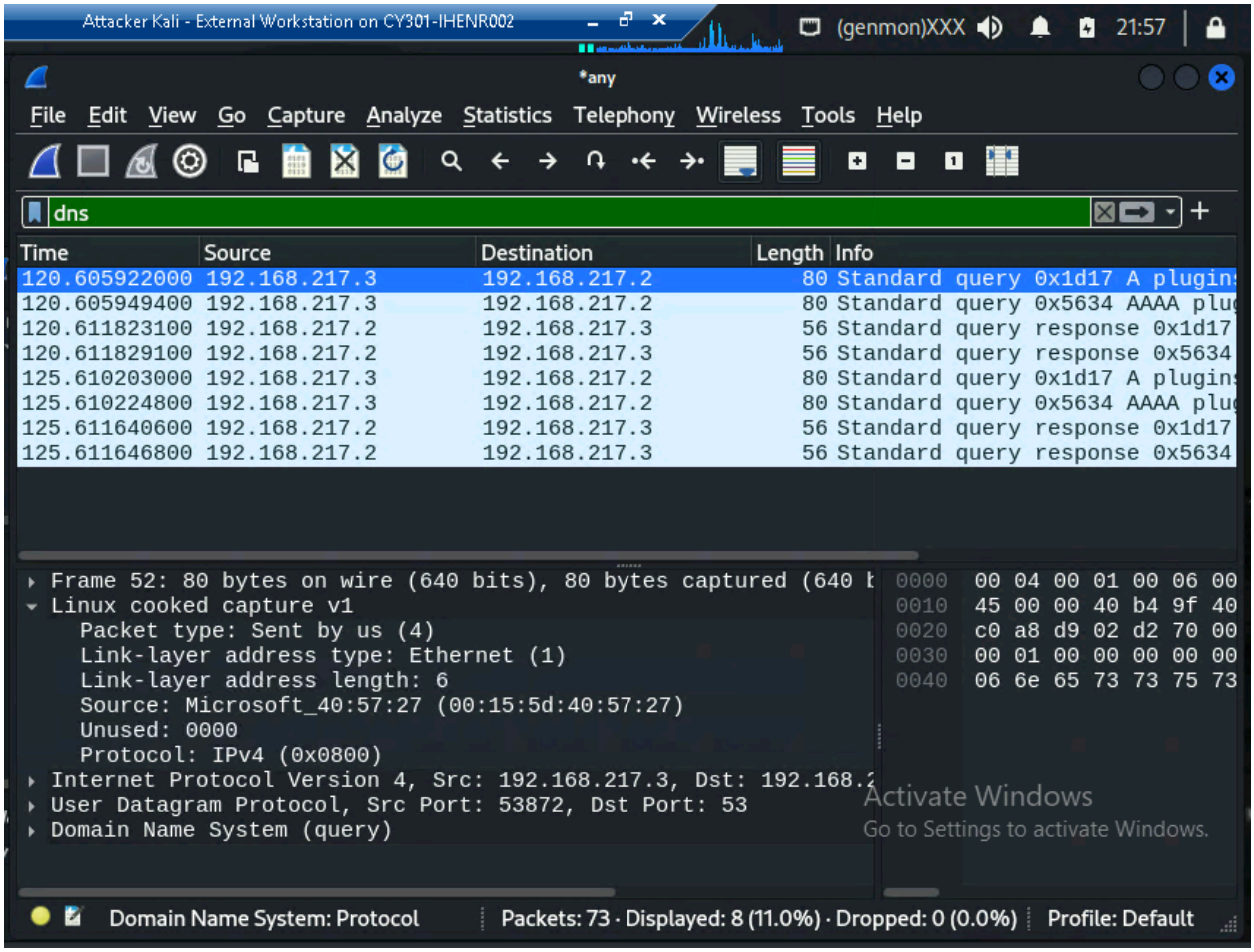
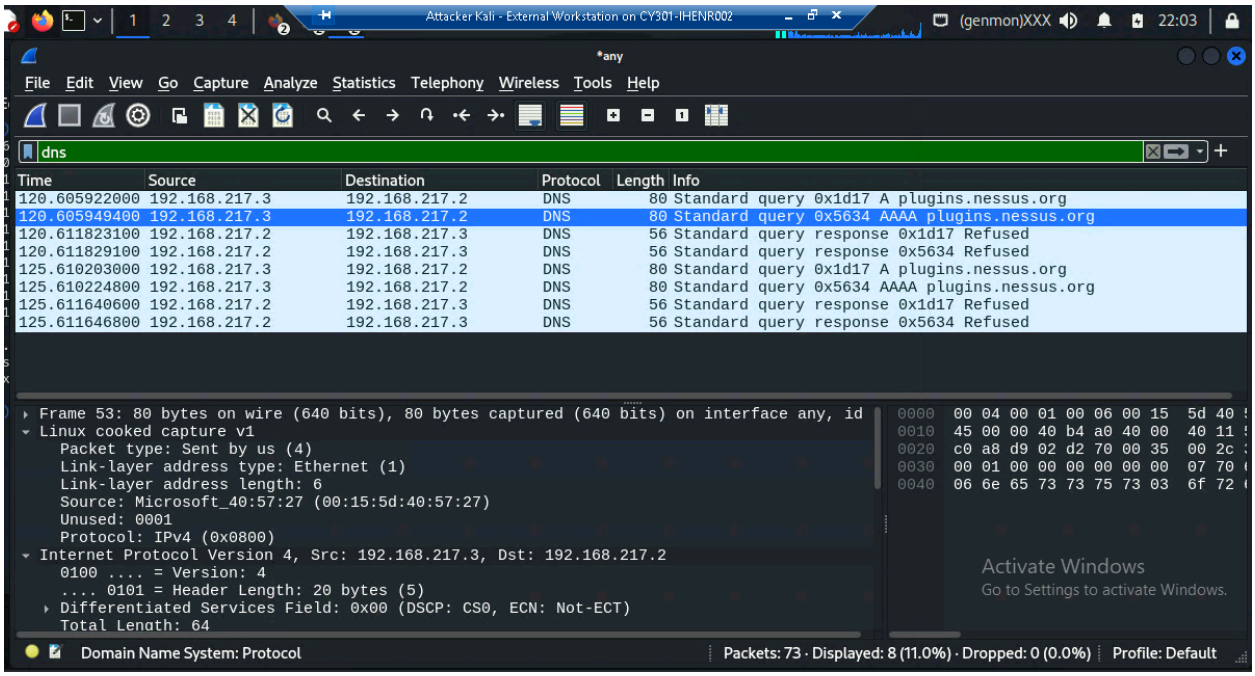
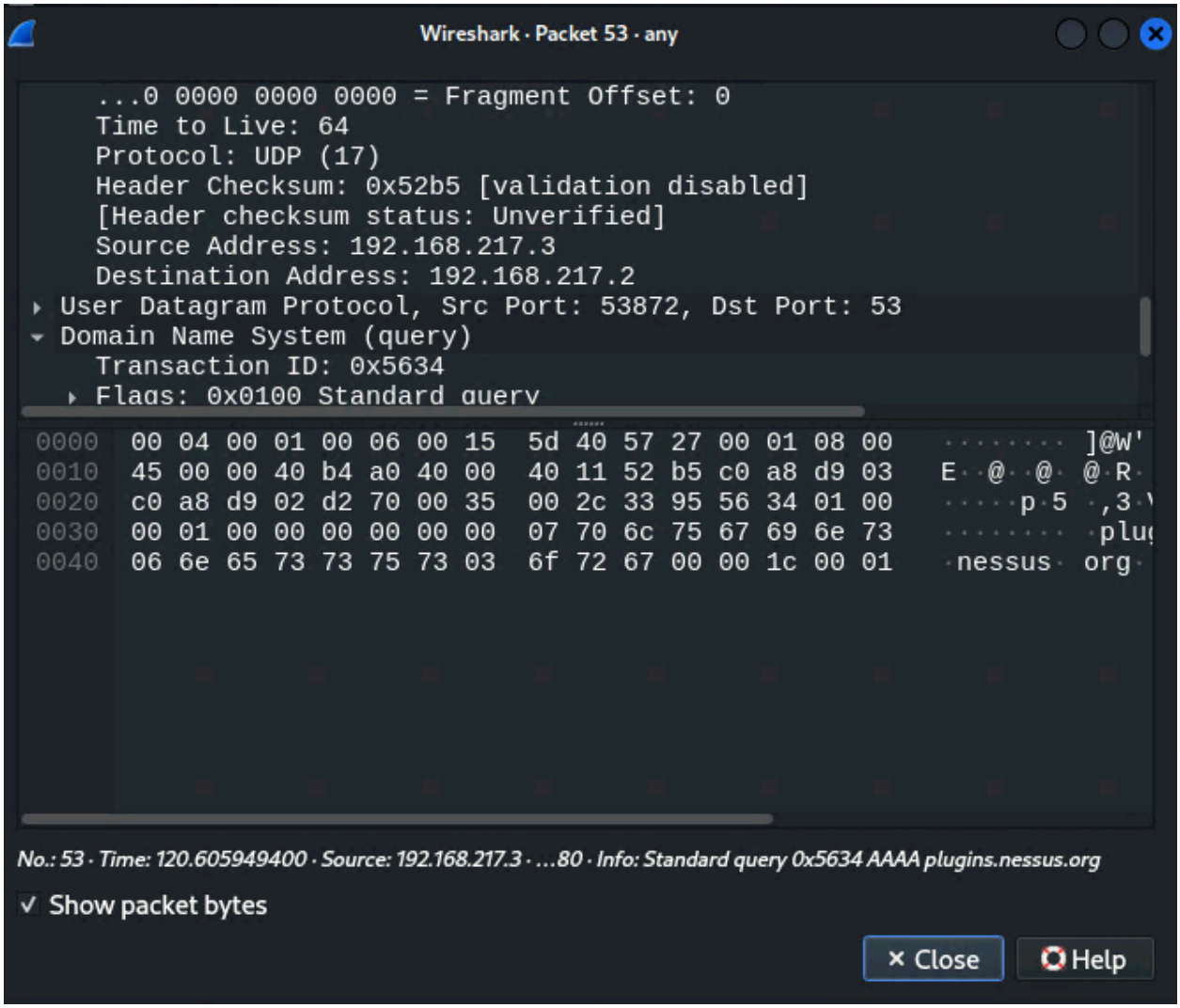
1. **Apply “DNS” as a display filter in Wireshark. How many packets are displayed?**



I typed “DNS” in the filter
73 packets total; 8 Displayed

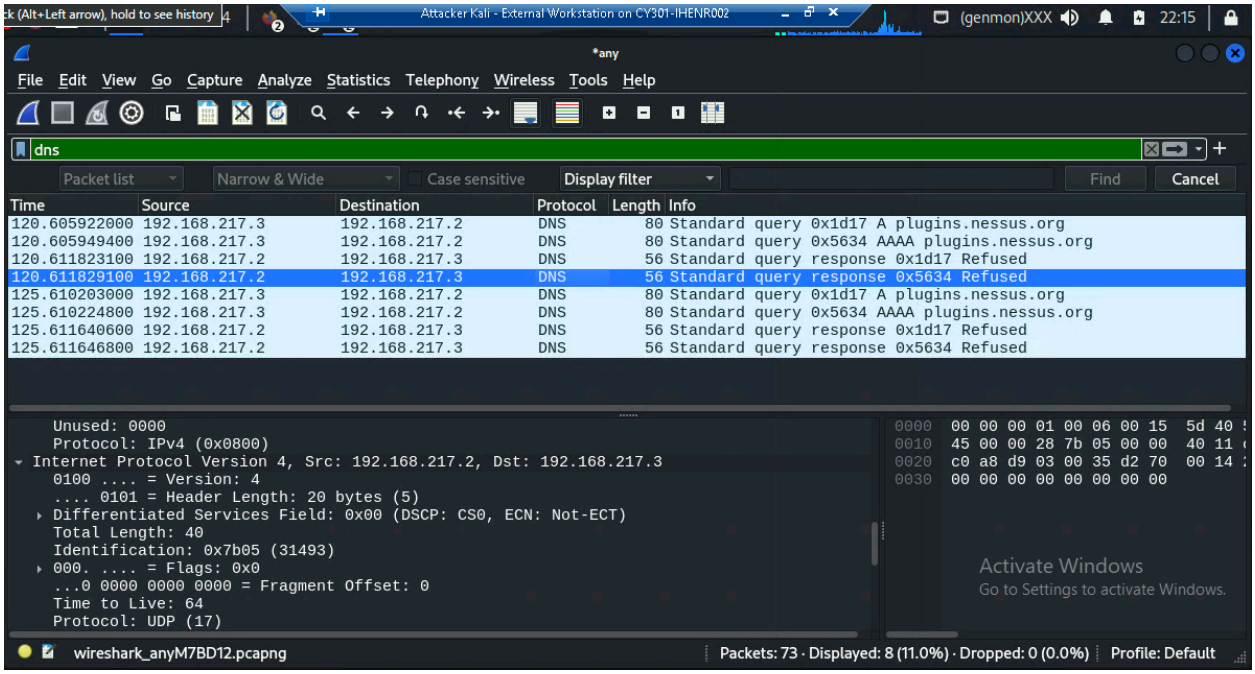
2. **Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format IP:port.**

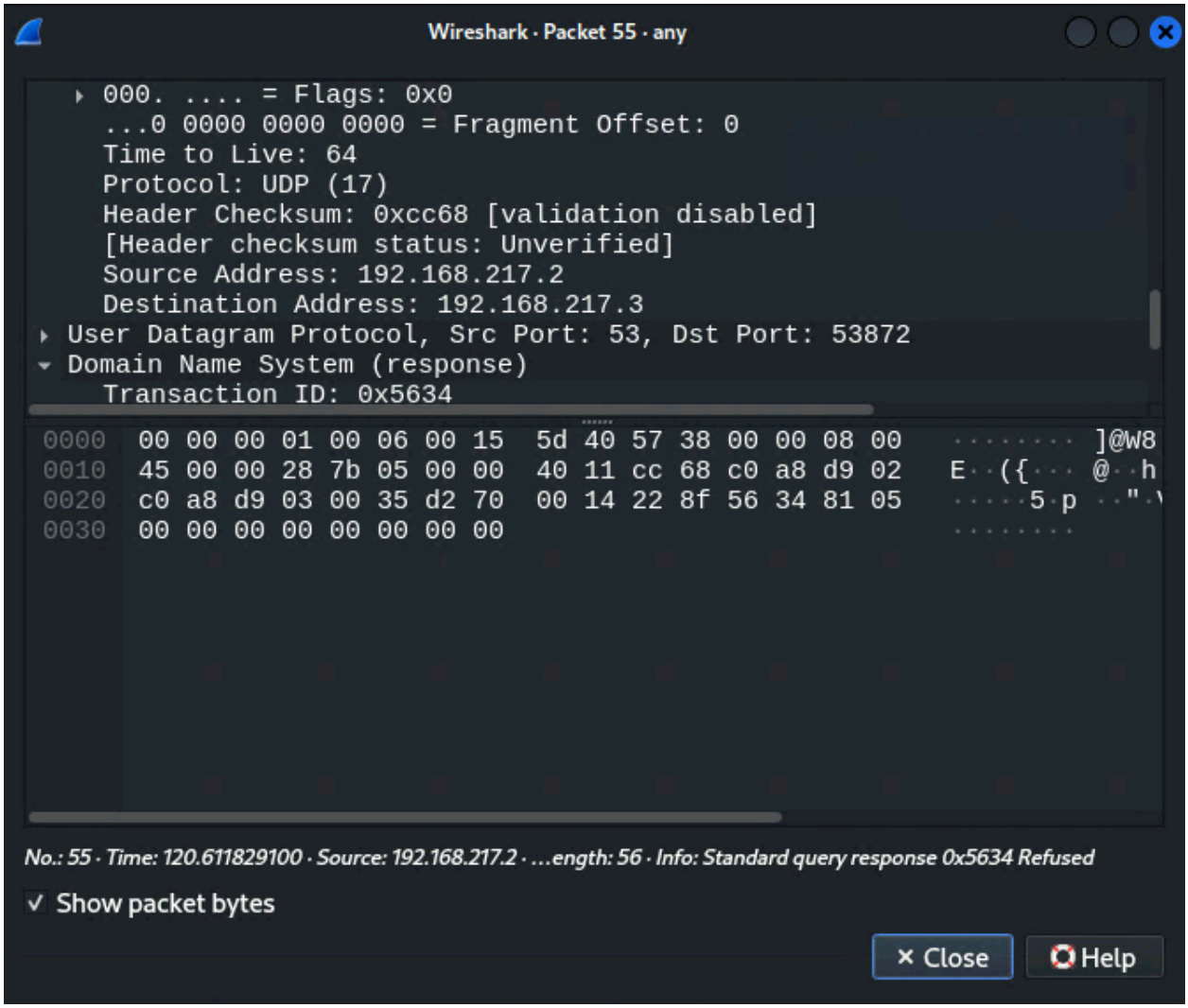

Attacker Kali - External Workstation on CY301-IHENR002
(genmon)XXX
22:03
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Time Source Destination Protocol Length Info
120.605922000 192.168.217.3 192.168.217.2 DNS 80 Standard query 0x1d17 A plugins.nessus.org
120.605949400 192.168.217.3 192.168.217.2 DNS 80 Standard query 0x5634 AAAA plugins.nessus.org
120.611823100 192.168.217.2 192.168.217.3 DNS 56 Standard query response 0x1d17 Refused
120.611829100 192.168.217.2 192.168.217.3 DNS 56 Standard query response 0x5634 Refused
125.610203000 192.168.217.3 192.168.217.2 DNS 80 Standard query 0x1d17 A plugins.nessus.org
125.610224800 192.168.217.3 192.168.217.2 DNS 80 Standard query 0x5634 AAAA plugins.nessus.org
125.611640600 192.168.217.2 192.168.217.3 DNS 56 Standard query response 0x1d17 Refused
125.611646800 192.168.217.2 192.168.217.3 DNS 56 Standard query response 0x5634 Refused
Frame 53: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface any, id
Linux cooked capture v1
Packet type: Sent by us (4)
Link-layer address type: Ethernet (1)
Link-layer address length: 6
Source: Microsoft_40:57:27 (00:15:5d:40:57:27)
Unused: 0001
Protocol: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.217.2
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 64
0000 00 04 00 01 00 06 00 15 5d 40
0010 45 00 00 40 b4 a0 40 00 40 11
0020 c0 a8 d9 02 d2 70 00 35 00 2c
0030 00 01 00 00 00 00 00 00 07 70
0040 06 6e 65 73 73 75 73 03 6f 72
Activate Windows
Go to Settings to activate Windows.
Domain Name System: Protocol
Packets: 73 · Displayed: 8 (11.0%) · Dropped: 0 (0.0%)
Profile: Default



I chose the second packet after filtering the DNS packets
Domain Name: plugins.nessus.org
Source IP/Port: 192.168.217.3:53872
Destination IP/Port: 192.168.217.2:53

3. **Find the corresponding DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port number? What is the message replied from the DNS server?**


Attacker Kali - External Workstation on CY301-IHENR002
(genmon)XXX
22:15
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel
Time Source Destination Protocol Length Info
120.605922000 192.168.217.3 192.168.217.2 DNS 80 Standard query 0x1d17 A plugins.nessus.org
120.605949400 192.168.217.3 192.168.217.2 DNS 80 Standard query 0x5634 AAAA plugins.nessus.org
120.611823100 192.168.217.2 192.168.217.3 DNS 56 Standard query response 0x1d17 Refused
120.611829100 192.168.217.2 192.168.217.3 DNS 56 Standard query response 0x5634 Refused
125.610203000 192.168.217.3 192.168.217.2 DNS 80 Standard query 0x1d17 A plugins.nessus.org
125.610224800 192.168.217.3 192.168.217.2 DNS 80 Standard query 0x5634 AAAA plugins.nessus.org
125.611640600 192.168.217.2 192.168.217.3 DNS 56 Standard query response 0x1d17 Refused
125.611646800 192.168.217.2 192.168.217.3 DNS 56 Standard query response 0x5634 Refused
Unused: 0000
Protocol: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.217.2, Dst: 192.168.217.3
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x7b05 (31493)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
0000 00 00 00 01 00 06 00 15 5d 40
0010 45 00 00 28 7b 05 00 00 40 11
0020 c0 a8 d9 03 00 35 d2 70 00 14
0030 00 00 00 00 00 00 00 00
Activate Windows
Go to Settings to activate Windows.
wireshark_anyM7BD12.pcapng
Packets: 73 · Displayed: 8 (11.0%) · Dropped: 0 (0.0%)
Profile: Default



Source IP/Port: 192.168.217.2:53
Destination IP/Port: 192.168.217.3:53872
Message: Refused