

Wireshark Lab: DNS

it's 2.5

As described in Section 2.4 of the text¹, the Domain Name System (DNS) translates hostnames to IP addresses, fulfilling a critical role in the Internet infrastructure. In this lab, we'll take a closer look at the client side of DNS. Recall that the client's role in the DNS is relatively simple – a client sends a *query* to its local DNS server, and receives a *response* back. As shown in Figures 2.19 and 2.20 in the textbook, much can go on “under the covers,” invisible to the DNS clients, as the hierarchical DNS servers communicate with each other to either recursively or iteratively resolve the client's DNS query. From the DNS client's standpoint, however, the protocol is quite simple – a query is formulated to the local DNS server and a response is received from that server.

it's 2.5

Before beginning this lab, you'll probably want to review DNS by reading Section 2.4 of the text. In particular, you may want to review the material on **local DNS servers**, **DNS caching**, **DNS records and messages**, and the **TYPE field** in the DNS record.

1. nslookup explanation (for the quiz)

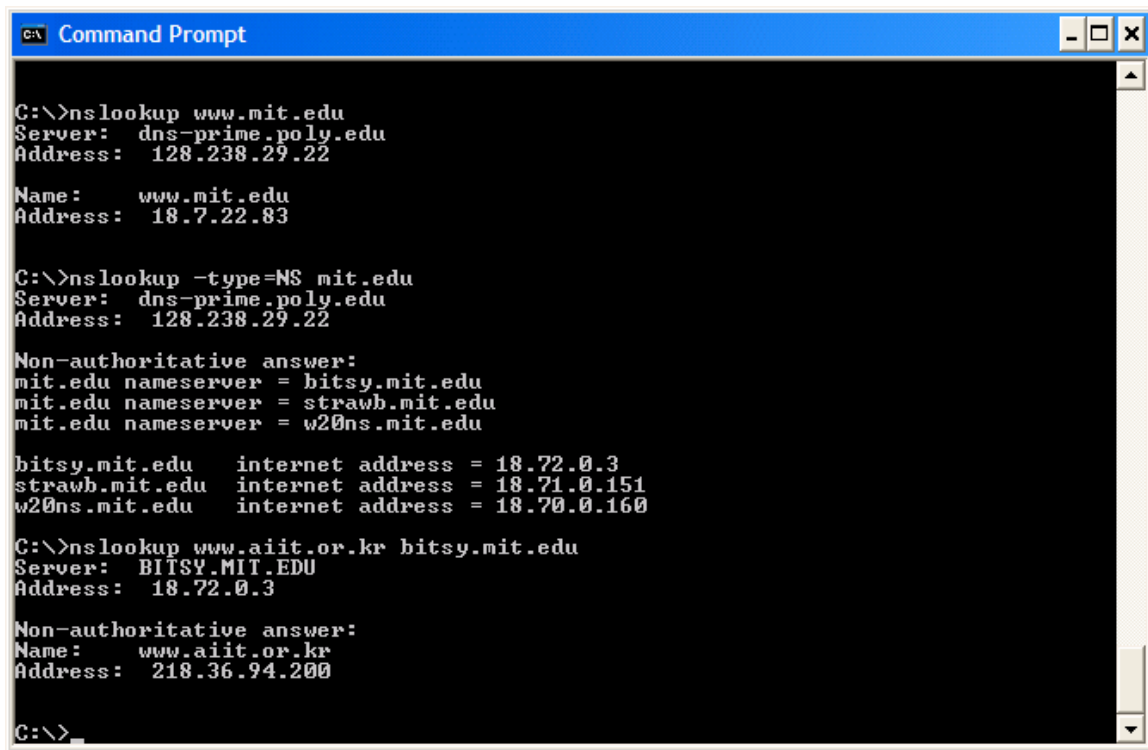
In this lab, we'll make extensive use of the *nslookup* tool, which is available in most Linux/Unix and Microsoft platforms today. To run *nslookup* in Linux/Unix, you just type the *nslookup* command on the command line. To run it in Windows, open the Command Prompt and run *nslookup* on the command line.

In its most basic operation, *nslookup* tool allows the host running the tool to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level-domain DNS server, an authoritative DNS server, or an intermediate DNS server (see the textbook for definitions of these terms). To accomplish this task, *nslookup* sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.

The above screenshot shows the results of three independent *nslookup* commands (displayed in the Windows Command Prompt). In this example, the client host is located on the campus of Polytechnic University in Brooklyn, where the default local DNS server is dns-prime.poly.edu. When running *nslookup*, if no DNS server is specified, then *nslookup* sends the query to the default DNS server, which in this case is dns-prime.poly.edu. Consider the first command:

```
nslookup www.mit.edu
```

In words, this command is saying “please send me the IP address for the host www.mit.edu”. As shown in the screenshot, the response from this command provides two pieces of information: (1) the name and IP address of the DNS server that provides the answer; and (2) the answer itself, which is the host name and IP address of www.mit.edu. Although the response came from the local DNS server at Polytechnic University, it is quite possible that this local DNS server iteratively contacted several other DNS servers to get the answer, as described in Section 2.4 of the textbook.



```
C:\>nslookup www.mit.edu
Server: dns-prime.poly.edu
Address: 128.238.29.22

Name: www.mit.edu
Address: 18.7.22.83

C:\>nslookup -type=NS mit.edu
Server: dns-prime.poly.edu
Address: 128.238.29.22

Non-authoritative answer:
mit.edu nameserver = bitsy.mit.edu
mit.edu nameserver = strawb.mit.edu
mit.edu nameserver = w20ns.mit.edu

bitsy.mit.edu internet address = 18.72.0.3
strawb.mit.edu internet address = 18.71.0.151
w20ns.mit.edu internet address = 18.70.0.160

C:\>nslookup www.aiit.or.kr bitsy.mit.edu
Server: BITSY.MIT.EDU
Address: 18.72.0.3

Non-authoritative answer:
Name: www.aiit.or.kr
Address: 218.36.94.200

C:\>
```

Now consider the second command:

```
nslookup -type=NS mit.edu
```

In this example, we have provided the option “-type=NS” and the domain “mit.edu”. This causes *nslookup* to send a query for a type-NS record to the default local DNS server. In

words, the query is saying, “please send me the host names of the authoritative DNS for mit.edu”. (When the `-type` option is not used, *nslookup* uses the default, which is to query for type A records.) The answer, displayed in the above screenshot, first indicates the DNS server that is providing the answer (which is the default local DNS server) along with three MIT nameservers. Each of these servers is indeed an authoritative DNS server for the hosts on the MIT campus. However, *nslookup* also indicates that the answer is “non-authoritative,” meaning that this answer came from the cache of some server rather than from an authoritative MIT DNS server. Finally, the answer also includes the IP addresses of the authoritative DNS servers at MIT. (Even though the type-NS query generated by *nslookup* did not explicitly ask for the IP addresses, the local DNS server returned these “for free” and *nslookup* displays the result.)

Now finally consider the third command:

```
nslookup www.aiit.or.kr bitsy.mit.edu
```

In this example, we indicate that we want the query sent to the DNS server bitsy.mit.edu rather than to the default DNS server (dns-prime.poly.edu). Thus, the query and reply transaction takes place directly between our querying host and bitsy.mit.edu. In this example, the DNS server bitsy.mit.edu provides the IP address of the host www.aiit.or.kr, which is a web server at the Advanced Institute of Information Technology (in Korea).

Now that we have gone through a few illustrative examples, you are perhaps wondering about the general syntax of *nslookup* commands. The syntax is:

```
nslookup -option1 -option2 host-to-find dns-server
```

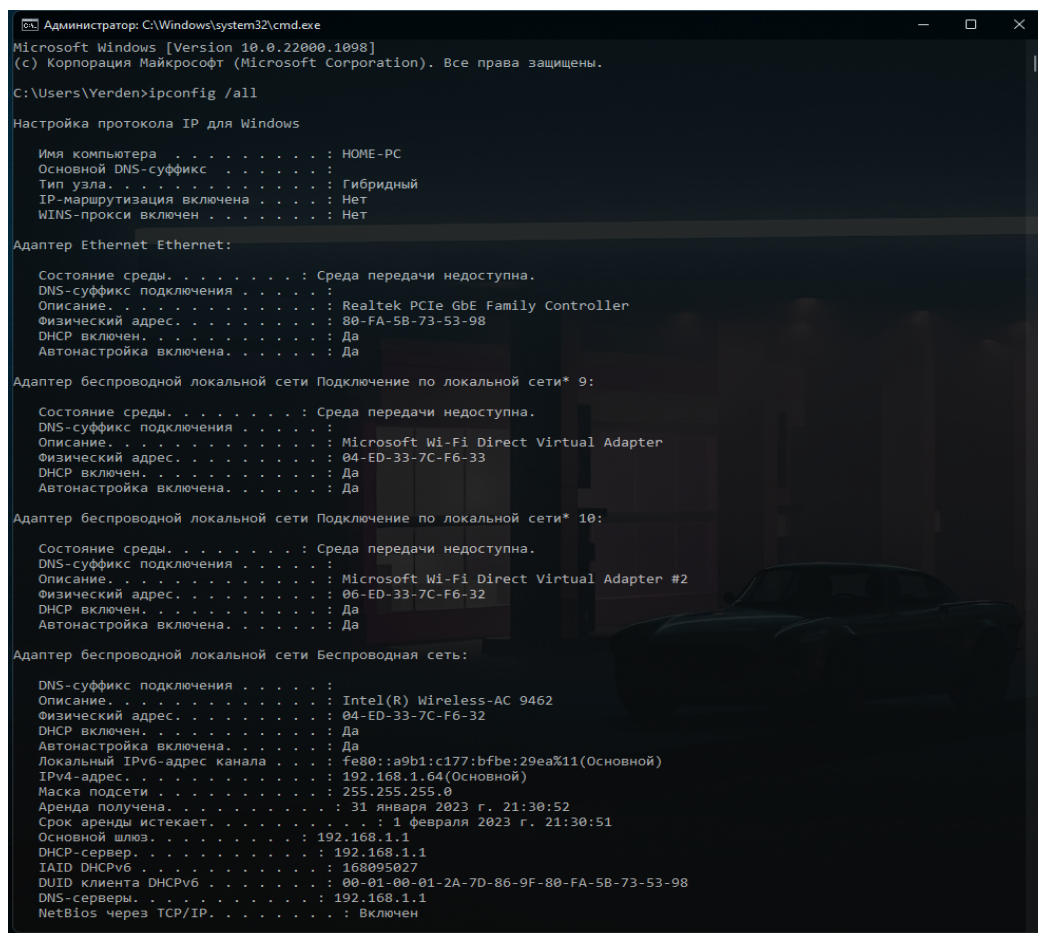
In general, *nslookup* can be run with zero, one, two or more options. And as we have seen in the above examples, the *dns-server* is optional as well; if it is not supplied, the query is sent to the default local DNS server.

2. ipconfig

ipconfig (for Windows) and *ifconfig* (for Linux/Unix) are among the most useful little utilities in your host, especially for debugging network issues. Here we'll only describe *ipconfig*, although the Linux/Unix *ifconfig* is very similar. *ipconfig* can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on. For example, if you all this information about your host simply by entering

```
ipconfig /all
```

into the Command Prompt, as shown in the following screenshot.



```
Администратор: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.22000.1098]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\Yerden>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : HOME-PC
Основной DNS-суффикс . . . . . :
Тип узла . . . . . : Гибридный
IP-маршрутизация включена . . . . . : Нет
WINS-прокси включен . . . . . : Нет

Адаптер Ethernet Ethernet:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Realtek PCIe GbE Family Controller
Физический адрес. . . . . : 80-FA-5B-73-53-98
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 9:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Физический адрес. . . . . : 04-ED-33-7C-F6-33
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 10:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Физический адрес. . . . . : 06-ED-33-7C-F6-32
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . :
Описание. . . . . : Intel(R) Wireless-AC 9462
Физический адрес. . . . . : 04-ED-33-7C-F6-32
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . . . : fe80::a9b1:c177:bfb6:29ea%11(Основной)
IPv4-адрес. . . . . : 192.168.1.64(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 31 января 2023 г. 21:30:52
Срок аренды истекает. . . . . : 1 февраля 2023 г. 21:30:51
Основной шлюз. . . . . : 192.168.1.1
DHCP-сервер. . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 168095027
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2A-7D-86-9F-80-FA-5B-73-53-98
DNS-серверы. . . . . : 192.168.1.1
NetBios через TCP/IP. . . . . : Включен
```

Figure 1-1. *ipconfig /all* on windows

ipconfig will show you all available network interface cards on your laptop, such as ethernet, wi-fi, virtual adapters, etc. Notice that, in the screenshot above, we are choosing the active interface, which is the last one, "Inter(R) Wireless-AC 9462" and we will use the data given there - DNS server, IPv4 address, MAC address.

1. Make a screenshot of *ipconfig/ifconfig* command from your terminal so we can see your DNS server, local IPv4 address and MAC address and they must be annotated with red. You **must** name it "*cmd-info*" and format can be *.jpg* or *.png*. You are not allowed to disguise or hide any data from that screenshot, otherwise you won't get any points for the lab.

ipconfig is also very useful for managing the DNS information stored in your host. In Section 2.5 we learned that a host can cache DNS records it recently obtained. To see these cached records, after the prompt *C:\>* provide the following command:

```
ipconfig /displaydns
```

Each entry shows the remaining Time to Live (TTL) in seconds. To clear the cache, enter

```
ipconfig /flushdns
```

Flushing the DNS cache clears all entries and reloads the entries from the hosts file.

3. Tracing DNS with Wireshark

Now that we are familiar with *nslookup* and *ipconfig*, we're ready to capture DNS packets and analyze their content. But before that, you will have to calculate your *newID* to know which website you will be using for this lab. On Moodle lab section, open *Calculate-NewID* file and find out your *newID*. Then, download the *websites.xlsx* excel file, use search to find your *newID* inside the excel file, and use the website url next to your *newID* on that row.

!Attention! Using someone else's website will lead to the nullification of your grade for that particular lab.

- Use *ipconfig* to empty the DNS cache in your host.
- Open your browser and **EMPTY YOUR BROWSER CACHE!**
- Open Wireshark and enter "ip.addr == your_local_IP_address" into the filter, where you obtain *your_local_IP_address* with *ipconfig*. This filter removes all packets that neither originate nor are destined to your host. Also, add "&& dns" filter, to show only dns packets.
- Start packet capture in Wireshark.
- With your browser, visit the Web page, which is next to your *newID* in the excel file *websites.xlsx*
- Stop packet capture.

Save your wireshark file, name it "*Lab3-p2*", file extension is default *.pcapng*. You should get something like shown below in Figure 2-1.

From those dns packets, pick a pair of DNS query and a DNS response to that query, where a DNS query is of type 'A' and the website url can be seen in the *Info* column of that DNS query packet. In Figure 2-1, it can be a packet #105, because I'm trying to access *androidpolice.com*.

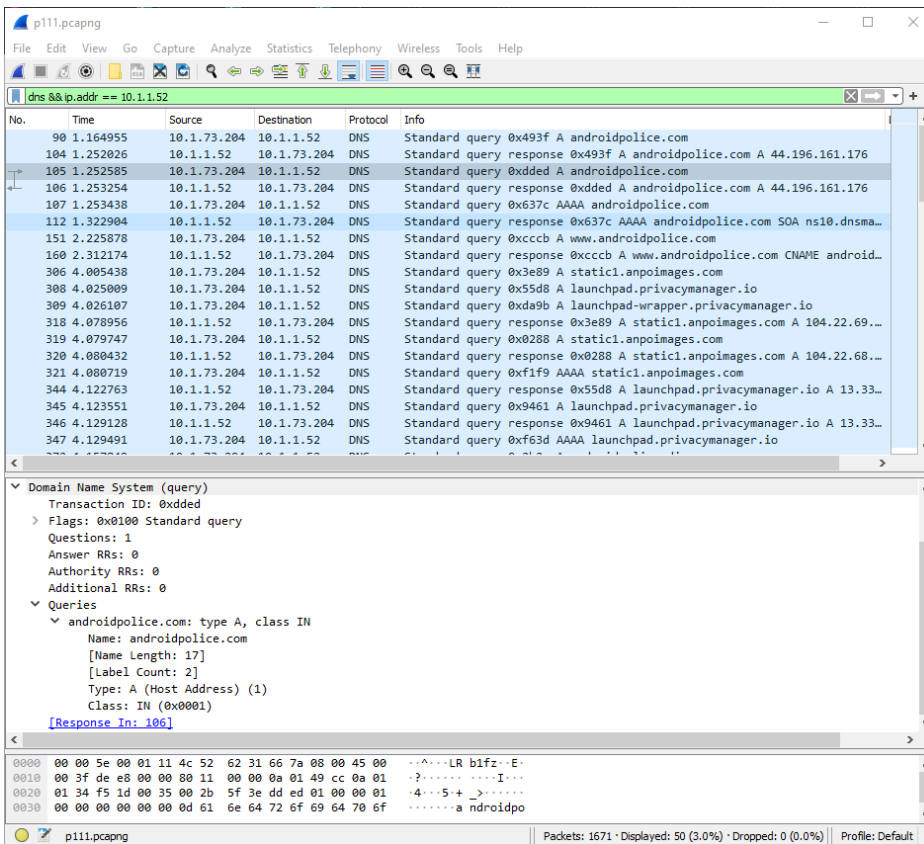


Figure 2-1. Capturing dns packets from accessing a website from the browser

2. Pick the DNS query and response messages. Tap to the DNS query packet and annotate the packet number of DNS query in your screenshot 'P2-1'.
3. On the same screenshot 'P2-1' annotate the packet number of the DNS response packet, which contains a response to your DNS query done in question 2.
4. On the same screenshot 'P2-1' annotate the source IP address in the DNS query packet. Where that IP address belongs to, according to your *cmd-info* screenshot? Write your answer on the screenshot, with red.
5. On the same screenshot 'P2-1' annotate the destination IP address in the DNS query packet. Where that IP address belongs to, according to your *cmd-info* screenshot? Write your answer on the screenshot, with red.
6. But how did you clarify that this DNS query is really of type 'A'? Annotate from the packet details window, inside DNS section. Annotate it in the screenshot 'P2-1'.
7. Now tap the DNS response message. Annotate its packet number on the screenshot 'P2-2'.
8. How many 'answers' are provided? Annotate the necessary field from DNS section, on 'P2-2'.
9. On the same screenshot 'P2-2' you should make one of the answers visible and annotate the *address*, *name* and *ttl* fields inside the *Answers* section.

Now you need to clear DNS cache from your terminal again and from your browser as well.

- Start packet capture.
- Do an *nslookup url*, where url is your website from the excel file.
- Stop packet capture.

Save your wireshark file, name it "*Lab3-p3*", file extension is default *.pcapng*. You should get something like shown below in Figure 3-1:

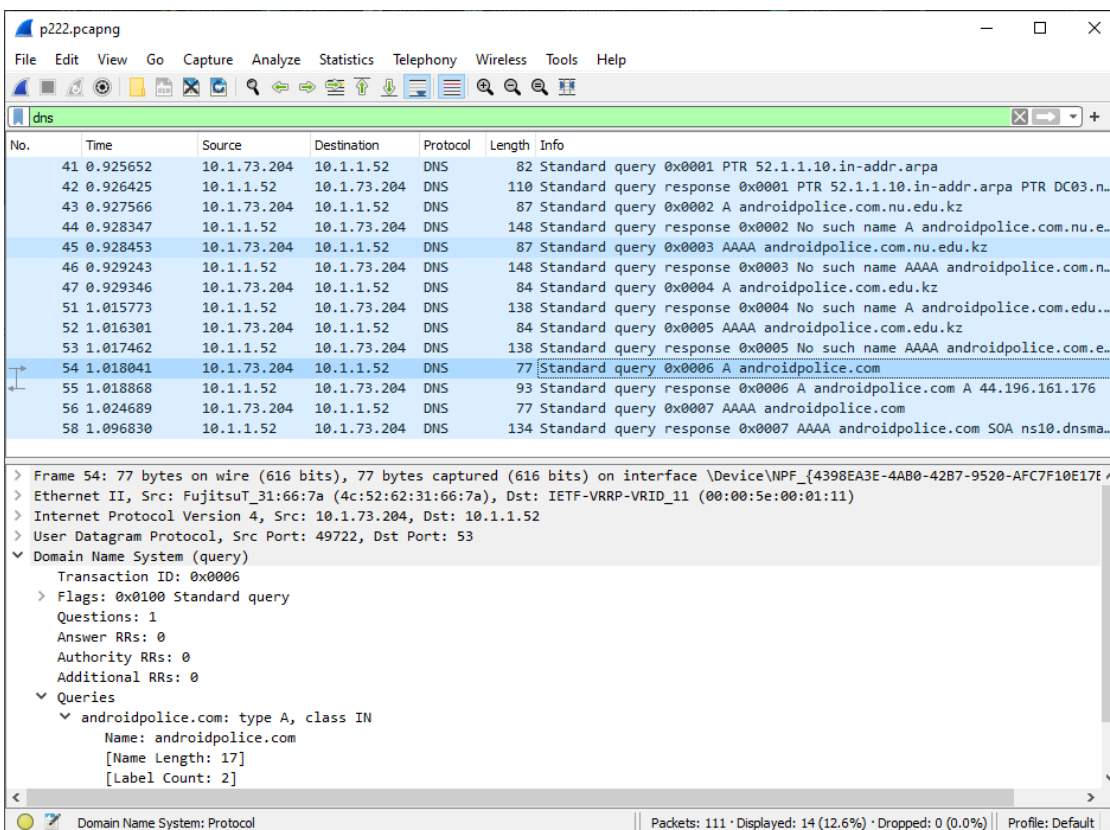


Figure 3-1. Capturing *nslookup* from terminal.

From those dns packets, pick a pair of DNS query and a DNS response to that query, where a DNS query is of type 'A' and the website url can be seen in the *Info* column of that DNS query packet. In Figure 3-1, it can be the packet #54, because I'm trying to access *androidpolice.com*.

10. Tap the DNS query packet, annotate its packet number on the screenshot named 'P3-1'.
11. Annotate source and destination ports inside UDP section. Are those ports the same as the ones from the packet you chose in Question 2, from the previous capture file "*Lab3-p2*"? Write "same" or "different" on the same screenshot 'P3-1'.
12. Why is it so? Explain the result of your answer for Q11. You can add 2-3 sentences on the screenshot 'P3-1'.
13. Now tap the DNS response packet, which is the actual response to the query done in the packet you chose in Q10. Annotate the packet number in the screenshot 'P3-2'.
14. Annotate in the screenshot 'P3-2' all the differences inside *DNS-Answers* section of this response packet and the response packet from Q7, which is from the file "*Lab3-p2*". If there is no difference, write "SAME" on the screenshot.

Now clear the DNS cache from your terminal again.

- Start packet capture.
- Do an *nslookup -type=NS url*, where url is your website from the excel file.
- Stop packet capture.

Save your wireshark file, name it "*Lab3-p4*", file extension is default *.pcapng*. Also, save your screenshot from terminal and name it "*cmd-nslookup-ns*". You should get something like shown below in Figure 4-1:

The image shows a Wireshark capture of DNS traffic. The packet list on the left shows several DNS queries and responses. Packet 30 is a standard query response for 'androidpolice.com' with 11 answers. The packet details pane on the right shows the structure of this response, including the transaction ID, flags, and a list of 11 authoritative name servers.

No.	Time	Source	Destination	Protocol	Info	Length
16	0.918864	10.1.73.204	10.1.1.52	DNS	Standard query 0x0001 PTR 52.1.1.10.in-addr.arpa	82
17	0.919621	10.1.1.52	10.1.73.204	DNS	Standard query response 0x0001 PTR 52.1.1.10.in-addr.arpa PTR DC03.n...	110
18	0.920518	10.1.73.204	10.1.1.52	DNS	Standard query 0x0002 NS androidpolice.com.nu.edu.kz	87
19	0.921243	10.1.1.52	10.1.73.204	DNS	Standard query response 0x0002 No such name NS androidpolice.com.nu...	148
20	0.921355	10.1.73.204	10.1.1.52	DNS	Standard query 0x0003 NS androidpolice.com.edu.kz	84
26	1.009377	10.1.1.52	10.1.73.204	DNS	Standard query response 0x0003 No such name NS androidpolice.com.edu...	138
27	1.009571	10.1.73.204	10.1.1.52	DNS	Standard query 0x0004 NS androidpolice.com	77
30	1.107052	10.1.1.52	10.1.73.204	DNS	Standard query response 0x0004 NS androidpolice.com NS ns13.dnsmadee...	439

Packet 30 details:

- Frame 30: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits) on interface \Device\NPF_{4398EA3E-4AB0-42B7-9520-AFC7F1E...}
- Ethernet II, Src: HewlettP_78:2b:26 (cc:3e:5f:78:2b:26), Dst: FujitsuT_31:66:7a (4c:52:62:31:66:7a)
- Internet Protocol Version 4, Src: 10.1.1.52, Dst: 10.1.73.204
- User Datagram Protocol, Src Port: 53, Dst Port: 54320
- Domain Name System (response)
 - Transaction ID: 0x0004
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 6
 - Authority RRs: 0
 - Additional RRs: 11
 - Queries
 - androidpolice.com: type NS, class IN
 - Name: androidpolice.com
 - [Name Length: 17]
 - [Label Count: 2]
 - Type: NS (authoritative Name Server) (2)
 - Class: IN (0x0001)
 - Answers
 - androidpolice.com: type NS, class IN, ns ns13.dnsmadeeasy.com
 - androidpolice.com: type NS, class IN, ns ns15.dnsmadeeasy.com
 - androidpolice.com: type NS, class IN, ns ns10.dnsmadeeasy.com
 - androidpolice.com: type NS, class IN, ns ns12.dnsmadeeasy.com
 - androidpolice.com: type NS, class IN, ns ns11.dnsmadeeasy.com
 - androidpolice.com: type NS, class IN, ns ns14.dnsmadeeasy.com

Figure 4-1. Capturing *nslookup -type=NS* from terminal.

From those dns packets, pick a DNS query, with type='NS' which has got the correct response to its query. That correct response should have the list of the servers, which you got in your terminal, after running *nslookup -type=NS*. In Figure 4-1, response packets #19 and #26 have the flag "no such name" up, meaning you won't find any *Answers* inside the DNS section. Packet #17 isn't of type 'NS', but packet #30 is 'NS' and seems to be fine, because it has all the entries we got from terminal.

15. Tap on the correct DNS query, annotate its packet number on the screenshot 'P4-1'.
16. Annotate on the screenshot 'P4-1' the type of the query inside the DNS section in the packet details window.
17. Tap on the correct DNS response packet. Annotate its packet number on the screenshot 'P4-2'.
18. How many answers are given inside the DNS section? Annotate so that each answer is visible, on the screenshot 'P4-2'. You don't have to show their content on the screenshot. Keep them so that each answer is written in 1 row.
19. Is this number the same as the number of entries given on "*cmd-nslookup-ns*"? Annotate on the screenshot 'P4-2' as YES or NO.

Submit:

cmd-info - screenshot of ipconfig/ifconfig from terminal (0 for the lab, if not uploaded)

cmd-nslookup-ns - screenshot of nslookup -type=NS from terminal

Lab3-p2 - wireshark capture file for web browser test

P2-1, P2-2 - screenshots for part 2.

Lab3-p3 - wireshark capture file for nslookup test from terminal

P3-1, P3-2 - screenshots for part 3.

Lab3-p4 - wireshark capture file for nslookup -type=NS test from terminal

P4-1, P4-2 - screenshots for the last part.

!Attention! Using wrong filename for screenshots or wireshark files will lead to loss of points.
If you don't submit a screenshot or a wireshark file for a particular part, that part will be graded as 0.

IMPORTANT! How to annotate a screenshot as a correct proof to your answer.
Incorrect proof doesn't give any points.

1) Incorrect proof:

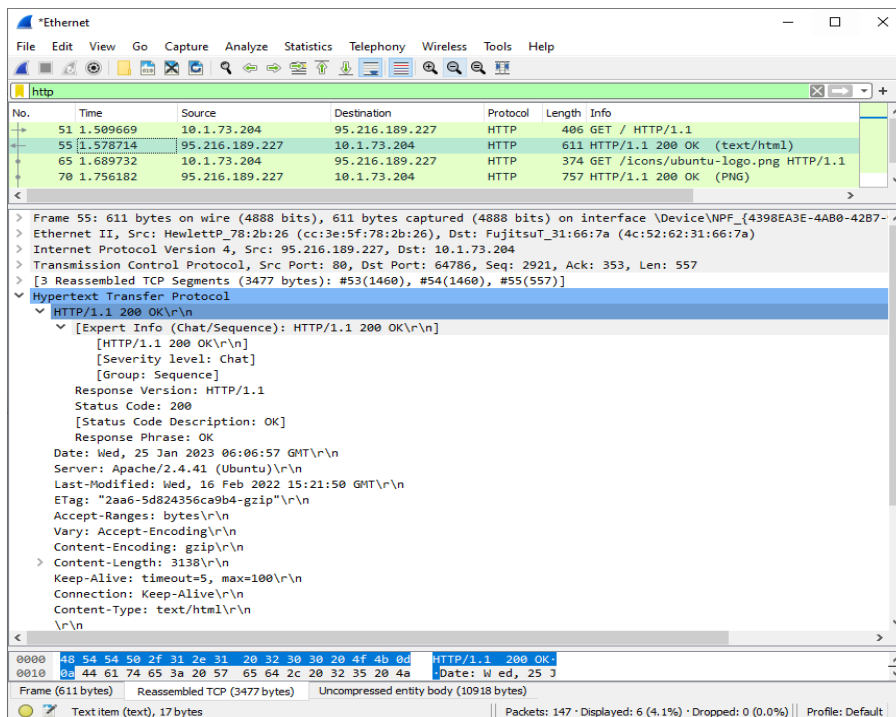


Figure 10: incorrect proof. No annotations.

2) Correct proof:

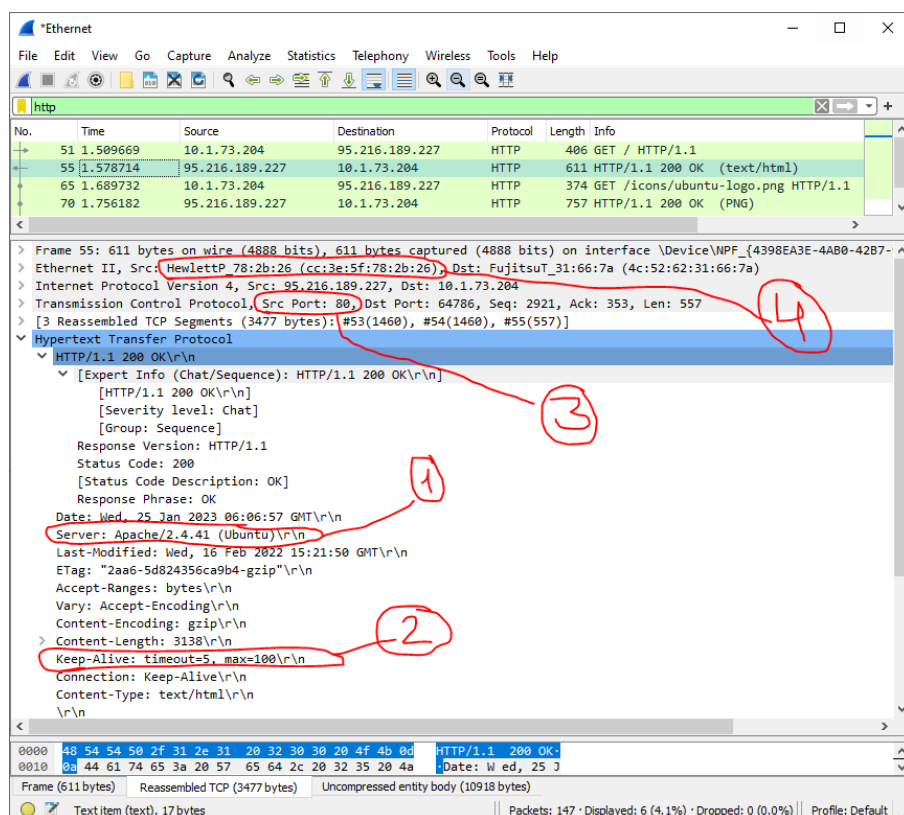


Figure 11: correct proof. Red annotations with question numbers shown.

3) Incorrect proof:

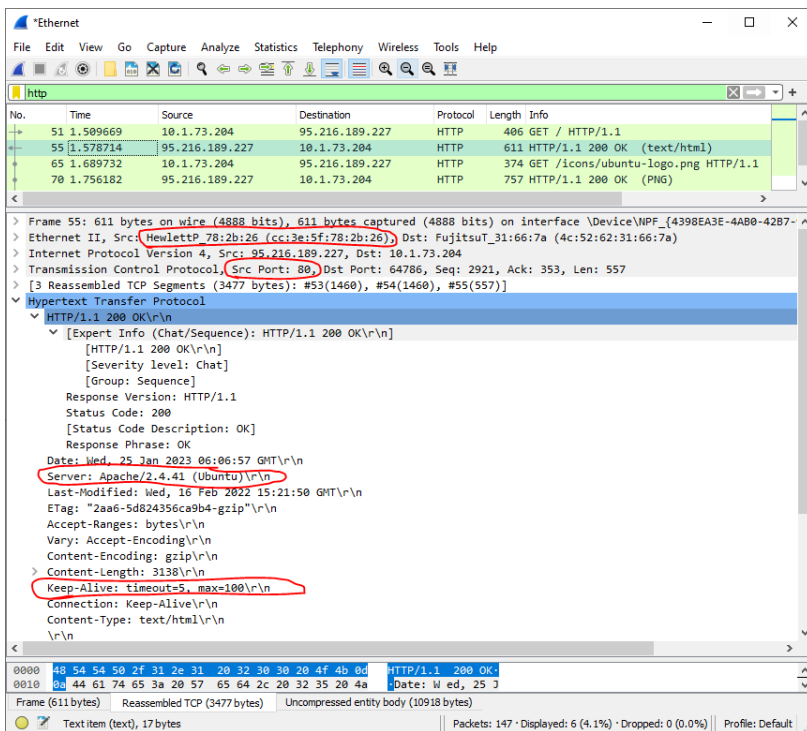


Figure 12: incorrect proof. Annotations without the question numbers.

4) Incorrect proof:

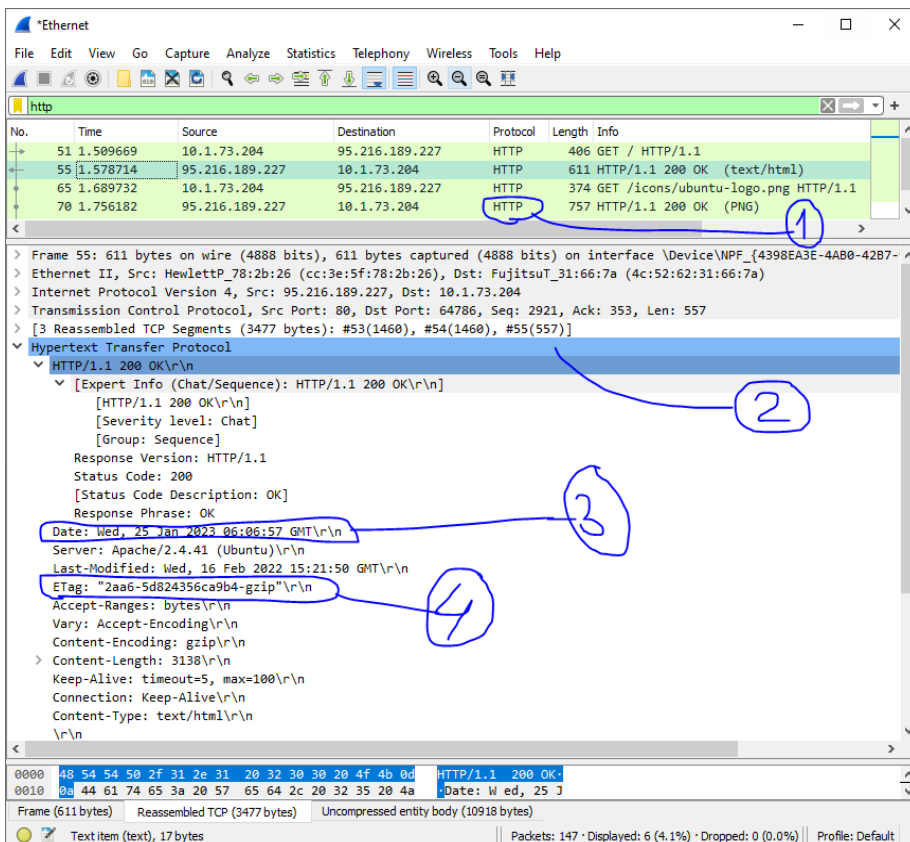


Figure 13: incorrect proof. Annotations are not red.