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:

```
No.     Time           Source                Destination           Protocol Length Info
Channel    Signal Stranght
     38 0.930615       192.168.1.107         128.119.245.12        HTTP     652    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/
1.1
Frame 38: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits) on interface \Device\NPF_{A1BA2240-64F3-4F12-995F-D42D06B55803},
id 0
    Interface id: 0 (\Device\NPF_{A1BA2240-64F3-4F12-995F-D42D06B55803})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 21, 2020 12:20:13.726922000 FLE Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1582280413.726922000 seconds
    [Time delta from previous captured frame: 0.000292000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.930615000 seconds]
    Frame Number: 38
    Frame Length: 652 bytes (5216 bits)
    Capture Length: 652 bytes (5216 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: HonHaiPr_b9:36:4d (a4:17:31:b9:36:4d), Dst: Tp-LinkT_de:11:f8 (b0:48:7a:de:11:f8)
Internet Protocol Version 4, Src: 192.168.1.107, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52901, Dst Port: 80, Seq: 1, Ack: 1, Len: 598
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    If-None-Match: "51-59f108e78d513"\r\n
    If-Modified-Since: Fri, 21 Feb 2020 06:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 44]
```

```
No.     Time           Source                Destination           Protocol Length Info
Channel    Signal Stranght
     44 1.047622       128.119.245.12        192.168.1.107         HTTP     293    HTTP/1.1 304 Not Modified
Frame 44: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{A1BA2240-64F3-4F12-995F-D42D06B55803},
id 0
    Interface id: 0 (\Device\NPF_{A1BA2240-64F3-4F12-995F-D42D06B55803})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 21, 2020 12:20:13.843929000 FLE Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1582280413.843929000 seconds
    [Time delta from previous captured frame: 0.001755000 seconds]
    [Time delta from previous displayed frame: 0.117007000 seconds]
    [Time since reference or first frame: 1.047622000 seconds]
    Frame Number: 44
    Frame Length: 293 bytes (2344 bits)
    Capture Length: 293 bytes (2344 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Tp-LinkT_de:11:f8 (b0:48:7a:de:11:f8), Dst: HonHaiPr_b9:36:4d (a4:17:31:b9:36:4d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.107
Transmission Control Protocol, Src Port: 80, Dst Port: 52901, Seq: 1, Ack: 599, Len: 239
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
    Date: Fri, 21 Feb 2020 10:20:13 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "51-59f108e78d513"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.117007000 seconds]
    [Request in frame: 38]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

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.

Название протокола	Расшифровка	Назначение
HTTP	*Hyper Text Transfer Protocol*	Протокол передачи гипертекста
FTP	*File Transfer Protocol*	протокол передачи файлов
SMTP	*Simple Mail Transfer Protocol*	Простой протокол отправки электронных писем
POP3	*Post Office Protocol 3*	Протокол получения электронных писем
NNTP	*News Net Transfer Protocol*	Протокол телеконференций

TCP (Transmission Control Protocol – протокол управления передачей), IP (Internet Protocol – межсетевой протокол), HTTP (Hyper Text Transfer Protocol — это протокол передачи гипертекста), FTP (File Transfer Protocol — это протокол передачи файлов), POP3 (Post Office Protocol — это стандартный протокол почтового соединения), SMTP (Simple Mail Transfer Protocol — протокол, который задает набор правил для передачи почты), DHCP (Dynamic Host Configuration Protocol – протокол динамического конфигурирования хоста).

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?

```
[Time delta from previous captured frame: 0.000292000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.930615000 seconds]
```

[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]

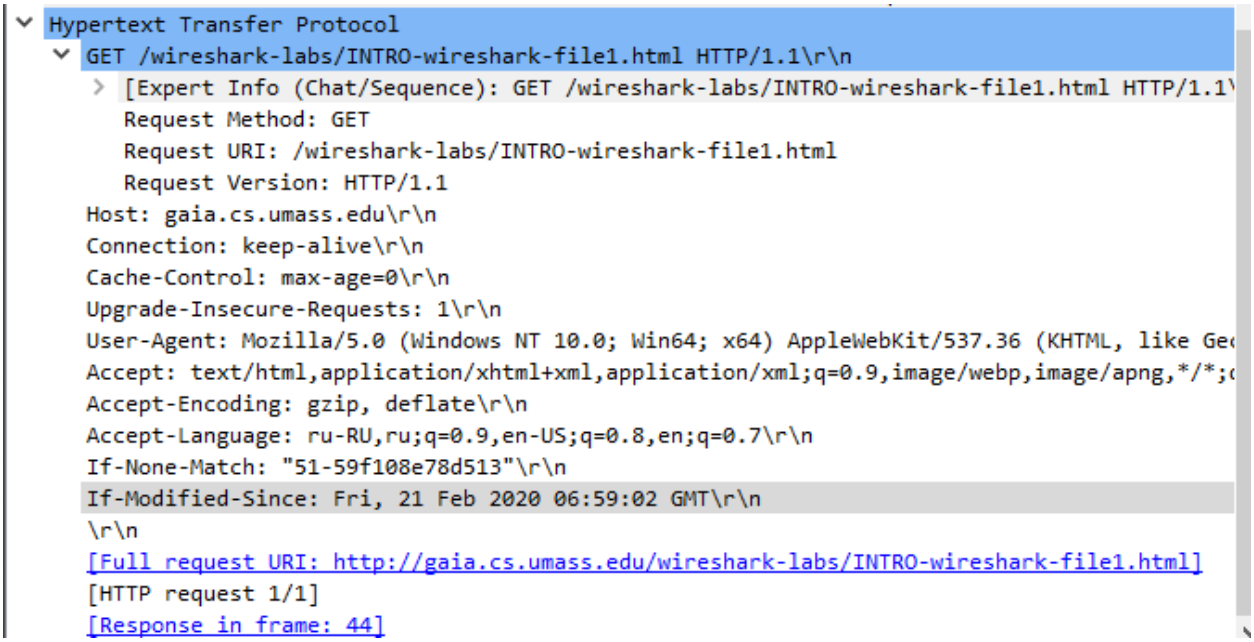
4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?

Source	Destination
192.168.1.107	128.119.245.12
128.119.245.12	192.168.1.107

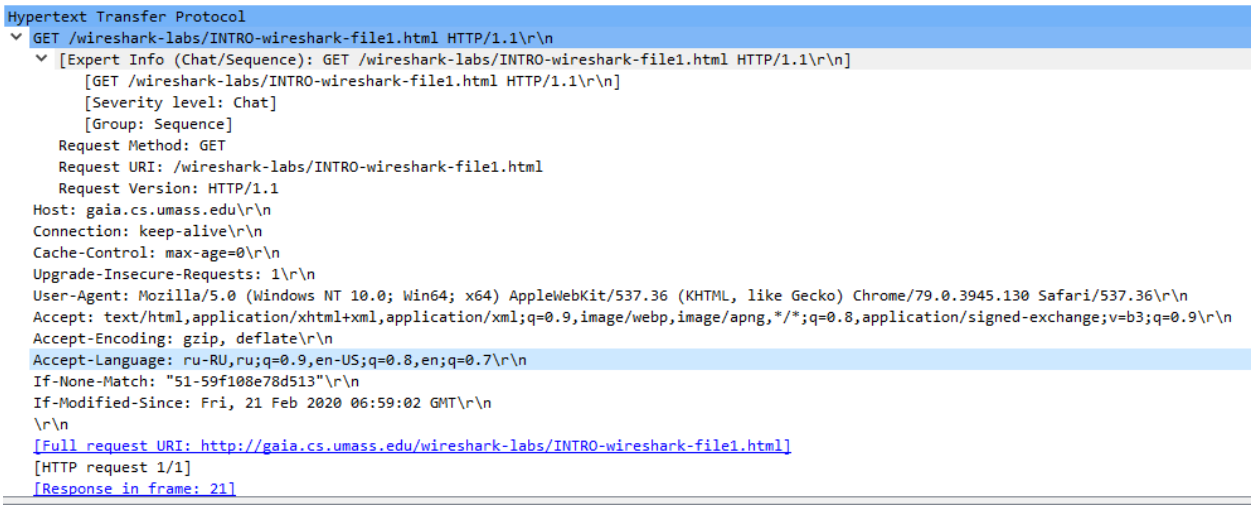
Source – вихідний адрес пакетів

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.