**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**

# **«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**

# **ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**

**Інститут прикладного системного аналізу**

**Кафедра математичних методів системного аналізу**

**Дисципліна: “Комп’ютерні мережі”**

**Лабораторна робота № 1**

Тема роботи: “ Основи захоплення та аналізу пакетів”

|  |  |
| --- | --- |
|  | Виконала: студентка  3 курсу групи КА-77  Деменкова В.В. |
|  | Прийняв: к.т.н. Кухарєв С.О. |

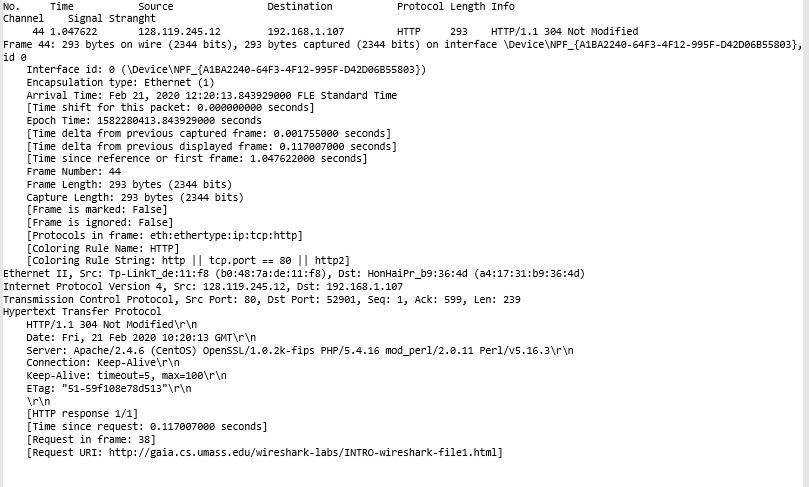
**Київ – 2020**

**Лабораторна робота № 1.**  Основи захоплення та аналізу пакетів

**Мета роботи:** Оволодіти методами роботи в середовищі захоплення та аналізу пакетів Wireshark, необхідними для дослідження мережевих протоколів.

**Отримані результати:**

****

****

**Контрольні питання:**

*1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?*

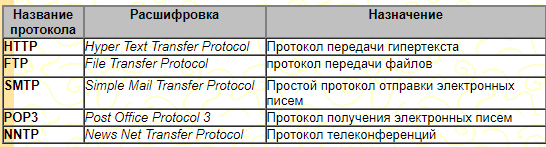
**TCP** (Transmission Control Protocol) - протокол управління передачею. Він визначає, яким чином інформація повинна бути розбита на пакети і відправлена по каналах зв'язку. TCP має пакети в потрібному порядку, а також перевіряє кожен пакет на наявність помилок при передачі.

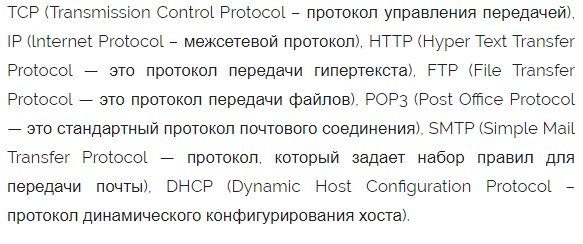
**UDP** (user datagram protocol) - відомий протокол, чимось схожий з TCP, який також функціонує на транспортному рівні. Основна відмінність - ненадійна передача даних: дані не проходять перевірку при отриманні. У деяких випадках цього цілком достатньо. За рахунок відправки меншої кількості пакетів, UDP працює спритніше ніж TCP. Немає необхідності встановлювати з'єднання і протокол використовується для відправки пакетів відразу на кілька пристроїв або IP телефонії.

Протокол додатки **HTTP** (hypertext transfer protocol) лежить в основі роботи всіх сайтів в Мережі. HTTP дає можливість запитувати необхідні ресурси у віддаленій системи, наприклад, веб сторінки і файли.

**SSDP** (Simple Service Discovery Protocol) - мережевий протокол, заснований на наборі протоколів Інтернету, службовець для оголошення і виявлення мережевих сервісів. SSDP дозволяє виявляти сервіси, не вимагаючи спеціальних механізмів статичної конфігурації або дій з боку серверів, таких як DHCP або DNS.

**ICMP** (Internet control message protocol) призначений для того, щоб пристрої могли обмінюватися повідомленнями. Це наприклад можуть бути повідомлення про помилки або інформаційні оповіщення. Дані цей протоколу не передає інформацію. Цей протокол знаходиться рівнем вище ніж протокол IP.





*2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?*

Протокол додатки HTTP (hypertext transfer protocol) лежить в основі роботи всіх сайтів в Мережі. HTTP дає можливість запитувати необхідні ресурси у віддаленій системи, наприклад, веб сторінки і файли.

*3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?*

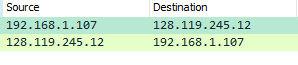


[Дельта часу від попереднього захопленого кадру: 0,000292000 секунд]

[Дельта часу від попереднього відображеного кадру: 0,000000000 секунд]

[Час з моменту посилання або першого кадру: 0,930615000 секунд]

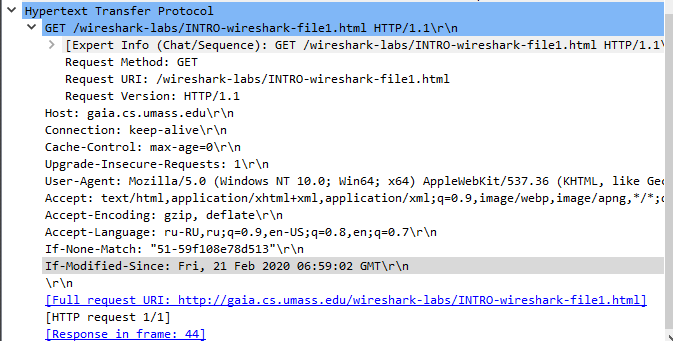
*4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?*



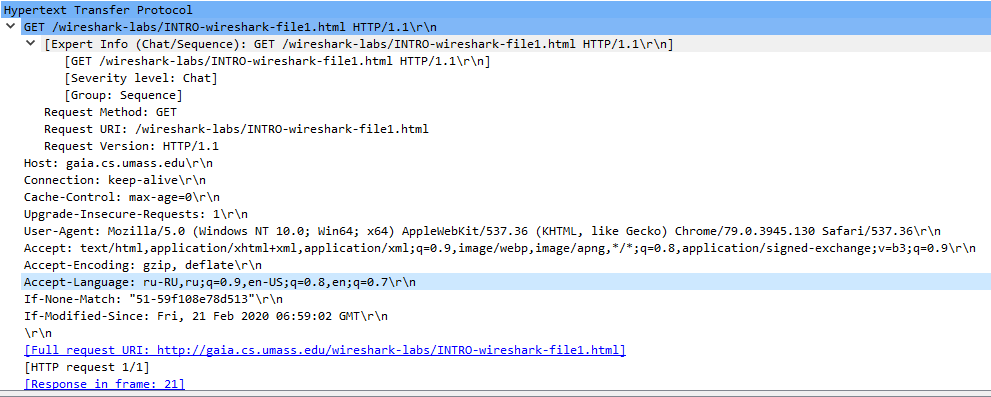
Source – вихідний адрес пакетів

Destination – цільова адреса пакетів

*5. Яким був перший рядок запиту на рівні протоколу HTTP?*



*6. Яким був перший рядок відповіді на рівні протоколу HTTP?*



**Висновок:** В данній лаботаторій роботі були розглянуті методи роботи в середовищі захоплення та аналізу пакетів Wireshark. Роздруковано перші пакети запиту та відповіді. Отримані роздруковані файли містять всю необхідну інформацію для дослідження мережевих протоколів, а саме присутні необхідні для захисту пакети та необхідні для захисту протоколу.