**Nội dung và hướng dẫn bài thực hành**

***Mục đích***

Thông qua bài thực hành này, sinh viên không chỉ hiểu rõ cách Wireshark hoạt động mà còn biết cách ứng dụng công cụ này để giám sát và bảo mật mạng. Điều này góp phần nâng cao năng lực phân tích và giải quyết vấn đề của sinh viên trong lĩnh vực bảo mật thông tin và quản trị hệ thống mạng, đồng thời trang bị kỹ năng quan trọng để đối phó với các thách thức thực tế trong an ninh mạng.

***Yêu cầu đối với sinh viên***

Có kiến thức cơ bản về hệ điều hành Linux, công cụ Wireshark.

***Nội dung thực hành***

Khởi động bài lab:

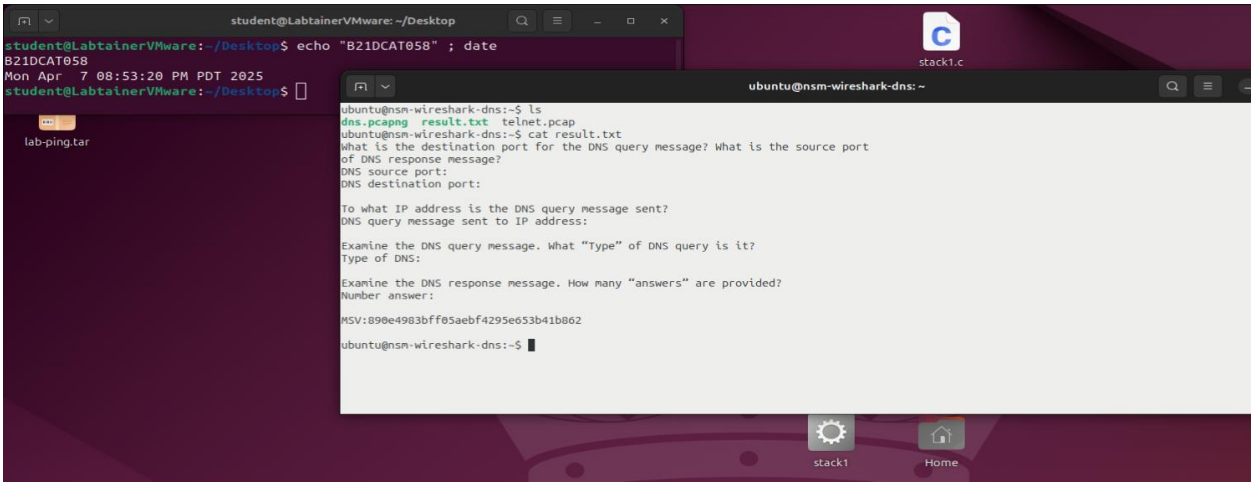
Vào terminal, gõ:

*Labtainer -r nsm-wireshark-dns*

*(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)*

Sau khi khởi động xong một terminal ảo sẽ xuất hiện. Trên terminal thực hiện mở file result.txt để điền kết quả:

*Sudo nano result.txt*

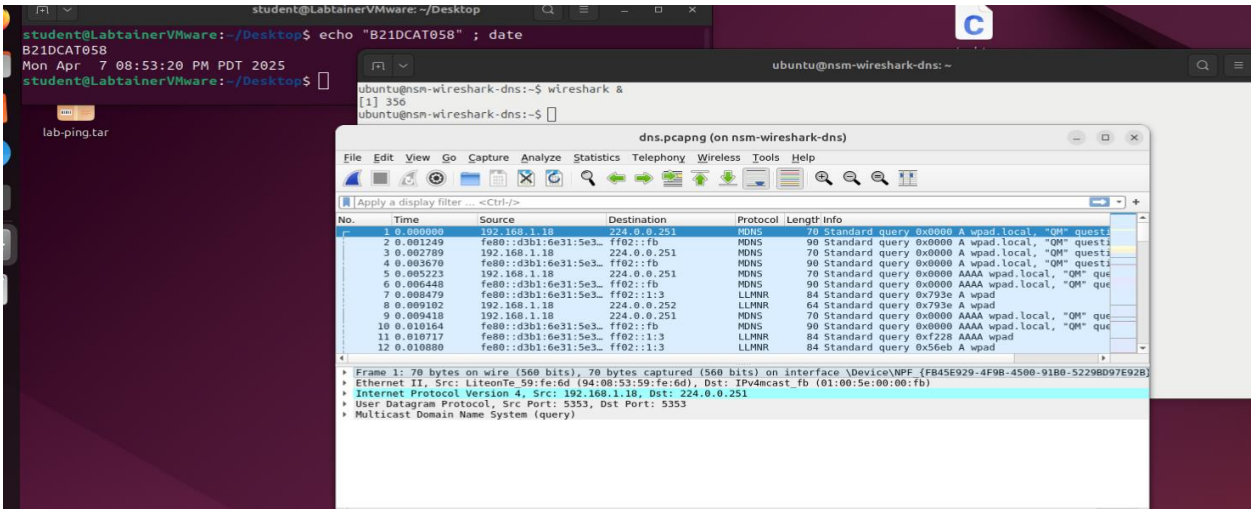


Bài lab đã tạo sẵn 1 file dns.pcap chứa nội dung các gói tin đã chụp. Chúng ta sẽ thực hiện mở file này bằng wireshark và thực hiện phân tích và trả lời câu hỏi trong file result.txt

Từ file dns.pcap ta sẽ tìm được các gói tin phù hợp với câu hỏi

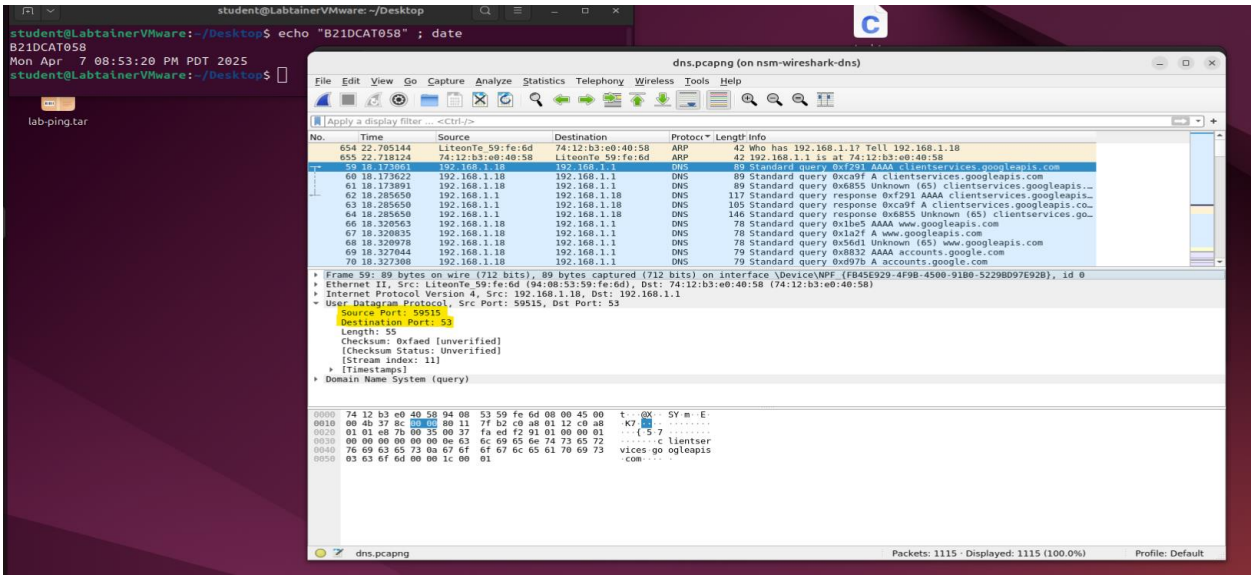
Câu trả lời sẽ phải điền vào file *result.txt*.

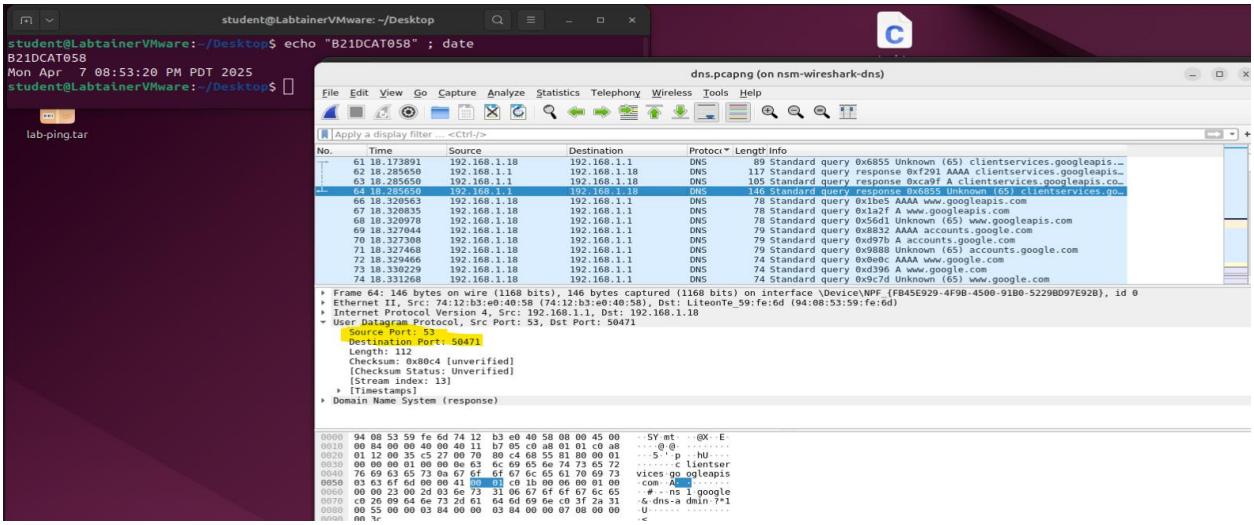
Đầu tiên thực hiện mở file "dns.pcapng" bằng Wireshark




**Task 1: What is the destination port for the DNS query message? What is the source port of DNS response message?**

- ➔ **DNS source port:53**
- ➔ **DNS destination port:53**
- Filter: dns
- Chọn một gói có **"Standard query"**, kiểm tra **UDP header**:
  - **Source port** là cổng tạm của client
  - **Destination port** là 53 (mặc định DNS server)
- Chọn gói **"Standard query response"**, source và destination port sẽ đảo ngược.

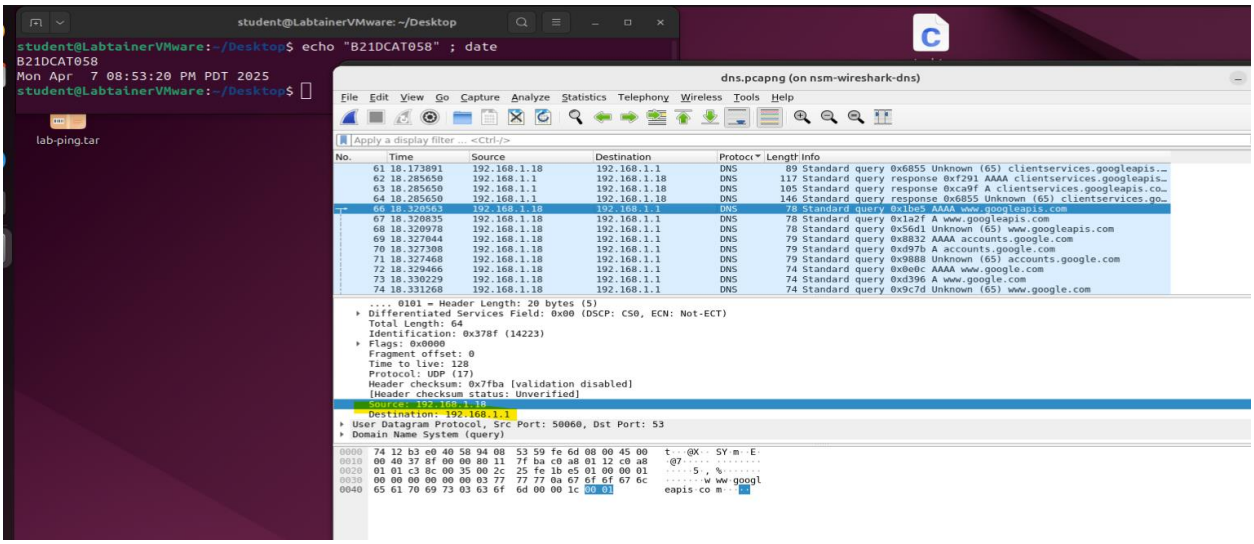

student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "B21DCAT058" ; date
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware:~/Desktop$
lab-ping.tar
dns.pcapng (on nsm-wireshark-dns)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
654 22.705144 LiteonTe_59:fe:6d 74:12:b3:e0:40:58 ARP 42 Who has 192.168.1.17 Tell 192.168.1.18
655 22.718124 74:12:b3:e0:40:58 LiteonTe_59:fe:6d ARP 42 192.168.1.1 is at 74:12:b3:e0:40:58
59 18.173061 192.168.1.18 192.168.1.1 DNS 89 Standard query 0xf291 AAAA clientservices.googleapis.com
60 18.173622 192.168.1.18 192.168.1.1 DNS 89 Standard query 0xca9f A clientservices.googleapis.com
61 18.173891 192.168.1.18 192.168.1.1 DNS 89 Standard query 0x6855 Unknown (65) clientservices.googleapis.com
62 18.285650 192.168.1.1 192.168.1.18 DNS 117 Standard query response 0xf291 AAAA clientservices.googleapis.com
63 18.285650 192.168.1.1 192.168.1.18 DNS 105 Standard query response 0xca9f A clientservices.googleapis.com
64 18.285650 192.168.1.1 192.168.1.18 DNS 146 Standard query response 0x6855 Unknown (65) clientservices.google.com
66 18.320563 192.168.1.18 192.168.1.1 DNS 78 Standard query 0x1be5 AAAA www.googleapis.com
67 18.320835 192.168.1.18 192.168.1.1 DNS 78 Standard query 0x1a2f A www.googleapis.com
68 18.320978 192.168.1.18 192.168.1.1 DNS 78 Standard query 0x56d1 Unknown (65) www.googleapis.com
69 18.327044 192.168.1.18 192.168.1.1 DNS 79 Standard query 0x8832 AAAA accounts.google.com
70 18.327308 192.168.1.18 192.168.1.1 DNS 79 Standard query 0xd97b A accounts.google.com
Frame 59: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{FB45E929-4F9B-4500-91B0-5229BD97E92B}, id 0
Ethernet II, Src: LiteonTe_59:fe:6d (94:08:53:59:fe:6d), Dst: 74:12:b3:e0:40:58 (74:12:b3:e0:40:58)
Internet Protocol Version 4, Src: 192.168.1.18, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 59515, Dst Port: 53
Source Port: 59515
Destination Port: 53
Length: 55
Checksum: 0xfaed [unverified]
[Checksum Status: Unverified]
[Stream index: 11]
[Timestamps]
Domain Name System (query)
0000 74 12 b3 e0 40 58 94 08 53 59 fe 6d 08 00 45 00
0010 00 4b 37 8c 00 00 80 11 7f b2 c0 a8 01 12 c0 a8
0020 01 01 e8 7b 00 35 00 37 fa ed f2 91 01 00 00 01
0030 00 00 00 00 00 00 0e 63 6c 69 65 6e 74 73 65 72
0040 76 69 63 65 73 0a 67 6f 6f 67 6c 65 61 70 69 73
0050 03 63 6f 6d 00 00 1c 00 01
dns.pcapng
Packets: 1115 · Displayed: 1115 (100.0%)
Profile: Default


student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "B21DCAT058" ; date
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware:~/Desktop$
lab-ping.tar
dns.pcapng (on nsm-wireshark-dns)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
61 18.173891 192.168.1.18 192.168.1.1 DNS 89 Standard query 0x6855 Unknown (65) clientservices.googleapis.com
62 18.285650 192.168.1.1 192.168.1.18 DNS 117 Standard query response 0xf291 AAAA clientservices.googleapis.com
63 18.285650 192.168.1.1 192.168.1.18 DNS 105 Standard query response 0xca9f A clientservices.googleapis.com
64 18.285650 192.168.1.1 192.168.1.18 DNS 146 Standard query response 0x6855 Unknown (65) clientservices.google.com
66 18.320563 192.168.1.18 192.168.1.1 DNS 78 Standard query 0x1be5 AAAA www.googleapis.com
67 18.320835 192.168.1.18 192.168.1.1 DNS 78 Standard query 0x1a2f A www.googleapis.com
68 18.320978 192.168.1.18 192.168.1.1 DNS 78 Standard query 0x56d1 Unknown (65) www.googleapis.com
69 18.327044 192.168.1.18 192.168.1.1 DNS 79 Standard query 0x8832 AAAA accounts.google.com
70 18.327308 192.168.1.18 192.168.1.1 DNS 79 Standard query 0xd97b A accounts.google.com
71 18.327468 192.168.1.18 192.168.1.1 DNS 79 Standard query 0x9888 Unknown (65) accounts.google.com
72 18.329466 192.168.1.18 192.168.1.1 DNS 74 Standard query 0x0e0c AAAA www.google.com
73 18.330229 192.168.1.18 192.168.1.1 DNS 74 Standard query 0xd396 A www.google.com
74 18.331268 192.168.1.18 192.168.1.1 DNS 74 Standard query 0x9c7d Unknown (65) www.google.com
Frame 64: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface \Device\NPF_{FB45E929-4F9B-4500-91B0-5229BD97E92B}, id 0
Ethernet II, Src: 74:12:b3:e0:40:58 (74:12:b3:e0:40:58), Dst: LiteonTe_59:fe:6d (94:08:53:59:fe:6d)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.18
User Datagram Protocol, Src Port: 53, Dst Port: 50471
Source Port: 53
Destination Port: 50471
Length: 112
Checksum: 0x80c4 [unverified]
[Checksum Status: Unverified]
[Stream index: 13]
[Timestamps]
Domain Name System (response)
0000 94 08 53 59 fe 6d 74 12 b3 e0 40 58 08 00 45 00
0010 00 84 00 00 40 00 40 11 b7 05 c0 a8 01 01 c0 a8
0020 01 12 00 35 c5 27 00 70 80 c4 68 55 81 80 00 01
0030 00 00 00 01 00 00 0e 63 6c 69 65 6e 74 73 65 72
0040 76 69 63 65 73 0a 67 6f 6f 67 6c 65 61 70 69 73
0050 03 63 6f 6d 00 00 41 00 01 c0 1b 00 06 00 01 00
0060 00 00 23 00 2d 03 6e 73 31 06 67 6f 6f 67 6c 65
0070 c0 26 09 64 6e 73 2d 61 64 6d 69 6e c0 3f 2a 31
0080 00 55 00 00 03 84 00 00 03 84 00 00 07 08 00 00
0090 00 3c

**Task 2: To what IP address is the DNS query message sent?**

➔ **DNS query message sent to IP address:192.168.1.1**

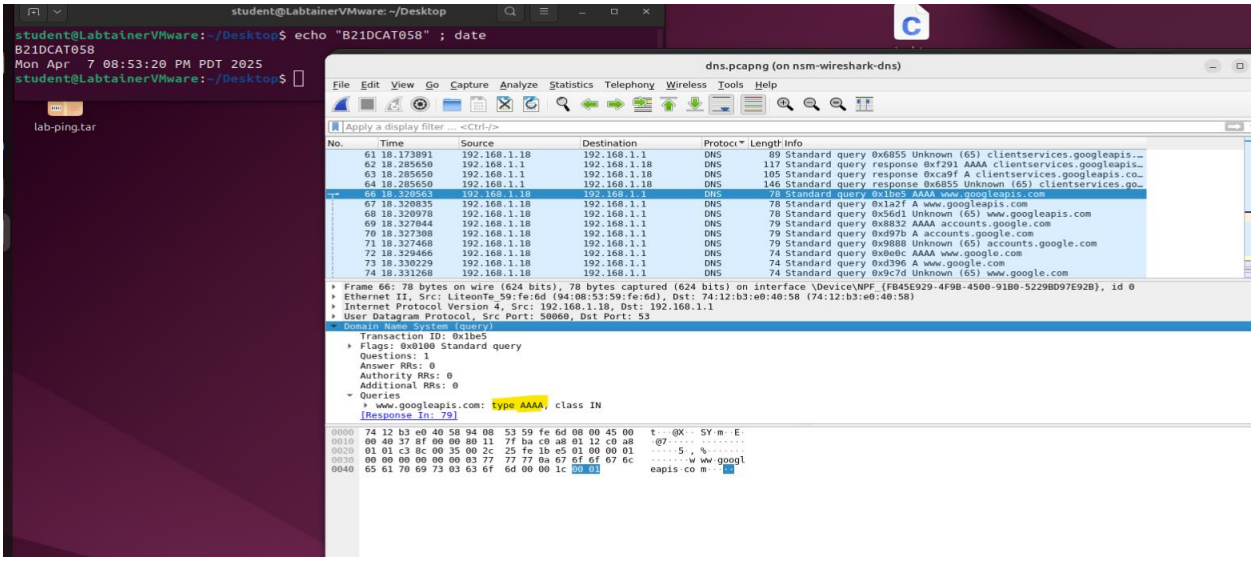
Trong gói Standard query, kiểm tra trường **Destination IP** (IP của DNS server)




**Task 3: Examine the DNS query message. What "Type" of DNS query is it?**

➔ **Type of DNS:AAAA**

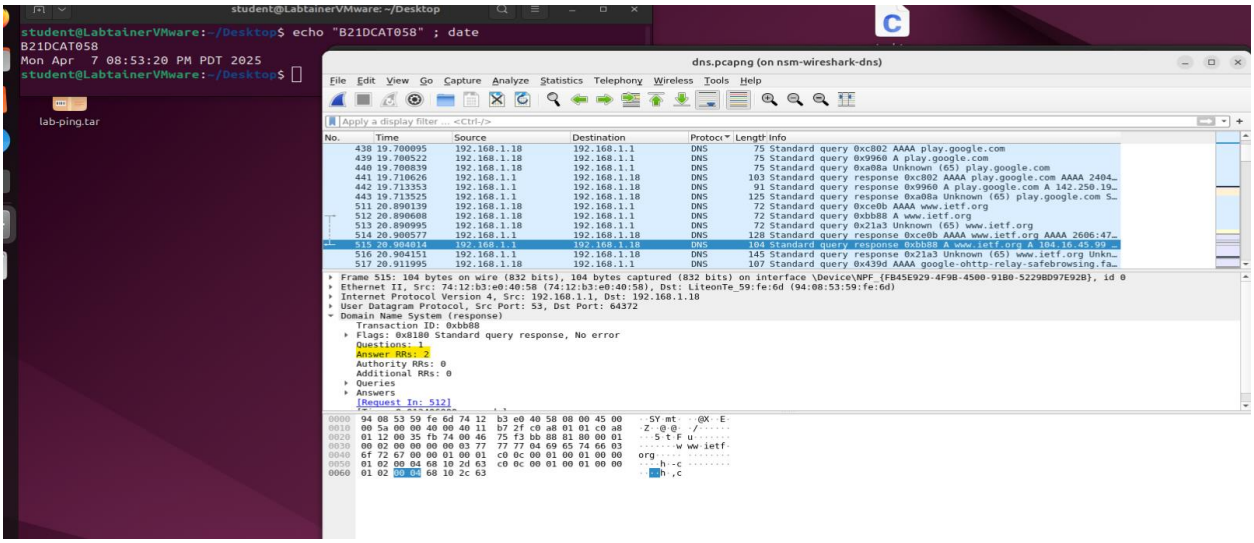
Trong phần **Domain Name System (query)**, xem trường **Type**



**Task 4: Examine the DNS response message. How many "answers" are provided?**

➔ **Number answer:2**

Tiến hành xem trong gói **Standard query response**




**Kết thúc bài lab:**

CheckWork: