МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра Інформаційної Безпеки

Практикум з Основ комп’ютерних мереж

Протоколи мережного рівня – IP і ICMP

Перевірив:
_____

Виконав:
студент І курсу
групи ФБ-01
Сахній Н.Р.

Київ 2021

Запустимо ***traceroute*** і змусимо відправляти дейтаграми різної довжини. Послідовність дій відрізняється в залежності від того, на якій платформі виконується – Unix/Linux чи Windows.

Linux/Unix

За допомогою команди ***traceroute*** розмір дейтаграми UDP, що посилається за призначенням, може бути явно встановлений шляхом зазначення кількості байтів дейтаграми. Це значення вводиться в команді ***traceroute*** відразу після імені або адреси призначення.

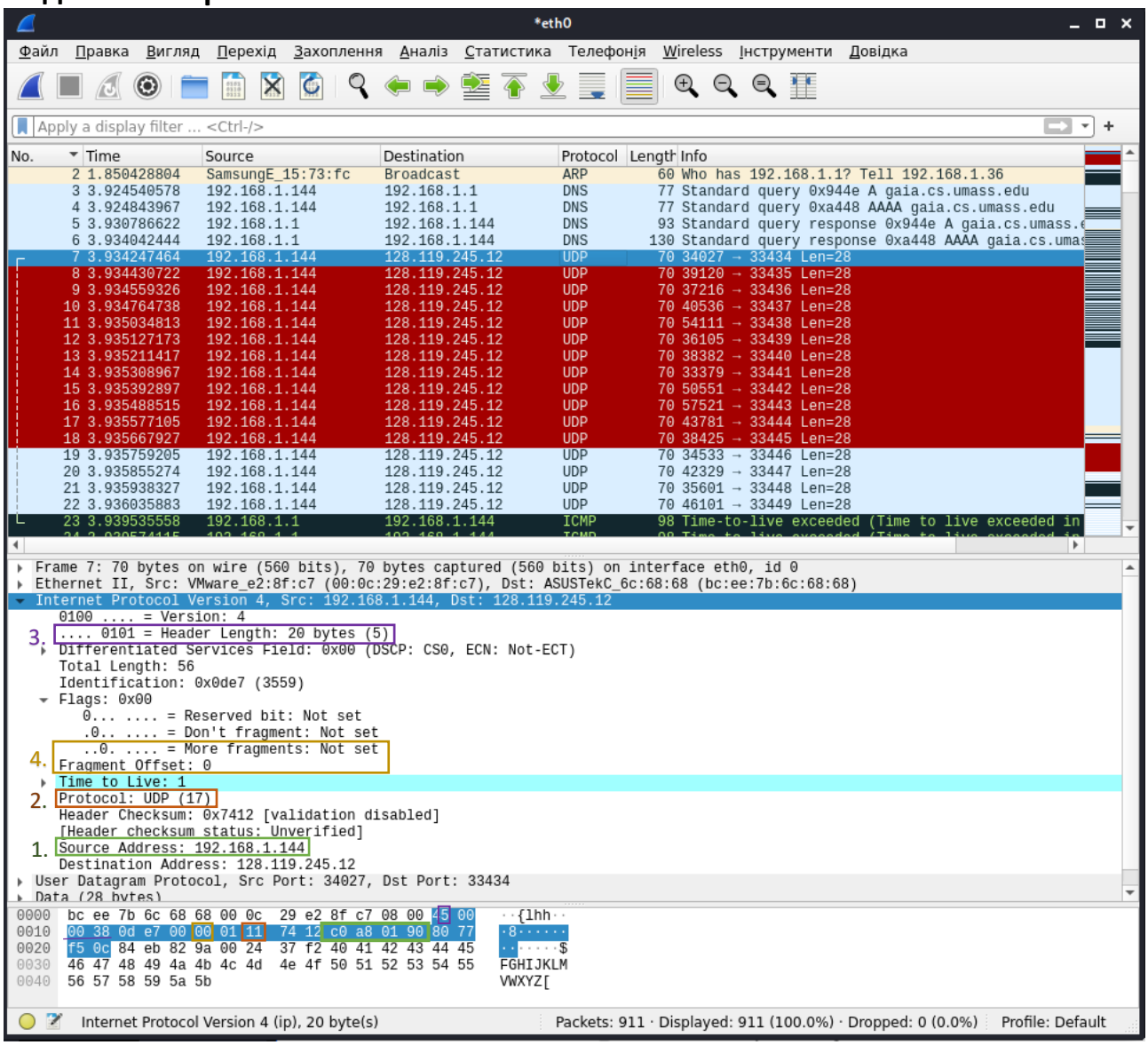
Наприклад, щоб ***traceroute*** відправила дейтаграму довжиною 2000 байт на адресу gaia.cs.umass.edu, команда має виглядати:

$ traceroute gaia.cs.umass.edu 2000

Виконаємо наступні дії:

1. Запустимо Wireshark і почнемо перехоплення пакетів.
2. Введемо 3 команди ***traceroute***, одна з довжиною 56 байт, наступна з довжиною 2000 байт, і остання з довжиною 3500 байт.
3. Зупинимо перехоплення пакетів

Дослідження перехоплених пакетів IP



У перехоплених даних ми повинні побачити серію ICMP exo-запитів або сегментів UDP, що були відправлені, та відповіді на них проміжних маршрутизаторів.

1. Виберемо перший ICMP ехо-запит, який був посланий моїм комп'ютером, і розкриємо деталі заголовку протоколу IP. Якою є IP адреса мого комп’ютера?

Як показано на рисунку зверху↑ IP адреса мого комп’ютера 192.168.1.144

2. Дивлячись на заголовок IP, сказати яким є значення поля протоколу вищого рівня.

Тут значення поля протоколу вищого рівня 17, яке означає, що на вищому рівні протокол UDP

3. Який розмір має IP заголовок? Скільки байтів містять дані корисного навантаження IP дейтаграми? Пояснити, як це визначено.

Розмір IP заголовка рівний 20 байтам. Дані корисного навантаження IP дейтаграми знаходяться як різниця довжини пакета та довжини заголовка: 56 – 20 = 36 (байтів)

4. Чи була ця IP дейтаграма фрагментована? Пояснити свою відповідь.

Ні, не була фрагментована, на що вказує флаг “More fragments” та “Зміщення пакета”, які рівні нулю.

Далі, відсортуємо пакети трасування за IP адресою відправника. Виберемо перший ICMP ехо-запит і розкриємо деталі заголовку протоколу IP.

5. Які поля IP дейтаграми завжди змінюються?

Identification (ідентифікує пакет), Header Checksum (забезпечує цілісність заголовку). Адже вони є унікальними для кожного пакета

6. Які поля IP дейтаграми не змінюються? Які поля не мають змінюватися? Які поля мають змінюватися? Чому?

Не змінюються: Version, Header Length, Total Length, Flags, Fragment Offset, Protocol, Source Address, Destination Address;

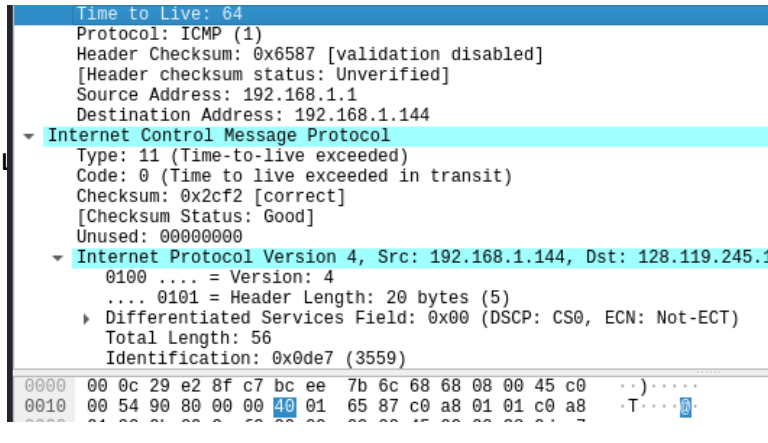
Не мають змінюватись: Version (бо ми використовуємо IPv4 для всіх запитів), Header Length (такі запити мають довжину 20 байт), Total Length (саме в тих запитах, що були відправлені з однаковою довжиною), Protocol (протокол вищого рівня для всіх пакетів буде UDP), Source Address та Destination Address (адже запити відбувається між двома незмінними вузлами);

Мають змінюватись: Identification (ідентифікує пакет, тому унікальне), Time to Live (має збільшуватись через кожні три запити), Header Checksum (забезпечує цілісність заголовку, унікальне).

Далі, знайдемо пакети ICMP відповідей.

7. Якими є значення полів ідентифіка

Identification 0x9080 (36992),
Time to Live: 64

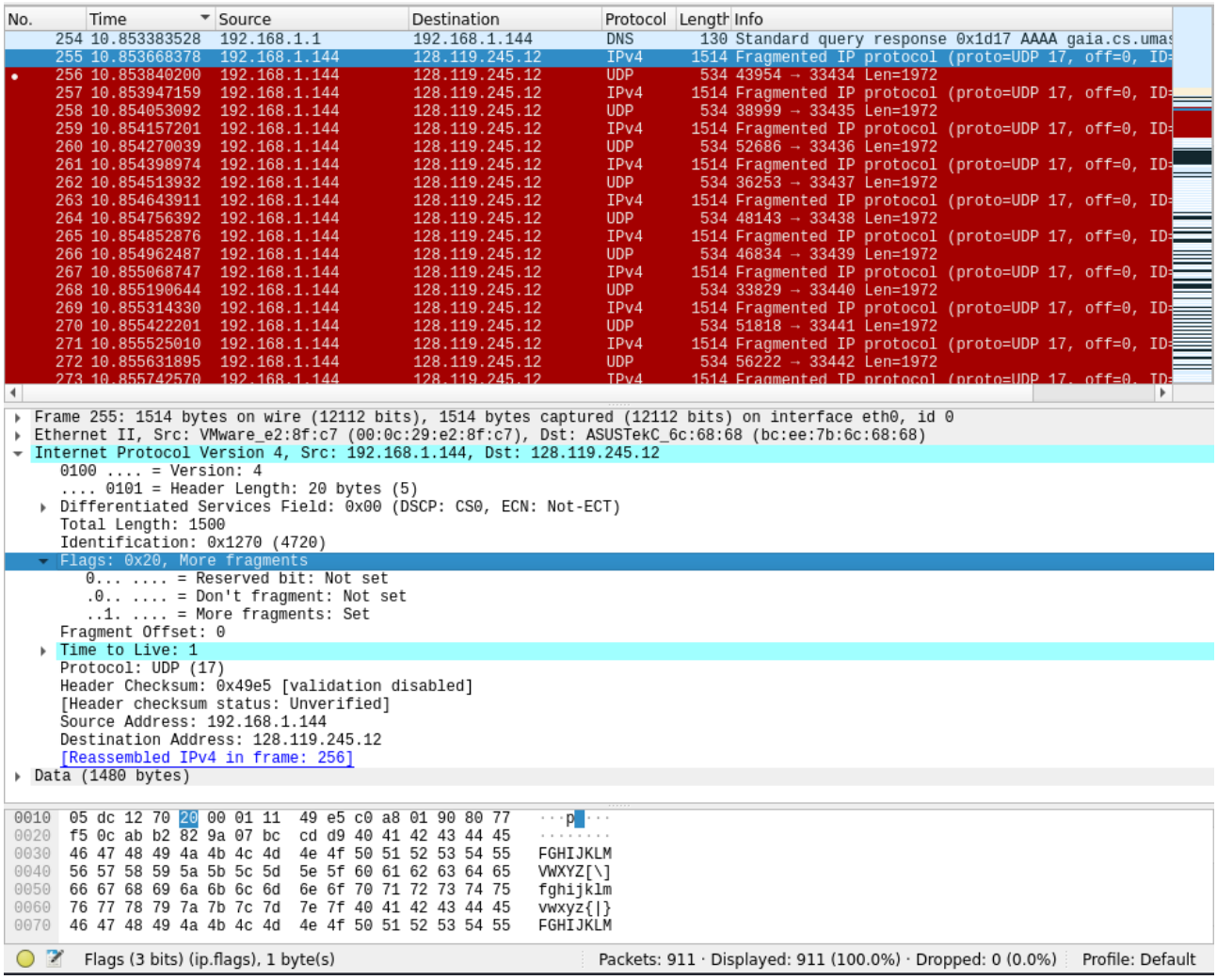


8. Чи ці значення не змінюються для всіх ICMP пакетів, що були послані на мій комп’ютер найближчим роутером? Чому?

Identification змінюється, адже це значення унікальне для кожного пакета.
TTL пакетів, що послані найближчим роутером не змінюється і є якомога більші, тому що пакет повинен точно повернутися до нас, поки не став не діючим.

Фрагментація

Відсортуємо лістинг пакетів за часом.



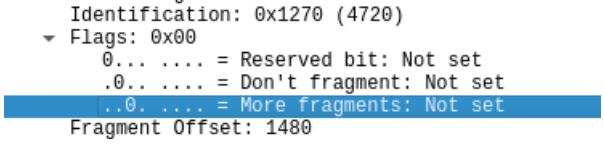
9. Знайдемо перший ICMP Echo Request. Чи було це повідомлення фрагментованим на декілька дейтаграм?

Знайдено перший пакет↑, що був відправлений після команди “traceroute 2000”. Воно фрагментоване на декілька дейтаграм.

10. Виведемо перший фрагмент фрагментованої IP дейтаграми. Яка інформація підкаже, що ця дейтаграма була фрагментована? Якої довжини ця IP дейтаграма?

Оскільки це перший фрагмент фрагментованої IP дейтаграми, то на фрагментованість вказує флаг 1 у полі More fragments: Set; Total Length: 1500 байт

11. Виведемо другий фрагмент. Яка інформація покаже, що це не перший фрагмент? Чи існують ще якісь фрагменти? Чому?



Те, що це фрагмент тієї ж IP дейтаграми вказує однакове значення Identification: 0x1270 (4720), а те, що він другий і після нього більше немає фрагментів вказує флаг0 у полі More fragments: Not set та поле Fragment Offset: 1480

12. Скільки фрагментів було створено з оригінальної дейтаграми?

3 оригінальної дейтаграми створено 2 фрагменти.

13. Яке поле змінюється в IP заголовку у фрагментах?

Total Length (для першого 1500 байтів, а для другого 520), Flags (у першому фрагменті має значення 20, а в другому 00), Fragment Offset (у першому 0, а в другому 1480) та Header checksum (унікальне значення).

Дослідження протоколу ICMP

Далі ми розглянемо деякі аспекти протоколу ICMP:

- ICMP повідомлення, які генеруються програмою *ping*;
- ICMP повідомлення, які генерується програмою ***traceroute***;
- Формат та зміст ICMP повідомлень.

ICMP та ping

Почнемо дослідження ICMP за допомогою програми *ping*. Програма *ping* – це простий засіб, який дозволяє будь-якому користувачеві перевірити досяжність деякої IP адреси. Програма *ping* відправляє пакет ICMP (exo-запит) на цільову IP адресу, яку ми перевіряємо, та або відповідає, надсилаючи нам пакет ICMP (exo-відповідь), або не відповідає.

Виконаймо наступне:

1. Запустимо командне вікно (Unix/Linux – shell).
2. Запустимо Wireshark і почнемо перехоплення пакетів.
3. В командному рядку наберемо команду

$ ping -c 10 <hostname>

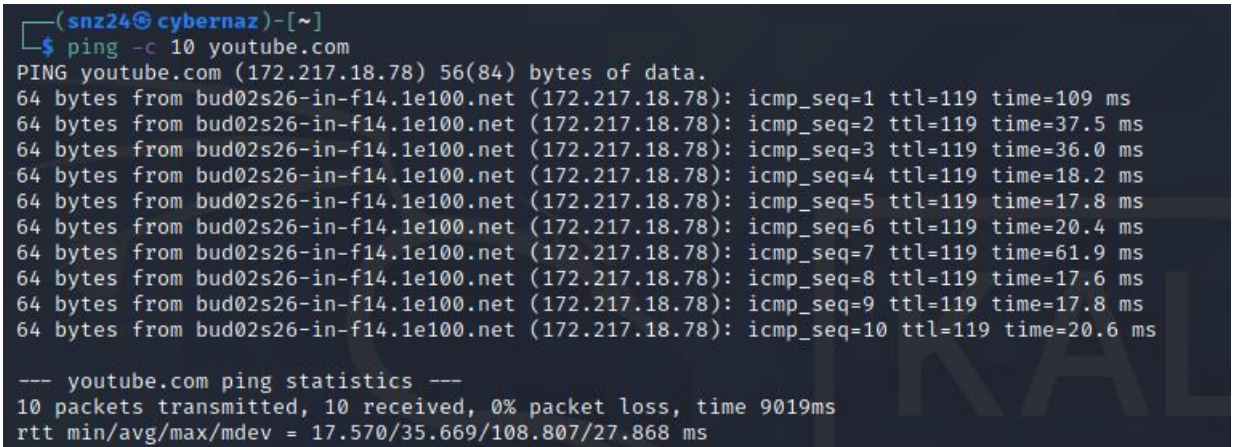
де *hostname* – це доменне ім'я або IP адреса хосту.

Пояснити, що означає аргумент 10:

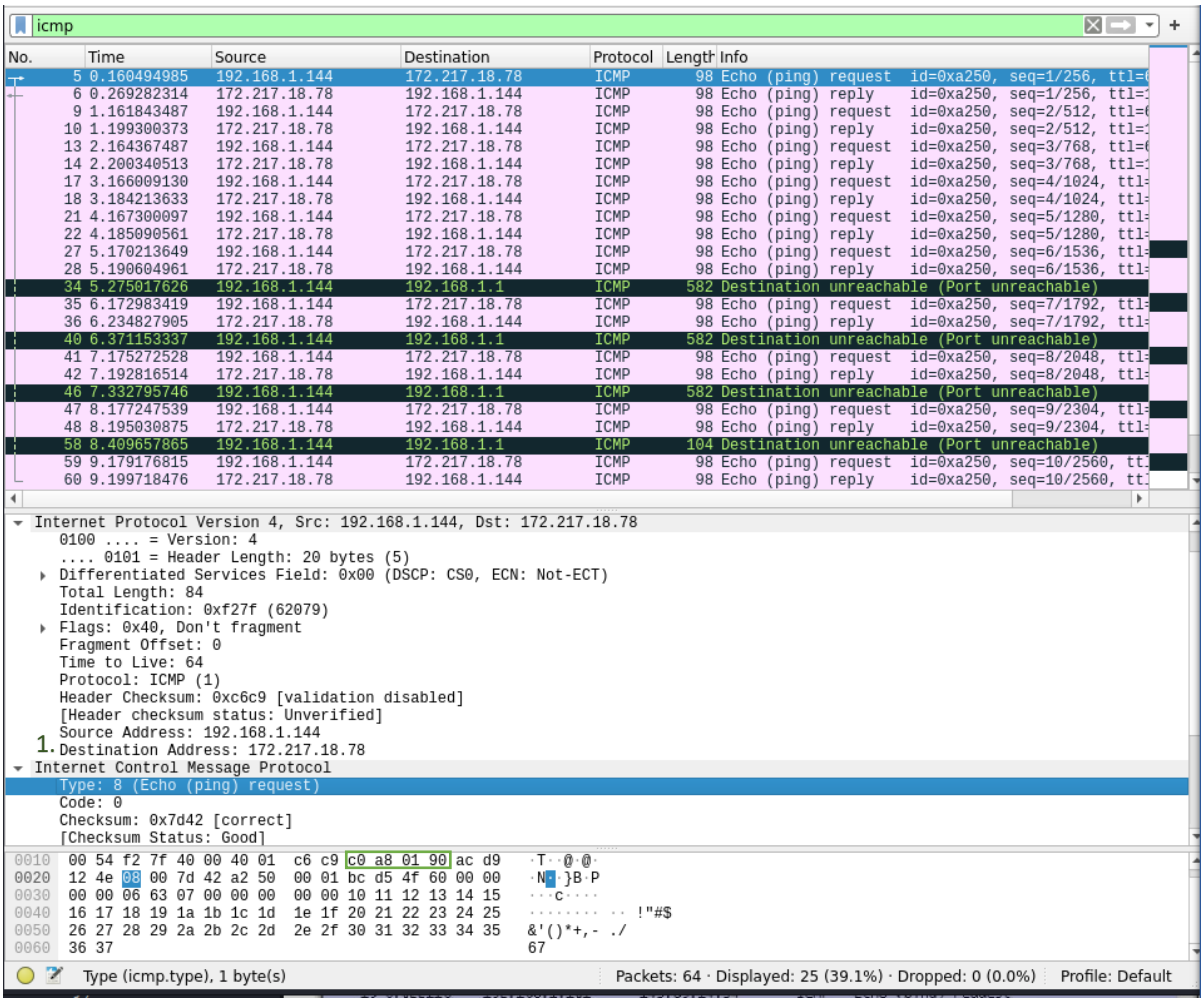
Означає, що TTL пакета дорівнює 10

4. Спостерігаємо за результатами, які виводить програма *ping*. Після завершення роботи програми треба зупинити перехоплення пакетів Wireshark.

По результатам *ping* – тесту дати відповіді на наступні запитання:



↑Результат роботи програми ping у Shell↑



↑Результат роботи програми ping у вікні Wireshark↑

1. Якою є IP адреса мого комп'ютера? Якою є IP адреса хоста призначення?

Source Address: 192.168.14.144, Destination Address: 172.217.18.78

2. Чому ICMP пакети не мають порта відправника та порта призначення?

Номери портів використовуються для того, щоб забезпечити роботу доставки process-to-process, але ICMP не є протоколом транспортного рівня, він є протоколом обміну повідомленнями на мережевому рівні

3. Яким є тип і код ICMP пакету, що був відправлений мною?

Type: 8 і Code: 0, що являються так званим ICMP exo-запитом

4. Яким є тип і код ICMP пакету, що був отриманий мною у відповідь?

Type: 0 і Code: 0, що являються так званою ICMP exo-відповіддю