**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**

Варіант 5.2

**Виконала**:

студентка групи ФБ-95

Гурджия Валерія Вахтангівна

**Лабораторна робота №3.1**

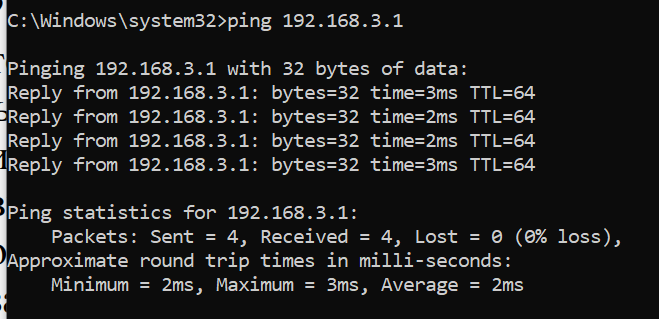
«Дослідження мережного трафіка за допомогою Wireshark»

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

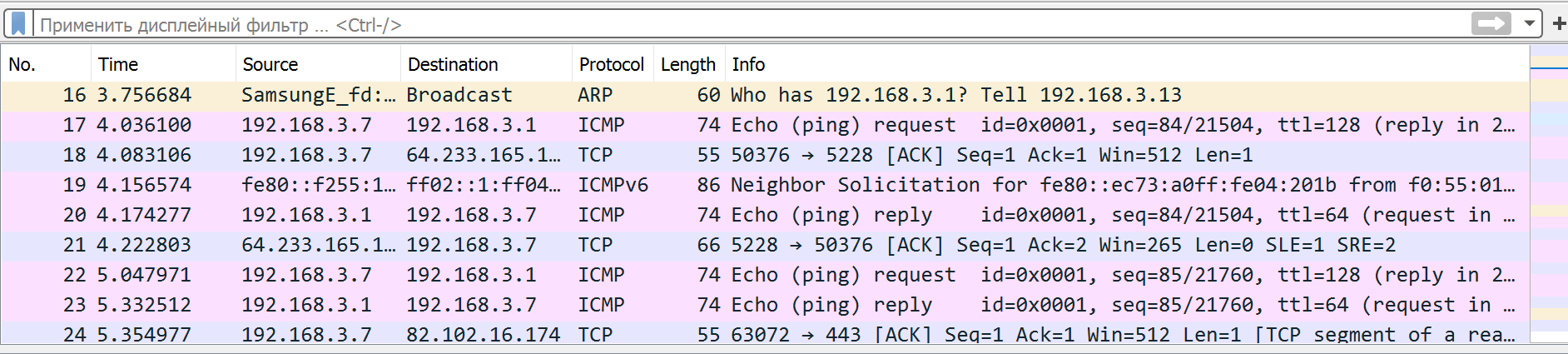
Очистимо ARP-кеш



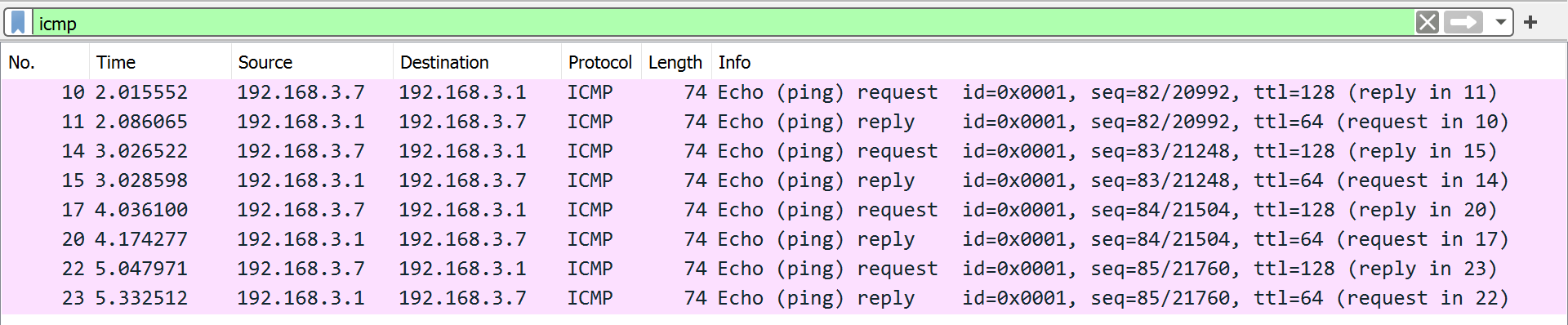
Перевіримо досяжність до адреси з ARP-таблиці



Зупинимо процес перехоплення пакетів



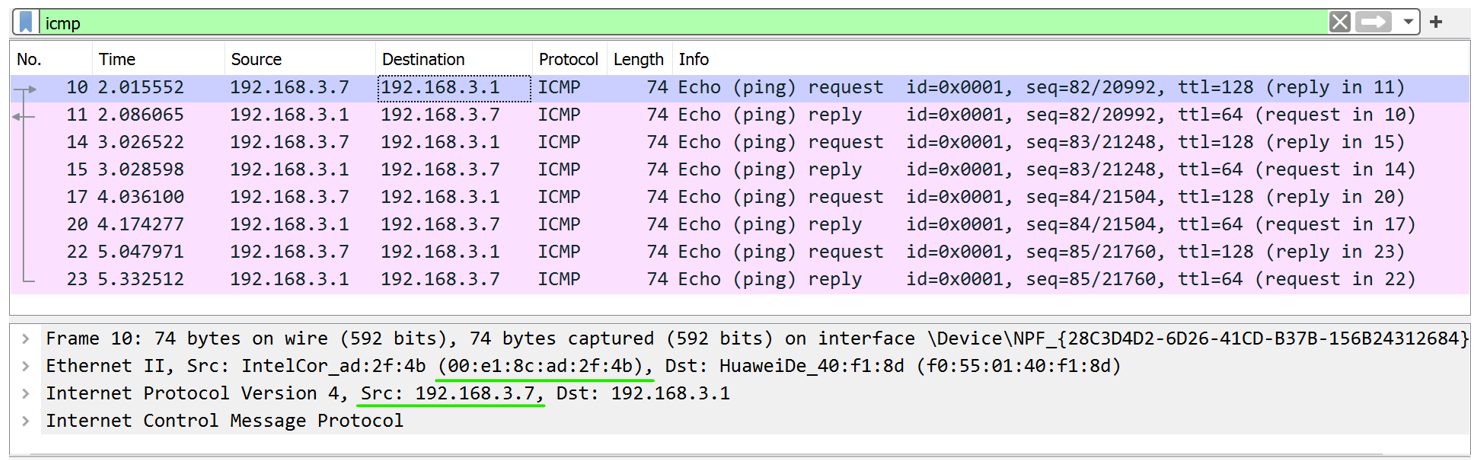
Використовуючи поле "Filter", відфільтруємо пакети по шаблону "icmp"



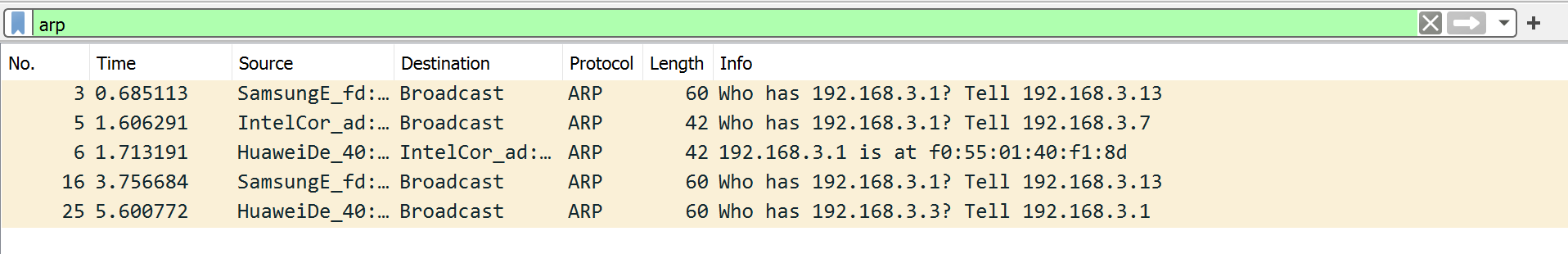
Бачимо 2 види пакетів – request і reply. Вони відрізняються заголовками Source, Destination та Info. З мого комп’ютера відправлені пакети з параметром request, отримані з параметром reply.

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.

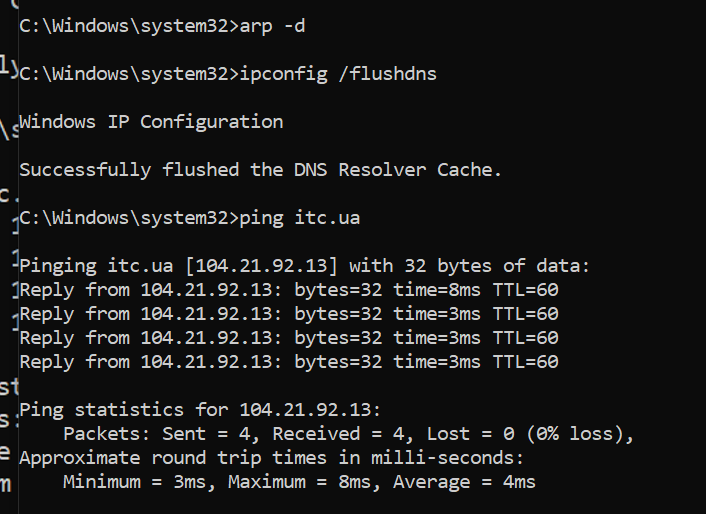


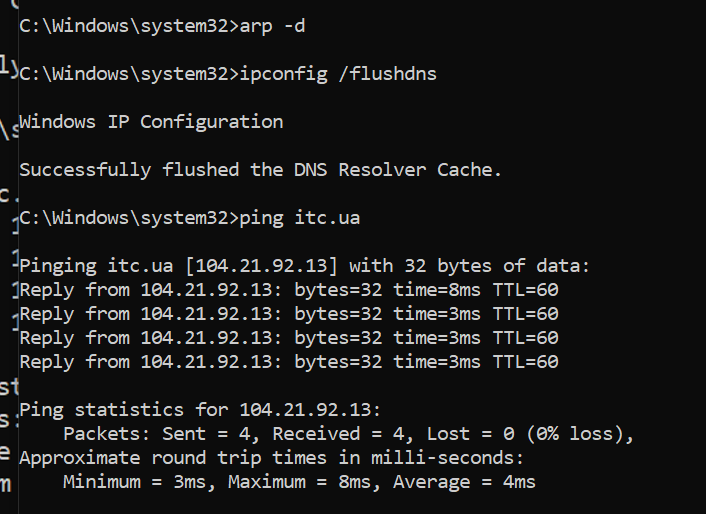
1. Відключили фільтр "icmp" і з усіх отриманих в п.1 пакетів виділили пакети "arp". Зберегли пакети, що залишилися.



1. Перевірка досяжності хоста за межами локальної мережі.

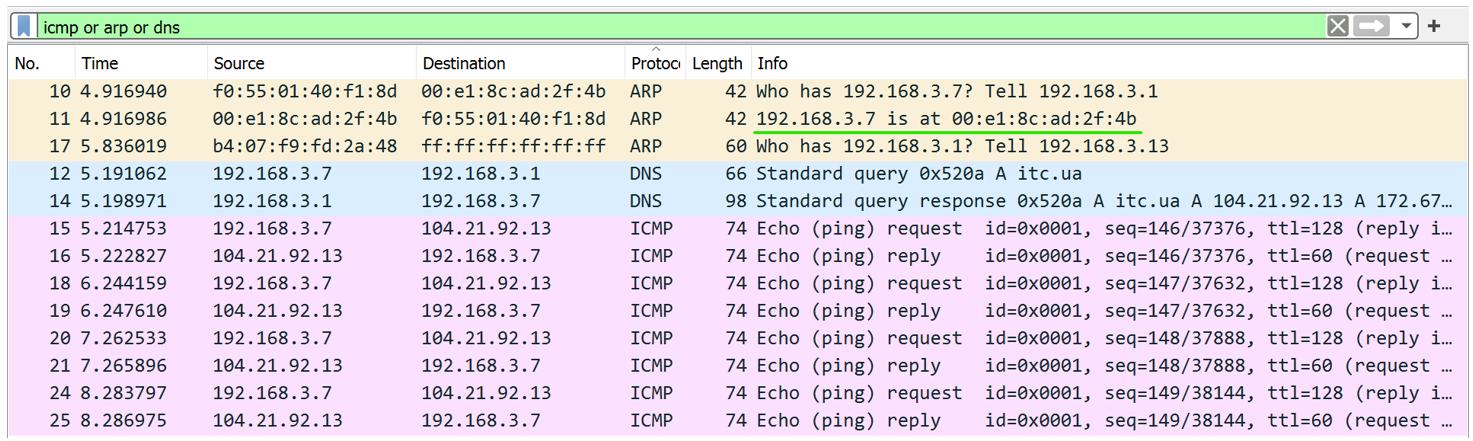
Очистили ARP-кеш та DNS-кеш



Перевірили досяжність хоста itc.ua

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

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

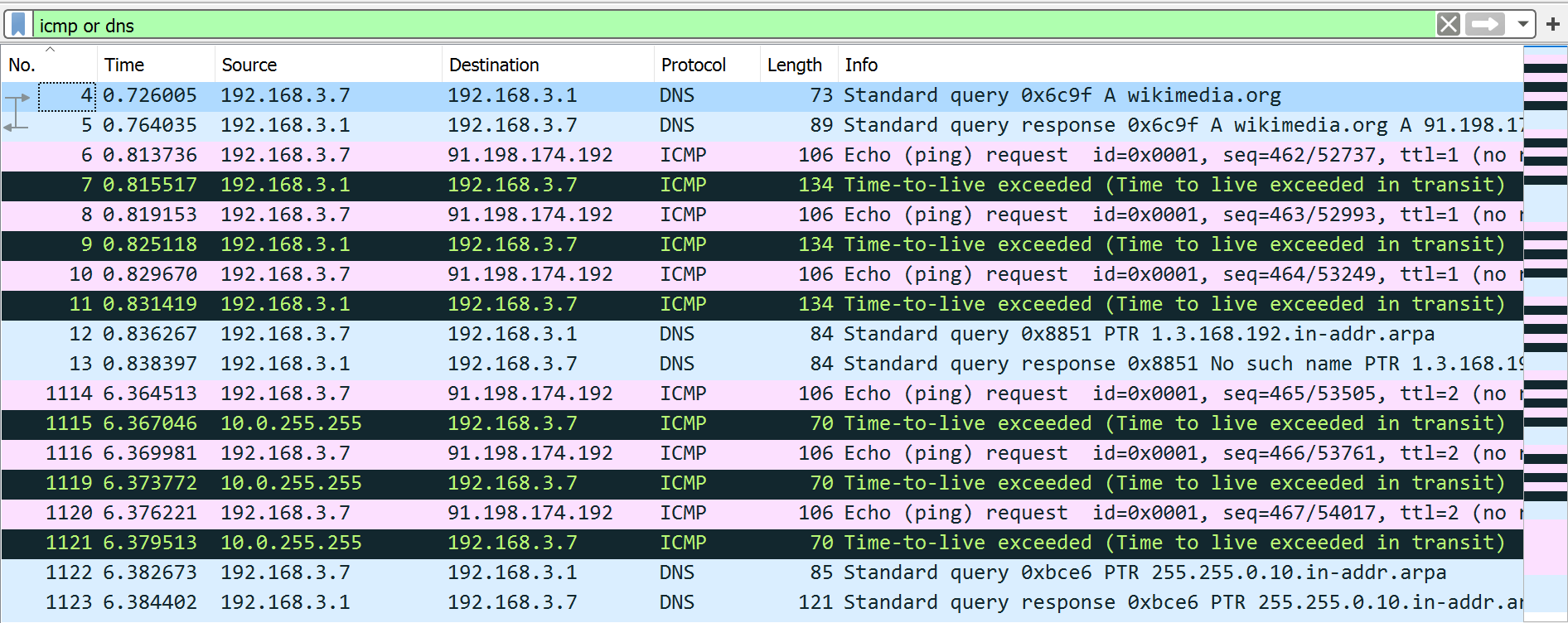


1. Трасування деякої адреси за межами локальної мережі.

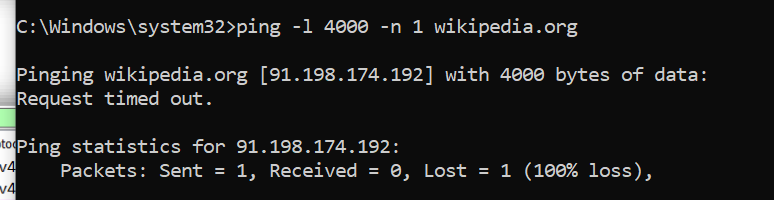
Виконали команду tracert

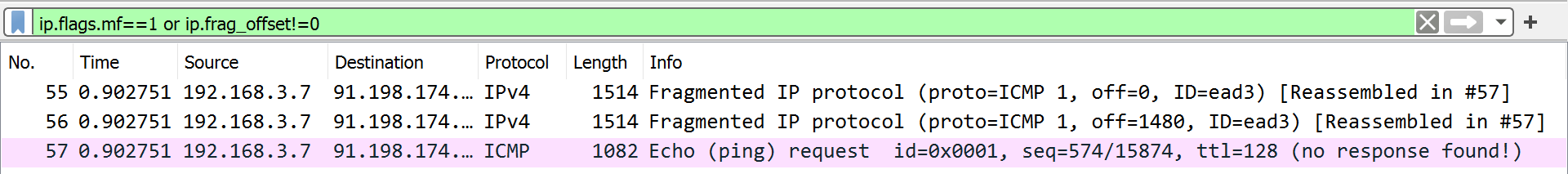
В перехопленні traceroute зустрічаються пакети icmp (для перевірки зв’язку з хостом) та dns (для отримання IP-адреси з імені хоста).

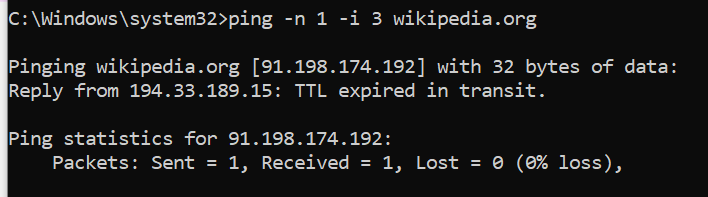
У пакетах ping перевіряється з’єднання з одним хостом, а у traceroute йде перевірка з кожним проміжним маршрутизатором, доки не дійде до кінцевої цілі. У заголовку протоколу ICMP встановлено TTL 1. Такий echo запит утиліта traceroute відправляє 3 рази. Потім з кожним разом TTL збільшується на 1, доки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

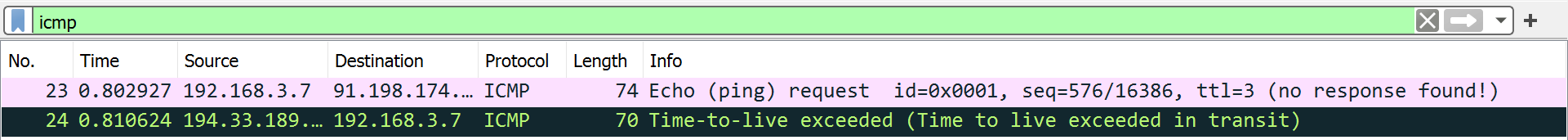


1. Фрагментація



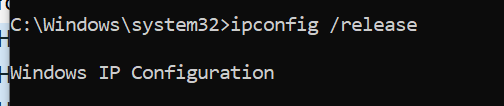


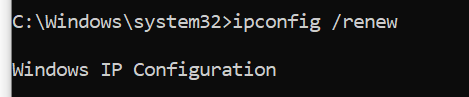


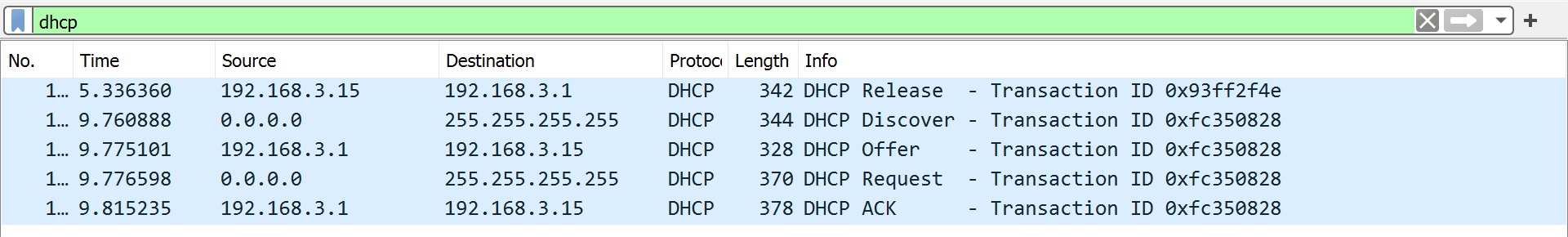


1. DHCP

Звільнення IPv4-адреси для вказаного адаптера.



Оновлення IPv4 адреси для вказаного адаптера.



**Відповіді на запитання:**

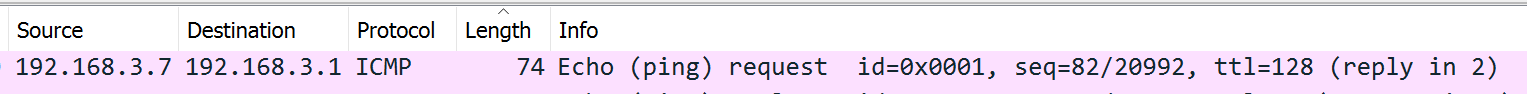
1. **Протокол ICMP:**

**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.

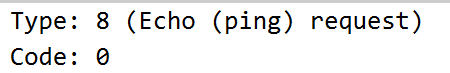
**Якою є ІР адреса вашого комп’ютера? Якою є ІР адреса хоста призначення?**

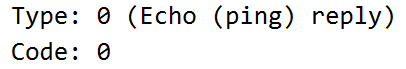
IP-адреса мого комп’ютера 192.168.3.7, IP-адреса хоста призначення 192.168.3.1

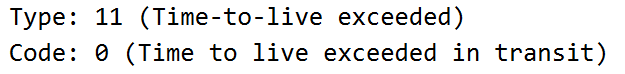


**Які види ICMP повідомлень вам зустрічалися. Які значення "тип" і "код" вони мають.**

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







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

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

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

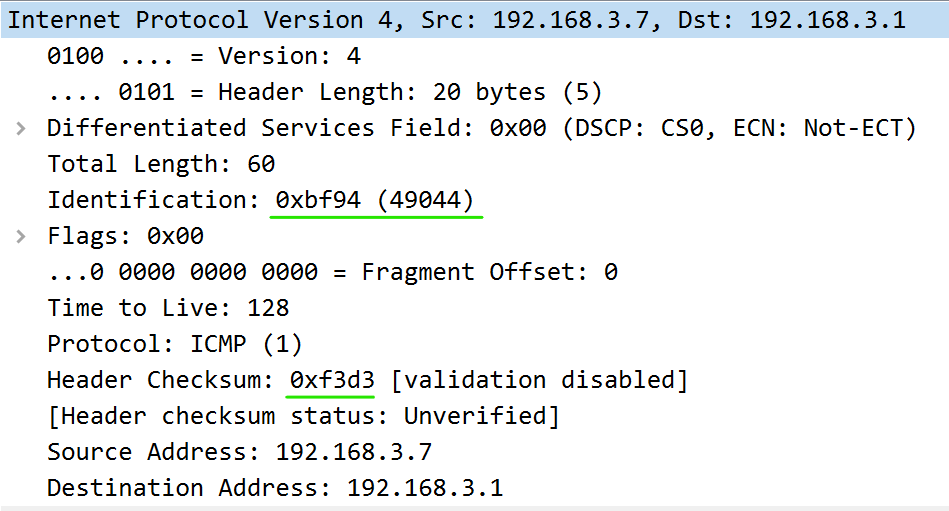
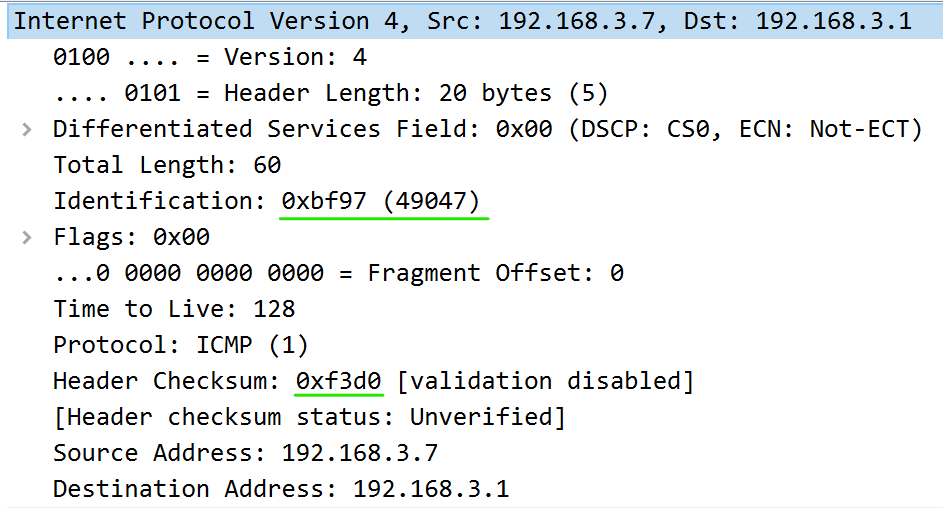
У одержуваних відповідях «echo (ping) reply» type 0, code 0.

**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-датаграми змінюються.**

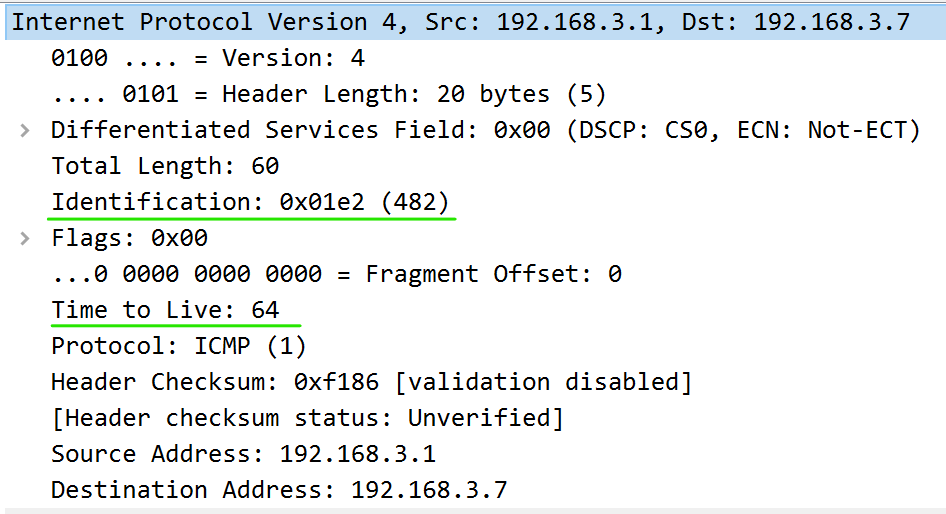
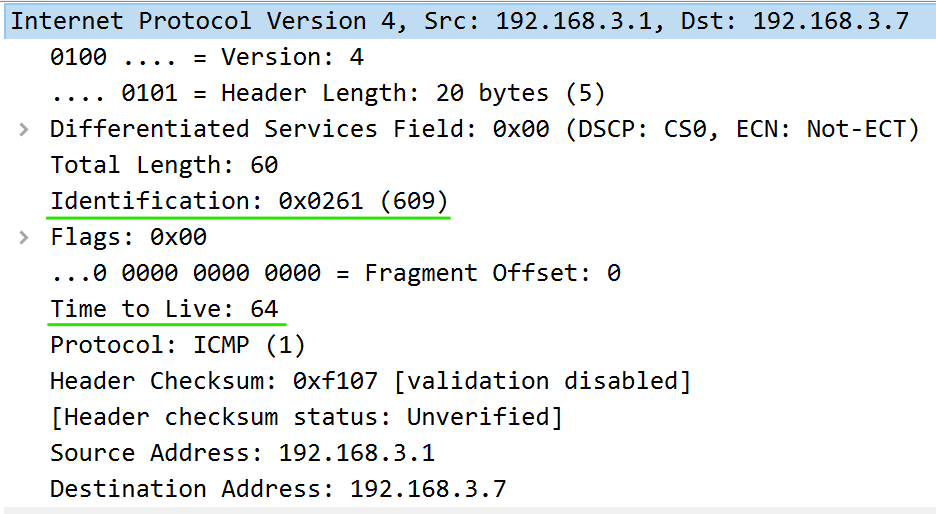
Візьмемо до прикладу перший та останній echo-запит:

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

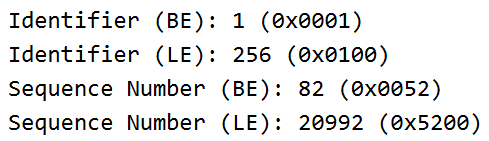
**На прикладі серії echo - відповідей визначте, якими є значення полів ідентифікатора (Identification) та TTL.**

Візьмемо до прикладу першу та останню echo-відповідь:

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.**



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

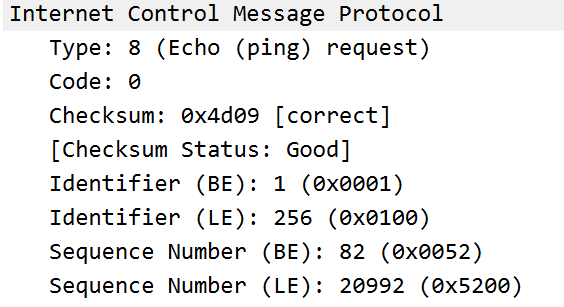
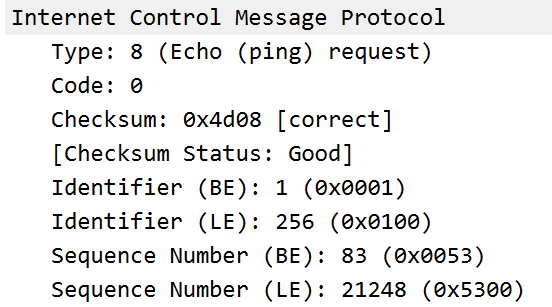
**Опишіть роботу утиліт ping і traceroute (tracert). В чому їх відмінність.**

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.

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

**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".**



Щоб повідомити про те, що час життя пакету завершився.

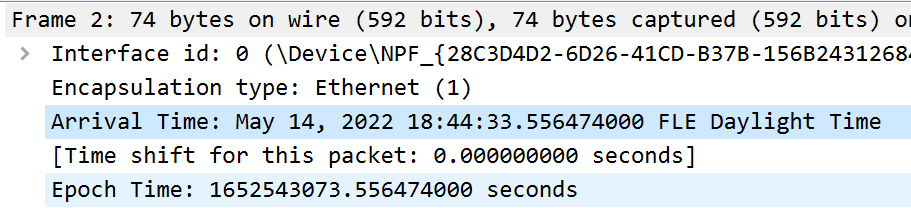
**Поясніть призначення параметрів -r і -s в команді ping.**

*-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



1. **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



1. **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).

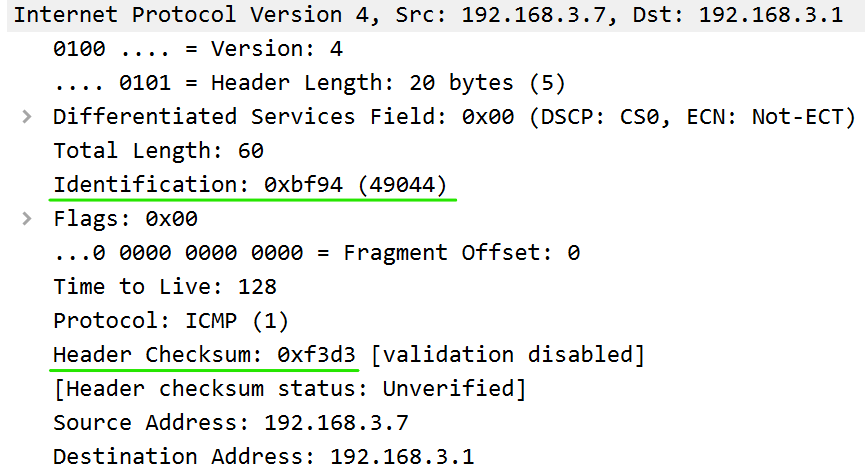
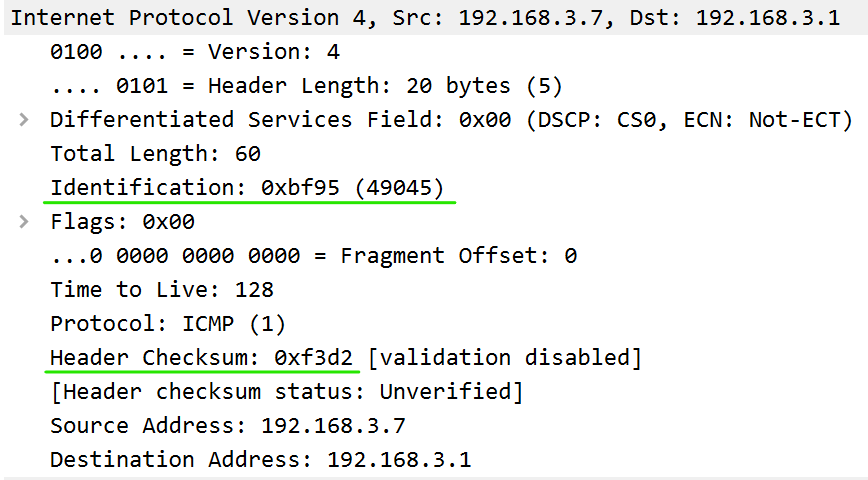
**Який розмір має стандартний ІР заголовок? Скільки байтів містять дані корисного навантаження ІР дейтаграми? Поясніть будь-ласка, як ви це визначили.**

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.

**Якими є значення полів ідентифікатора та TTL.**

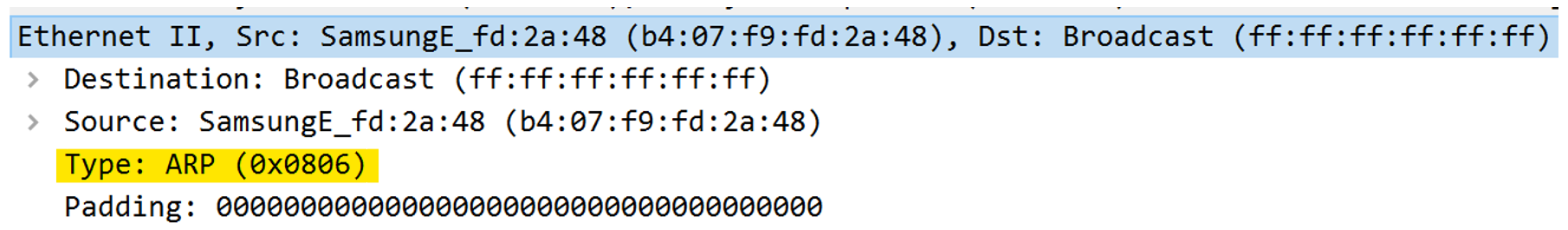
Якщо взяти до прикладу echo-запити, то можна побачити, що якщо був виконаний звичайний ping, то з кожним запитом поле ідентифікатора збільшується на 1, а TTL = 128 (залишається сталим). Якщо була виконана команда traceroute, то значення TTL буде збільшуватись з кожними трьома запитами на 1, поки не дійде до потрібного маршрутизатора.

1. **Протокол ARP:**

**Опишіть формат пакета і призначення полів заголовка протоколу ARP.**

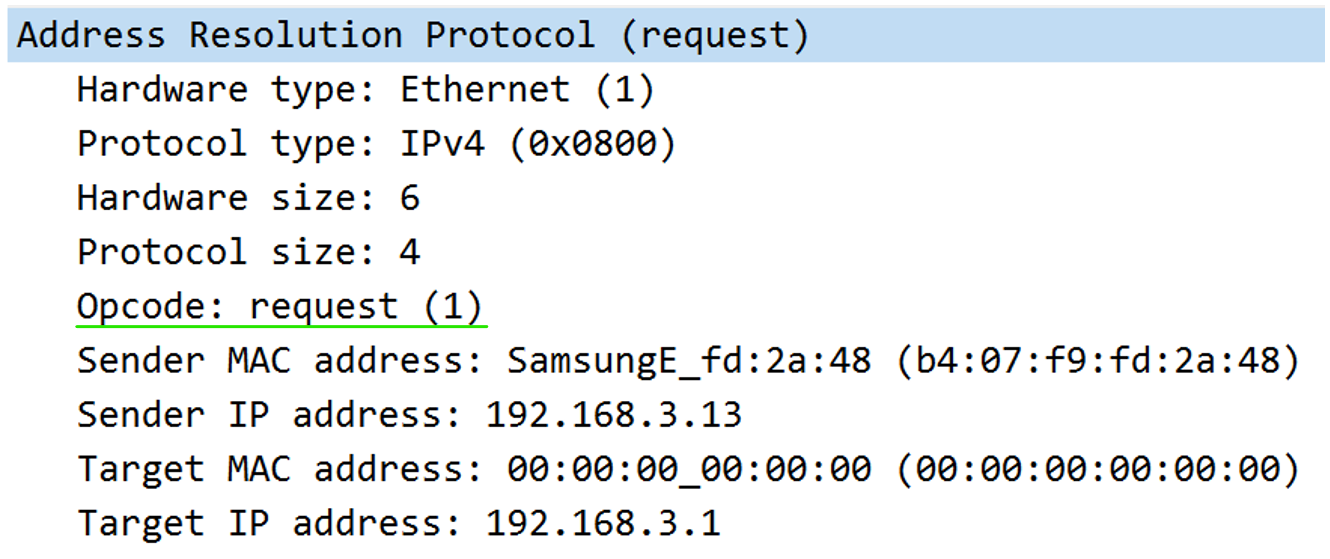
* Hardware type – тип обладнання (розмір: 2 байти)
* Protocol type – тип протоколу. Протокол вищого рівня, для якого використовується запит ARP (розмір: 2 байти)
* Hardware size – довжина MAC-адреси (розмір: 1 байт)
* Protocol size – довжина адреси протоколу (розмір: 1 байт)
* Opcode – операція. Функція 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.**



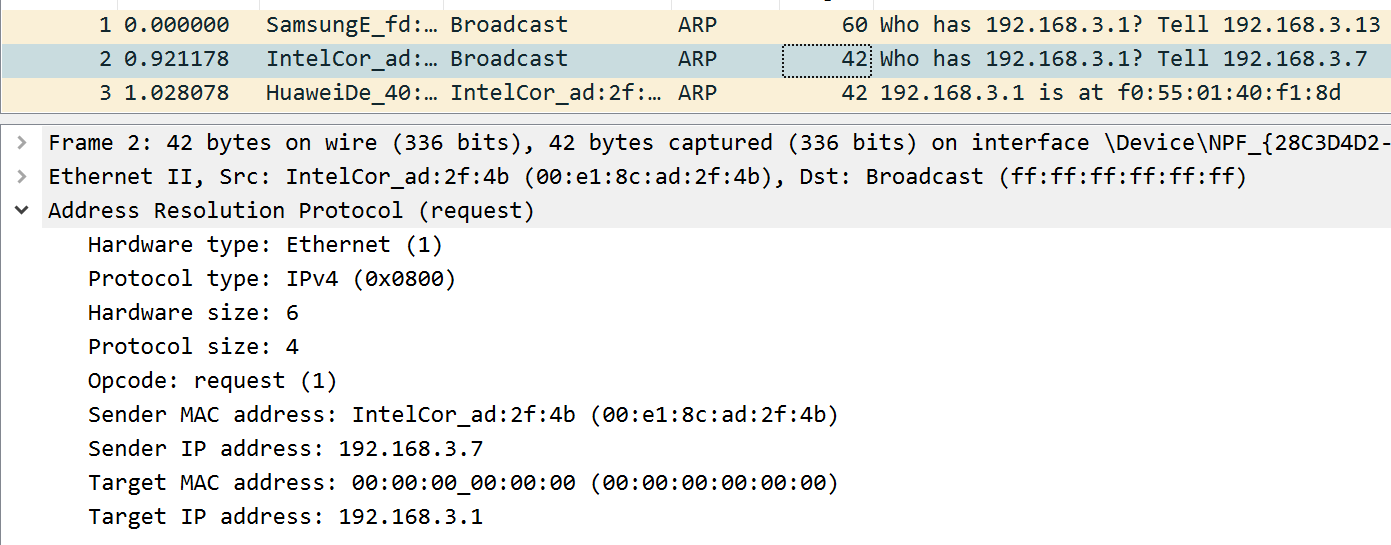
**Яким полем ідентифікуються (відрізняються) запит і відповідь ARP.**

Opcode

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

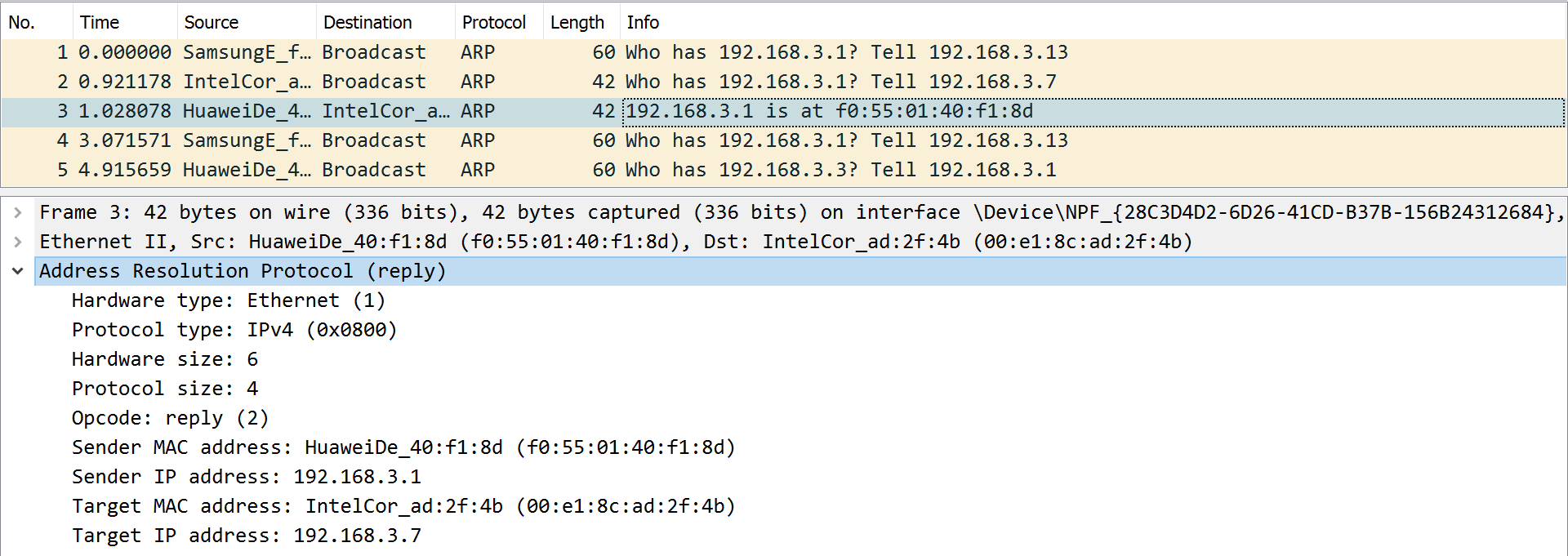
ARP-запит:



ARP-відповідь:

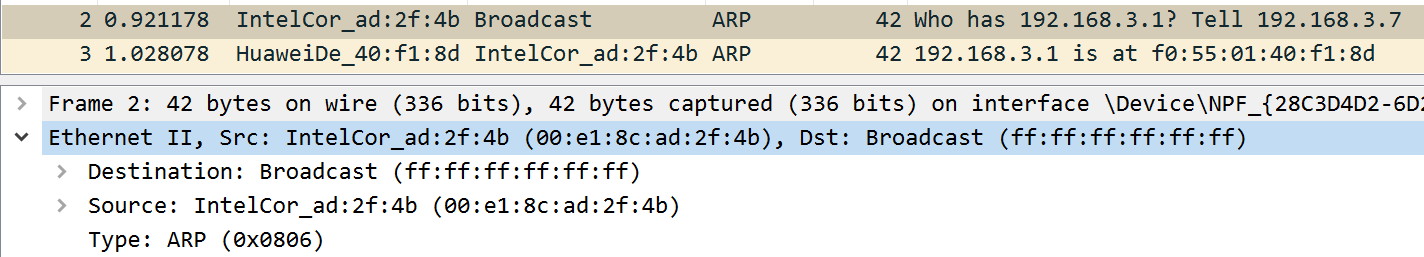


**Знайдіть повідомлення ARP, що було надіслано у відповідь на деякий запит ARP.**

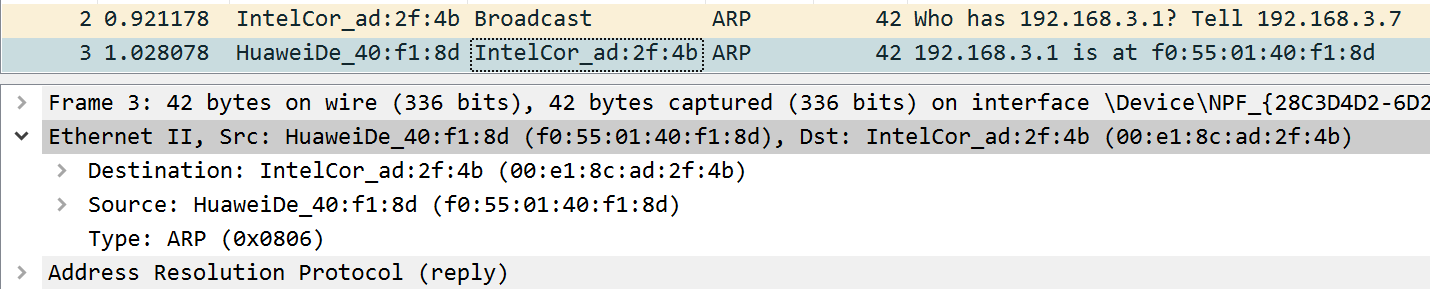


**Які значення мають адреса відправника і адреса одержувача в кадрах Ethernet, що містять повідомлення ARP?**

ARP-запит



ARP-відповідь



**Чи містить ARP повідомлення IP адресу відправника.**

Так



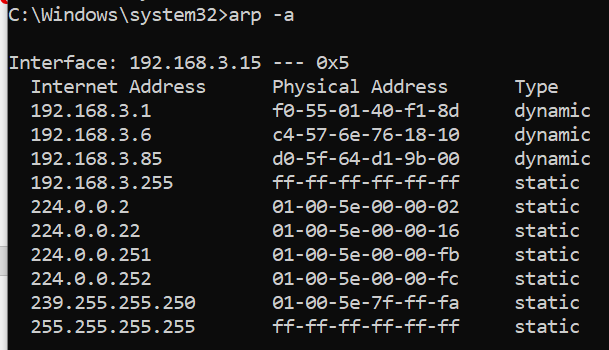
**З якого байту кадру Ethernet починається поле opcode? Які** **значення** **має поле opcode в різних ARP пакетах?**

Поле opcode починається з 7 байту.

Має значення reply (2) та request (1)

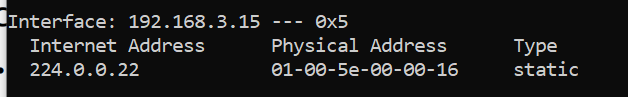
**Перевірте** **вміст ARP - кеша комп'ютера. Прокоментуйте результат. Як очистити вміст ARP - кеша.**

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



Очищаємо кеш командою arp -d



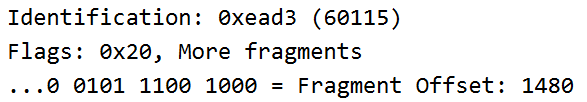


1. **Фрагментація пакетів:**

**Чи фрагментуються IP-датаграми, що відправляються вашим вузлом.**

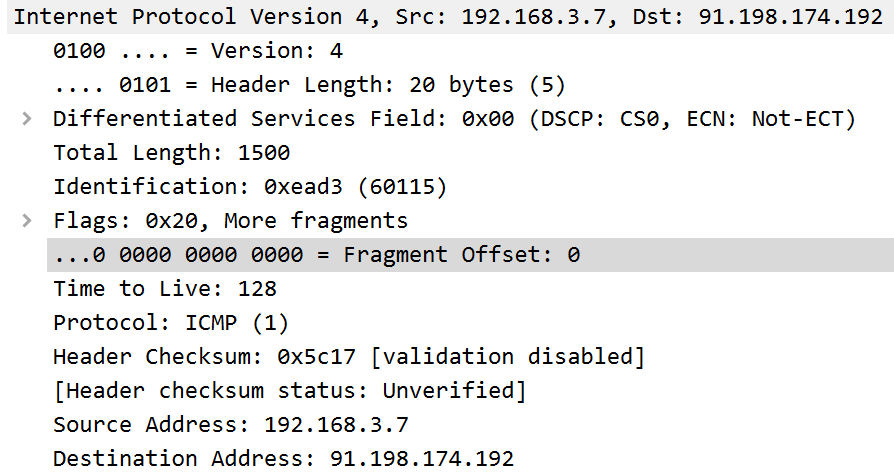
Так

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

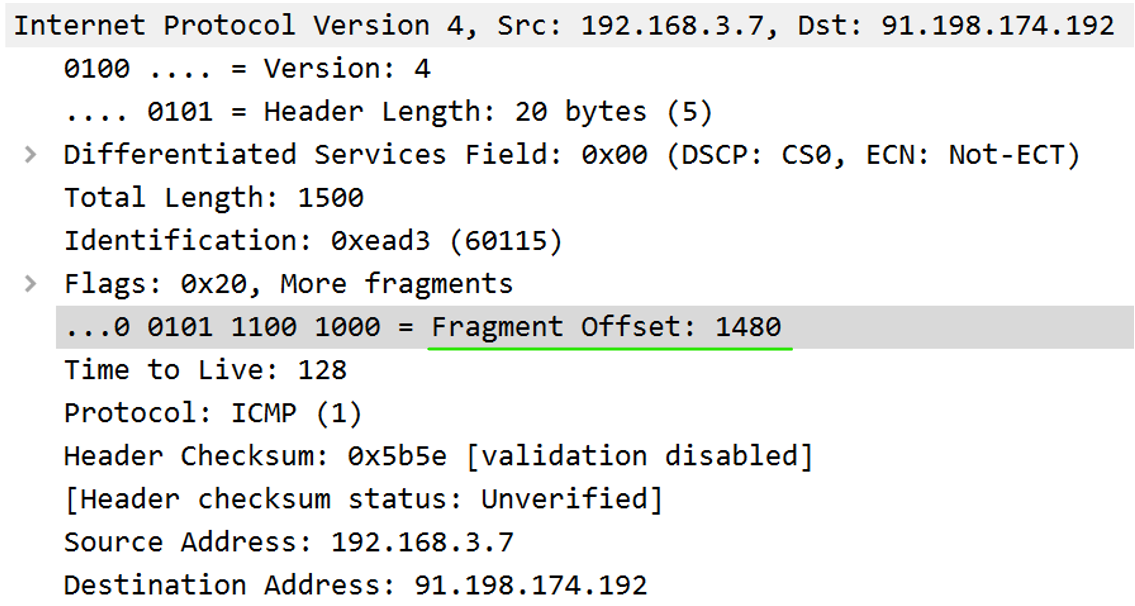


У фрагментах поле Identification однакове, поле Flags вказує на те, що далі є ще фрагменти, Fragment offset показує зміщення фрагменту, у всіх фрагментах, окрім першого, це поле буде ненульовим.

**Виведіть перший фрагмент фрагментованої ІР датаграми.**

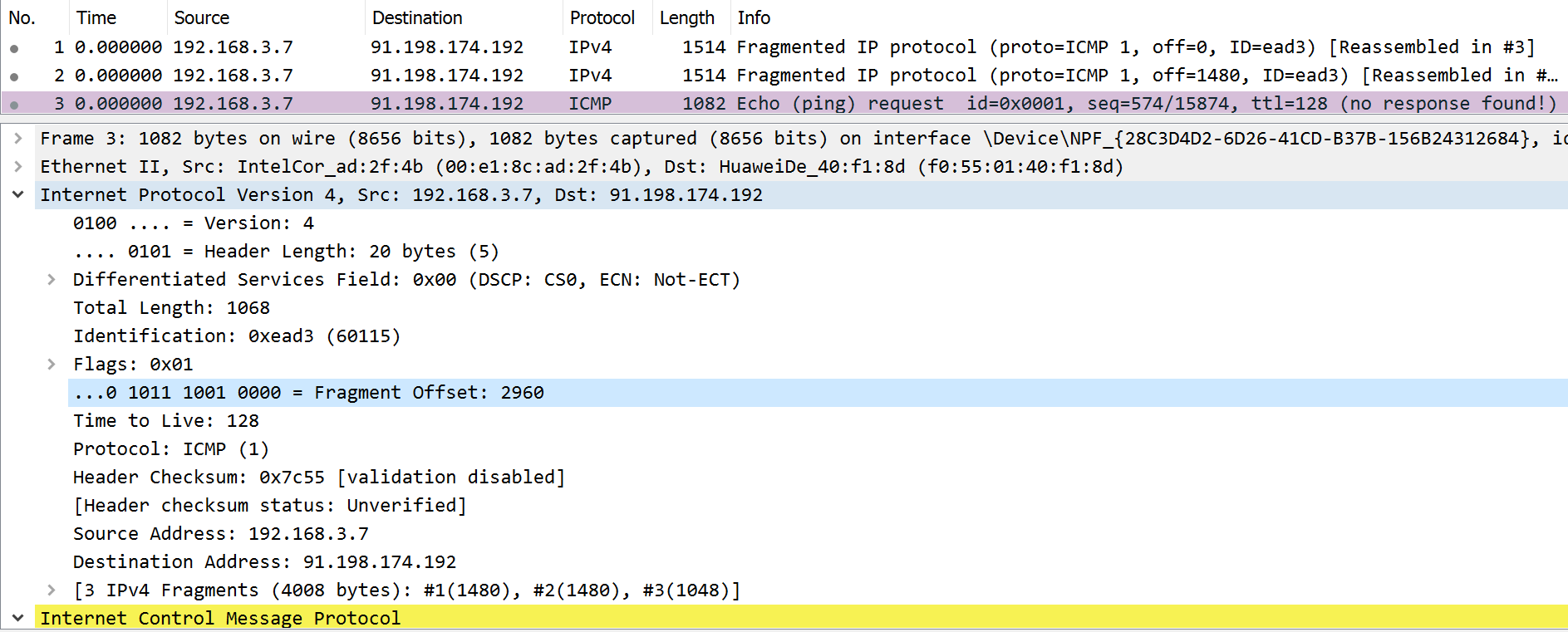


**Виведіть другий фрагмент. Яка інформація покаже, що це не перший фрагмент?**



**Чи існують ще якісь фрагменти? Чому?**

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



**Яке поле змінилося в заголовку ІР в першому і другому фрагментах.**

Fragment offset та Header Checksum.

**Які поля змінюються в ІР 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.

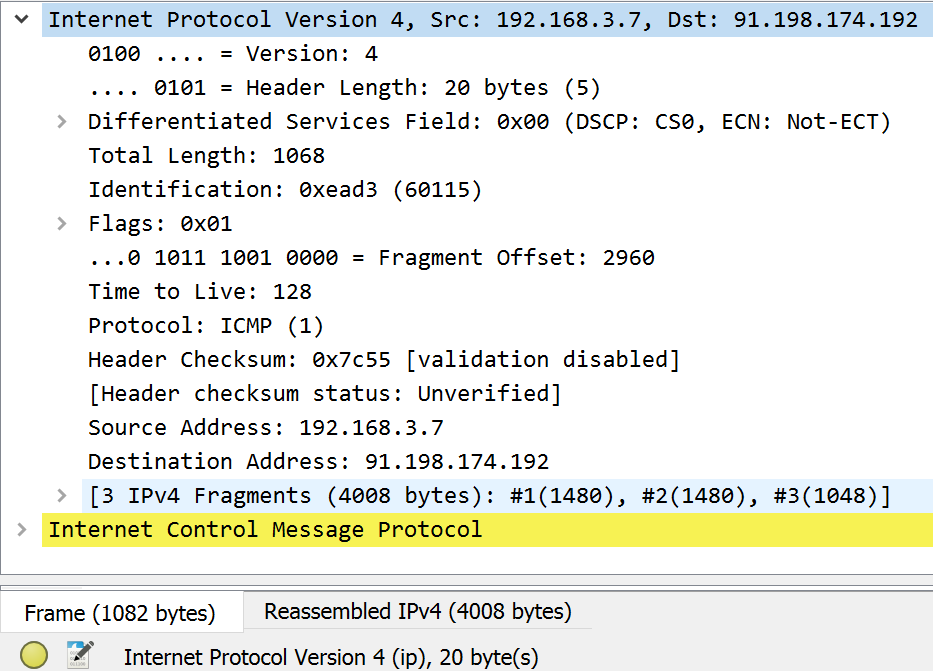
**Чи з****мінюється** **ідентифікатор датаграми в її фрагментах і яке його значення.**

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**



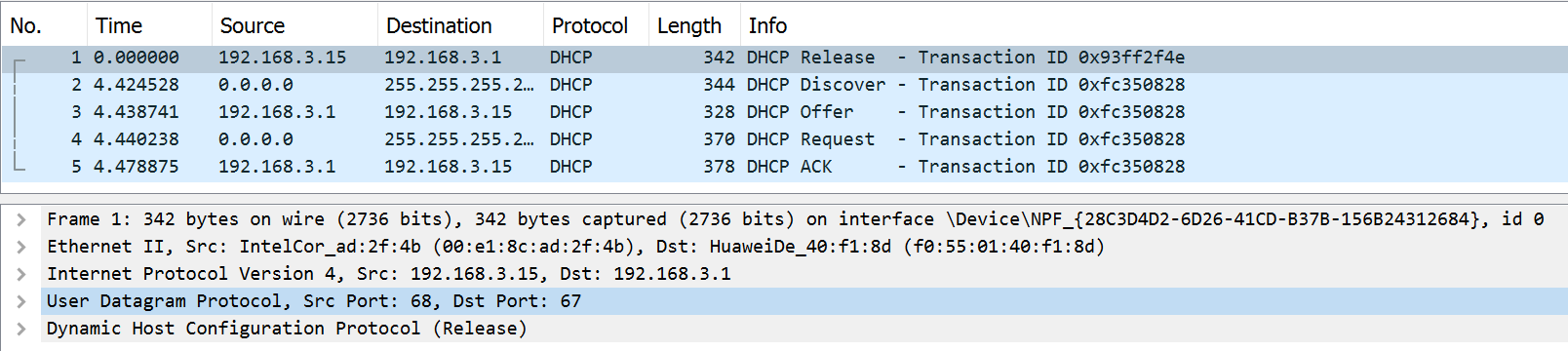
1. **Протокол DHCP:**

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

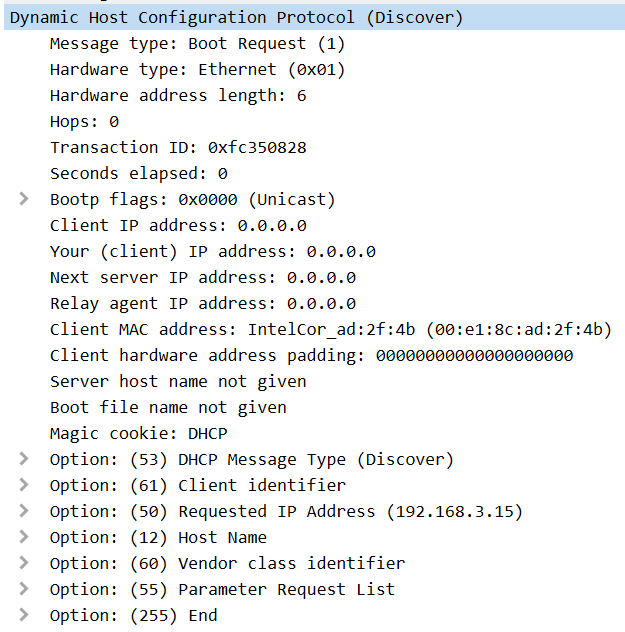
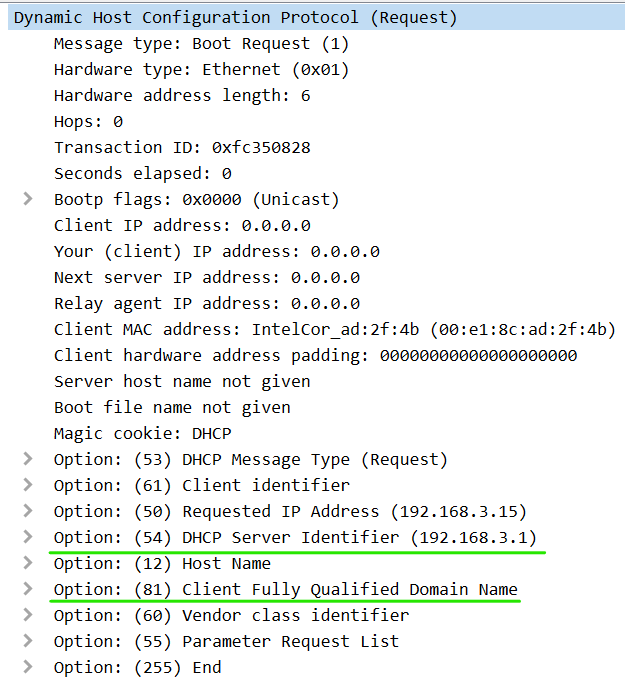
* Release – пакет, що передає повідомлення про звільнення оренди IP адреси.
* Discover – широкомовний мережевий пакет, який клієнт відправляє з метою знайти DHCP-сервер у мережі.
* Offer – пакет, що відправляє сервер, отримавши запит від клієнта, з IP адресою та годиною оренди.
* Request – пакет, що 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 ІР (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

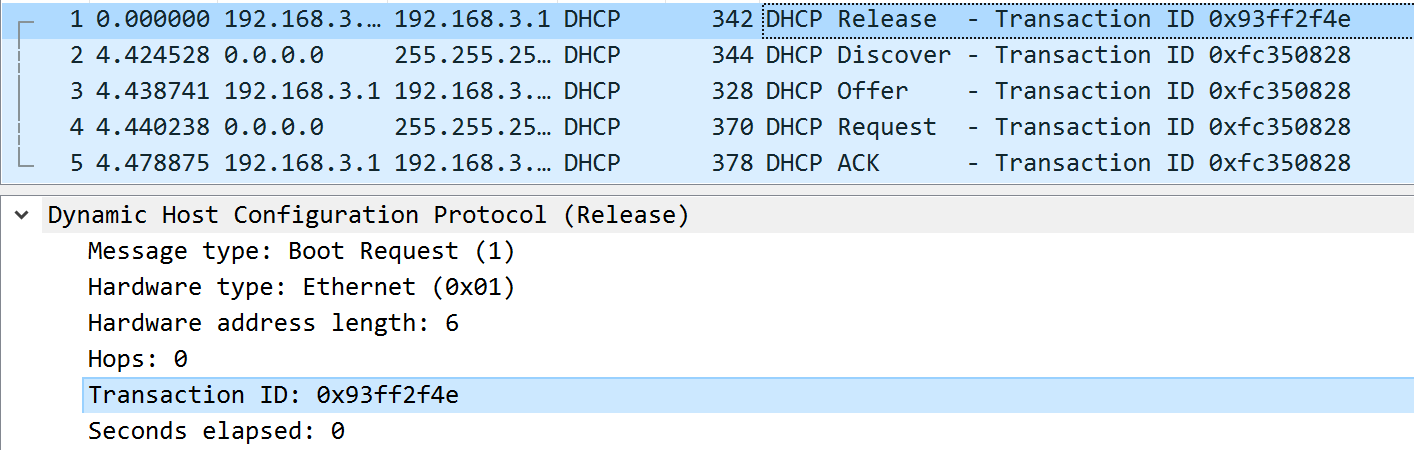
****

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

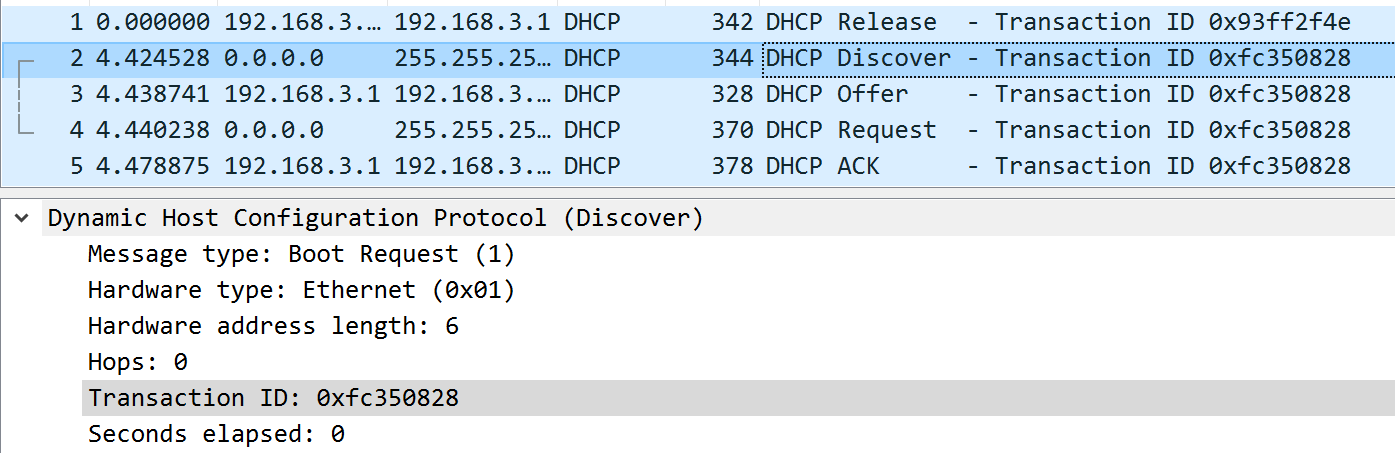
 

**Як змінюється це поле в послідовності запитів. Яке значення Transaction-ID в кожному з перших чотирьох Discover/Offer/Request/ACK DHCP пакетів.**

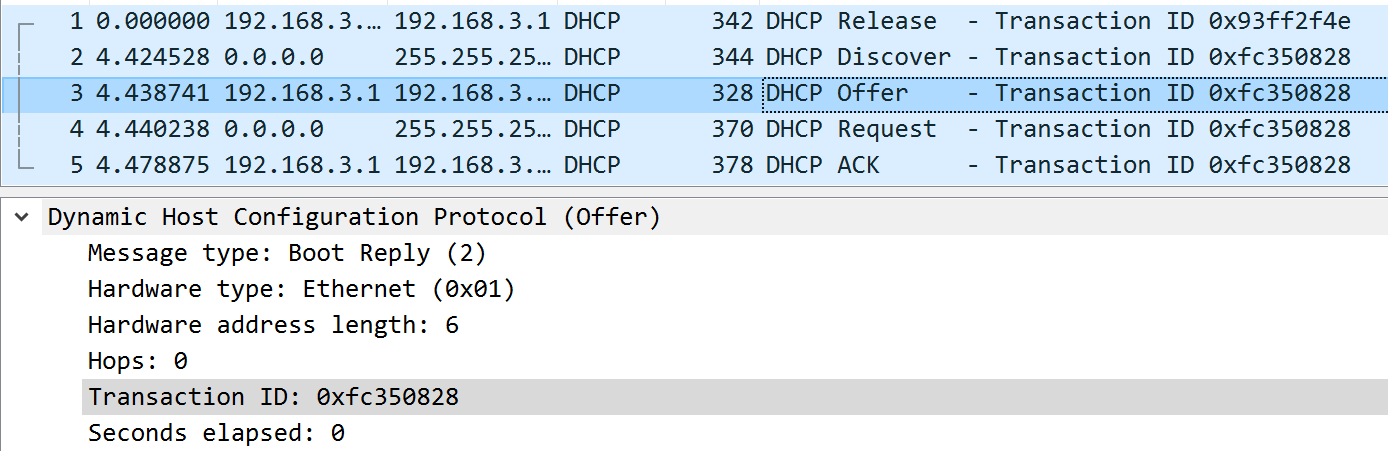
Release



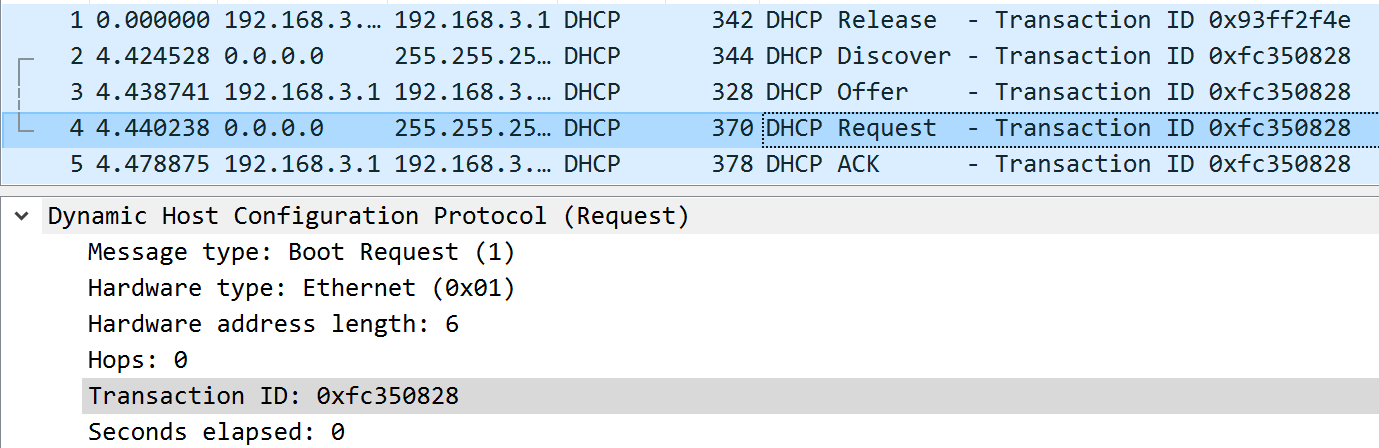
Discover



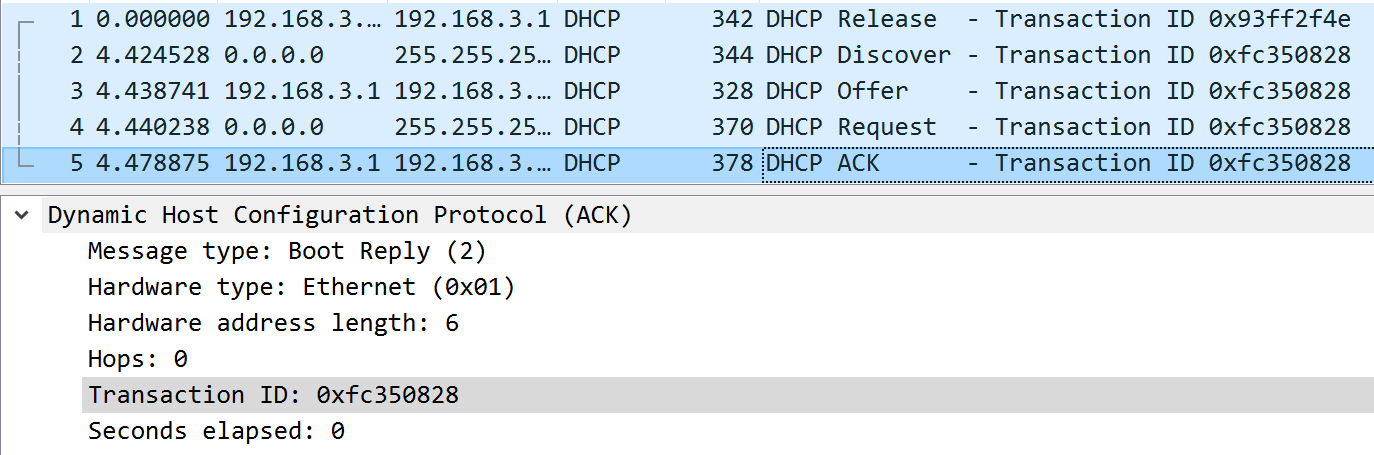
Offer



Request



ACK

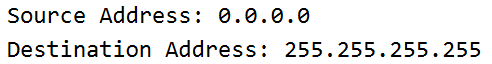


У Discover, Offer, Request та ACK значення transaction ID однакове, у Release значення інше, бо це окрема операція.

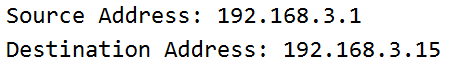
**Комп’ютер використовує DHCP пакет для отримання різних мережних налаштувань, зокрема отримання IP адреси. Але ця IP адреса не затверджена до закінчення обміну в останньому четвертому повідомленні. Якщо ж це дійсно так, то яке значення IP адреси використовується для обміну початковими 4-ма повідомленнями. 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

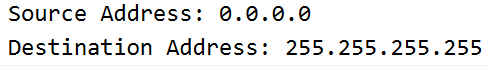
DHCP Discover



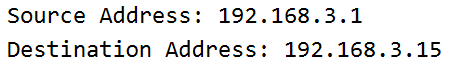
DHCP Offer



DHCP Request



DHCP ACK



**Яка IP адреса вашого DHCP сервера.**

****

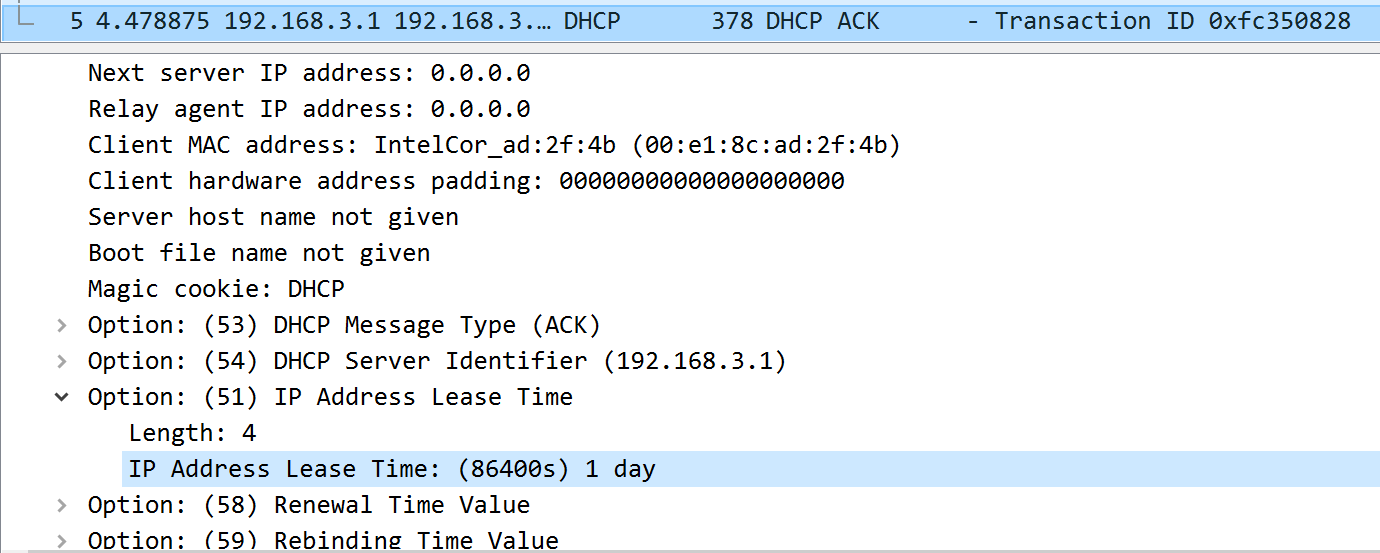
**Яка IP адреса пропонується DHCP сервером для вашого комп’ютера у DHCP Offer повідомленні? Вкажіть, в якому DHCP повідомленні міститься запропонована IP адреса.**

В DHCP Offer міститься запропонована IP адреса

****

**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.



**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.

**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

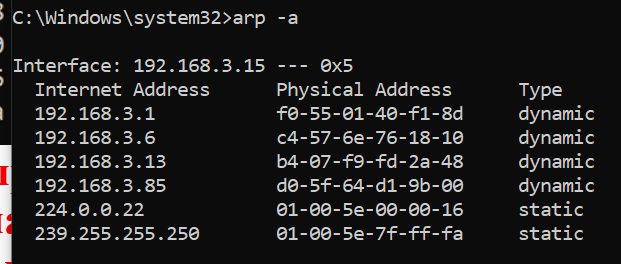
Канальний рівень даних: ARP

**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.



**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



По IP-адресі



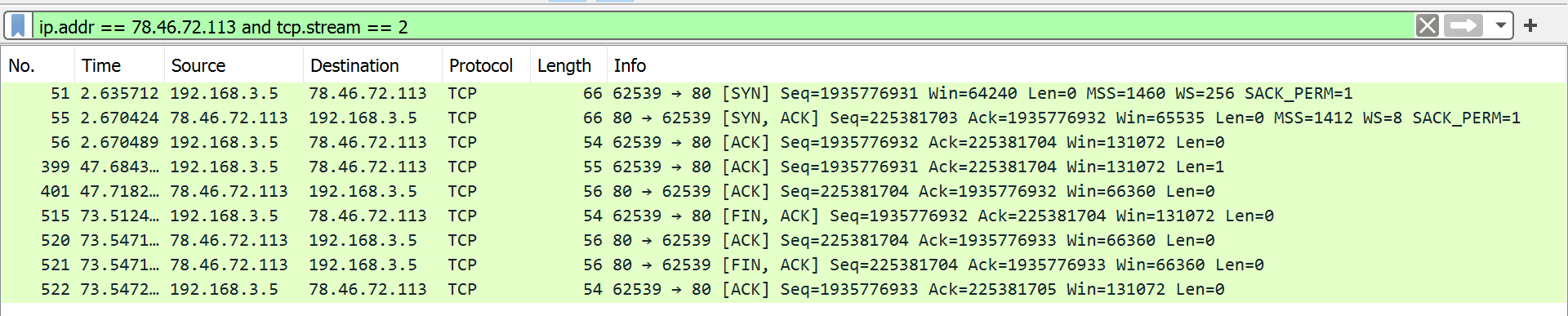
По MAC-адресі та протоколу



**Лабораторна робота №3.2**

«Дослідження мережних протоколів TCP та UDP»

1. Відкрили Web-сторінку за протоколом HTTP та зупинили запис пакетів.



Під номерами 51, 55 та 56 – встановлення з’єднання

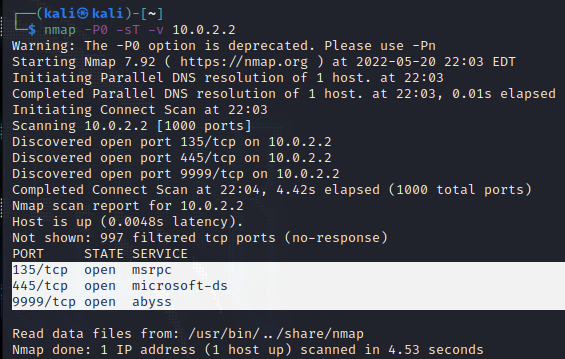
Під номерами 515 та 520 – завершення з’єднання сервером

Під номерами 521 та 522 – завершення з’єднання клієнтом

1. Сканування портів.

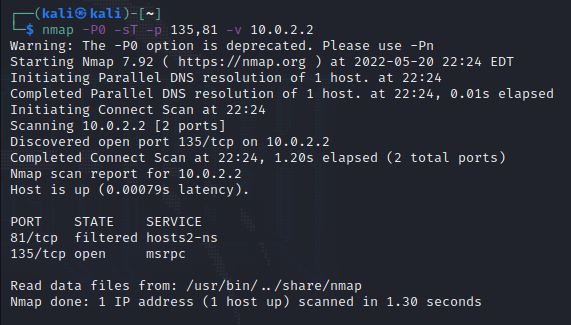
Перейдемо в Linux, так як там ми зможемо використовувати nmap.

Визначимо, які порти на хості є «відкритими».



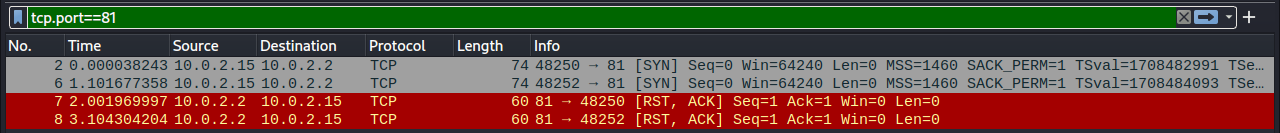
Виберемо порти: 81 – закритий, 135 – відкритий.

* Connect сканування



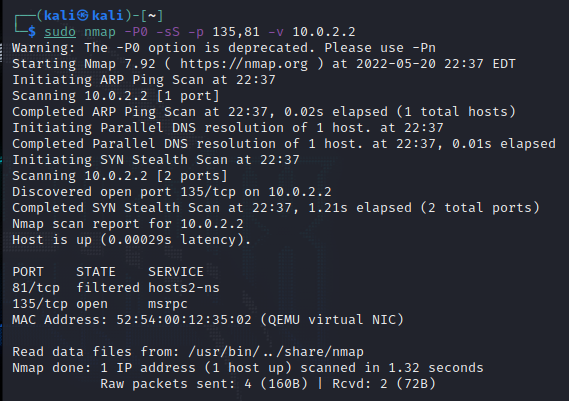


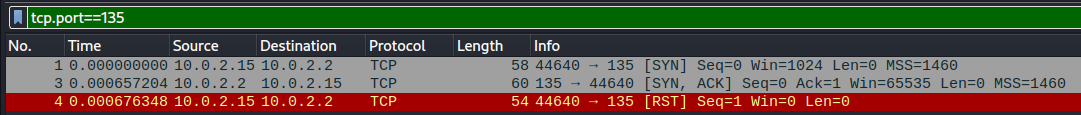
У відкритих портах спочатку від Source передається пакет з флагом SYN, у відповідь отримує пакет з флагом SYN, ACK. Потім Source знову передає пакет з флагом RST, ACK.



У закритих портах спочатку від Source передається пакет з флагом SYN, у відповідь отримує пакет RST, ACK.

* SYN сканування



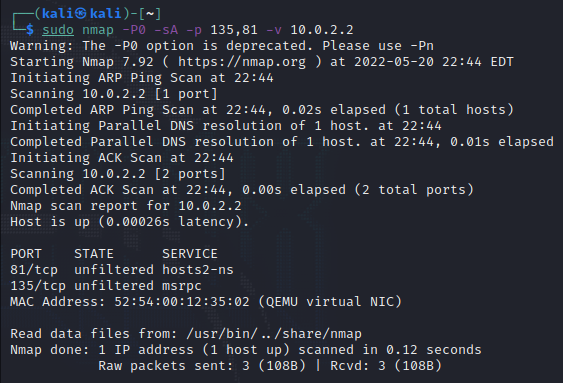


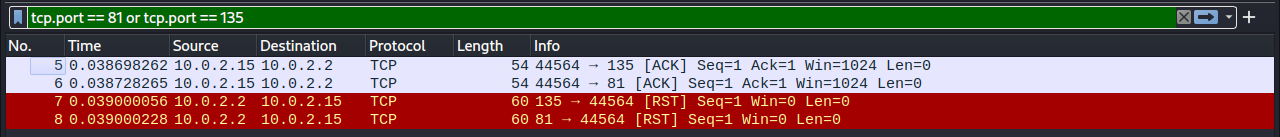
У відкритих портах спочатку від Source передається пакет з флагом SYN, у відповідь отримує пакет з флагом SYN, ACK. Потім Source знову передає пакет з флагом RST.



У закритих портах спочатку від Source передається пакет з флагом SYN, у відповідь отримує пакет з флагом RST, ACK.

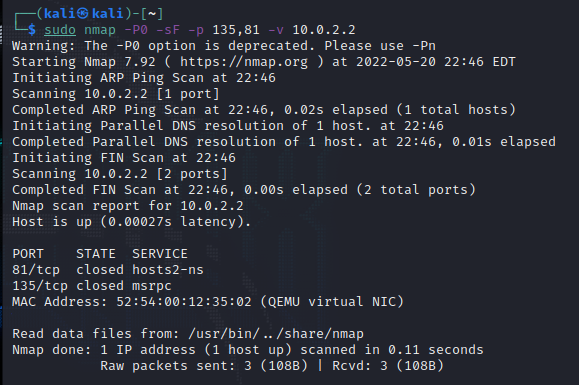
* ACK сканування

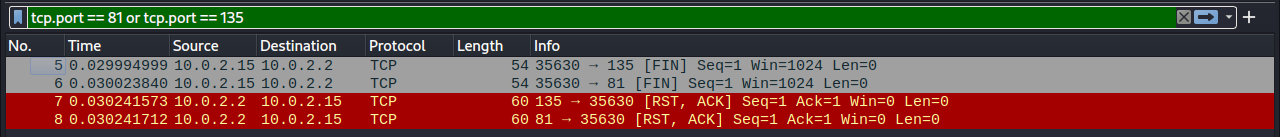




У відкритих портах спочатку від Source передається пакет з флагом ACK. Потім Source знову передає пакет з флагом RST.

* FIN сканування

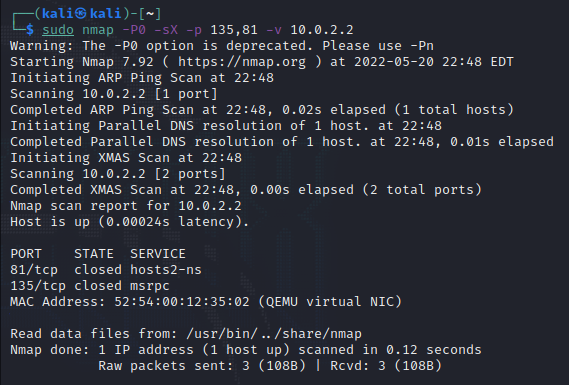


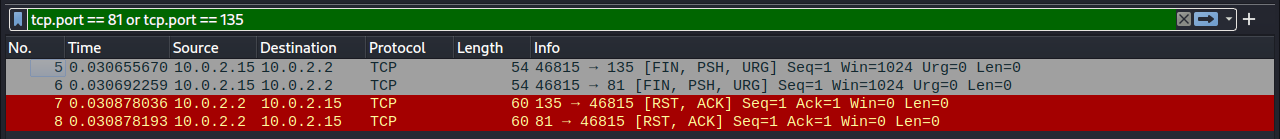


У відкритих портах від Source передається пакет з флагом FIN.

У закритих портах від Source передається пакет з флагом ACK, у відповідь отримує пакет з флагом RST, ACK.

* XMAS сканування

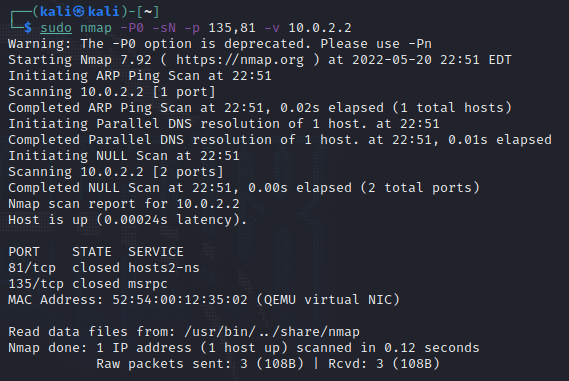


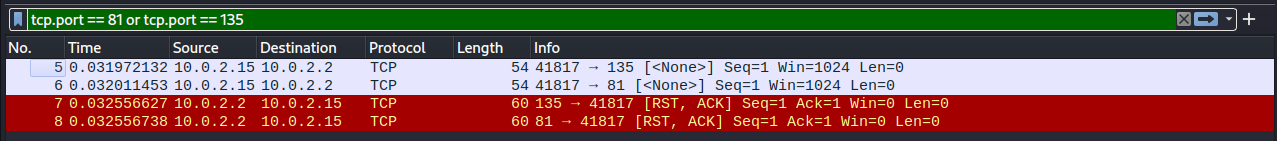


У відкритих портах від Source передається пакет з флагом FIN, PUSH, URG.

У закритих портах від Source передається пакет з флагом FIN, PUSH, URG, у відповідь отримує пакет з флагом RST, ACK.

* NULL сканування

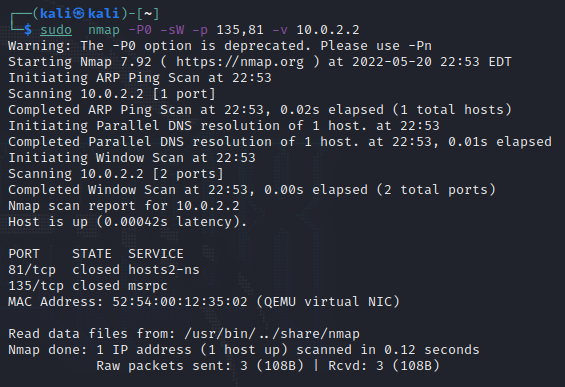


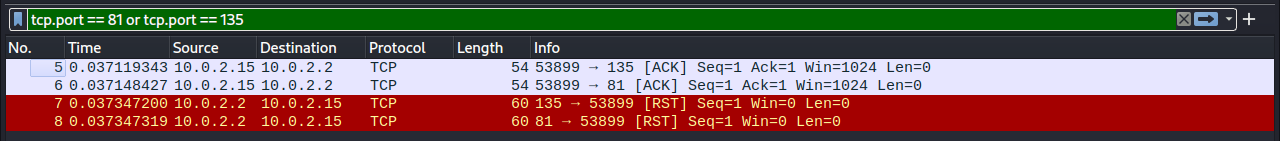


У відкритих портах від Source передається пакет без флагу.

У закритих портах від Source передається пакет без флагу, у відповідь отримує пакет з флагом RST, ACK.

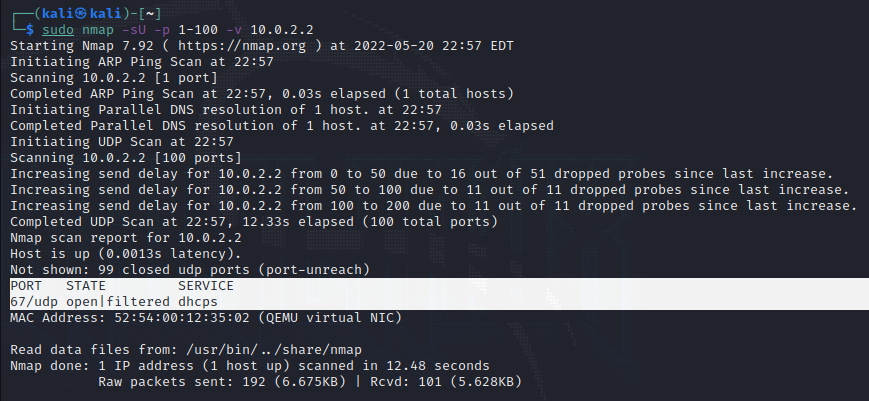
* WIN сканування

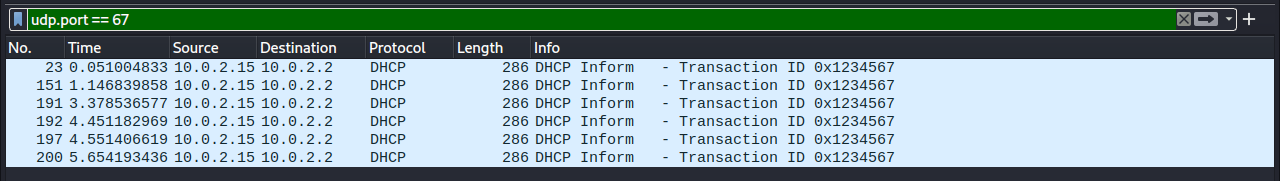




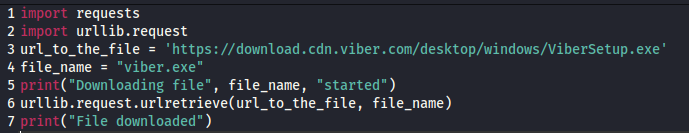
У закритих портах від Source передається пакет з флагом ACK, у відповідь отримує пакет з флагом RST.

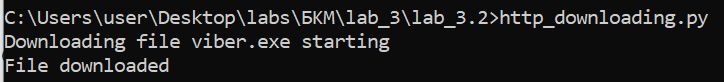
Просканували UDP порти у діапазоні від 1 до 100.

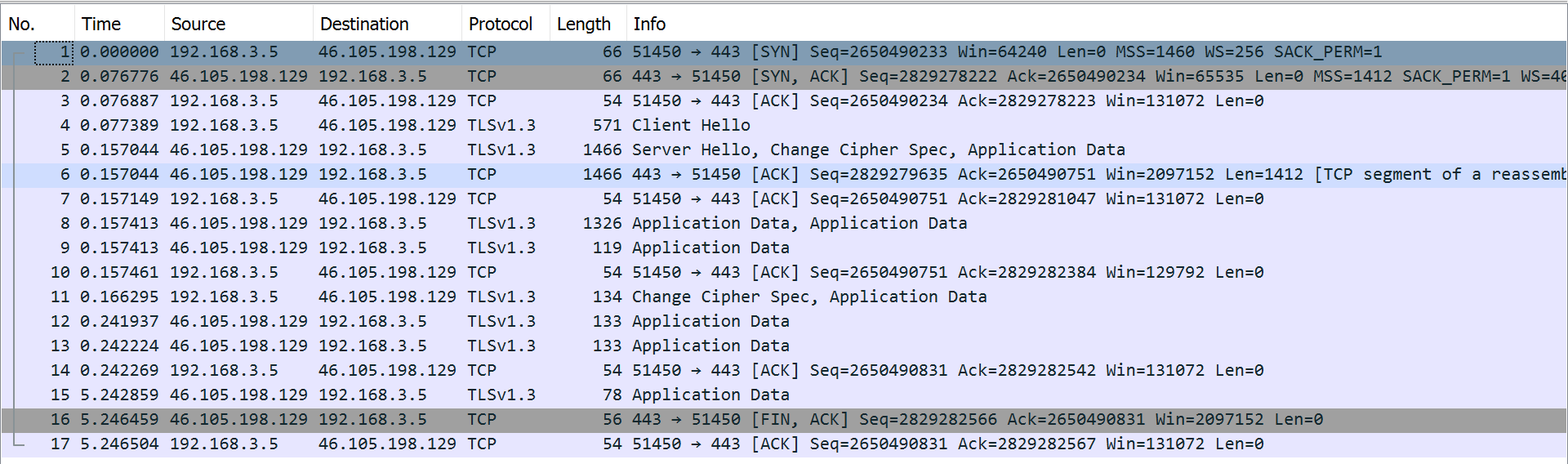


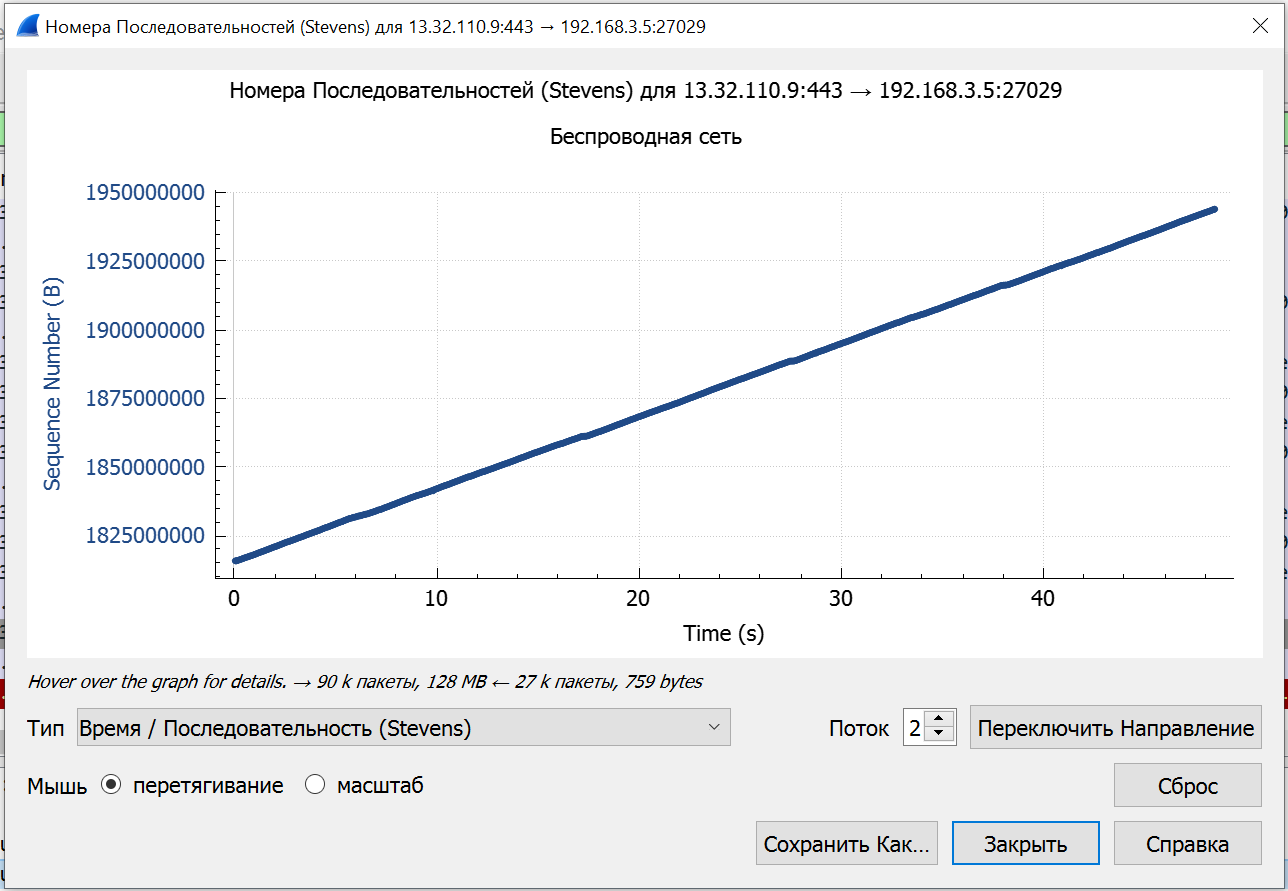


1. За допомогою python скрипта завантажили файл по протоколу http







Графік залежності номерів послідовності TCP від часу

**Відповіді на питання**

**1. Протокол TCP:**

**Опишіть формат повідомлення TCP.**

* Source Port – порт джерела, який використовується для передачі пакету
* Destination Port – порт призначення, на який буде передаватися пакет
* Stream Index – номер, який використовується для ідентифікації сегмента TCP
* Conversation completeness – порядковий номер, який слід очікувати в наступному пакеті від іншого пристрою, що бере участь у зв'язку.
* Sequence Number – порядковий номер пакета
* Acknowledgment Number – номер підтвердження
* Header Length – довжина заголовка
* Flags – прапори URG, ACK, PSH, RST, SYN та FIN для визначення типу пакету TCP, який передається.
* URG — поле «Покажчик важливості» задіяне
* ACK — поле «Номер підтвердження» задіяне
* PSH - інструктує одержувача проштовхнути дані, що накопичилися в приймальному буфері, у додаток користувача
* RST – обірвати з'єднання, скинути буфер (очищення буфера)
* SYN — прапор, встановлений, вказує на завершення з'єднання.
* Calculated Window Size – розмір буфера приймача TCP в байтах
* Checksum – використовується для того, щоб переконатися, що вміст заголовка TCP і дані не пошкоджені після доставки.
* Urgent Pointer – показник важливості

**Який номер протоколу відповідає TCP.**



**Опишіть послідовність встановлення з'єднання. Які параметри при цьому необхідно синхронізувати сторонам. Які номери послідовностей мають перші пакети з'єднання.**

З'єднання з трьома рукостисканнями:

Перше рукостискання: При встановленні з'єднання клієнт відправляє пакет SYN на сервер, очікуючи на підтвердження сервера;

Друге рукостискання: Сервер приймає пакет SYN і має його підтвердити, відправляючи пакет SYN + ACK;

Третє рукостискання: Клієнт отримує пакет SYN + ACK сервера, відправляє пакет підтвердження на сервер.

**Який порядковий номер (sequence number) TCP SYN пакета, що ініціює TCP з'єднання.**



**Що в цьому TCP пакеті вказує, що він є SYN пакетом.**

Наявність флагу SYN та відсутність флагу ACK.

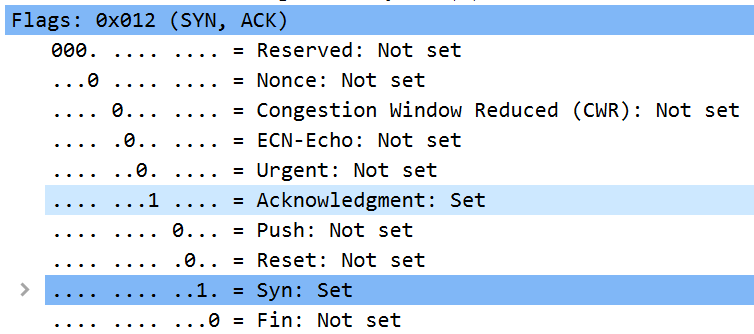
**Який порядковий номер відповідного SYN+ACK пакета.**



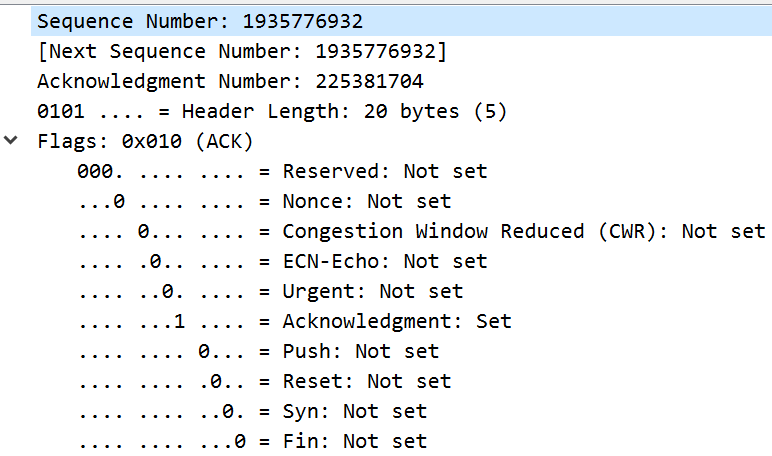
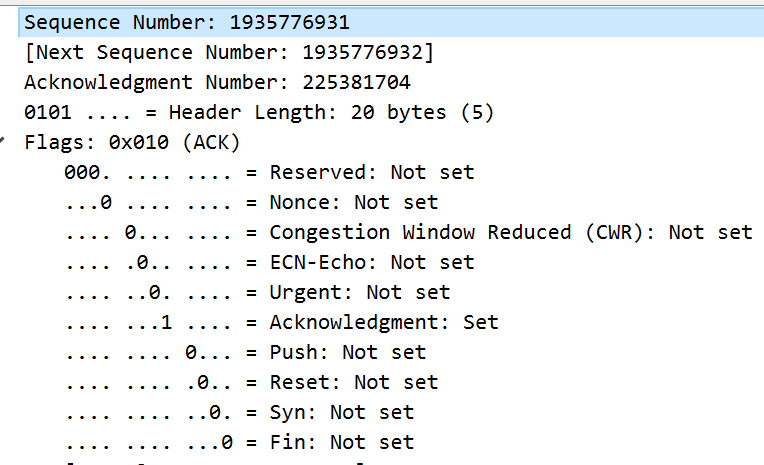
**Що в TCP пакеті вказує, що він є SYN ACK пакетом?**

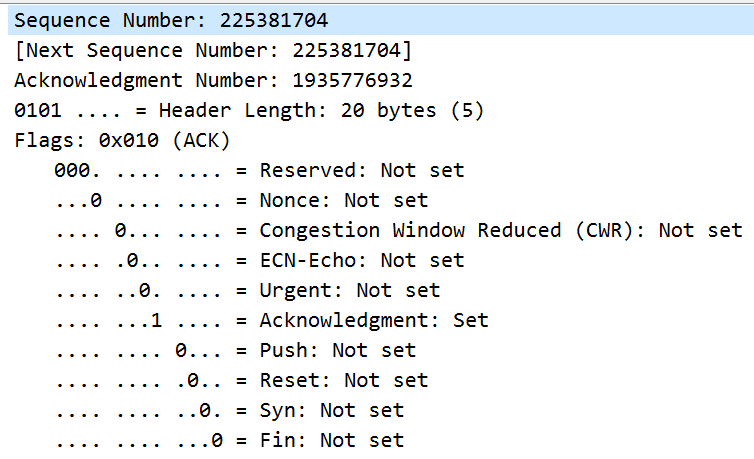
Наявність флагів SYN та ACK.

**Яке значення поля підтвердження «ACKnowledgement» містить даний пакет. Звідки сервер взяв це значення?**

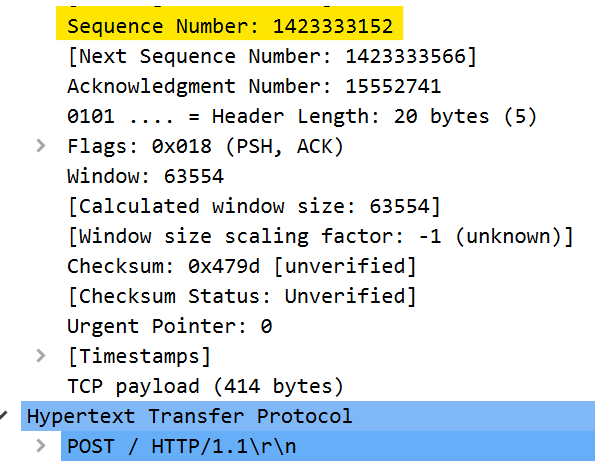


**Які значення ідентифікаторів в наступних декількох сегментах.**

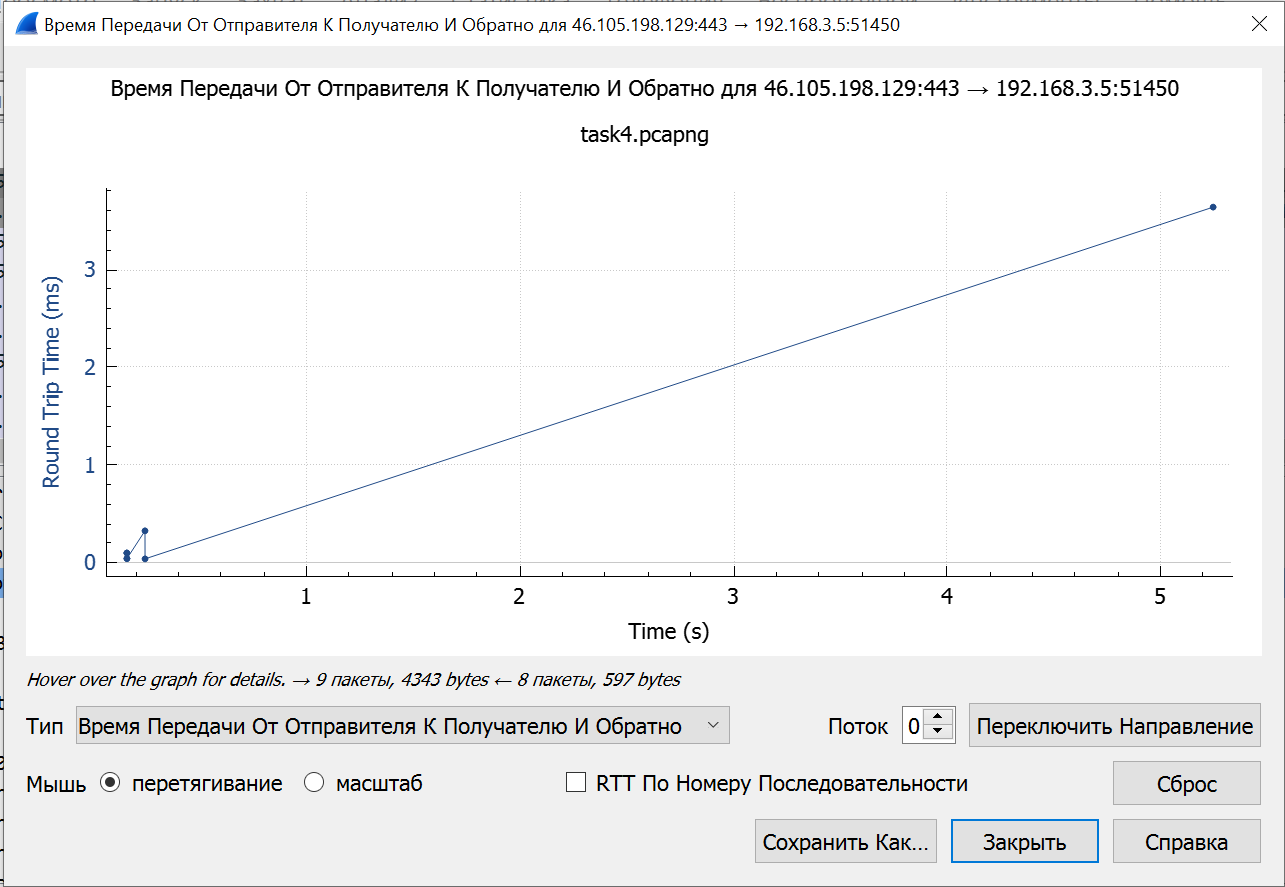
 



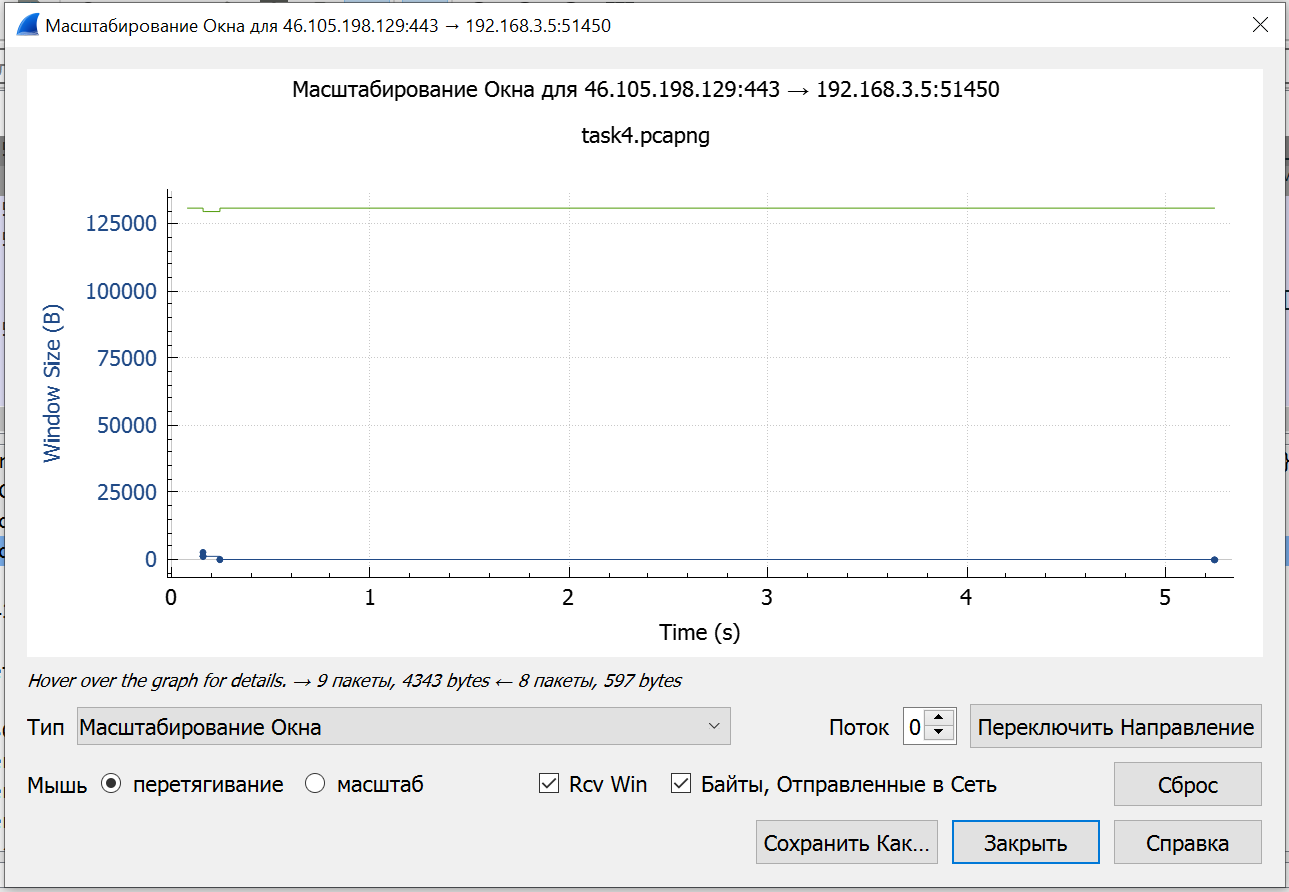
**Який порядковий номер TCP сегмента, що містить HTTP POST команду? (Для знаходження команди POST вам потрібно детальніше глянути на вміст пакету у вікні детального перегляду та знайти у полі даних фрагмент з командою “POST”.)**



**У Wireshark порахуйте значення RTT для з'єднання в цілому. Яка середня швидкість передачі для даного TCP з'єднання. На графіку предачі ТСР пакетів покажіть різні фази з'єднання. Де працює механізм запобігання перевантаження.**



**Розмір буфера у сервера**



**2. Протокол UDP:**

**Виберіть один UDP пакет. Визначте, скільки полів міститься в заголовку обраного UDP пакета. Перерахуйте ці поля. Визначте довжину кожного поля в заголовку UDP.**

* Source Port – порт, який використовується для передачі пакету (2 байти)
* Destination Port – порт, на який буде передаватися пакет (2 байти)
* Length – довжина пакета (2 байти)
* Checksum – контрольна сума. Використовується для того, щоб переконатися, що вміст заголовка UDP і дані не пошкоджені після прибуття (2 байти)

**Яку максимальну кількість байтів може переносити UDP пакет?**

Теоретично, максимальний розмір поля - 65535 байт для UDP-датаграми (8 байт на заголовок та 65527 на дані)

**Який максимальний номер порту джерела повідомлення можливий? (Яке максимальне значення може мати номер порту.)**

Кількість портів обмежена з урахуванням 16-бітної адресації (216 = 65536, початок - "0")

**Який номер протоколу відповідає UDP?**



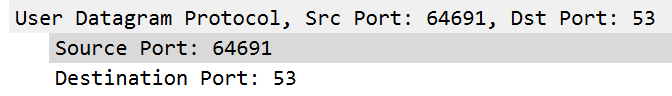
**Пошукайте “UDP” в пошуковій системі Google, та з`ясуйте, по яким полям UDP рахує контрольну суму (checksum).**

Контрольна сума - 16 бітне доповнення до одиниці суми псевдо-заголовка, заповненого інформацією з IP заголовка, UDP заголовка та даних, вирівняних до межі двох байт.

Якщо обчислена сума дорівнює нулю, вона передається як всі одиниці (еквівалентне значення додаткового коду). Нульова контрольна сума в пакеті означає, що сторона, що передає, не вказала контрольну суму (з метою налагодження або при використанні протоколів вищого рівня яким все одно).

**Дослідіть пару UDP пакетів, з яких перший пакет був відправлений вашим комп’ютером, а другий – відповідь на нього. Опишіть взаємозв’язок між номерами портів в цих двох пакетів.**

UDP пакет, відправлений моїм комп’ютером



Відповідь на відправлений UDP пакет

