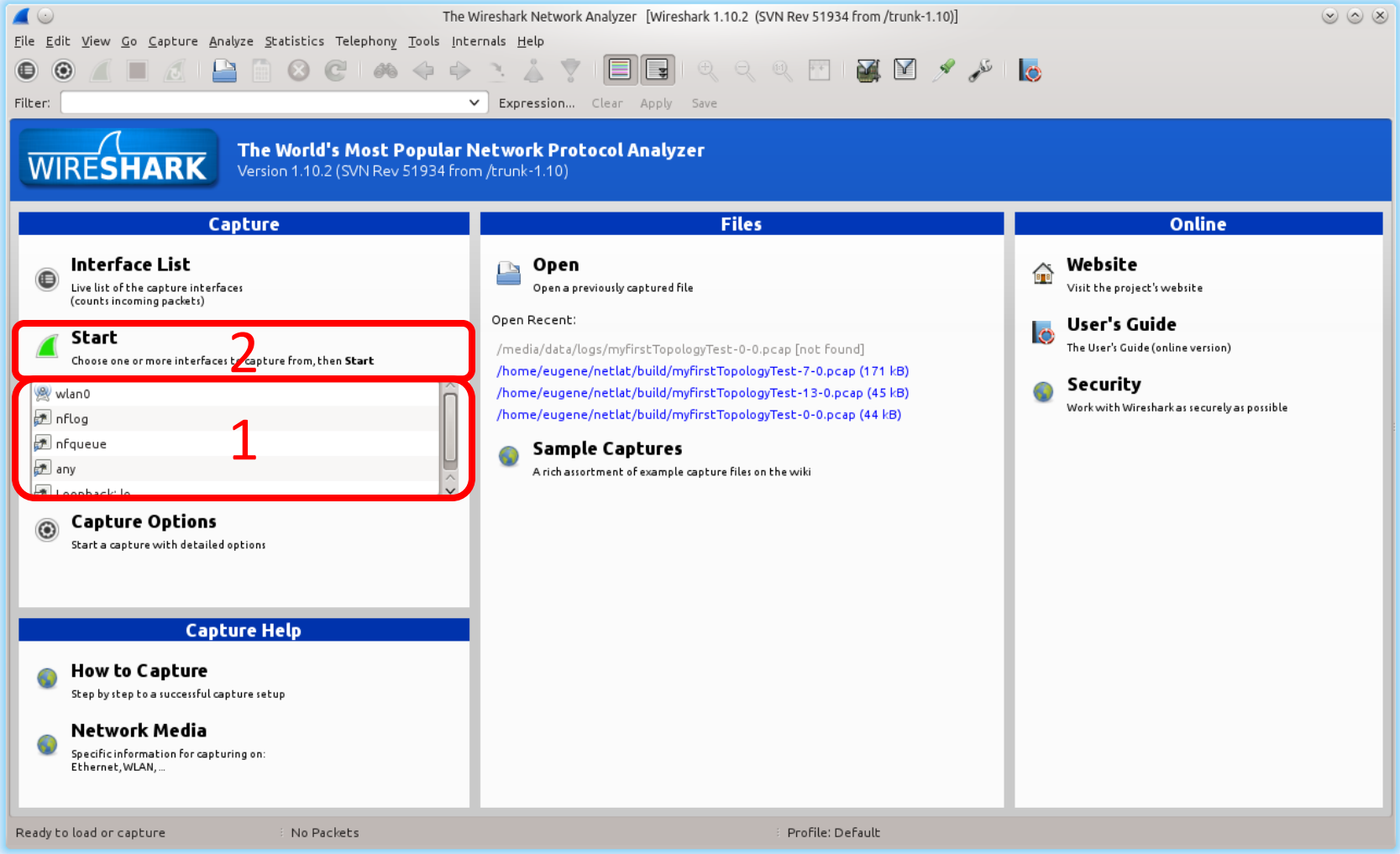
Wireshark

- Самый популярный анализатор пакетов
  - Кроссплатформенность (Win, Mac, Linux)
  - Богатые функциональные возможности
  - Графический интрефейс
  - 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...
Connected to ya.ru.
Escape character is '^]'.
```

1

```
Trololo
```

2

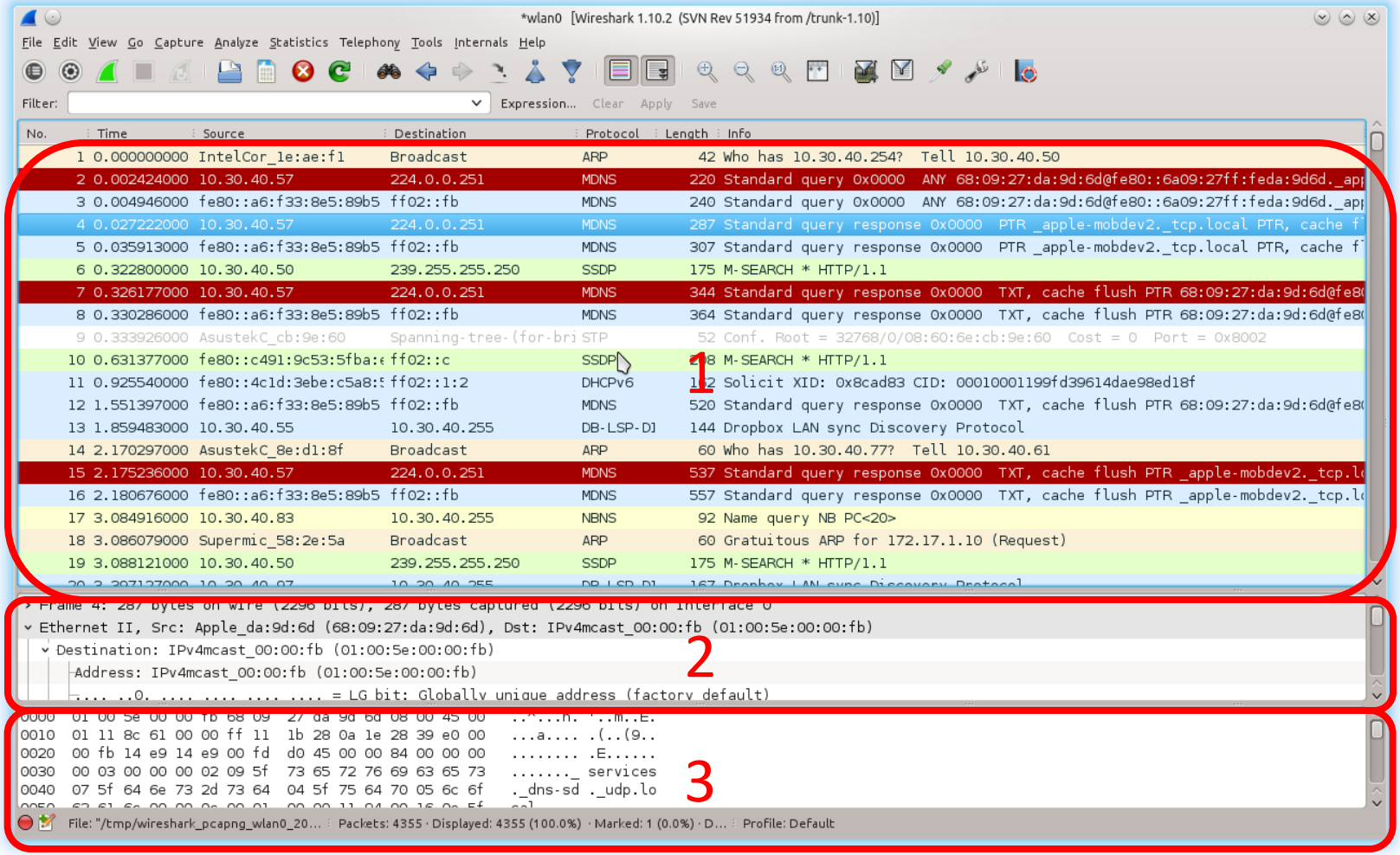
```
<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

3

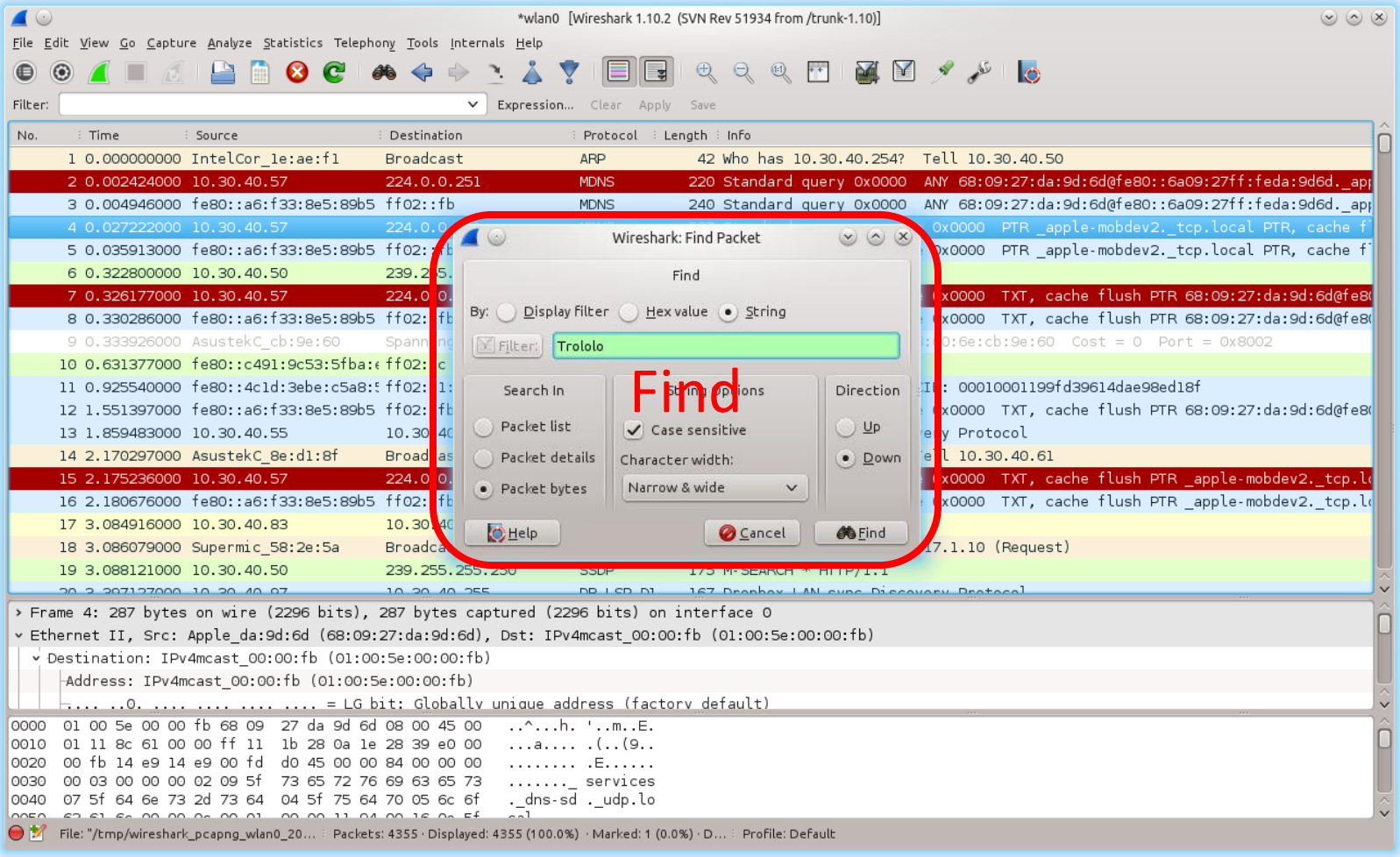
```
Connection closed by foreign host.
```

4

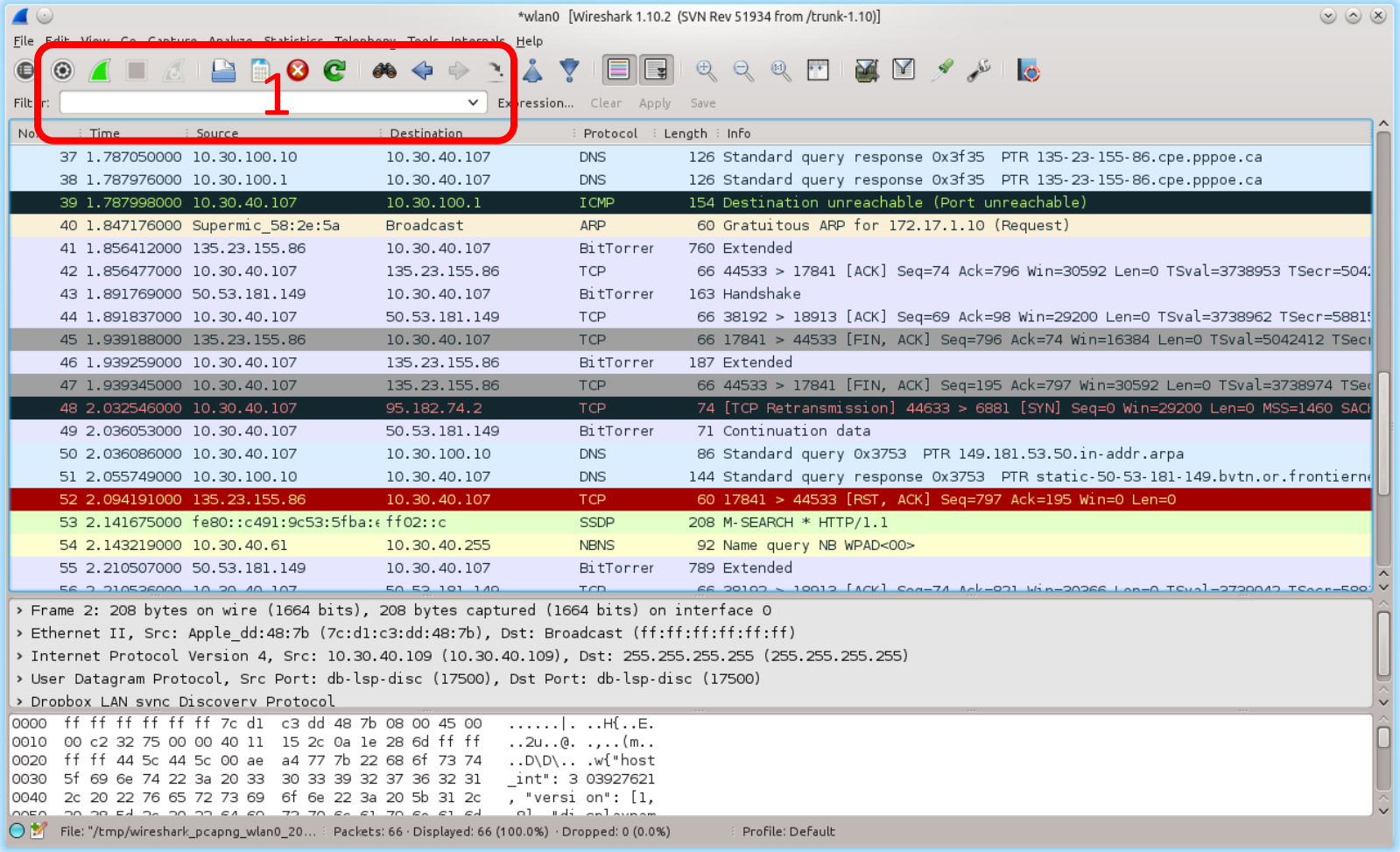
Просмотр захваченного трафика



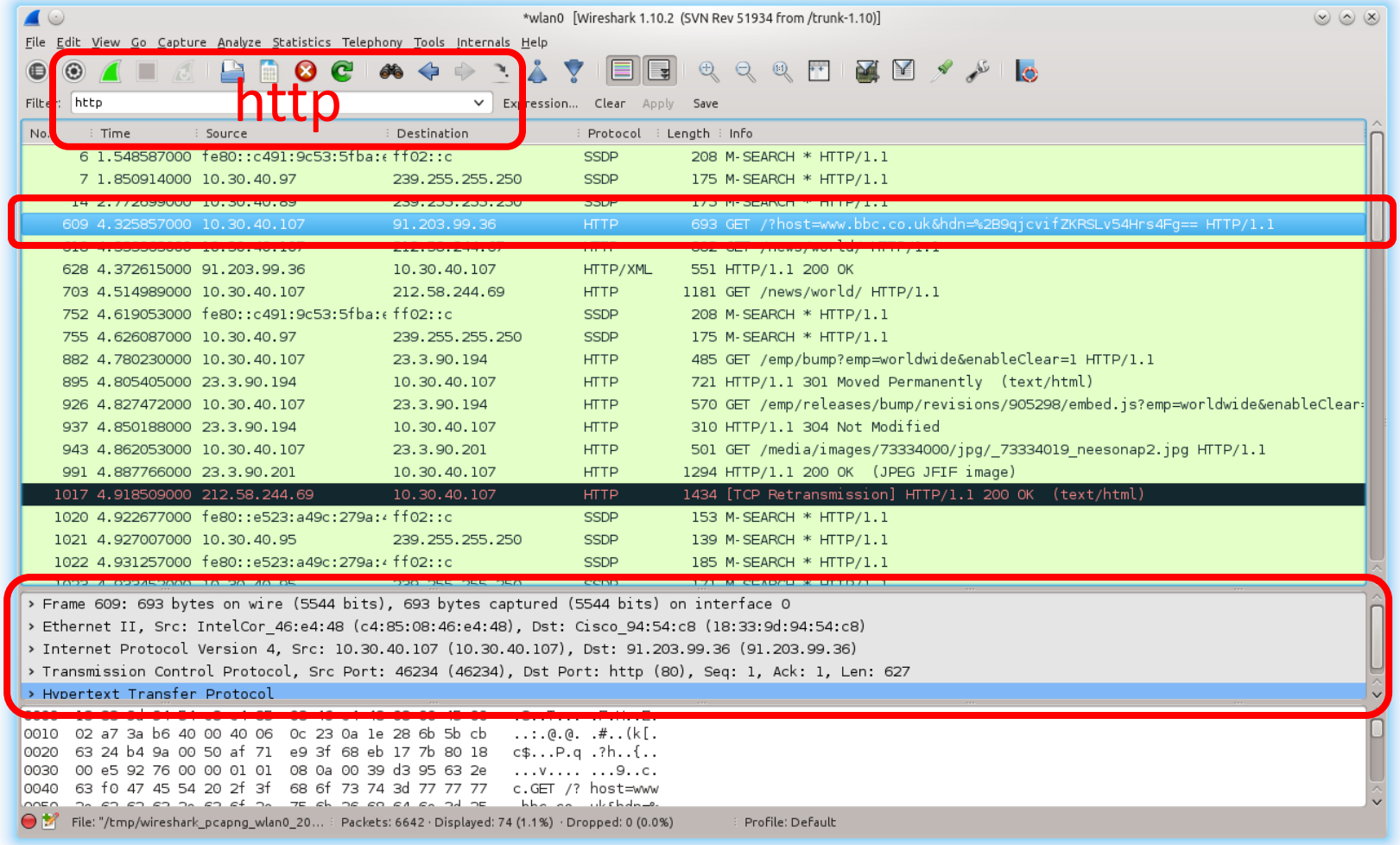
Просмотр захваченного трафика



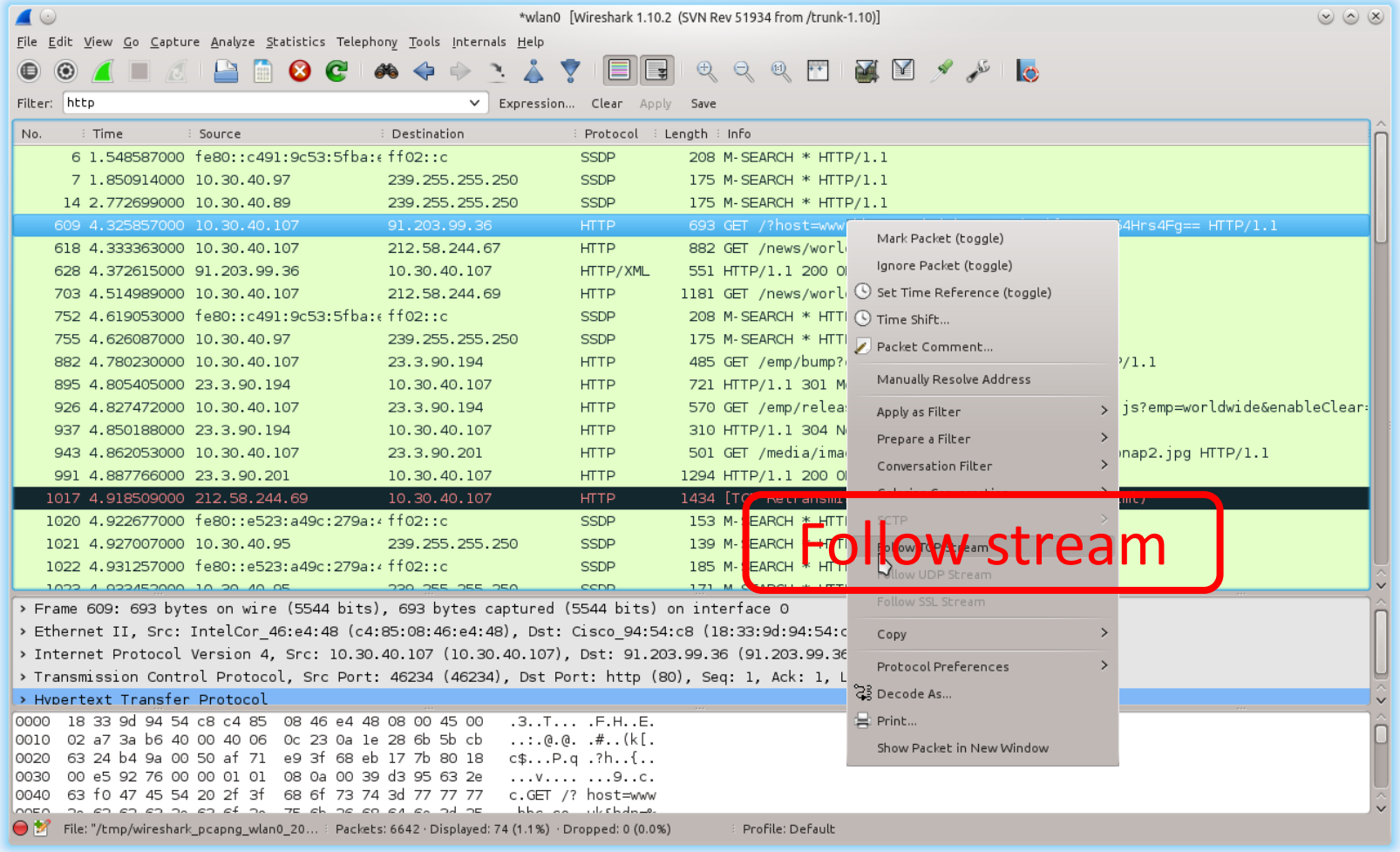
Перехват трафика на интерфейсе (2)



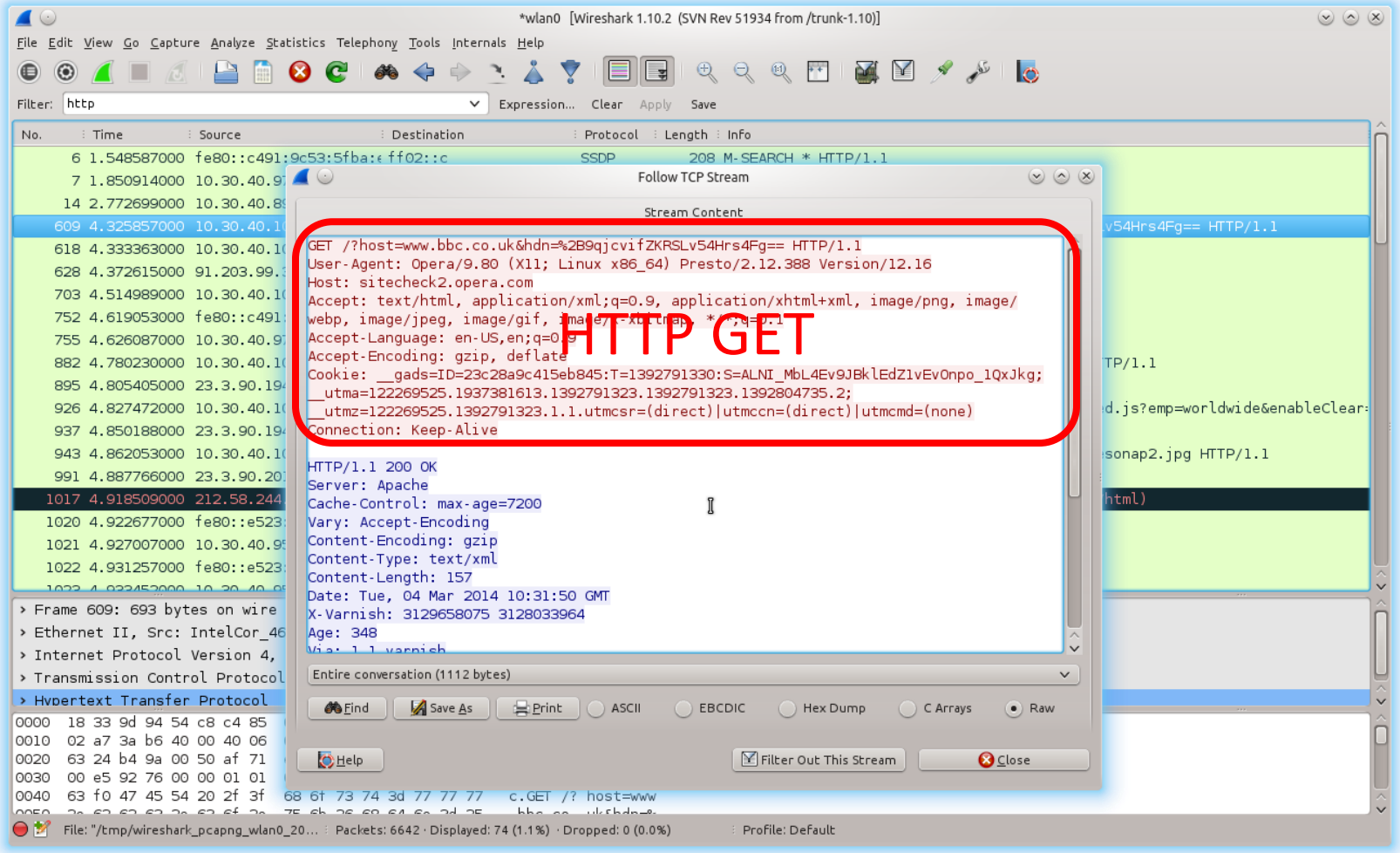
Перехват трафика на интерфейсе (3)



Перехват трафика на интерфейсе (4)



Перехват трафика на интерфейсе (5)



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 (TCP)

- 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 TCP-сессию
- Отфильтровать только пакеты от yandex.ru
- Определить sequence number TCP-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

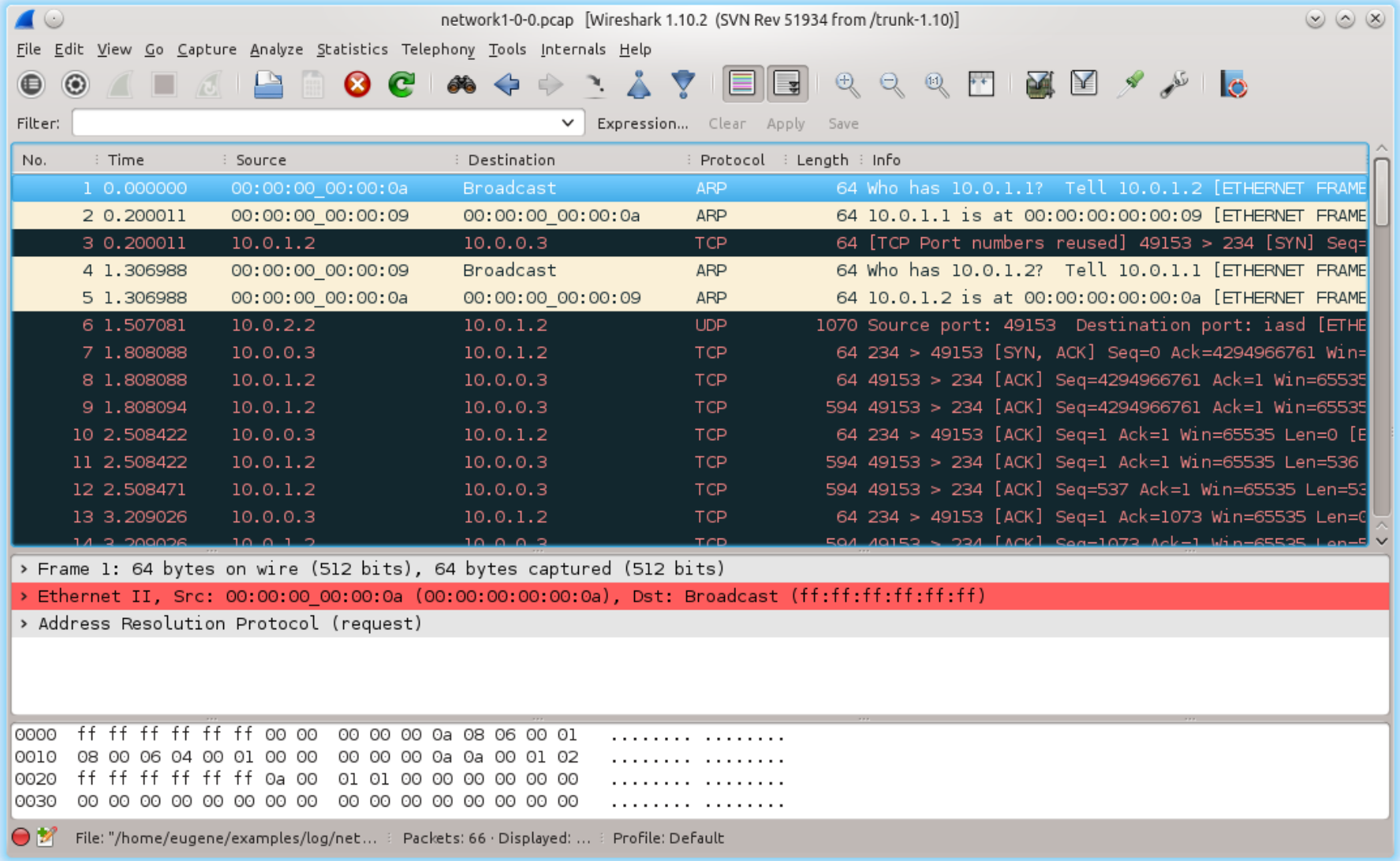
Построение конфигурации сети по заданному набору *.pcap файлов

- 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



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

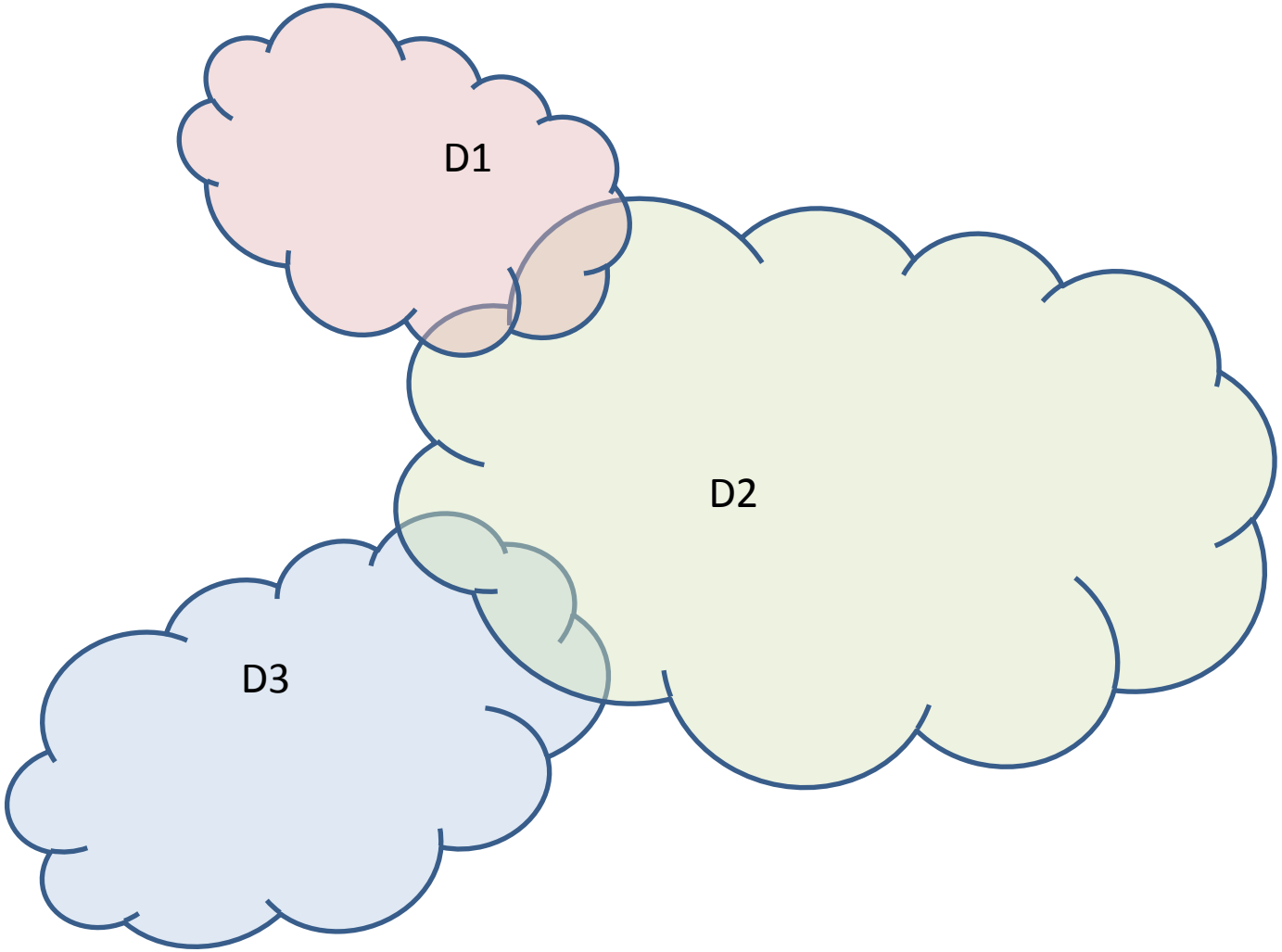
Flow #	Src Itf #	Dst Itf #	Protocol	Edges
1	1:49153	4:234	TCP	1-2
2	3:49153	1:432	UDP	1-2

После анализа всех таблиц…

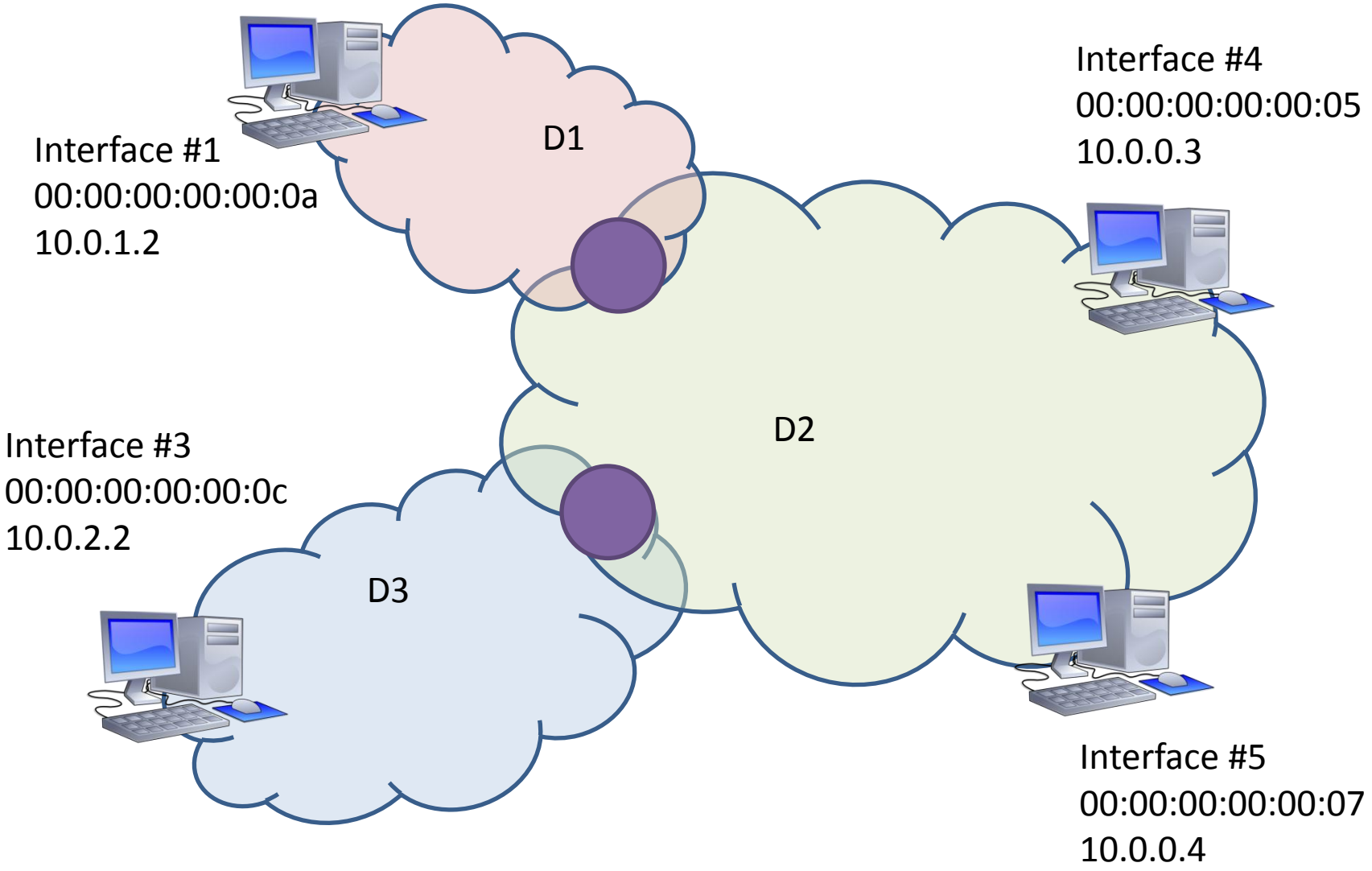
Interface #	Domain #	Eth Address	IPv4 Address
1	1	00:00:00:00:00:0a	10.0.1.2
2	1	00:00:00:00:00:09	10.0.1.1
3	3	00:00:00:00:00:0c	10.0.2.2
4	2	00:00:00:00:00:05	10.0.0.3
5	2	00:00:00:00:00:07	10.0.0.4
6	2	00:00:00:00:00:03	10.0.0.2
7	2	00:00:00:00:00:01	10.0.0.1
8	3	00:00:00:00:00:0b	10.0.2.1

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