

Lab 12 Response Outline

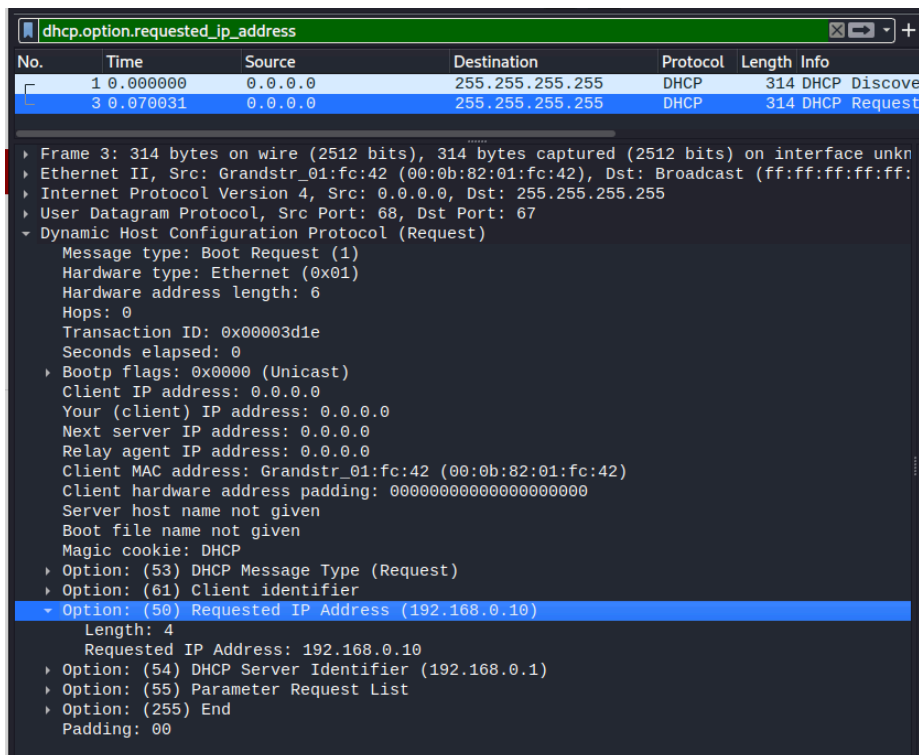
Lab 12: Threat Hunting with Network Data

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?

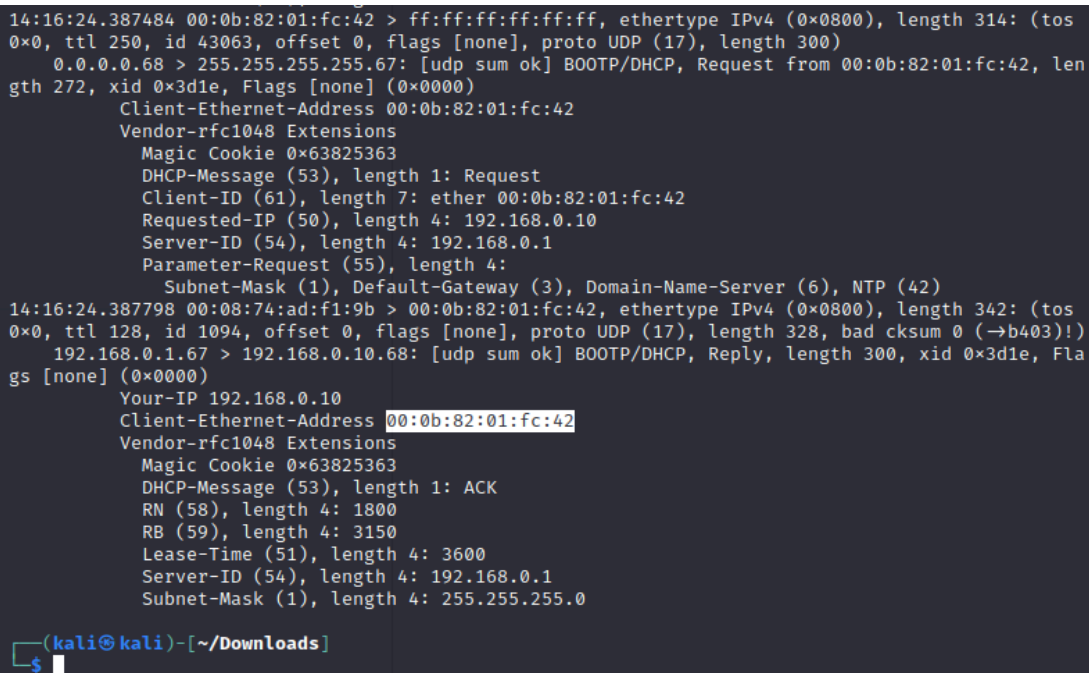
From the above screenshot, we can see the Client MAC address and the Requested IP Address which is 192.168.0.10.

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 (0x0800), length 314: (tos
0x0, 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 0x3d1e, Flags [none] (0x0000)
Client-Ethernet-Address 00:0b:82:01:fc:42
Vendor-rfc1048 Extensions
  Magic Cookie 0x63825363
  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 (0x0800), length 342: (tos
0x0, 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 0x3d1e, Fla
gs [none] (0x0000)
Your-IP 192.168.0.10
Client-Ethernet-Address 00:0b:82:01:fc:42
Vendor-rfc1048 Extensions
  Magic Cookie 0x63825363
  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:

nbns.name						
No.	Time	Source	Destination	Protocol	Length	Info
5	0.079412	10.2.4.101	10.2.4.1	NBNS	110	Registra
6	0.079577	10.2.4.101	10.2.4.1	NBNS	110	Registra
7	0.079585	10.2.4.101	10.2.4.1	NBNS	110	Registra
19	1.586660	10.2.4.101	10.2.4.1	NBNS	110	Registra
20	1.586661	10.2.4.101	10.2.4.1	NBNS	110	Registra
21	1.586661	10.2.4.101	10.2.4.1	NBNS	110	Registra
30	3.102708	10.2.4.101	10.2.4.1	NBNS	110	Registra
31	3.102709	10.2.4.101	10.2.4.1	NBNS	110	Registra
32	3.102709	10.2.4.101	10.2.4.1	NBNS	110	Registra

▶ Frame 5: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
 ▶ Ethernet II, Src: HewlettP_69:53:5a (00:01:e6:69:53:5a), Dst: Netgear_b6:93:f1 (20:e5:2a:
 ▶ Internet Protocol Version 4, Src: 10.2.4.101, Dst: 10.2.4.1
 ▶ User Datagram Protocol, Src Port: 137, Dst Port: 137
 ▼ NetBIOS Name Service
 Transaction ID: 0xe50b
 ▶ Flags: 0x2900, Opcode: Registration, Recursion desired
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 1
 ▶ Queries
 ▼ Additional records
 ▼ MARTIN-WIN-PC<00>: type NB, class IN
 Name: MARTIN-WIN-PC<00> (Workstation/Redirector)
 Type: NB (32)
 Class: IN (1)
 Time to live: 3 days, 11 hours, 20 minutes
 Data length: 6
 ▶ Name flags: 0x6000, ONT: Unknown (H-node, unique)
 Addr: 10.2.4.101

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
File Actions Edit View Help
(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)
```

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

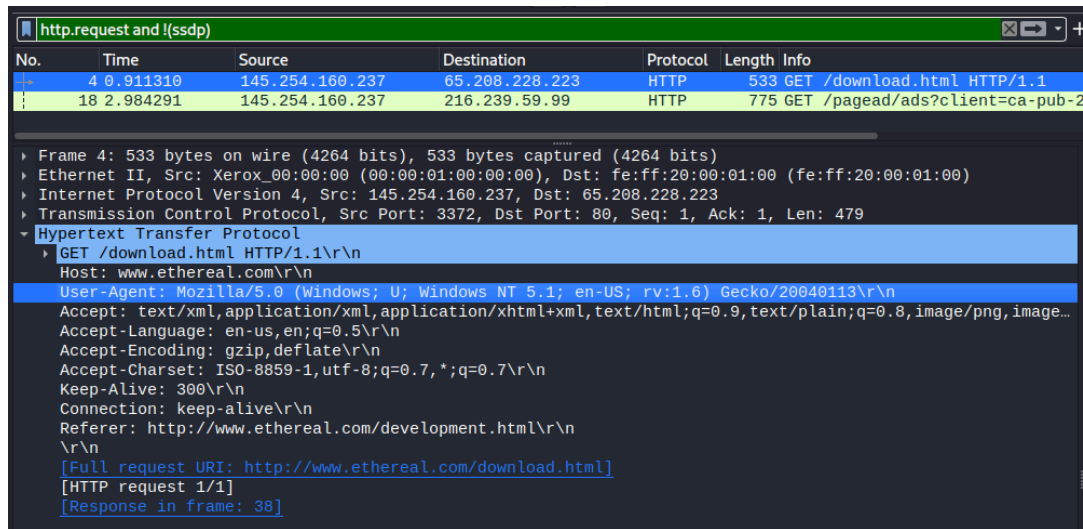
The above screenshot gives the same info as Test 3’s screenshot.

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:



```
http.request and !ssdp
No.    Time           Source            Destination       Protocol Length Info
18 2.984291 145.254.160.237 65.208.228.223   HTTP      775 GET /pagead/ads?client=ca-pub-2

> Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
> Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
> Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
> Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
> Hypertext Transfer Protocol
  > GET /download.html HTTP/1.1\r\n
    Host: www.ethereal.com\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image...
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://www.ethereal.com/development.html\r\n
    \r\n
    [Full request URI: http://www.ethereal.com/download.html]
    [HTTP request 1/1]
    [Response in frame: 38]
```

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

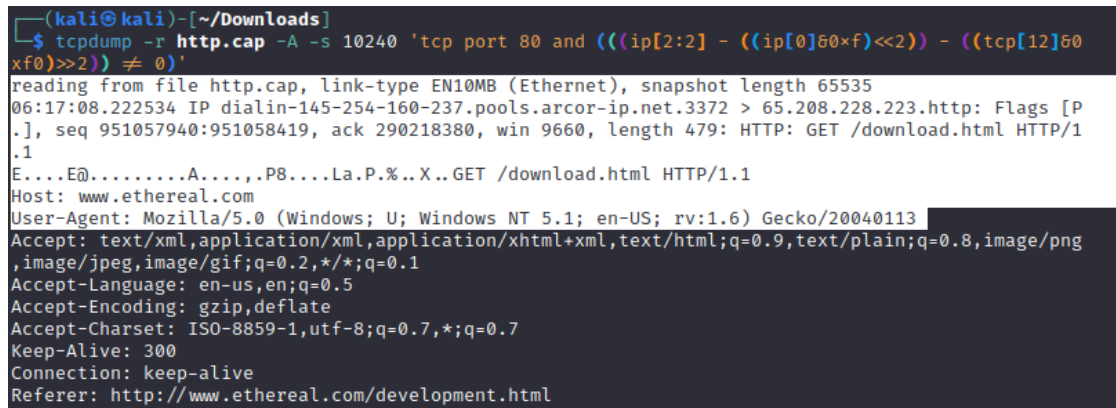
The above screenshot shows the HTTP requests components such as URL, HOST and User Agent.

Test 6: Use Tcpdump

Summary of test experience:

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

Screenshot of test results:



```
(kali@kali)-[~/Downloads]
$ tcpdump -r http.cap -A -s 10240 'tcp port 80 and (((ip[2:2] - ((ip[0]&0xf)<<2)) - ((tcp[12]&0xf0)>>2)) != 0)'
reading from file http.cap, link-type EN10MB (Ethernet), snapshot length 65535
06:17:08.222534 IP dialin-145-254-160-237.pools.arcor-ip.net.3372 > 65.208.228.223.http: Flags [P
.], seq 951057940:951058419, ack 290218380, win 9660, length 479: HTTP: GET /download.html HTTP/1
.1
E...E@.....A....,P8....La.P.%..X..GET /download.html HTTP/1.1
Host: www.ethereal.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png
,image/jpeg,image/gif;q=0.2,*/*;q=0.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.ethereal.com/development.html
```

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

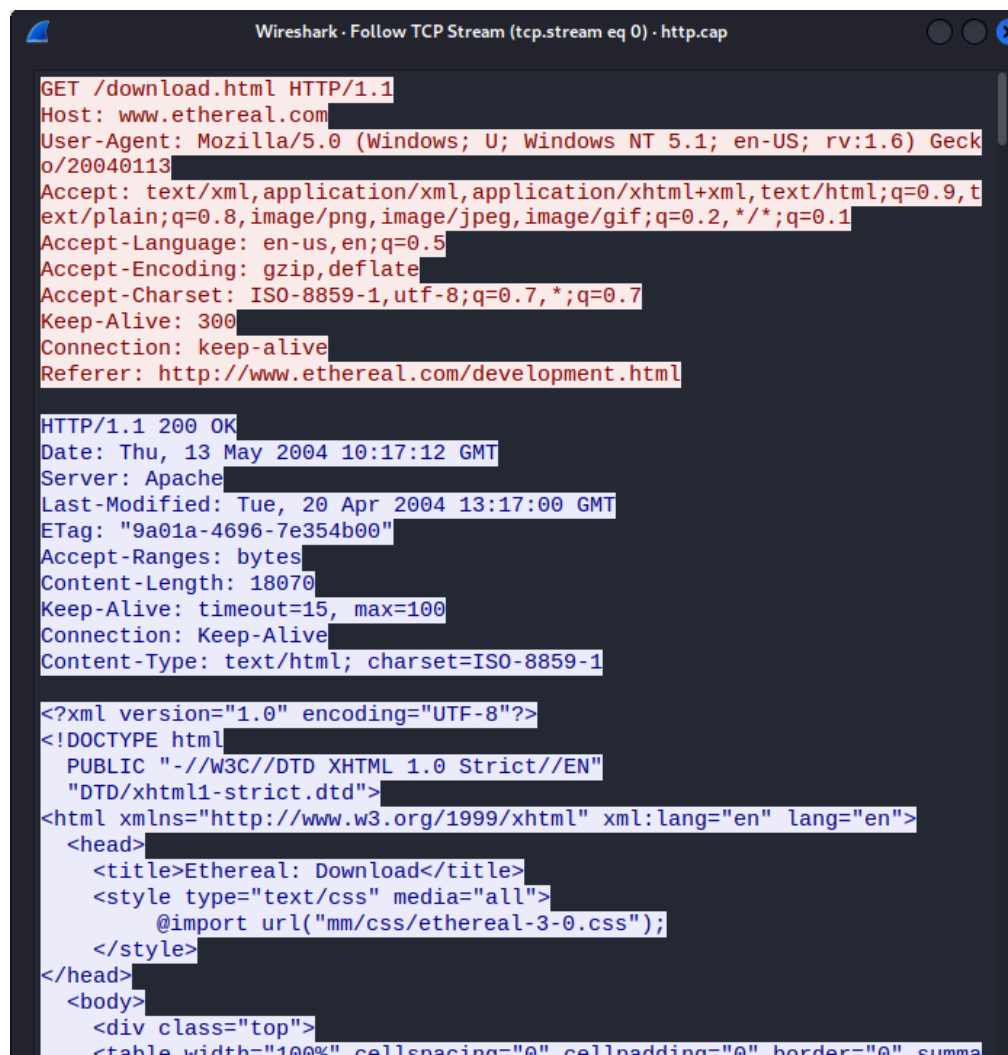
The above screenshot gives the same info as Test 5's screenshot.

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:



The screenshot shows a Wireshark window titled "Wireshark - Follow TCP Stream (tcp.stream eq 0) - http.cap". It displays the details of an HTTP transaction. The request is a GET for /download.html from www.ethereal.com, using Mozilla/5.0 as the user agent. The response is an HTTP/1.1 200 OK from an Apache server, with a content type of text/html and a status of 200 OK. The response body is an XML document with a title "Ethereal: Download" and a table structure.

```
GET /download.html HTTP/1.1
Host: www.ethereal.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.ethereal.com/development.html

HTTP/1.1 200 OK
Date: Thu, 13 May 2004 10:17:12 GMT
Server: Apache
Last-Modified: Tue, 20 Apr 2004 13:17:00 GMT
ETag: "9a01a-4696-7e354b00"
Accept-Ranges: bytes
Content-Length: 18070
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=ISO-8859-1

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html
  PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
  <head>
    <title>Ethereal: Download</title>
    <style type="text/css" media="all">
      @import url("mm/css/ethereal-3-0.css");
    </style>
  </head>
  <body>
    <div class="top">
      <table width="100%" cellspacing="0" cellpadding="0" border="0" summa
```

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.