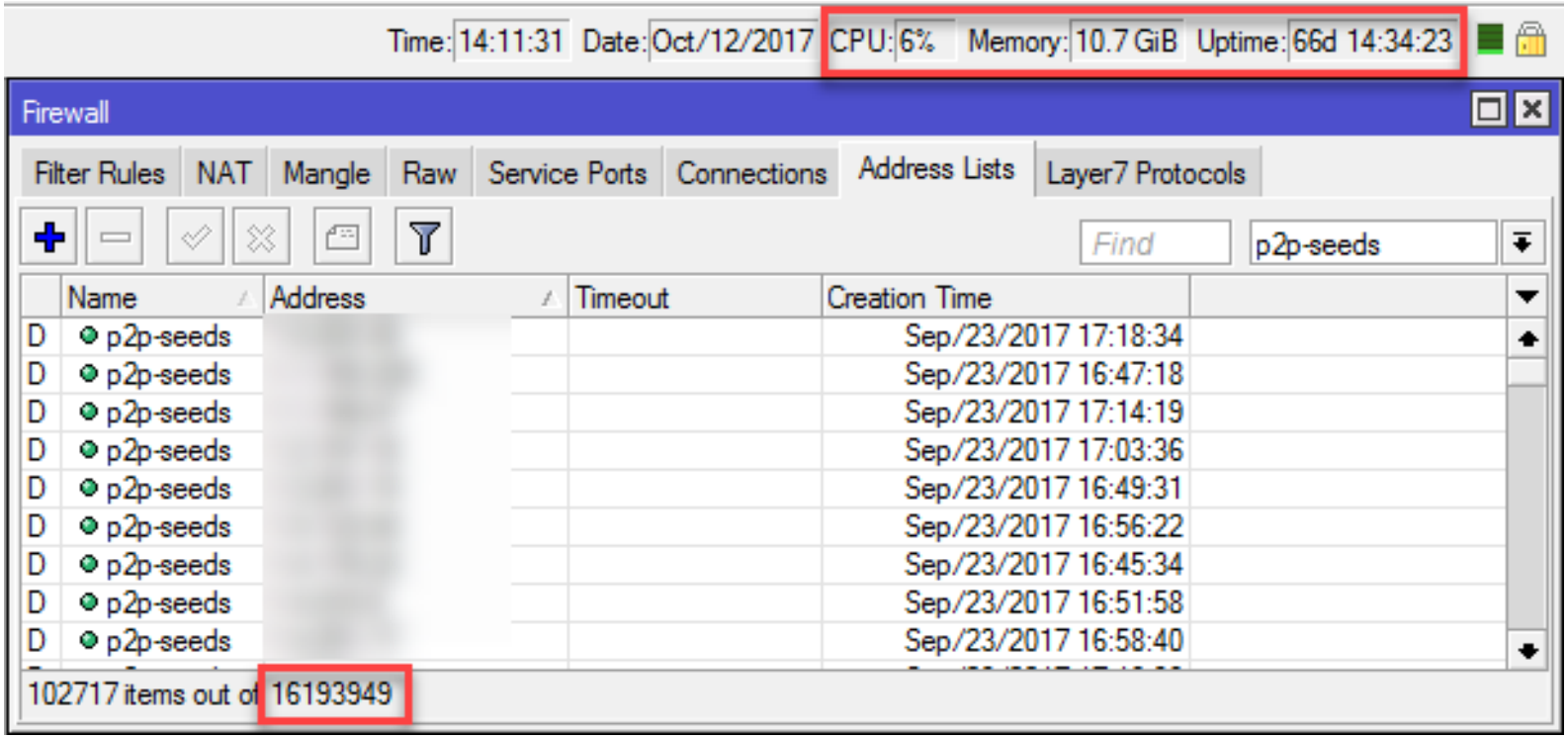
Файлы | Информация | Пиры | Трекеры | Скорость

IP	Клиент	Флаги	%	Загрузка	Отдача	Запр...	Отдано	Загружено
	Transmission 2.84	D XE	100.0	1.6 КБ/s		4 | 0		1.28 МБ
	µTorrent 3.4.2	DS HX	100.0	1.1 КБ/s		1 | 0		128 КБ
	µTorrent Mac 1.8.7	D H	100.0	0.7 КБ/s		3 | 0		560 КБ
	µTorrent Mac 1.8.7	D HXE	100.0	0.5 КБ/s		3 | 0		1.25 МБ
	µTorrent 3.5	D HEP	100.0	0.4 КБ/s		2 | 0		112 КБ
	MediaGet2 2.01.3726	D HEP	100.0	0.4 КБ/s		2 | 0		64.0 КБ
	µTorrent 3.5	D HEP	100.0	0.4 КБ/s		2 | 0		
	Zona 2.0.0.6	D HXE	100.0	0.3 КБ/s		5 | 0		448 КБ
	µTorrent 3.5	D H	100.0	0.2 КБ/s		4 | 0		16.0 КБ
	MediaGet2 2.01.3680	d HE	100.0	0.1 КБ/s	0.1 КБ/s			
	MediaGet2 2.01.3673	d HE	100.0	0.1 КБ/s				
	µTorrent 3.5	DS H	100.0	0.1 КБ/s		1 | 0		112 КБ
	MediaGet2 2.01.3731	d HP	100.0	0.1 КБ/s				

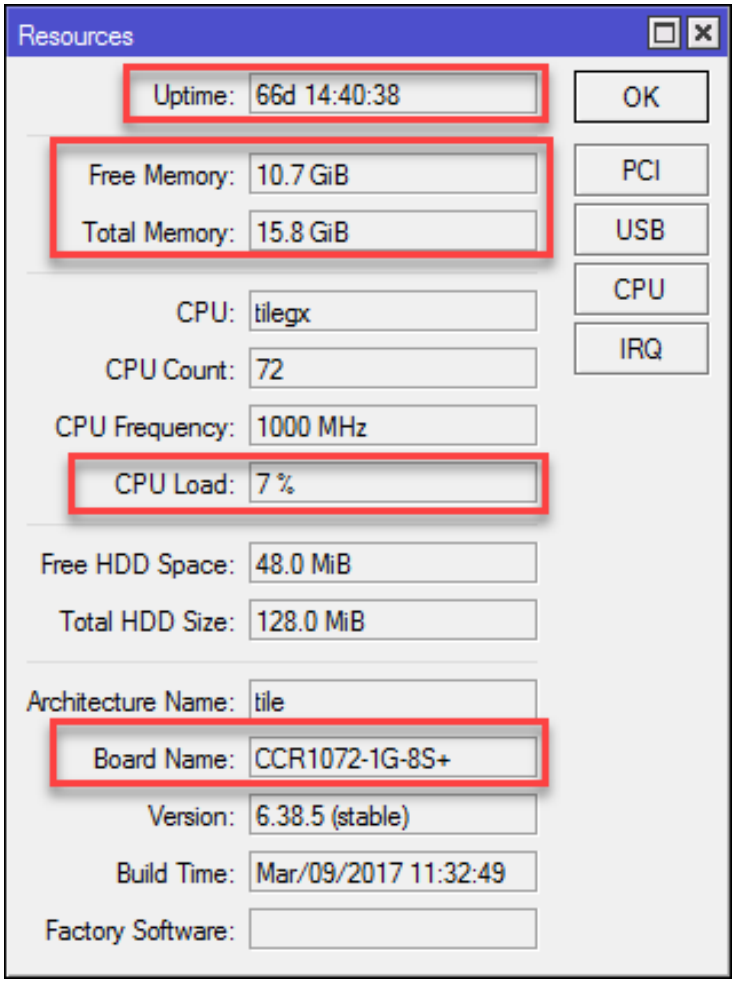
DHT: 705 узлов (обновление) | П: 54.8 КБ/с | В: 519.5 МБ | О: 5.8 КБ/с В: 60.6 МБ

Опыт эксплуатации

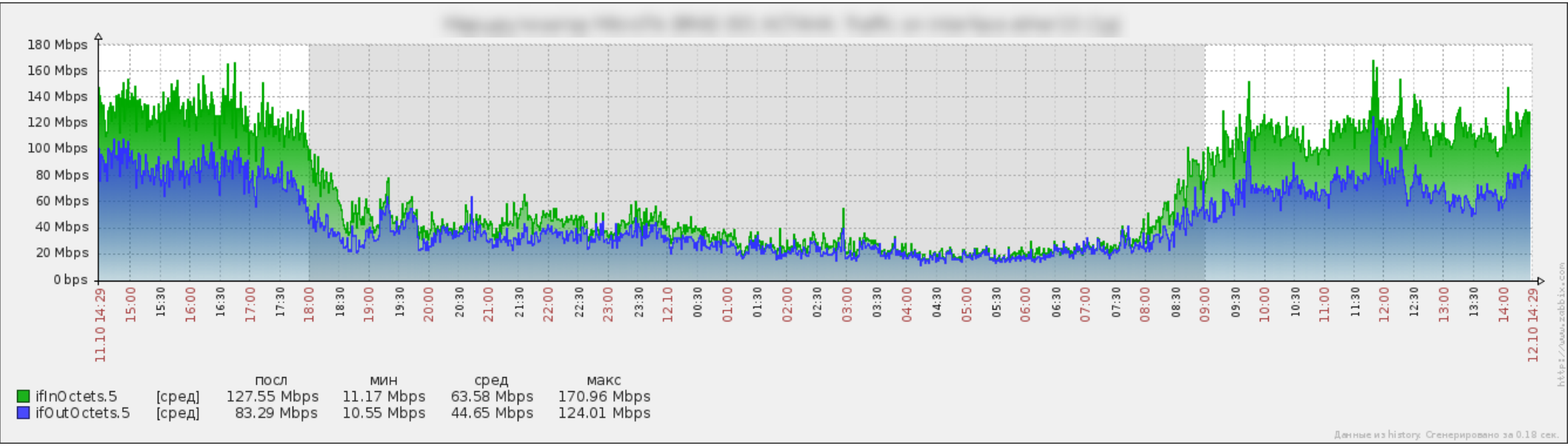


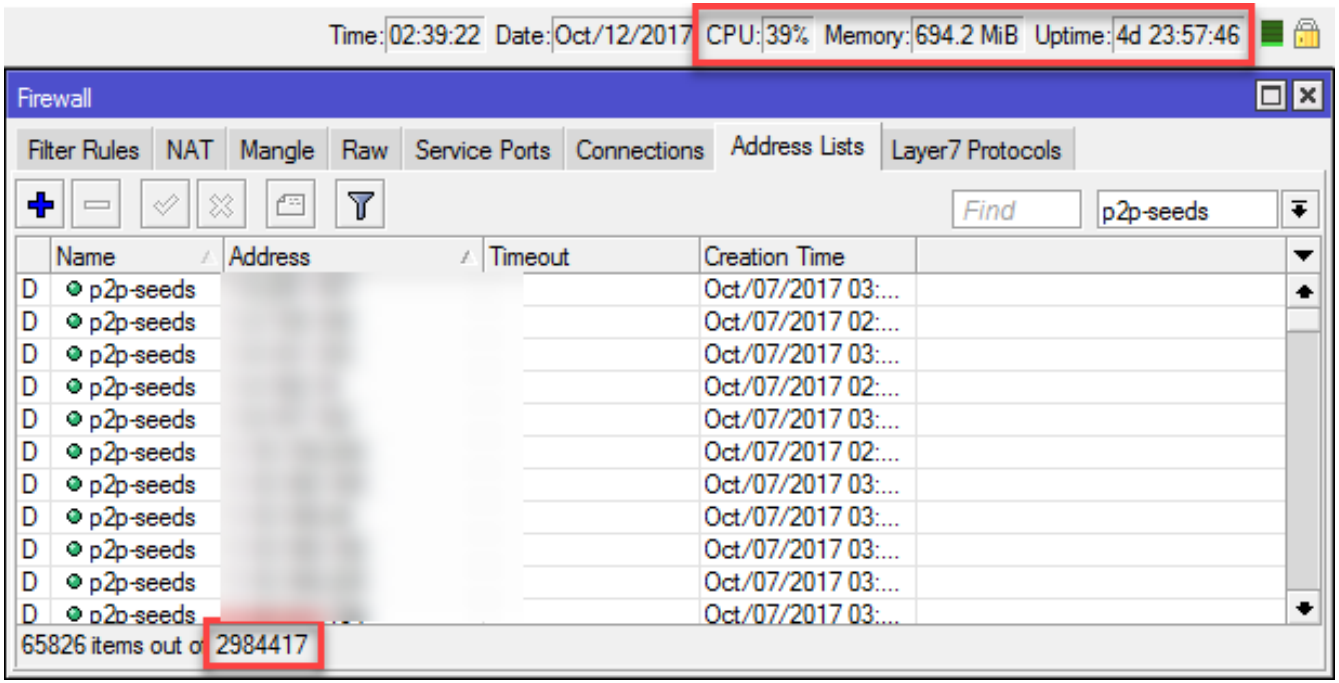


Опыт эксплуатации

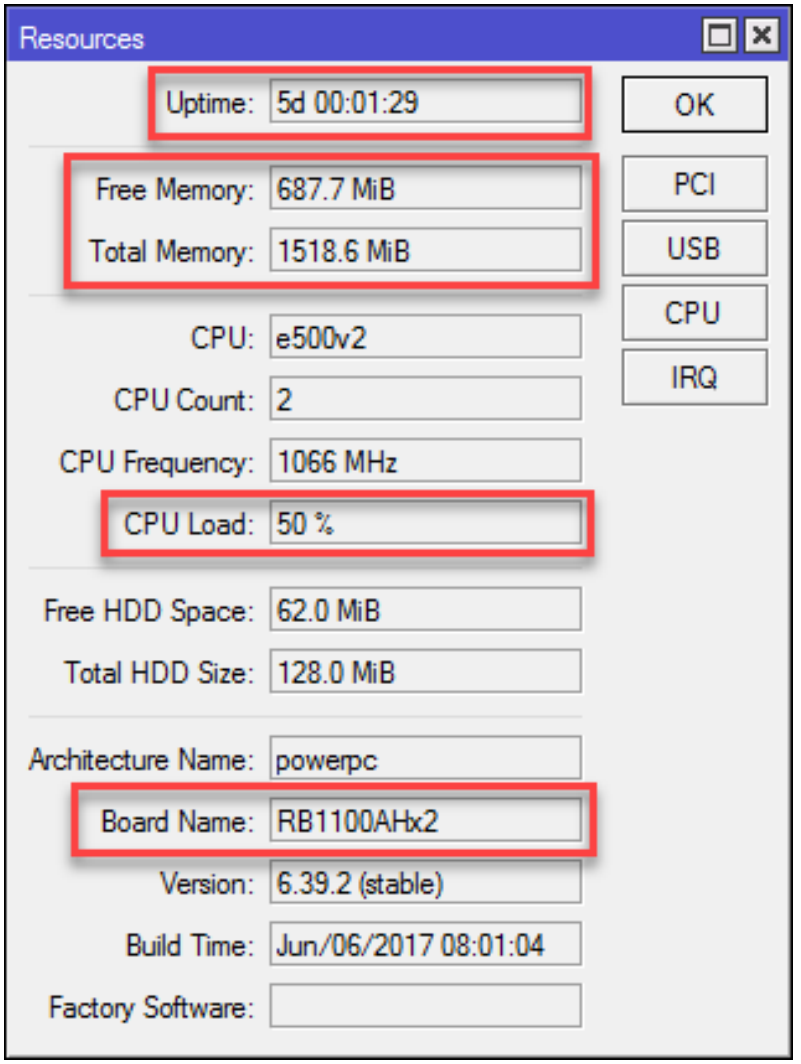


Опыт эксплуатации





Опыт эксплуатации



Спасибо за внимание!