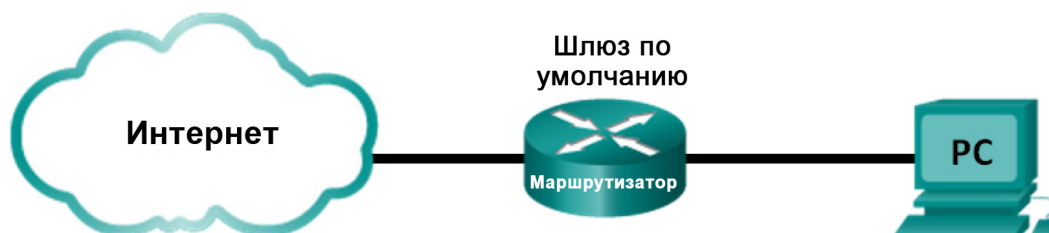


Лабораторная работа. Изучение процесса трехстороннего квитирования протокола TCP с помощью программы Wireshark

Топология



Задачи

Часть 1. Подготовка программы Wireshark к захвату пакетов

Часть 2. Захват, поиск и изучение пакетов

Общие сведения/сценарий

В данной лабораторной работе вам предстоит воспользоваться программой Wireshark для захвата и изучения пакетов, которыми обмениваются браузер ПК, использующий HTTP-протокол, и веб-сервер, например www.google.com. При первом запуске на узле приложения, например HTTP или FTP, протокол TCP устанавливает между двумя узлами надежный TCP-сеанс с помощью трехстороннего квитирования. Например, при просмотре интернет-страниц через веб-браузер ПК инициируется трехстороннее квитирование и устанавливается сеанс связи между хост-компьютером и веб-сервером. Одновременно на ПК могут иметь место сразу несколько активных TCP-сеансов с разными веб-сайтами.

Примечание. Эту лабораторную работу нельзя выполнять при помощи Netlab. Для выполнения работы необходим доступ в Интернет.

Необходимые ресурсы

Один ПК (Windows 7 или 8 с доступом к командной строке, выходом в Интернет и установленной программой Wireshark)

Часть 1: Подготовка программы Wireshark к захвату пакетов

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

Шаг 1: Узнайте адреса интерфейсов ПК.

В данной лабораторной работе вам необходимо узнать IP-адрес компьютера и физический адрес сетевой платы, также называемый MAC-адресом.

а. Откройте окно командной строки, введите команду `ipconfig /all` и нажмите клавишу Enter.

```
Physical Address. . . . . : 00-1A-73-EA-63-8C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::a858:5f3e:35e2:d38f%14(Preferred)
IPv4 Address. . . . . : 192.168.1.130(Preferred)
Subnet Mask . . . . . : 255.255.255.0
```

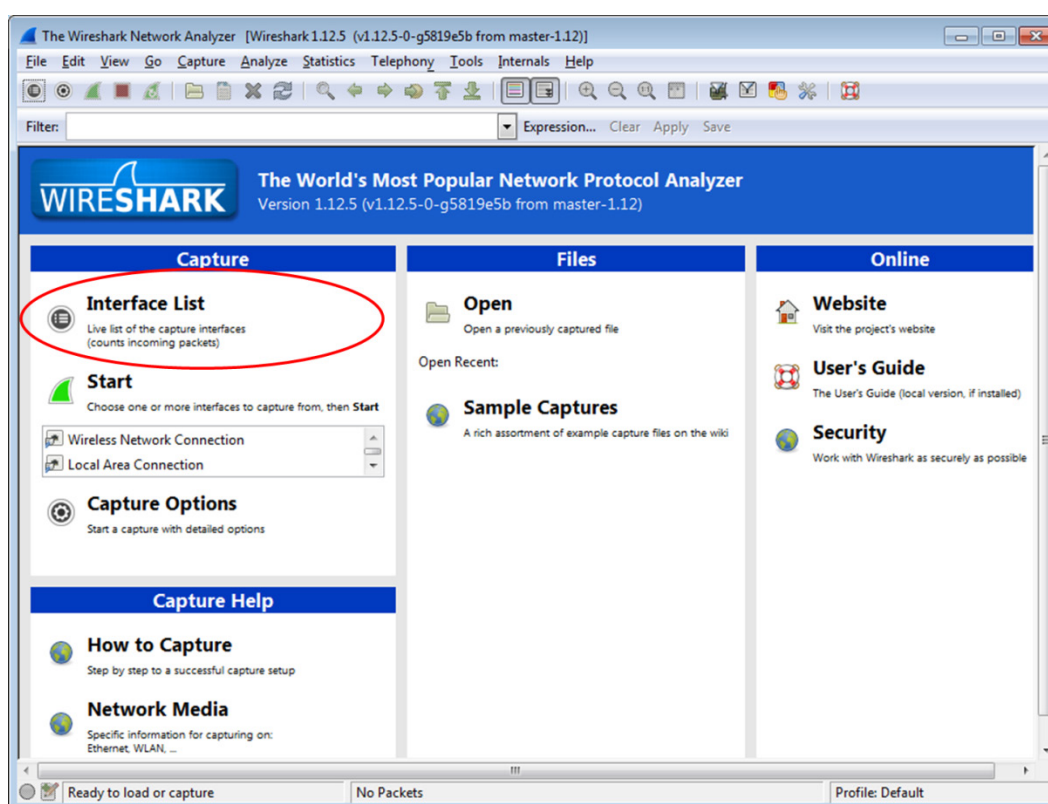
- b. Запишите полученные IP-адреса и MAC-адреса, связанные с выбранным адаптером Ethernet. Это адрес источника, который требуется найти при изучении захваченных пакетов.

IP-адрес узла ПК: _____

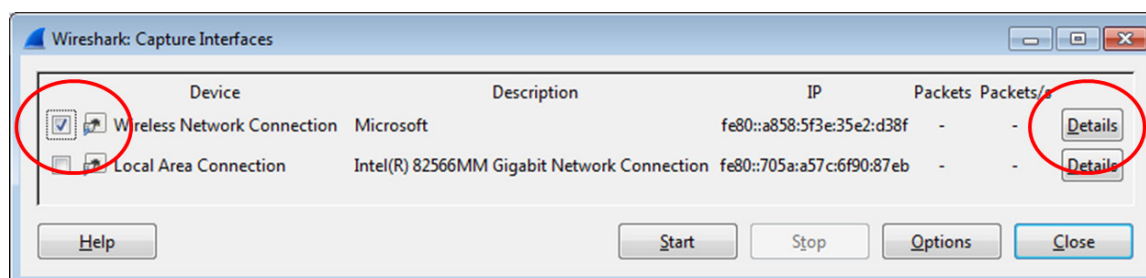
MAC-адрес узла ПК: _____

Шаг 2: Запустите программу Wireshark и выберите подходящий интерфейс.

- a. Нажмите кнопку **Пуск**. Во всплывающем меню дважды щелкните **Wireshark**.
- b. После запуска программы Wireshark нажмите на **Interface List** (Список интерфейсов).



- c. В окне **Wireshark: Capture Interfaces** (Захватить интерфейсы) установите флажок рядом с интерфейсом, подключенным к вашей локальной сети.



Примечание. Если перечислено 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 1Б. Проверив данные, закройте окно со сведениями об интерфейсе.

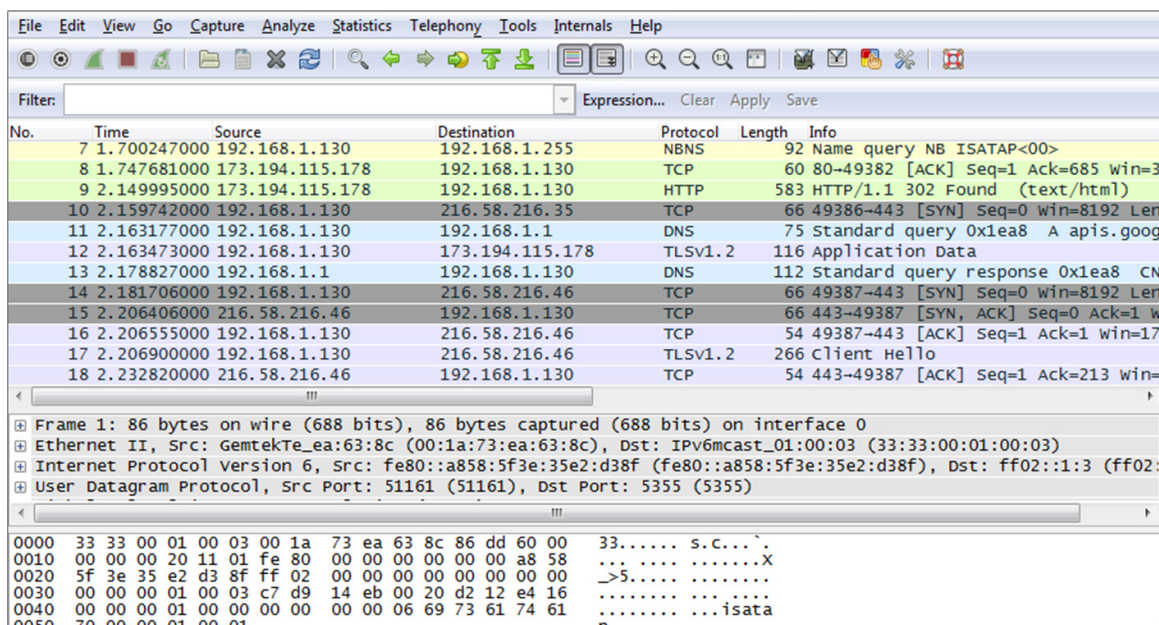
Часть 2: Захват, поиск и изучение пакетов

Шаг 1: Выполните захват данных.

- Нажмите кнопку **Start** (Начать), чтобы начать захват данных.
- Перейдите на сайт www.google.com. Сверните окно браузера и вернитесь в Wireshark. Остановите процесс захвата данных.

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

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



No.	Time	Source	Destination	Protocol	Length	Info
7	1.700247000	192.168.1.130	192.168.1.255	NBNS	92	Name query NB ISATAP<00>
8	1.747681000	173.194.115.178	192.168.1.130	TCP	60	80→49382 [ACK] Seq=1 Ack=685 win=3
9	2.149995000	173.194.115.178	192.168.1.130	HTTP	583	HTTP/1.1 302 Found (text/html)
10	2.159742000	192.168.1.130	216.58.216.35	TCP	66	49386→443 [SYN] Seq=0 win=8192 Len
11	2.163177000	192.168.1.130	192.168.1.1	DNS	75	Standard query 0x1ea8 A apis.goog
12	2.163473000	192.168.1.130	173.194.115.178	TLSv1.2	116	Application Data
13	2.178827000	192.168.1.1	192.168.1.130	DNS	112	Standard query response 0x1ea8 CN
14	2.181706000	192.168.1.130	216.58.216.46	TCP	66	49387→443 [SYN] Seq=0 win=8192 Len
15	2.206406000	216.58.216.46	192.168.1.130	TCP	66	443→49387 [SYN, ACK] Seq=0 Ack=1 w
16	2.206555000	192.168.1.130	216.58.216.46	TCP	54	49387→443 [ACK] Seq=1 Ack=1 win=17
17	2.206900000	192.168.1.130	216.58.216.46	TLSv1.2	266	Client Hello
18	2.232820000	216.58.216.46	192.168.1.130	TCP	54	443→49387 [ACK] Seq=1 Ack=213 win=

Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
 Ethernet II, Src: GemtekTe_ea:63:8c (00:1a:73:ea:63:8c), Dst: IPv6mcast_01:00:03 (33:33:00:01:00:03)
 Internet Protocol version 6, Src: fe80::a858:5f3e:35e2:d38f (fe80::a858:5f3e:35e2:d38f), Dst: ff02::1:3 (ff02::1:3)
 User Datagram Protocol, Src Port: 51161 (51161), Dst Port: 5355 (5355)

```

0000  33 33 00 01 00 03 00 1a 73 ea 63 8c 86 dd 60 00  33.....s.c...
0010  00 00 00 00 20 11 01 fe 80 00 00 00 00 00 00 a8 58  ... ..X
0020  5f 3e 35 e2 d3 8f ff 02 00 00 00 00 00 00 00 00 00  >5.....
0030  00 00 00 00 01 00 03 c7 d9 14 eb 00 20 d2 12 e4 16  .....
0040  00 00 00 01 00 00 00 00 00 00 06 69 73 61 74 61  .....isata
0050  70 00 00 01 00 01 00 00 00 00 00 00 00 00 00 00  n
  
```

Шаг 2: Найдите соответствующие пакеты для веб-сеанса.

Если компьютер включен недавно и еще не использовался для доступа в Интернет, в захваченных данных вы сможете увидеть весь процесс, включая протокол разрешения адресов (ARP), службу доменных имен (DNS) и трехстороннее квитирование TCP. Если ПК уже имел запись ARP для шлюза по умолчанию, то он создал DNS-запрос для преобразования адреса www.google.com.

- В кадре 11 показан DNS-запрос от ПК к DNS-серверу, который пытается преобразовать доменное имя www.google.com в IP-адрес веб-сервера. Прежде чем отправить первый пакет на веб-сервер, ПК должен узнать IP-адрес.

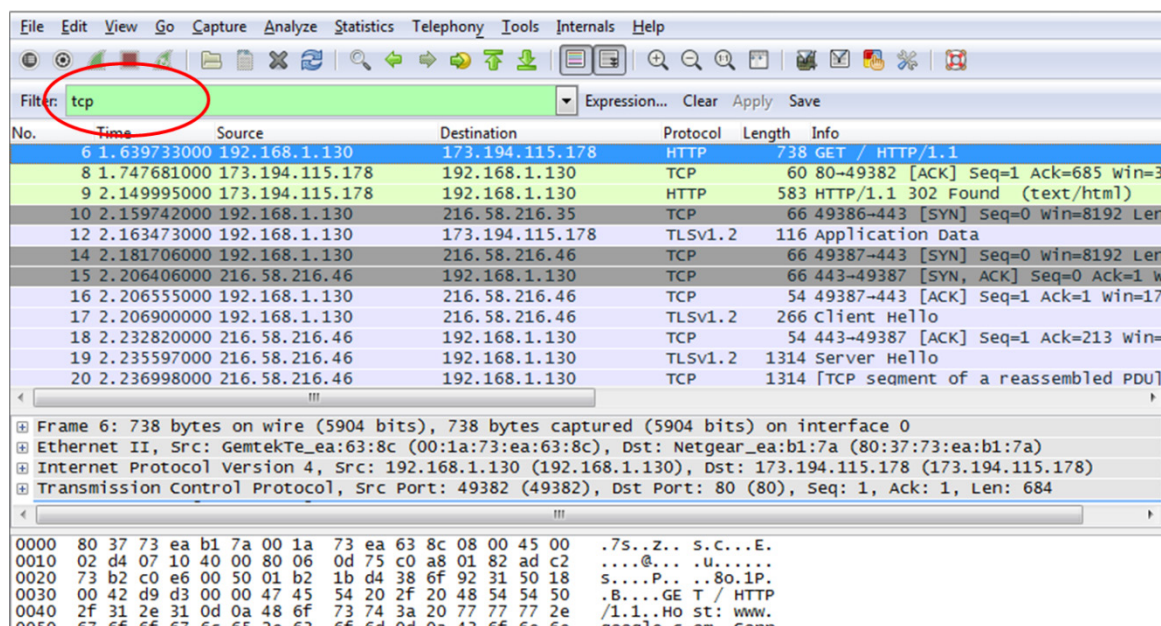
Назовите IP-адрес DNS-сервера, запрошенного компьютером. _____

- Кадр 13 представляет собой ответ DNS-сервера. Он содержит IP-адрес сайта www.google.com.

- с. Найдите соответствующий пакет, чтобы запустить процедуру трехстороннего квитирования. В данном примере кадр 14 является началом трехстороннего квитирования TCP.

Назовите IP-адрес веб-сервера Google. _____

- д. Если вы получили много пакетов, не связанных с TCP-соединением, возможно, целесообразно воспользоваться средствами фильтрации программы Wireshark. В поле значения фильтра программы Wireshark введите **tcp** и нажмите **Enter**.



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

- В нашем примере кадр 14 представляет собой начало трехстороннего квитирования между ПК и веб-сервером Google. На панели списка пакетов (верхний раздел основного окна) выберите кадр. После этого будет выделена строка и отображена декодированная информация из этого пакета в двух нижних панелях. Изучите данные TCP в панели сведений о пакетах (средний раздел основного окна).
- На панели сведений о пакетах нажмите на значок **+** слева от строки Transmission Control Protocol (Протокол управления передачей данных), чтобы увидеть подробную информацию о TCP.
- Нажмите на значок **+** слева от строки Flags (Флаги). Обратите внимание на порты источника и места назначения, а также на установленные флаги.

Примечание. Чтобы отобразить все необходимые данные, может потребоваться скорректировать размеры верхнего и среднего окон программы Wireshark.

Filter: tcp

No.	Time	Source	Destination	Protocol	Length	Info
8	1.747681000	173.194.115.178	192.168.1.130	TCP	60	80→49382 [ACK] Seq=1 Ack=685 win=3
9	2.149995000	173.194.115.178	192.168.1.130	HTTP	583	HTTP/1.1 302 Found (text/html)
10	2.159742000	192.168.1.130	216.58.216.35	TCP	66	49386→443 [SYN] Seq=0 win=8192 Len=
12	2.163473000	192.168.1.130	173.194.115.178	TLSv1.2	116	Application Data
14	2.181706000	192.168.1.130	216.58.216.46	TCP	66	49387→443 [SYN] Seq=0 win=8192 Len=
15	2.206406000	216.58.216.46	192.168.1.130	TCP	66	443→49387 [SYN, ACK] Seq=0 Ack=1 W
16	2.206555000	192.168.1.130	216.58.216.46	TCP	54	49387→443 [ACK] Seq=1 Ack=1 Win=17
17	2.206600000	192.168.1.130	216.58.216.46	TLSv1.2	266	Client Hello

Frame 14: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: GemtekTe_ea:63:8c (00:1a:73:ea:63:8c), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)

Internet Protocol Version 4, Src: 192.168.1.130 (192.168.1.130), Dst: 216.58.216.46 (216.58.216.46)

Transmission Control Protocol, Src Port: 49387 (49387), Dst Port: 443 (443), Seq: 0, Len: 0

Source Port: 49387 (49387)

Destination Port: 443 (443)

[Stream index: 3]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

Acknowledgment number: 0

Header Length: 32 bytes

... 0000 0000 0010 = Flags: 0x002 (SYN)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...0 = Acknowledgment: Not set

.... 0... = Push: Not set

.... 0.. = Reset: Not set

.... 1. = Syn: Set

.... 0 = Fin: Not set

window size value: 8192

[calculated window size: 8192]

Checksum: 0x5c37 [validation disabled]

Urgent pointer: 0

Назовите номер порта источника TCP. _____

Как бы вы классифицировали порт источника? _____

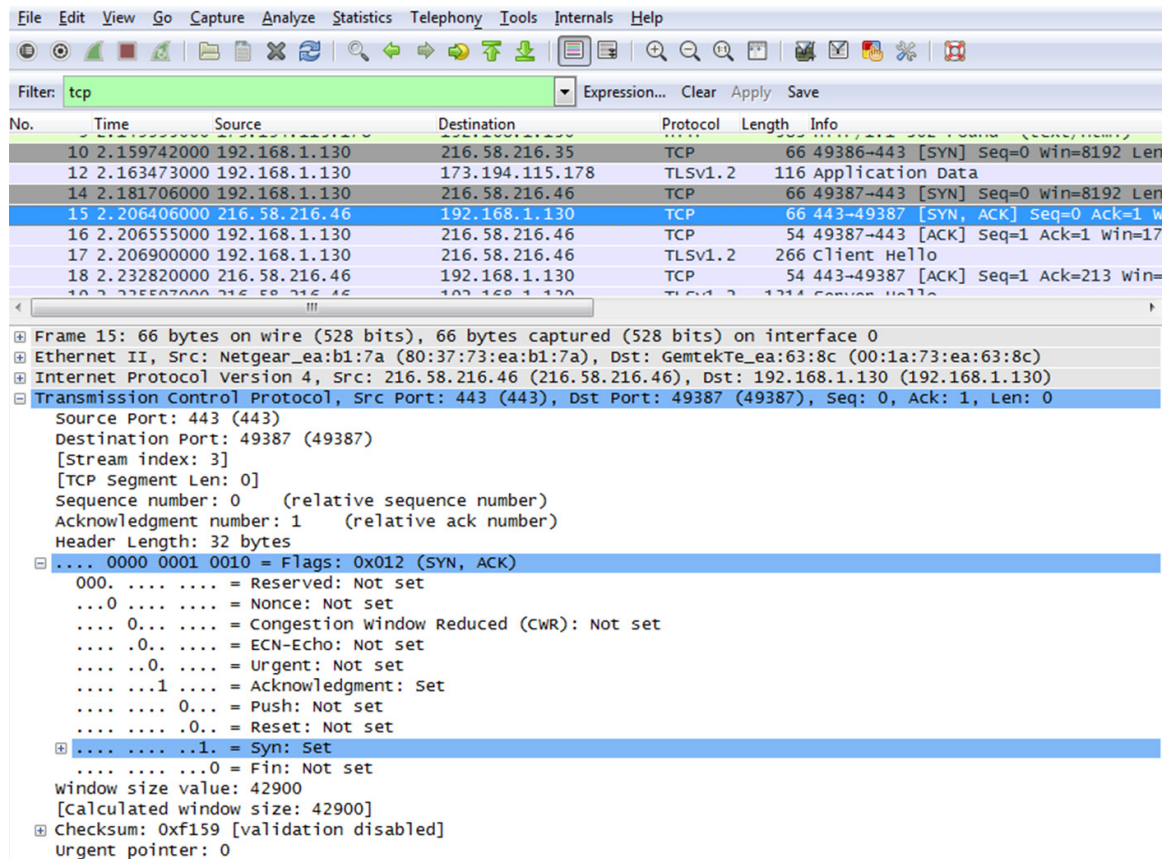
Назовите номер порта назначения TCP. _____

Как бы вы классифицировали порт назначения? _____

Какие установлены флаги? _____

Какое значение задано для относительного порядкового номера? _____

- d. Чтобы выбрать следующий кадр в трехстороннем квитировании, в меню программы Wireshark выберите пункт **Go** (Перейти), а затем **Next Packet In Conversation** (Следующий пакет в диалоге). В данном примере это кадр 15. Это ответ веб-сервера Google на исходный запрос для начала сеанса.

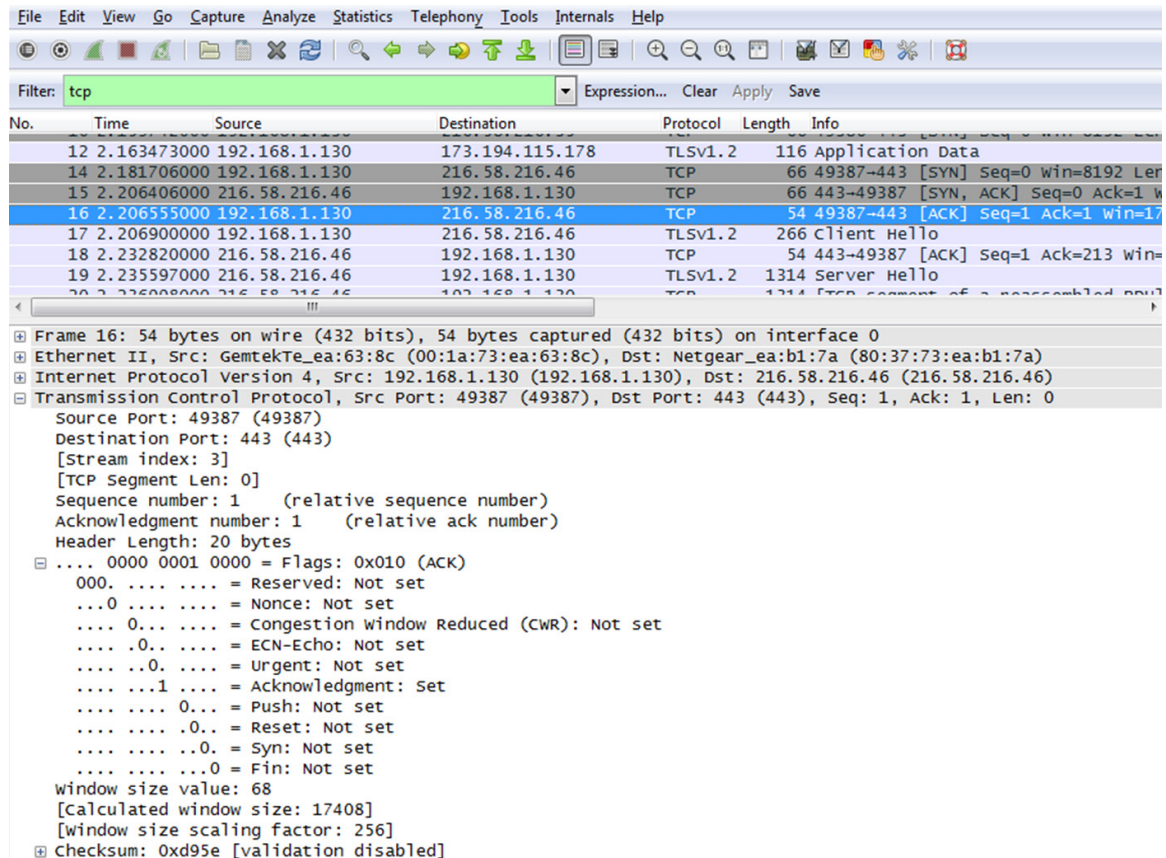


Назовите значения портов источника и назначения. _____

Какие установлены флаги? _____

Какие значения заданы для относительного порядкового номера и относительного номера подтверждения? _____

- e. И наконец, изучите третий пакет трехстороннего квитирования в данном примере. Нажав на кадр 16 в верхнем окне, вы увидите следующую информацию в данном примере:



Изучите третий и последний пакет квитирования.

Какие установлены флаги?

Для относительного последовательного номера и относительного номера подтверждения в качестве исходного значения выбрано значение 1. TCP-соединение установлено, и теперь может быть начата передача данных между ПК-источником и веб-сервером.

f. Закройте программу Wireshark.

Вопросы для повторения

- В программе Wireshark предусмотрены сотни фильтров. В большой сети может существовать множество фильтров и различных типов трафика. Укажите три фильтра, которые могут быть полезны для сетевого администратора.
- Как еще можно использовать программу Wireshark в сети предприятия?