**Харківський національний економічний університет**

**імені Семена Кузнеця**

**ЗВІТ**

**З ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ № 3**

**за дисципліною: *“*** **Корпоративні мережі та системи доступу**”

**на тему: “Аналіз захоплених пакетів TCP за допомогою програми Wireshark ”**

**Виконав: студент факультету Інформаційних технологій**

**3 курсу, спец. Кібербезпека,**

**групи 6.04.125.010.21.2**

**Бойко Вадим Віталійович**

**Перевірив:**

**Чугай Андрій Михайлович**

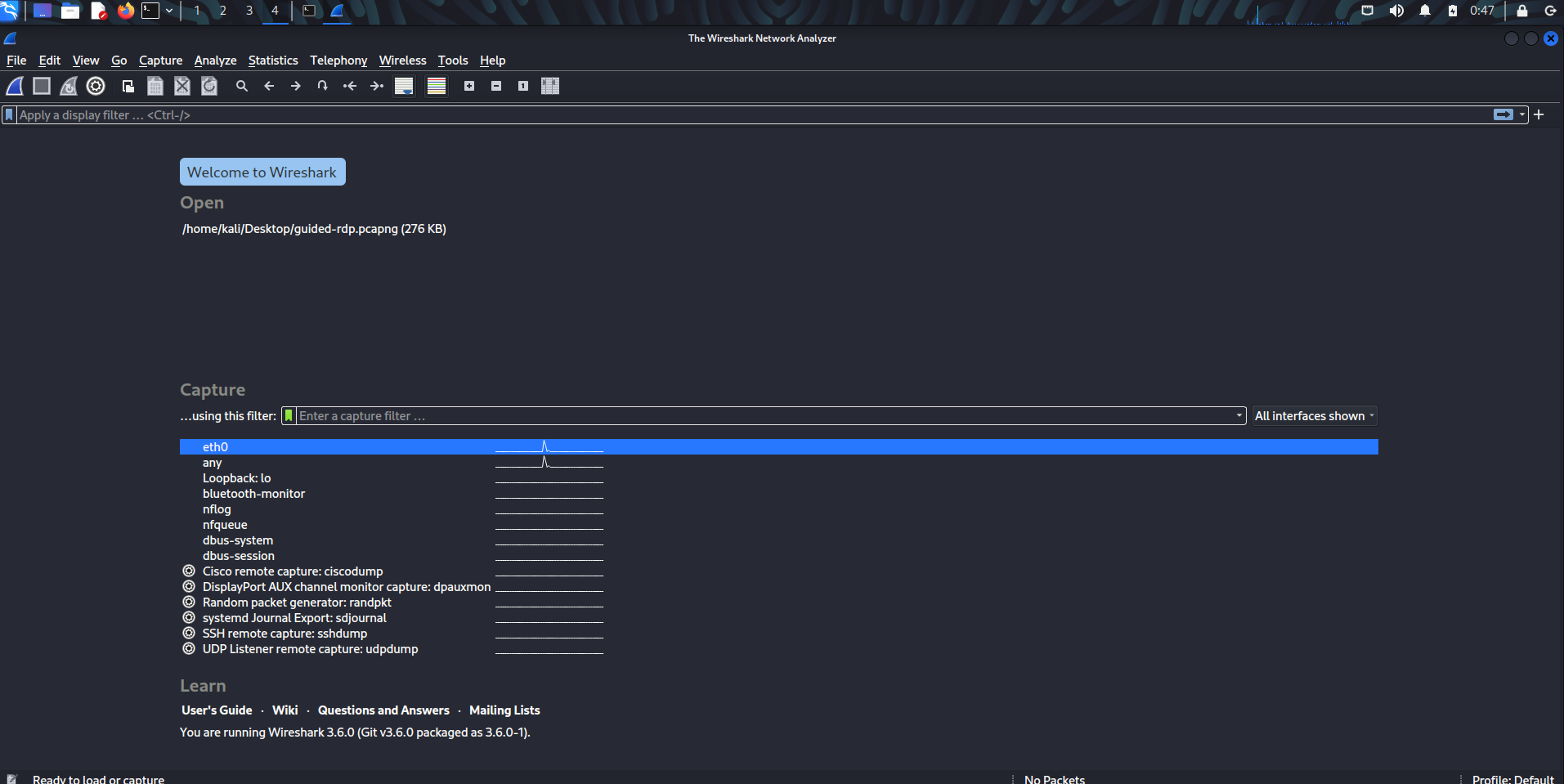
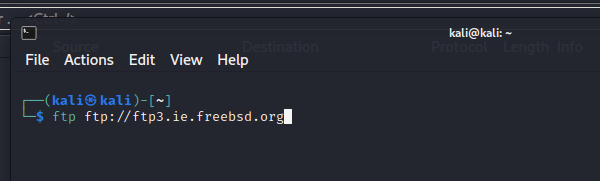
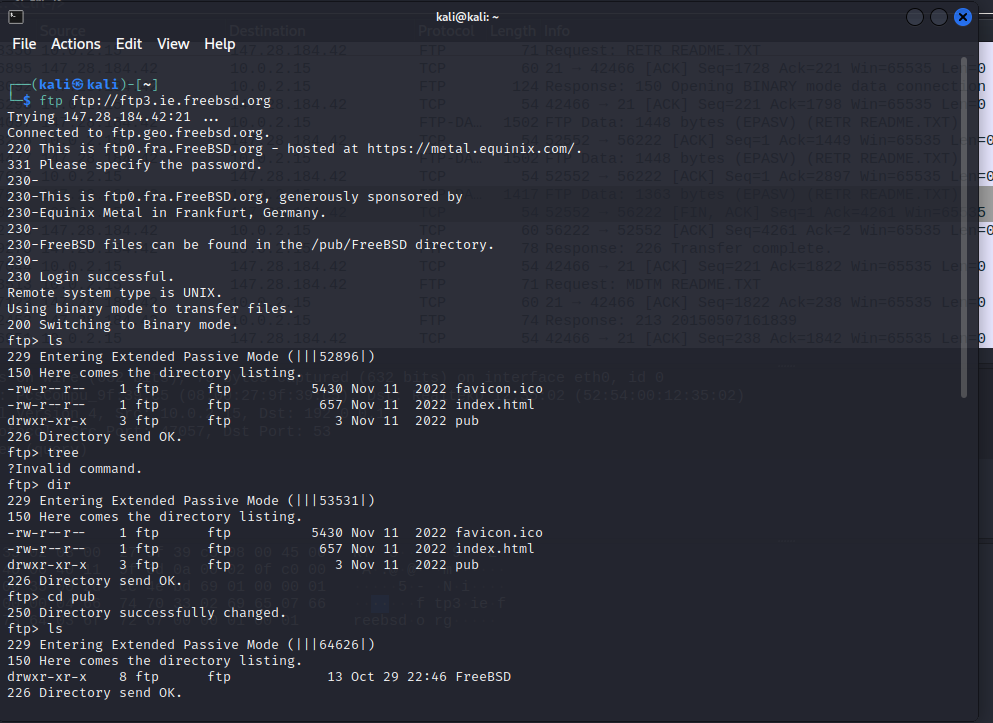
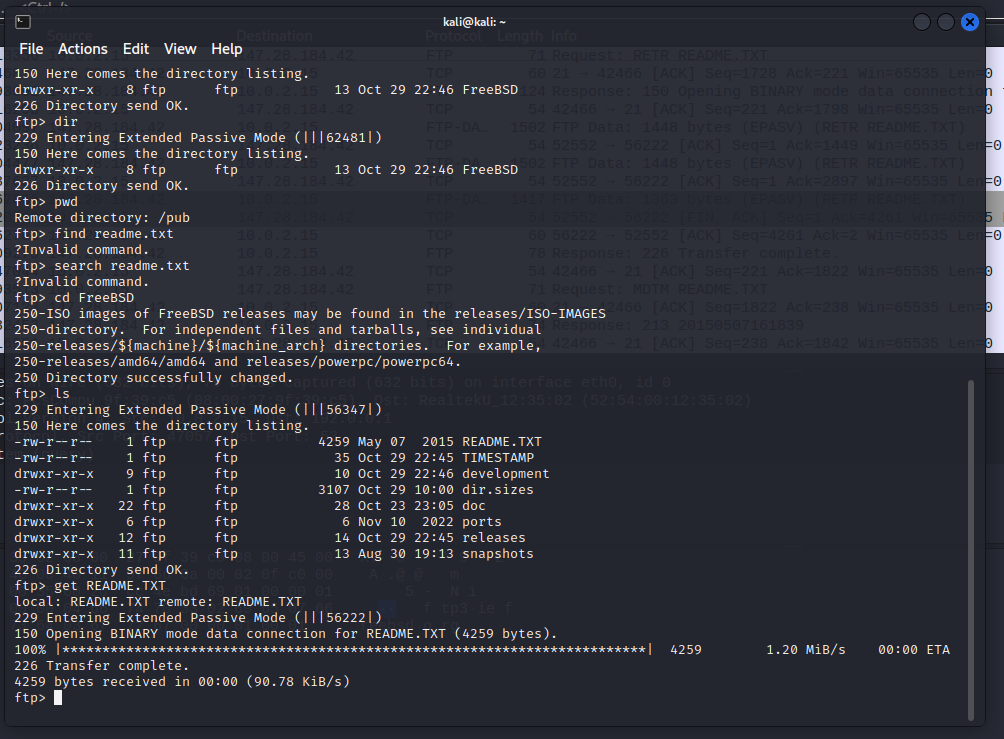
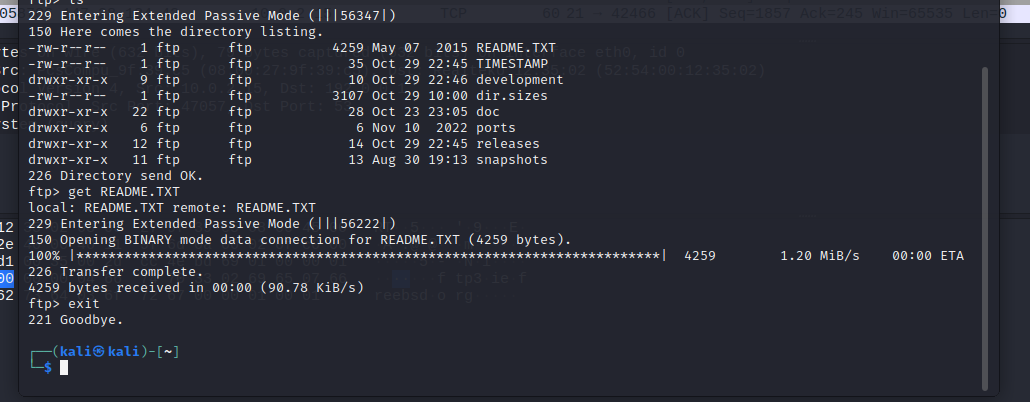
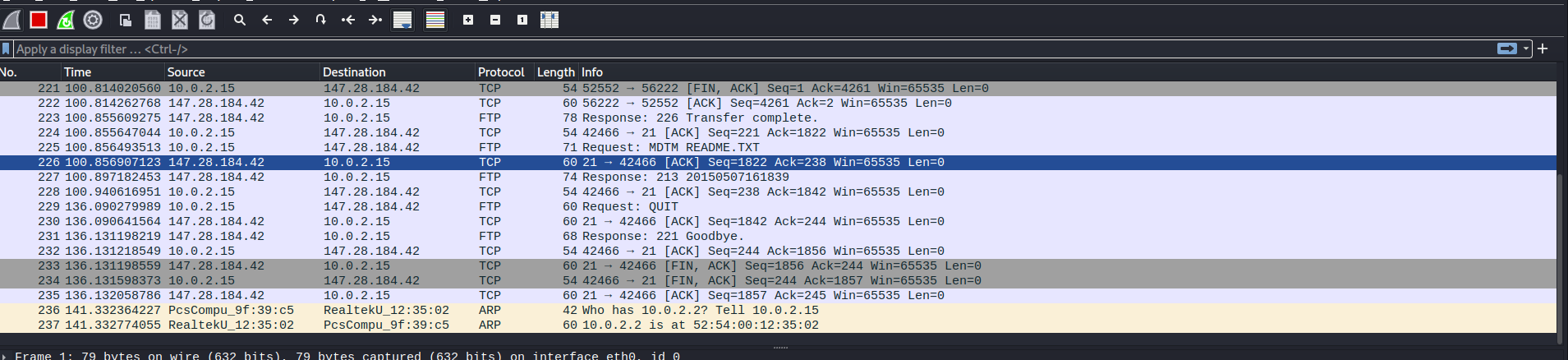
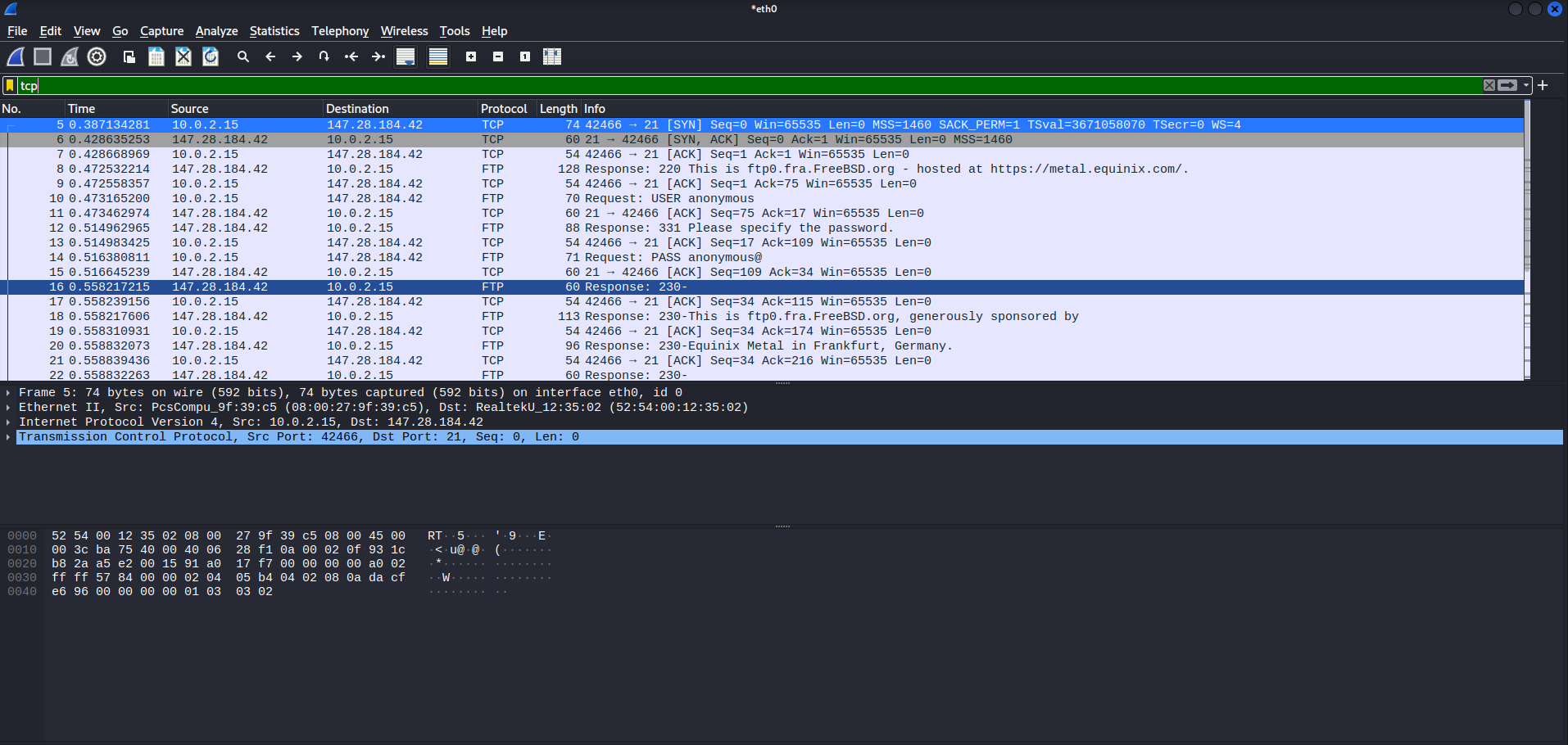
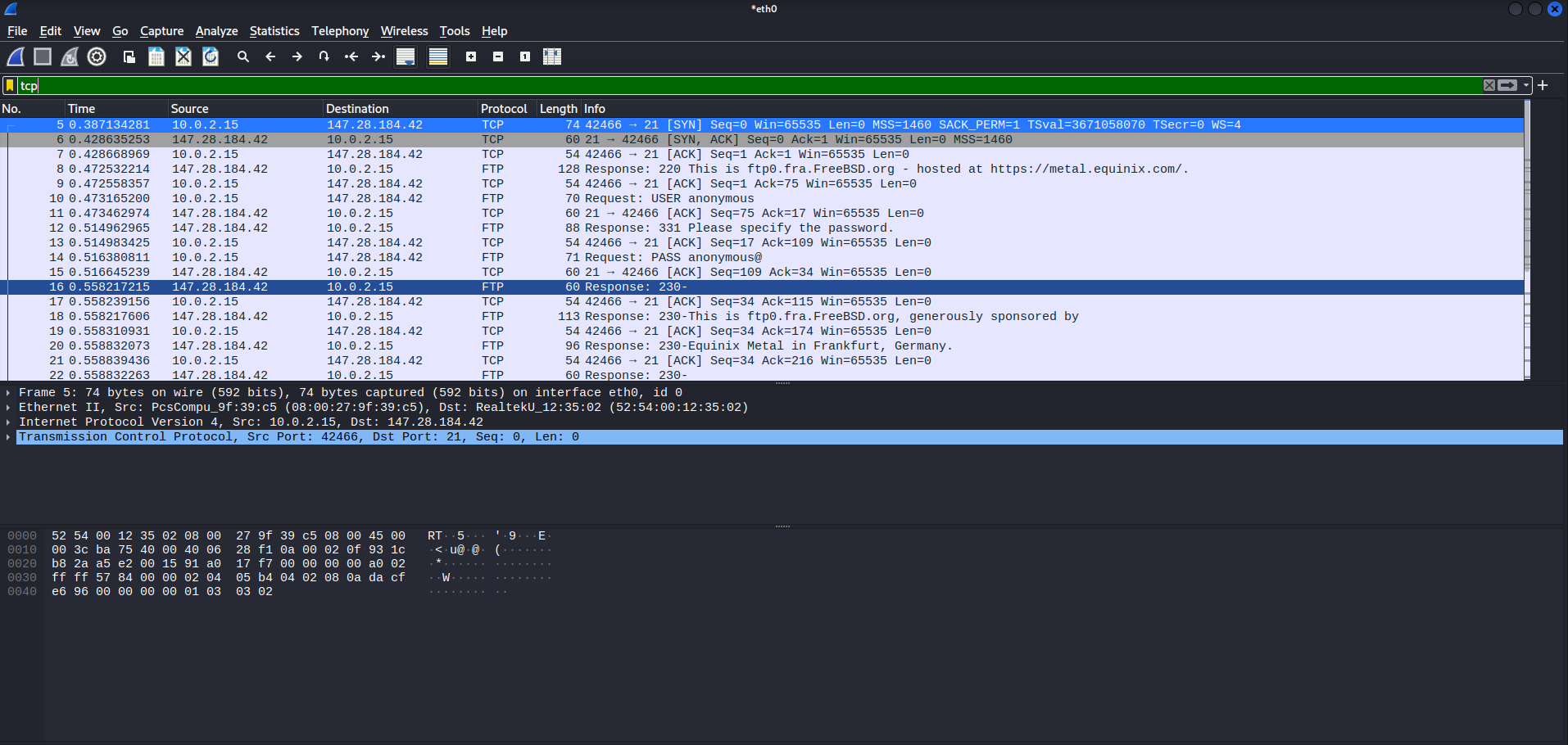
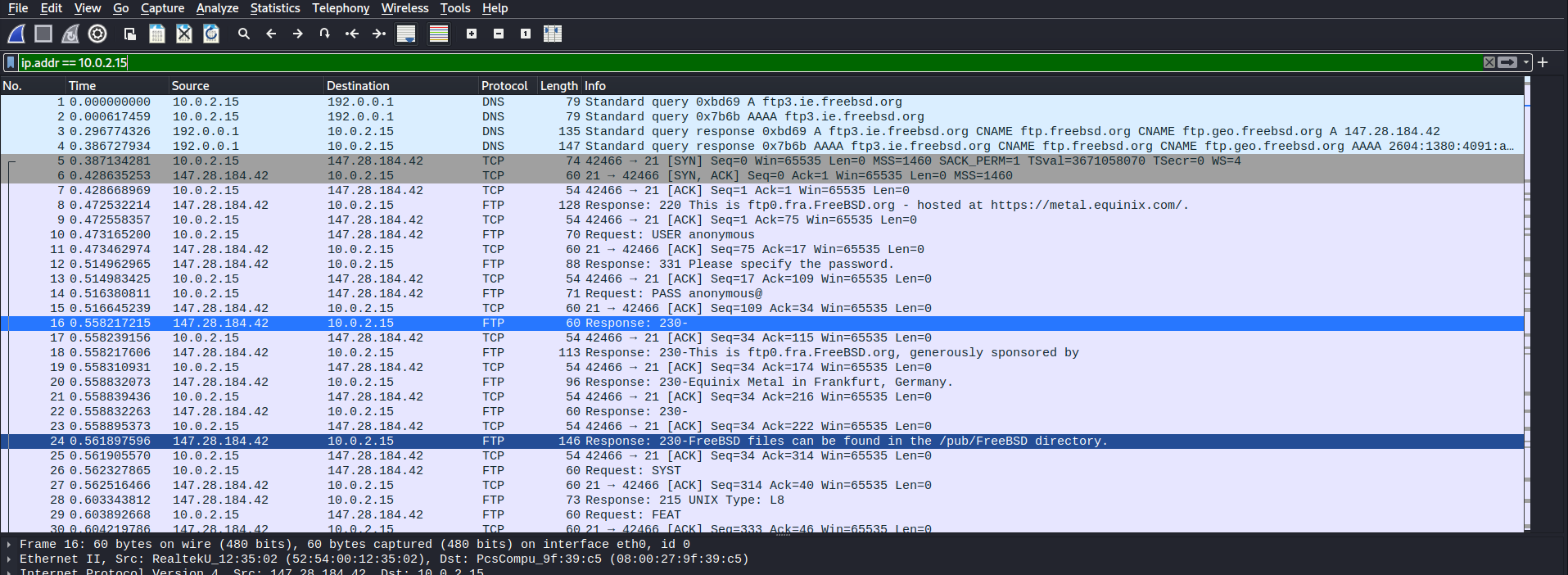
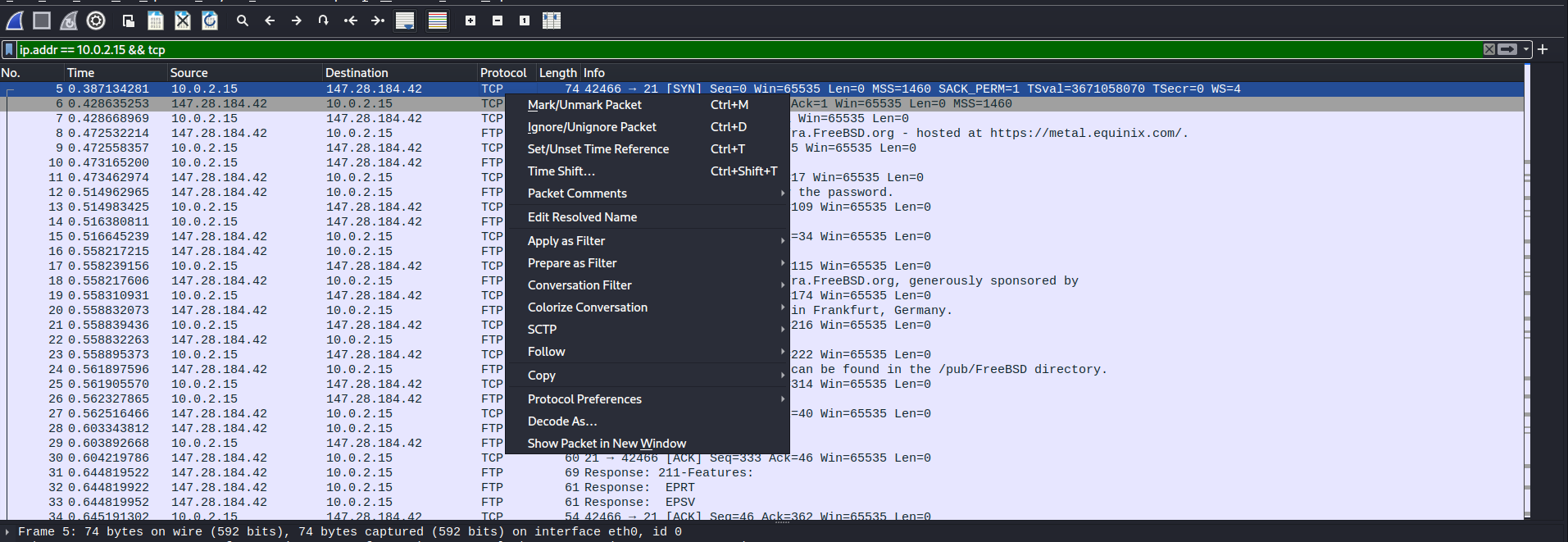
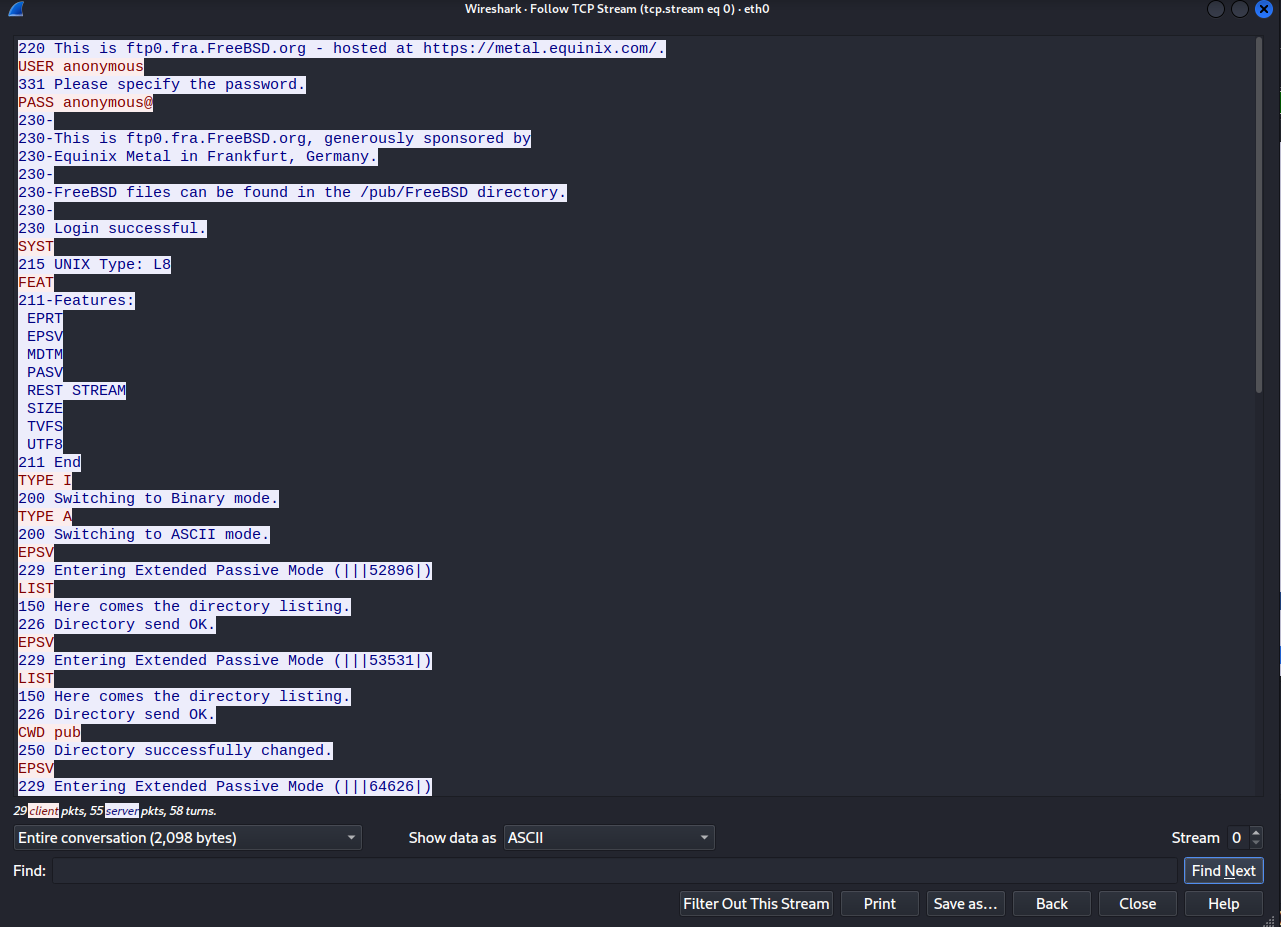
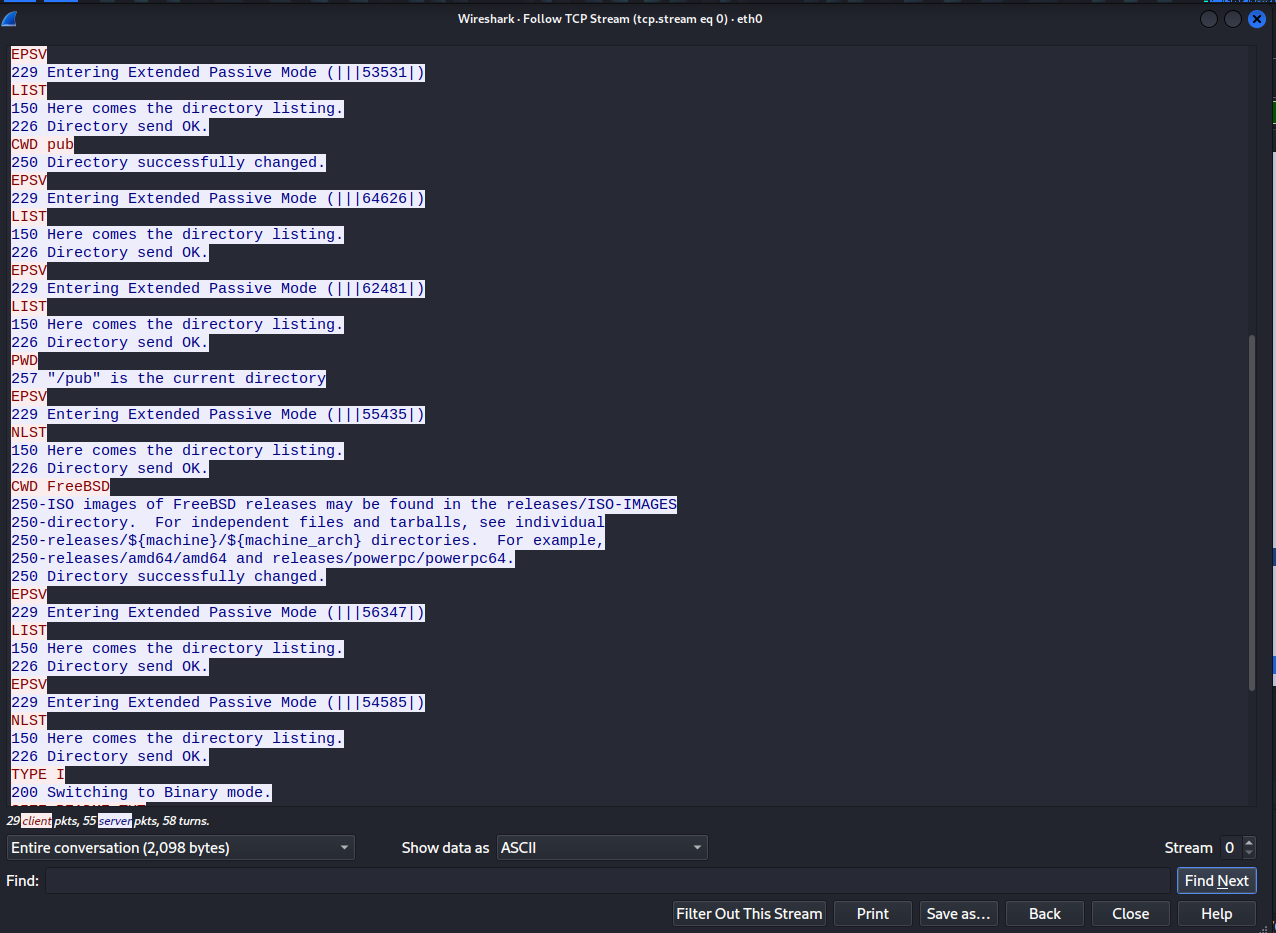
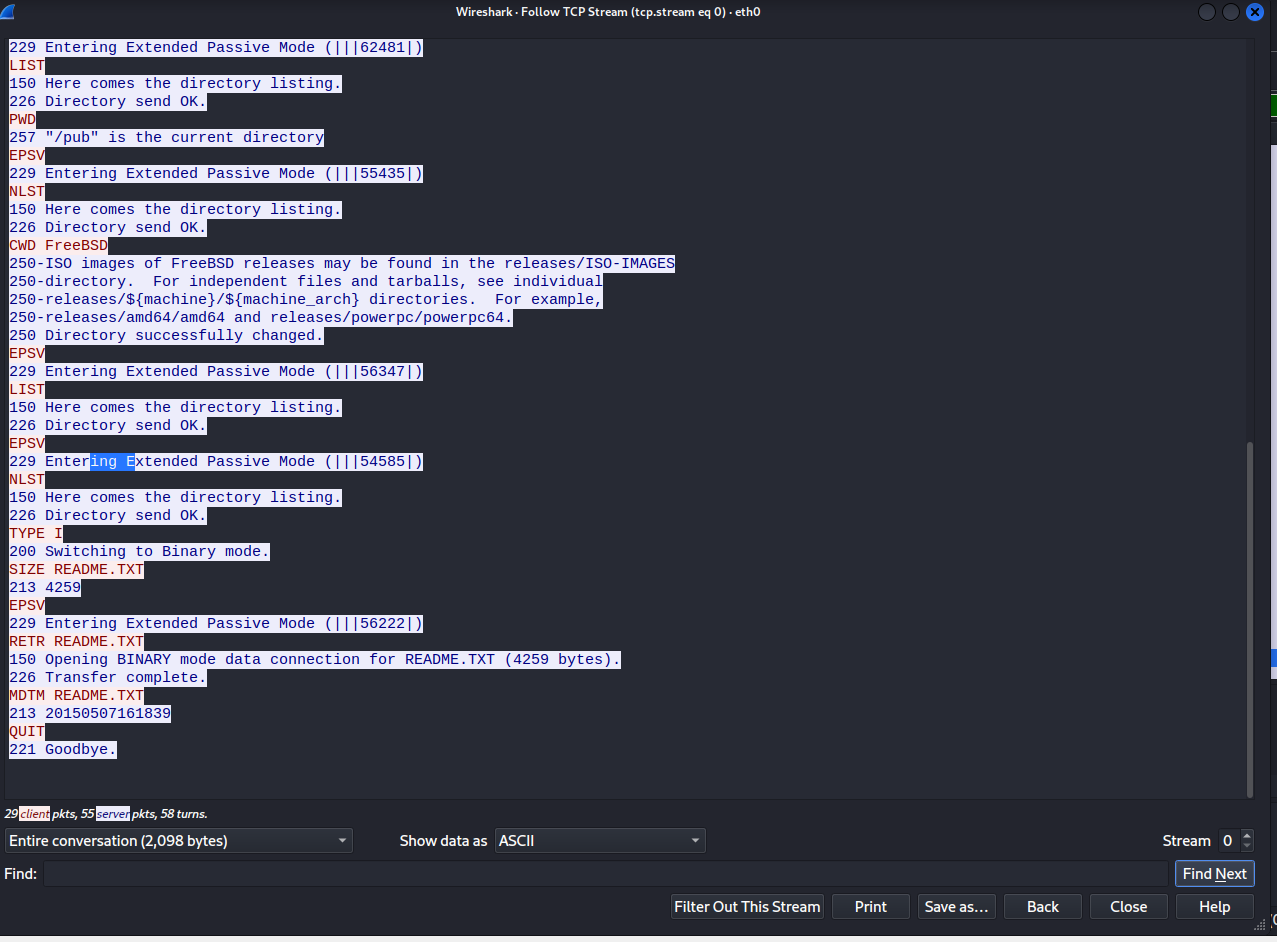
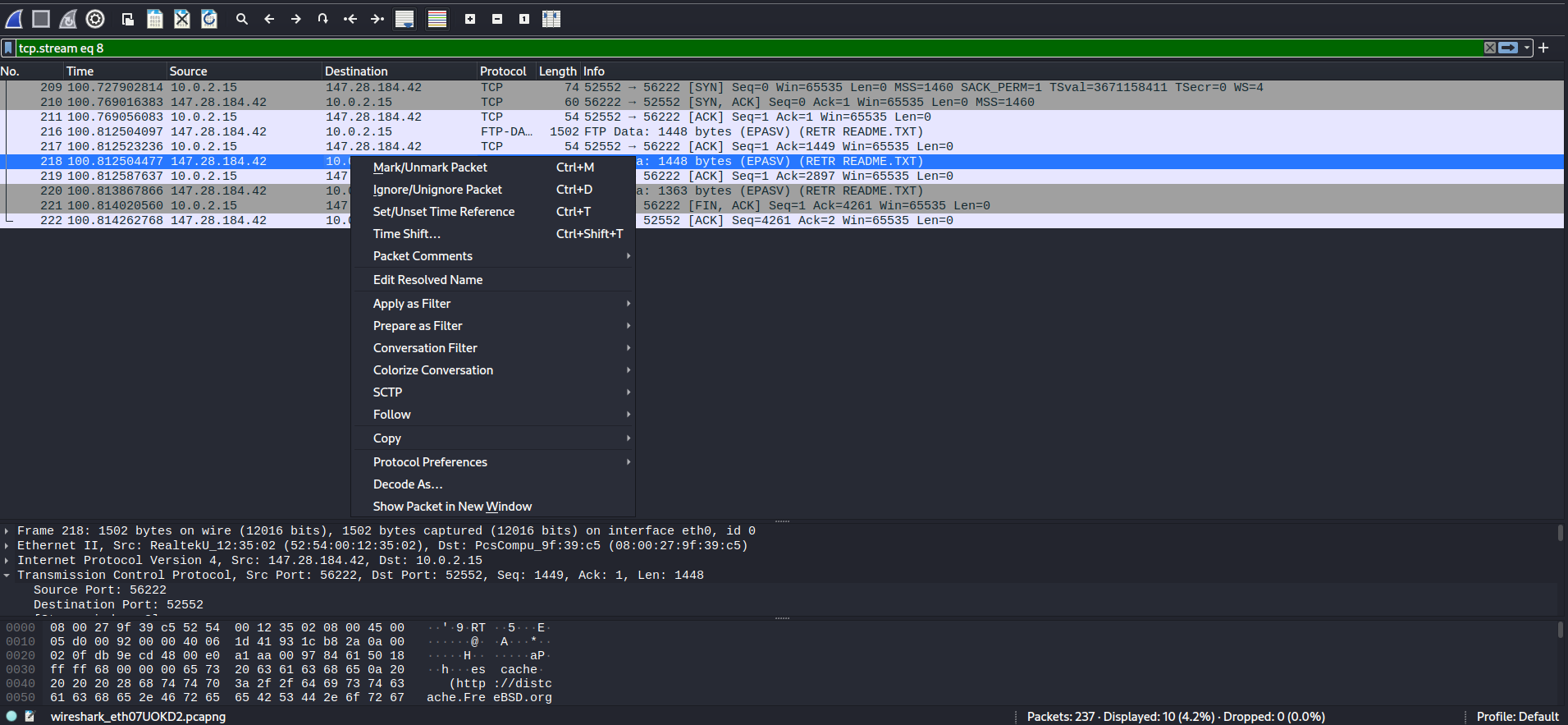
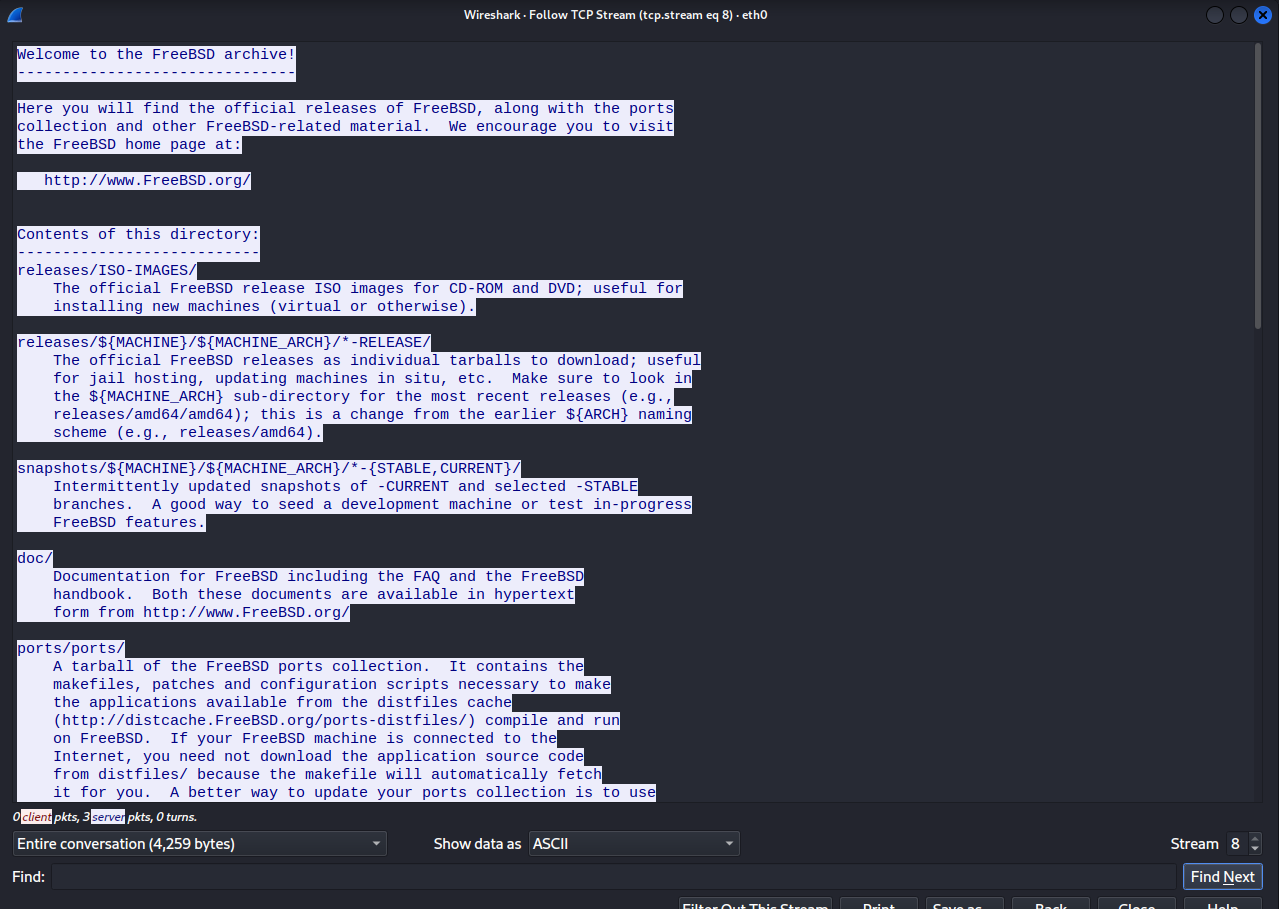
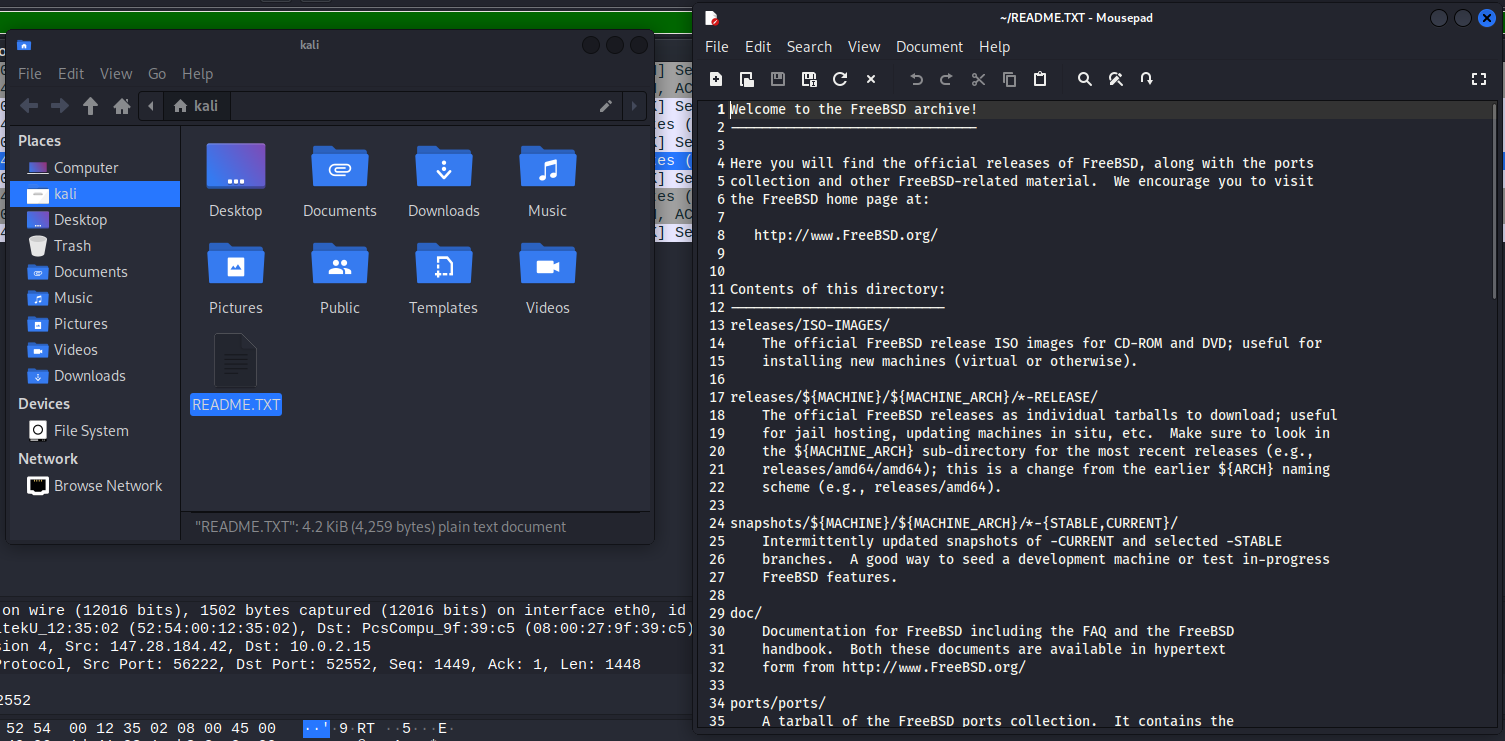
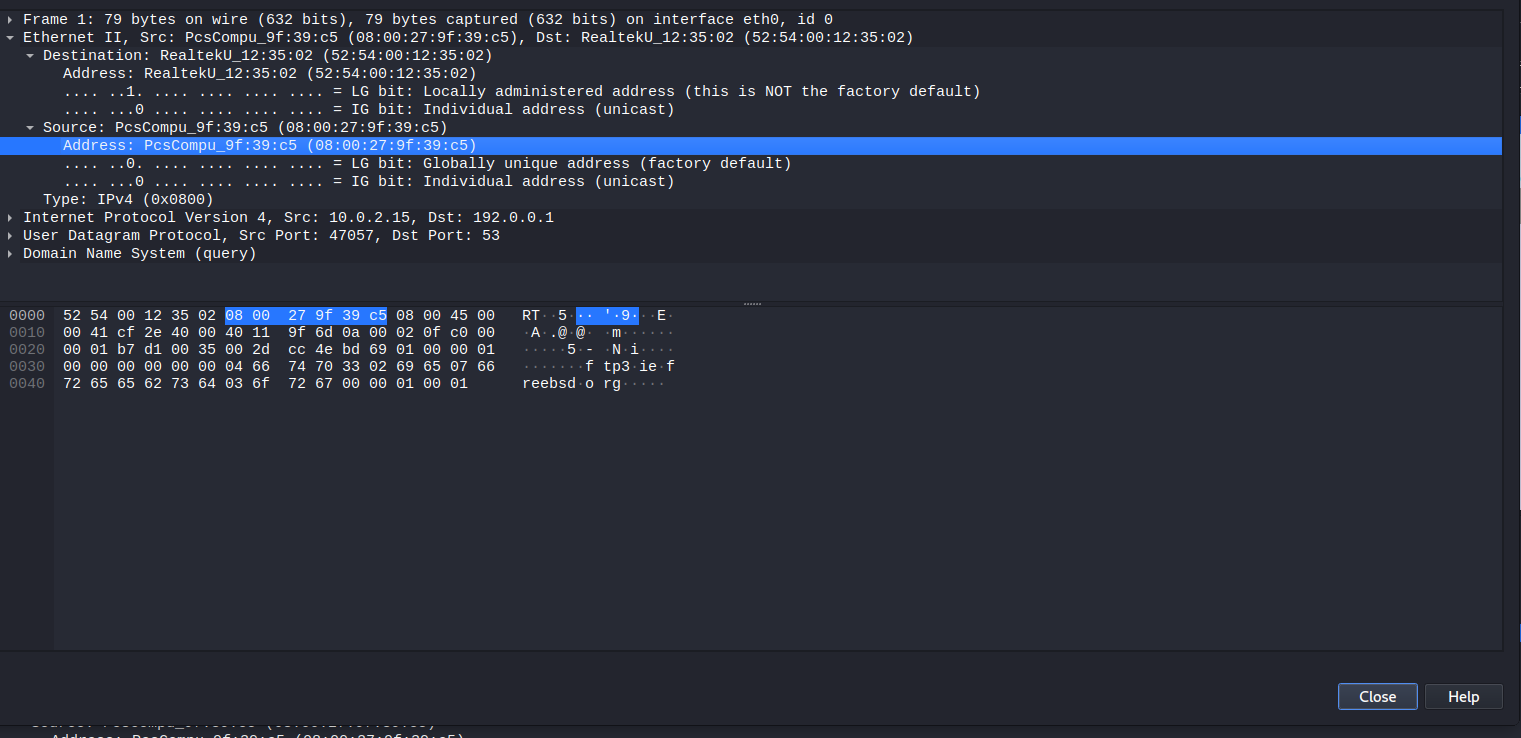
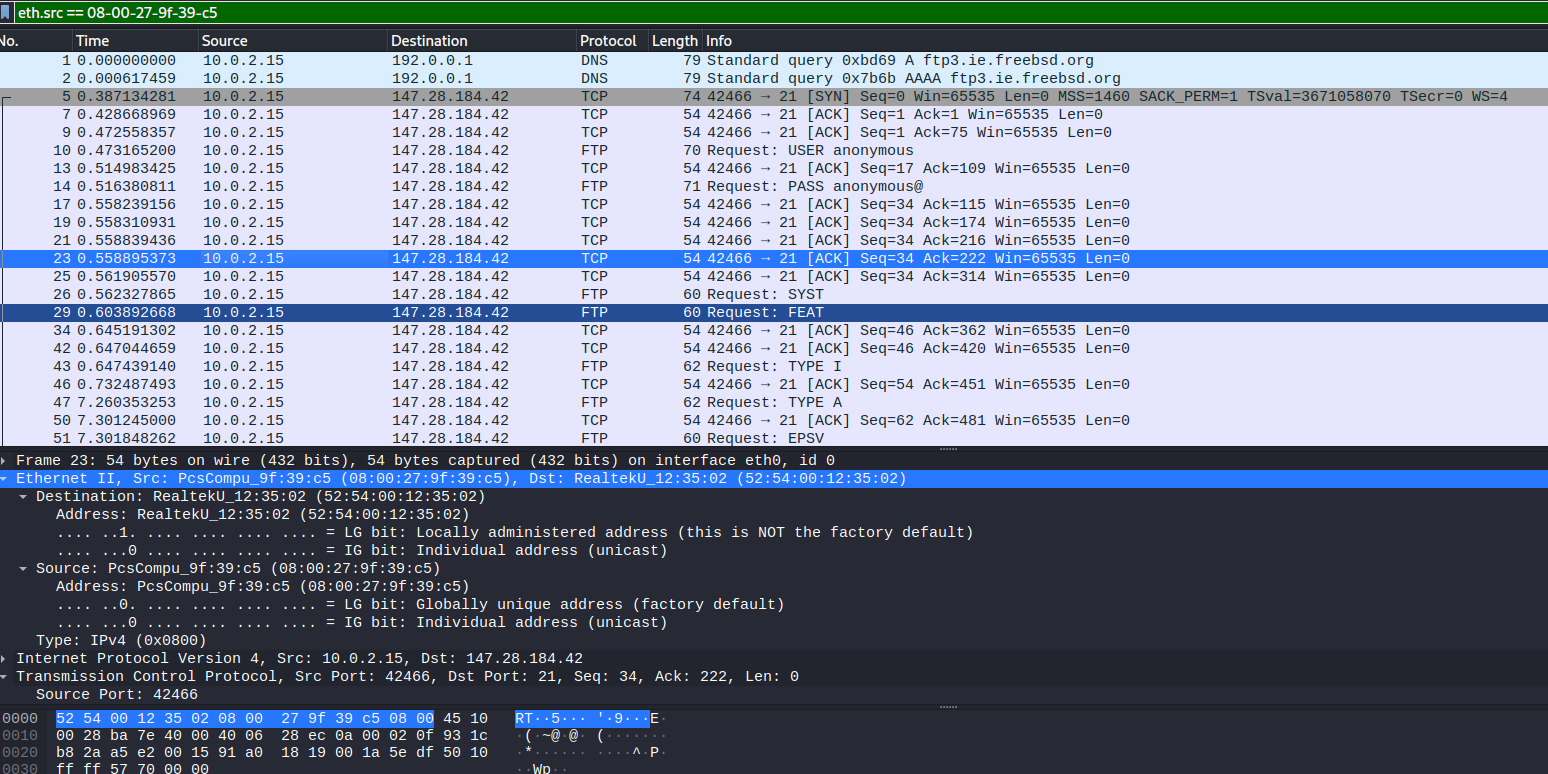
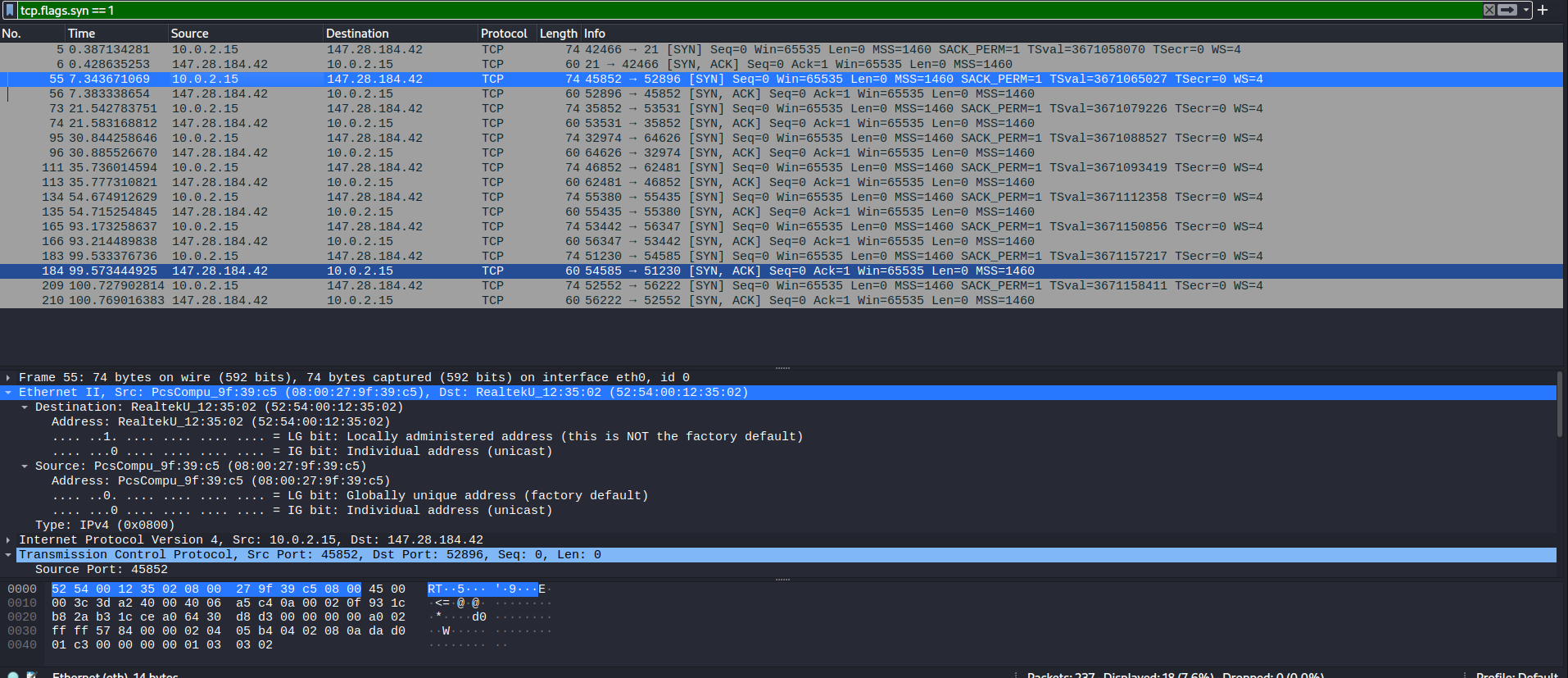
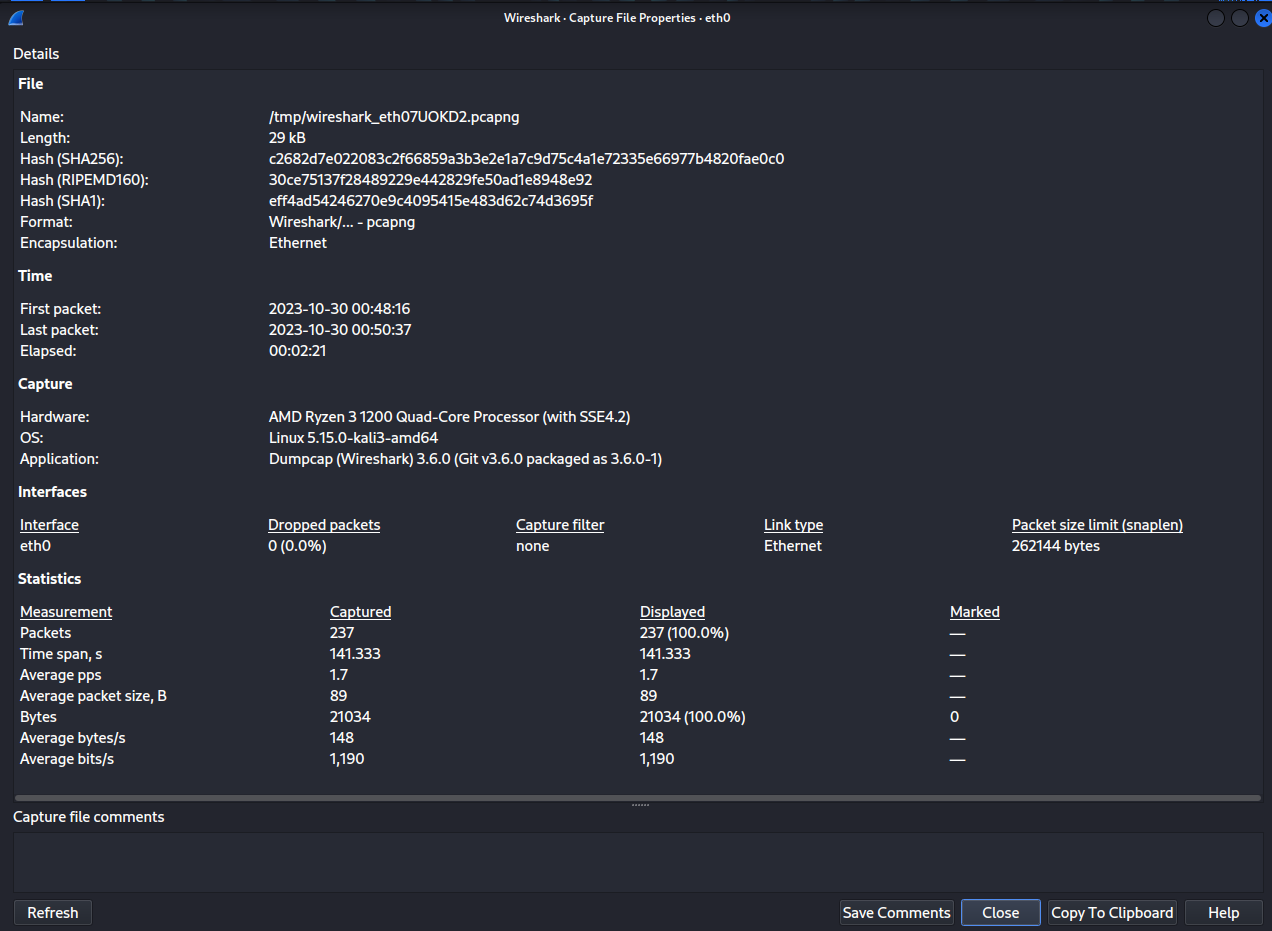
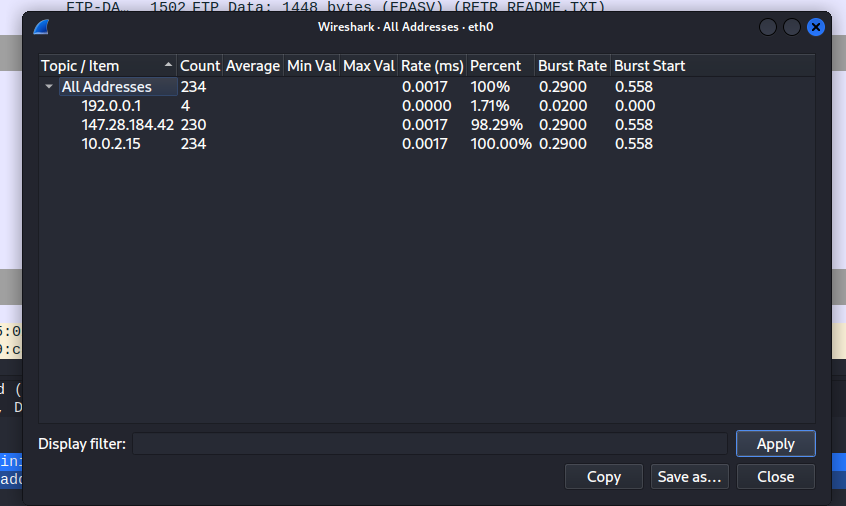
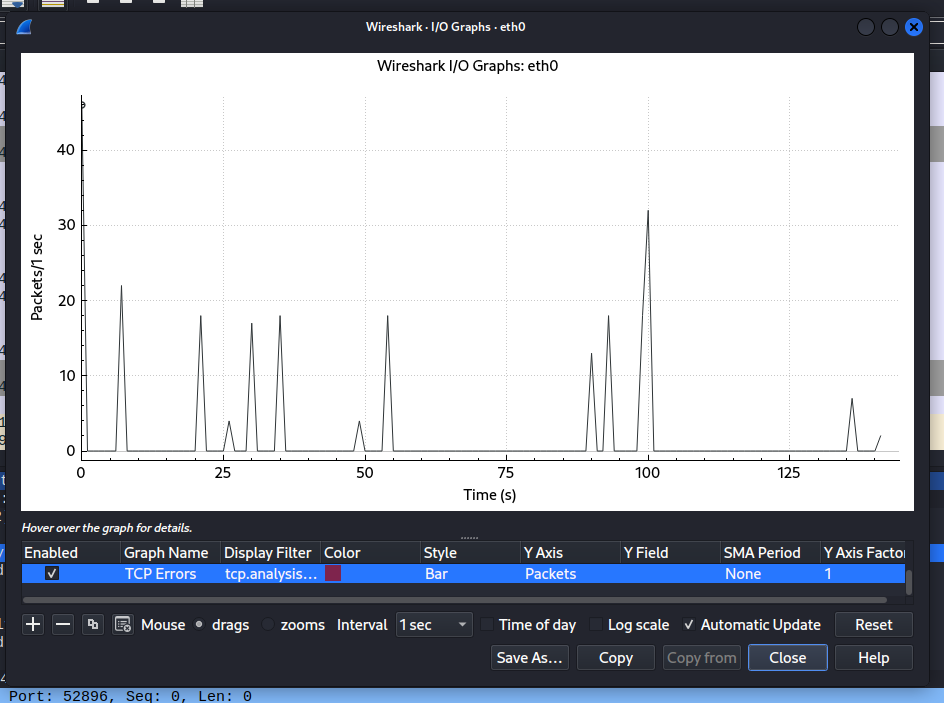
**ХНЕУ ім. С. Кузнеця**

**2023**

**Завдання:**

1. Ознайомитись з можливостями фільтрації даних за різними ознаками, зокрема, за МАС-адресою відправника і отримувача. Фільтр створюється за описаною вище методикою. Відповідно до рекомендачій викладача сформувати фільтр за МАСадресою.
2. Розглянути результат інкапсуляції при передачі даних. В захоплених пакетах виділити службову інформацію (заголовки) всіх блоків даних, а також, за наявністю, кінцевика.
3. Використовуючи фільтр відображення tcp.flags.syn = = 1 відібрати сегментизапити, які містять встановлений прапорець SYN у заголовку та сегментивідповіді, які містять встановлені прапорці SYN та ACK. Провести аналіз поля
4. Options заголовку TCP. Яке значення MSS використовується в з’єднанні, що аналізується?
   1. За допомогою меню «Statistics» необхідно отримати і додати до звіту таку

**Хід роботи:**

1. Відкриваю Wireshark та вмикаю режим захоплення  
   
2. У терміналі під’єднуюсь до ftp серверу  
   
3. Протягом сесії знайду потрібний файл та завантажу його  
     
     
   
4. Вимкну режим захоплення  
   
5. Оберу фільтр tcp  
   
6. Пакет №5-7 обмін ключами, та через те, що ми їх знаємо – можемо побачити подальший трафік  
   
7. Додам фільтр ip адреси  
   
8. Додам фільтр ip адреси та типу протоколу, оберу протокол та натисну «Folow – TCP Stream»  
   
9. У відкрившимуся вікні бачу сесію, та ті самі команди, що я писав у терміналі  
     
     
   
10. Наступним кроком оберу пакет з файлом та натисну «Follow – TCP Stream»  
    
11. У відкрившемуся вікні я можу побачити файл, що скачував  
    
12. Також відкрию даний файл на ПК, для верифікації файлу, та бачу, що файли ідентичні  
    
13. Для фільтрації пакетів за MAC адресою, спочатку відкрию пакет та знайду MAC адресу та за нею буду фільтрувати  
    
14. Як результат бачу наступне  
    
15. Також виконаю фільтрацію за «tcp.flag.syn == 1»  
    
16. Також зроблю статистику захоплених пакетів  
      
    Й можу побачити, що всього 237 пакетів  
    Середня швидкість – 1190 байт в секунду  
    Середній розмір пакетів – 89 байт  
    Час початку – 00:48:16 та кінець захоплення 00:50:37
17. IP адреси  
    
18. IO Graphs  
    
19. Висновок – я проаналізував ftp трафік, виконав фільтрацію пакетів та отримав статистику захоплених пакетів