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

Дослідження Ethernet та ARP

Перевірив:
_____

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

Київ 2021

Завдання. Перехоплення кадрів Ethernet

Відкрив програму Wireshark та почав перехоплення пакетів. Далі ввів наступну силку сайту http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html, що показає US Bill of Rights.
Зупинив перехоплення пакетів. Знайшов номери пакетів запитів HTTP GET, що були надіслані з мого комп'ютера на gaia.cs.umass.edu, потім HTTP повідомлення-відповіді, що були надіслані на мій комп'ютер сервером gaia.cs.umass.edu.

Як показано на рис.1 пакет 95 містить повідомлення HTTP GET, надіслане з мого комп’ютера на gaia.cs.umass.edu

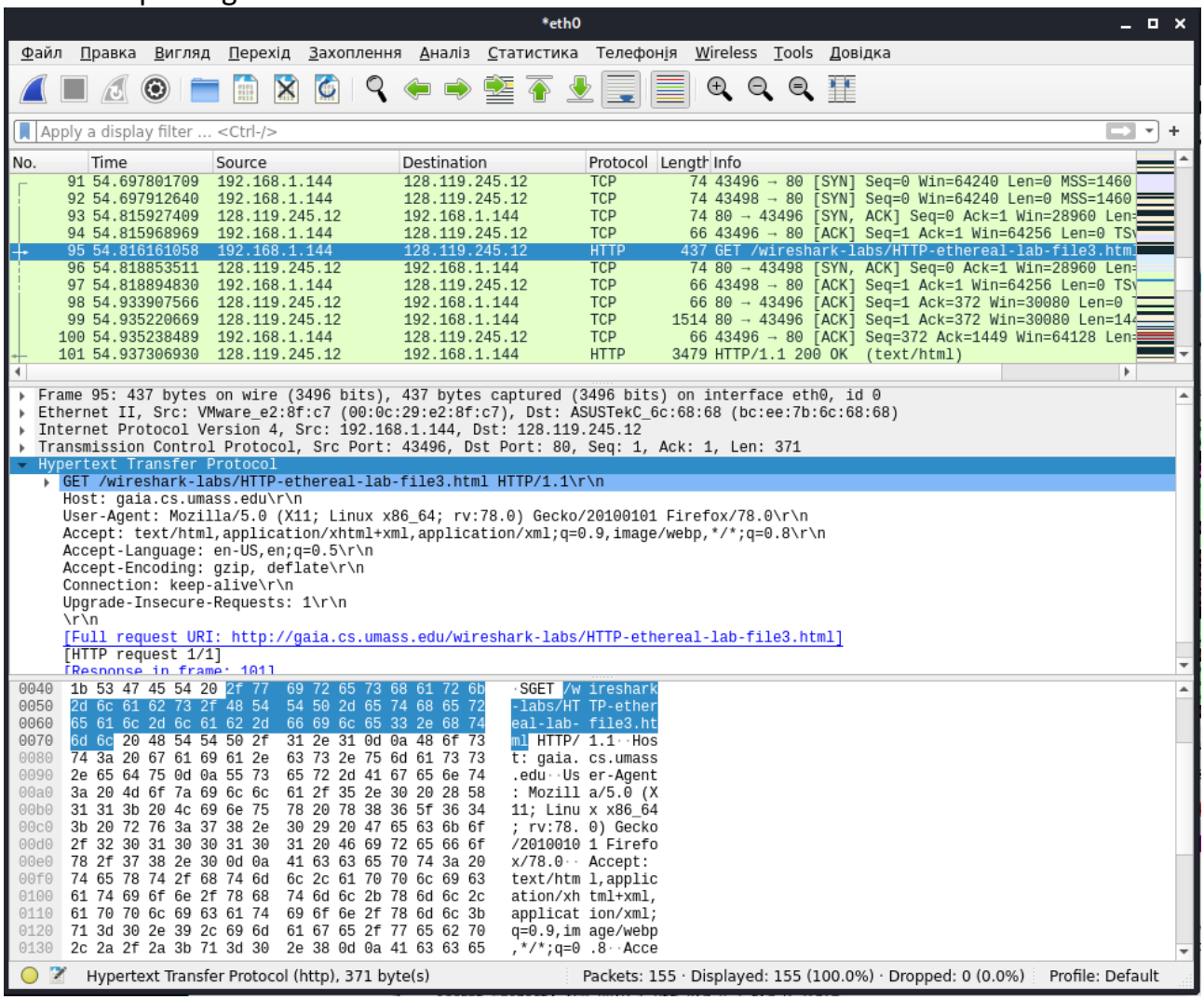

Рис.1 Запит HTTP GET

Вікно Wireshark, що показане на рис. 2 після того, як зняли прапорець з IP в Enabled Protocols. А також виділений пакет 95, що містить повідомлення HTTP GET

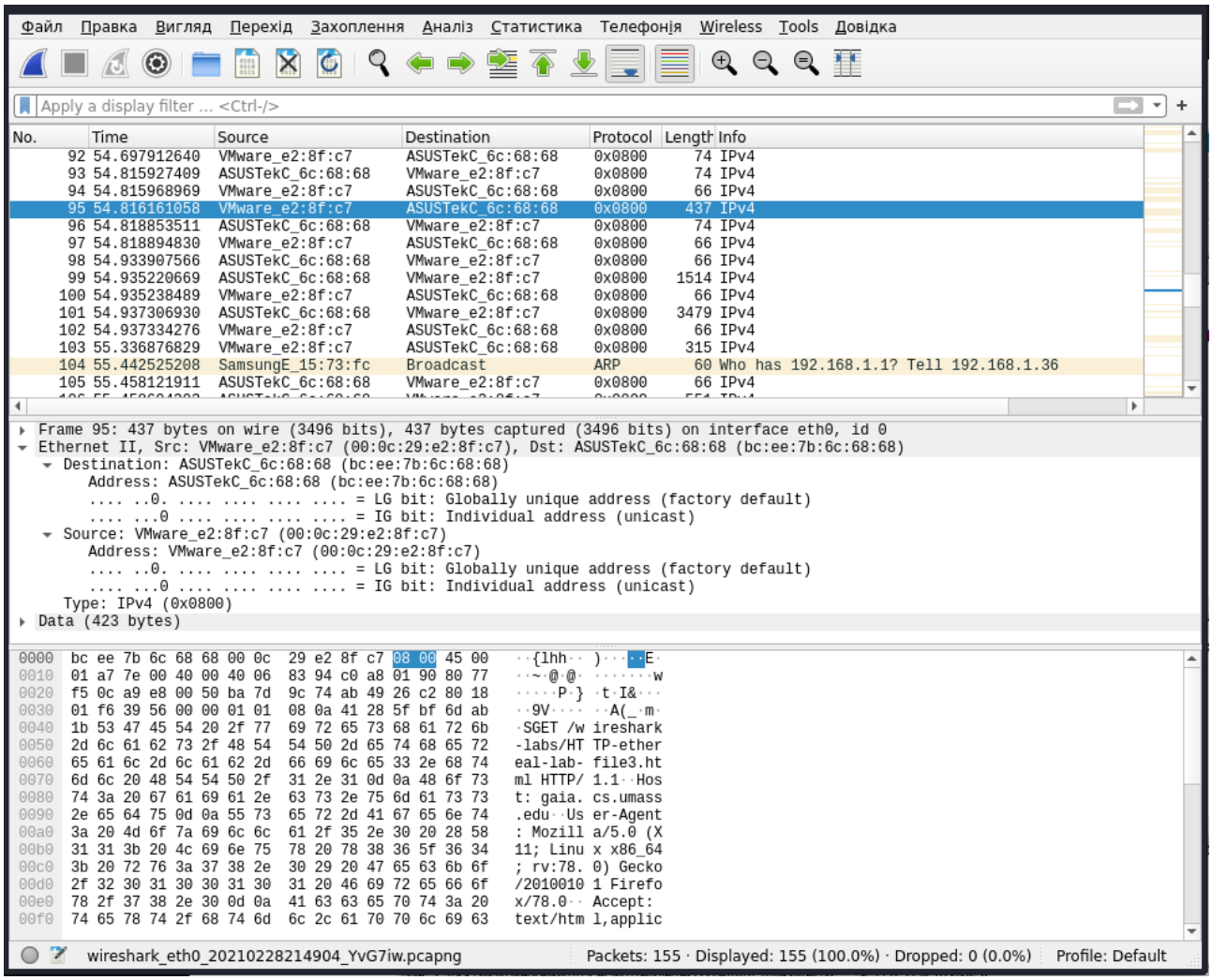

Рис.2 Аналіз кадрів Ethernet

Відповіді на контрольні питання 1-5, які базуються на перехоплених кадрах Ethernet, що містять повідомлення HTTP GET:

1. Якою є 48-бітна MAC адреса Вашого комп’ютера?

ASUSTekC_6c:68:68 (bc:ee:7b:6c:68:68)

2. Якою є 48-бітна MAC адреса отримувача Ethernet кадру? Чи є ця адреса адресою? Якщо ні, то який пристрій має цю Ethernet адресу?

VMware_e2:8f:c7 (00:0c:29:e2:8f:c7) не є адресою сервера gaia.cs.umass.edu, ця MAC адреса належить моїй віртуальній машині на VWware

3. Дайте шістнадцяткове представлення двох-байтового поля типу кадру Ethernet. Що означають біт(и) які дорівнюють 1?

На рис.2 виділено синім 08 00 дане поле в Ethernet II вказує на тип кадру, що визначає буфер пам'яті, в якому повинен зберігатися кадр.

Перший біт адреси одержувача обмежене спеціальним значенням. Якщо він дорівнює 0, то це адреса конкретного пристрою, а якщо 1 - широкомовний.

4. Який відступ в кадрі Ethernet має літера “GET”?
Відступ літери “G” 66 байтів, тобто їй відповідає байт 47

5. Яке шістнадцяткове значення має поле CRC в цьому кадрі? Що це за поле?
Поле контрольної суми (Frame Check Sequence. FCS) складається з 4 байт, вміщуючих контрольну суму. Це значення обчислюється за алгоритмом CRC-32. Після одержання кадру робоча станція виконує власне обчислення контрольної суми для цього кадру, порівнює отримане значення зі значенням поля контрольної суми і, таким чином, визначає, чи не перекручений отриманий кадр. Це поле знаходиться в кінці кадру Ethernet

Відповіді на контрольні питання 6-10, які базуються на перехоплених кадрах Ethernet, що містять повідомлення HTTP відповіді:
На рис.1 пакет 101 містить повідомлення HTTP OK

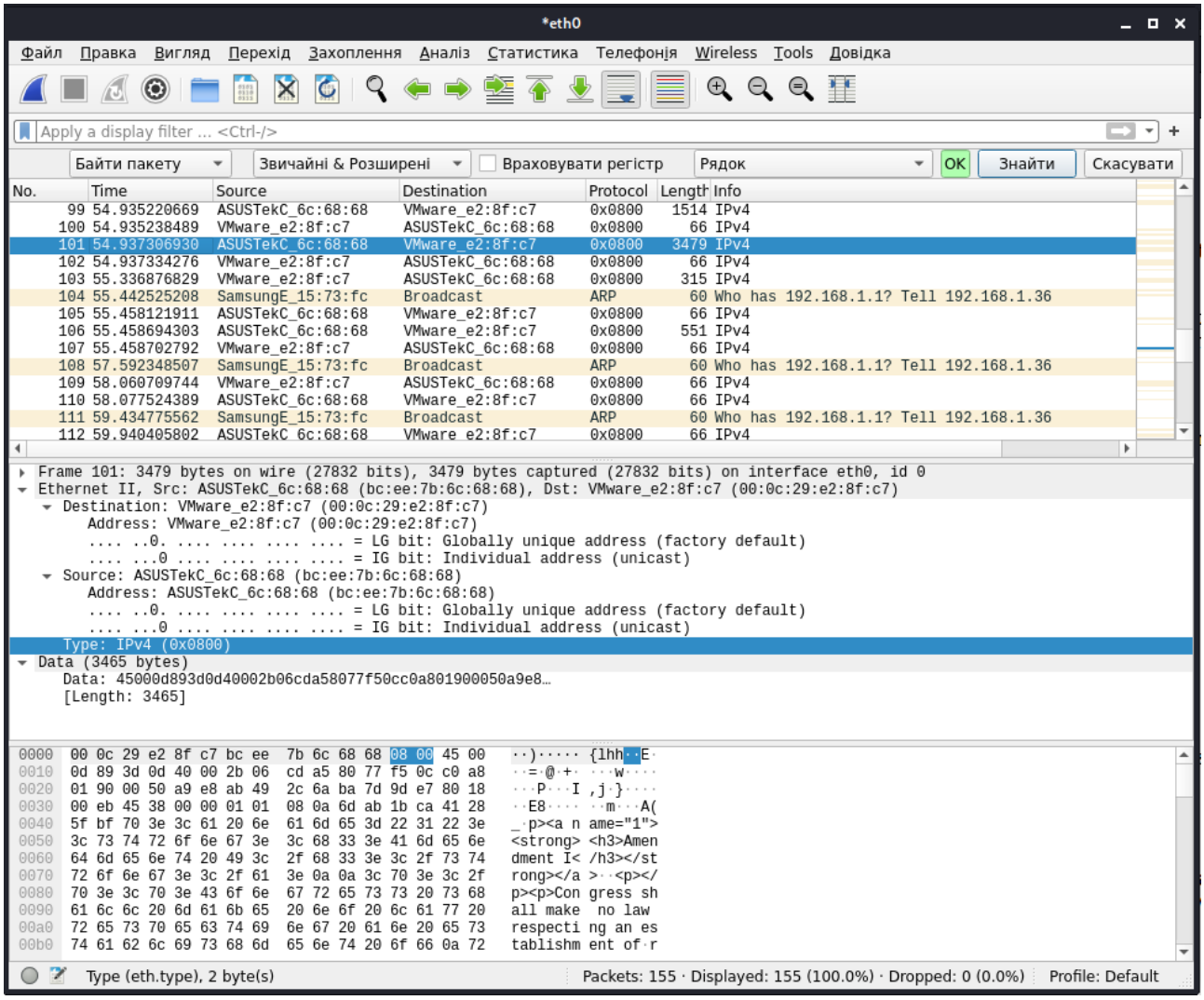

Рис.3 Аналіз кадрів для запиту HTTP OK,

6. Якою є адреса відправника кадру? Чи є це адреса вашого комп’ютера або адреса gaia.cs.umass.edu.

VMware_e2:8f:c7 (00:0c:29:e2:8f:c7) не є адресою сервера gaia.cs.umass.edu, ця MAC адреса належить моїй віртуальній машині на VWware

7. Якою є 48-бітна адреса отримувача Ethernet кадру? Чи є це адреса вашого комп'ютера? Якщо ні, то який пристрій має цю Ethernet адресу?

ASUSTekC_6c:68:68 (bc:ee:7b:6c:68:68), так вона є адресою мого ПК

8. Дайте шістнадцяткове представлення двох-байтового поля типу кадру Ethernet. Що означає біт(и), які дорівнюють 1?

На рис.3 виділено синім 08 00 дане поле в Ethernet II вказує на тип кадру, який вказує тип протоколу верхнього рівня, що вклали в свій пакет у поле даних цього кадру.

9. Який відступ в кадрі Ethernet має літера"O" в "OK"?

Із пакету 99 відступ літери "O" 79 байтів, тобто йому відповідає байт 4f

10. Яке шістнадцяткове значення має поле CRC в цьому кадрі? Що це за поле?

Поле контрольної суми (Frame Check Sequence. FCS) складається з 4 байт, вміщуючих контрольну суму. Це значення обчислюється за алгоритмом CRC-32. Після одержання кадру робоча станція виконує власне обчислення контрольної суми для цього кадру, порівнює отримане значення зі значенням поля контрольної суми і, таким чином, визначає, чи не перекручений отриманий кадр. Це поле знаходиться в кінці кадру Ethernet

Кадр Ethernet DIX(II)

6	6	2	46-1500	4
DA	SA	T	DATA	FCS

Рис.4 Формат типу кадрів Ethernet DIX(II)

Завдання. Спостереження за ARP в дії

```
┌──(snz24㉿cybernaz)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
router.asus.com          ether   bc:ee:7b:6c:68:68   C                     eth0

┌──(snz24㉿cybernaz)-[~]
└─$ arp -d *
Відео: Невідомий вузол
```

Виконавши команду **arp,** ми бачимо вміст arp-кеша комп'ютера, який містить IP-адреси і відповідні їм MAC-адреси вузлів локальної мережі, а також HWtype (тип обладнання), Flags Mask (який тип запису розміщується в пам'яті), Iface (назва інтерфейсу).

Далі було здійснено очищення arp-кеша.

Вікно Wireshark, що показане на рис. 5 після того, як зняли прапорець з IP в Enabled Protocols. А також виділений пакет 481, що містить повідомлення ARP-запиту↓

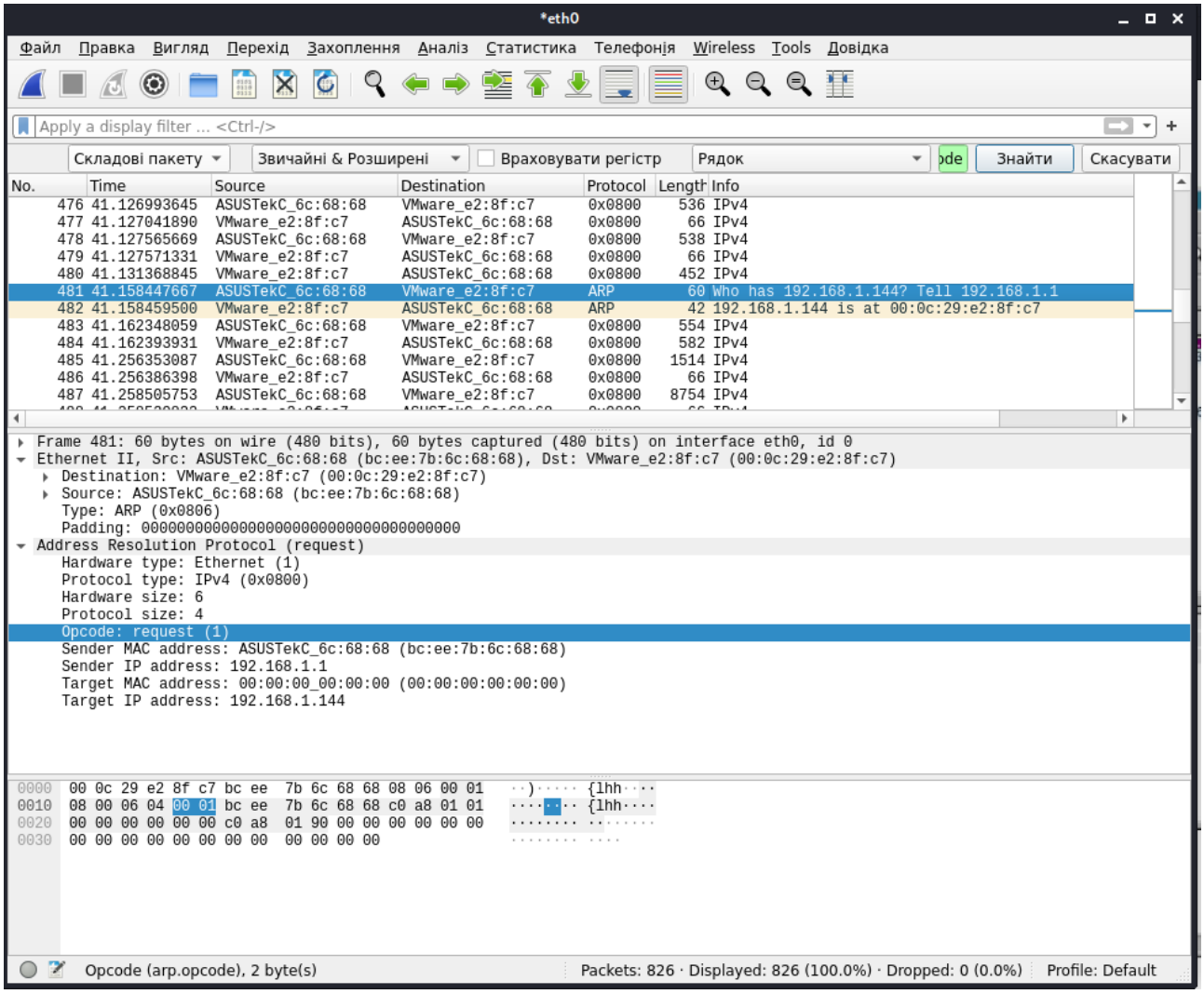

Рис.5 Дослідження протоколу ARP

Відповіді на контрольні запитання 11-16:

11. Які шістнадцяткові значення мають адреса відправника і адреса одержувача в кадрах Ethernet, що містить повідомлення ARP?

ASUSTekC_6c:68:68 (bc:ee:7b:6c:68:68) – адреса відправника запиту;
VMware_e2:8f:c7 (00:0c:29:e2:8f:c7) – адреса одержувача.

12. Дайте шістнадцяткове представлення поля типу кадру Ethernet.

Код 08 06 це тип протоколу трансляції адреси (ARP).

13. З якого байту кадру Ethernet починається поле opcode?

Як показано на рис. 5, воно починається з 21-го байта

14. Яке значення має поле opcode?

Поле opcode позначає чи пакет є запитом (1) чи відповіддю (2), його шістнадцяткове значення 00 01, виділено синім на рис. 5

15. Чи містить ARP повідомлення IP адресу відправника?

Так містить. ARP 60 Who has 192.168.1.144? Tell 192.168.1.1

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

Це пакет 482 (на рис.5). У ньому міститься MAC-адрес одержувача запиту