University of Utah
School of Computing
CS 6967: Security Operations

Lab 12 Response Outline

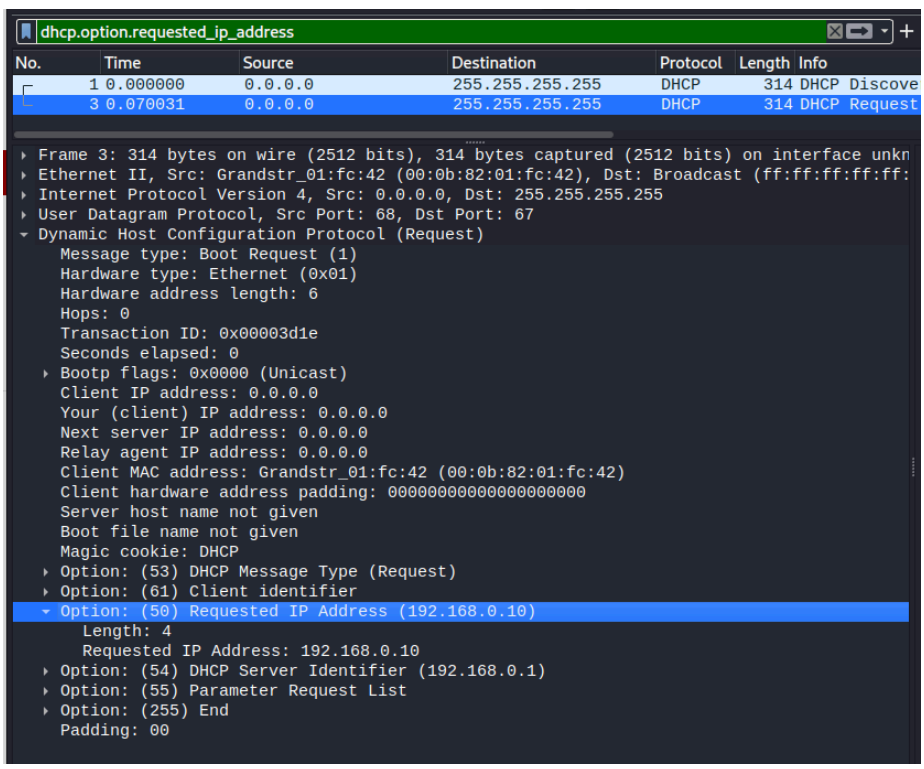
Lab 12: Threat Hunting with Network Data

Test 1: Test the Pcap

Summary of test experience:

This test requires us to load a pcap file using wireshark and apply the 'dhcp.option.requested_ip_address' filter to get the DHCP packets that include the requested IP address option. This can be useful for troubleshooting DHCP-related issues or monitoring DHCP requests for specific IP addresses.

Screenshot of test results:



Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

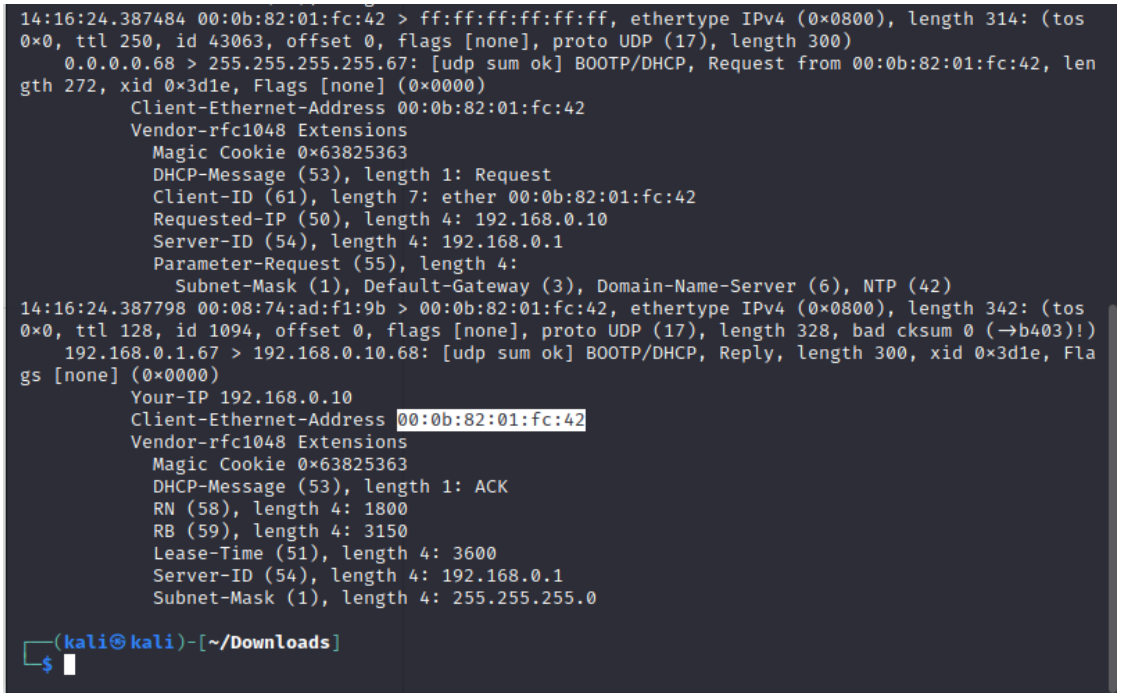
From the above screenshot, we can see the Client MAC address and the Requested IP Address which is 192.168.0.10.

Test 2: Use Tcpdump

Summary of test experience:

Here, I did Task 1 but using a tcpdump command. The overall provided command is using tcpdump to read packets from the PCAP file, filter for packets with source or destination ports 67 or 68 (DHCP traffic), print the link-level header, and display detailed information with increased verbosity.

Screenshot of test results:



```
14:16:24.387484 00:0b:82:01:fc:42 > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0×0800), length 314: (tos
0×0, ttl 250, id 43063, offset 0, flags [none], proto UDP (17), length 300)
    0.0.0.0.68 > 255.255.255.255.67: [udp sum ok] BOOTP/DHCP, Request from 00:0b:82:01:fc:42, len
gth 272, xid 0×3d1e, Flags [none] (0×0000)
          Client-Ethernet-Address 00:0b:82:01:fc:42
          Vendor-rfc1048 Extensions
            Magic Cookie 0×63825363
            DHCP-Message (53), length 1: Request
            Client-ID (61), length 7: ether 00:0b:82:01:fc:42
            Requested-IP (50), length 4: 192.168.0.10
            Server-ID (54), length 4: 192.168.0.1
            Parameter-Request (55), length 4:
              Subnet-Mask (1), Default-Gateway (3), Domain-Name-Server (6), NTP (42)
14:16:24.387798 00:08:74:ad:f1:9b > 00:0b:82:01:fc:42, ethertype IPv4 (0×0800), length 342: (tos
0×0, ttl 128, id 1094, offset 0, flags [none], proto UDP (17), length 328, bad cksum 0 (→b403)!)
    192.168.0.1.67 > 192.168.0.10.68: [udp sum ok] BOOTP/DHCP, Reply, length 300, xid 0×3d1e, Fla
gs [none] (0×0000)
          Your-IP 192.168.0.10
          Client-Ethernet-Address 00:0b:82:01:fc:42
          Vendor-rfc1048 Extensions
            Magic Cookie 0×63825363
            DHCP-Message (53), length 1: ACK
            RN (58), length 4: 1800
            RB (59), length 4: 3150
            Lease-Time (51), length 4: 3600
            Server-ID (54), length 4: 192.168.0.1
            Subnet-Mask (1), length 4: 255.255.255.0

┌──(kali㉿kali)-[~/Downloads]
└─$
```

Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

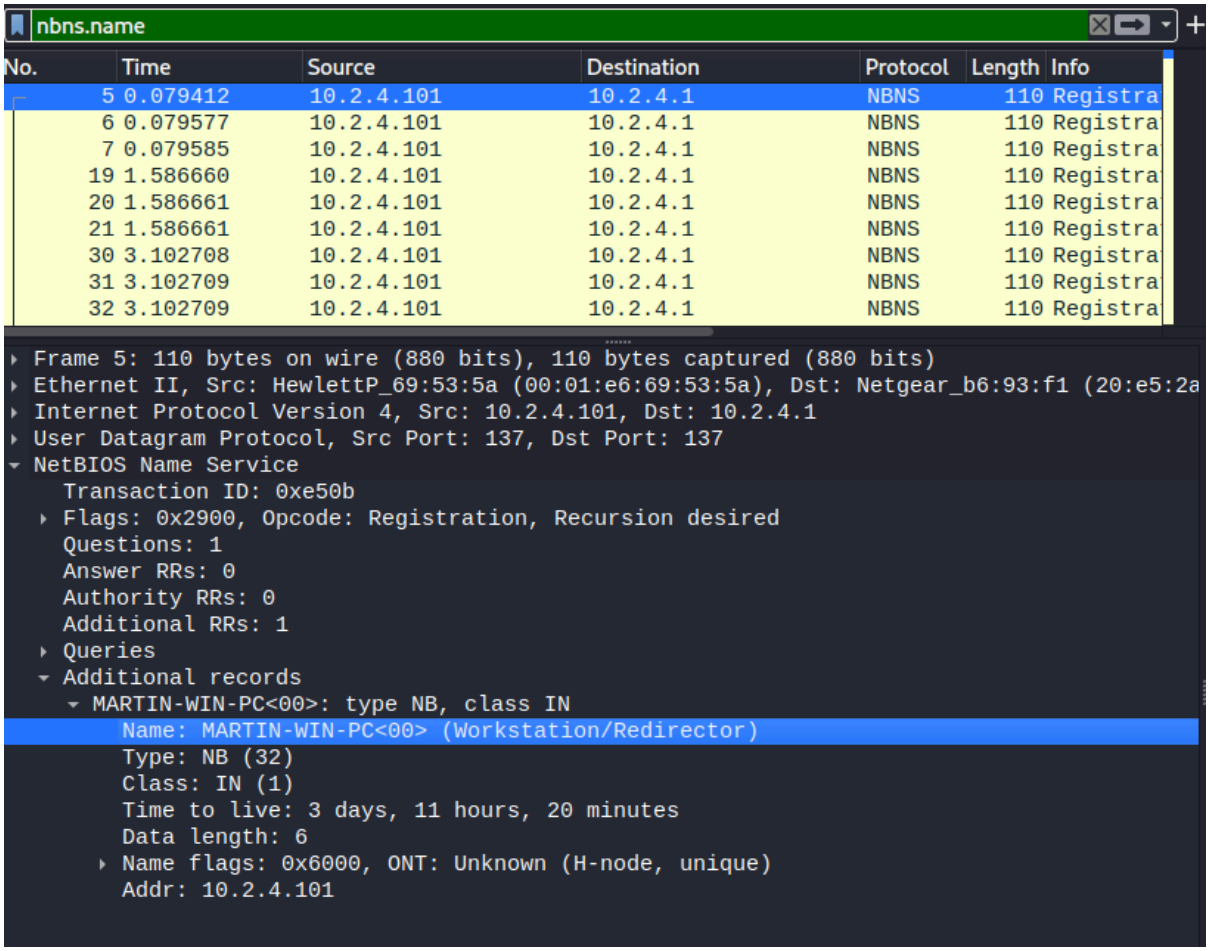
The above screenshot gives the same info as Test 1's screenshot.

Test 3: Test the Pcap

Summary of test experience:

This test requires us to load a pcap file using wireshark and apply the 'nbns.name' filter to get the packets that include NetBIOS name information. This can be useful for troubleshooting NetBIOS-related issues or monitoring NetBIOS name resolution on the network.

Screenshot of test results:



Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

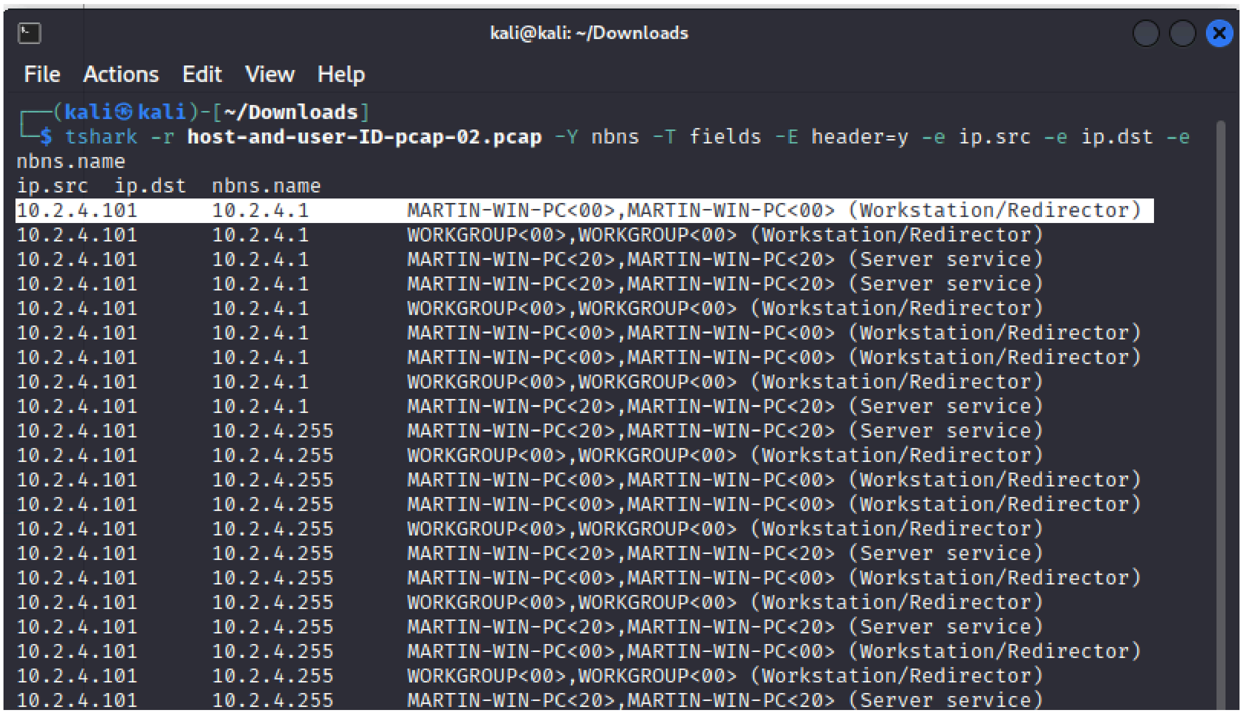
From the above image, we can see that the Workstation name is MARTIN-WIN-PC<00>

Test 4: Use Tshark

Summary of test experience:

Here, I did Task 3 but using Tshark, the command line tool of Wireshark.

Screenshot of test results:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ tshark -r host-and-user-ID-pcap-02.pcap -Y nbns -T fields -E header=y -e ip.src -e ip.dst -e
nbns.name
ip.src  ip.dst  nbns.name
10.2.4.101      10.2.4.1        MARTIN-WIN-PC<00>,MARTIN-WIN-PC<00> (Workstation/Redirector)
10.2.4.101      10.2.4.1        WORKGROUP<00>,WORKGROUP<00> (Workstation/Redirector)
10.2.4.101      10.2.4.1        MARTIN-WIN-PC<20>,MARTIN-WIN-PC<20> (Server service)
10.2.4.101      10.2.4.1        MARTIN-WIN-PC<20>,MARTIN-WIN-PC<20> (Server service)
10.2.4.101      10.2.4.1        WORKGROUP<00>,WORKGROUP<00> (Workstation/Redirector)
10.2.4.101      10.2.4.1        MARTIN-WIN-PC<00>,MARTIN-WIN-PC<00> (Workstation/Redirector)
10.2.4.101      10.2.4.1        MARTIN-WIN-PC<00>,MARTIN-WIN-PC<00> (Workstation/Redirector)
10.2.4.101      10.2.4.1        WORKGROUP<00>,WORKGROUP<00> (Workstation/Redirector)
10.2.4.101      10.2.4.1        MARTIN-WIN-PC<20>,MARTIN-WIN-PC<20> (Server service)
10.2.4.101      10.2.4.255      MARTIN-WIN-PC<20>,MARTIN-WIN-PC<20> (Server service)
10.2.4.101      10.2.4.255      WORKGROUP<00>,WORKGROUP<00> (Workstation/Redirector)
10.2.4.101      10.2.4.255      MARTIN-WIN-PC<00>,MARTIN-WIN-PC<00> (Workstation/Redirector)
10.2.4.101      10.2.4.255      MARTIN-WIN-PC<00>,MARTIN-WIN-PC<00> (Workstation/Redirector)
10.2.4.101      10.2.4.255      WORKGROUP<00>,WORKGROUP<00> (Workstation/Redirector)
10.2.4.101      10.2.4.255      MARTIN-WIN-PC<20>,MARTIN-WIN-PC<20> (Server service)
10.2.4.101      10.2.4.255      MARTIN-WIN-PC<00>,MARTIN-WIN-PC<00> (Workstation/Redirector)
10.2.4.101      10.2.4.255      WORKGROUP<00>,WORKGROUP<00> (Workstation/Redirector)
10.2.4.101      10.2.4.255      MARTIN-WIN-PC<20>,MARTIN-WIN-PC<20> (Server service)
10.2.4.101      10.2.4.255      MARTIN-WIN-PC<00>,MARTIN-WIN-PC<00> (Workstation/Redirector)
10.2.4.101      10.2.4.255      WORKGROUP<00>,WORKGROUP<00> (Workstation/Redirector)
10.2.4.101      10.2.4.255      MARTIN-WIN-PC<20>,MARTIN-WIN-PC<20> (Server service)
```

Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

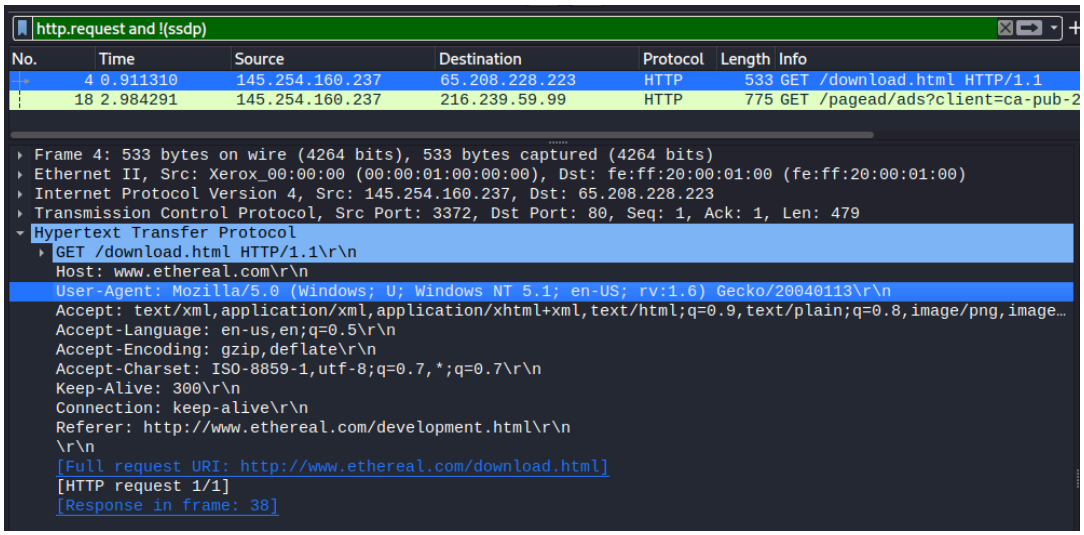
The above screenshot gives the same info as Test 3’s screenshot.

Test 5: Test the Pcap

Summary of test experience:

This test requires us to load a pcap file using wireshark and apply the ‘http.request and !(ssdp)’ filter to get only HTTP request packets, excluding those related to SSDP.

Screenshot of test results:



Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

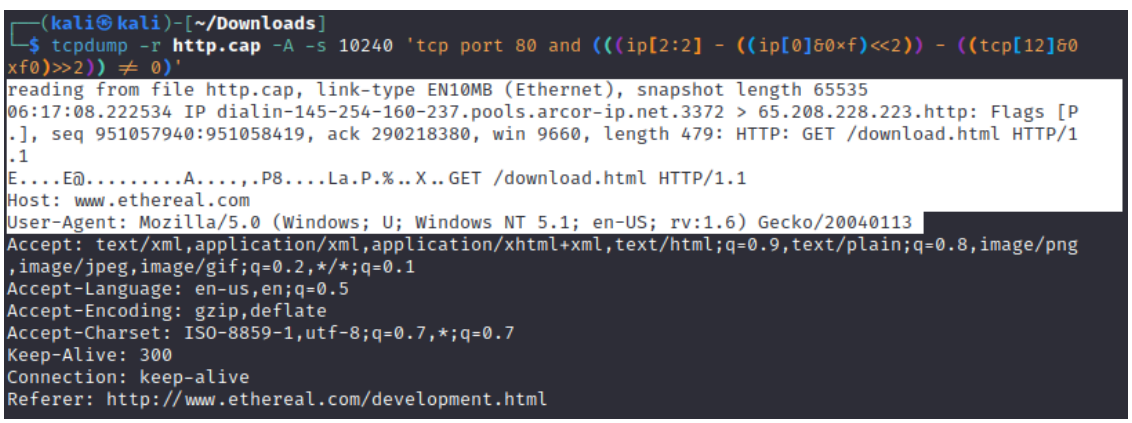
The above screenshot shows the HTTP requests components such as URL, HOST and User Agent.

Test 6: Use Tcpdump

Summary of test experience:

Here, I did Task 5 but using the tcpdump command.

Screenshot of test results:



Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

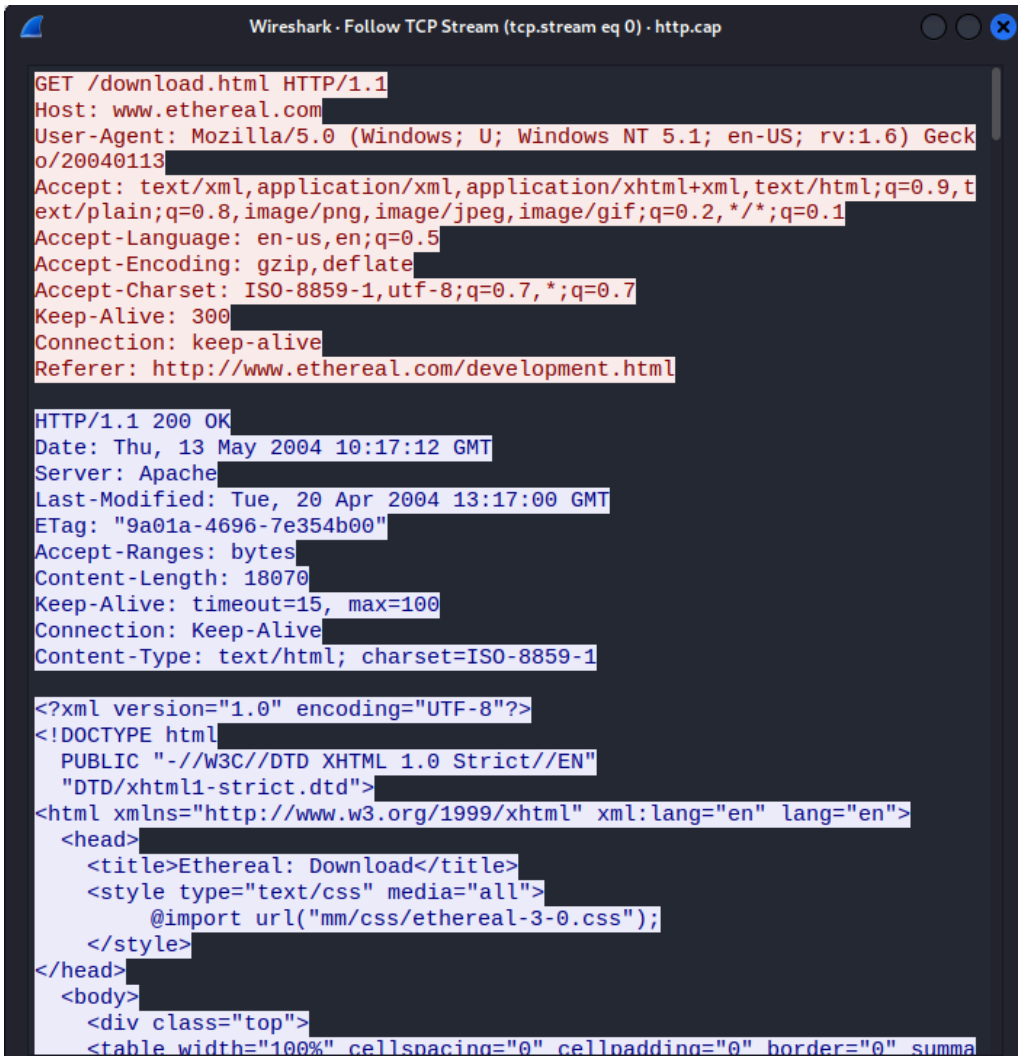
The above screenshot gives the same info as Test 5's screenshot.

Test 7: Follow the TCP Stream

Summary of test experience:

Task 7 requires us to follow the TCP stream of the HTTP request we saw earlier to find the response from the server to the request.

Screenshot of test results:



Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

From the server response, we can see that an Apache server responded with status 200 which is a successful response from a server.