



Міністерство освіти і науки України  
Національний технічний університет України  
«Київський політехнічний інститут ім. І. Сікорського»  
Інститут Прикладного Системного Аналізу

**Лабораторна робота №1**  
**з дисципліни Комп'ютерні мережі**

Виконала  
студентка групи КА-77  
Кулина Анісія

Прийняв Кухарєв С.О.

**Київ 2020**

## Тема. Основи захоплення та аналізу пакетів

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

### Хід роботи:

The screenshot displays the Wireshark network protocol analyzer interface. At the top, the status bar indicates 'Беспроводная сеть' (Wireless network). The menu bar includes options like 'Файл', 'Редактирование', 'Просмотр', 'Запуск', 'Захват', 'Анализ', 'Статистика', 'Телефония', 'Беспроводной', 'Инструменты', and 'Помощь'. The toolbar contains icons for various functions such as opening files, saving, and analyzing. The main window is divided into three panes. The top pane shows a list of captured packets with columns for 'No.', 'Time', 'Source', 'Destination', 'Protocol', 'Length', and 'Info'. Two packets are visible: packet 47 (HTTP GET /favicon.ico) and packet 50 (HTTP 404 Not Found). The middle pane shows the packet details for the selected packet (47), including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) fields. The bottom pane shows the packet bytes, with the Hypertext Transfer Protocol (HTTP) section expanded.

No.	Time	Source	Destination	Protocol	Length	Info
47	5.622201	192.168.0.107	128.119.245.12	HTTP	473	GET /favicon.ico HTTP/1.1
50	5.750756	128.119.245.12	192.168.0.107	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Frame 47: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface \Device\NPF\_{D188B22A-F911-49C2-A5FA-8155FDF0233A}, id 0  
> Ethernet II, Src: IntelCor\_Aa:4f:d4 (20:16:b9:4a:4f:d4), Dst: Tp-LinkT\_43:60:08 (b0:4e:26:43:60:08)  
> Internet Protocol Version 4, Src: 192.168.0.107, Dst: 128.119.245.12  
▼ Transmission Control Protocol, Src Port: 50832, Dst Port: 80, Seq: 1, Ack: 1, Len: 419  
Source Port: 50832  
Destination Port: 80  
[Stream index: 4]  
[TCP Segment Len: 419]  
Sequence number: 1 (relative sequence number)  
Sequence number (raw): 2401661898  
[Next sequence number: 420 (relative sequence number)]  
Acknowledgment number: 1 (relative ack number)  
Acknowledgment number (raw): 633177138  
0101 .... = Header Length: 20 bytes (5)  
> Flags: 0x018 (PSH, ACK)  
Window size value: 513  
[Calculated window size: 131328]  
[Window size scaling factor: 256]  
Checksum: 0x52fa [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0  
> [SEQ/ACK analysis]  
> [Timestamps]  
TCP payload (419 bytes)  
> Hypertext Transfer Protocol

### Контрольні запитання:

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

Protocol	Leng	Protocol	Protocol	Ler
		ARP		
NBNS		IGMPv2		
ARP		IGMPv2		
ARP		IGMPv2	ARP	
IGMPv2		LOOP	TCP	
ARP		IGMPv2	DNS	
ARP		IGMPv2	DNS	
ARP		ARP	TCP	
IGMPv2		ARP	TCP	
IGMPv2		ARP	TCP	
ARP		IGMPv2	TLSv1.3	
IGMPv2		ARP	TCP	
IGMPv2		IGMPv2	TLSv1.3	
IGMPv2		IGMPv2	TLSv1.3	
UDP	1	ARP	TLSv1.3	
IGMPv2		IGMPv2	TLSv1.3	
IGMPv2		IGMPv2	TLSv1.3	
IGMPv2		LOOP	TCP	
ARP		TLSv1.2	TLSv1.3	
ARP		TCP	TCP	
ARP		ARP	TCP	

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

```
> Frame 212: 670 bytes on wire (5360 bits), 670 bytes captured (5360 bits) on interface \Device\NPF_{61808B2C-82AF-4154-B8FA-97705F7E0524}, id 0
> Ethernet II, Src: RealtekS_36:03:69 (00:e0:4c:36:03:69), Dst: Hangzhou_a4:1d:d7 (00:0f:e2:a4:1d:d7)
> Internet Protocol Version 4, Src: 77.47.202.31, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54799, Dst Port: 80, Seq: 1, Ack: 1, Len: 616
> Hypertext Transfer Protocol
```

3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до

отримання першого пакету з відповіддю сервера?

6.446791

6.575107

0.128316

```

Frame 223: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{61808B
  Interface id: 0 (\Device\NPF_{61808B2C-82AF-4154-B8FA-97705F7E0524})
    Interface name: \Device\NPF_{61808B2C-82AF-4154-B8FA-97705F7E0524}
    Interface description: Ethernet 2
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar  4, 2020 00:14:04.737996000 Финляндия (зима)
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1583273644.737996000 seconds
    [Time delta from previous captured frame: 0.009022000 seconds]
    [Time delta from previous displayed frame: 0.128316000 seconds]
    [Time since reference or first frame: 6.575107000 seconds]
    Frame Number: 223
    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: Hangzhou_a4:1d:d7 (00:0f:e2:a4:1d:d7), Dst: RealtekS_36:03:69 (00:e0:4c:36:03:69)
    Internet Protocol Version 4, Src: 128.119.245.12, Dst: 77.47.202.31

```

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

```

  Ethernet II, Src: RealtekS_36:03:69 (00:e0:4c:36:03:69), Dst: Hangzhou_a4:1d:d7 (00:0f:e2:a4:1d:d7)
  Internet Protocol Version 4, Src: 77.47.202.31, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 656
    Identification: 0x4f22 (20258)
    > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 77.47.202.31
    Destination: 128.119.245.12

    Protocol: TCP (6)
    Header checksum: 0x505d [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 77.47.202.31

```

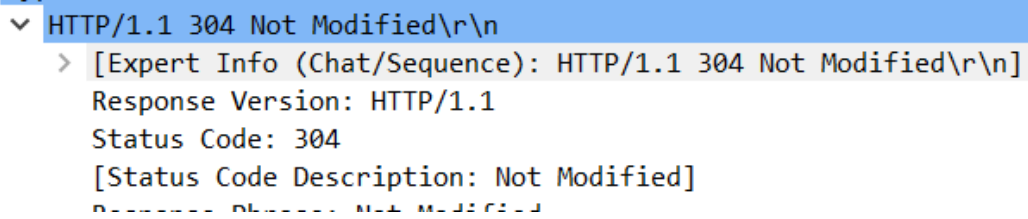
5. Яким був перший рядок запиту на рівні протоколу HTTP?

```

Hypertext Transfer Protocol
  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
    Request Method: GET

```

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



Wireshark packet capture screenshot showing an HTTP 304 Not Modified response. The packet list on the left shows a packet of type 'HTTP' with status '304 Not Modified'. The packet details pane on the right shows the 'Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n'. The packet bytes pane on the right shows the raw data of the response.

```
HTTP/1.1 304 Not Modified\r\n> [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\nResponse Version: HTTP/1.1Status Code: 304[Status Code Description: Not Modified]
```

**Висновки:** в ході виконання роботи були набуті навички користування середовищем Wireshark для захоплення та аналізу пакетів. Було визначено за який час було відправлено перший запит та отримано відповідь.