Министерство науки и высшего образования Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

“НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО”

Факультет ПИиКТ



ОТЧЁТ

По лабораторной работе №4

«Анализ трафика компьютерных сетей с помощью утилиты Wireshark»

По предмету: Компьютерные сети

Студент:

Степанов М.А.

Группа P33301

Преподаватель:

Алиев Т. И.

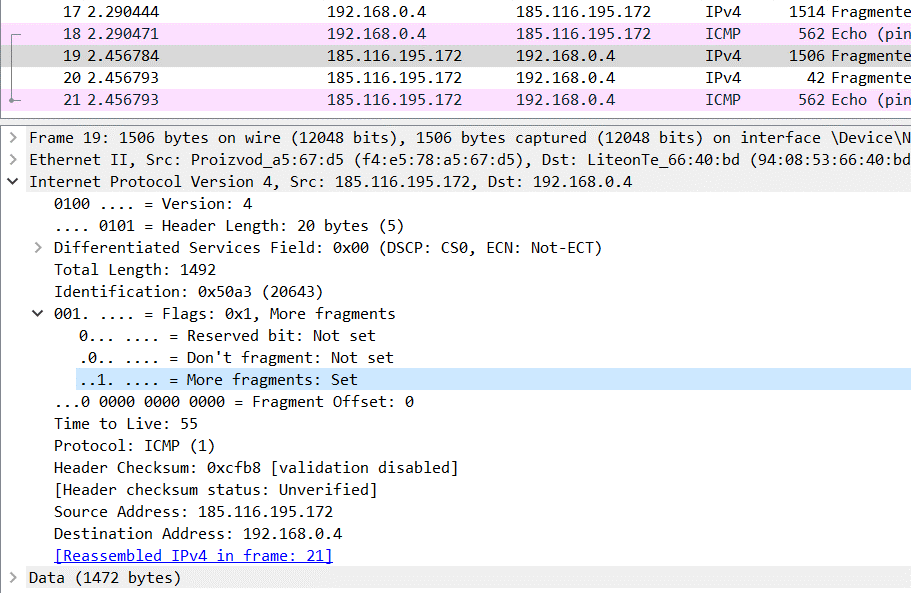
Санкт – Петербург

2023

**Анализ трафика утилиты *ping.***

Вариант: smart-sts.kz

Пакеты делятся на фрагменты размером по 1480 байт максимум, а на признак последнего фрагмента указывает флаг *More fragments* в заголовке IPv4.

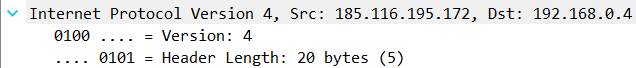


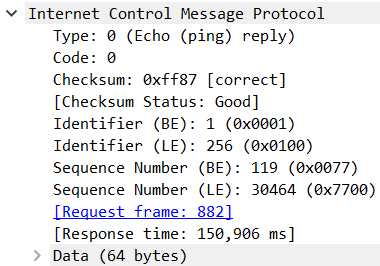
Количество фрагментов при передаче ping-пакета равно (N div 1480 + 1), где N – количество передаваемых байт.

TTL пакетов можно задать при помощи флага *-i* утилиты *ping.* В поле данных ping-пакета содержится последовательность ASCII символов (повторяется английский алфавит).

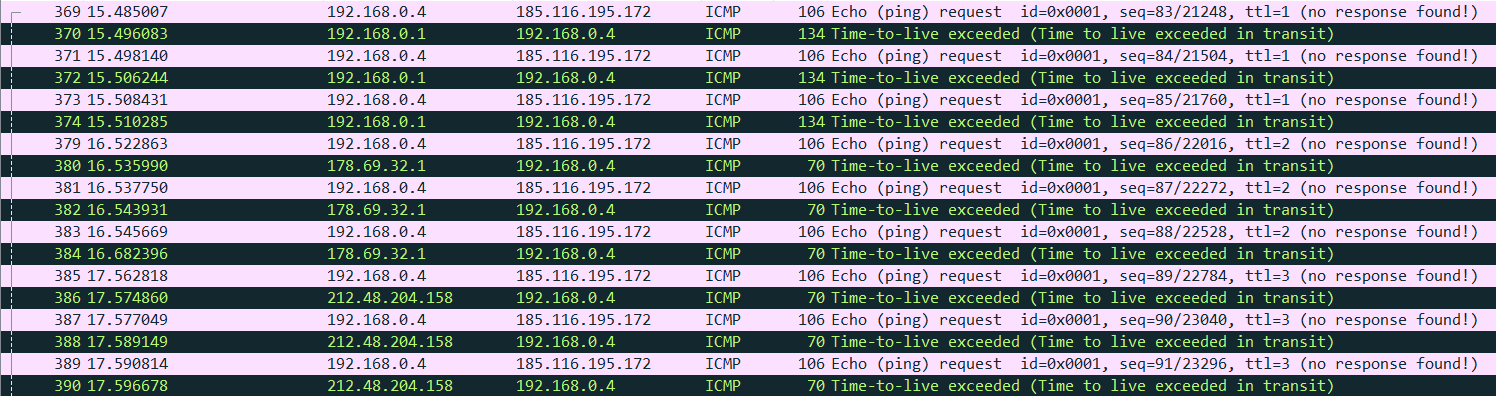
**Анализ трафика утилиты *tracert.***

В заголовке IP содержится 20 байт, в поле данных – 64 байта.

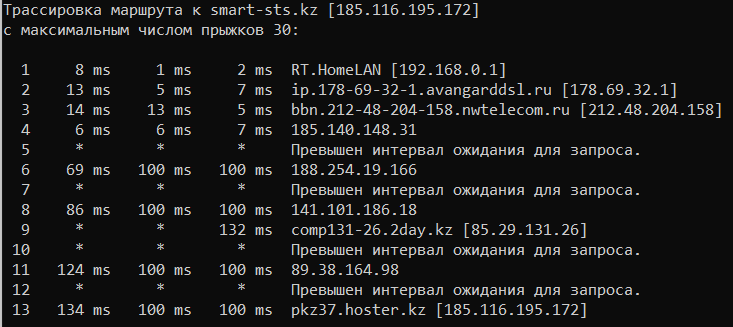




Утилита последовательно отправляет по 3 пакета, каждый раз увеличивая TTL на 1, по истечение которого, пакет возвращается и дает информацию о последнем узле на его пути. Таким образом выстраивается маршрут до пункта назначения.



Генерируемые ICMP-пакеты отличаются от генерируемых утилитой ping размером и содержимым данных, а также установленным TTL. Полученные пакеты были двух типов: «ошибочные» (черные) и «корректные» (розовые), и оба этих типа необходимы – черные информируют о промежуточных узлах маршрута, а розовые – о финальном. Если убрать ключ *-d*, будет генерироваться дополнительный трафик в виде доменных имен узлов:

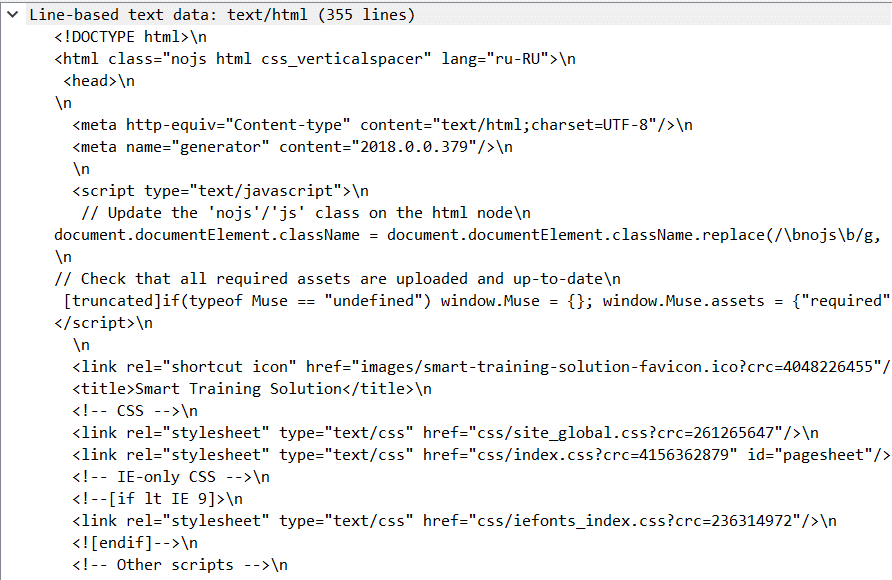


**Анализ HTTP-трафика**

Пара пакетов «запрос-ответ»:



Как видно, код ответа – 200, значит полученные данные корректны. Содержимое поля данных ответа:



Пара пакетов после перезагрузки страницы:



Код ответа – 304, значит данные на странице не изменились и поле данных отсутствует вовсе.

**Анализ ARP-трафика**

При первом (относительно очистки arp таблиц) открытии сайты был отправлен ARP-запрос на ближайший маршрутизатор.



Можно заметить, что мы отправляем данный запрос не к конкретному серверу, на котором находится наш сайт, а к ближайшему маршрутизатору (широковещательный запрос, broadcast), поскольку нам не требуется отследить местоположение и существование в целом данного компьютера, достаточно лишь информации о том, что ближайший маршрутизатор знает, куда дальше передавать запрос.

Некоторые запросы содержат mac адреса маршрутизатора и компьютера, с которого происходят запросы. Эти адреса используются для маршрутизации внутри локальной беспроводной сети для составления ARP-таблиц.

Позже данные MAC-адреса используются и в HTTP запросах на сетевом уровне для передачи данных между компьютером и маршрутизатором.

IP адрес же в запросах необходим для нахождения конфликтов в сети и заполнения ARP-таблиц.

**Анализ DNS-трафика**

При первом (относительно очистки кэша) открытии сайта был послан DNS-запрос (id 732340):



Как видно, адрес получателя отличается от фактического адреса сайта. Это происходит потому, что компьютер не знает этого адреса, он знает лишь доменное имя, поэтому он отправляет DNS запрос на ближайший DNS-сервер, который (через пару строк) вернул ему нужный IP-адрес.

Существует несколько типов DNS запросов:

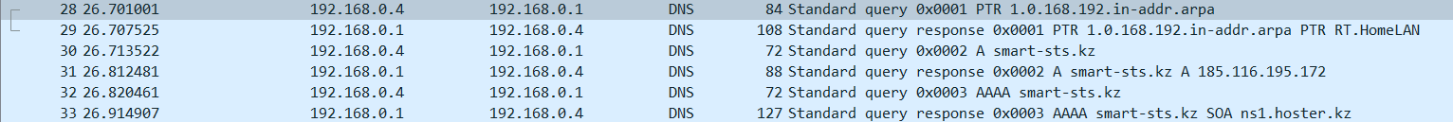
* Прямой
* Обратный
* Рекурсивный
* Итеративный

Также при обращении к сайту через браузер могут возникать дополнительные DNS запросы, в случае если некоторые медиа файлы находятся на другом хосте.

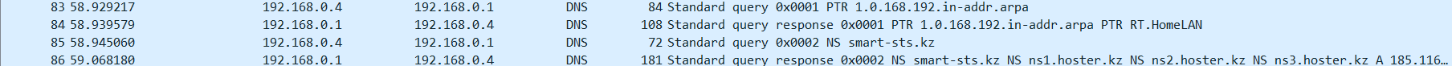


**Анализ трафика утилиты *nslookup.***

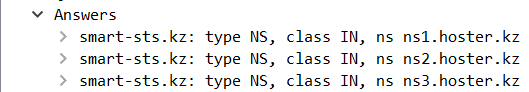
Обычный DNS-запрос:



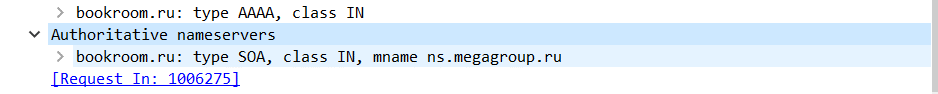
NS DNS-запрос:



Отличия трафиков в том, что второй запрос содержит информацию не о IP-адресе нашего сайта, а об доменных серверах, которые обслуживают этот сайт (в поле Answers):

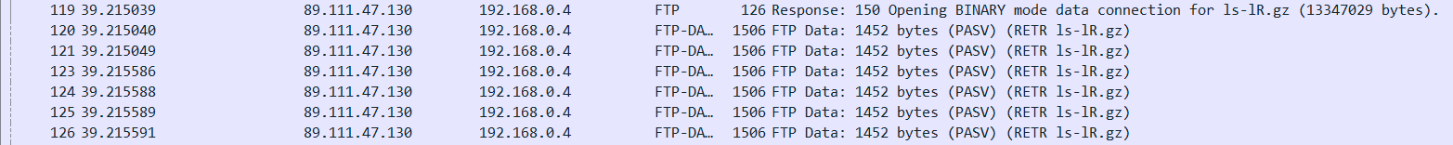


Имя сервера, возвратившего авторитативный отклик:



**Анализ FTP-трафика.**

Данные фрагментируются на фрагменты по 1460 байт по «протоколу» FTP-DATA, который по факту просто является FTP, настроенным на порт 20:

****

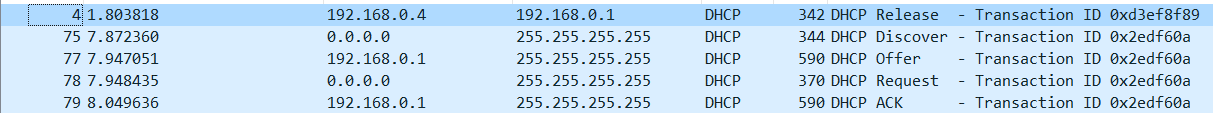
В общем же случае существует 2 порта для подключения по FTP:

*«The well known TCP port for FTP control is 21 and for FTP data is 20»*

порт 21 для управления (FTP) и порт 20 для передачи данных (FTP-DATA). В нашем случае для получения ответа используется динамический порт

**Анализ DHCP-трафика.**

Последовательность пакетов:



Пакеты Discover и Request отличаются тем, что первый еще не знает о местоположении DHCP-сервера, и пытается его найти. Второй же лишь является ответом на Offer, соглашается на предложенный IP-адрес.

Адрес источника и назначения меняется в процессе передачи сообщений, так как некоторые запросы отсылаются широковещательно, а некоторые к конкретному DHCP серверу

Адрес DHCP-сервера:

Изображение выглядит как текст, Шрифт, снимок экрана, линия

Автоматически созданное описание