

Лабораторная работа: наблюдение за процессом трёхстороннего рукопожатия TCP с помощью программы Wireshark

Топология



Задачи

Часть 1. Подготовка программы Wireshark к захвату пакетов

- Выберите подходящий интерфейс сетевого адаптера для захвата пакетов.

Часть 2. Захват, поиск и изучение пакетов

- Захватите данные веб-сеанса на узле www.google.com.
- Найдите соответствующие пакеты для веб-сеанса.
- Изучите содержащиеся в пакетах данные, включая IP-адреса, номера портов TCP и флажки управления TCP.

Исходные данные/сценарий

В данной лабораторной работе вам предстоит воспользоваться программой Wireshark для захвата и изучения пакетов, сгенерированных между браузером ПК, где используется HTTP-протокол, и веб-сервером, например www.google.com. При первом запуске приложения на узле, например HTTP или FTP, TCP устанавливает связь между двумя узлами с помощью трёхстороннего рукопожатия. Например, при просмотре интернет-страниц через веб-браузер ПК трёхстороннее рукопожатие позволяет установить связь между узловым ПК и веб-сервером. Одновременно на ПК могут иметь место сразу несколько активных сеансов TCP с разными веб-сайтами.

Примечание. Эту лабораторную работу нельзя выполнять при помощи Netlab. Она предполагает наличие доступа к Интернету.

Необходимые ресурсы

1 ПК (Windows 7, Vista или XP с доступом к командной строке, доступу к Интернету и установленному анализатору пакетов Wireshark)

1. Подготовка программы Wireshark к захвату пакетов

В части 1 вам необходимо запустить программу Wireshark и выбрать подходящие интерфейсы для начала захвата пакетов.

1. Узнайте адреса интерфейсов ПК.

Для выполнения лабораторной работы вам нужно узнать IP-адрес своего ПК и физический адрес сетевого адаптера, который также называется MAC-адресом.

- а. Откройте окно командной строки, введите **ipconfig /all** и нажмите клавишу ВВОД.

```
Physical Address. . . . . : C8-0A-A9-FA-DE-0D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.1.130(Preferred)
Subnet Mask. . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, December 01, 2012 1:43:35 PM
Lease Expires . . . . . : Sunday, December 02, 2012 1:43:35 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

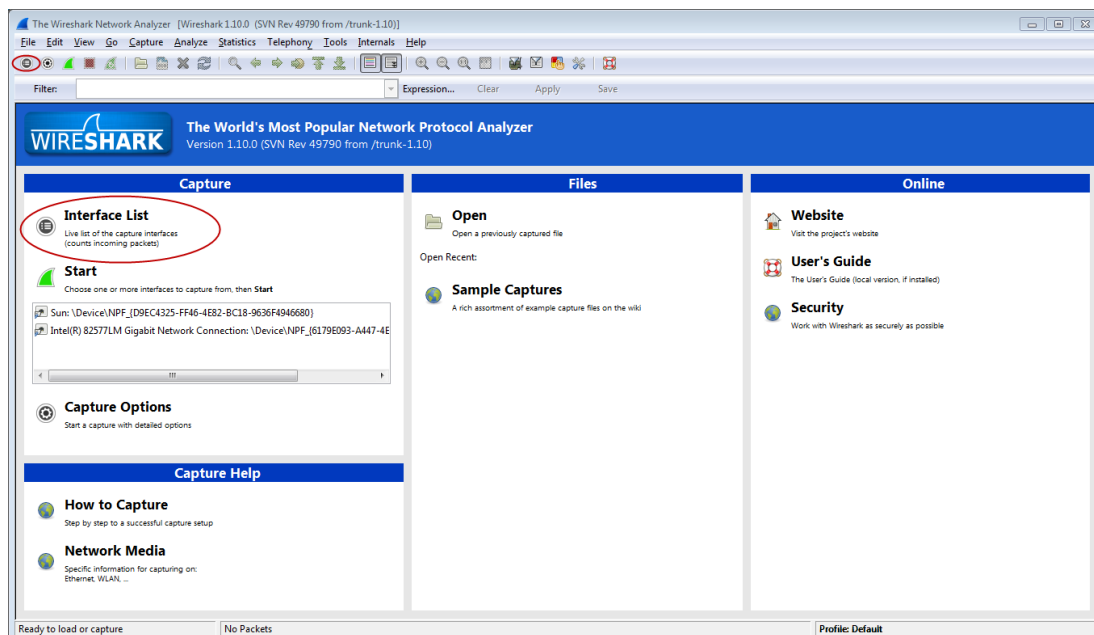
- б. Запишите IP- и MAC-адреса, связанные с выбранным адаптером Ethernet, поскольку это и есть тот адрес источника, который нужно искать при анализе захваченных пакетов.

IP-адрес узла ПК: _____

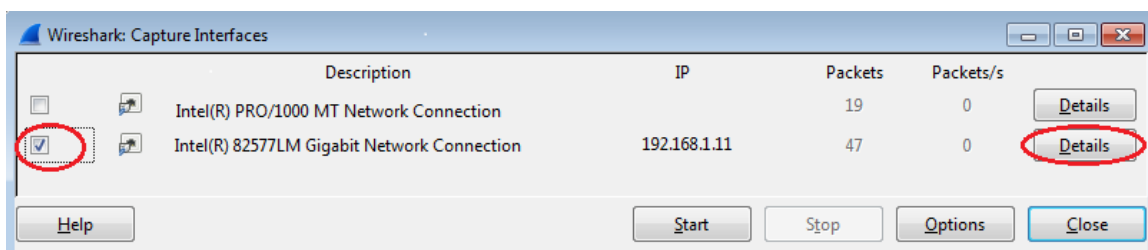
MAC-адрес узла ПК: _____

2. Запустите программу Wireshark и выберите подходящий интерфейс.

- а. Нажмите кнопку **Пуск** и дважды нажмите на **Wireshark**.
- б. Запустив программу Wireshark, нажмите на параметр **Interface List** (Список интерфейсов).



- с. В окне **Wireshark: Capture Interfaces** (Захват интерфейсов) установите флажок напротив интерфейса подключения к вашей локальной сети.



Примечание. Если указано несколько интерфейсов и вы не уверены в выборе, нажмите кнопку **Details** (Сведения). Откройте вкладку **802.3 (Ethernet)** и убедитесь в том, что MAC-адрес соответствует тому, что вы записали в шаге 1b. Проверив данные, закройте окно со сведениями об интерфейсе.

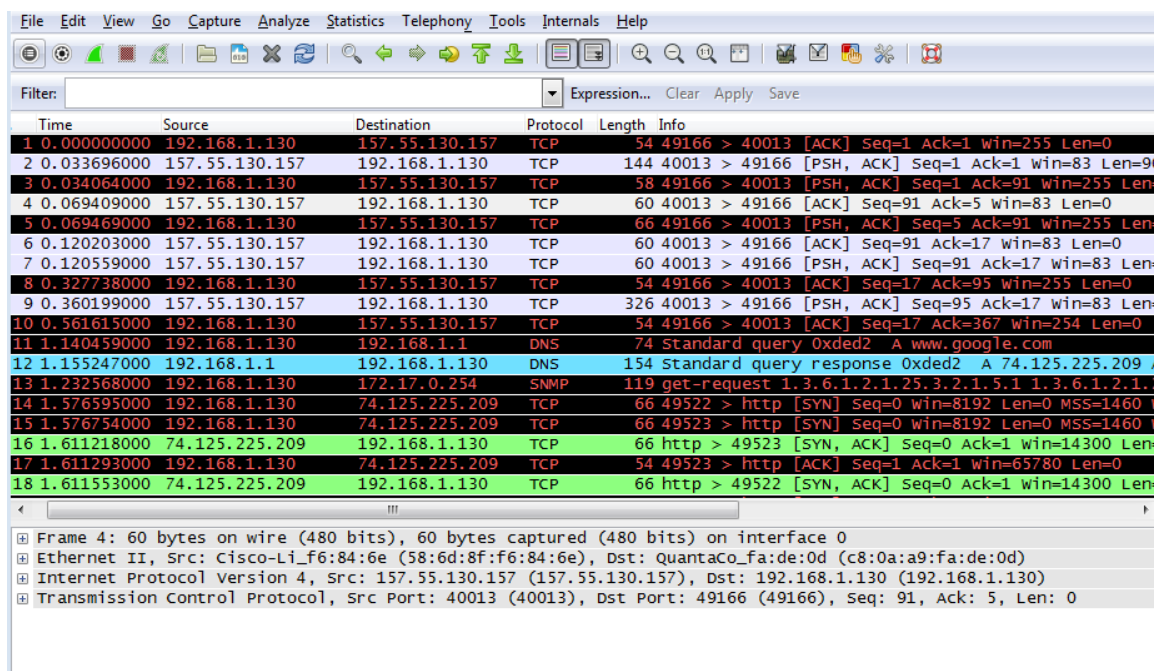
2. Захват, поиск и изучение пакетов

1. Нажмите кнопку **Start** (Старт), чтобы начать захват данных.

- Откройте веб-сайт www.google.com. Сверните окно Google и вернитесь в программу Wireshark. Остановите процесс захвата данных. Вы увидите захваченный трафик, как показано на шаге b.

Примечание. Инструктор может предложить вам другой веб-сайт. В этом случае введите название или адрес сайта в соответствующее поле:

- Теперь окно перехвата данных активно. Найдите столбцы **Source** (Источник), **Destination** (Назначение) и **Protocol** (Протокол).



Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.130	157.55.130.157	TCP	54 49166 > 40013 [ACK] Seq=1 Ack=1 win=255 Len=0
2	0.033696000	157.55.130.157	192.168.1.130	TCP	144 40013 > 49166 [PSH, ACK] Seq=1 Ack=1 win=83 Len=90
3	0.034064000	192.168.1.130	157.55.130.157	TCP	58 49166 > 40013 [PSH, ACK] Seq=1 Ack=91 win=255 Len=0
4	0.069409000	157.55.130.157	192.168.1.130	TCP	60 40013 > 49166 [ACK] Seq=91 Ack=5 win=83 Len=0
5	0.069469000	192.168.1.130	157.55.130.157	TCP	66 49166 > 40013 [PSH, ACK] Seq=5 Ack=91 win=255 Len=0
6	0.120203000	157.55.130.157	192.168.1.130	TCP	60 40013 > 49166 [ACK] Seq=91 Ack=17 win=83 Len=0
7	0.120559000	157.55.130.157	192.168.1.130	TCP	60 40013 > 49166 [PSH, ACK] Seq=91 Ack=17 win=83 Len=0
8	0.327738000	192.168.1.130	157.55.130.157	TCP	54 49166 > 40013 [ACK] Seq=17 Ack=95 win=255 Len=0
9	0.360199000	157.55.130.157	192.168.1.130	TCP	326 40013 > 49166 [PSH, ACK] Seq=95 Ack=17 win=83 Len=0
10	0.561615000	192.168.1.130	157.55.130.157	TCP	54 49166 > 40013 [ACK] Seq=17 Ack=367 win=254 Len=0
11	1.140459000	192.168.1.130	192.168.1.1	DNS	74 Standard query 0xded2 A www.google.com
12	1.155247000	192.168.1.1	192.168.1.130	DNS	154 Standard query response 0xded2 A 74.125.225.209
13	1.232568000	192.168.1.130	172.17.0.254	SNMP	119 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.2
14	1.576595000	192.168.1.130	74.125.225.209	TCP	66 49522 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460
15	1.576754000	192.168.1.130	74.125.225.209	TCP	66 49523 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460
16	1.611218000	74.125.225.209	192.168.1.130	TCP	66 http > 49523 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0
17	1.611293000	192.168.1.130	74.125.225.209	TCP	54 49523 > http [ACK] Seq=1 Ack=1 win=65780 Len=0
18	1.611553000	74.125.225.209	192.168.1.130	TCP	66 http > 49522 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0

Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: Cisco-Li_f6:84:6e (58:6d:8f:f6:84:6e), Dst: QuantaCo_fa:de:0d (c8:0a:a9:fa:de:0d)
 Internet Protocol Version 4, Src: 157.55.130.157 (157.55.130.157), Dst: 192.168.1.130 (192.168.1.130)
 Transmission Control Protocol, Src Port: 40013 (40013), Dst Port: 49166 (49166), Seq: 91, Ack: 5, Len: 0

2. Найдите соответствующие пакеты для веб-сеанса.

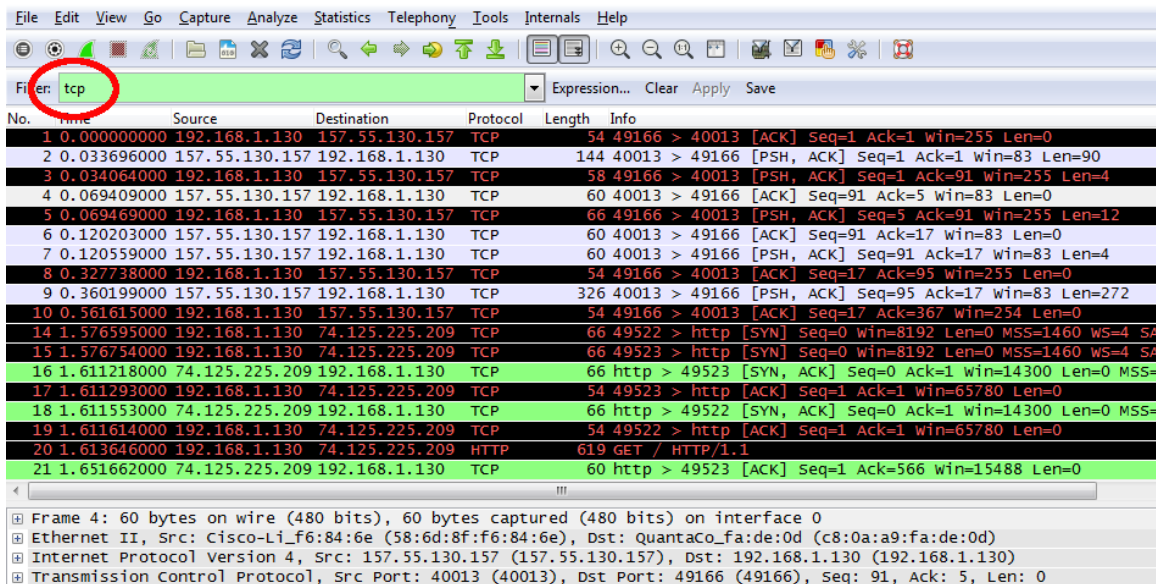
Если компьютер включён недавно и еще не использовался для доступа к Интернету, в захваченных данных вы сможете увидеть весь процесс, включая протокол разрешения адресов (ARP), службу доменных имен (DNS) и трёхстороннее рукопожатие TCP. На экране захвата в части 2, шаг 1 показаны все пакеты, которые ПК должен отправить на адрес www.google.com. В данном случае ПК уже имел запись ARP для шлюза по умолчанию, поэтому первым делом он создал DNS-запрос для преобразования www.google.com.

- В кадре 11 показан DNS-запрос от ПК к DNS-серверу, призванный преобразовать доменное имя www.google.com в IP-адрес веб-сервера. ПК должен знать IP-адрес до отправления первого пакета на веб-сервер.

Назовите IP-адрес DNS-сервера, запрошенного компьютером. _____

- Кадр 12 показывает ответ DNS-сервера, содержащий IP-адрес www.google.com.

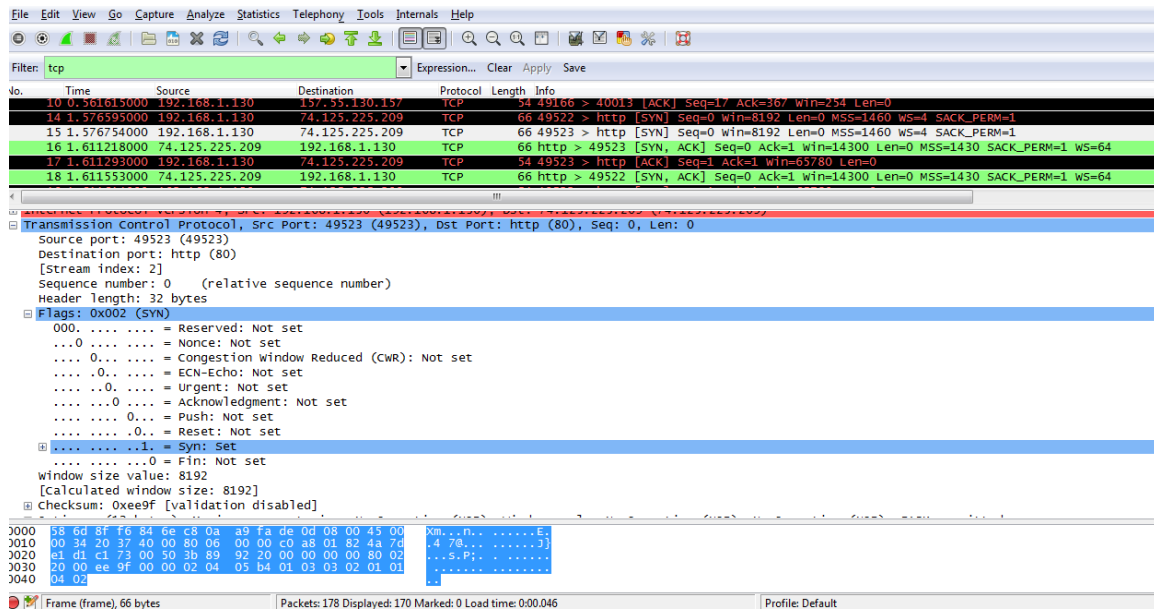
- с. Найдите соответствующий пакет, чтобы запустить процедуру трёхстороннего рукопожатия. В данном примере кадр 15 показывает начало трёхстороннего рукопожатия TCP.
- Назовите IP-адрес веб-сервера Google. _____
- д. Если вы получили много пакетов, связанных с TCP-соединением, воспользуйтесь фильтрами программы Wireshark. В поле фильтра программы Wireshark введите **tcp** и нажмите клавишу ВВОД.



3. Изучите содержащиеся в пакетах данные, включая IP-адреса, номера портов TCP и флажки управления TCP.

- а. В нашем примере кадр 15 показывает начало трёхстороннего рукопожатия между ПК и веб-сервером Google. На панели списка пакетов (верхний раздел основного окна) выберите кадр. После этого будет выделена строка и отображена зашифрованная информация из пакета в двух нижних панелях. Проверьте данные TCP в панели сведений о пакетах (средний раздел основного окна).
- б. На панели нажмите на значок + слева от строки Transmission Control Protocol (Протокол управления передачей данных), чтобы увидеть подробную информацию о TCP.
- с. Слева от флажков нажмите на значок +. Обратите внимание на порты источника и назначения, а также на установленные флажки.

Примечание. Чтобы отобразить все необходимые данные, скорректируйте размеры окон программы Wireshark.



Назовите номер порта источника TCP. _____

Как бы вы классифицировали порт источника? _____

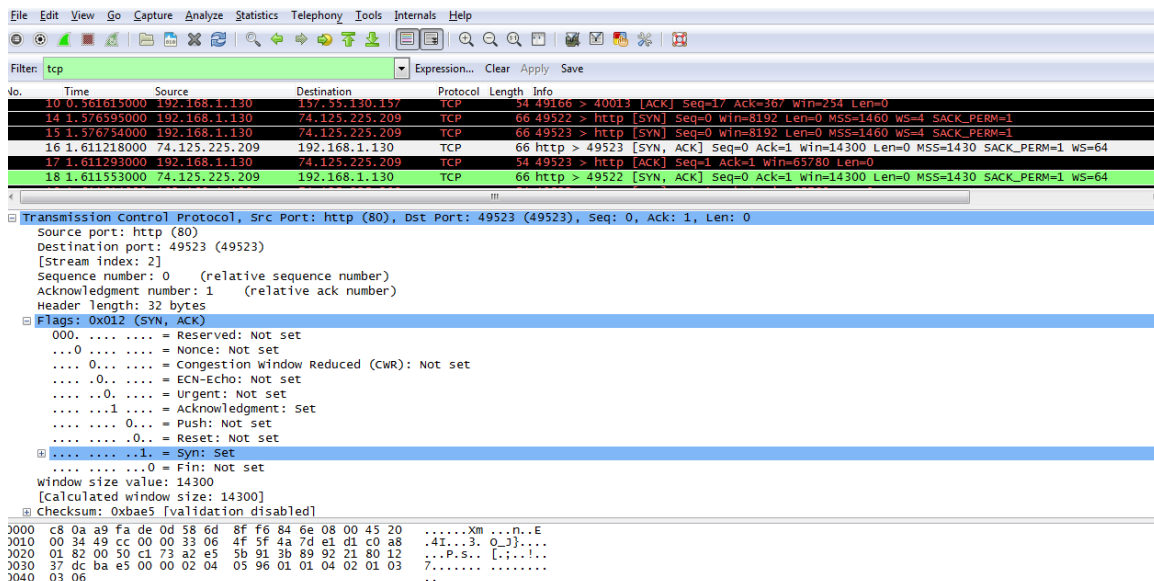
Назовите номер порта назначения TCP. _____

Как бы вы классифицировали порт назначения? _____

Какие установлены флажки? _____

На какое значение настроен относительный последовательный номер? _____

- d. Чтобы выбрать следующий кадр в трёхстороннем рукопожатии, в меню программы Wireshark выберите параметр **Go** (Перейти), а затем **Next Packet In Conversation** (Следующий пакет коммуникации). В данном примере это кадр 16. Это ответ веб-сервера Google на исходный запрос для начала сеанса.



Назовите значения портов источника и назначения. _____

Какие установлены флажки? _____

На какие значения настроены относительный последовательный номер и номер подтверждения? _____

- е. И, наконец, изучите третий пакет трёхстороннего рукопожатия в данном примере. Нажав на кадр 17 в верхнем окне, вы увидите следующую информацию в данном примере:

No.	Time	Source	Destination	Protocol	Length	Info
12	1.155247000	192.168.1.1	192.168.1.130	DNS	154	Standard query response Oxded2 A 74.125.225.209 A 74.125.225.210 A 74.125.225.212 A
13	1.232568000	192.168.1.130	172.17.0.254	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1 1.3.6.1.2.1.25.3.5.1.2
14	1.576595000	192.168.1.130	74.125.225.209	TCP	66	49523 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
15	1.576754000	192.168.1.130	74.125.225.209	TCP	66	49523 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
16	1.611218000	74.125.225.209	192.168.1.130	TCP	66	http > 49523 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64
17	1.611293000	192.168.1.130	74.125.225.209	TCP	54	49523 > http [ACK] Seq=1 Ack=1 win=65780 Len=0
18	1.611553000	74.125.225.209	192.168.1.130	TCP	66	http > 49523 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64

Transmission Control Protocol, Src Port: 49523 (49523), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0	
Source port:	49523 (49523)
Destination port:	http (80)
[Stream index: 2]	
Sequence number:	1 (relative sequence number)
Acknowledgment number:	1 (relative ack number)
Header Length:	20 bytes
Flags:	0x010 (ACK)
000. = Reserved: Not set ...0 = Nonce: Not set0... = Congestion Window Reduced (CWR): Not set0... = ECN-Echo: Not set0... = Urgent: Not set1... = Acknowledgment: Set0... = Push: Not set0... = Reset: Not set0... = Syn: Not set0... = Fin: Not set window size value: 16445 [Calculated window size: 65780]	

Raw Data	
0000	58 6d 8f f6 84 6e c8 0a a9 fa de 0d 08 00 45 00
0010	00 28 20 38 40 00 80 06 00 00 c0 a8 01 82 4a 7d
0020	e1 d1 c1 73 00 50 3b 89 92 21 a2 e5 5b 92 50 10
0030	40 3d ee 93 00 00

Изучите третий и последний пакет рукопожатия.

Какие установлены флажки? _____

Для относительного последовательного номера и номера подтверждения в качестве исходного значения выбрана единица. Соединение TCP настроено. Теперь можно начать передачу данных между ПК источника и веб-сервером.

- ф. Закройте программу Wireshark.

Вопросы на закрепление

- В программе Wireshark доступны сотни фильтров. В большой сети может быть множество фильтров и различных типов трафика. Какие три фильтра в списке будут наиболее полезны для сетевого администратора?

- Как ещё можно использовать программу Wireshark в производственной сети?

