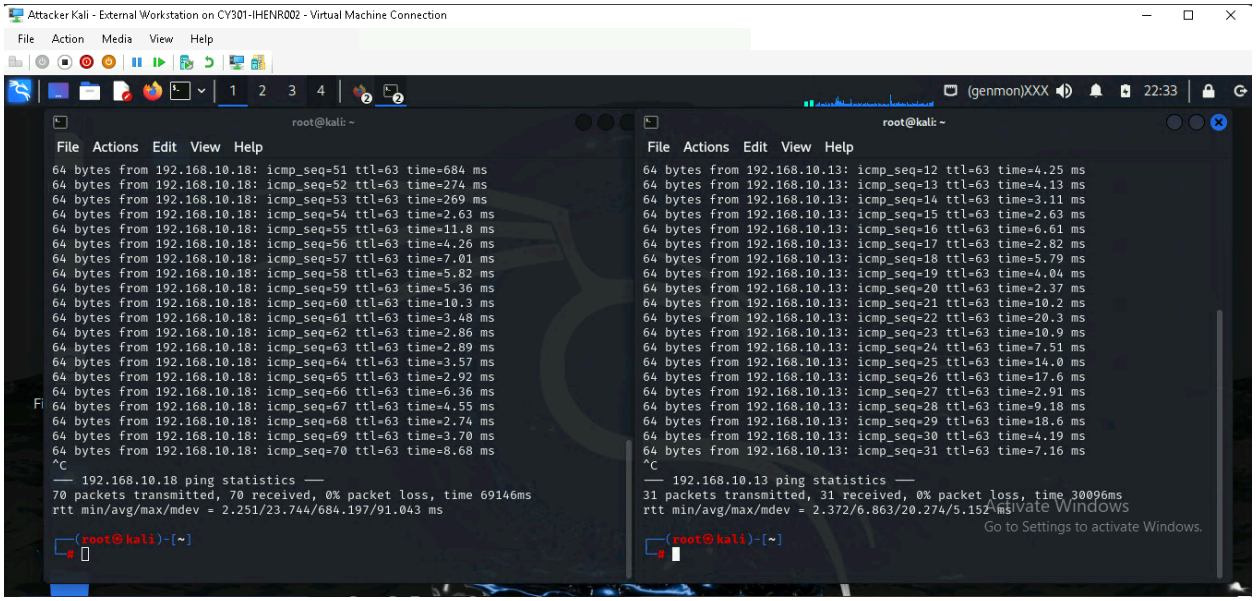
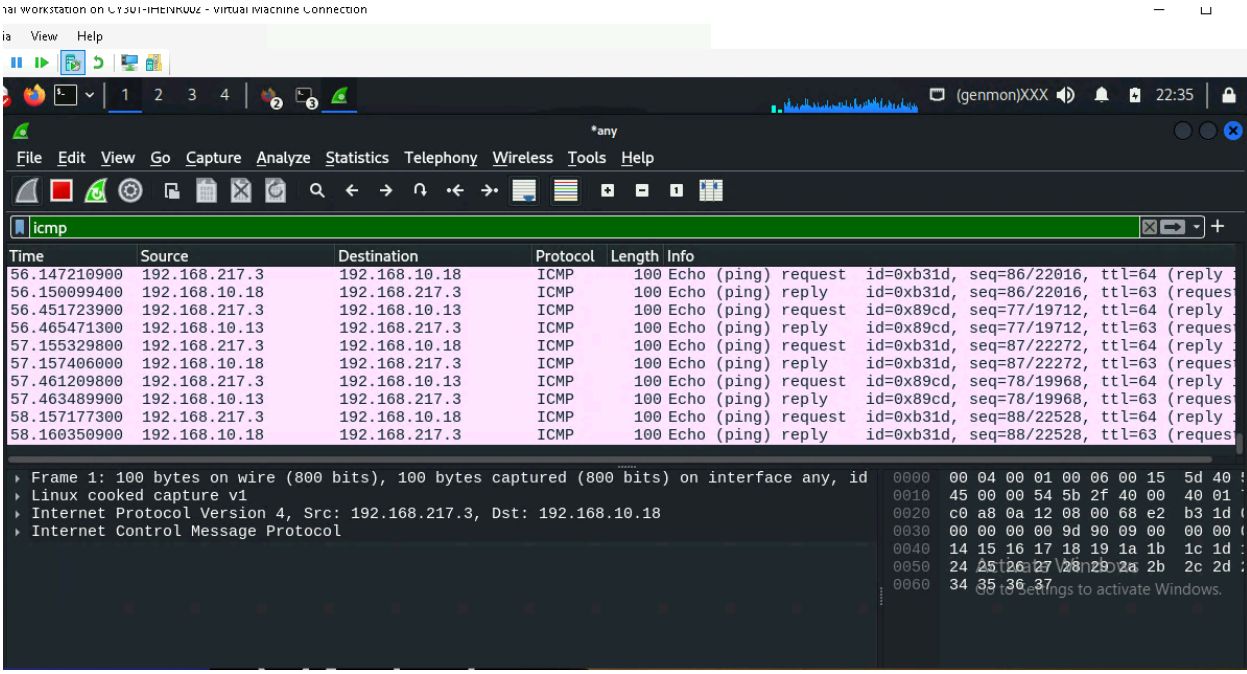
Traffic Tracing and Sniffing

1. **Open two terminals on External Kali VM. Use one to ping Ubuntu VM, and use the other to ping Internal Kali**



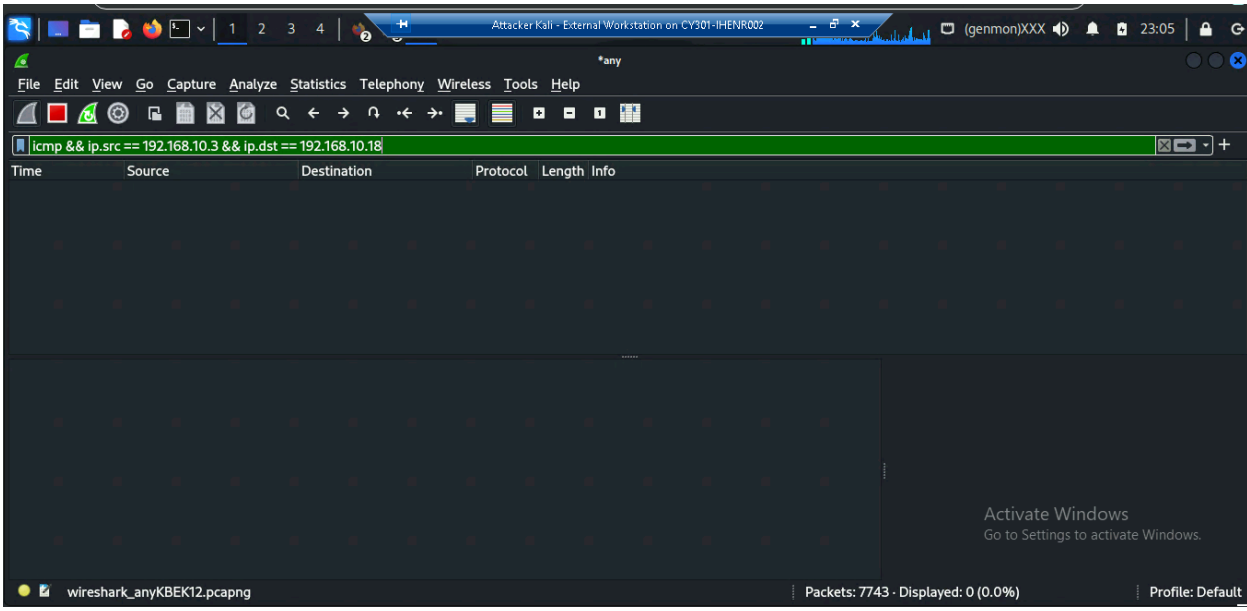
In external kali, I opened two terminals to ping ubuntu (left) and internal kali (right)
I did ping them again after I took the screenshots

   a. **Apply proper display or capture filter on Internal Kali VM to show active ICMP traffic**



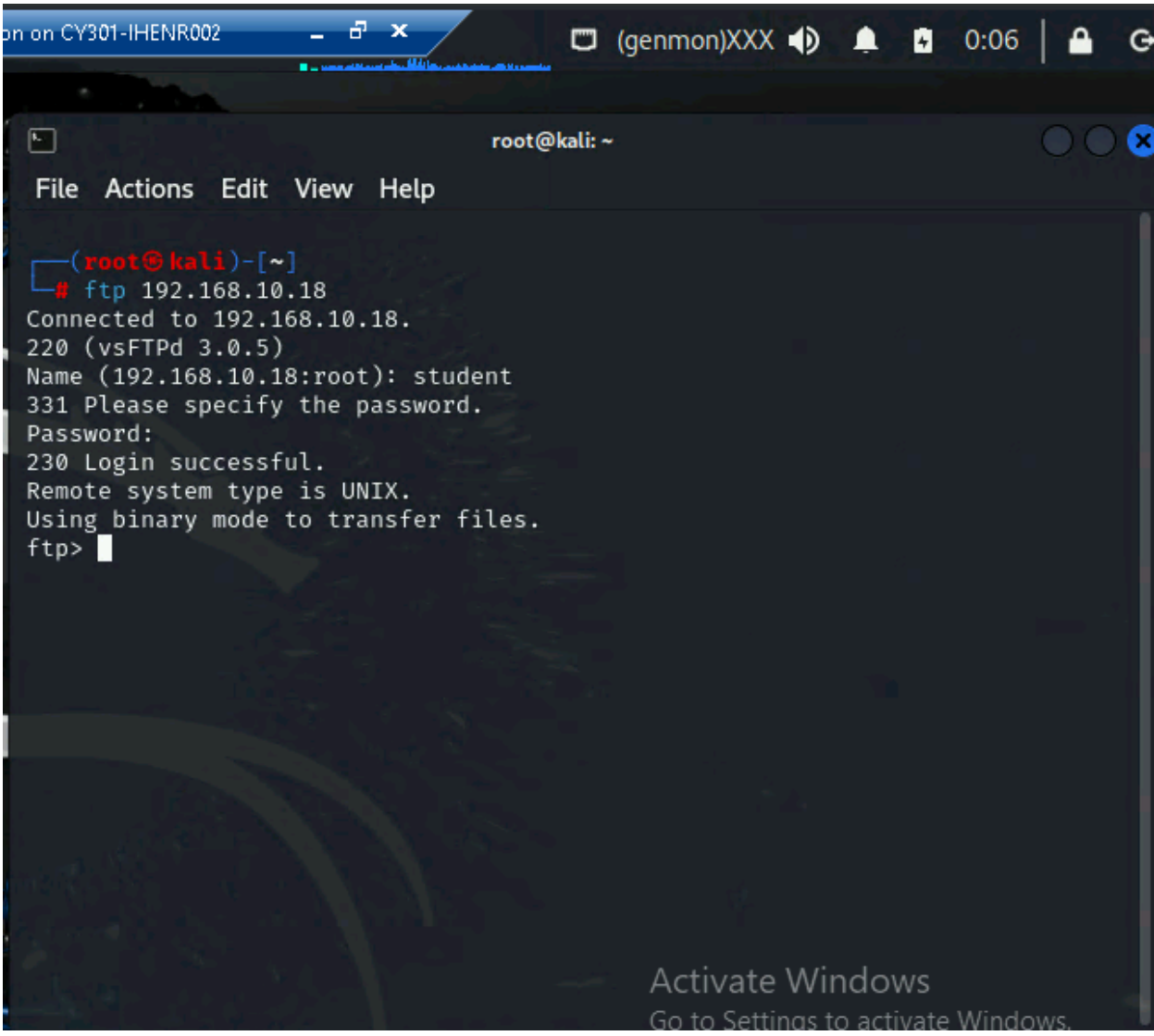
I opened wireshark using another window, listened on the “any” interface, and typed in “icmp” into the filter.

b. **Apply proper display or capture filter on Internal Kali VM that ONLY displays ICMP request originated from <u>External Kali VM</u> and goes to <u>Ubuntu 64-bit VM</u>**



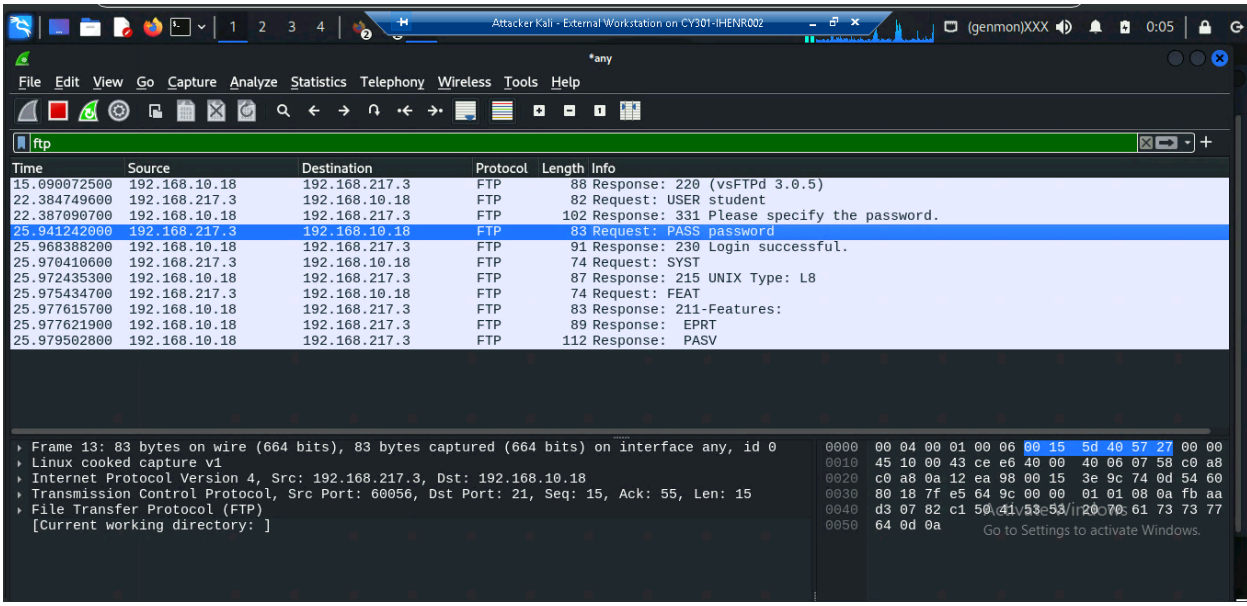
I typed “icmp” into the filter along with the external kali source ip and the ubuntu destination ip to narrow down any traffic between the VMs.

2. **Sniff FTP traffic**
   a. **Ubuntu VM is also serving as an FTP server inside the LAN network. Now, you need to use External Kali to access this FTP server by using the command: ftp [ip_addr of ubuntu VM]. The username for the FTP server is cyse301, and the password is password. You can follow the steps below to access the FTP server.**



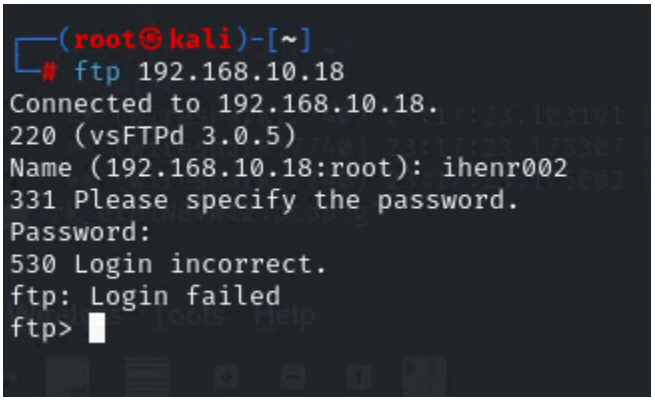
In a window in external kali, I typed in ftp and the ip address for ubuntu, then used the given username and password.

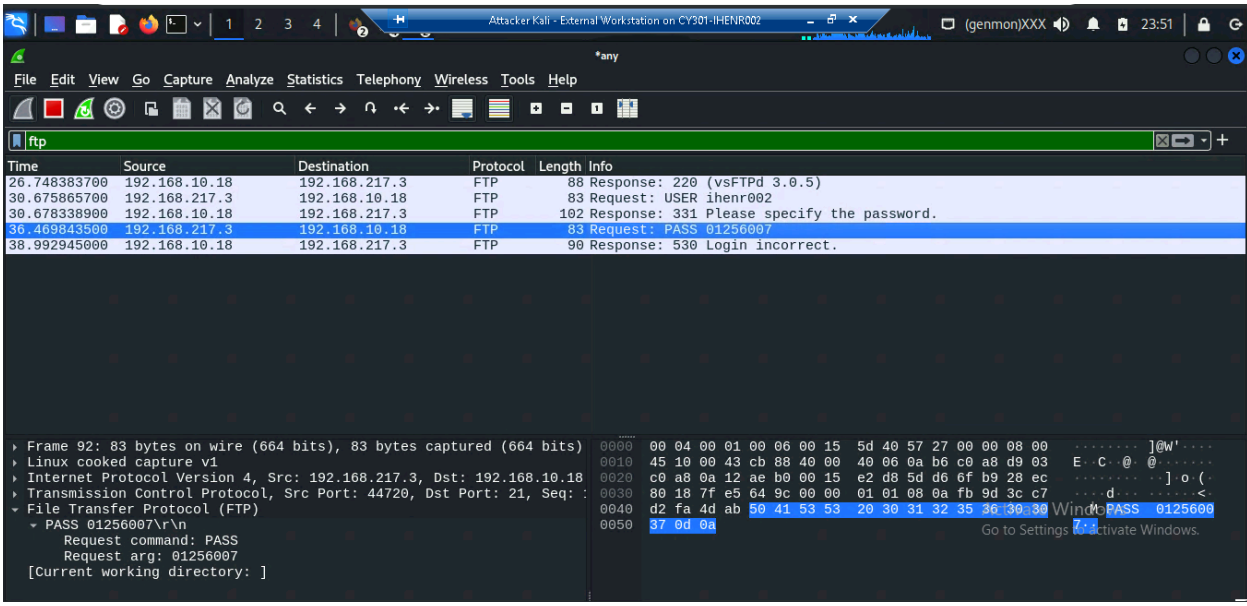
b. **Unfortunately, Internal Kali, the attacker, is also sniffing to the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to screenshot and explain how you find the password.**



I opened wireshark and listened in under the “any” interface. I filtered it so I could only see ftp traffic. Then I opened a new external kali window and tried to access the ftp server again using the same steps from above. I went back to wireshark and double clicked the password request which gave me the password I typed in.

c. **After you successfully find the username & password from the FTP traffic, repeat the previous step (2a), and use your MIDAS ID as the username and UIN as the password to reassess the FTP server from External Kali. Although External Kali may not access the FTP server, you need to intercept the packets containing these “secrets” from the attacker VM, which is Internal Kali.**





I repeated the steps from part (a), but this time I used my userID and UIN for the username and password. Then I went back to wireshark and looked at the password input to find my UIN.