**Сетевое программирование**

Лабораторная работа №1

**Задание:** в соответствии с вариантом (таблица 2) требуется проанализировать трафик, захваченный программой Wireshark, а именно:

1) рассмотреть структуру пакета, указав назначение каждого заголовка;

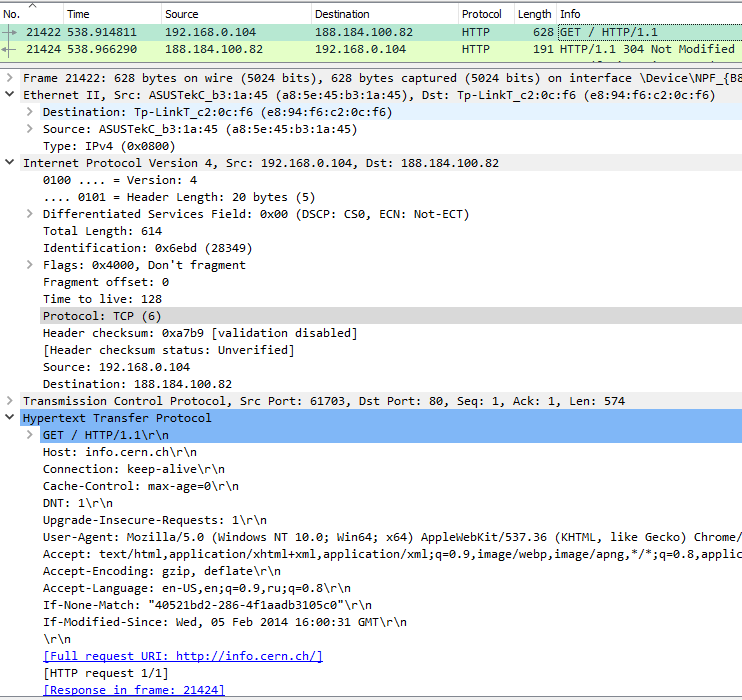
2) пояснить механизм инкапсуляции протоколов. В отчете привести скриншоты, иллюстрирующие ответы на поставленные в задании вопросы (также пакет можно распечатать прямо из программы Wireshark), сохраненные версии захваченного трафика (так называемый дамп трафика) в формате pcap (это стандартный формат сохранения трафика в Wireshark) для протоколов варианта.

**Вариант 7**

Протокол 1 – http усл get

Для того, чтобы рассмотреть данный протокол, нужно было найти сайт с незащищённым http-соединением и обновить страницу после её первой загрузки. После первого запроса страницы сервер возвращает ответ, в котором можно найти 2 заголовка – Last-Modified и ETag. Первый хранит дату и время последнего изменения страницы, а второй –идентификатор этой версии. Они будут использоваться в следующем GET запросе при обновлении страницы для получения свежей версии страницы, если она за это время изменилась. Если нет – возвращается ответ со статус кодом 304, говорящий, что изменений нет.

В моём случае сервер сравнил версию страницы с той, которая есть у меня, увидел, что они идентичны и отправил ответ с кодом 304.



Структура:

Ethernet пакет

|  |  |  |
| --- | --- | --- |
| **Поле** | **Значение** | **Описание** |
| Адрес назначения | Tp-LinkT\_c2:0c:f6 (e8:94:f6:c2:0c:f6) |  |
| Адрес источника | ASUSTekC\_b3:1a:45 (a8:5e:45:b3:1a:45) |  |
| Тип | IPv4 (0x0800) |  |
| Данные | IP | Инкапсулированный IP - пакет |

IP пакет

|  |  |  |
| --- | --- | --- |
| **Поле** | **Значение** | **Описание** |
| Версия IP протокола | 0100 .... = Version: 4 | Версия – 4 |
| Длина заголовка | .... 0101 = Header Length: 20 bytes (5) | Длина заголовка – 20 байт |
| Полная длина | 614 |  |
| TTL | 128 | Время жизни пакета |
| Протокол | TCP (6) |  |
| Адрес источника | 192.168.0.104 |  |
| Адрес назначения | 188.184.100.82 |  |
| Данные | TCP | Инкапсулированный TCP - пакет |

TCP пакет

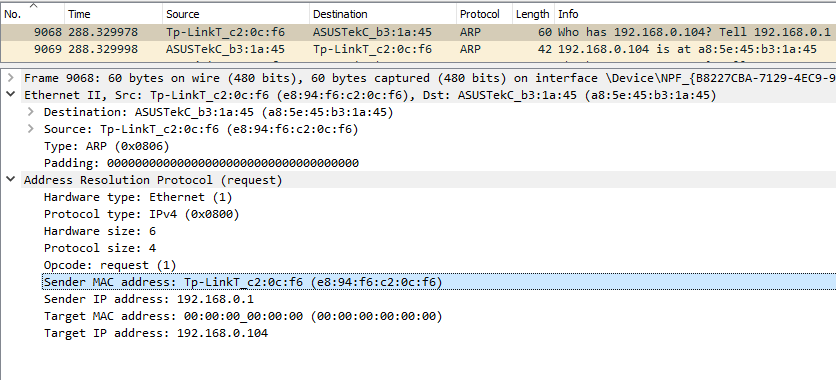
|  |  |  |
| --- | --- | --- |
| **Поле** | **Значение** | **Описание** |
| Порт источника | 61703 |  |
| Порт назначения | 80 | Стандартный порт приёма TCP пакетов |
| Длина заголовка | 0101 .... = Header Length: 20 bytes (5) |  |
| Checksum | 0xde8a |  |
| Данные | HTTP | Инкапсулированный HTTP - пакет |

Http пакет

|  |  |  |
| --- | --- | --- |
| **Поле** | **Значение** | **Описание** |
| Метод запроса | GET |  |
| Версия | HTTP/1.1 |  |
| URI | / |  |
| Хост | info.cern.ch\r\n |  |
| If-None-Match | "40521bd2-286-4f1aadb3105c0"\r\n | Значение этого поля это ETag версии страницы, которая была запрошена раньше |
| If-Modified-Since | Wed, 05 Feb 2014 16:00:31 GMT\r\n | Время последней модификации загруженной страницы |

Протокол 2 – Arp

Здесь показана попытка моего роутера узнать MAC-адрес моего сетевого устройства.



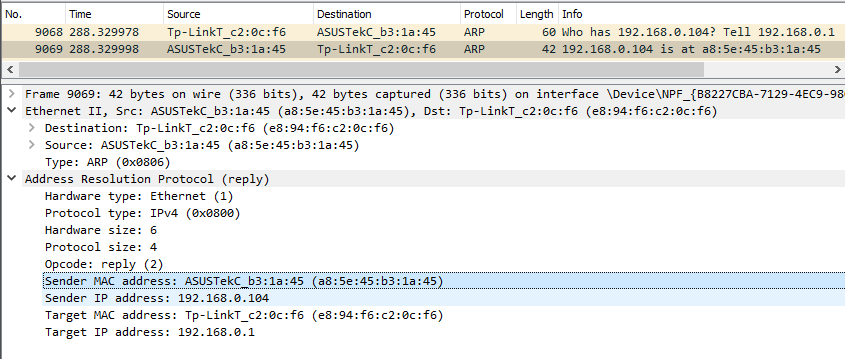
Структура

Ethernet пакет

|  |  |  |
| --- | --- | --- |
| **Поле** | **Значение** | **Описание** |
| Адрес назначения | ASUSTekC\_b3:1a:45 (a8:5e:45:b3:1a:45) |  |
| Адрес источника | Tp-LinkT\_c2:0c:f6 (e8:94:f6:c2:0c:f6) |  |
| Тип | ARP (0x0806) |  |
| Данные | ARP | Инкапсулированный ARP - пакет |

ARP пакет

|  |  |  |
| --- | --- | --- |
| **Поле** | **Значение** | **Описание** |
| Тип оборудования | Ethernet (1) |  |
| Тип протокола | IPv4 (0x0800) |  |
| MAC адрес отправителя | Tp-LinkT\_c2:0c:f6 (e8:94:f6:c2:0c:f6) |  |
| IP адрес отправителя | 192.168.0.1 |  |
| MAC адрес таргета | 00:00:00\_00:00:00 (00:00:00:00:00:00) | Хочет узнать |
| IP адрес таргета | 192.168.0.104 |  |



На скриншоте выше показано, как в ответ приходит ARP пакет с MAC-адресом, который мой роутер хотел узнать.