

**Комп'ютерні інформаційні  
мережі**

**ЛАБОРАТОРНА РОБОТА №7**

**Аналіз IP-пакетів і повідомлень  
керуючих протоколів.  
Утиліти для діагностики мережі  
на мережевому рівні**

Виконав:

Студент групи ПМі-31

Яцуляк Андрій

**Мета:** Здобути практичні навички з інтерпретації IP-пакетів і повідомлень керуючих протоколів, а також використання консольних утиліт для діагностики мережі на мережевому рівні.

## Хід роботи

1. Опрацював теоретичний матеріал.
2. Ознайомився з базовою мережевою конфігурацією свого ноутбука, виконавши в консолі команду `ipconfig`:

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Подключение по локальной сети* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Подключение по локальной сети* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Беспроводная сеть 2:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::86f5:3a79:80cd:db8f%19
    IPv4 Address. . . . . : 192.168.0.103
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Ethernet adapter Сетевое подключение Bluetooth:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

3. Отримав більш детальну інформацію командою `ipconfig /all`:

```
C:\>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : DESKTOP-3KG48E2
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

Ethernet adapter Ethernet:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address. . . . . : 38-F3-AB-BC-5C-DA
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

Wireless LAN adapter Подключение по локальной сети\* 1:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 92-0F-0C-88-42-5F
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

Wireless LAN adapter Подключение по локальной сети\* 2:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : D2-0F-0C-88-42-5F
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
```

Wireless LAN adapter Беспроводная сеть 2:

```
Connection-specific DNS Suffix . :  
Description . . . . . : Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC  
Physical Address. . . . . : 90-0F-0C-88-42-5F  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::86f5:3a79:80cd:db8f%19(Preferred)  
IPv4 Address. . . . . : 192.168.0.103(Preferred)  
Subnet Mask . . . . . : 255.255.255.0  
Lease Obtained. . . . . : Sunday, November 19, 2023 7:38:23 PM  
Lease Expires . . . . . : Sunday, November 19, 2023 11:00:12 PM  
Default Gateway . . . . . : 192.168.0.1  
DHCP Server . . . . . : 192.168.0.1  
DHCPv6 IAID . . . . . : 294653708  
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-D8-0E-37-38-F3-AB-BC-5C-DA  
DNS Servers . . . . . : 192.168.0.1  
NetBIOS over Tcpip. . . . . : Enabled
```

Ethernet adapter Сетевое подключение Bluetooth:

```
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :  
Description . . . . . : Bluetooth Device (Personal Area Network)  
Physical Address. . . . . : 90-0F-0C-88-42-60  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . : Yes
```

4. Команда `ipconfig /renew` оновлює конфігурацію DHCP для всіх адаптерів (якщо адаптер не вказано) або для певного адаптера, якщо включено параметр адаптера. Цей параметр доступний лише на комп'ютерах з адаптерами, налаштованими на автоматичне отримання IP-адреси.  
Команда `ipconfig /release` надсилає повідомлення DHCPRELEASE серверу DHCP, щоб звільнити поточну конфігурацію DHCP і скасувати конфігурацію IP-адреси для всіх адаптерів (якщо адаптер не вказано) або для окремого адаптера, якщо включено параметр адаптера. Цей параметр вмикає TCP/IP для адаптерів, налаштованих на автоматичне отримання IP-адреси.
5. Переглянув активні TCP-з'єднання за допомогою команди `netstat`:



## Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:49677	DESKTOP-3KG48E2:49678	ESTABLISHED
TCP	127.0.0.1:49678	DESKTOP-3KG48E2:49677	ESTABLISHED
TCP	127.0.0.1:49679	DESKTOP-3KG48E2:49680	ESTABLISHED
TCP	127.0.0.1:49680	DESKTOP-3KG48E2:49679	ESTABLISHED
TCP	127.0.0.1:49781	DESKTOP-3KG48E2:49795	ESTABLISHED
TCP	127.0.0.1:49781	DESKTOP-3KG48E2:49814	ESTABLISHED
TCP	127.0.0.1:49795	DESKTOP-3KG48E2:49781	ESTABLISHED
TCP	127.0.0.1:49814	DESKTOP-3KG48E2:49781	ESTABLISHED
TCP	192.168.0.103:49703	20.199.120.182:https	ESTABLISHED
TCP	192.168.0.103:49709	57:7500	ESTABLISHED
TCP	192.168.0.103:49778	162.159.135.234:https	ESTABLISHED
TCP	192.168.0.103:49784	52.112.238.117:https	ESTABLISHED
TCP	192.168.0.103:49809	172.64.148.154:https	ESTABLISHED
TCP	192.168.0.103:49820	172.64.148.154:https	ESTABLISHED
TCP	192.168.0.103:49854	52.123.159.172:https	ESTABLISHED
TCP	192.168.0.103:51675	1b-140-82-112-26-iad:https	ESTABLISHED
TCP	192.168.0.103:59342	ws-in-f188:5228	ESTABLISHED
TCP	192.168.0.103:59741	a23-64-12-34:https	CLOSE_WAIT
TCP	192.168.0.103:59742	a23-64-12-34:https	CLOSE_WAIT
TCP	192.168.0.103:59743	a23-64-12-34:https	CLOSE_WAIT
TCP	192.168.0.103:59744	a23-64-12-34:https	CLOSE_WAIT
TCP	192.168.0.103:62849	149.154.167.41:https	ESTABLISHED
TCP	192.168.0.103:62876	waw07s06-in-f14:https	TIME_WAIT
TCP	192.168.0.103:62877	204.79.197.239:https	TIME_WAIT
TCP	192.168.0.103:62878	104.18.39.102:https	TIME_WAIT
TCP	192.168.0.103:62879	server-18-245-60-10:https	TIME_WAIT
TCP	192.168.0.103:62880	52.123.159.136:https	TIME_WAIT
TCP	192.168.0.103:62882	waw07s06-in-f14:https	TIME_WAIT
TCP	192.168.0.103:62883	52.123.159.136:https	TIME_WAIT
TCP	192.168.0.103:62884	waw02s16-in-f13:https	TIME_WAIT
TCP	192.168.0.103:62885	149.154.167.216:https	TIME_WAIT
TCP	192.168.0.103:62887	waw07s06-in-f14:https	TIME_WAIT
TCP	192.168.0.103:62888	149.154.167.41:https	ESTABLISHED
TCP	192.168.0.103:62889	149.154.167.41:http	TIME_WAIT
TCP	192.168.0.103:62890	52.123.159.136:https	TIME_WAIT
TCP	192.168.0.103:62893	kbp03s03-in-f28:https	TIME_WAIT
TCP	192.168.0.103:62895	kbp03s03-in-f28:https	TIME_WAIT
TCP	192.168.0.103:62898	kbp03s03-in-f28:https	TIME_WAIT
TCP	192.168.0.103:62899	fra16s67-in-f7:https	TIME_WAIT
TCP	192.168.0.103:62900	kbp03s03-in-f28:https	TIME_WAIT
TCP	192.168.0.103:62901	kbp03s03-in-f28:https	TIME_WAIT
TCP	192.168.0.103:62902	waw02s22-in-f3:https	ESTABLISHED
TCP	192.168.0.103:62903	13.69.239.74:https	ESTABLISHED
TCP	192.168.0.103:62904	194.44.64.32:https	ESTABLISHED
TCP	192.168.0.103:62905	176:http	TIME_WAIT

Опис отриманих станів.

ESTABLISHED - цей стан вказує на те, що TCP-з'єднання активне і дані можна надсилати або отримувати. Це означає, що з'єднання між локальною та віддаленою системами успішно встановлено, і обидві готові до обміну даними.

SYN\_SENT – цей стан відображається, коли система надіслала запит на підключення TCP (SYN) до віддаленої системи, але ще не отримала підтвердження (SYN-ACK) від віддаленої системи.

CLOSE\_WAIT – цей стан вказує на те, що віддалена система закрила з'єднання, а локальна система чекає, поки програма підтвердить запит на закриття. По суті, це означає, що з'єднання перебуває в процесі закриття, але локальна програма все ще має виконати операцію закриття.

TIME\_WAIT – цей стан виникає після того, як локальна система закрила з'єднання та очікує на будь-які затримані пакети, які ще можуть бути в дорозі. Стан TIME\_WAIT гарантує, що обидві сторони з'єднання мають достатньо часу для обробки будь-яких затриманих пакетів, і запобігає плутанині, якщо нові з'єднання встановлюються з однаковими номерами портів.

Параметр -n наказує netstat відображати числові адреси замість того, щоб перетворювати їх на імена хостів. Іншими словами, IP-адреси відображатимуться в цифровій формі, а не в доменні імена:



```
C:\>netstat -n
```

# Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:49669	127.0.0.1:49670	ESTABLISHED
TCP	127.0.0.1:49670	127.0.0.1:49669	ESTABLISHED
TCP	127.0.0.1:49671	127.0.0.1:49672	ESTABLISHED
TCP	127.0.0.1:49672	127.0.0.1:49671	ESTABLISHED
TCP	127.0.0.1:49716	127.0.0.1:63834	ESTABLISHED
TCP	127.0.0.1:49716	127.0.0.1:63836	ESTABLISHED
TCP	127.0.0.1:63834	127.0.0.1:49716	ESTABLISHED
TCP	127.0.0.1:63836	127.0.0.1:49716	ESTABLISHED
TCP	192.168.0.103:52538	52.112.238.117:443	ESTABLISHED
TCP	192.168.0.103:52557	64.233.161.188:5228	ESTABLISHED
TCP	192.168.0.103:52575	20.199.120.151:443	ESTABLISHED
TCP	192.168.0.103:52589	34.141.12.164:7500	ESTABLISHED
TCP	192.168.0.103:52591	149.154.167.41:443	ESTABLISHED
TCP	192.168.0.103:60003	192.229.221.95:80	TIME_WAIT
TCP	192.168.0.103:60025	192.229.221.95:80	TIME_WAIT
TCP	192.168.0.103:60075	2.21.173.58:443	ESTABLISHED
TCP	192.168.0.103:60087	193.200.65.149:443	TIME_WAIT
TCP	192.168.0.103:60092	194.55.244.181:443	TIME_WAIT
TCP	192.168.0.103:60093	194.55.244.185:443	TIME_WAIT
TCP	192.168.0.103:60094	104.19.231.122:443	TIME_WAIT
TCP	192.168.0.103:60095	104.17.109.212:443	TIME_WAIT
TCP	192.168.0.103:60099	149.154.167.216:443	TIME_WAIT
TCP	192.168.0.103:60100	149.154.167.216:80	TIME_WAIT
TCP	192.168.0.103:60101	193.200.65.149:443	TIME_WAIT
TCP	192.168.0.103:60102	195.209.108.38:443	TIME_WAIT
TCP	192.168.0.103:60103	195.209.108.57:443	TIME_WAIT
TCP	192.168.0.103:60105	35.168.243.244:443	TIME_WAIT
TCP	192.168.0.103:60109	193.200.65.149:443	TIME_WAIT
TCP	192.168.0.103:60111	88.218.242.3:443	TIME_WAIT
TCP	192.168.0.103:60116	88.218.242.3:443	TIME_WAIT
TCP	192.168.0.103:60125	193.200.65.149:443	TIME_WAIT
TCP	192.168.0.103:60126	148.251.4.142:443	TIME_WAIT
TCP	192.168.0.103:60127	195.201.108.196:443	TIME_WAIT
TCP	192.168.0.103:60128	104.17.109.212:443	TIME_WAIT
TCP	192.168.0.103:60131	195.209.108.38:443	TIME_WAIT
TCP	192.168.0.103:60134	195.209.108.57:443	TIME_WAIT
TCP	192.168.0.103:60137	193.200.65.151:443	TIME_WAIT
TCP	192.168.0.103:60138	52.123.136.137:443	TIME_WAIT
TCP	192.168.0.103:60140	88.218.242.3:443	TIME_WAIT
TCP	192.168.0.103:60141	149.154.167.41:443	ESTABLISHED
TCP	192.168.0.103:60143	149.154.167.41:443	ESTABLISHED
TCP	192.168.0.103:60145	193.200.65.151:443	TIME_WAIT
TCP	192.168.0.103:60149	88.218.242.3:443	TIME_WAIT
TCP	192.168.0.103:60151	148.251.4.142:443	TIME_WAIT
TCP	192.168.0.103:60152	195.201.108.196:443	TIME_WAIT

Параметр -а показує всі активні з'єднання та порти прослуховування, включаючи TCP і UDP. Він відображає стан кожного сокета в системі:



```
C:\>netstat -a
```

### Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	DESKTOP-3KG48E2:0	LISTENING
TCP	0.0.0.0:445	DESKTOP-3KG48E2:0	LISTENING
TCP	0.0.0.0:3306	DESKTOP-3KG48E2:0	LISTENING
TCP	0.0.0.0:5040	DESKTOP-3KG48E2:0	LISTENING
TCP	0.0.0.0:5357	DESKTOP-3KG48E2:0	LISTENING
TCP	0.0.0.0:5432	DESKTOP-3KG48E2:0	LISTENING
TCP	0.0.0.0:33060	DESKTOP-3KG48E2:0	LISTENING
TCP	0.0.0.0:49664	DESKTOP-3KG48E2:0	LISTENING
TCP	0.0.0.0:49665	DESKTOP-3KG48E2:0	LISTENING
TCP	0.0.0.0:49666	DESKTOP-3KG48E2:0	LISTENING
TCP	0.0.0.0:49667	DESKTOP-3KG48E2:0	LISTENING
TCP	0.0.0.0:49668	DESKTOP-3KG48E2:0	LISTENING
TCP	0.0.0.0:49673	DESKTOP-3KG48E2:0	LISTENING
TCP	0.0.0.0:49677	DESKTOP-3KG48E2:0	LISTENING
TCP	0.0.0.0:50128	DESKTOP-3KG48E2:0	LISTENING
TCP	0.0.0.0:50131	DESKTOP-3KG48E2:0	LISTENING
TCP	127.0.0.1:5939	DESKTOP-3KG48E2:0	LISTENING
TCP	127.0.0.1:6463	DESKTOP-3KG48E2:0	LISTENING
TCP	127.0.0.1:9100	DESKTOP-3KG48E2:0	LISTENING
TCP	127.0.0.1:9180	DESKTOP-3KG48E2:0	LISTENING
TCP	127.0.0.1:12025	DESKTOP-3KG48E2:0	LISTENING
TCP	127.0.0.1:12110	DESKTOP-3KG48E2:0	LISTENING
TCP	127.0.0.1:12119	DESKTOP-3KG48E2:0	LISTENING
TCP	127.0.0.1:12143	DESKTOP-3KG48E2:0	LISTENING
TCP	127.0.0.1:12465	DESKTOP-3KG48E2:0	LISTENING
TCP	127.0.0.1:12563	DESKTOP-3KG48E2:0	LISTENING
TCP	127.0.0.1:12993	DESKTOP-3KG48E2:0	LISTENING
TCP	127.0.0.1:12995	DESKTOP-3KG48E2:0	LISTENING
TCP	127.0.0.1:27017	DESKTOP-3KG48E2:0	LISTENING
TCP	127.0.0.1:27275	DESKTOP-3KG48E2:0	LISTENING
TCP	127.0.0.1:49669	DESKTOP-3KG48E2:49670	ESTABLISHED
TCP	127.0.0.1:49670	DESKTOP-3KG48E2:49669	ESTABLISHED
TCP	127.0.0.1:49671	DESKTOP-3KG48E2:49672	ESTABLISHED
TCP	127.0.0.1:49672	DESKTOP-3KG48E2:49671	ESTABLISHED
TCP	127.0.0.1:49716	DESKTOP-3KG48E2:0	LISTENING
TCP	127.0.0.1:49716	DESKTOP-3KG48E2:63834	ESTABLISHED
TCP	127.0.0.1:49716	DESKTOP-3KG48E2:63836	ESTABLISHED
TCP	127.0.0.1:63834	DESKTOP-3KG48E2:49716	ESTABLISHED
TCP	127.0.0.1:63836	DESKTOP-3KG48E2:49716	ESTABLISHED
TCP	192.168.0.103:139	DESKTOP-3KG48E2:0	LISTENING
TCP	192.168.0.103:52538	52.112.238.117:https	ESTABLISHED
TCP	192.168.0.103:52557	lh-in-f188:5228	ESTABLISHED

6. Для отримання статистики про отримані/відправлені пакети виконав команду netstat -e:

```
C:\>netstat -e
Interface Statistics

              Received              Sent
Bytes          3598087871          190335775
Unicast packets 3498852             1202502
Non-unicast packets 34223             5082
Discards                0                0
Errors                  0                0
Unknown protocols      0
```

7. Запустив Wireshark від імені адміністратора.  
8. Від'єднався від мережі.  
9. Почав захоплення пакетів.  
10. Підключився до мережі.  
11. Здійснив активність в браузері.  
12. Закінчив захоплення пакетів та зберіг результати у файл.  
13. Обрав пакет для аналізу. Біти, які відповідають заголовку:

```
3978 10.896115 172.217.133.199 192.168.0.103 TLSv1.3 356 Application Data, Application Data, Application Data, Application Data
3979 10.896220 192.168.0.103 172.217.133.199 TCP 54 49975 → 443 [ACK] Seq=14244 Ack=467426 Win=132352 Len=0
3980 10.910192 172.217.133.199 192.168.0.103 TLSv1.3 695 Application Data, Application Data, Application Data, Application Data
3981 10.910297 192.168.0.103 172.217.133.199 TCP 54 49976 → 443 [ACK] Seq=11976 Ack=507143 Win=530944 Len=0
3982 10.911337 172.217.133.199 192.168.0.103 TLSv1.3 599 Application Data, Application Data, Application Data, Application Data
3983 10.935727 172.217.133.199 192.168.0.103 TLSv1.3 361 Application Data, Application Data, Application Data, Application Data
3984 10.936453 172.217.133.199 192.168.0.103 TLSv1.3 1462 Application Data, Application Data
3985 10.936453 172.217.133.199 192.168.0.103 TCP 1462 443 → 49975 [ACK] Seq=469141 Ack=14244 Win=98304 Len=1408 [TCP segment of a reassembled PDU]
3986 10.936545 192.168.0.103 172.217.133.199 TCP 54 49975 → 443 [ACK] Seq=14244 Ack=470549 Win=132352 Len=0
3987 10.936747 172.217.133.199 192.168.0.103 TCP 1462 443 → 49975 [ACK] Seq=470549 Ack=14244 Win=98304 Len=1408 [TCP segment of a reassembled PDU]
3988 10.936747 172.217.133.199 192.168.0.103 TCP 1462 443 → 49975 [PSH, ACK] Seq=471957 Ack=14244 Win=98304 Len=1408 [TCP segment of a reassembled PDU]
3989 10.936848 192.168.0.103 172.217.133.199 TCP 54 49975 → 443 [ACK] Seq=14244 Ack=473365 Win=132352 Len=0
3990 10.938370 172.217.133.199 192.168.0.103 TCP 1462 443 → 49975 [ACK] Seq=473365 Ack=14244 Win=98304 Len=1408 [TCP segment of a reassembled PDU]
3991 10.938466 192.168.0.103 172.217.133.199 TCP 54 49975 → 443 [ACK] Seq=14244 Ack=474773 Win=132352 Len=0
3992 10.938717 172.217.133.199 192.168.0.103 TCP 1462 443 → 49975 [ACK] Seq=474773 Ack=14244 Win=98304 Len=1408 [TCP segment of a reassembled PDU]
3993 10.938717 172.217.133.199 192.168.0.103 TLSv1.3 270 Application Data, Application Data
3994 10.938786 192.168.0.103 172.217.133.199 TCP 54 49975 → 443 [ACK] Seq=14244 Ack=476397 Win=132352 Len=0
3995 10.954648 172.217.133.199 192.168.0.103 TLSv1.3 608 Application Data, Application Data, Application Data, Application Data
> Frame 3988: 1462 bytes on wire (11696 bits), 1462 bytes captured (11696 bits) on interface \Device\NPF...
> Ethernet II, Src: Tp-LinkT cd:e4:da (ec:08:6b:cd:e4:da), Dst: CloudNet_88:42:5f (90:0f:0c:88:42:5f)
> Internet Protocol Version 4, Src: 172.217.133.199, Dst: 192.168.0.103
> Transmission Control Protocol, Src Port: 443, Dst Port: 49975, Seq: 471957, Ack: 14244, Len: 1408
```

14. Розгорнув заголовок та отримав більш детальну інформацію:

```
▼ Internet Protocol Version 4, Src: 172.217.133.199, Dst: 192.168.0.103
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1448
    Identification: 0xb63d (46653)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 59
    Protocol: TCP (6)
    Header Checksum: 0xd062 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.217.133.199
    Destination Address: 192.168.0.103
```

Version (0100 ...) - версія IP-протоколу. У цьому випадку це 4, що рівне 0100 у двійковому записі.

Header Length (... 0101) - представляє довжину IP-заголовка в 32-розрядних словах. У даному випадку це 5, а оскільки кожне слово має 4 байти, загальна довжина заголовка становить  $5 * 4 = 20$  байтів.

Differentiated Services Field (DSCP: CS0, ECN: Not-ECT) - використовуються для маркування якості обслуговування.

Total Length - вказується загальна довжина IP-пакета (header + data). У даному прикладі це 1448 байт.

Identification - 16-бітове поле, яке використовується для унікальної ідентифікації фрагмента. Фрагменти пакета матимуть однакове ідентифікаційне значення. У даному випадку це 46653 (0xb63d).

Flags (000. ....) - використовується для керування інформацією, пов'язаною з фрагментацією.

Fragment Offset (...0 0000 0000 0000) - вказує позицію фрагмента у вихідному потоці даних. У даному випадку зміщення фрагмента дорівнює 0.

Time to Live (TTL) - позначає максимальний час, протягом якого пакет може жити в мережі. Він зменшується кожним маршрутизатором, через який проходить пакет. У даному випадку це 59.

Protocol - визначає протокол, який використовується в частині даних пакета. У даному випадку це TCP (6).

Header Checksum - контрольна сума для заголовка для забезпечення цілісності даних. Контрольна сума обчислюється по всьому заголовку. У даному випадку значення контрольної суми дорівнює 0x781d.

Source Address – IP-адреса відправника. У даному випадку це 172.217.133.199.

Destination Address - IP-адреса одержувача. У даному випадку це 192.168.0.103.

- 15. “Біти 0100 поля Версія (Version) дають десяткове число 4, яке відповідає протоколу IPv4. Чому тоді біти 0101 (десяткове число 5) поля Довжина заголовку Комп’ютерні інформаційні мережі:**

**лабораторна робота “Аналіз IP-пакетів і повідомлень керуючих ...”  
— сторінка 4 (Header Length) відповідають значенню 20 байт, а не 5 байт?”.**

Header Length (... 0101) - представляє довжину IP-заголовка в 32-розрядних словах. У даному випадку це 5, а оскільки кожне слово має 4 байти, загальна довжина заголовка становить  $5 * 4 = 20$  байтів.

**16. “Який розмір корисних даних?”.**

Довжина хедера = 20 байт, загальна довжина = 1448 байт, отже розмір корисних даних – 1428 байт.

**17. “Що Ви можете сказати про одержувача та відправника за виглядом їхніх IP-адрес?”.**

IP-адреса відправника 172.217.133.199 - глобальна адреса, яка може вказувати на зовнішній пристрій

IP-адреса отримувача 192.168.0.103 є адресою мого Wifi-адаптера.

**18. Інформація про тип обслуговування.**

Поле DSCP складається з двох частин:

- DSCP (6 біт): Ця частина поля визначає значення DSCP і вказує на клас обслуговування. Ці 6 біт визначають 64 різних значення DSCP, які використовуються для призначення пакетам різного пріоритету обслуговування в мережі.
- ECN (Explicit Congestion Notification) (2 біти): Ця частина поля використовується для вказівки на стан перевантаження в мережі. Два біти ECN можуть приймати значення 00 (не використовується), 01 (ECT - ECT(0)), 10 (ECT(1)), або 11 (CE - Congestion Experienced).

Значення DSCP та ECN визначаються при визначенні якості обслуговування для пакета. Вони використовуються для вказівки на пріоритет обслуговування і стан перевантаження в мережі. Наприклад, важливі пакети можуть мати більший пріоритет, або, якщо мережа перевантажена, може використовуватися управління затримкою для зменшення витрат пакетів в мережі.

**19. Відфільтрував протоколи динамічної конфігурації хостів (DHCP) з усіх:**

bootp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xf94f2929
4	0.009486	192.168.0.1	192.168.0.103	DHCP	590	DHCP ACK - Transaction ID 0xf94f2929

**20. Обрав DHCP запит для аналізу:**



bootp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xf94f2929
4	0.009486	192.168.0.1	192.168.0.103	DHCP	590	DHCP ACK - Transaction ID 0xf94f2929

> Frame 1: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits) on interface \Device\NPF\_{DA8BD7...} 0000 ff ff ff f  
 > Ethernet II, Src: CloudNet\_88:42:5f (90:0f:0c:88:42:5f), Dst: Broadcast (ff:ff:ff:ff:ff:ff) 0010 01 5e 85 d  
 > Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255 0020 ff ff 00 4

- Source: Зазвичай вказується 0.0.0.0 або IP-адреса самого клієнта, оскільки DHCP-клієнт ще не отримав IP-адресу від DHCP-сервера.
- Destination: Зазвичай вказується 255.255.255.255, оскільки DHCP-клієнт спрямовує свій запит на весь локальний підмережвий діапазон і намагається звернутися до будь-якого

21. доступного DHCP-сервера.Обрав DHCP відповідь для аналізу:

bootp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xf94f2929
4	0.009486	192.168.0.1	192.168.0.103	DHCP	590	DHCP ACK - Transaction ID 0xf94f2929

> Frame 4: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF\_{DA8BD7...} 0000 90 0f 0c 8  
 > Ethernet II, Src: Tp-LinkT\_cd:e4:da (ec:08:6b:cd:e4:da), Dst: CloudNet\_88:42:5f (90:0f:0c:88:42:5f) 0010 02 40 56 c  
 > Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103 0020 00 67 00 4

- Source: Це IP-адреса DHCP-сервера, який відправляє підтвердження клієнту.
- Destination: Це IP-адреса DHCP-клієнта, якому призначається IP-адреса та інші мережеві параметри.

22. Інформація, що передається у DHCP запиті:



- ▼ Dynamic Host Configuration Protocol (Request)
  - Message type: Boot Request (1)
  - Hardware type: Ethernet (0x01)
  - Hardware address length: 6
  - Hops: 0
  - Transaction ID: 0xf94f2929
  - Seconds elapsed: 0
  - Bootp flags: 0x0000 (Unicast)
  - Client IP address: 0.0.0.0
  - Your (client) IP address: 0.0.0.0
  - Next server IP address: 0.0.0.0
  - Relay agent IP address: 0.0.0.0
  - Client MAC address: CloudNet\_88:42:5f (90:0f:0c:88:42:5f)
  - Client hardware address padding: 0000000000000000000000
  - Server host name not given
  - Boot file name not given
  - Magic cookie: DHCP
- ▼ Option: (53) DHCP Message Type (Request)
  - Length: 1
  - DHCP: Request (3)
- ▼ Option: (61) Client identifier
  - Length: 7
  - Hardware type: Ethernet (0x01)
  - Client MAC address: CloudNet\_88:42:5f (90:0f:0c:88:42:5f)
- ▼ Option: (50) Requested IP Address (192.168.0.103)
  - Length: 4
  - Requested IP Address: 192.168.0.103
- ▼ Option: (12) Host Name
  - Length: 15
  - Host Name: DESKTOP-3KG48E2

- > Option: (53) DHCP Message Type (Request)
- > Option: (61) Client identifier
- > Option: (50) Requested IP Address (192.168.0.103)
- > Option: (12) Host Name
- ▼ Option: (81) Client Fully Qualified Domain Name
  - Length: 18
  - > Flags: 0x00
  - A-RR result: 0
  - PTR-RR result: 0
  - Client name: DESKTOP-3KG48E2
- ▼ Option: (60) Vendor class identifier
  - Length: 8
  - Vendor class identifier: MSFT 5.0
- ▼ Option: (55) Parameter Request List
  - Length: 14
  - Parameter Request List Item: (1) Subnet Mask
  - Parameter Request List Item: (3) Router
  - Parameter Request List Item: (6) Domain Name Server
  - Parameter Request List Item: (15) Domain Name
  - Parameter Request List Item: (31) Perform Router Discover
  - Parameter Request List Item: (33) Static Route
  - Parameter Request List Item: (43) Vendor-Specific Information
  - Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
  - Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
  - Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
  - Parameter Request List Item: (119) Domain Search
  - Parameter Request List Item: (121) Classless Static Route
  - Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
  - Parameter Request List Item: (252) Private/Proxy autodiscovery
- ▼ Option: (255) End
  - Option End: 255

23. Ввів у консолі команду *hostname* та переконався, що ім'я комп'ютера збігається з іменем у DHCP-запиті та з іменем у пункті 3.

24. Інформація, що передається у DHCP відповіді:



```

C:\>ping google.com

Pinging google.com [142.250.186.206] with 32 bytes of data:
Reply from 142.250.186.206: bytes=32 time=26ms TTL=118
Reply from 142.250.186.206: bytes=32 time=26ms TTL=118
Reply from 142.250.186.206: bytes=32 time=30ms TTL=118
Reply from 142.250.186.206: bytes=32 time=27ms TTL=118

Ping statistics for 142.250.186.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 30ms, Average = 27ms

C:\>nslookup google.com
Server:    UnKnown
Address:   192.168.0.1

Non-authoritative answer:
Name:      google.com
Addresses: 2a00:1450:401b:808::200e
           142.250.186.206

```

27. Зупинив захоплення пакетів. Знову застосував фільтр ісмп та переконався, що цього разу результат не порожній:

No.	Time	Source	Destination	Protocol	Length	Info
176	4.637082	192.168.0.103	142.250.186.206	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 178)
178	4.663037	142.250.186.206	192.168.0.103	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=118 (request in 176)
208	5.650885	192.168.0.103	142.250.186.206	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 211)
211	5.676831	142.250.186.206	192.168.0.103	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=118 (request in 208)
231	6.668582	192.168.0.103	142.250.186.206	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 232)
232	6.698669	142.250.186.206	192.168.0.103	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=118 (request in 231)
279	7.680213	192.168.0.103	142.250.186.206	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 282)

28. TTL в ICMP-запиті та відповіді може відрізнятися через різні шляхи, які вони пройшли в мережі та різні відстані до точки призначення та назад.

29. В попередньому захопленні я отримав 2 типи ICMP-повідомлень: 8 - ехо-запит та 0 - ехо відповідь:

No.	Time	Source	Destination	Protocol	Length	Info
176	4.637082	192.168.0.103	142.250.186.206	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 178)
178	4.663037	142.250.186.206	192.168.0.103	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=118 (request in 176)
208	5.650885	192.168.0.103	142.250.186.206	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 211)

  

> Frame 176: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{DA88D773-0000-ec 08 6b cd e4 da 90 0f} 0c 88 42 5f 08 00 45 00 --k....	
> Ethernet II, Src: CloudNet_88:42:5f (90:0f:0c:88:42:5f), Dst: Tp-LinkT_cd:e4:da (ec:08:6b:cd:e4:da)	0010 00 3c 6e 0a 00 00 80 01 c1 de c0 a8 00 67 8e fa <n....
> Internet Protocol Version 4, Src: 192.168.0.103, Dst: 142.250.186.206	0020 ba ce 08 00 4d 56 00 01 00 05 61 62 63 64 65 66 ....MV-
> Internet Control Message Protocol	0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklm
Type: 8 (Echo (ping) request)	0040 77 61 62 63 64 65 66 67 68 69 wabcdefj
Code: 0	
Checksum: 0x4d56 [correct]	
[Checksum Status: Good]	
Identifier (BE): 1 (0x0001)	
Identifier (LE): 256 (0x0100)	
Sequence Number (BE): 5 (0x0005)	
Sequence Number (LE): 1280 (0x0500)	
[Response frame: 178]	
Data (32 bytes)	
Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869	
[Length: 32]	







```
C:\>tracert google.com

Tracing route to google.com [142.250.203.206]
over a maximum of 30 hops:

  1      3 ms      1 ms      3 ms      192.168.0.1
  2     11 ms      2 ms      3 ms      10.10.10.11
  3     62 ms     14 ms     18 ms     194.44.229.201
  4     14 ms     13 ms     15 ms     194.44.212.36
  5     23 ms     23 ms     15 ms     209.85.168.96
  6     13 ms     12 ms     12 ms     108.170.248.155
  7     48 ms     60 ms     27 ms     142.251.242.35
  8     29 ms     28 ms     32 ms     108.170.250.209
  9     27 ms     27 ms     26 ms     209.85.252.109
 10     27 ms     33 ms     25 ms     waw02s22-in-f14.1e100.net [142.250.203.206]

Trace complete.
```

Отже, щоб пакет потрапив до сервера google.com з IP-адресою 142.250.203.206, йому потрібно пройти 9 проміжних маршрутизаторів

32. Зупинив захоплення пакетів. Помітивши певну послідовність полів TTL для пакетів:

No.	Time	Source	Destination	Protocol	Length	Info
2137	12.819347	192.168.0.103	142.250.203.206	ICMP	106	Echo (ping) request id=0x0001, seq=13/3328, ttl=1 (no response found!)
2138	12.822441	192.168.0.1	192.168.0.103	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
2139	12.824910	192.168.0.103	142.250.203.206	ICMP	106	Echo (ping) request id=0x0001, seq=14/3584, ttl=1 (no response found!)
2140	12.826582	192.168.0.1	192.168.0.103	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
2141	12.827593	192.168.0.103	142.250.203.206	ICMP	106	Echo (ping) request id=0x0001, seq=15/3840, ttl=1 (no response found!)
2144	12.831447	192.168.0.1	192.168.0.103	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
2150	12.848703	192.168.0.1	192.168.0.103	ICMP	120	Destination unreachable (Port unreachable)
2165	14.358705	192.168.0.1	192.168.0.103	ICMP	120	Destination unreachable (Port unreachable)
2170	15.868048	192.168.0.1	192.168.0.103	ICMP	120	Destination unreachable (Port unreachable)
2199	18.382291	192.168.0.103	142.250.203.206	ICMP	106	Echo (ping) request id=0x0001, seq=16/4096, ttl=2 (no response found!)
2200	18.393887	10.10.10.11	192.168.0.103	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
2201	18.394652	192.168.0.103	142.250.203.206	ICMP	106	Echo (ping) request id=0x0001, seq=17/4352, ttl=2 (no response found!)
2203	18.396715	10.10.10.11	192.168.0.103	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
2204	18.397407	192.168.0.103	142.250.203.206	ICMP	106	Echo (ping) request id=0x0001, seq=18/4608, ttl=2 (no response found!)
2206	18.400406	10.10.10.11	192.168.0.103	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
4451	23.941482	192.168.0.103	142.250.203.206	ICMP	106	Echo (ping) request id=0x0001, seq=19/4864, ttl=3 (no response found!)
4453	24.004297	194.44.229.201	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4455	24.005474	192.168.0.103	142.250.203.206	ICMP	106	Echo (ping) request id=0x0001, seq=20/5120, ttl=3 (no response found!)
4456	24.020197	194.44.229.201	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4457	24.021627	192.168.0.103	142.250.203.206	ICMP	106	Echo (ping) request id=0x0001, seq=21/5376, ttl=3 (no response found!)
4458	24.039683	194.44.229.201	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4462	24.059954	10.10.10.11	192.168.0.103	ICMP	120	Destination unreachable (Port unreachable)
4481	25.571376	10.10.10.11	192.168.0.103	ICMP	120	Destination unreachable (Port unreachable)
4485	27.084273	10.10.10.11	192.168.0.103	ICMP	120	Destination unreachable (Port unreachable)
4503	29.579676	192.168.0.103	142.250.203.206	ICMP	106	Echo (ping) request id=0x0001, seq=22/5632, ttl=4 (no response found!)
4504	29.593425	194.44.212.36	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4505	29.595132	192.168.0.103	142.250.203.206	ICMP	106	Echo (ping) request id=0x0001, seq=23/5888, ttl=4 (no response found!)
4507	29.608520	194.44.212.36	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4508	29.609822	192.168.0.103	142.250.203.206	ICMP	106	Echo (ping) request id=0x0001, seq=24/6144, ttl=4 (no response found!)
4510	29.625367	194.44.212.36	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4518	29.655157	10.10.10.11	192.168.0.103	ICMP	120	Destination unreachable (Port unreachable)
4524	31.155929	10.10.10.11	192.168.0.103	ICMP	120	Destination unreachable (Port unreachable)
4529	32.667793	10.10.10.11	192.168.0.103	ICMP	120	Destination unreachable (Port unreachable)
5990	35.165817	192.168.0.103	142.250.203.206	ICMP	106	Echo (ping) request id=0x0001, seq=25/6400, ttl=5 (no response found!)
5991	35.189342	209.85.168.96	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5992	35.190835	192.168.0.103	142.250.203.206	ICMP	106	Echo (ping) request id=0x0001, seq=26/6656, ttl=5 (no response found!)
5993	35.213781	209.85.168.96	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5994	35.215376	192.168.0.103	142.250.203.206	ICMP	106	Echo (ping) request id=0x0001, seq=27/6912, ttl=5 (no response found!)

дійшов наступного висновку. Утиліта tracert використовує ICMP-пакети для відстеження маршруту до пункту призначення. Кожен пакет має поле TTL (Time to Live), яке визначає, скільки маршрутизаторів може пройти пакет перед викиданням. Починаючи з TTL = 1, кожен маршрутизатор, через який

проходить пакет, зменшує TTL на одиницю, і якщо TTL стає рівним нулю, маршрутизатор відкидає пакет та надсилає повідомлення про помилку назад.

33. Стандартна утиліта `ping` сама по собі не надає детальної інформації про маршрут, яким пакети досягають місця призначення. `ping` в основному перевіряє доступність хоста, надсилаючи повідомлення ICMP Echo Request і очікуючи повідомлень ICMP Echo Reply.

**Висновок:** Під час виконання лабораторної роботи я здобув практичні навички з інтерпретації IP-пакетів і повідомлень керуючих протоколів, а також використання консольних утиліт для діагностики мережі на мережевому рівні.