

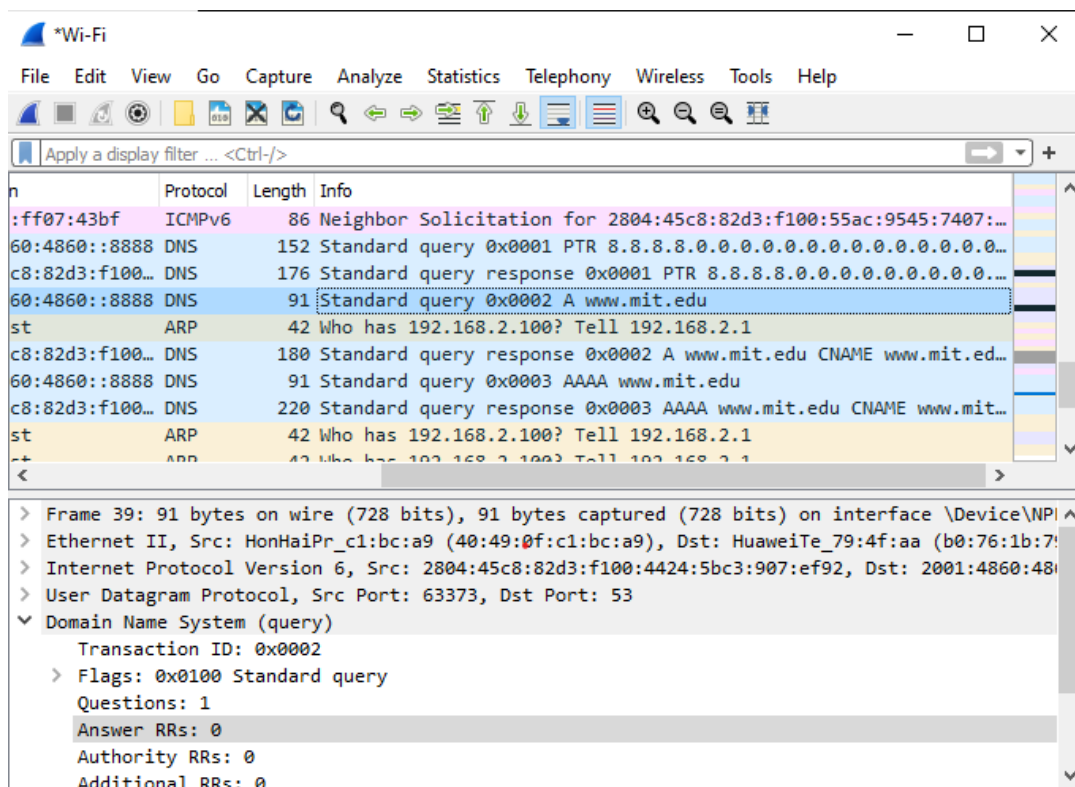
UNIVERSIDADE FEDERAL DE OURO PRETO
CIÊNCIA DA COMPUTAÇÃO

ROBSON NOVATO LOBÃO - 20.1.4018

WIRESHARK 3 - DNS

Ouro Preto
2022

1. O endereço IP é 45.76.189.25 e o web server utilizado foi o site da Asian Institute of Technology
2. O endereço utilizado foi do site da Cambridge University.
cam.ac.uk nameserver = dns0.eng.cam.ac.uk
cam.ac.uk nameserver = ns2.ic.ac.uk
cam.ac.uk nameserver = dns0.cl.cam.ac.uk
cam.ac.uk nameserver = ns3.mythic-beasts.com
cam.ac.uk nameserver = auth0.dns.cam.ac.uk
cam.ac.uk nameserver = ns1.mythic-beasts.com
3. O endereço IP encontrado foi: 98.137.11.163
4. UDP
5. Destination: 56866, Source: 443.
6. 192.168.2.112, Sim o mandado e o meu acusado no ipconfig são os mesmos.
7. Ele é "Type A", Não foi encontrada nenhuma resposta, o Type A funciona como um endereço padrão para gravar DNS's.
8. No meu caso apenas uma resposta é provida contendo o endereço IP do site que foi pedido para ser acessado.
9. Sim, 4.31.198.44 que é o endereço provido pelo servidor DNS do site utilizado para o enunciado do exercício.
10. Não, tudo é carregado uma vez só na chamada da query principal.
11. Source port: 78326. Dest port: 45
12. 192.168.2.112, sim
13. Type A e não há respostas na query
14. 3 respostas, duas com CNAME e outra com o endereço do host.
- 15.



16. 2001:4860:4860::8888, sim é o mesmo

17. Type A, Não
18. Uma resposta nomeada como Standard query response, e não provê os outros endereços IP
- 19.

The image shows a Windows command prompt window on the left and a Wireshark network traffic analysis window on the right.

Command Prompt Window:

```
C:\Users\rnlob>nslookup www.mit.edu
Servidor: dns.google
Address: 2001:4860:4860::8888

Não é resposta autoritativa:
Nome: e9566.dscb.akamaiedge.net
Addresses: 2600:1419:b400:1ad::255e
           2600:1419:b400:188::255e
           104.112.146.103
Aliases:   www.mit.edu
           www.mit.edu.edgekey.net

C:\Users\rnlob>nslookup -type=NS mit.edu
Servidor: dns.google
Address: 2001:4860:4860::8888

Não é resposta autoritativa:
mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use2.akam.net

C:\Users\rnlob>
```

Wireshark Window:

The Wireshark window shows a packet capture of network traffic. The packet list on the left shows several DNS packets. The packet details pane on the right shows the structure of a DNS packet (Standard query response) for the domain `mit.edu`. The packet is of type `NS` (Name Server) and class `IN`. The details pane shows the following information:

- Length: 33
- Checksum: 0xa644 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 6]
- [Timestamps]
- UDP payload (25 bytes)
- Domain Name System (query)
 - Transaction ID: 0x0002
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - mit.edu: type NS, class IN
 - Name: mit.edu
 - [Name Length: 7]
 - [Label Count: 2]
 - Type: NS (authoritative Name Server) (2)
 - Class: IN (0x0001)

The packet list shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
52	7.856110	fe80::1	ff02::1:ff07:43bf	ICMPv6	86	Neighbor So
53	8.011328	2804:45c8:82d3:f100::	2001:4860:4860::8888	DNS	152	Standard qu
54	8.026595	2001:4860:4860::8888	2804:45c8:82d3:f100::	DNS	176	Standard qu
55	8.028832	2804:45c8:82d3:f100::	2001:4860:4860::8888	DNS	87	Standard qu
56	8.065486	2001:4860:4860::8888	2804:45c8:82d3:f100::	DNS	254	Standard qu
57	8.555434	HuaweiTe_79:4f:aa	Broadcast	ARP	42	who has 192
58	8.855718	fe80::1	ff02::1:ff07:43bf	ICMPv6	86	Neighbor So
59	10.861980	fe80::1	ff02::1:ff07:43bf	ICMPv6	86	Neighbor So
60	11.240464	2800:3f0:4004:811::	2804:45c8:82d3:f100::	UDP	100	443 + 57575

20. 192.168.2.112, sim
21. Type A, sem respostas.
22. Só uma resposta, com a query response novamente do request enviado pela primeira query.

23.

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

n	Protocol	Length	Info
c8:82d3:f100...	DNS	167	Standard query response 0xb9fb No such name A bitsy.mit.ed SO...
60:4860::8888	DNS	94	Standard query 0x0002 A www.aiit.or.kr
:ff07:43bf	ICMPv6	86	Neighbor Solicitation for 2804:45c8:82d3:f100:55ac:9545:7407:...
st	ARP	42	Who has 192.168.2.100? Tell 192.168.2.1
c8:82d3:f100...	DNS	110	Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
60:4860::8888	DNS	94	Standard query 0x0003 AAAA www.aiit.or.kr
:ff07:43bf	ICMPv6	86	Neighbor Solicitation for 2804:45c8:82d3:f100:55ac:9545:7407:...
c8:82d3:f100...	DNS	148	Standard query response 0x0003 AAAA www.aiit.or.kr SOA ns9.dn...
st	ARP	42	Who has 192.168.2.100? Tell 192.168.2.1

> Frame 18: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF...
 > Ethernet II, Src: HonHaiPr_c1:bc:a9 (40:49:0f:c1:bc:a9), Dst: HuaweiTe_79:4f:aa (b0:76:1b:7f:4f:aa)
 > Internet Protocol Version 6, Src: 2804:45c8:82d3:f100:4424:5bc3:907:ef92, Dst: 2001:4860:4860:4860:0000:0000:0000:0000
 > User Datagram Protocol, Src Port: 64958, Dst Port: 53
 > Source Port: 64958
 > Destination Port: 53
 > Length: 40
 > Checksum: 0x0ca0 [unverified]
 > [Checksum Status: Unverified]
 > [Stream index: 6]
 > [Timestamps]
 > UDP payload (32 bytes)
 > Domain Name System (query)
 > Transaction ID: 0x0002
 > Flags: 0x0100 Standard query
 > Questions: 1
 > Answer RRs: 0
 > Authority RRs: 0
 > Additional RRs: 0
 > Queries
 > www.aiit.or.kr: type A, class IN
 > Name: www.aiit.or.kr

Text item (text) | Packets: 30 · Displayed: 30 (100.0%) · Dropped: 0 (0.0%) | Profile: Default