**Brent Berghmans 1334252**

**Wireshark DNS**

**1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?**

nslookup japan.go.jp

Website: japan.go.jp

Address: 202.32.211.142

**2. Run nslookup to determine the authoritative DNS servers for a university in Europe.**

nslookup -type=NS uhasselt.be

nameserver = ns.belnet.be

nameserver = dns.uhasselt.be

**3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?**

nslookup type=NS pop.mail.yahoo.com

primary name server = yf1.yahoo.com

nslookup yf1.yahoo.com

address: 68.142.254.14

**4. Locate the DNS query and response messages. Are then sent over UDP or TCP?**

Dit gebeurt over UDP, de dns pakketten hebben een “User Datagram Protocal” deel, dit duidt op UDP.

**5. What is the destination port for the DNS query message? What is the source port of DNS response message?**

In Wireshark heb ik 2 query messages staan, beiden messages hebben als destination port 53.

En zijn ook 2 respectievelijke reponses die beide source port 53 gebruiken.

**6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?**

Het IP address van de DNS query is 2a02:1800:100::43:1.

In ipconfig /all heb ik 2 DNS servers:

2a02:1800:100::43:1

2a02:1800:100::43:2

Het eerste address is hetzelfde als bij de DNS query.

**7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

Zoals eerder vermeld werden er 2 messages verstuurd, het ene heeft type A, het andere heeft type AAAA.

Beide messages hebben 0 Answer RRs.

**8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?**

Ik heb ook 2 DNS response messages, beide messages hebben 3 Answer RRs.

1 antwoord is een Canonical Name.

De 2 volgende antwoorden zijn beiden IPv6 addressen.

**9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?**

Ja, in de DNS response message stond het ip: 2400:cb00:2048:1::6814:155

Dit is ook de destination van het volgend TCP SYN pakket.

**10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?**

Neen. Ik er gebeuren geen DNS lookups voor de GET request van een image.

**11. What is the destination port for the DNS query message? What is the source port of DNS response message?**

DNS query message destination: Poort 53.

DNS response message source: Poort 53

**12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?**

2a02:1800:100::43:1

Ja dit is 1 van de 2 ip’s van mijn default DNS servers, zoals vermeld in antwoord 6.

**13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

Type: A en 0 Answer RRs.

**14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?**

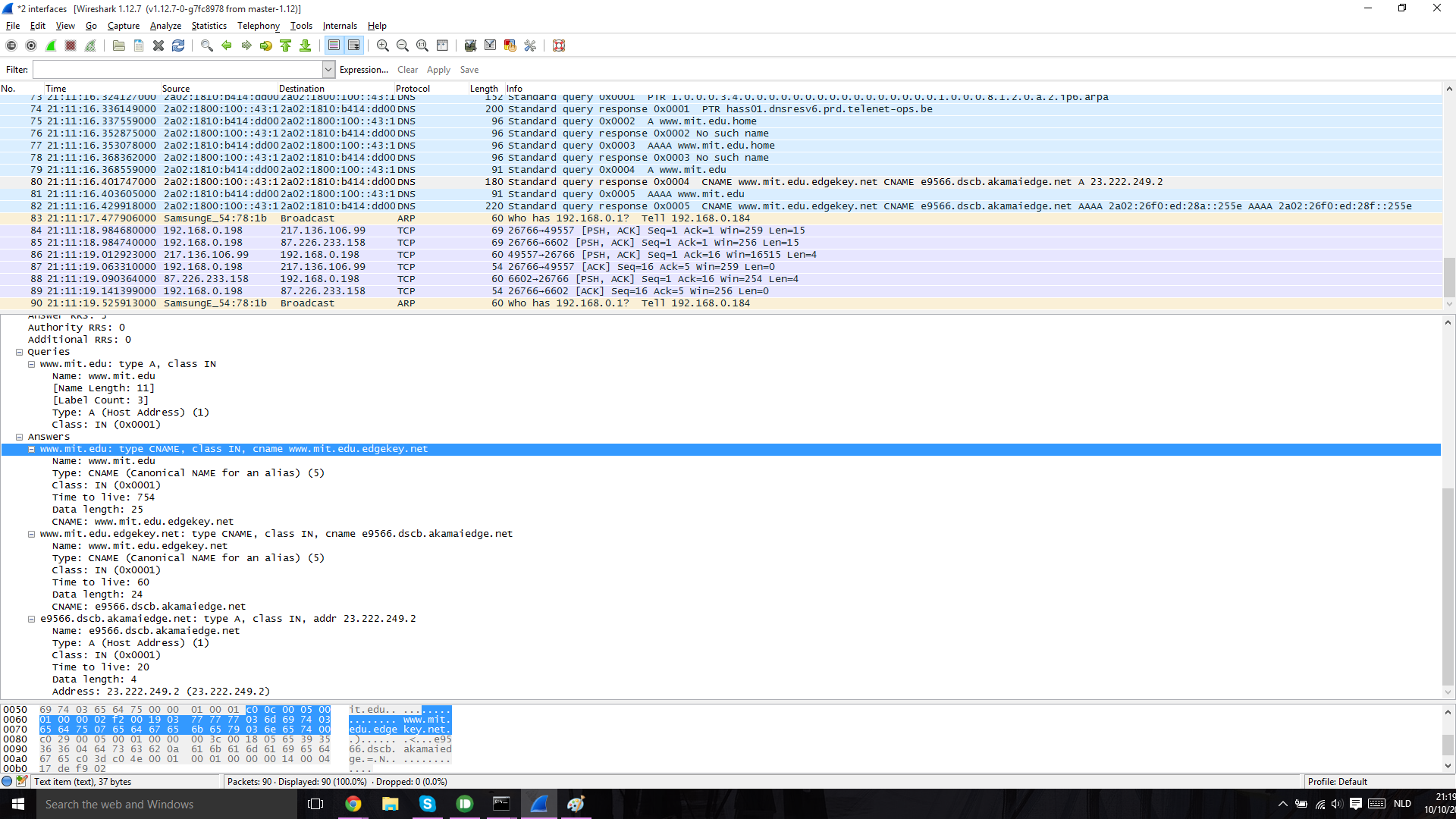
3 Answers RRs

1: De Canonical Name: [www.mit.edu.edgekey.net](http://www.mit.edu.edgekey.net)

2: De Canonical Name voor [www.mit.edu.edgekey.net](http://www.mit.edu.edgekey.net): e9566.dscb.akamaiedge.net

3: Het ip van e9566.dscb.akamaiedge.net: 23.222.249.2

**15. Provide a screenshot.**



**16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?**

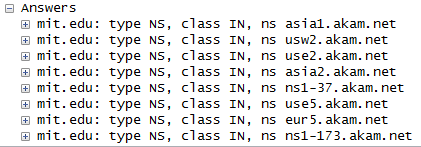
Ja, 2a02:1800:100::43:1, zie antwoord 12.

**17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

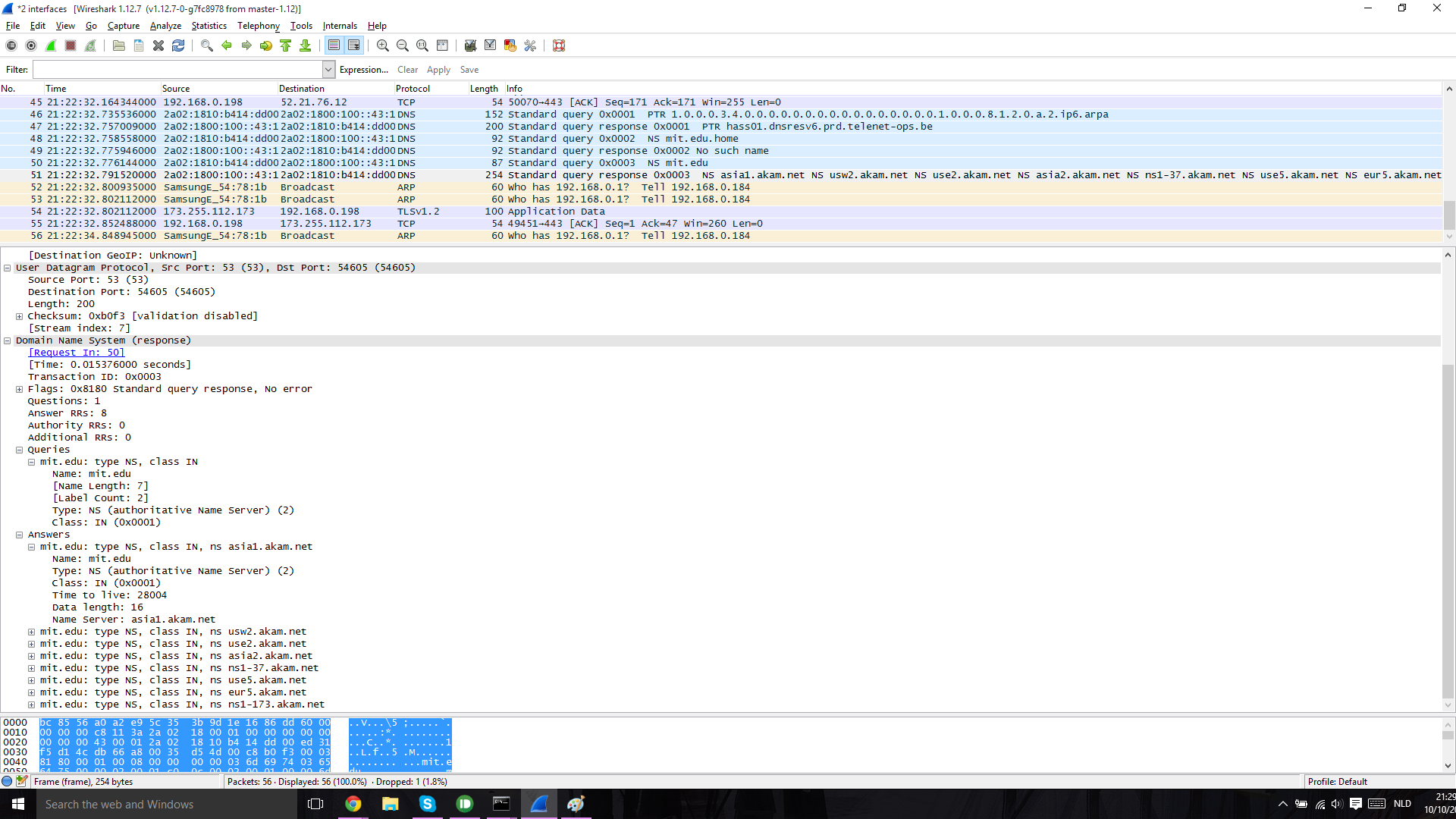
Het type is “NS” en het heeft 0 Answer RRs.

**18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?**

Het geeft de namen van 8 nameservers terug, niet hun ip.



**19. Provide a screenshot.**

****

**20. To wha IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?**

Neen, het wordt verstuurd naar 18.72.0.3.

(Maar ik gebruik de traces van de cursus omdat [www.aiit.or.kr](http://www.aiit.or.kr) offline is.)

**21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

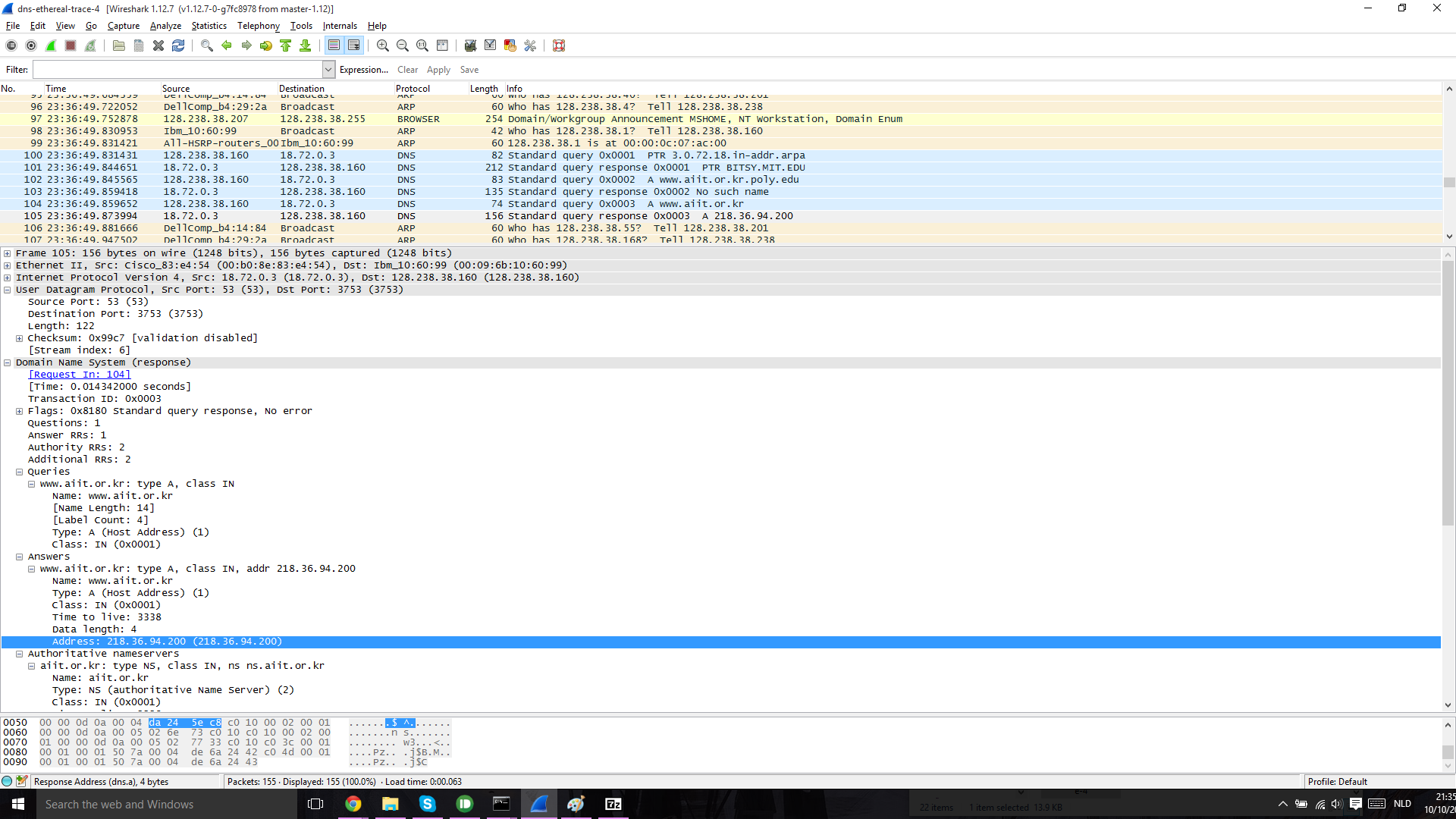
Het is opnieuw type A en heeft 0 answers RRs.

**22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?**

Het heeft 1 answer RRs.

Het bevat het ip van [www.aiit.or.kr](http://www.aiit.or.kr): 218.36.94.200

**23. Provide a screenshot.**

****