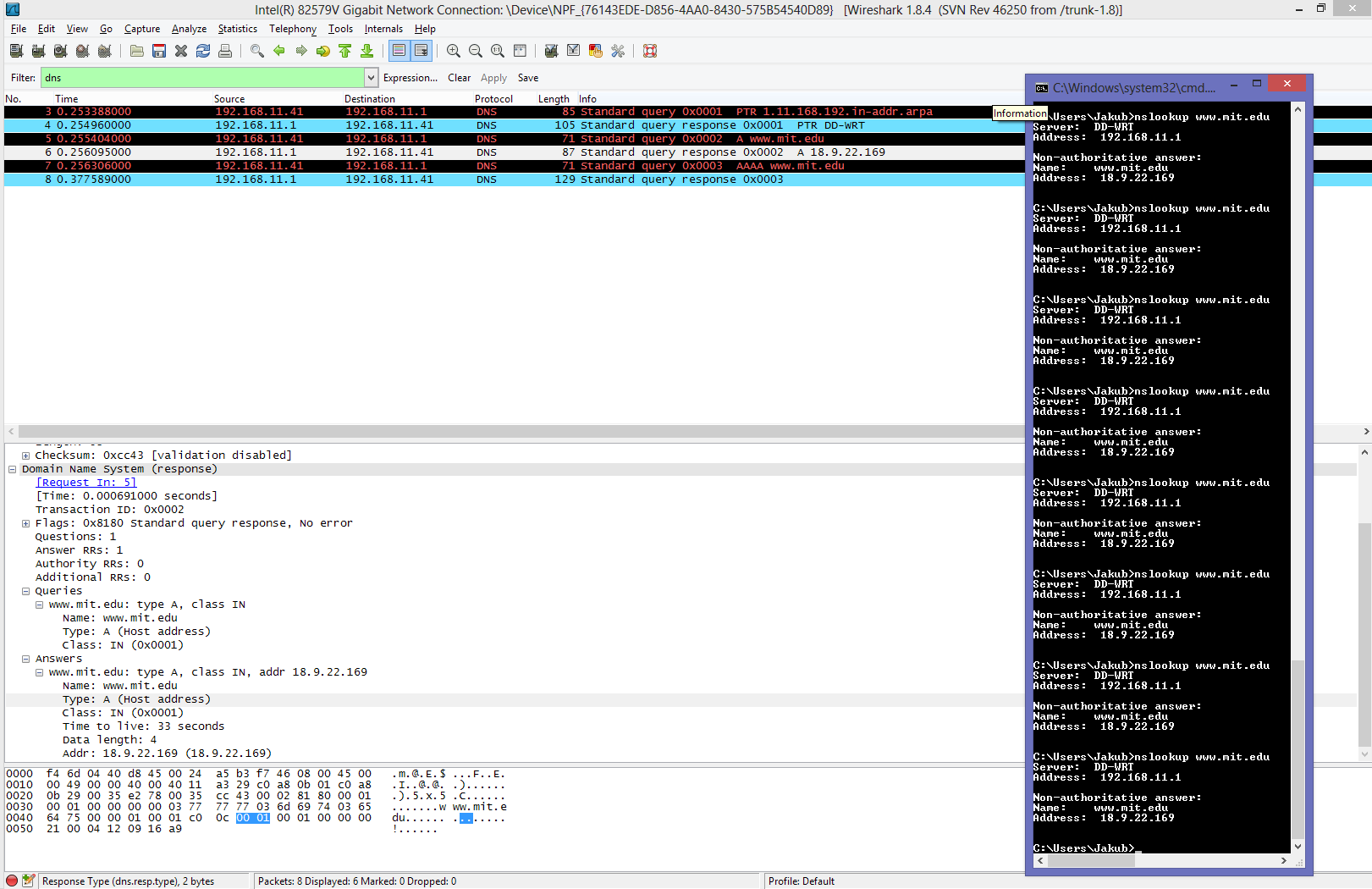
Jakub Szpunar

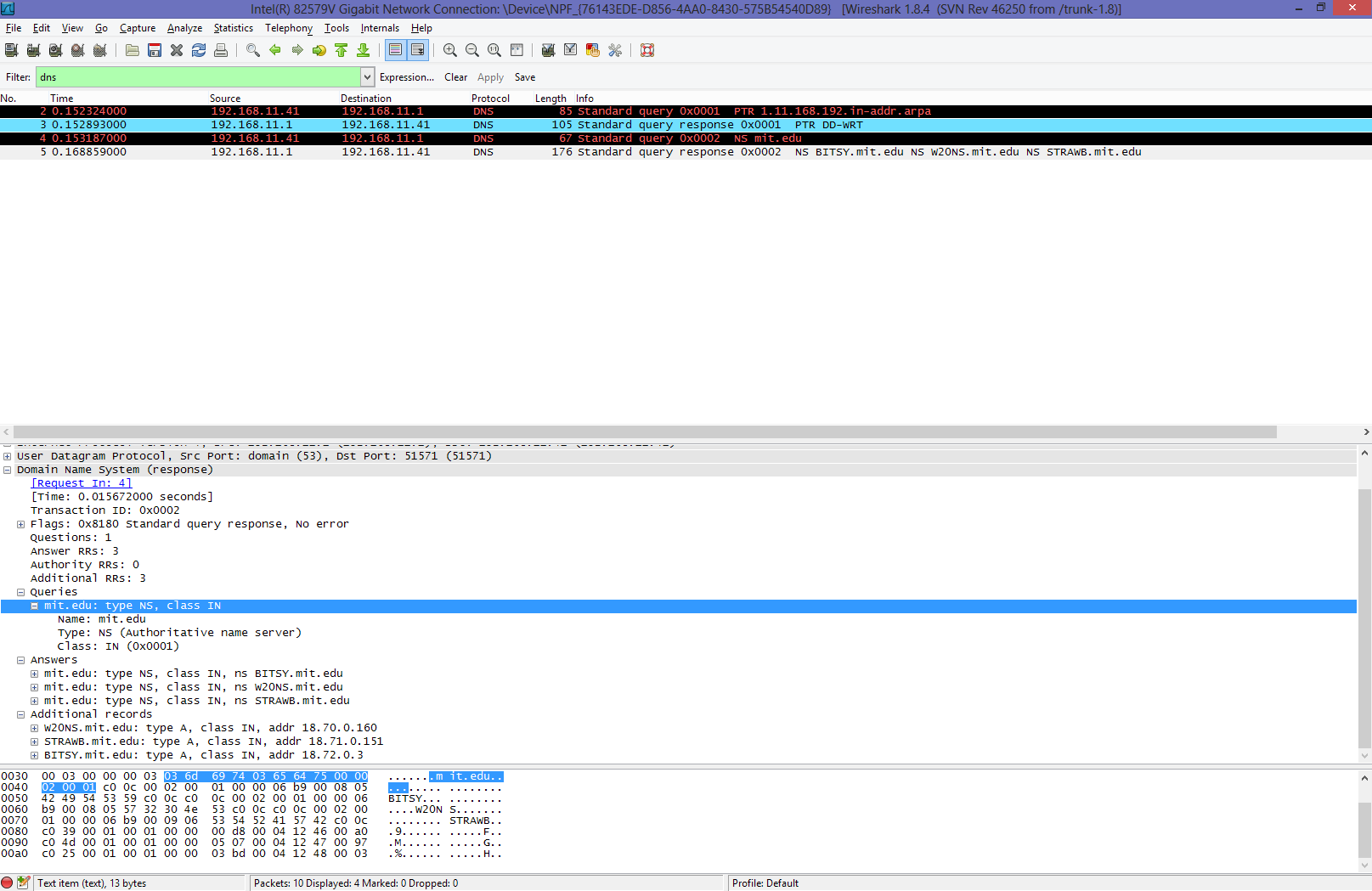
CS4480

WS Lab 3

1. nslookup on [www.asus.com.cn](http://www.asus.com.cn). The site seems to have two ip addresses: 61.244.111.116 or 210.14.136.146
2. Looking up uj.edu.pl, an authoritative DNS server returned is theta.uoks.uj.edu.pl
3. Using the DNS server from #2, a mail server returned for yahoo.com when using –type=mx is 68.142.255.16.
4. Bothe query and responses are sent using UDP.
5. The destination port of the query and the source port of the response are both 53.
6. The DNS query is set to 192.168.11.1. Under ipconfig, the DNS server for my Ethernet connection is also 192.168.11.1. This is interesting as that is the local address of my router. In my routers configuration, it displays additional outside DNS server. It looks like my router can act as a local DNS cache/server. My router runs DD-WRT firmware.
7. The query type is A. The query message has no answer field.
8. There is only one answer sent back in response to the query. The answer is of type A, and it contains the name of the site, the type of query, the class of query, the TTL, the length of data, and the IP address of the site. The ip address is 64.170.98.30
9. Yes, some of the tcp syn packets are directed at 64.170.98.30
10. No further DNS queries are sent to get the images. All of the images appear to reside on the same server, so local DNS caching is likely used.
11. The destination port of the query and the source port of the response are both 53.
12. The DNS server is again, 192.168.11.1, this is my default DNS server.
13. The query is of type A, and has no answers.
14. Only one answer is returned. It is type A. It has the name, class, TTL, data length, and addr. The address is 18.9.22.169.
15. See next page.



1. The query is sent to 192.168.11.1. This is my default DNS.
2. The query type is NS. The query contains no answers.
3. The response contains three nameservers. BITSY.mit.edu, W20NS.mit.edu, and STRAWB.mit.edu. In Additional records, the IP addresses of the servers are sent. 18.72.0.3, 18.70.0.160, and 18.71.0.151.
4. See next page.



1. There are two separate type A DNS queries, for the next four questions, I am going to use the query about aiit.or.kr, and not bitsy.mit.edu. The IP address of the query is sent to 18.72.0.3, which is bitsy.mit.edu as found out in #18. This is not my default DNS server.
2. The DNS query is type A. The query contains no answers.
3. There are two answers provided. One is of type CNAME, and contains the canonical name for aiit.or.kr which is aiit.or.kr. The other answer is of type A and has the address of aiit.or.kr as 27.102.206.87
4. See next page:

