МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

**Звіт**

Про виконання лабораторної роботи №8

**«Транспортні протоколи – TCP та UDP»**

Виконав:

Студент групи ФЕП-11

Коберський Данило

Перевірив:

Продивус А.М.

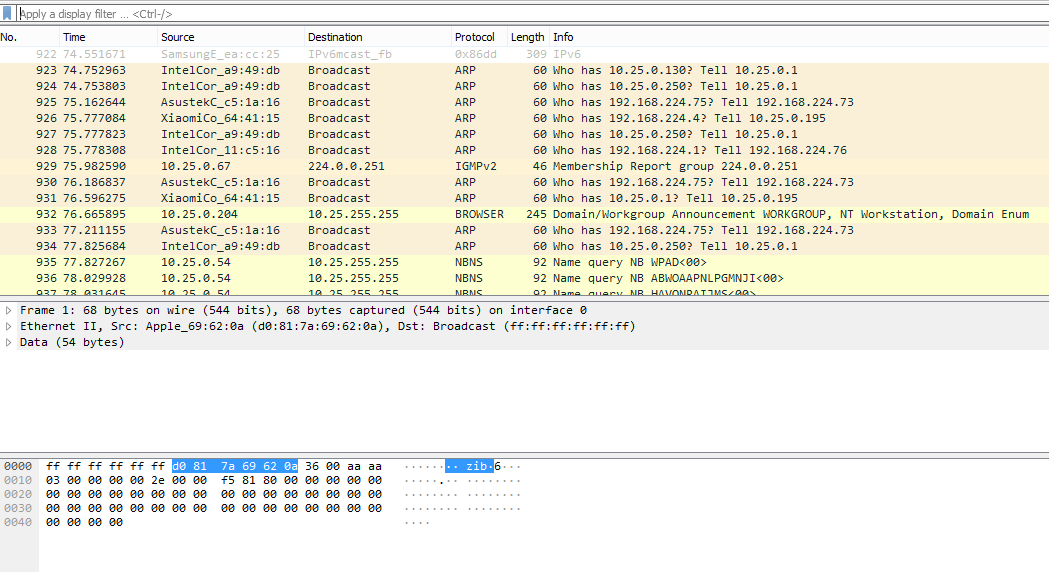
Львів 2019

**Мета:** Вивчити роботу протоколу TCP, зокрема, механізм з’єднання та структуру заголовку. Вивчити протокол UDP.

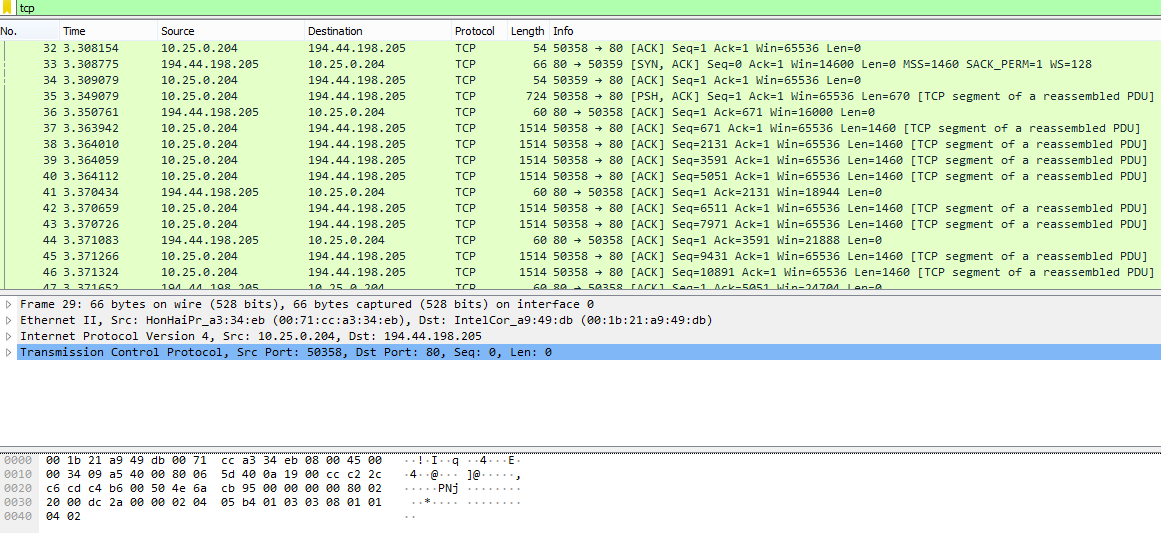
**Хід роботи:**

**Дослідження протоколу TCP**

1. Перехоплення TCP пакетів, переданих від вашого комп’ютера на віддалений сервер
2. Запустив web браузер. Зайшов на <http://elct.lnu.edu.ua/kin/alice.txt> та завантажив файл «Alice in Wonderland» у ASCII кодуванні на мій комп’ютер.
3. Зайшов на <http://elct.lnu.edu.ua/kin/submit.html>
4. В полі вводу вказав повний шлях до щойно завантаженого локального файлу, але ще не натискав кнопку “Upload alice.txt file”.
5. Тепер, запустив Wireshark та розпочав перехоплення пакетів (Capture->Options), та натиснув кнопку OK у вікні налаштувань Wireshark Packet Capture
6. Повернувся до браузера та натиснула кнопку “Upload alice.txt file” для завантаження файлу на сервер gaia.cs.umass.edu. Як тільки файл завантажився, невеличке привітальне повідомлення відобразилось у моєму браузері.
7. Зупинив перехоплення пакетів. Вікно Wireshark виглядало так:



1. Спершу, відфільтрувала пакети, що відображаються у вікні Wireshark, набравши **“tcp”** у полі фільтру, що знаходиться на верхній панелі.



**Відповіді на запитання**

1. Яка IP адреса та номер TCP порту використовується вашим комп’ютером (джерелом) для відправки файлу на elct.lnu.edu.ua?

Моїм комп’ютером використовується **IP адреса: 10.25.0.204**

Номер **TCP** порту мого комп’ютера: **50382**

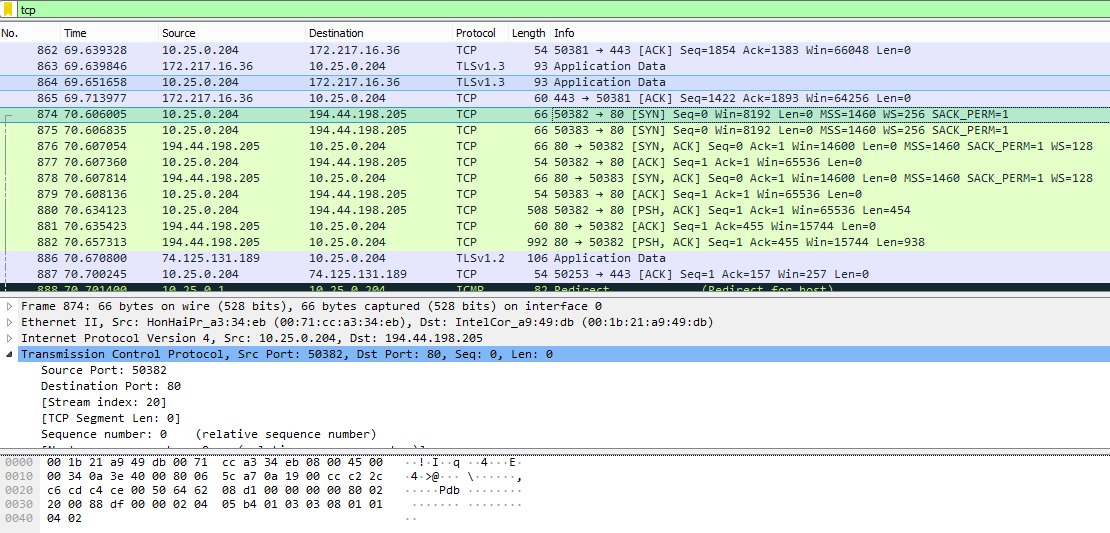


1. Яка IP адреса у elct.lnu.edu.ua? Який номер порту використовується для прийому/відправлення TCP пакетів?

IP адреса у elct.lnu.edu.ua?: **194.44.198.205** Номер порту що використовується: 80



Змінимо список відображених пакетів у **Wireshark** так, щоб він показував TCP сегменти, що використовуються для передачі HTTP повідомлень. Вибираємо пункт меню **Analyze->Enabled Protocols**, та знімаємо галочку з **HTTP**, отримуємо:



1. Який порядковий номер (sequence number) TCP SYN пакета, який використовується для ініціювання TCP з'єднання між комп'ютером клієнта і elct.lnu.edu.ua? Що в цьому TCP пакеті вказує, що він є SYN пакетом?

Порядковий номер(Sequence number) 0. На те, що це SYN пакет вказує встановлений в одиницю спеціальний прапорець SYN set:

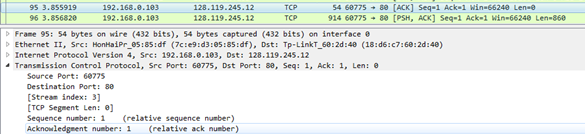
Untitled

1. Який порядковий номер SYN ACK пакета, відісланого elct.lnu.edu.ua? клієнту у відповідь на його SYN пакет? Яке значення поля «ACKnowledgement» у SYN ACK пакеті? Звідки сервер gaia.cs.umass.edu взяв це значення? Що в TCP пакеті вказує, що він є SYN ACK пакетом?

Порядковий номер SYN ACK пакета 0. Проте acknowlegment number – 1. Це значення сервер взяв наступним чином: при отриманні SYN пакета він бере його номер послідовності(0) та додає до нього 1, після чого поміщує отримане значення в acknowlegment number. На те, що це SYN ACK пакет вказують відповідні прапорці встановлені в 1:

Untitled

1. Який порядковий номер TCP сегмента, що містить HTTP POST команду? Для знаходження команди POST вам потрібно детальніше глянути на вміст пакету у вікні детального перегляду та знайти у полі даних фрагмент з командою “POST”.



Порядковий номер такого пакета 1:

1. Розгляньте перший TCP пакет, що містить команду HTTP POST. Які порядкові номери перших шести TCP пакетів, що використовувалися для передачі фалу (починаючи з пакету, що містить HTTP POST команду)? Який час відправлення кожного такого пакету? Коли приходив пакет-підтвердження (ACK) для кожного відправленого пакету? Підрахувавши різницю між часом відправки TCP сегмента та часом отримання пакету підтвердження про доставку, вкажіть RTT час (Round-Trip Time – час обороту повідомлення) для кожного з шести сегментів.

Порядкові номери:

1(час відправлення: 3.777697; час прибуття підтв.: 3.778209) RTT = 0,000512, 1461(час відправлення: 3.777723; час прибуття підтв.: 3.886114) RTT = 0,108391, 2921(час відправлення: 3.777747; час прибуття підтв.: 3.886118) RTT = 0,108371, 4381(час відправлення: 3.778330; час прибуття підтв.: 3.886119) RTT = 0,107789, 5841(час відправлення: 3.777801; час прибуття підтв.: 3.886120) RTT = 0,108319, 7301(час відправлення: 3.777824; час прибуття підтв.: 3.886715) RTT = 0,108891.

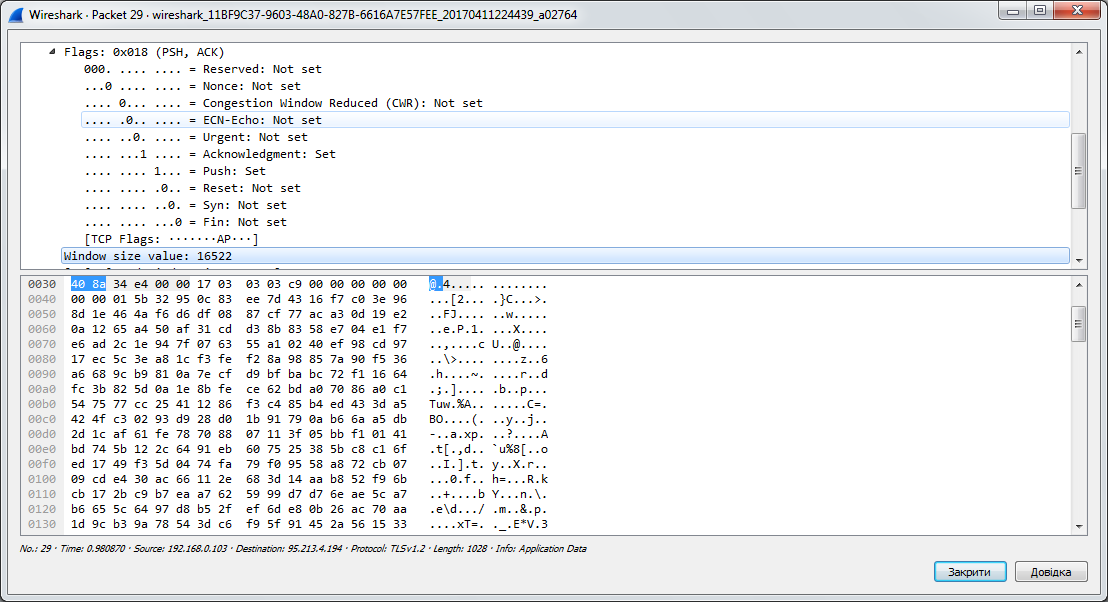
1. Яка довжина кожного з шести TCP сегментів?

Перших п’яти — 1460 байт. Шостого — 892 байти.

1. Який мінімальний розмір буферу був у сервера під час передавання файлу? Чи призупинялася передача даних через недостачу буферу на сервері?

**Window size value: 16522**

Передача даних не призупинялася, оскільки прапорці Nonce і CWR не встановлені:

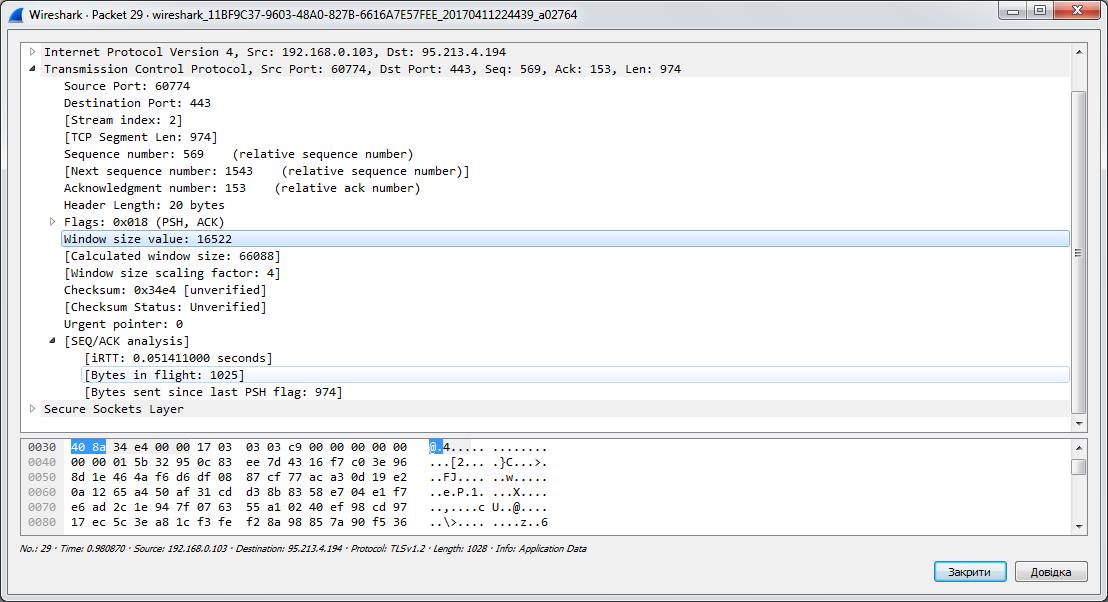


1. Чи були повторені якісь TCP сегменти? Що ви перевіряли (в перехоплених пакетах) для відповіді на це запитання?

Ні, повторених сегментів не було. Зробив перевірку чи не зустрічалися 2 однакові пакети з однаковим порядковим номером.

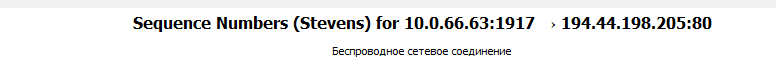
1. Яка пропускна спроможність (кількість передавання байтів за одиницю часу) для TCP з’єднання? Поясніть, як ви підрахували цю величину.

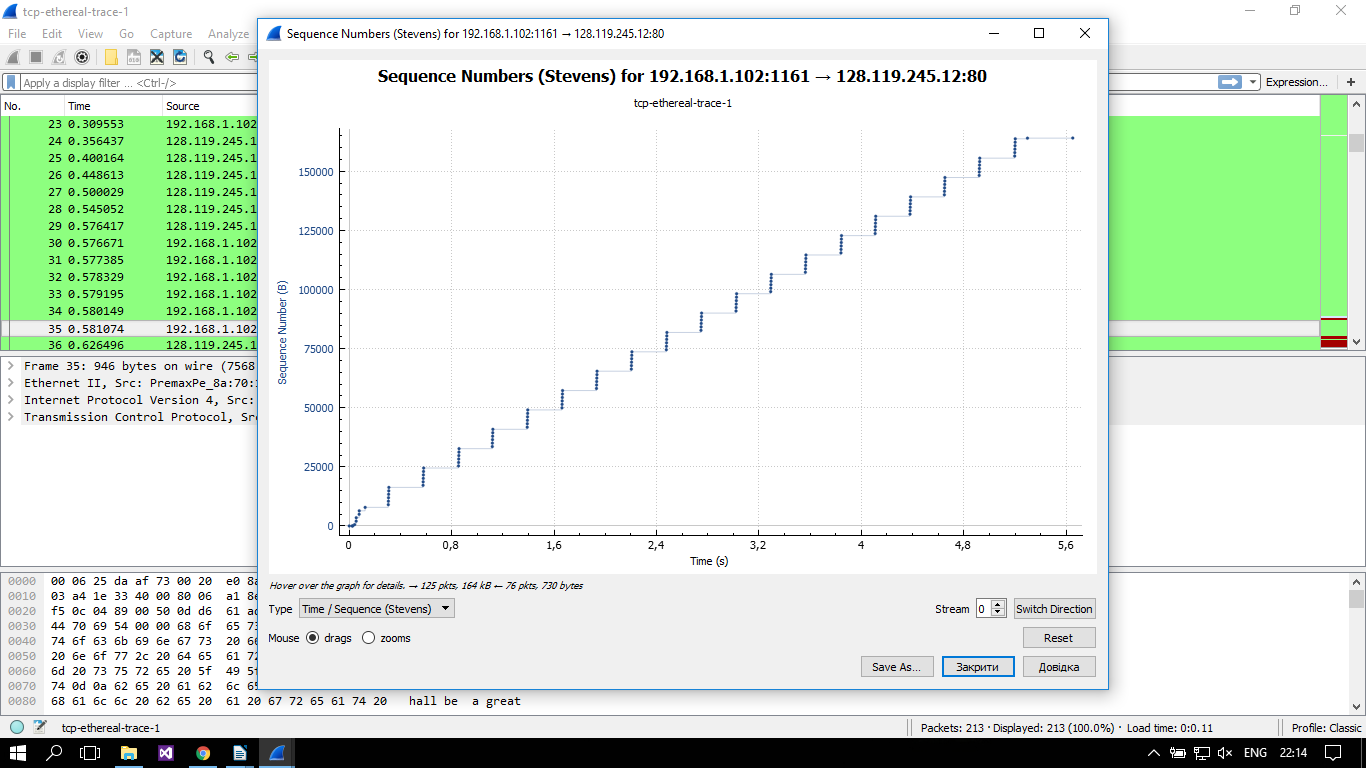
Пропускна спроможність становить 1025 байт за 0.051411000 секунди. Взято з SYN ACK сегмента, а саме з поля максимального розміру сегмента та часу передачі сегмента:



**Керування перевантаженням TCP**

**8.** Виберіть пункт меню : Statistics->TCP Stream Graph-> Time-Sequence-> Graph(Stevens). Ви маєте побачити графік, схожий на приведений на рис. (який був створений через збережений файл перехоплених пакетів tcp-ethereal-trace-1, що знаходиться за адресою: <http://gaia.cs.umass.edu/wireshark-labs/wireshark-trac>.

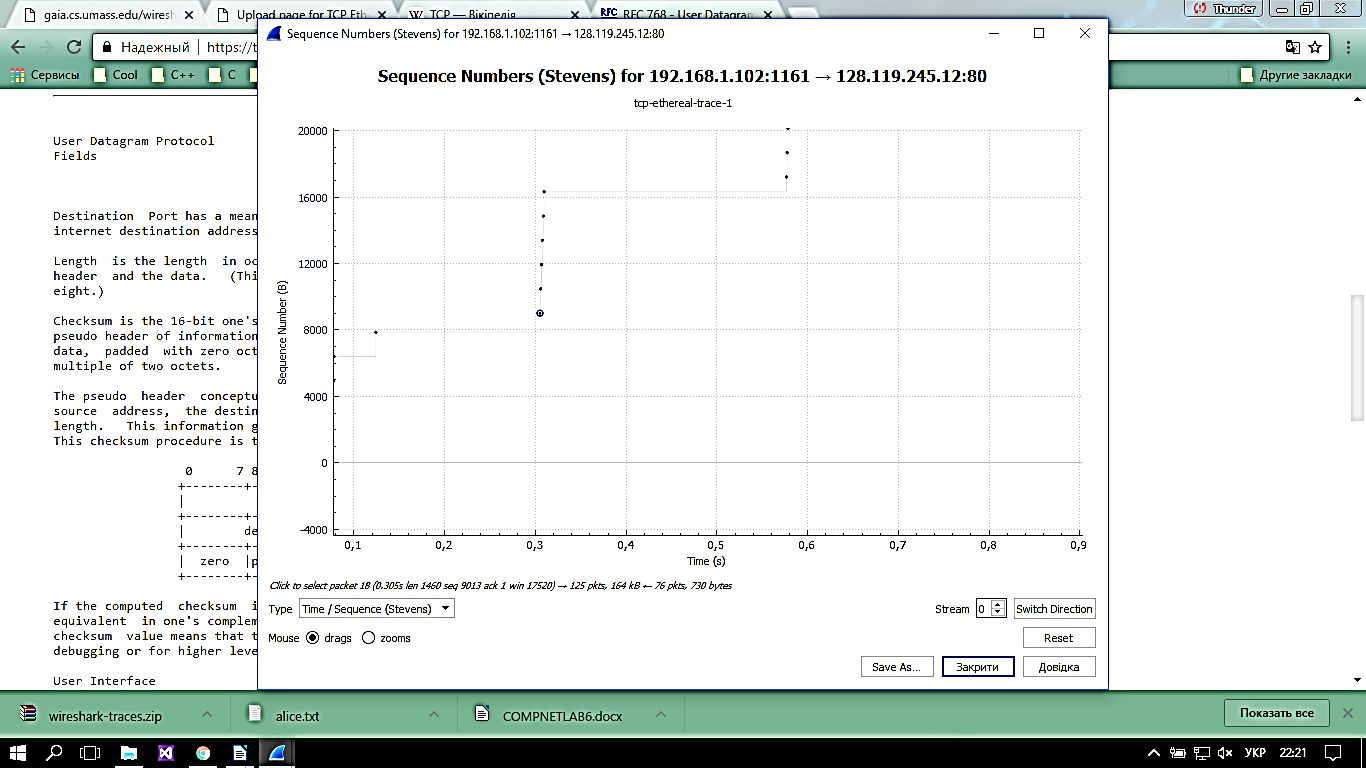




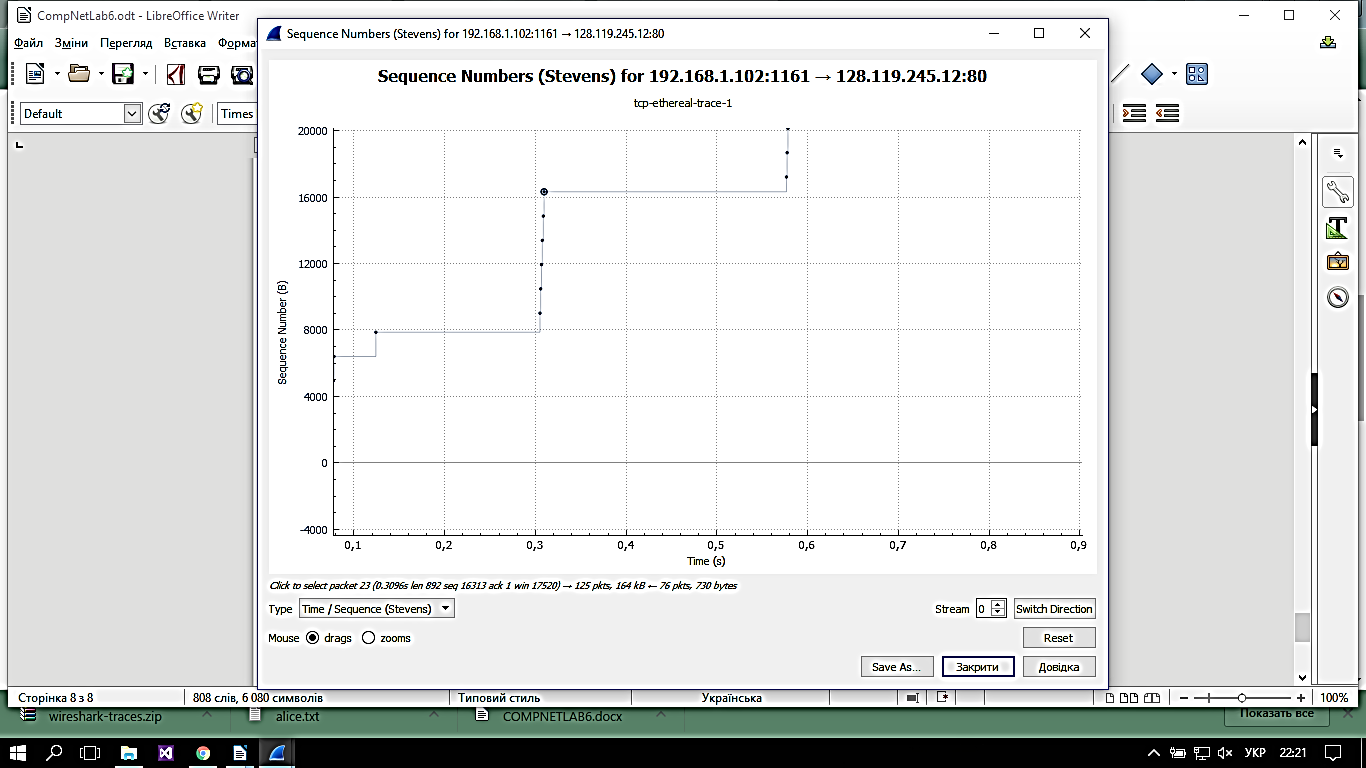
**9.** Вказати, де починаються фази передавання TCP пакетів та де вони

закінчуються і де працює механізм уникнення TCP заторів?

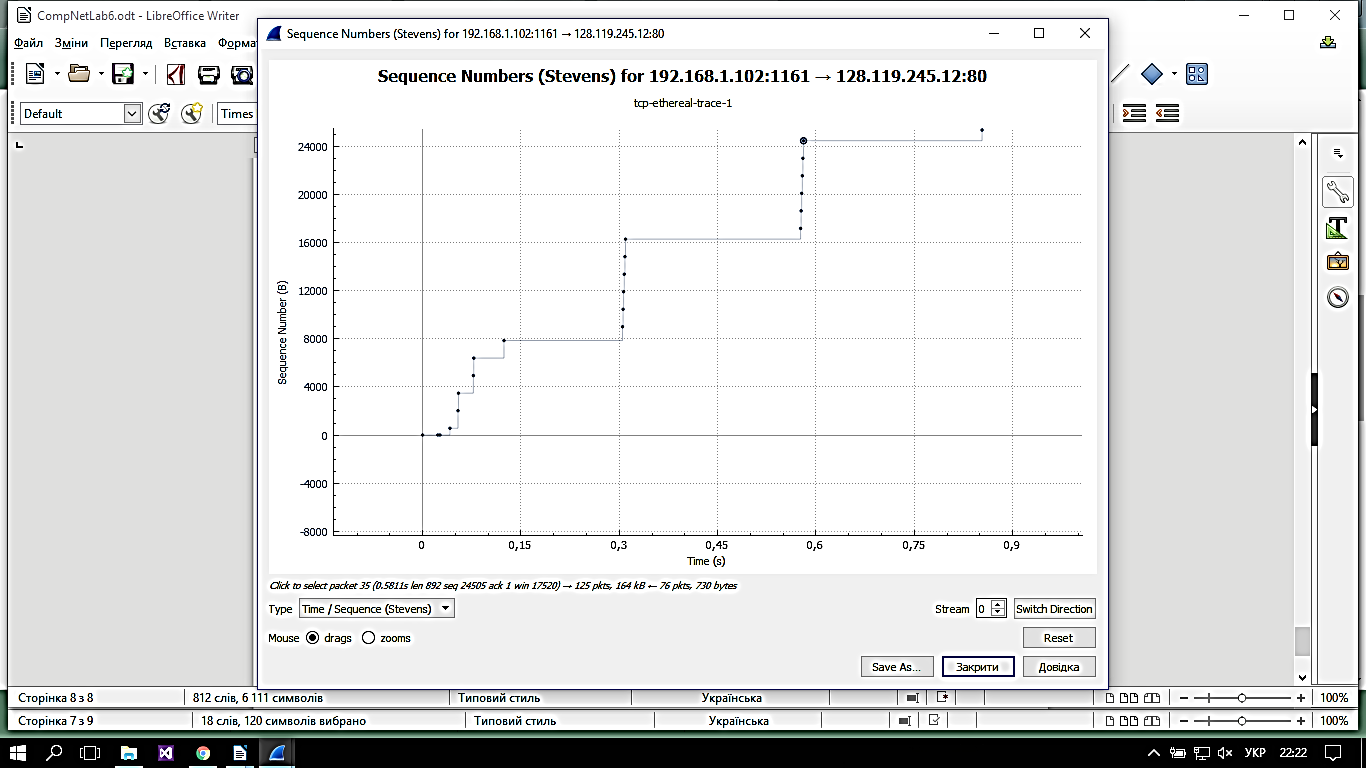
Починаються:



Закінчуються:

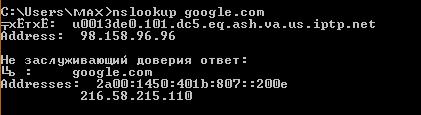


Механізм уникнення TCP заторів — це часовий проміжок між фазами:

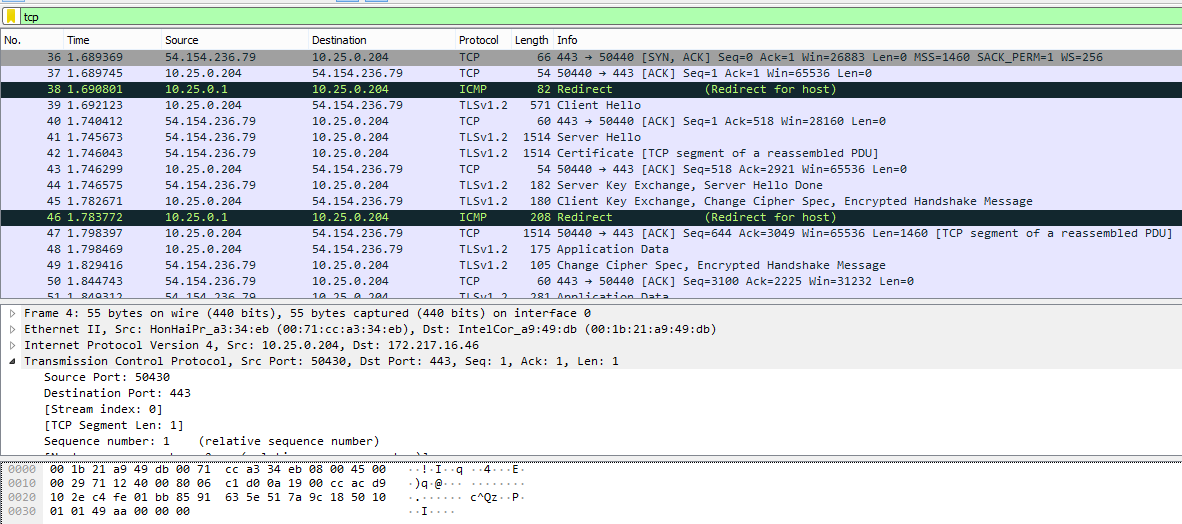


**Дослідження протоколу UDP**

Розпочніть перехоплення пакетів за допомогою Wireshark, а потім зробіть що-небудь для того, щоб ваш хост почав приймати та передавати UDP пакети (один з можливих варіантів – це скористатися командою nslookup, яка розглядалася в лабораторній роботі по DNS). Після зупинки перехоплення пакетів налаштуйте фільтр відображення пакетів так, щоб Wireshark відображав лише UDP пакети. Виберіть один з UDP пакетів, та розгорніть його дані у вікні детального перегляду.



Запускаємо перехоплення пакетів. Використовую команду nslookup google.com для відправки UDP запитів, після чого зупиняємо перехоплення



1. Виберіть один пакет. Визначте, скільки полів міститься в заголовку обраного UDP пакета. Перерахуйте ці поля.

В заголовку міститься 4 поля: Source port, destination port, length, checksum.

1. Визначте довжину кожного поля в UDP заголовку .

Довжина кожного поля становить 2 байти:

Untitled

1. Значення в полі Length (розмір) - це розмір чого? Покажіть це на прикладі перехопленого вами UDP пакету.

Це розмір дейтаграми (заголовка та даних). Оскільки заголовок має довжину 8 байт а дані 38 байт, то довжина дейтаграми має складати 46 байт, що можна побачити на прикладі:



1. Яку максимальну кількість байтів може переносити UDP пакет?

65507 байт (65535 - 20(на IP заголовок) - 8(на UDP заголовок) = 65507).

1. Який максимальний номер порту джерела повідомлення?

Від 0 до 65535.

1. Який номер протоколу відповідає UDP? Дайте відповідь у десятковому та шістнадцятирічному представленнях (для відповіді вам знадобиться заглянути в заголовки IP протоколу).

У десятковому — 17

У шістнадцятирічному — 11

1. Пошукайте “UDP” в пошуковій системі Google, та скажіть по яким полям UDP рахує контрольну суму (checksum).

По полям, що знаходяться у заголовку.

1. Дослідіть пару UDP пакетів, з яких перший пакет був відправлений вашим комп’ютером, а другий – відповідь на нього. Опишіть взаємозв’язок між номерами портів в цих двох пакетів.

Untitled

Номер порту отримувача у пакеті — запиті збігається з номером порту джерела у пакеті — відповіді. Номер порту мого комп’ютера у пакеті — запиті збігається з номером порту отримувача у пакеті — відповіді.

1. Перехопіть маленький UDP пакет. Вручну підрахуйте контрольну суму пакету. Покажіть всю послідовність дій та прокоментуйте кожен крок.

Untitled

Розділяємо цю послідовність на 4 16-бітних слова і додаємо їх: 0035 + е6сс + 0057 + 9575 = 17ссd. Тепер виконуємо інверсію всіх бітів отриманого слова: ffff – 17ccd = 0x8332.

**Висновок:**

На цій лабораторної роботи, я вивчив роботу з протоколами TCP та UDP, а також отримування та аналіз інформацій за допомогою програми Wireshark. Також виконано додаткове завдання: розрахунок контрольної суми UPD пакета.