

**Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут**

«Безпека комп'ютерних мереж»

Лабораторна робота №3.1
Варіант 5.2

«Дослідження мережного трафіка за допомогою Wireshark»

Виконала:
студентка групи ФБ-95
Гурджия Валерія Вахтангівна

1. Перевірка досяжності деякої IP-адреси в межах локальної мережі.

Очистимо ARP-кеш

```
C:\Windows\system32>arp -d
```

Перевіримо досяжність до адреси з ARP-таблиці

```
C:\Windows\system32>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.3.1: bytes=32 time=3ms TTL=64
Reply from 192.168.3.1: bytes=32 time=2ms TTL=64
Reply from 192.168.3.1: bytes=32 time=2ms TTL=64
Reply from 192.168.3.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Зупинимо процес перехоплення пакетів

Применить дисплейный фильтр ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
16	3.756684	SamsungE_fd:...	Broadcast	ARP	60	Who has 192.168.3.1? Tell 192.168.3.13
17	4.036100	192.168.3.7	192.168.3.1	ICMP	74	Echo (ping) request id=0x0001, seq=84/21504, ttl=128 (reply in 2...
18	4.083106	192.168.3.7	64.233.165.1...	TCP	55	50376 → 5228 [ACK] Seq=1 Ack=1 Win=512 Len=1
19	4.156574	fe80::f255:1...	ff02::1:ff04...	ICMPv6	86	Neighbor Solicitation for fe80::ec73:a0ff:fe04:201b from f0:55:01...
20	4.174277	192.168.3.1	192.168.3.7	ICMP	74	Echo (ping) reply id=0x0001, seq=84/21504, ttl=64 (request in ...
21	4.222803	64.233.165.1...	192.168.3.7	TCP	66	5228 → 50376 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
22	5.047971	192.168.3.7	192.168.3.1	ICMP	74	Echo (ping) request id=0x0001, seq=85/21760, ttl=128 (reply in 2...
23	5.332512	192.168.3.1	192.168.3.7	ICMP	74	Echo (ping) reply id=0x0001, seq=85/21760, ttl=64 (request in ...
24	5.354977	192.168.3.7	82.102.16.174	TCP	55	63072 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a rea...

Використовуючи поле "Filter", відфільтруємо пакети по шаблону "icmp"

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
10	2.015552	192.168.3.7	192.168.3.1	ICMP	74	Echo (ping) request id=0x0001, seq=82/20992, ttl=128 (reply in 11)
11	2.086065	192.168.3.1	192.168.3.7	ICMP	74	Echo (ping) reply id=0x0001, seq=82/20992, ttl=64 (request in 10)
14	3.026522	192.168.3.7	192.168.3.1	ICMP	74	Echo (ping) request id=0x0001, seq=83/21248, ttl=128 (reply in 15)
15	3.028598	192.168.3.1	192.168.3.7	ICMP	74	Echo (ping) reply id=0x0001, seq=83/21248, ttl=64 (request in 14)
17	4.036100	192.168.3.7	192.168.3.1	ICMP	74	Echo (ping) request id=0x0001, seq=84/21504, ttl=128 (reply in 20)
20	4.174277	192.168.3.1	192.168.3.7	ICMP	74	Echo (ping) reply id=0x0001, seq=84/21504, ttl=64 (request in 17)
22	5.047971	192.168.3.7	192.168.3.1	ICMP	74	Echo (ping) request id=0x0001, seq=85/21760, ttl=128 (reply in 23)
23	5.332512	192.168.3.1	192.168.3.7	ICMP	74	Echo (ping) reply id=0x0001, seq=85/21760, ttl=64 (request in 22)

Бачимо 2 види пакетів – request і reply. Вони відрізняються заголовками Source, Destination та Info. З мого комп'ютера відправлені пакети з параметром request, отримані з параметром reply.

Кожен пакет має 4 заголовки. Ethernet показує MAC-адреси комп'ютера та адреси до якої пінгувалися. IPv4 відповідно показує IP-адреси.

IP-адреса мого комп'ютера 192.168.3.7, MAC-адреса 00:e1:8c:ad:2f:4b.

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
10	2.015552	192.168.3.7	192.168.3.1	ICMP	74	Echo (ping) request id=0x0001, seq=82/20992, ttl=128 (reply in 11)
11	2.086065	192.168.3.1	192.168.3.7	ICMP	74	Echo (ping) reply id=0x0001, seq=82/20992, ttl=64 (request in 10)
14	3.026522	192.168.3.7	192.168.3.1	ICMP	74	Echo (ping) request id=0x0001, seq=83/21248, ttl=128 (reply in 15)
15	3.028598	192.168.3.1	192.168.3.7	ICMP	74	Echo (ping) reply id=0x0001, seq=83/21248, ttl=64 (request in 14)
17	4.036100	192.168.3.7	192.168.3.1	ICMP	74	Echo (ping) request id=0x0001, seq=84/21504, ttl=128 (reply in 20)
20	4.174277	192.168.3.1	192.168.3.7	ICMP	74	Echo (ping) reply id=0x0001, seq=84/21504, ttl=64 (request in 17)
22	5.047971	192.168.3.7	192.168.3.1	ICMP	74	Echo (ping) request id=0x0001, seq=85/21760, ttl=128 (reply in 23)
23	5.332512	192.168.3.1	192.168.3.7	ICMP	74	Echo (ping) reply id=0x0001, seq=85/21760, ttl=64 (request in 22)

> Frame 10: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{28C3D4D2-6D26-41CD-B37B-156B24312684}

> Ethernet II, Src: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b), Dst: HuaweiDe_40:f1:8d (f0:55:01:40:f1:8d)

> Internet Protocol Version 4, Src: 192.168.3.7, Dst: 192.168.3.1

> Internet Control Message Protocol

2. Відключили фільтр "icmp" і з усіх отриманих в п.1 пакетів виділили пакети "arp". Зберегли пакети, що залишилися.

arp						
No.	Time	Source	Destination	Protocol	Length	Info
3	0.685113	SamsungE_fd:...	Broadcast	ARP	60	Who has 192.168.3.1? Tell 192.168.3.13
5	1.606291	IntelCor_ad:...	Broadcast	ARP	42	Who has 192.168.3.1? Tell 192.168.3.7
6	1.713191	HuaweiDe_40:...	IntelCor_ad:...	ARP	42	192.168.3.1 is at f0:55:01:40:f1:8d
16	3.756684	SamsungE_fd:...	Broadcast	ARP	60	Who has 192.168.3.1? Tell 192.168.3.13
25	5.600772	HuaweiDe_40:...	Broadcast	ARP	60	Who has 192.168.3.3? Tell 192.168.3.1

3. Перевірка досяжності хоста за межами локальної мережі.

Очистили ARP-кеш та DNS-кеш

```
C:\Windows\system32>arp -d

C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

Перевірили досяжність хоста its.ua

```
C:\Windows\system32>ping itc.ua

Pinging itc.ua [104.21.92.13] with 32 bytes of data:
Reply from 104.21.92.13: bytes=32 time=8ms TTL=60
Reply from 104.21.92.13: bytes=32 time=3ms TTL=60
Reply from 104.21.92.13: bytes=32 time=3ms TTL=60
Reply from 104.21.92.13: bytes=32 time=3ms TTL=60

Ping statistics for 104.21.92.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 8ms, Average = 4ms
```

Зупинили перехоплення пакетів та відфільтрували пакети за умовою "arp or icmp or dns".

По протоколу ARP хост отримав MAC-адресу 00:e1:8c:ad:2f:4b

icmp or arp or dns						
No.	Time	Source	Destination	Protocol	Length	Info
10	4.916940	f0:55:01:40:f1:8d	00:e1:8c:ad:2f:4b	ARP	42	Who has 192.168.3.7? Tell 192.168.3.1
11	4.916986	00:e1:8c:ad:2f:4b	f0:55:01:40:f1:8d	ARP	42	192.168.3.7 is at 00:e1:8c:ad:2f:4b
17	5.836019	b4:07:f9:fd:2a:48	ff:ff:ff:ff:ff:ff	ARP	60	Who has 192.168.3.1? Tell 192.168.3.13
12	5.191062	192.168.3.7	192.168.3.1	DNS	66	Standard query 0x520a A itc.ua
14	5.198971	192.168.3.1	192.168.3.7	DNS	98	Standard query response 0x520a A itc.ua A 104.21.92.13 A 172.67...
15	5.214753	192.168.3.7	104.21.92.13	ICMP	74	Echo (ping) request id=0x0001, seq=146/37376, ttl=128 (reply i...
16	5.222827	104.21.92.13	192.168.3.7	ICMP	74	Echo (ping) reply id=0x0001, seq=146/37376, ttl=60 (request ...
18	6.244159	192.168.3.7	104.21.92.13	ICMP	74	Echo (ping) request id=0x0001, seq=147/37632, ttl=128 (reply i...
19	6.247610	104.21.92.13	192.168.3.7	ICMP	74	Echo (ping) reply id=0x0001, seq=147/37632, ttl=60 (request ...
20	7.262533	192.168.3.7	104.21.92.13	ICMP	74	Echo (ping) request id=0x0001, seq=148/37888, ttl=128 (reply i...
21	7.265896	104.21.92.13	192.168.3.7	ICMP	74	Echo (ping) reply id=0x0001, seq=148/37888, ttl=60 (request ...
24	8.283797	192.168.3.7	104.21.92.13	ICMP	74	Echo (ping) request id=0x0001, seq=149/38144, ttl=128 (reply i...
25	8.286975	104.21.92.13	192.168.3.7	ICMP	74	Echo (ping) reply id=0x0001, seq=149/38144, ttl=60 (request ...

4. Трасування деякої адреси за межами локальної мережі.

Виконали команду tracert

```
C:\Windows\system32>tracert wikipedia.org

Tracing route to wikipedia.org [91.198.174.192]
over a maximum of 30 hops:

  1     3 ms     3 ms     4 ms    192.168.3.1
  2    68 ms     7 ms    23 ms    mx960-ri-clients.lanet [10.0.255.255]
  3     4 ms     7 ms     5 ms    194.33.189.15
  4     3 ms     5 ms     8 ms    ae1-210.RT.BMB.KIV.UA.retn.net [87.245.247.158]
  5    44 ms    47 ms    39 ms    ae5-10.RT.TC2.AMS.NL.retn.net [87.245.234.113]
  6    39 ms    38 ms    46 ms    ae2.cr2-esams.wikimedia.org [80.249.209.176]
  7    43 ms    40 ms    57 ms    text-lb.esams.wikimedia.org [91.198.174.192]

Trace complete.
```

В перехопленні traceroute зустрічаються пакети icmp (для перевірки зв'язку з хостом) та dns (для отримання IP-адреси з імені хоста).

У пакетах ping перевіряється з'єднання з одним хостом, а у traceroute йде перевірка з кожним проміжним маршрутизатором, доки не дійде до кінцевої цілі. У заголовку протоколу ICMP встановлено TTL 1. Такий echo запит утиліта traceroute відправляє 3 рази. Потім з кожним разом TTL збільшується на 1, доки пакет не дійде до потрібної адреси.

icmp or dns						
No.	Time	Source	Destination	Protocol	Length	Info
4	0.726005	192.168.3.7	192.168.3.1	DNS	73	Standard query 0x6c9f A wikipedia.org
5	0.764035	192.168.3.1	192.168.3.7	DNS	89	Standard query response 0x6c9f A wikipedia.org A 91.198.174.192
6	0.813736	192.168.3.7	91.198.174.192	ICMP	106	Echo (ping) request id=0x0001, seq=462/52737, ttl=1 (no response found!)
7	0.815517	192.168.3.1	192.168.3.7	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
8	0.819153	192.168.3.7	91.198.174.192	ICMP	106	Echo (ping) request id=0x0001, seq=463/52993, ttl=1 (no response found!)
9	0.825118	192.168.3.1	192.168.3.7	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
10	0.829670	192.168.3.7	91.198.174.192	ICMP	106	Echo (ping) request id=0x0001, seq=464/53249, ttl=1 (no response found!)
11	0.831419	192.168.3.1	192.168.3.7	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12	0.836267	192.168.3.7	192.168.3.1	DNS	84	Standard query 0x8851 PTR 1.3.168.192.in-addr.arpa
13	0.838397	192.168.3.1	192.168.3.7	DNS	84	Standard query response 0x8851 No such name PTR 1.3.168.192.in-addr.arpa
1114	6.364513	192.168.3.7	91.198.174.192	ICMP	106	Echo (ping) request id=0x0001, seq=465/53505, ttl=2 (no response found!)
1115	6.367046	10.0.255.255	192.168.3.7	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1116	6.369981	192.168.3.7	91.198.174.192	ICMP	106	Echo (ping) request id=0x0001, seq=466/53761, ttl=2 (no response found!)
1119	6.373772	10.0.255.255	192.168.3.7	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1120	6.376221	192.168.3.7	91.198.174.192	ICMP	106	Echo (ping) request id=0x0001, seq=467/54017, ttl=2 (no response found!)
1121	6.379513	10.0.255.255	192.168.3.7	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1122	6.382673	192.168.3.7	192.168.3.1	DNS	85	Standard query 0xbce6 PTR 255.255.0.10.in-addr.arpa
1123	6.384402	192.168.3.1	192.168.3.7	DNS	121	Standard query response 0xbce6 PTR 255.255.0.10.in-addr.arpa

5. Фрагментація

```
C:\Windows\system32>ping -l 4000 -n 1 wikipedia.org

Pinging wikipedia.org [91.198.174.192] with 4000 bytes of data:
Request timed out.

Ping statistics for 91.198.174.192:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
```

ip.flags.mf==1 or ip.frag_offset!=0						
No.	Time	Source	Destination	Protocol	Length	Info
55	0.902751	192.168.3.7	91.198.174....	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=ead3) [Reassembled in #57]
56	0.902751	192.168.3.7	91.198.174....	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=ead3) [Reassembled in #57]
57	0.902751	192.168.3.7	91.198.174....	ICMP	1082	Echo (ping) request id=0x0001, seq=574/15874, ttl=128 (no response found!)

```
C:\Windows\system32>ping -n 1 -i 3 wikipedia.org

Pinging wikipedia.org [91.198.174.192] with 32 bytes of data:
Reply from 194.33.189.15: TTL expired in transit.

Ping statistics for 91.198.174.192:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
23	0.802927	192.168.3.7	91.198.174....	ICMP	74	Echo (ping) request id=0x0001, seq=576/16386, ttl=3 (no response found!)
24	0.810624	194.33.189....	192.168.3.7	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

6. DHCP

Звільнення IPv4-адреси для вказаного адаптера.

```
C:\Windows\system32>ipconfig /release
```

Windows IP Configuration

Оновлення IPv4 адреси для вказаного адаптера.

```
C:\Windows\system32>ipconfig /renew
```

Windows IP Configuration

dhcp						
No.	Time	Source	Destination	Protoco	Length	Info
1...	5.336360	192.168.3.15	192.168.3.1	DHCP	342	DHCP Release - Transaction ID 0x93ff2f4e
1...	9.760888	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xfc350828
1...	9.775101	192.168.3.1	192.168.3.15	DHCP	328	DHCP Offer - Transaction ID 0xfc350828
1...	9.776598	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xfc350828
1...	9.815235	192.168.3.1	192.168.3.15	DHCP	378	DHCP ACK - Transaction ID 0xfc350828

Відповіді на запитання:

1. Протокол ICMP:

Опишіть формат пакета і призначення полів заголовка протоколу ICMP.

- Type – тип повідомлення (розмір: 1 байт)
- Code – конкретизує назначення повідомлення (розмір: 1 байт)
- Checksum – контрольна сума. Використовується для того, щоб переконатися, що вміст заголовка ICMP і дані не пошкоджені після прибуття (розмір: 2 байти).
- Additional information - частина, яка змінюється залежно від полів Тип і Код.

Якою є IP адреса вашого комп'ютера? Якою є IP адреса хоста призначення?

IP-адреса мого комп'ютера 192.168.3.7, IP-адреса хоста призначення 192.168.3.1

Source	Destination	Protocol	Length	Info
192.168.3.7	192.168.3.1	ICMP	74	Echo (ping) request id=0x0001, seq=82/20992, ttl=128 (reply in 2)

Які види ICMP повідомлень вам зустрічалися. Які значення "тип" і "код" вони мають.

У ході виконання лабораторної роботи мені зустрічалися «echo (ping) request» (запит), «echo (ping) reply» (відповідь) та «Time-to-live exceeded» (перевищен час очікування).

Type: 8 (Echo (ping) request)

Code: 0

Type: 0 (Echo (ping) reply)

Code: 0

Type: 11 (Time-to-live exceeded)

Code: 0 (Time to live exceeded in transit)

Яким є тип і код ICMP пакету, що був відправлений вами?

У відправлених запитах «echo (ping) request» type 8, code 0.

Яким є тип і код ICMP пакету, що був отриманий вами у відповідь?

У одержуваних відповідях «echo (ping) reply» type 0, code 0.

Чи змінюються в процесі виконання команди розміри заголовка IP і повідомлень ICMP. Чим можна пояснити дану ситуацію.

Пакети мають фіксований розмір, розміри заголовків не змінюються.

На прикладі серії echo - запитів покажіть, які поля в заголовку IP-датограми змінюються.

Візьмемо до прикладу перший та останній echo-запит:

Internet Protocol Version 4, Src: 192.168.3.7, Dst: 192.168.3.1	Internet Protocol Version 4, Src: 192.168.3.7, Dst: 192.168.3.1
0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 60 Identification: <u>0xbf94 (49044)</u> > Flags: 0x00 ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 128 Protocol: ICMP (1) Header Checksum: <u>0xf3d3</u> [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.3.7 Destination Address: 192.168.3.1	0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 60 Identification: <u>0xbf97 (49047)</u> > Flags: 0x00 ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 128 Protocol: ICMP (1) Header Checksum: <u>0xf3d0</u> [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.3.7 Destination Address: 192.168.3.1

Бачимо, що змінюються поля Identification (з кожним запитом збільшується на 1) та Header Checksum.

На прикладі серії echo - відповідей визначте, якими є значення полів ідентифікатора (Identification) та TTL.

Візьмемо до прикладу першу та останню echo-відповідь:

```
Internet Protocol Version 4, Src: 192.168.3.1, Dst: 192.168.3.7
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x01e2 (482)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xf186 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.3.1
    Destination Address: 192.168.3.7
```

```
Internet Protocol Version 4, Src: 192.168.3.1, Dst: 192.168.3.7
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x0261 (609)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xf107 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.3.1
    Destination Address: 192.168.3.7
```

Бачимо, що TTL залишається сталим, а Identification з кожною відповіддю збільшується.

Яким чином ведуть себе значення полів ідентифікатора та номера послідовності в заголовках ICMP захоплених кадрів.

```
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 82 (0x0052)
Sequence Number (LE): 20992 (0x5200)
```

Заголовки Identifier залишаються сталими, Sequence Number з кожним запитом збільшуються.

Опишіть роботу утиліт ping і traceroute (tracert). В чому їх відмінність.

Ping використовується для перевірки підключення до іншого комп'ютера на рівні IP.

Traceroute дозволяє простежити маршрут проходження даних до віддаленого адресата в мережах TCP/IP.

Якими параметрами відрізняються кілька послідовних echo-запитів.

Взяли до прикладу перший та другий echo-запити.

```
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d09 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 82 (0x0052)
  Sequence Number (LE): 20992 (0x5200)
```

```
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d08 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 83 (0x0053)
  Sequence Number (LE): 21248 (0x5300)
```

Як бачимо, вони відрізняються полями Checksum, Sequence Number (BE) та Checksum, Sequence Number (DE)

Опишіть пакети, що передаються traceroute (tracert) і одержані у відповідь.

Спочатку у заголовку протоколу ICMP встановлено TTL 1. Такий echo запит утиліта traceroute відправляє 3 рази. Потім з кожним разом TTL збільшується на 1, доки пакет не дійде до потрібної адреси. Поки не дійдемо до кінцевого маршрутизатора, у відповідь одержуються ICMP протоколи з Time-to-live exceeded. Потім отримуємо відповіді, як у звичайному ping.

З якою метою вузли надсилають ICMP повідомлення "type11".

Type: 11 (Time-to-live exceeded)

Щоб повідомити про те, що час життя пакету завершився.

Поясніть призначення параметрів -r і -s в команді ping.

-r Запис маршруту для вказаної кількості переходів

-s Задає довжину пакетів. Ця опція застосовується для перевірки роботи функцій фрагментації та повторного збирання пакетів.

Яким чином в кадрах передається штамп часу.

Час фіксується у заголовку Frame

```
Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on  
> Interface id: 0 (\Device\NPF_{28C3D4D2-6D26-41CD-B37B-156B2431268}  
Encapsulation type: Ethernet (1)  
Arrival Time: May 14, 2022 18:44:33.556474000 FLE Daylight Time  
[Time shift for this packet: 0.000000000 seconds]  
Epoch Time: 1652543073.556474000 seconds
```

2. Ethernet – фрейм:

В одному з перехоплених пакетів вкажіть поля заголовка Ethernet і поясніть призначення цих полів.

- Destination: показує MAC-адресу отримувача пакету (розмір: 6 байтів).
- Source: показує MAC-адресу відправника пакету (розмір: 2 байтів).
- Type: ідентифікує тип протоколу (розмір: 2 байти).

Яка версія технології Ethernet використовується у вашій мережі.

Ethernet II

Які розміри кадрів Ethernet, заголовків IP і повідомлень ICMP, чи змінюються вони в послідовності пакетів, що генеруються при виконанні команди.

розмір Ethernet – 14 байт (не змінюється), IP – 20 байт (не змінюється), ICMP (може змінюватись в залежності від повідомлення).

Яким у фреймі є значення поля протоколу верхнього рівня. Які ще значення зустрічаються в перехоплених пакетах (відповісти після виконання всього завдання).

В Ethernet Type: IPv4 (0x0800), зустрічалося Type: ARP (0x0806)

Яку MAC-адресу має мережна карта вашого комп'ютера, а яку маршрутизатор мережі.

мережна карта комп'ютера: 00:e1:8c:ad:2f:4b

мережна карта маршрутизатора мережі: f0:55:01:40:f1:8d

```
Ethernet II, Src: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b), Dst: HuaweiDe_40:f1:8d (f0:55:01:40:f1:8d)
```

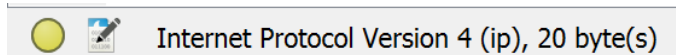
3. Протокол IP:

Опишіть формат і значення полів заголовка IP- датаграми.

- Version – версія IP-адреси, що використовується (розмір: 1 байт).
- Header Length – довжина заголовка IP (розмір: 1 байт).
- Differentiated Services Field – тип служби. Використовується маршрутизаторами для визначення пріоритетності трафіку (розмір: 1 байт).
- Total Length – довжина IP-заголовка та даних, що містяться в пакеті (розмір: 2 байти).
- Identification – унікальний ідентифікаційний номер, що використовується для ідентифікації пакета (розмір: 2 байти).
- Flags – Прапори. Використовуються для визначення того, чи є пакет частиною послідовності фрагментованих пакетів (розмір: 3 біта).
- Fragment Offset – Зміщення фрагмента (розмір: 13 біт).
- Time to Live – визначає тривалість життя пакета (розмір: 1 байт).
- Protocol – протокол. Визначає заголовок транспортного рівня, який інкапсулює заголовок IPv4 (розмір: 1 байт).
- Header Checksum – контрольна сума заголовка. Використовується для перевірки того, що вміст заголовка IP не пошкоджено (розмір: 2 байти).
- Source Address – IP-адреса джерела (розмір: 4 байти).
- Destination Address – IP-адреса призначення (розмір: 4 байти).

Який розмір має стандартний IP заголовок? Скільки байтів містять дані корисного навантаження IP дейтаграми? Поясніть будь-ласка, як ви це визначили.

20 байт



Які поля заголовка змінюються в послідовності IP датаграм, а які залишаються незмінними в кожному пакеті трафіка.

Взяли до прикладу 2 echo-запити, бачимо, що відрізняються поля Identification та Header Checksum.

```
Internet Protocol Version 4, Src: 192.168.3.7, Dst: 192.168.3.1
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0xbf94 (49044)
> Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0xf3d3 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.3.7
Destination Address: 192.168.3.1
```

```
Internet Protocol Version 4, Src: 192.168.3.7, Dst: 192.168.3.1
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0xbf95 (49045)
> Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0xf3d2 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.3.7
Destination Address: 192.168.3.1
```

Якими є значення полів ідентифікатора та TTL.

Якщо взяти до прикладу echo-запити, то можна побачити, що якщо був виконаний звичайний ping, то з кожним запитом поле ідентифікатора збільшується на 1, а TTL = 128 (залишається сталим). Якщо була виконана

команда `tracert`, то значення TTL буде збільшуватись з кожними трьома запитами на 1, поки не дійде до потрібного маршрутизатора.

4. Протокол ARP:

Опишіть формат пакета і призначення полів заголовка протоколу ARP.

- Hardware type – тип обладнання (розмір: 2 байти)
- Protocol type – тип протоколу. Протокол вищого рівня, для якого використовується запит ARP (розмір: 2 байти)
- Hardware size – довжина MAC-адреси (розмір: 1 байт)
- Protocol size – довжина адреси протоколу (розмір: 1 байт)
- Opcode – операція. Функція ARP-пакета: 1 для запиту або 2 для відповіді (розмір: 2 байти)
- Sender MAC – MAC-адреса відправника (розмір: 6 байт)
- Sender IP address – IP-адреса відправника (розмір: 4 байти)
- Target MAC address – MAC-адреса отримувача (розмір: 6 байти)
- Target IP address – IP-адреса отримувача (розмір: 4 байти)

Яке значення поля "тип протоколу" в кадрі Ethernet вказує на протокол ARP.

```
Ethernet II, Src: SamsungE_fd:2a:48 (b4:07:f9:fd:2a:48), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)
> Source: SamsungE_fd:2a:48 (b4:07:f9:fd:2a:48)
Type: ARP (0x0806)
Padding: 00000000000000000000000000000000
```

Яким полем ідентифікуються (відрізняються) запит і відповідь ARP.

Opcode

Address Resolution Protocol (request)	Address Resolution Protocol (reply)
Hardware type: Ethernet (1)	Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)	Protocol type: IPv4 (0x0800)
Hardware size: 6	Hardware size: 6
Protocol size: 4	Protocol size: 4
<u>Opcode: request (1)</u>	<u>Opcode: reply (2)</u>
Sender MAC address: SamsungE_fd:2a:48 (b4:07:f9:fd:2a:48)	Sender MAC address: HuaweiDe_40:f1:8d (f0:55:01:40:f1:8d)
Sender IP address: 192.168.3.13	Sender IP address: 192.168.3.1
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)	Target MAC address: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b)
Target IP address: 192.168.3.1	Target IP address: 192.168.3.7

Які значення полів встановлює відправник в ARP-запиті і отримує в ARP-відповіді.

ARP-запит:

1	0.000000	SamsungE_fd::...	Broadcast	ARP	60	Who has 192.168.3.1? Tell 192.168.3.13
2	0.921178	IntelCor_ad::...	Broadcast	ARP	42	Who has 192.168.3.1? Tell 192.168.3.7
3	1.028078	HuaweiDe 40::...	IntelCor ad:2f::	ARP	42	192.168.3.1 is at f0:55:01:40:f1:8d

```
> Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{28C3D4D2-
> Ethernet II, Src: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b)
    Sender IP address: 192.168.3.7
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.3.1
```

ARP-відповідь:

1	0.000000	SamsungE_fd:...	Broadcast	ARP	60	Who has 192.168.3.1? Tell 192.168.3.13
2	0.921178	IntelCor_ad:...	Broadcast	ARP	42	Who has 192.168.3.1? Tell 192.168.3.7
3	1.028078	HuaweiDe_40:...	IntelCor_ad:2f:...	ARP	42	192.168.3.1 is at f0:55:01:40:f1:8d

> Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{28C3D4D2-6D26-41CD-B37B-156B24312684}, Ethernet II, Src: HuaweiDe_40:f1:8d (f0:55:01:40:f1:8d), Dst: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b)

▼ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: HuaweiDe_40:f1:8d (f0:55:01:40:f1:8d)
Sender IP address: 192.168.3.1
Target MAC address: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b)
Target IP address: 192.168.3.7

Знайдіть повідомлення ARP, що було надіслано у відповідь на деякий запит ARP.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	SamsungE_f...	Broadcast	ARP	60	Who has 192.168.3.1? Tell 192.168.3.13
2	0.921178	IntelCor_a...	Broadcast	ARP	42	Who has 192.168.3.1? Tell 192.168.3.7
3	1.028078	HuaweiDe_4...	IntelCor_a...	ARP	42	192.168.3.1 is at f0:55:01:40:f1:8d
4	3.071571	SamsungE_f...	Broadcast	ARP	60	Who has 192.168.3.1? Tell 192.168.3.13
5	4.915659	HuaweiDe_4...	Broadcast	ARP	60	Who has 192.168.3.3? Tell 192.168.3.1

> Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{28C3D4D2-6D26-41CD-B37B-156B24312684}, Ethernet II, Src: HuaweiDe_40:f1:8d (f0:55:01:40:f1:8d), Dst: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b)

▼ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: HuaweiDe_40:f1:8d (f0:55:01:40:f1:8d)
Sender IP address: 192.168.3.1
Target MAC address: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b)
Target IP address: 192.168.3.7

Які значення мають адреса відправника і адреса одержувача в кадрах Ethernet, що містять повідомлення ARP?

ARP-запит

2	0.921178	IntelCor_ad:2f:4b	Broadcast	ARP	42	Who has 192.168.3.1? Tell 192.168.3.7
3	1.028078	HuaweiDe_40:f1:8d	IntelCor_ad:2f:4b	ARP	42	192.168.3.1 is at f0:55:01:40:f1:8d

> Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{28C3D4D2-6D26-41CD-B37B-156B24312684}, Ethernet II, Src: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Destination: Broadcast (ff:ff:ff:ff:ff:ff)
> Source: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b)
Type: ARP (0x0806)

ARP-відповідь

2	0.921178	IntelCor_ad:2f:4b	Broadcast	ARP	42	Who has 192.168.3.1? Tell 192.168.3.7
3	1.028078	HuaweiDe_40:f1:8d	IntelCor_ad:2f:4b	ARP	42	192.168.3.1 is at f0:55:01:40:f1:8d

> Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{28C3D4D2-6D26-41CD-B37B-156B24312684}, Ethernet II, Src: HuaweiDe_40:f1:8d (f0:55:01:40:f1:8d), Dst: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b)

> Destination: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b)
> Source: HuaweiDe_40:f1:8d (f0:55:01:40:f1:8d)
Type: ARP (0x0806)

Чи містить ARP повідомлення IP адресу відправника.

Так

```
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: HuaweiDe_40:f1:8d (f0:55:01:40:f1:8d)
  Sender IP address: 192.168.3.1
  Target MAC address: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b)
  Target IP address: 192.168.3.7
```

З якого байту кадру Ethernet починається поле opcode? Які значення має поле opcode в різних ARP пакетах?

Поле opcode починається з 7 байту.

Має значення reply (2) та request (1)

Перевірте вміст ARP - кеша комп'ютера. Прокоментуйте результат. Як очистити вміст ARP - кеша.

Вміст ARP - кеша комп'ютера перевіряється командою arp -a

```
C:\Windows\system32>arp -a

Interface: 192.168.3.15 --- 0x5
   Internet Address      Physical Address      Type
192.168.3.1              f0-55-01-40-f1-8d    dynamic
192.168.3.6              c4-57-6e-76-18-10    dynamic
192.168.3.85             d0-5f-64-d1-9b-00    dynamic
192.168.3.255            ff-ff-ff-ff-ff-ff    static
224.0.0.2                01-00-5e-00-00-02    static
224.0.0.22               01-00-5e-00-00-16    static
224.0.0.251              01-00-5e-00-00-fb    static
224.0.0.252              01-00-5e-00-00-fc    static
239.255.255.250          01-00-5e-7f-ff-fa    static
255.255.255.255          ff-ff-ff-ff-ff-ff    static
```

Очищаємо кеш командою arp -d

```
C:\Windows\system32>arp -d

Interface: 192.168.3.15 --- 0x5
   Internet Address      Physical Address      Type
224.0.0.22               01-00-5e-00-00-16    static
```

5. Фрагментація пакетів:

Чи фрагментуються IP-датаграми, що відправляються вашим вузлом.

Так

Як визначити, що деяка IP датаграма була фрагментована і які поля заголовка IP на це вказують. Якої довжини була ця IP датаграма?

```
Identification: 0xead3 (60115)
Flags: 0x20, More fragments
...0 0101 1100 1000 = Fragment Offset: 1480
```

У фрагментах поле Identification однакове, поле Flags вказує на те, що далі є ще фрагменти, Fragment offset показує зміщення фрагменту, у всіх фрагментах, окрім першого, це поле буде ненульовим.

Виведіть перший фрагмент фрагментованої IP датаграми.

```
Internet Protocol Version 4, Src: 192.168.3.7, Dst: 91.198.174.192
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xead3 (60115)
  > Flags: 0x20, More fragments
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x5c17 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.3.7
    Destination Address: 91.198.174.192
```

Виведіть другий фрагмент. Яка інформація покаже, що це не перший фрагмент?

```
Internet Protocol Version 4, Src: 192.168.3.7, Dst: 91.198.174.192
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xead3 (60115)
  > Flags: 0x20, More fragments
    ...0 0101 1100 1000 = Fragment Offset: 1480
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x5b5e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.3.7
    Destination Address: 91.198.174.192
```

Чи існують ще якісь фрагменти? Чому?

Ще є останній фрагмент, в якому є заголовок протоколу пакета.

No.	Time	Source	Destination	Protocol	Length	Info
• 1	0.000000	192.168.3.7	91.198.174.192	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=ead3) [Reassembled in #3]
• 2	0.000000	192.168.3.7	91.198.174.192	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=ead3) [Reassembled in #...
• 3	0.000000	192.168.3.7	91.198.174.192	ICMP	1082	Echo (ping) request id=0x0001, seq=574/15874, ttl=128 (no response found!)
Frame 3: 1082 bytes on wire (8656 bits), 1082 bytes captured (8656 bits) on interface \Device\NPF_{28C3D4D2-6D26-41CD-B37B-156B24312684}, ic...						
Ethernet II, Src: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b), Dst: HuaweiDe_40:f1:8d (f0:55:01:40:f1:8d)						
▼	Internet Protocol Version 4, Src: 192.168.3.7, Dst: 91.198.174.192					
	0100 = Version: 4					
 0101 = Header Length: 20 bytes (5)					
	> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
	Total Length: 1068					
	Identification: 0xead3 (60115)					
	> Flags: 0x01					
	...0 1011 1001 0000 = Fragment Offset: 2960					
	Time to Live: 128					
	Protocol: ICMP (1)					
	Header Checksum: 0x7c55 [validation disabled]					
	[Header checksum status: Unverified]					
	Source Address: 192.168.3.7					
	Destination Address: 91.198.174.192					
	> [3 IPv4 Fragments (4008 bytes): #1(1480), #2(1480), #3(1048)]					
▼	Internet Control Message Protocol					

Яке поле змінилося в заголовку IP в першому і другому фрагментах.
Fragment offset та Header Checksum.

Які поля змінюються в IP заголовку у фрагментах?

Fragment offset, Header Checksum, Total Length та Flags.

Скільки фрагментів було створено з оригінальної датаграми?

3 фрагменти.

Які розміри різних фрагментів однієї і тієї ж датаграми.

У першому та другому фрагментах: 1500 байт, у третьому: 1068 байт.
Чи змінюється ідентифікатор датаграми в її фрагментах і яке його значення.

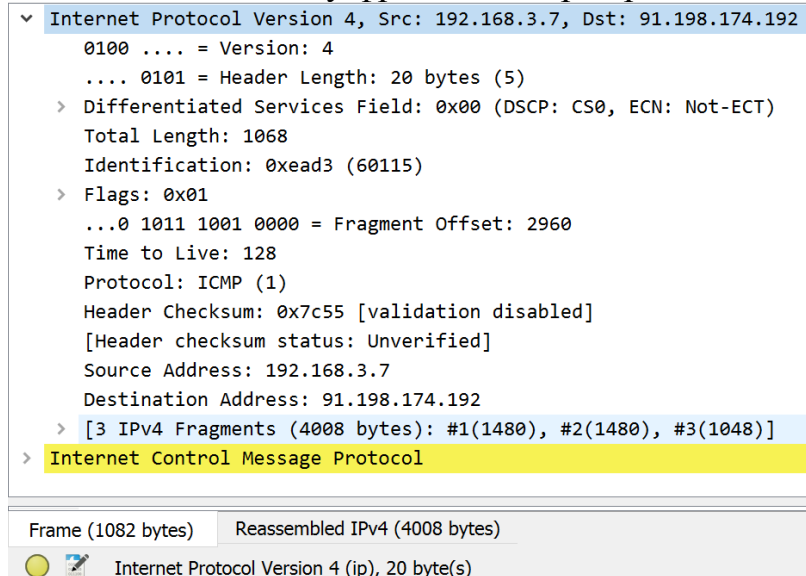
Ідентифікатор не змінюється. Значення = 0xead3 (60115).

Які поля заголовка IP призначені для збірки вихідної датаграми з фрагментів в правильній послідовності.

Fragment offset

Як визначити розмір вихідної датаграми, що була фрагментована.

Можна в останньому фрагменті перевірити останнє поле заголовка IP- датаграми



У яких фрагментах вихідної датаграми присутній заголовок ICMP.

В останньому.

Як змінюється поле «час життя»?

Час життя у всіх фрагментах був однаковим

Time to Live: 128

6. Протокол DHCP:

Опишіть формат пакета і призначення полів заголовка протоколу DHCP і типи повідомлень, що передаються.

- Release – пакет, що передає повідомлення про звільнення оренди IP адреси.
 - Discover – широкомовний мережевий пакет, який клієнт відправляє з метою знайти DHCP-сервер у мережі.
 - Offer – пакет, що відправляє сервер, отримавши запит від клієнта, з IP адресою та годиною оренди.
 - Request – пакет, що відправляє клієнт серверу, з обраною IP адресою.
 - ACK – пакет підтвердження, який сервер надсилає клієнту.
-
- Message type – вказує, чи є пакет запитом DHCP чи відповіддю DHCP (розмір: 1 байт)
 - Hardware type – тип апаратного забезпечення (розмір: 1 байт)

- Hardware address length – довжина апаратної адреси (розмір: 1 байт)
- Hops – використовується агентами ретрансляції для допомоги у пошуку сервера DHCP (розмір: 1 байт)
- Transaction ID – випадкове число, яке використовується для поєднання запитів із відповідями (розмір: 4 байти)
- Second elapsed – Секунди з моменту, коли клієнт вперше запитав адресу від сервера DHCP (розмір: 2 байти)
- Bootp flags – прапори. Типи трафіку, який може приймати DHCP-клієнт (одноадресний, широкомовний тощо) (розмір: 2 байти)
- Client IP – IP-адреса клієнта, отримана з поля IP (розмір: 4 байти)
- Your (client) IP address – IP-адреса, запропонована сервером DHCP (зрештою, стає значенням поля IP-адреса клієнта) (розмір: 4 байти)
- Next server IP address – IP-адреса сервера DHCP (розмір: 4 байти)
- Relay agent IP address – IP-адреса шлюзу мережі за замовчуванням (розмір: 4 байти)
- Client MAC address – MAC-адреса клієнта (розмір: 6 байтів)
- Client hardware address padding – MAC-адреса клієнта (розмір: 10 байтів)
- Server host name - Ім'я хоста сервера (розмір: 64 байтів)
- Boot File – Завантажувальний файл для використання DHCP (розмір: 128 байтів)
- Parameters – Використовуються для розширення структури пакету DHCP, щоб надати йому більше можливостей

DHCP повідомлення відправляються через UDP або TCP пакети?

UDP

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.3.15	192.168.3.1	DHCP	342	DHCP Release - Transaction ID 0x93ff2f4e
2	4.424528	0.0.0.0	255.255.255.2...	DHCP	344	DHCP Discover - Transaction ID 0xfc350828
3	4.438741	192.168.3.1	192.168.3.15	DHCP	328	DHCP Offer - Transaction ID 0xfc350828
4	4.440238	0.0.0.0	255.255.255.2...	DHCP	370	DHCP Request - Transaction ID 0xfc350828
5	4.478875	192.168.3.1	192.168.3.15	DHCP	378	DHCP ACK - Transaction ID 0xfc350828

>	Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{28C3D4D2-6D26-41CD-B37B-156B24312684}, id 0
>	Ethernet II, Src: IntelCor_ad:2f:4b (08:e1:8c:ad:2f:4b), Dst: HuaweiDe_40:f1:8d (f0:55:01:40:f1:8d)
>	Internet Protocol Version 4, Src: 192.168.3.15, Dst: 192.168.3.1
>	User Datagram Protocol, Src Port: 68, Dst Port: 67
>	Dynamic Host Configuration Protocol (Release)

Які значення полів у повідомленні DHCP Discover відрізняють його від повідомлення DHCP Request.

Dynamic Host Configuration Protocol (Discover)

```
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0xfc350828
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: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Discover)
> Option: (61) Client identifier
> Option: (50) Requested IP Address (192.168.3.15)
> Option: (12) Host Name
> Option: (60) Vendor class identifier
> Option: (55) Parameter Request List
> Option: (255) End
```

Dynamic Host Configuration Protocol (Request)

```
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0xfc350828
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: IntelCor_ad:2f:4b (00:e1:8c:ad:2f:4b)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Request)
> Option: (61) Client identifier
> Option: (50) Requested IP Address (192.168.3.15)
> Option: (54) DHCP Server Identifier (192.168.3.1)
> Option: (12) Host Name
> Option: (81) Client Fully Qualified Domain Name
> Option: (60) Vendor class identifier
> Option: (55) Parameter Request List
> Option: (255) End
```

Як змінюється це поле в послідовності запитів. Яке значення Transaction-ID в кожному з перших чотирьох Discover/Offer/Request/ACK DHCP пакетів.

Release

Transaction ID: 0x93ff2f4e

Discover

Transaction ID: 0xfc350828

Offer

Transaction ID: 0xfc350828

Request

Transaction ID: 0xfc350828

ACK

Transaction ID: 0xfc350828

У Discover, Offer, Request та ACK значення transaction ID однакове, у Release значення інше, бо це окрема операція.

Комп'ютер використовує DHCP пакет для отримання різних мережних налаштувань, зокрема отримання IP адреси. Але ця IP адреса не затверджена до закінчення обміну в останньому четвертому повідомленні. Якщо ж це дійсно так, то яке значення IP адреси використовується для обміну початковими 4-ма повідомленнями. Для кожного з перших 4-х DHCP повідомлень (Discover/Offer/Request/ACK DHCP), визначте IP адресу відправника та адресу призначення у IP пакеті.

0.0.0.0

DHCP Discover

Source Address: 0.0.0.0

Destination Address: 255.255.255.255

DHCP Offer

Source Address: 192.168.3.1
Destination Address: 192.168.3.15

DHCP Request

Source Address: 0.0.0.0
Destination Address: 255.255.255.255

DHCP ACK

Source Address: 192.168.3.1
Destination Address: 192.168.3.15

Яка IP адреса вашого DHCP сервера.

Option: (54) DHCP Server Identifier (192.168.3.1)

Яка IP адреса пропонується DHCP сервером для вашого комп'ютера у DHCP Offer повідомленні? Вкажіть, в якому DHCP повідомленні міститься запропонована IP адреса.

В DHCP Offer міститься запропонована IP адреса

Your (client) IP address: 192.168.3.15

Поясніть призначення поля Lease time (час оренди). Наскільки довгий цей час у вашому експерименті?

Коли час оренди DHCP закінчується, комп'ютер автоматично звільняє свою IP-адресу і просить маршрутизатор дати йому новий.

✓ Option: (51) IP Address Lease Time
Length: 4

IP Address Lease Time: (86400s) 1 day

➤ Option: (58) Renewal Time Value

Яке призначення DHCP Release повідомлення? Чи DHCP сервер відправляє підтвердження отримання DHCP Release повідомлення від клієнта? Що станеться, якщо DHCP Release повідомлення буде втрачене?

Release – пакет, що передає повідомлення про звільнення оренди IP адреси.

DHCP сервер не відправляє підтвердження отримання DHCP Release повідомлення. Якщо DHCP Release повідомлення буде втрачене, то сервер не зможе відправляти йому повідомлення, бо не буде знати адресу клієнта.

Чому протокол DHCP може розпізнаватися у Wireshark як BOOTP.

Тому що протокол DHCP є розширеною версією BOOTP. BOOTP підтримує статичне налаштування IP-адрес, а DHCP підтримує динамічне налаштування.

7.

Пакети яких ще протоколів зустрічаються серед перехоплених у вашій мережі.

TCP – Transmission Control Protocol

DNS – Domain Name System

IGMP – Internet Group Management Protocol

LLMNR – Link-local Multicast Name Resolution

NetBIOS - Network Basic Input/Output System

TLS – Transport Layer Security

UDP – User Datagram Protocol

До якого рівня взаємодії відносяться дані протоколи.

Рівень програм: DHCP, DNS, LLMNR

Рівень презентації: TLS

Рівень сеансу: NetBIOS

Транспортний рівень: TCP, UDP

Мережевий рівень: ICMP, IGMP

Канальний рівень даних: ARP

Скільки заголовків може бути у кожного пакета.

В цій лабораторній роботі у пакетах було від 3 до 5 заголовків.

Визначіть, які пари MAC і IP адреси у інших хостів вашої локальної мережі.

Вони зберігаються у ARP таблиці.

```
C:\Windows\system32>arp -a


Interface: 192.168.3.15 --- 0x5
Internet Address      Physical Address      Type
192.168.3.1           f0-55-01-40-f1-8d     dynamic
192.168.3.6           c4-57-6e-76-18-10     dynamic
192.168.3.13          b4-07-f9-fd-2a-48     dynamic
192.168.3.85          d0-5f-64-d1-9b-00     dynamic
224.0.0.22            01-00-5e-00-00-16     static
239.255.255.250       01-00-5e-7f-ff-fa     static
```

Яку стандартну довжину має кожний заголовок.


20 байтів

Як відфільтрувати збережені пакети по MAC та/або IP адресі та по протоколу (arp, icmp, http, dhcp).


По MAC-адресі

 eth.addr == ff:ff:ff:ff:ff:ff

По IP-адресі

 ip.addr == 192.0.2.1

По MAC-адресі та протоколу

 eth.addr == ff:ff:ff:ff:ff:ff and http