

Лабораторна робота 3

Аналіз захоплених пакетів TCP за допомогою програми Wireshark

Завдання 1

За допомогою програми Wireshark необхідно виконати захоплення даних сеансу FTP і визначити значення полів заголовків протоколу TCP при передачі файлів з використанням протоколу FTP між хост-комп'ютером і анонімним FTP- сервером. Під'єднання до анонімного FTP-серверу і завантаження файлу виконується за допомогою браузера.

1. Активізувати режим захоплення даних з використанням програми Wireshark.
2. Завантажити файл довідки README.TXT.
 - 2.1. Під'єднатися до FTP-сервера центру FreeBSD: <ftp://ftp3.ie.freebsd.org>.
 - 2.2. В розділі pub/FreeBSD знайти і завантажити файл README.TXT (рисунок 2.9).
 - 2.3. Після завершення завантаження файлу зупинити захоплення даних програмою Wireshark.


Содержание /		
Имя	Размер	Дата изменения
 favicon.ico	5.3 kB	21.04.2020, 03:00:00
 index.html	668 B	21.04.2020, 03:00:00
 pub/		21.04.2020, 03:00:00
Имя	Размер	Дата изменения
 FreeBSD/		28.10.2020, 13:45:00
Имя	Размер	Дата изменения
 README.TXT	4.2 kB	07.05.2015, 03:00:00
 TIMESTAMP	35 B	28.10.2020, 13:45:00
 development/		28.10.2020, 13:45:00
 dir.sizes	2.6 kB	28.10.2020, 12:00:00
 doc/		12.11.2017, 02:00:00
 ports/		12.11.2017, 02:00:00
 releases/		28.10.2020, 13:45:00
 snapshots/		09.11.2018, 02:00:00

Рисунок 2.9 - Скріншот екрану

3. Відкрити головне вікно програми Wireshark.

Під час сеансу FTP-підключення до сайту **ftp3.ie.freebsd.org** захоплюється достатньо велика кількість блоків даних. Для того, щоб обмежити кількість цих даних для подальшого аналізу, необхідно застосувати фільтр відображення `tcp and ip.addr == 139.178.72.202` в полі Filter і натиснути клавішу Enter (рис. 2.10). Введена IP-адреса 139.178.72.202 є адресою сайту **ftp3.ie.freebsd.org**.

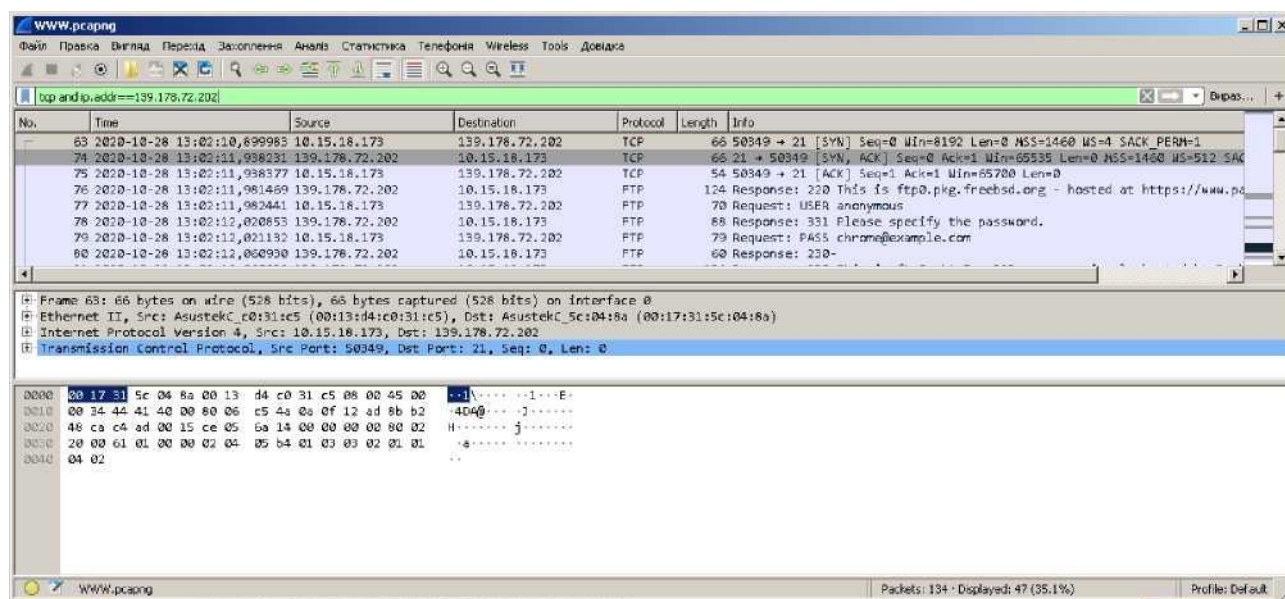


Рисунок 2.10 - Приклад захоплення блоків даних

4. Проаналізувати поля заголовків сегментів TCP.

Після застосування фільтру TCP в перших трьох блоках, показаних у верхньому розділі панелі, відображено створення надійного сеансу зв'язку протоколом транспортного рівня TCP.

Послідовність [SYN], [SYN, ACK] і [ACK] ілюструє тристороннє квотування (рисунок 2.11).

No.	Time	Source	Destination	Protocol	Length	Info
63	2020-10-28 13:02:10,899983	10.15.18.173	139.178.72.202	TCP	66	50349 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
74	2020-10-28 13:02:11,998231	139.178.72.202	10.15.18.173	TCP	66	21 → 50349 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=512 SACK_PERM=1
75	2020-10-28 13:02:11,998377	10.15.18.173	139.178.72.202	TCP	54	50349 → 21 [ACK] Seq=1 Ack=1 Win=65700 Len=0

Рисунок 2.11 - Встановлення з'єднання (триразове рукошлякування)

Протокол TCP, як правило, використовується під час сеансу зв'язку для управління доставкою IP-дейтаграм, перевірки їх отримання і керування розміром вікна. Для кожного обміну даними між FTP-клієнтом і FTP-сервером запускається новий сеанс TCP. Після завершення передачі даних сеанс TCP закривається. Після завершення сеансу FTP протокол TCP виконує планове відключення і припиняє роботу.

Програма Wireshark відображає докладні дані TCP-пакетів на панелі відомостей про пакети (середній розділ). Виділити перший фрагмент TCP і розгорнути його. Відкриється розгорнутий фрагмент TCP, аналогічний представленому на рисунку 2.12.

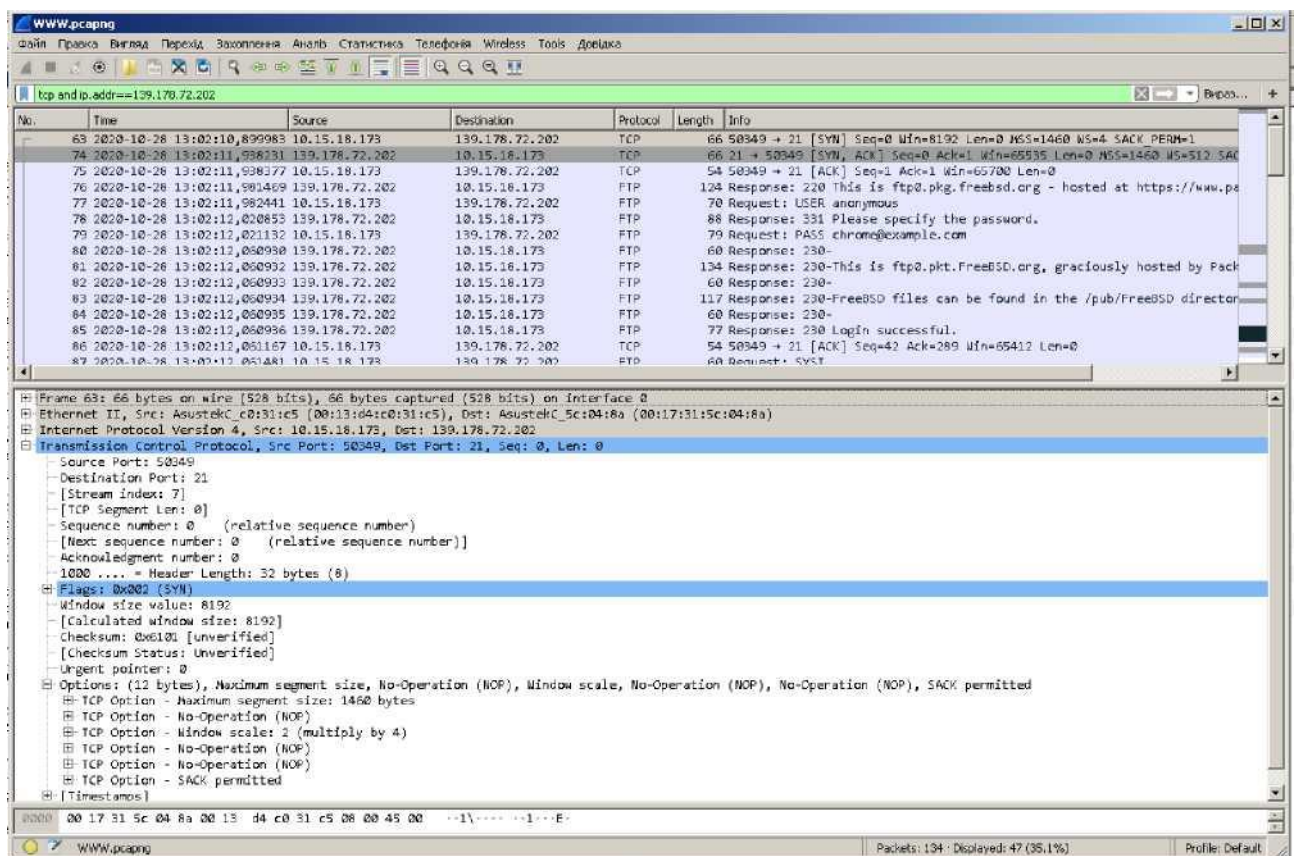


Рисунок 2.12 - Приклад розгорнутого фрагменту TCP
До кожного поля надаються пояснення.

- Поле TCP Source Port Number (номер порту джерела) призначене для хост- вузла, який відкрив з'єднання.
- Поле TCP Destination Port Number (номер порту призначення) використовується для ідентифікації протоколу верхнього рівня або додатку на віддаленому сайті. Значення в діапазоні від 0 до 1023 зв'язані з популярними сервісами і застосуваннями, наприклад Telnet, FTP і HTTP. Комбінація IP-адреси джерела, порту джерела, IP-адреси призначення і порту призначення однозначно визначають сеанс як для відправника, так і для отримувача. В наведених прикладах вказано порт призначення 21, який використовується для FTP. FTP-сервери прослуховують порт 21 для підключення FTP-клієнтів.
- В полі Sequence Number (порядковий номер) вказується номер першого октету в сегменті.
- В полі Acknowledgment Number (номер підтвердження) вказується наступний октет, який очікується отримувачем.
- Значення в полі Flags виконують особливу роль в управлінні сеансами і опрацюванні сегментів. Найчастіше використовуються наступні:
 - ACK — підтвердження отримання сегменту.
 - SYN — синхронізація, встановлюється тільки в першому TCP-сегменті в процесі тристороннього квотування.
 - FIN — завершення, запит про припинення сеансу TCP.
- Window size (розмір вікна) — це значення віна зміщення, яке визначає число октетів, які можуть бути передані до надходження підтвердження.
- Поле Urgent pointer (вказівник важливості) використовується тільки з встановленим прапорцем важливості Urgent (URG), коли користувачу необхідно передати важливі дані отримувачу, на які потрібно звернути особливу увагу.
- Поле Options (параметри) - поле змінної довжини; може бути відсутнім або містити одну опцію або список опцій, які реалізують додаткові послуги протоколу TCP. В лабораторній роботі треба звернути особливу увагу на опцію максимального розміру TCP-сегменту MSS.

Після встановлення сеансу TCP з'являється можливість для передачі FTP-трафіка між робочою станцією та FTP-сервером. FTP-клієнт і сервер взаємодіють один з одним, не помічаючи, що при цьому TCP займається управлінням сеансом.

Після завершення сеансу FTP клієнт FTP відправляє команду quit (завершити). FTP-сервер підтверджує припинення сеансу FTP, відправляючи Response: 221 Goodbye. У відповідь на це сеанс TCP FTP-сервера відправляє сегмент TCP FTP-клієнту, повідомляючи про припинення сеансу TCP.

Сеанс TCP FTP-клієнта підтверджує отримання сегмента припинення сеансу, після чого відправляє власне повідомлення про припинення сеансу TCP. FTP-сервер, який ініціював припинення сеансу TCP, відправляє сегмент з встановленим бітом ACK з підтвердженням припинення, і сеанс TCP завершується. Послідовність цих дій представлена на рисунку 2.13.

Коли FTP-сервер передав всі дані, відправляється сегмент з встановленим прапорцем FIN. Робоча станція у відповідь відправляє ACK, щоб підтвердити отримання FIN. Станція відправляє сегмент з встановленим бітом FIN FTP- серверу для завершення сеансу TCP. FTP-сервер відправляє відповідь, яка містить встановлений біт ACK для підтвердження отримання FIN від робочої станції. Після цього сеанс TCP між FTP-сервером і робочою станцією завершується.

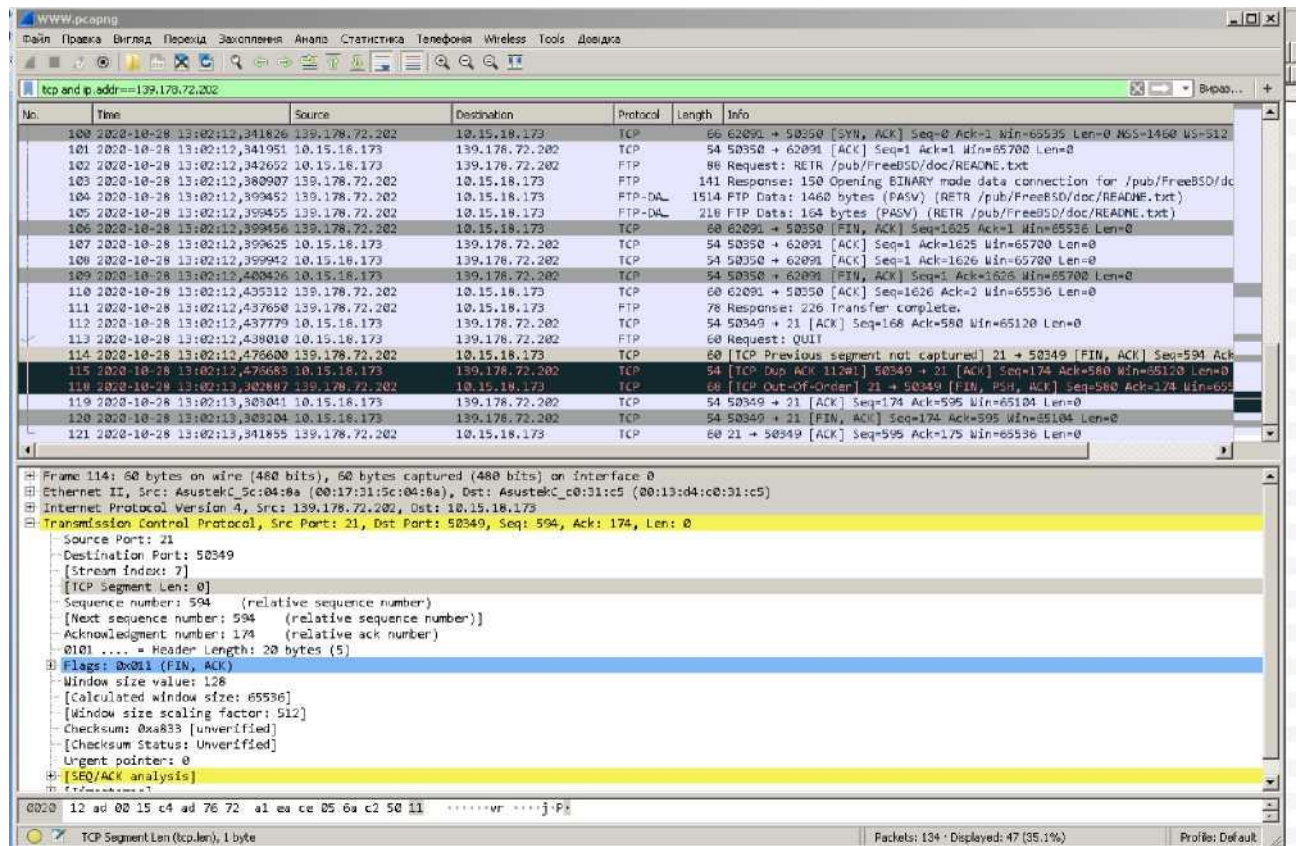


Рисунок 2.13 - Приклад сеансу TCP

Завдання

1. Ознайомитись з можливостями фільтрації даних за різними ознаками, зокрема, за MAC-адресою відправника і отримувача. Фільтр створюється за описаною вище методикою. Відповідно до рекомендацій викладача сформувати фільтр за MAC-адресою.
2. Розглянути результат інкапсуляції при передачі даних. В захоплених пакетах виділити службову інформацію (заголовки) всіх блоків даних, а також, за наявністю, кінцевика.
3. Використовуючи фільтр відображення **tcp.flags.syn == 1** відібрати сегменти-запити, які містять встановлений прапорець **SYN** у заголовку та сегменти-відповіді, які містять встановлені прапорці **SYN** та **ACK**. Провести аналіз поля

Options заголовку TCP. Яке значення MSS використовується в з'єднанні, що аналізується?

4. За допомогою меню «Statistics» необхідно отримати і додати до звіту таку

інформацію:

- кількість захоплених пакетів та байтів;
- середня швидкість передачі даних (в бітах за секунду);
- середній розмір пакета;
- час, протягом якого здійснювалось захоплення трафіку;
- вивести таблицю Ethernet Conversations та пояснити вміст її рядків;
- вивести IO Grafts, за допомогою якого визначити пікову швидкість передачі даних протягом інтервалу, що підлягає аналізу.

5. За результатами роботи зробити висновки.

Контрольні запитання

1. Поясніть процедуру створення TCP-сегментів і UDP-дейтаграм на транспортному рівні стеку протоколів TCP/IP?
2. Яка довжина заголовків протоколів транспортного рівня UDP і TCP?
3. Поясніть назви та призначення полів у заголовках протоколів транспортного рівня?
4. Як вираховується контрольна сума TCP-сегменту та UDP-дейтаграми?
5. Які поля входять до складу псевдозаголовку?
6. Як відбувається встановлення і розірвання TCP-з'єднання?
7. Яка довжина заголовку протоколу мережевого рівня (IP-заголовку)?
8. Які поля містить IP-заголовок та їх призначення?
9. Які види фільтрів підтримує аналізатор трафіку Wireshark?

