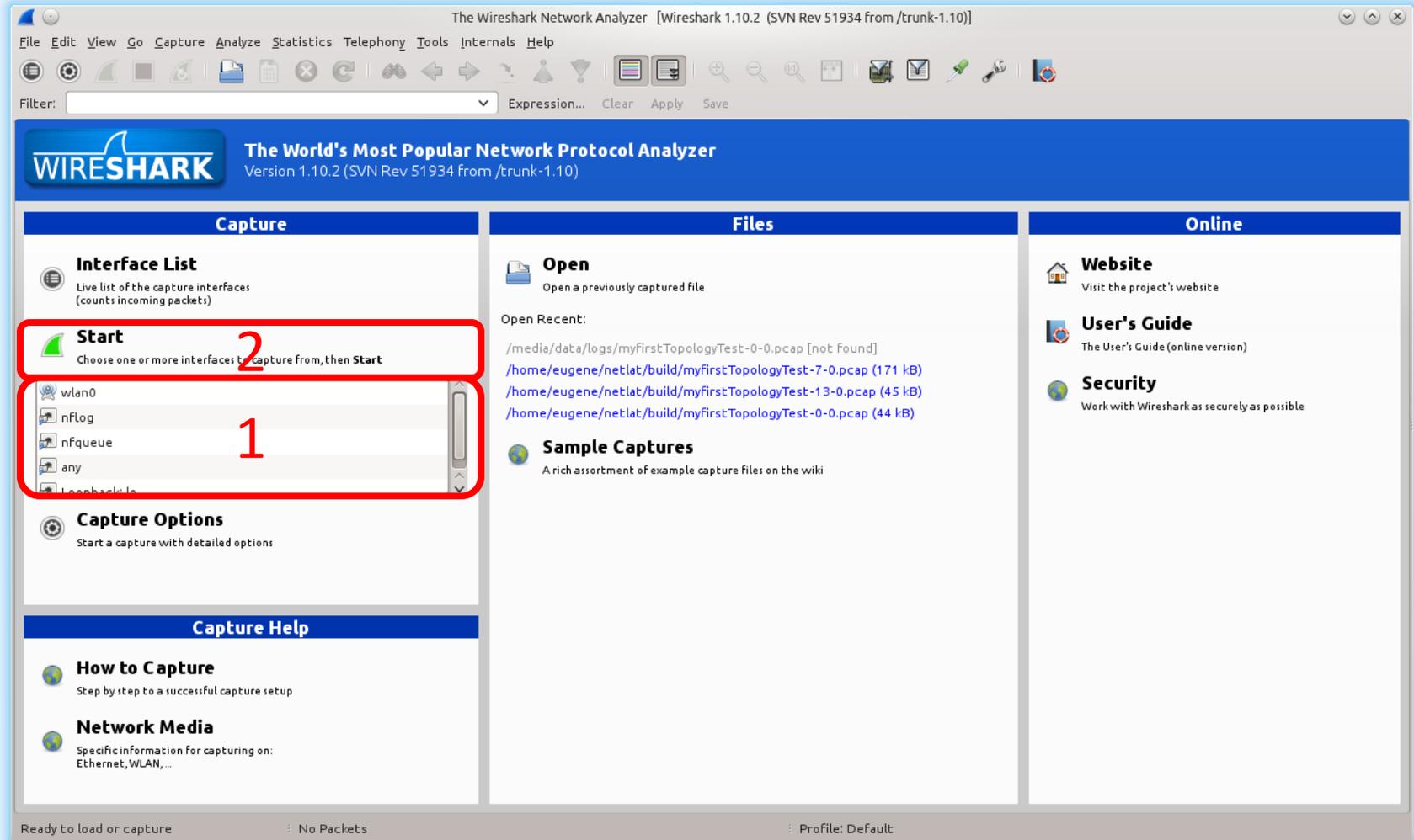


Wireshark

- Самый популярный анализатор пакетов
 - Кроссплатформенность (Win, Mac, Linux)
 - Богатые функциональные возможности
 - Графический интерфейс
 - Open Source (<http://www.wireshark.org>)
- Анализаторы трафика
 - Захватывают трафик
 - Декодируют сырые пакеты (разбор протоколов)
 - Анализируют последовательности пакетов

Перехват трафика на интерфейсе



Перехват трафика на интерфейсе

- *# usermod -a -G wireshark user*
- Или запускать wireshark под root

Формируем пакет

```
user@host:~$telnet ya.ru 80
```

```
Trying 213.180.193.3...
```

1

```
Connected to ya.ru.
```

```
Escape character is '^['.
```

```
Trololo
```

2

```
<html>
```

```
<head><title>400 Bad Request</title></head>
```

```
<body bgcolor="white">
```

```
<center><h1>400 Bad Request</h1></center>
```

3

```
<hr><center>nginx</center>
```

```
</body>
```

```
</html>
```

```
Connection closed by foreign host. 4
```

Просмотр захваченного трафика

The screenshot displays the Wireshark interface with the following details:

- Packet List (Table):**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	IntelCor_1e:ae:f1	Broadcast	ARP	42	Who has 10.30.40.254? Tell 10.30.40.50
2	0.002424000	10.30.40.57	224.0.0.251	MDNS	220	Standard query 0x0000 ANY 68:09:27:da:9d:6d@fe80::6a09:27ff:feda:9d6d._apj
3	0.004946000	fe80::a6:f33:8e5:89b5	ff02::fb	MDNS	240	Standard query 0x0000 ANY 68:09:27:da:9d:6d@fe80::6a09:27ff:feda:9d6d._apj
4	0.027222000	10.30.40.57	224.0.0.251	MDNS	287	Standard query response 0x0000 PTR_apple-mobdev2._tcp.local PTR, cache f
5	0.035913000	fe80::a6:f33:8e5:89b5	ff02::fb	MDNS	307	Standard query response 0x0000 PTR_apple-mobdev2._tcp.local PTR, cache f
6	0.322800000	10.30.40.50	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
7	0.326177000	10.30.40.57	224.0.0.251	MDNS	344	Standard query response 0x0000 TXT, cache flush PTR 68:09:27:da:9d:6d@fe80
8	0.330286000	fe80::a6:f33:8e5:89b5	ff02::fb	MDNS	364	Standard query response 0x0000 TXT, cache flush PTR 68:09:27:da:9d:6d@fe80
9	0.333926000	AsustekC_cb:9e:60	Spanning-tree-(for-bri	STP	52	Conf. Root = 32768/0/08:60:6e:cb:9e:60 Cost = 0 Port = 0x8002
10	0.631377000	fe80::c491:9c53:5fba:e	ff02::c	SSDP	118	M-SEARCH * HTTP/1.1
11	0.925540000	fe80::4c1d:3ebe:c5a8:f	ff02::1:2	DHCPv6	112	Solicit XID: 0x8cad83 CID: 00010001199fd39614dae98ed18f
12	1.551397000	fe80::a6:f33:8e5:89b5	ff02::fb	MDNS	520	Standard query response 0x0000 TXT, cache flush PTR 68:09:27:da:9d:6d@fe80
13	1.859483000	10.30.40.55	10.30.40.255	DB-LSP-DI	144	Dropbox LAN sync Discovery Protocol
14	2.170297000	AsustekC_8e:d1:8f	Broadcast	ARP	60	Who has 10.30.40.77? Tell 10.30.40.61
15	2.175236000	10.30.40.57	224.0.0.251	MDNS	537	Standard query response 0x0000 TXT, cache flush PTR_apple-mobdev2._tcp.l
16	2.180676000	fe80::a6:f33:8e5:89b5	ff02::fb	MDNS	557	Standard query response 0x0000 TXT, cache flush PTR_apple-mobdev2._tcp.l
17	3.084916000	10.30.40.83	10.30.40.255	NBNS	92	Name query NB PC<20>
18	3.086079000	Supermic_58:2e:5a	Broadcast	ARP	60	Gratuitous ARP for 172.17.1.10 (Request)
19	3.088121000	10.30.40.50	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
20	3.207137000	10.30.40.87	10.30.40.255	DB-LSP-DI	167	Dropbox LAN sync Discovery Protocol

Packet Details (Frame 4):

- Ethernet II, Src: Apple_da:9d:6d (68:09:27:da:9d:6d), Dst: IPv4mcast_00:00:fb (01:00:5e:00:00:fb)
- Destination: IPv4mcast_00:00:fb (01:00:5e:00:00:fb)
- Address: IPv4mcast_00:00:fb (01:00:5e:00:00:fb)
-0. = LG bit: Globally unique address (factory default)

Packet Bytes:

```
0000 01 00 5e 00 00 fb 68 09 27 da 9d 6d 08 00 45 00  ..K..N..M..E.  
0010 01 11 8c 61 00 00 ff 11 1b 28 0a 1e 28 39 e0 00  ...a....(..(9..  
0020 00 fb 14 e9 14 e9 00 fd d0 45 00 00 84 00 00 00  .....E.....  
0030 00 03 00 00 00 02 09 5f 73 65 72 76 69 63 65 73  ....._services  
0040 07 5f 64 6e 73 2d 73 64 04 5f 75 64 70 05 6c 6f  .._dns-sd _udp.Lo  
0050 63 61 6e 00 00 00 00 01 00 00 11 04 00 16 00 5f  c1
```

Просмотр захваченного трафика

The screenshot displays the Wireshark interface with a network traffic capture on the wlan0 interface. The main window shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. A 'Find Packet' dialog box is overlaid on the interface, with the search term 'Trololo' entered in the 'Filter' field. The dialog box also shows options for searching by Display filter, Hex value, or String, and checkboxes for Case sensitive and Packet bytes. The main window shows a list of captured packets, including ARP, MDNS, and TXT. The packet details pane shows the structure of the selected packet, including Ethernet II and IPv4mcast information.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	IntelCor_le:ae:f1	Broadcast	ARP	42	who has 10.30.40.254? Tell 10.30.40.50
2	0.002424000	10.30.40.57	224.0.0.251	MDNS	220	Standard query 0x0000 ANY 68:09:27:da:9d:6d@fe80::6a09:27ff:feda:9d6d._ap
3	0.004946000	fe80::a6:f33:8e5:89b5	ff02::fb	MDNS	240	Standard query 0x0000 ANY 68:09:27:da:9d:6d@fe80::6a09:27ff:feda:9d6d._ap
4	0.027222000	10.30.40.57	224.0.0.251	MDNS	220	Standard query 0x0000 PTR_apple-mobdev2._tcp.local PTR, cache f
5	0.035913000	fe80::a6:f33:8e5:89b5	ff02::fb	MDNS	240	Standard query 0x0000 PTR_apple-mobdev2._tcp.local PTR, cache f
6	0.322800000	10.30.40.50	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
7	0.326177000	10.30.40.57	224.0.0.251	MDNS	220	Standard query 0x0000 TXT, cache flush PTR 68:09:27:da:9d:6d@fe80::6a09:27ff:feda:9d6d._ap
8	0.330286000	fe80::a6:f33:8e5:89b5	ff02::fb	MDNS	240	Standard query 0x0000 TXT, cache flush PTR 68:09:27:da:9d:6d@fe80::6a09:27ff:feda:9d6d._ap
9	0.333926000	AsustekC_cb:9e:60	Spanning	LLDP	167	DPadbox LAN-cups-Discovery-Protocol
10	0.631377000	fe80::c491:9c53:5fba:c	ff02::c	MDNS	220	Standard query 0x0000 Cost = 0 Port = 0x8002
11	0.925540000	fe80::4c1d:3ebe:c5a8:f	ff02::1	MDNS	220	Standard query 0x0000 PTR_apple-mobdev2._tcp.local PTR, cache f
12	1.551397000	fe80::a6:f33:8e5:89b5	ff02::fb	MDNS	240	Standard query 0x0000 PTR_apple-mobdev2._tcp.local PTR, cache f
13	1.859483000	10.30.40.55	10.30.40.57	TCP	60	64800 → 64800 [RST] Seq=10010001199fd39614dae98ed18f Win=0 Len=0
14	2.170297000	AsustekC_8e:d1:8f	Broadca	LLDP	167	DPadbox LAN-cups-Discovery-Protocol
15	2.175236000	10.30.40.57	224.0.0.251	MDNS	220	Standard query 0x0000 TXT, cache flush PTR_apple-mobdev2._tcp.l
16	2.180676000	fe80::a6:f33:8e5:89b5	ff02::fb	MDNS	240	Standard query 0x0000 TXT, cache flush PTR_apple-mobdev2._tcp.l
17	3.084916000	10.30.40.83	10.30.40.57	TCP	60	64800 → 64800 [RST] Seq=10010001199fd39614dae98ed18f Win=0 Len=0
18	3.086079000	Supermic_58:2e:5a	Broadca	LLDP	167	DPadbox LAN-cups-Discovery-Protocol
19	3.088121000	10.30.40.50	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
20	3.201327000	10.30.40.87	10.30.40.255	UDP	167	DPadbox LAN-cups-Discovery-Protocol

Frame 4: 287 bytes on wire (2296 bits), 287 bytes captured (2296 bits) on interface 0
Ethernet II, Src: Apple_da:9d:6d (68:09:27:da:9d:6d), Dst: IPv4mcast_00:00:fb (01:00:5e:00:00:fb)
Destination: IPv4mcast_00:00:fb (01:00:5e:00:00:fb)
Address: IPv4mcast_00:00:fb (01:00:5e:00:00:fb)
.....0. = LG bit: Globally unique address (factory default)
0000 01 00 5e 00 00 fb 68 09 27 da 9d 6d 08 00 45 00 ..^...h.!.m..E.
0010 01 11 8c 61 00 00 ff 11 1b 28 0a 1e 28 39 e0 00 ...a....(..(9..
0020 00 fb 14 e9 14 e9 00 fd d0 45 00 00 84 00 00 00E.....
0030 00 03 00 00 00 02 09 5f 73 65 72 76 69 63 65 73_services
0040 07 5f 64 6e 73 2d 73 64 04 5f 75 64 70 05 6c 6f ..._dns-sd _udp.lo
0050 63 61 6e 00 00 00 01 00 00 11 64 00 16 00 5f ...al...
File: "/tmp/wireshark_pcapng_wlan0_20... Packets: 4355 · Displayed: 4355 (100.0%) · Marked: 1 (0.0%) · D... · Profile: Default

Перехват трафика на интерфейсе (2)

The screenshot displays the Wireshark 1.10.2 interface with the following details:

- Toolbar:** A red box highlights the icons for starting capture (green play button), stopping capture (red stop button), and refreshing the capture (circular arrow).
- Filter:** The filter field is empty, and a red '1' is placed above it.
- Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
37	1.787050000	10.30.100.10	10.30.40.107	DNS	126	Standard query response 0x3f35 PTR 135-23-155-86.cpe.pppoe.ca
38	1.787976000	10.30.100.1	10.30.40.107	DNS	126	Standard query response 0x3f35 PTR 135-23-155-86.cpe.pppoe.ca
39	1.787998000	10.30.40.107	10.30.100.1	ICMP	154	Destination unreachable (Port unreachable)
40	1.847176000	Supermic_58:2e:5a	Broadcast	ARP	60	Gratuitous ARP for 172.17.1.10 (Request)
41	1.856412000	135.23.155.86	10.30.40.107	BitTorrent	760	Extended
42	1.856477000	10.30.40.107	135.23.155.86	TCP	66	44533 > 17841 [ACK] Seq=74 Ack=796 Win=30592 Len=0 TSval=3738953 TSecr=504:
43	1.891769000	50.53.181.149	10.30.40.107	BitTorrent	163	Handshake
44	1.891837000	10.30.40.107	50.53.181.149	TCP	66	38192 > 18913 [ACK] Seq=69 Ack=98 Win=29200 Len=0 TSval=3738962 TSecr=5881:
45	1.939188000	135.23.155.86	10.30.40.107	TCP	66	17841 > 44533 [FIN, ACK] Seq=796 Ack=74 Win=16384 Len=0 TSval=5042412 TSecr:
46	1.939259000	10.30.40.107	135.23.155.86	BitTorrent	187	Extended
47	1.939345000	10.30.40.107	135.23.155.86	TCP	66	44533 > 17841 [FIN, ACK] Seq=195 Ack=797 Win=30592 Len=0 TSval=3738974 TSecr:
48	2.032546000	10.30.40.107	95.182.74.2	TCP	74	[TCP Retransmission] 44633 > 6881 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK:
49	2.036053000	10.30.40.107	50.53.181.149	BitTorrent	71	Continuation data
50	2.036086000	10.30.40.107	10.30.100.10	DNS	86	Standard query 0x3753 PTR 149.181.53.50.in-addr.arpa
51	2.055749000	10.30.100.10	10.30.40.107	DNS	144	Standard query response 0x3753 PTR static-50-53-181-149.bvtn.or.frontierrn
52	2.094191000	135.23.155.86	10.30.40.107	TCP	60	17841 > 44533 [RST, ACK] Seq=797 Ack=195 Win=0 Len=0
53	2.141675000	fe80::c491:9c53:5fba::c	10.30.40.255	SSDP	208	M-SEARCH * HTTP/1.1
54	2.143219000	10.30.40.61	10.30.40.255	NBNS	92	Name query NB WPAD<00>
55	2.210507000	50.53.181.149	10.30.40.107	BitTorrent	789	Extended
56	2.210526000	10.30.40.107	50.53.181.149	TCP	66	38192 > 18913 [ACK] Seq=74 Ack=98 Win=29266 Len=0 TSval=3739042 TSecr=5881:
- Packet Details:**
 - Frame 2: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface 0
 - Ethernet II, Src: Apple_dd:48:7b (7c:d1:c3:dd:48:7b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Internet Protocol Version 4, Src: 10.30.40.109 (10.30.40.109), Dst: 255.255.255.255 (255.255.255.255)
 - User Datagram Protocol, Src Port: db-lsp-disc (17500), Dst Port: db-lsp-disc (17500)
 - Dropbox LAN svcn Discovery Protocol
- Packet Bytes:**

```
0000 ff ff ff ff ff ff 7c d1 c3 dd 48 7b 08 00 45 00 .....|. ..H{.E.
0010 00 c2 32 75 00 00 40 11 15 2c 0a 1e 28 6d ff ff ..2u..@. ...(.m.
0020 ff ff 44 5c 44 5c 00 ae a4 77 7b 22 68 6f 73 74 ..D\D\... .w{"host
0030 5f 69 6e 74 22 3a 20 33 30 33 39 32 37 36 32 31 _int": 3 03927621
0040 2c 20 22 76 65 72 73 69 6f 6e 22 3a 20 5b 31 2c , "versi on": [1,
0050 20 20 5d 2c 20 22 64 60 72 70 6e 61 70 6e 61 6d ol -di caloun
```

File: "/tmp/wireshark_pcapng_wlan0_20... Packets: 66 · Displayed: 66 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Перехват трафика на интерфейсе (3)

The screenshot displays the Wireshark interface with the following details:

- Filter:** http
- Packet List:** A table showing network packets. Packet 609 is highlighted in blue, with a red box around it. The entry is: No. 609, Time 4.325857000, Source 10.30.40.107, Destination 91.203.99.36, Protocol HTTP, Length 693, Info GET /?host=www.bbc.co.uk&hdn=%2B9qjcvifZKRSLv54Hrs4Fg== HTTP/1.1.
- Packet Details:** The details pane for packet 609 is expanded, showing:
 - Frame 609: 693 bytes on wire (5544 bits), 693 bytes captured (5544 bits) on interface 0
 - Ethernet II, Src: IntelCor_46:e4:48 (c4:85:08:46:e4:48), Dst: Cisco_94:54:c8 (18:33:9d:94:54:c8)
 - Internet Protocol Version 4, Src: 10.30.40.107 (10.30.40.107), Dst: 91.203.99.36 (91.203.99.36)
 - Transmission Control Protocol, Src Port: 46234 (46234), Dst Port: http (80), Seq: 1, Ack: 1, Len: 627
 - Hypertext Transfer Protocol

Перехват трафика на интерфейсе (4)

The screenshot displays the Wireshark interface with the following details:

- Window title: *wlan0 [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
- Filter: http
- Packet list table:

No.	Time	Source	Destination	Protocol	Length	Info
6	1.548587000	fe80::c491:9c53:5fba:ε ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
7	1.850914000	10.30.40.97	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
14	2.772699000	10.30.40.89	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
609	4.325857000	10.30.40.107	91.203.99.36	HTTP	693	GET /?host=www... HTTP/1.1
618	4.333363000	10.30.40.107	212.58.244.67	HTTP	882	GET /news/worl... HTTP/1.1
628	4.372615000	91.203.99.36	10.30.40.107	HTTP/XML	551	HTTP/1.1 200 O... HTTP/1.1
703	4.514989000	10.30.40.107	212.58.244.69	HTTP	1181	GET /news/worl... HTTP/1.1
752	4.619053000	fe80::c491:9c53:5fba:ε ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
755	4.626087000	10.30.40.97	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
882	4.780230000	10.30.40.107	23.3.90.194	HTTP	485	GET /emp/bump?... HTTP/1.1
895	4.805405000	23.3.90.194	10.30.40.107	HTTP	721	HTTP/1.1 301 M... HTTP/1.1
926	4.827472000	10.30.40.107	23.3.90.194	HTTP	570	GET /emp/relea... HTTP/1.1
937	4.850188000	23.3.90.194	10.30.40.107	HTTP	310	HTTP/1.1 304 N... HTTP/1.1
943	4.862053000	10.30.40.107	23.3.90.201	HTTP	501	GET /media/ima... HTTP/1.1
991	4.887766000	23.3.90.201	10.30.40.107	HTTP	1294	HTTP/1.1 200 O... HTTP/1.1
1017	4.918509000	212.58.244.69	10.30.40.107	HTTP	1434	[TCP Retransmission] GET /... HTTP/1.1
1020	4.922677000	fe80::e523:a49c:279a:ε ff02::c		SSDP	153	M-SEARCH * HTTP/1.1
1021	4.927007000	10.30.40.95	239.255.255.250	SSDP	139	M-SEARCH * HTTP/1.1
1022	4.931257000	fe80::e523:a49c:279a:ε ff02::c		SSDP	185	M-SEARCH * HTTP/1.1
1023	4.932453000	10.30.40.95	239.255.255.250	SSDP	171	M-SEARCH * HTTP/1.1

Packet 609 details:

- Frame 609: 693 bytes on wire (5544 bits), 693 bytes captured (5544 bits) on interface 0
- Ethernet II, Src: IntelCor_46:e4:48 (c4:85:08:46:e4:48), Dst: Cisco_94:54:c8 (18:33:9d:94:54:c8)
- Internet Protocol Version 4, Src: 10.30.40.107 (10.30.40.107), Dst: 91.203.99.36 (91.203.99.36)
- Transmission Control Protocol, Src Port: 46234 (46234), Dst Port: http (80), Seq: 1, Ack: 1, Len: 693
- Hypertext Transfer Protocol

Hex dump for packet 609:

```
0000 18 33 9d 94 54 c8 c4 85 08 46 e4 48 08 00 45 00  .3..T... .F.H..E.
0010 02 a7 3a b6 40 00 40 06 0c 23 0a 1e 28 6b 5b cb  ...@.@. .#..(k[.
0020 63 24 b4 9a 00 50 af 71 e9 3f 68 eb 17 7b 80 18  c$. .P.q ?h. {..
0030 00 e5 92 76 00 00 01 01 08 0a 00 39 d3 95 63 2e  ...v.... ..9..c.
0040 63 f0 47 45 54 20 2f 3f 68 6f 73 74 3d 77 77 77  c.GET /? host=www
0050 7a 62 62 62 7a 62 6f 7a 75 6b 76 68 64 6a 7d 75  hba.aa. ukthdn?%
```

Перехват трафика на интерфейсе (5)

The screenshot displays the Wireshark interface with the following details:

- Filter:** http
- Packet List:** Shows a packet at time 4.918509000, source 10.30.40.1, and destination 212.58.244.102.
- Packet Details:** Shows the structure of the captured packet:
 - Frame 609: 693 bytes on wire (Ethernet II, Src: IntelCor_46...)
 - Internet Protocol Version 4, Src: 10.30.40.1, Destination: 212.58.244.102
 - Transmission Control Protocol, Src Port: 54432, Dst Port: 80
 - Hypertext Transfer Protocol:**
 - GET /?host=www.bbc.co.uk&hdn=%2B9qjcvifZKRLv54Hrs4Fg== HTTP/1.1
 - User-Agent: Opera/9.80 (X11; Linux x86_64) Presto/2.12.388 Version/12.16
 - Host: sitecheck2.opera.com
 - Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/webp, image/jpeg, image/gif, image/x-xbitmap; q=0.1
 - Accept-Language: en-US,en;q=0.9
 - Accept-Encoding: gzip, deflate
 - Cookie: __gads=ID=23c28a9c415eb845:T=1392791330:S=ALNI_MbL4Ev9JBkEdZ1vEvOnpo_1QxJkg; __utma=122269525.1937381613.1392791323.1392791323.1392804735.2; __utmz=122269525.1392791323.1.1.utmcsrc=(direct)|utmccn=(direct)|utmcmd=(none)
 - Connection: Keep-Alive
 - HTTP/1.1 200 OK
 - Server: Apache
 - Cache-Control: max-age=7200
 - Vary: Accept-Encoding
 - Content-Encoding: gzip
 - Content-Type: text/xml
 - Content-Length: 157
 - Date: Tue, 04 Mar 2014 10:31:50 GMT
 - X-Varnish: 3129658075 3128033964
 - Age: 348
 - Via: 1.1 varnish

- Packet Bytes:** Shows the raw data of the packet, including the request line and headers.

The text "HTTP GET" is overlaid in red on the packet details pane.

Примеры фильтров

Страница не найдена:

```
http.response.code == 404
```

Начало TCP сессии:

```
tcp.flags.syn == 1
```

Обращение к DNS серверу:

```
udp.port == 53
```

Выбор всех пакетов из конкретной сети:

```
ip.dst==10.30.40.0/24
```

Произвольные предикаты:

```
eth.addr[3-4] == 00:08 && udp.srcport==23
```

TCP

- Wireshark по умолчанию показывает относительные номера последовательности
- *Edit->Preferences->Protocols->TCP->Relative Sequence Numbers* отключить

Задание (ТСР)

- Запустить захват пакетов
- Отправить произвольную строку на `yandex.ru:80` при помощи `telnet`, дождаться ответа от `yandex.ru`
- Остановить захват пакетов
- При помощи фильтра отобразить только эту ТСР-сессию
- Отфильтровать только пакеты от `yandex.ru`
- Определить `sequence number` ТСР-сегмента, содержащего `Bad Request`

Задание (ARP)

- Определить при помощи Wireshark MAC-адрес шлюза по умолчанию

Задание (ARP)

- Опустить wlan
- Запустить захват пакетов на wlan
- Поднять wlan, подождать несколько секунд
- Остановить захват пакетов
- Отфильтровать ARP
- Найти пакет ARP (ARP-ответ), в котором указан MAC-адрес шлюза по умолчанию

Задание (DHCP)

- Определить IP-адрес, предлагаемый вашему хосту DHCP-сервером
- Подсказка: фильтровать по bootp

Построение конфигурации сети по заданному набору *.pcap файлов

- Wireshark позволяет сохранять и открывать дампы сетевого трафика из файлов *.pcap (Packet CAPture)

Модельная задача:

- Пусть задан набор *.pcap файлов, полученных путём захвата трафика на каждом сетевом интерфейсе хостов и маршрутизаторов сети. Необходимо восстановить топологию сети и пути передачи потоков через сеть.

Просматриваем файлы

The image shows a Wireshark window titled "network1-0-0.pcap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, Help), a toolbar with various icons, and a filter field. The main display area shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The first packet (No. 1) is an ARP request from 00:00:00_00:00:0a to Broadcast, asking for the MAC address of 10.0.1.2. The second packet (No. 2) is an ARP response from 00:00:00_00:00:09 to 00:00:00_00:00:0a, stating that 10.0.1.1 is at 00:00:00:00:00:09. The third packet (No. 3) is a TCP SYN packet from 10.0.1.2 to 10.0.0.3, port 49153 to 234. The fourth packet (No. 4) is another ARP request from 00:00:00_00:00:09 to Broadcast, asking for the MAC address of 10.0.1.2. The fifth packet (No. 5) is an ARP response from 00:00:00_00:00:0a to 00:00:00_00:00:09, stating that 10.0.1.2 is at 00:00:00:00:00:0a. The sixth packet (No. 6) is a UDP packet from 10.0.2.2 to 10.0.1.2, source port 49153, destination port iasd. The seventh packet (No. 7) is a TCP SYN, ACK packet from 10.0.0.3 to 10.0.1.2, port 234 to 49153. The eighth packet (No. 8) is a TCP ACK packet from 10.0.1.2 to 10.0.0.3, port 49153 to 234. The ninth packet (No. 9) is a TCP ACK packet from 10.0.1.2 to 10.0.0.3, port 49153 to 234. The tenth packet (No. 10) is a TCP ACK packet from 10.0.0.3 to 10.0.1.2, port 234 to 49153. The eleventh packet (No. 11) is a TCP ACK packet from 10.0.1.2 to 10.0.0.3, port 49153 to 234. The twelfth packet (No. 12) is a TCP ACK packet from 10.0.1.2 to 10.0.0.3, port 49153 to 234. The thirteenth packet (No. 13) is a TCP ACK packet from 10.0.0.3 to 10.0.1.2, port 234 to 49153. The fourteenth packet (No. 14) is a TCP ACK packet from 10.0.1.2 to 10.0.0.3, port 49153 to 234.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:00:00_00:00:0a	Broadcast	ARP	64	Who has 10.0.1.2? Tell 10.0.1.2 [ETHERNET FRAME]
2	0.200011	00:00:00_00:00:09	00:00:00_00:00:0a	ARP	64	10.0.1.1 is at 00:00:00:00:00:09 [ETHERNET FRAME]
3	0.200011	10.0.1.2	10.0.0.3	TCP	64	[TCP Port numbers reused] 49153 > 234 [SYN] Seq=...
4	1.306988	00:00:00_00:00:09	Broadcast	ARP	64	Who has 10.0.1.2? Tell 10.0.1.1 [ETHERNET FRAME]
5	1.306988	00:00:00_00:00:0a	00:00:00_00:00:09	ARP	64	10.0.1.2 is at 00:00:00:00:00:0a [ETHERNET FRAME]
6	1.507081	10.0.2.2	10.0.1.2	UDP	1070	Source port: 49153 Destination port: iasd [ETHE...
7	1.808088	10.0.0.3	10.0.1.2	TCP	64	234 > 49153 [SYN, ACK] Seq=0 Ack=4294966761 Win=...
8	1.808088	10.0.1.2	10.0.0.3	TCP	64	49153 > 234 [ACK] Seq=4294966761 Ack=1 Win=65535...
9	1.808094	10.0.1.2	10.0.0.3	TCP	594	49153 > 234 [ACK] Seq=4294966761 Ack=1 Win=65535...
10	2.508422	10.0.0.3	10.0.1.2	TCP	64	234 > 49153 [ACK] Seq=1 Ack=1 Win=65535 Len=0 [E...
11	2.508422	10.0.1.2	10.0.0.3	TCP	594	49153 > 234 [ACK] Seq=1 Ack=1 Win=65535 Len=536...
12	2.508471	10.0.1.2	10.0.0.3	TCP	594	49153 > 234 [ACK] Seq=537 Ack=1 Win=65535 Len=53...
13	3.209026	10.0.0.3	10.0.1.2	TCP	64	234 > 49153 [ACK] Seq=1 Ack=1073 Win=65535 Len=0...
14	3.209026	10.0.1.2	10.0.0.3	TCP	594	49153 > 234 [ACK] Seq=1073 Ack=1 Win=65535 Len=5...

> Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
> Ethernet II, Src: 00:00:00_00:00:0a (00:00:00:00:00:0a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

```
0000 ff ff ff ff ff ff 00 00 00 00 00 0a 08 06 00 01 .....  
0010 08 00 06 04 00 01 00 00 00 00 00 0a 0a 00 01 02 .....  
0020 ff ff ff ff ff ff 0a 00 01 01 00 00 00 00 00 00 .....  
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

File: "/home/eugene/examples/log/net... Packets: 66 · Displayed: ... Profile: Default

Информация о сети

Алгоритм анализа пакетов:

1. Записать в таблицу все MAC адреса из дампа
2. Соотнести MAC и IP адреса по ARP протоколу
3. Записать информацию о всех соединениях L4

Interface #	Domain #	Eth Address	IPv4 Address
1	1	00:00:00:00:00:0a	10.0.1.2
2	1	00:00:00:00:00:09	10.0.1.1
3			10.0.2.2
4			10.0.0.3

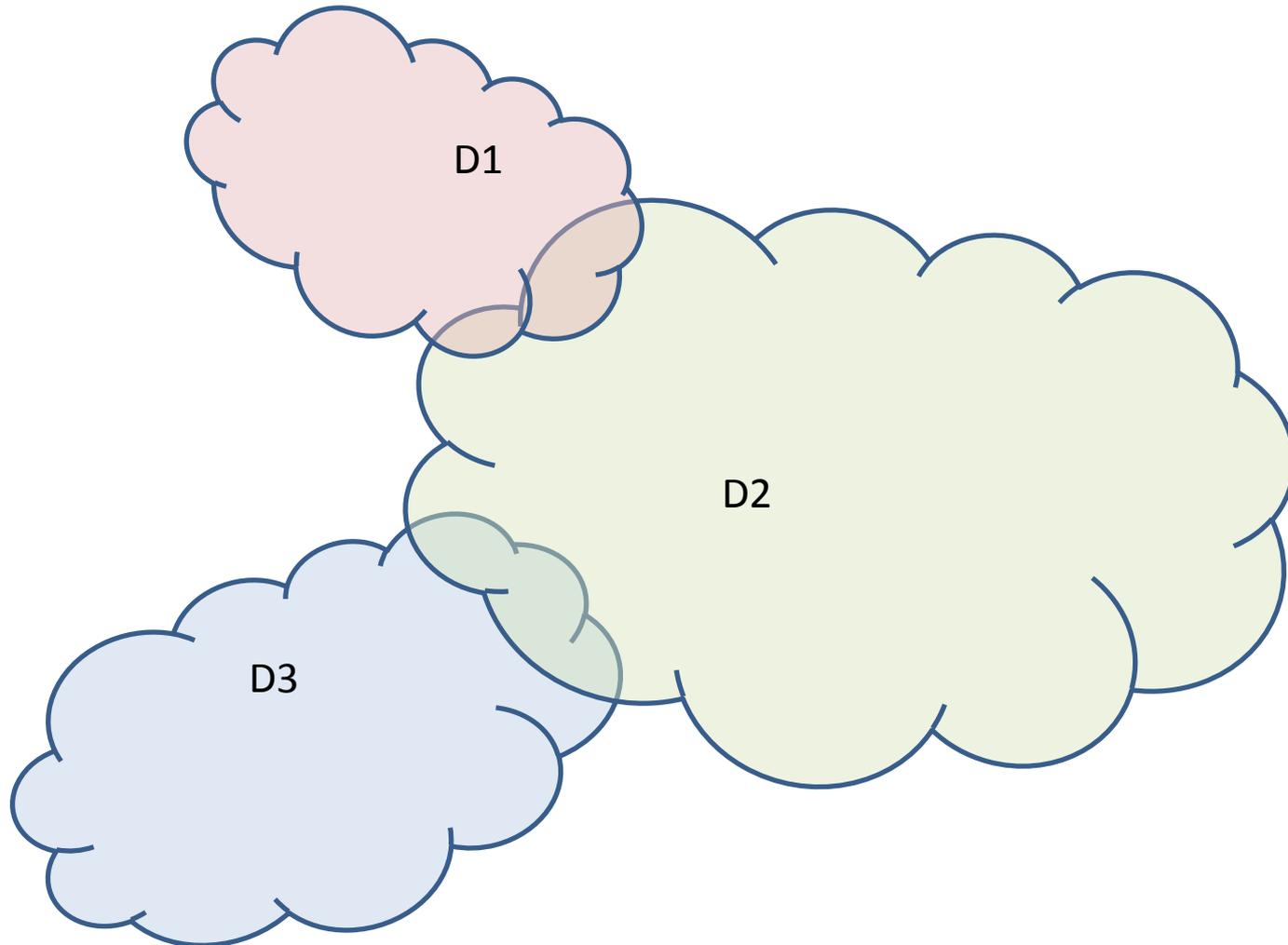
Flow #	Src Itf #	Dst Itf #	Protocol	Edges
1	1:49153	4:234	TCP	1-2
2	3:49153	1:432	UDP	1-2

После анализа всех таблиц...

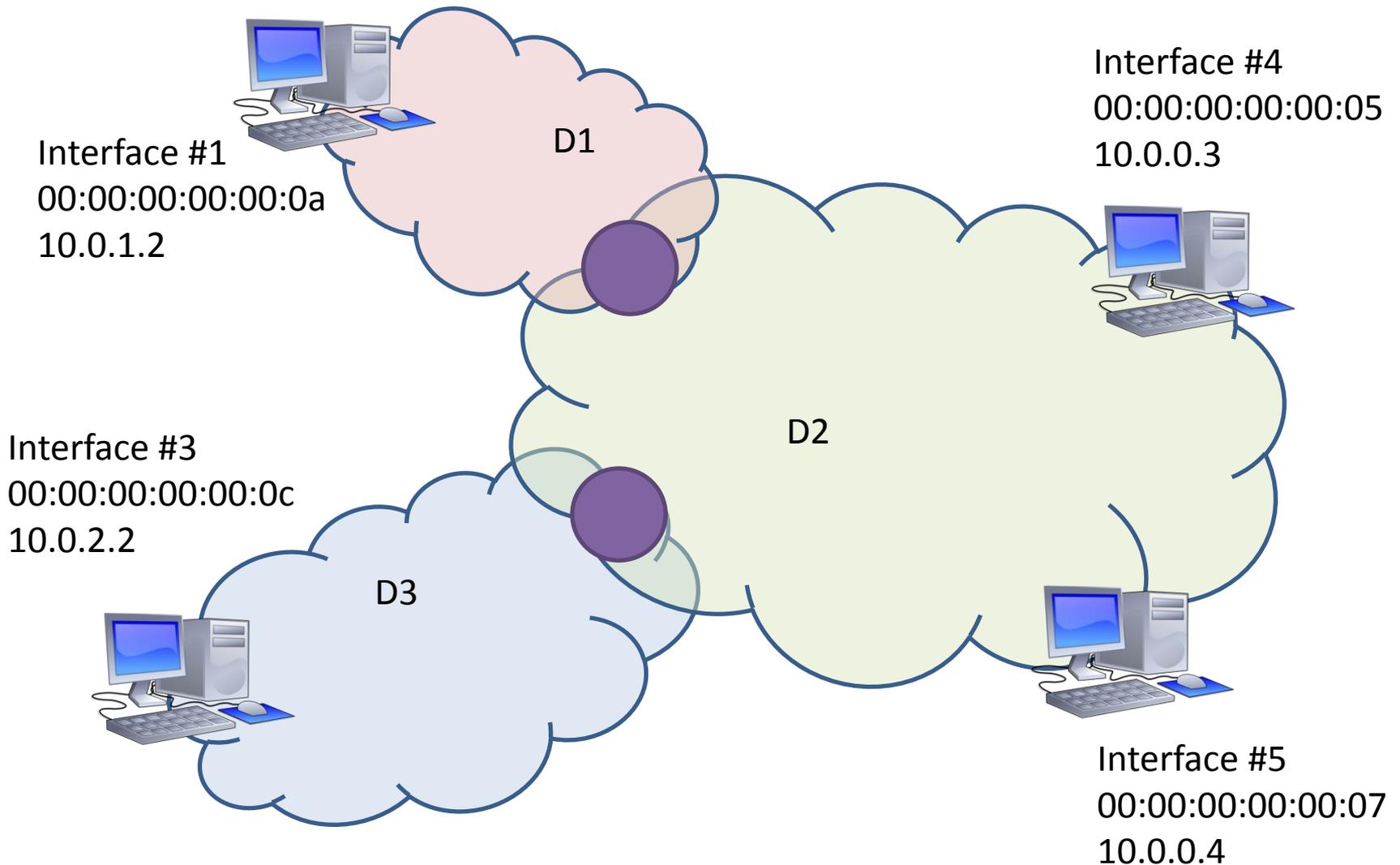
Interface #	Domain #	Eth Address	IPv4 Address
1	1	00:00:00:00:00:0a	10.0.1.2
2	1	00:00:00:00:00:09	10.0.1.1
3	3	00:00:00:00:00:0c	10.0.2.2
4	2	00:00:00:00:00:05	10.0.0.3
5	2	00:00:00:00:00:07	10.0.0.4
6	2	00:00:00:00:00:03	10.0.0.2
7	2	00:00:00:00:00:01	10.0.0.1
8	3	00:00:00:00:00:0b	10.0.2.1

Flow #	Src Itf #	Dst Itf #	Protocol	Edges
1	1:49153	4:234	TCP	1-2, 7-4
2	3:49153	1:432	UDP	3-8, 6-7, 1-2
3	4:49153	5:789	TCP	4-5

Зависимости между доменами



Расположение интерфейсов



Прокладка маршрутов

