

Лабораторная работа №1

«Знакомство с базовыми возможностями Wireshark»

Целью данной работы является приобретение навыков работы в интерфейсе командной строки Windows/Linux, а также захвата сетевого трафика в сегменте локальной сети и анализа собранной информации с помощью программного анализатора протоколов Wireshark.

Теоретические основы

1. Анализатор протоколов Wireshark

Для наблюдения процессов, происходящих в локальных сетях, существуют специальные программы, которые называются сетевыми анализаторами (мониторами, «сниферами»). Такая программа дает возможность принимать и анализировать информацию, распространяется через сеть, при этом не только ту, которая направлена к «своему» компьютеру, но и любую информацию, которой обмениваются компьютеры в одном сегменте общего доступа. Этот процесс принято называть захват (отслеживание) кадров. Первое условие, необходимое для работы такой программы – это доступ к устройству, выполняющему функции 1-2 уровней модели OSI, то есть сетевому адаптеру. Поэтому после запуска программы сначала выбирается сетевое устройство, с которого будет производиться захват данных (Ethernet, беспроводная сеть и др.)

Как и большинство программ такого класса, Wireshark содержит следующие основные компоненты: фильтр захвата, буфер кадров, декодер протоколов, фильтр отображения захваченных кадров и модуль статистики с элементами экспертной системы. К несомненным достоинствам Wireshark относятся:

- наличие реализаций для Unix и Windows;
- наличие исходного кода программы;
- возможность захвата трафика в сетевых сегментах различных базовых технологий;
- возможность анализа огромного числа протоколов (более 700);
- возможность экспорта/импорта файлов данных в формат распространенных анализаторов (несколько десятков форматов);
- мощная и удобная система поиска и фильтрации информации в буфере пакетов;
- возможность сохранения на диск выделенного фрагмента пакета;
- наличие полезных утилит командной строки для осуществления захвата трафика и обработки сохраненных файлов.

ПО Wireshark распространяется свободно. Скачать его можно по ссылке <https://www.wireshark.org/download.html>

Общий вид окна приложения представлен на рис. 1.

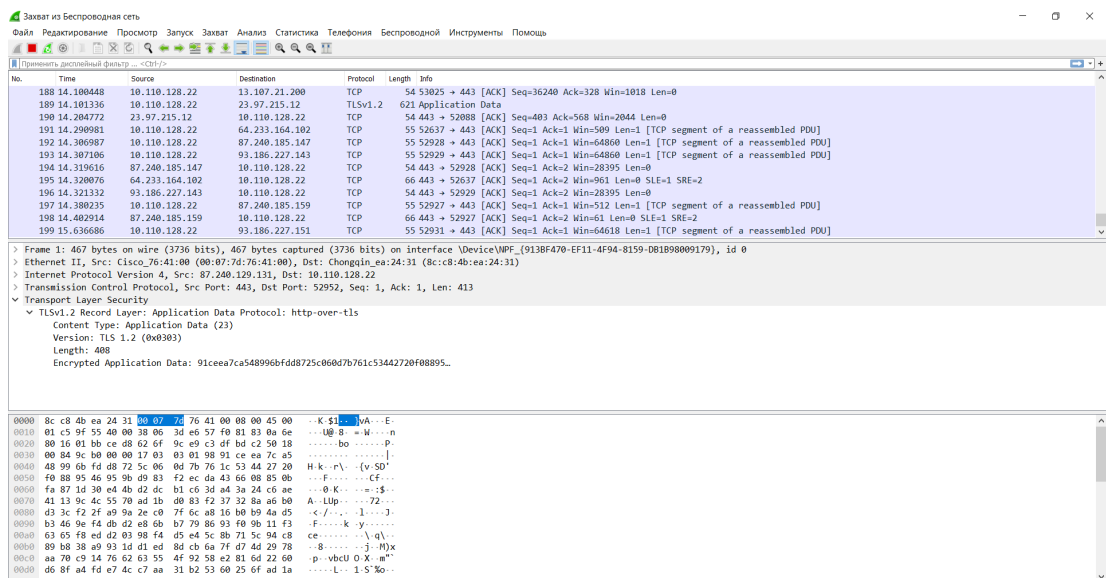


Рис. 1. Общий вид приложения Wireshark

Пользовательский интерфейс программы содержит следующие компоненты:

- меню команд и панель инструментов;
- фильтр отображения пакетов;
- список пакетов в буфере;
- панель отображения декодера протоколов;
- панель отображения пакета в шестнадцатеричном коде и символах ASCII.

Панель со списком пакетов построено отображает характеристики того или иного пакета (номер по порядку в буфере, время захвата, адреса источника и получателя, тип протокола и общая информация о нем). Перемещение по списку осуществляется с помощью мыши или клавиатуры, причем информация на двух других панелях обновляется автоматически. На панели декодера протоколов, нажимая указателем мыши на символы «>» или «V», можно отображать информацию о полях заголовков протоколов с требуемым уровнем детализации. При выборе того или иного служебного поля в заголовке оно автоматически выделяется на нижней панели, где отображается текущий пакет в шестнадцатеричном виде.

2. Работа с командной строкой

Нажмите комбинацию клавиш «Win+R». В окне «Выполнить» задайте команду *cmd* (либо задайте её в строке поиска). Откроется режим работы с командной строкой.

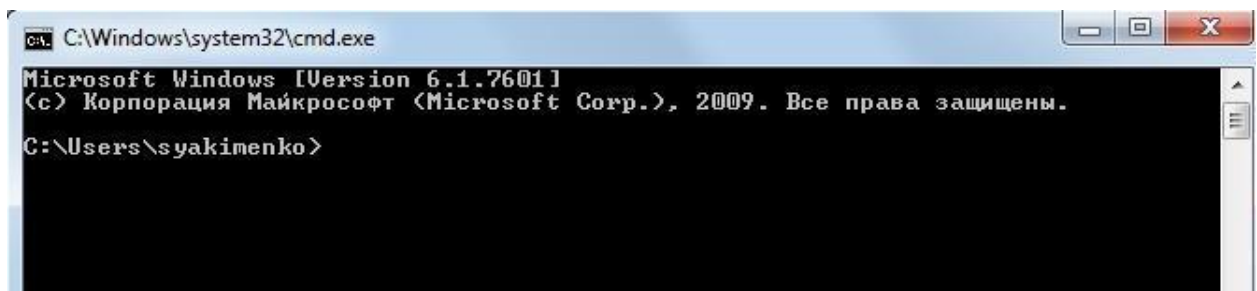
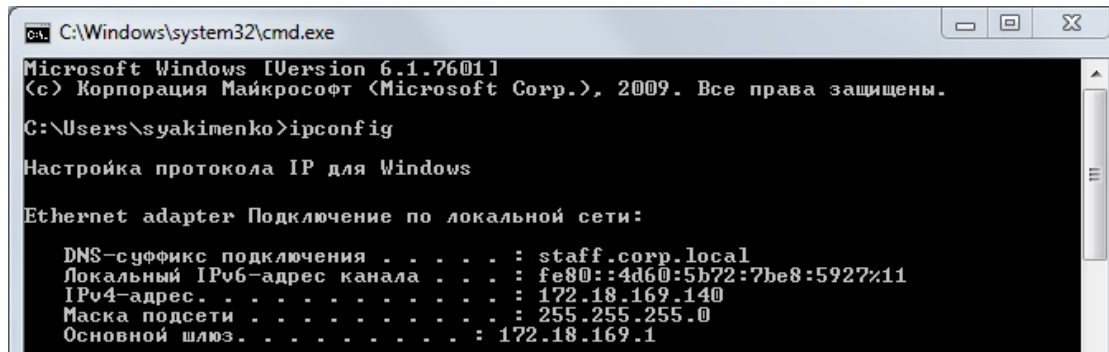


Рис. 2. Интерфейс командной строки Windows

Введите команду *ipconfig* (для Linux и MAC – *ifconfig*). Команда IPCONFIG используется для отображения текущих настроек протокола TCP/IP и для обновления некоторых параметров, задаваемых при автоматическом конфигурировании сетевых интерфейсов при использовании протокола Dynamic Host Configuration Protocol (DHCP).



```
cmd C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\syakimenko>ipconfig

Настройка протокола IP для Windows

Ethernet adapter Подключение по локальной сети:

    DNS-суффикс подключения . . . . . : staff.corp.local
    Локальный IPv6-адрес канала . . . . : fe80::4d60:5b72:7be8:5927%11
    IPv4-адрес. . . . . : 172.18.169.140
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 172.18.169.1
```

Рис.3. Демонстрация работы утилиты ipconfig

Другая утилита - Ping (Packet InterNet Grouper) - это системная программа, предназначенная для проверки соединений в сетях на основе TCP/IP. Она отправляет Echo-Request запросы протокола ICMP указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply). Время между отправкой запроса и получением ответа (RTT, Round Trip Time) позволяет определять двусторонние задержки (RTT) по маршруту и частоту потери пакетов. Что позволяет косвенно определять загруженность каналов передачи данных и промежуточных устройств. Полное отсутствие ICMP-ответов может также означать, что удалённый узел (или какой-либо из промежуточных маршрутизаторов) блокирует ICMP Echo-Reply или игнорирует ICMP Echo-Request.

Синтаксис:

`ping -параметры конечное_имя`

Конечное имя – это доменное имя или IP-адрес хоста

Некоторые параметры:

`ping [-t] [-n число] [-l размер]`

-t - Непрерывная отправка пакетов. Для завершения и вывода статистики используются комбинации клавиш Ctrl + Break (вывод статистики и продолжение), и Ctrl + C.

-n число - Число отправляемых эхо-запросов.

-l размер - Размер поля данных в байтах отправляемого запроса.

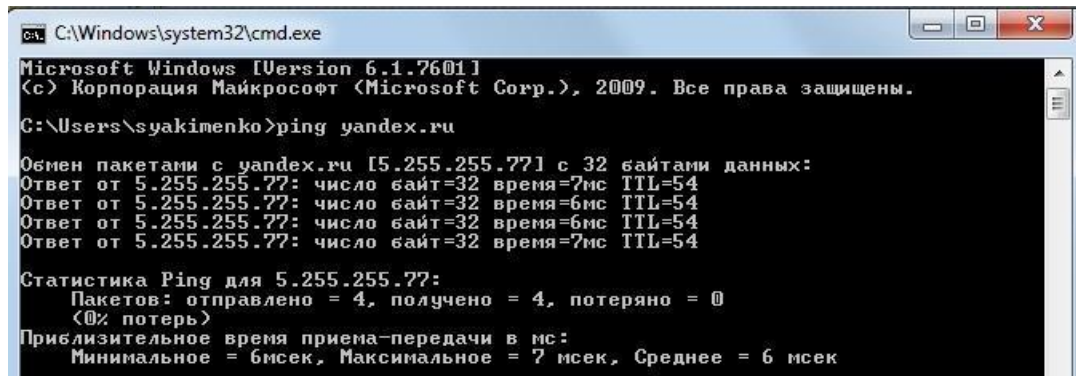
Ping можно использовать для тестирования как имени хоста (DNS или NetBIOS), так и его IP-адреса.

Примеры использования:

`ping google.com` - эхо-запрос к узлу с именем google.com с параметрами по умолчанию - количество пакетов равно 4, длина массива данных = 32 байта.

ping -n 6 -l 100 ab57.ru - опрос узла ab57.ru 6 раз пакетами с данными длиной в 100 байт

Протестируем подключение к сайту yandex.ru:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\syakimenko>ping yandex.ru

Обмен пакетами с yandex.ru [5.255.255.77] с 32 байтами данных:
Ответ от 5.255.255.77: число байт=32 время=7мс TTL=54
Ответ от 5.255.255.77: число байт=32 время=6мс TTL=54
Ответ от 5.255.255.77: число байт=32 время=6мс TTL=54
Ответ от 5.255.255.77: число байт=32 время=7мс TTL=54

Статистика Ping для 5.255.255.77:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
    Минимальное = 6мсек, Максимальное = 7 мсек, Среднее = 6 мсек
```

Рис.4. Демонстрация работы утилиты ping

По умолчанию, если не применяются никакие параметры, отправляется 4 эхо-запроса размером 32 байта.

Сервер yandex.ru с IP-адресом 5.255.255.77 прислал 4 ответа на наши запросы.

3. Работа с браузером

Перед тем как открывать ссылку в браузере, запустим захват пакетов WireShark.

Далее откроем в браузере веб-сайта не использующий шифрование: <http://neverssl.com/>:

NeverSSL

What?

This website is for when you try to open Facebook, Google, Amazon, etc on a wifi network, and nothing happens. Type "http://neverssl.com" into your browser's url bar, and you'll be able to log on.

How?

neverssl.com will never use SSL (also known as TLS). No encryption, no strong authentication, no [HSTS](#), no HTTP/2.0, just plain old unencrypted HTTP and forever stuck in the dark ages of internet security.

Why?

Normally, that's a bad idea. You should always use SSL and secure encryption when possible. In fact, it's such a bad idea that most websites are now using https by default.

And that's great, but it also means that if you're relying on poorly-behaved wifi networks, it can be hard to get online. Secure browsers and websites using https make it impossible for those wifi networks to send you to a login or payment page. Basically, those networks can't tap into your connection just like attackers can't. Modern browsers are so good that they can remember when a website supports encryption and even if you type in the website name, they'll use https.

And if the network never redirects you to this page, well as you can see, you're not missing much.

Рис.5. Работа с браузером

Теперь переходим в WireShark. Для того чтобы быстро найти нужный нам пакет, мы используем фильтр http.

HTTP — это протокол, позволяющий получать различные ресурсы, например HTML-документы. Протокол HTTP лежит в основе обмена данными в Интернете. HTTP является протоколом клиент-серверного взаимодействия, что означает инициирование запросов к серверу самим получателем, обычно веб-браузером (web-browser).

Нам необходимо найти пакет со значением 200 OK в поле «Info» — это код успешного запроса.

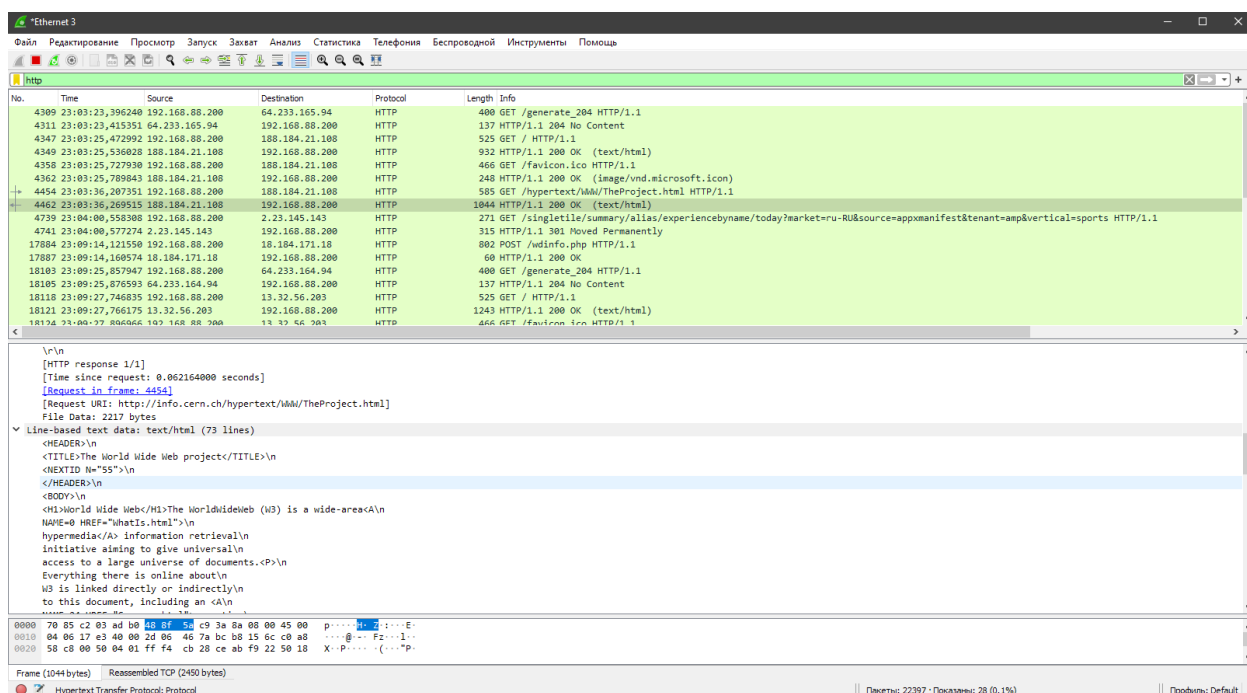


Рис. 6. Перехват веб-страницы

Раскройте в панели отображения декодера протоколов поле «Line-based text data»: вы увидите содержимое нашей веб-страницы.

Ход работы

1. Узнайте IP-адрес вашего компьютера с помощью утилиты *ipconfig*. Сделайте скриншоты (и по итогу остальных пунктов).
2. Запустите Wireshark и разверните главное окно приложения на весь экран (для удобства работы). Выбрать сетевой адаптер, на котором будет происходить мониторинг (Ethernet, Беспроводная сеть и др. – в зависимости от способа вашего подключения).
3. Начать захват пакетов. Протестируйте подключение к серверу какого-либо известного сайта с помощью утилиты *ping*. Измените количество запросов, например, до 3: *ping -n 3 конечное_имя*.
4. С помощью фильтра *icmp* найдите в WireShark перехваченные запросы (*request*) и ответы (*reply*) утилиты *ping*. Совпадает ли количество ответов с количеством, полученным в п.3? С помощью п.1. проанализируйте поля *source* (источник) и *destination* (получатель) перехваченных кадров.
5. По примеру, описанному в методических указаниях, откройте копию первого в мире веб-сайта в браузере: <http://info.cern.ch/hypertext/WWW/TheProject.html>
Перехватите содержимое веб-страницы.

