МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС

«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»

НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО» КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

# Практична робота №5

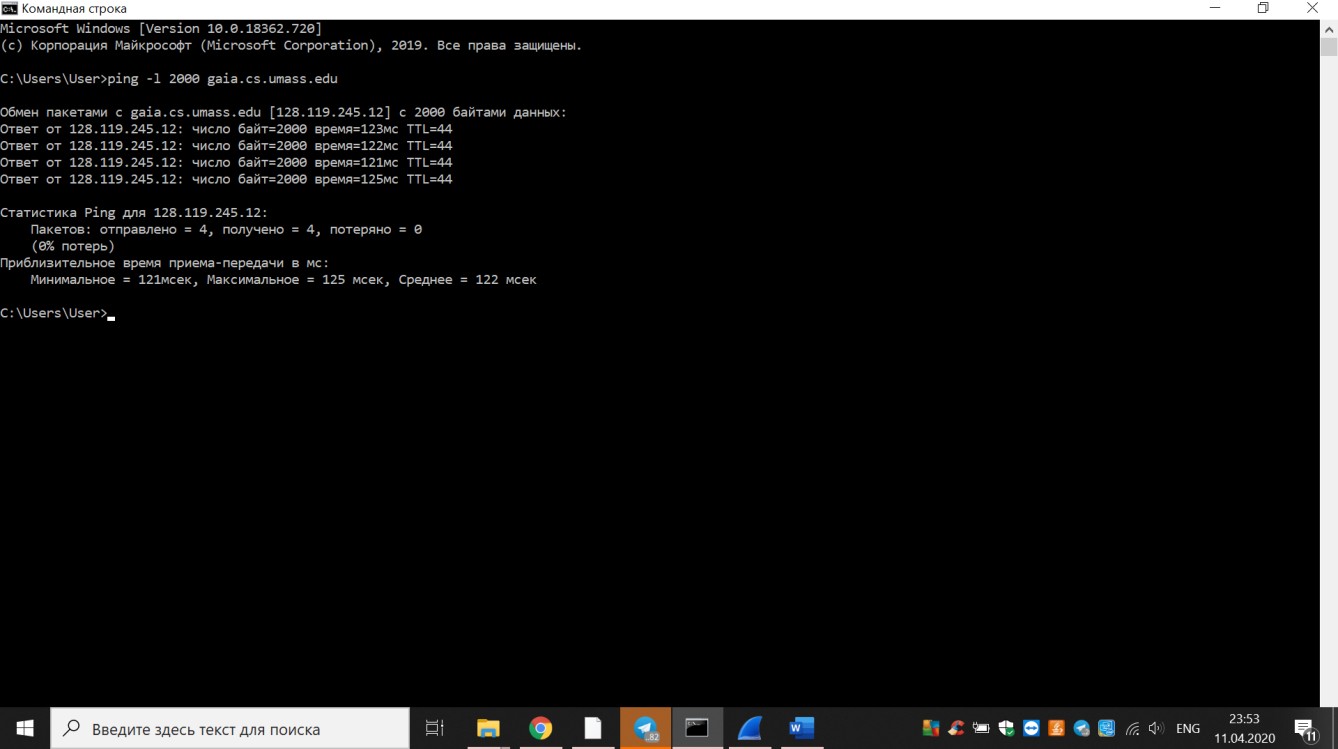
**з курсу «Комп'ютерні мережі»**

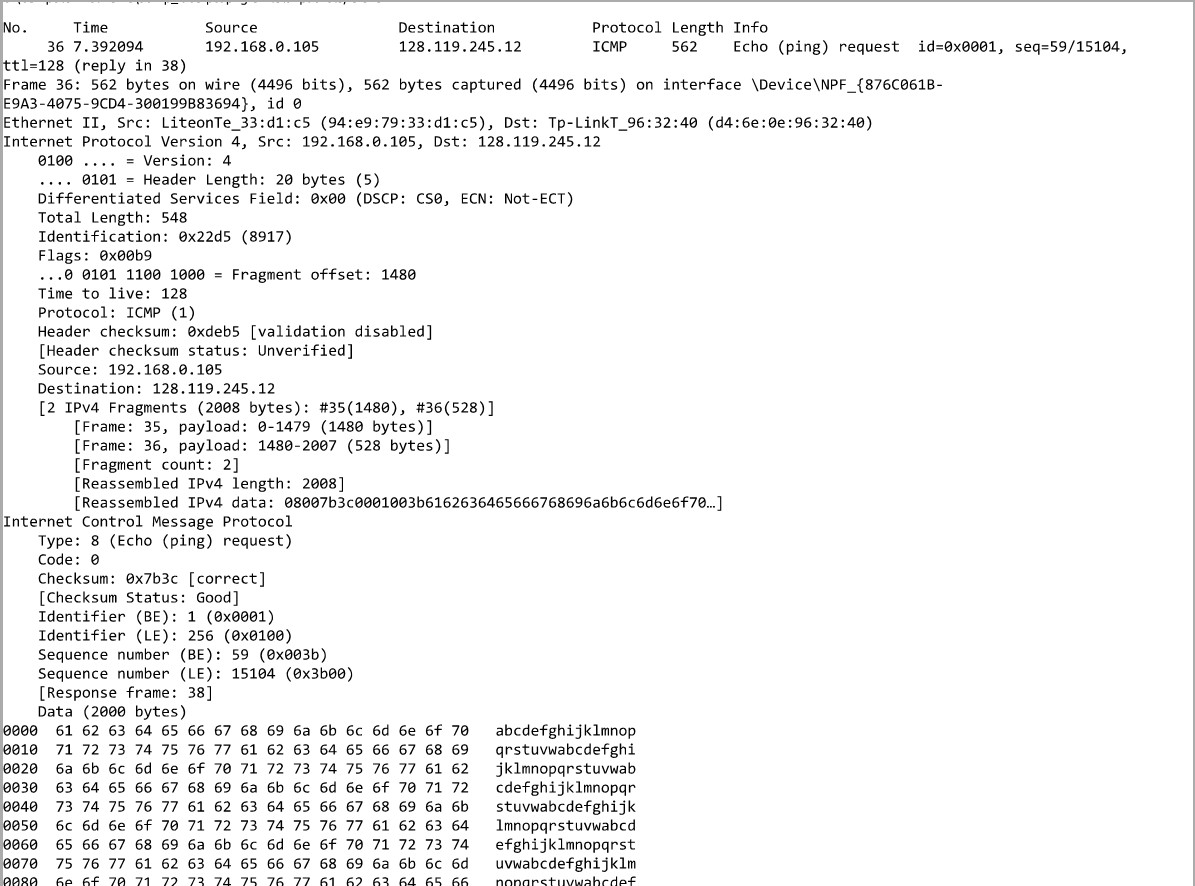
## Виконала студентка 3 курсу

**групи КА-72 Господінова Валерія**

**Прийняв: Кухарєв С.О.**

**Київ – 2020 р.**







Контрольні запитання:

1. **Визначте IP адреси вашої та цільової робочих станцій.**

Моя - 192.168.0.105, цільова - 128.119.245.12.

1. **Яке значення в полі номера протоколу вищого рівня в заголовку IP першого пакету із запитом ICMP?**

Protocol: ICMP (1)

1. **Скільки байт займає заголовок IP першого пакету із запитом ICMP? Скільки байт займає корисна інформація (payload) пакету? Поясніть як ви встановили кількість байт корисної інформації.**

Header Length: 20 bytes 2008 байт = 1480 + 528

[2 IPv4 Fragments (2008 bytes): #35(1480), #36(528)]

[Frame: 35, payload: 0-1479 (1480 bytes)]

[Frame: 36, payload: 1480-2007 (528 bytes)]

[Fragment count: 2] [Reassembled IPv4 length: 2008]

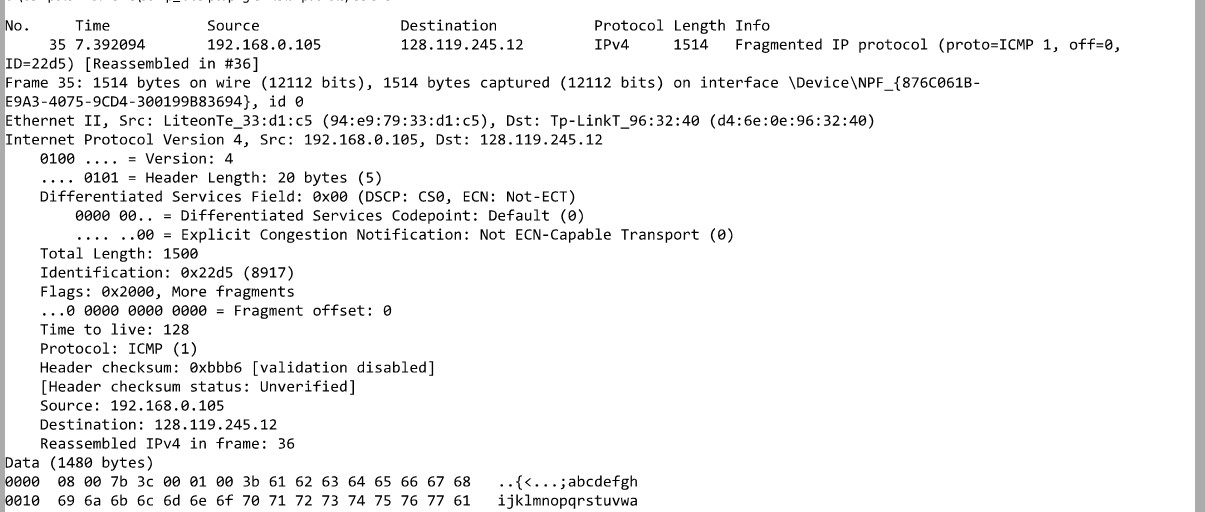
[Reassembled IPv4 data: 08007b3c0001003b6162636465666768696a6b6c6d6e6f70…]

1. **Дослідіть пакет із пунктів 2/3. Чи фрагментований цей пакет? Поясніть як ви встановили фрагментацію пакету. Як можна встановити номер фрагменту, що передається у пакеті?**

Так, фрагментований. По номеру фрейма.

[2 IPv4 Fragments (2008 bytes): #35(1480), #36(528)]

1. **Знайдіть наступний фрагмент датаграми IP. Яка інформація дозволяє встановити наявність наступних фрагментів, що мають слідувати за другим фрагментом?**



Reassembled IPv4 in frame: 36

Той самий фрагмент, що і в попередньому питанні.

1. **Які поля протоколу IP відрізняють перший фрагмент від другого?**

Тільки назва фрейму та Upper Layer Protocol

1. **Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Які поля заголовку IP завжди змінюються?**

Identification та Header checksum.

1. **Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Які поля заголовку IP мають зберігати свої значення? Які поля мають змінюватися? Чому?**

Поля, які зберігають свої значення:

* + Version (ми використовуємо IPv4 для всіх пакетів)
  + header length (всі пакети – ICMP)
  + source IP, destination IP (Ми пінгуємо одну і ту ж адресу)
  + Differentiated Services (всі ICMP пакети одного службового типу)
  + Time to live

Поля, які змінюють свої значення:

* + Upper Layer Protocol (всі загаловки ICMP мають унікальні поля, що змінюються)
  + Identification (IP пакети мають мати різні id)
  + Header checksum (оскільки заголовки змінюються, то контрольна сума

1. **Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Опишіть закономірність зміни значень поля Identification рівня IP.** Збільшується на 1. Наприклад:

0x000022d5 (8917)

0x000022d6 (8918)

1. **Розгляньте послідовність пакетів IP із повідомленнями TTL-exceeded від найближчого маршрутизатора. Які значення встановлені у полях Identification та TTL?**

Таких повідомлень не було, оскільки утиліта ping на Windows не змінює TTL для різних запитів.

1. **Розгляньте послідовність пакетів IP із повідомленнями TTL-exceeded від найближчого маршрутизатора. Які значення встановлені у полях Identification та TTL? Чи змінюються ці значення для різних пакетів у послідовності? Чому?**

Поле Identification має змінюватись для кожної ICMP TTL-exceeded відповіді. Якщо дві або більше IP датаграми мають однаковий Identification, то це означає, що вони є фрагментами однієї великої IP датаграми. Поле TTL завжди однакове, бо у найближчого маршрутизатора він завжди однаковий.

Висновки:

В ході виконання даної лабораторної роботи, були покращено навички використання програми Wireshark для захоплення пакетів. Було проаналізовано протоколи IP та було проведено аналіз деталей роботи даних протоколів.