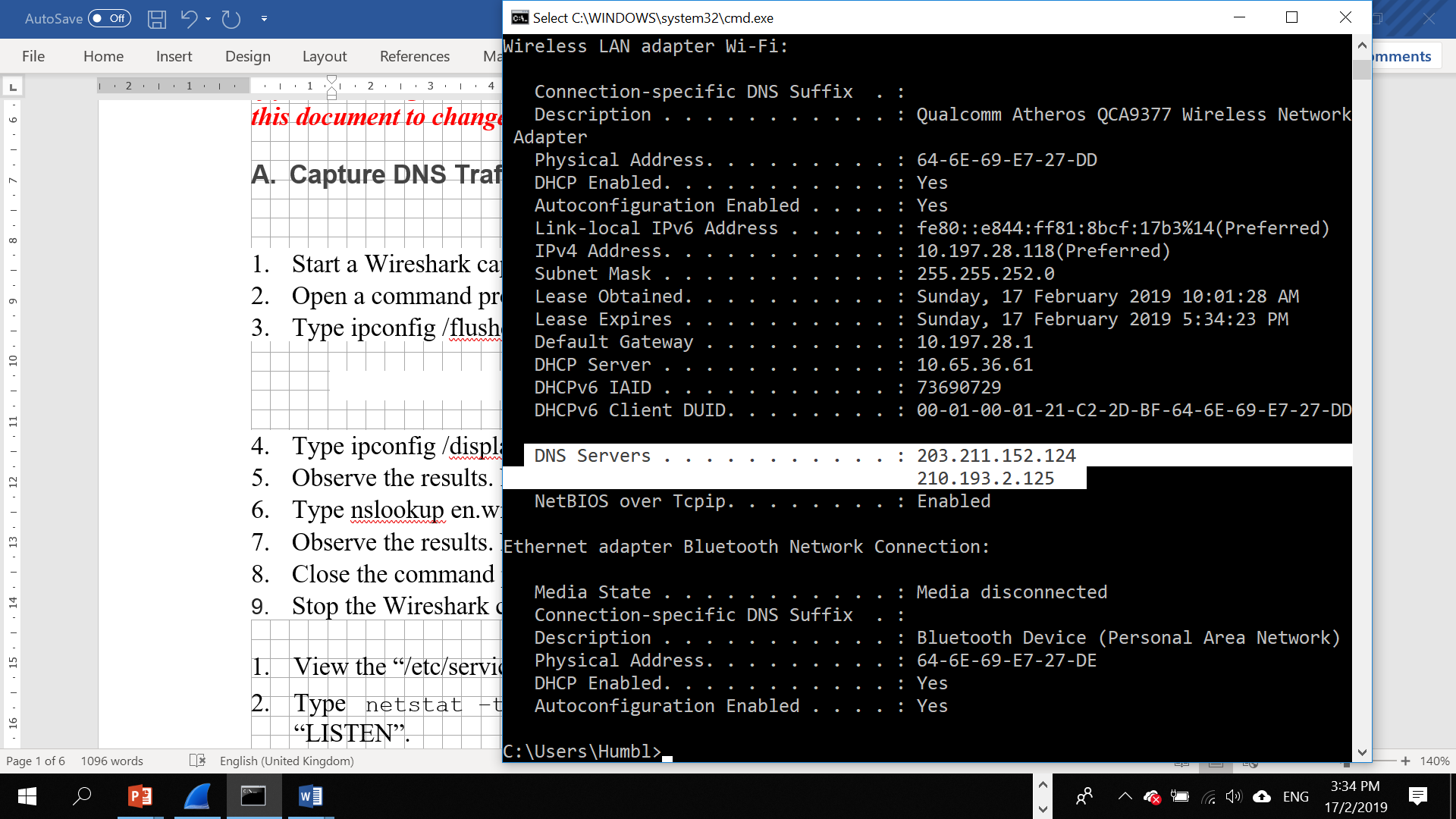
**Practical 07**

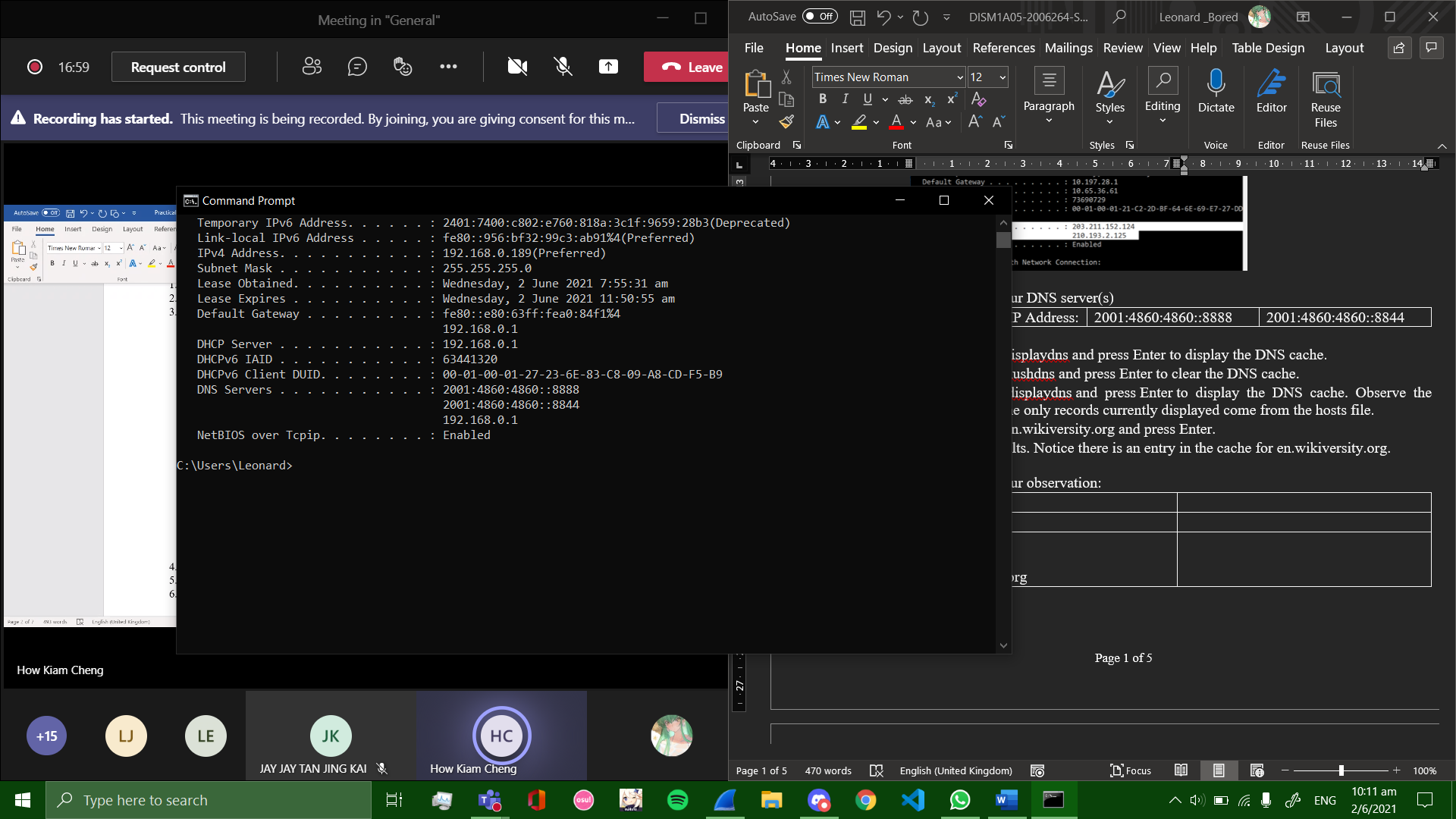
**Capture DNS Traffic**

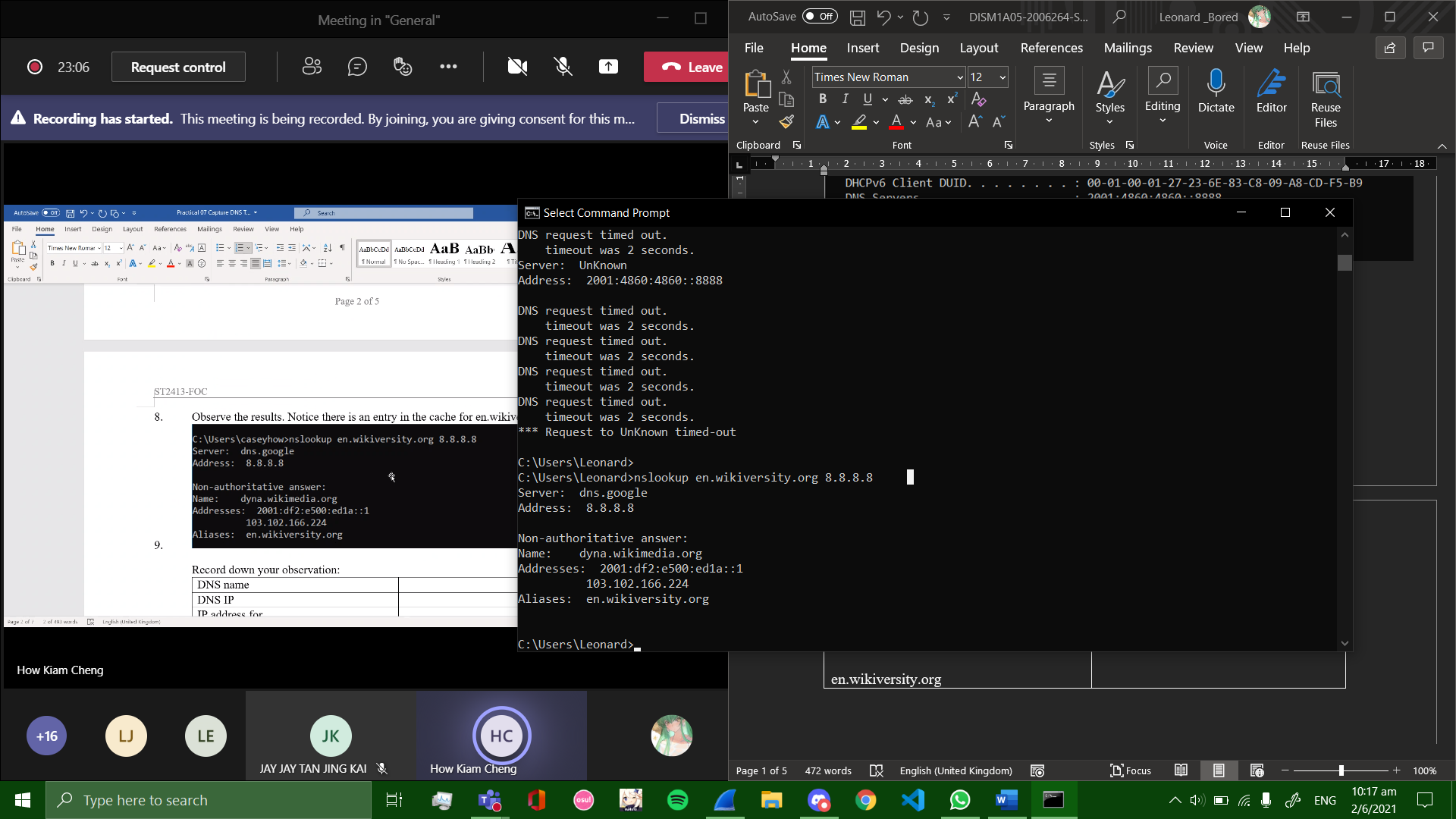
1. Capture DNS Traffic
2. Analyze DNS Request Traffic
3. Analyze DNS Response Traffic
4. **Capture DNS Traffic**
5. [Start a Wireshark capture](https://en.wikiversity.org/wiki/Wireshark/Start).
6. [Open a command prompt](https://en.wikiversity.org/wiki/Command_Prompt/Open).
7. Type ipconfig /all to locate the DNS server(s)



Record down your DNS server(s)

|  |  |  |
| --- | --- | --- |
| DNS server(s) IP Address: | 2001:4860:4860::8888 | 2001:4860:4860::8844 |
|  | 192.168.0.1 |  |

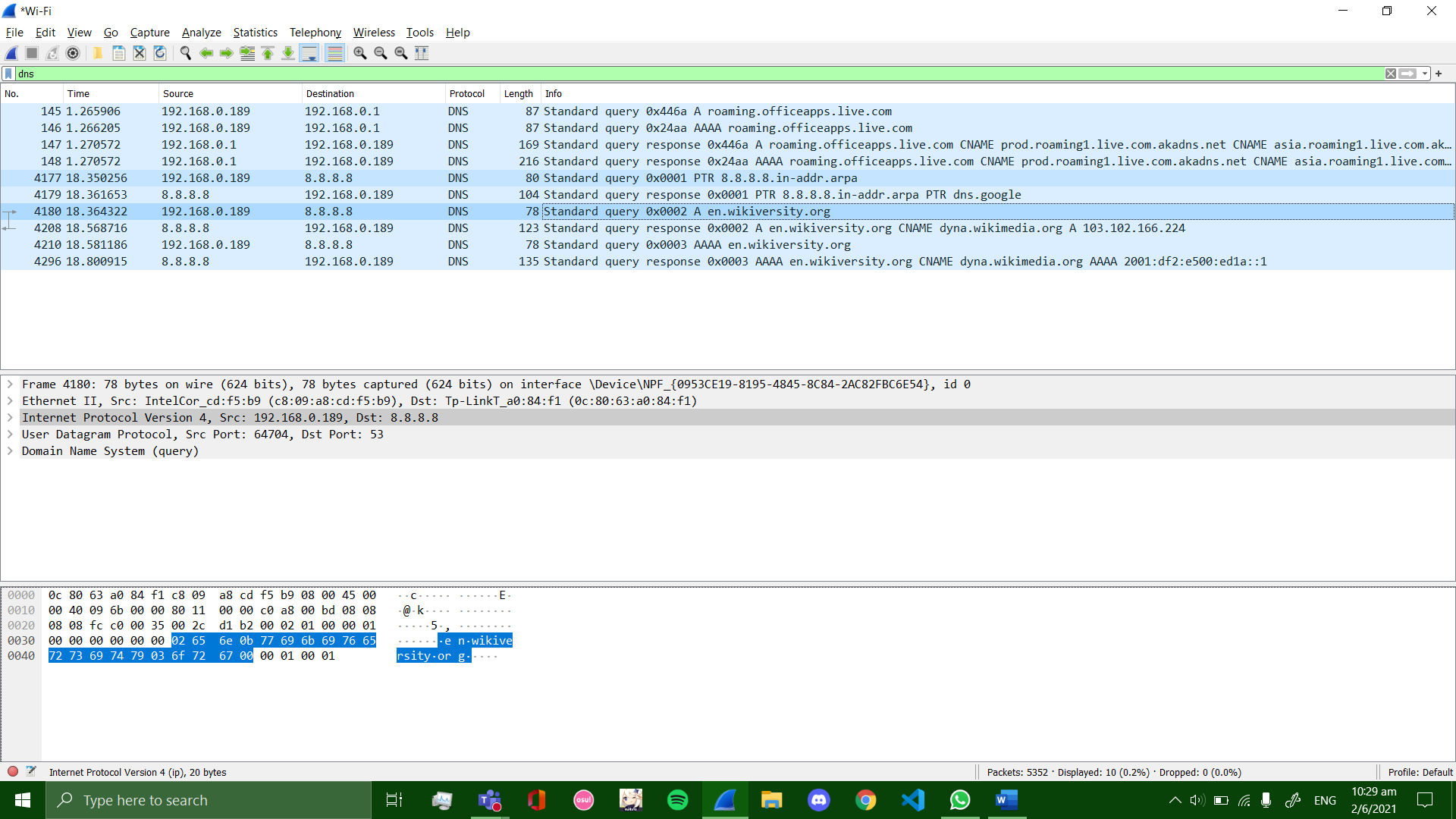


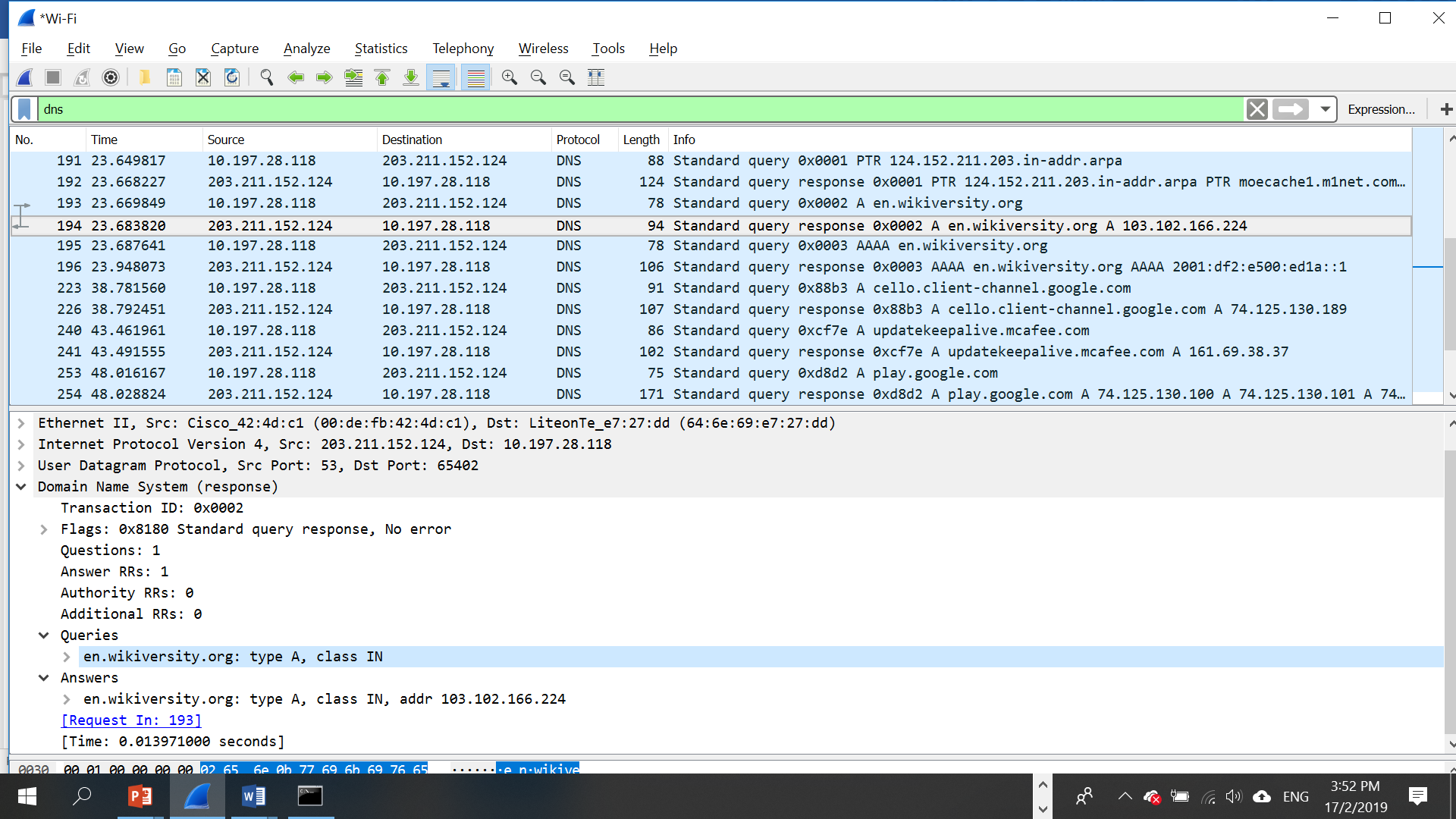
1. Type ipconfig /displaydns and press Enter to display the DNS cache.
2. Type ipconfig /flushdns and press Enter to clear the DNS cache.
3. Type ipconfig /displaydns and press Enter to display the DNS cache. Observe the results. Notice the only records currently displayed come from the [hosts file](https://en.wikiversity.org/wiki/Hosts_file).
4. Type nslookup en.wikiversity.org  8.8.8.8 and press Enter.
5. Observe the results. Notice there is an entry in the cache for en.wikiversity.org.
6. 

Record down your observation:

|  |  |
| --- | --- |
| DNS name | dns.google |
| DNS IP | 8.8.8.8 |
| IP address for  en.wikiversity.org | 103.102.166.224 |

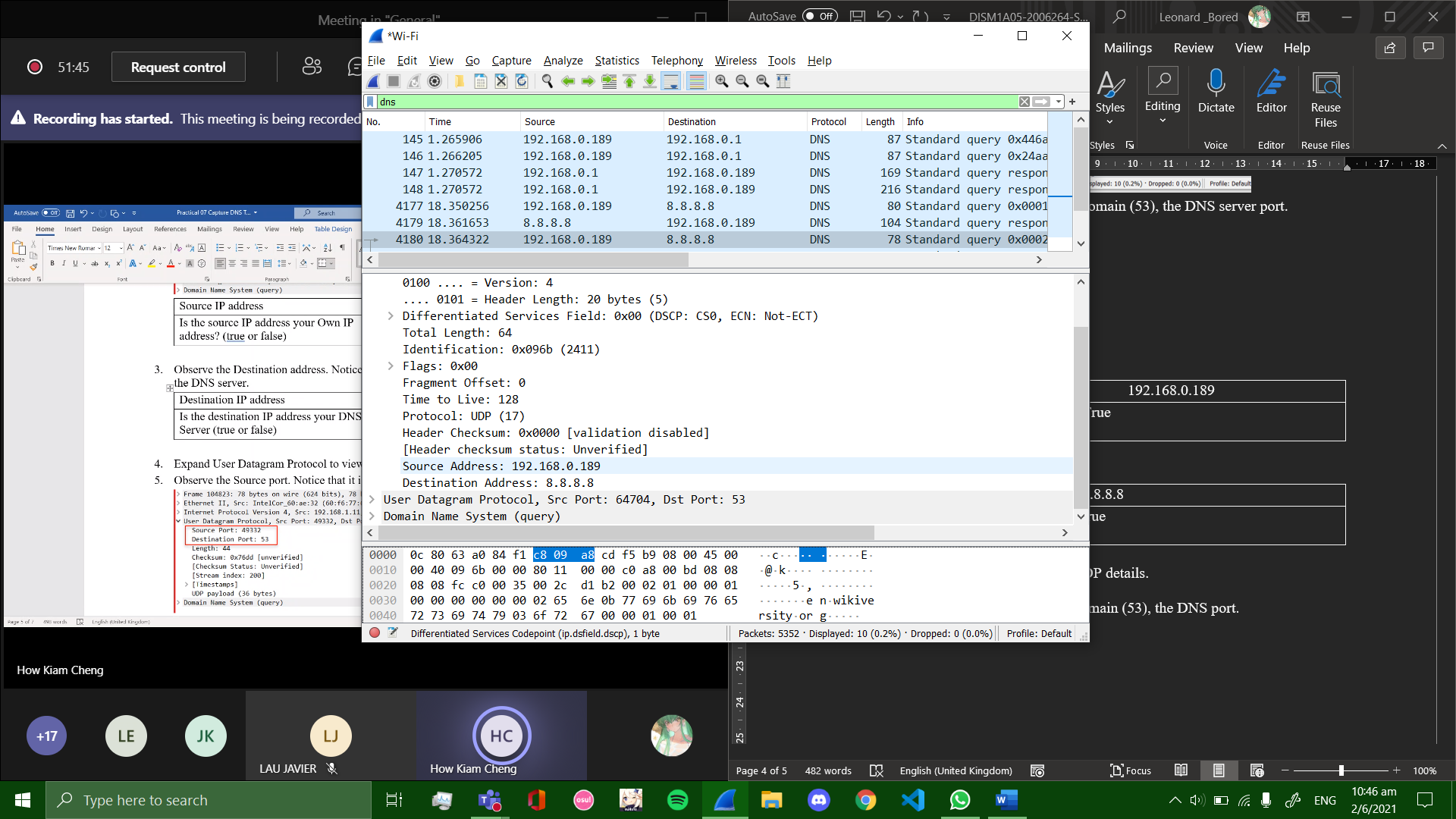
1. Close the command prompt.
2. [Stop the Wireshark capture](https://en.wikiversity.org/wiki/Wireshark/Stop).
3. **Analyze DNS Request Traffic**
4. Observe the traffic captured in the top Wireshark packet list pane. To view only DNS traffic, type udp.port == 53 (lower case) in the Filter box and press Enter.
5. Select the DNS packet labeled Standard query A en.wikiversity.org.
6. Observe the packet details in the middle Wireshark packet details pane. Notice that it is an Ethernet II / Internet Protocol Version 4 / User Datagram Protocol / Domain Name System (query) frame.
7. Observe the DNS request and response





**Record down CNAME and A records in response to the DNS query.**

|  |  |
| --- | --- |
| **CNAME** | **dyna.wikimedia.org** |
| **A Records** | **103.102.166.244** |

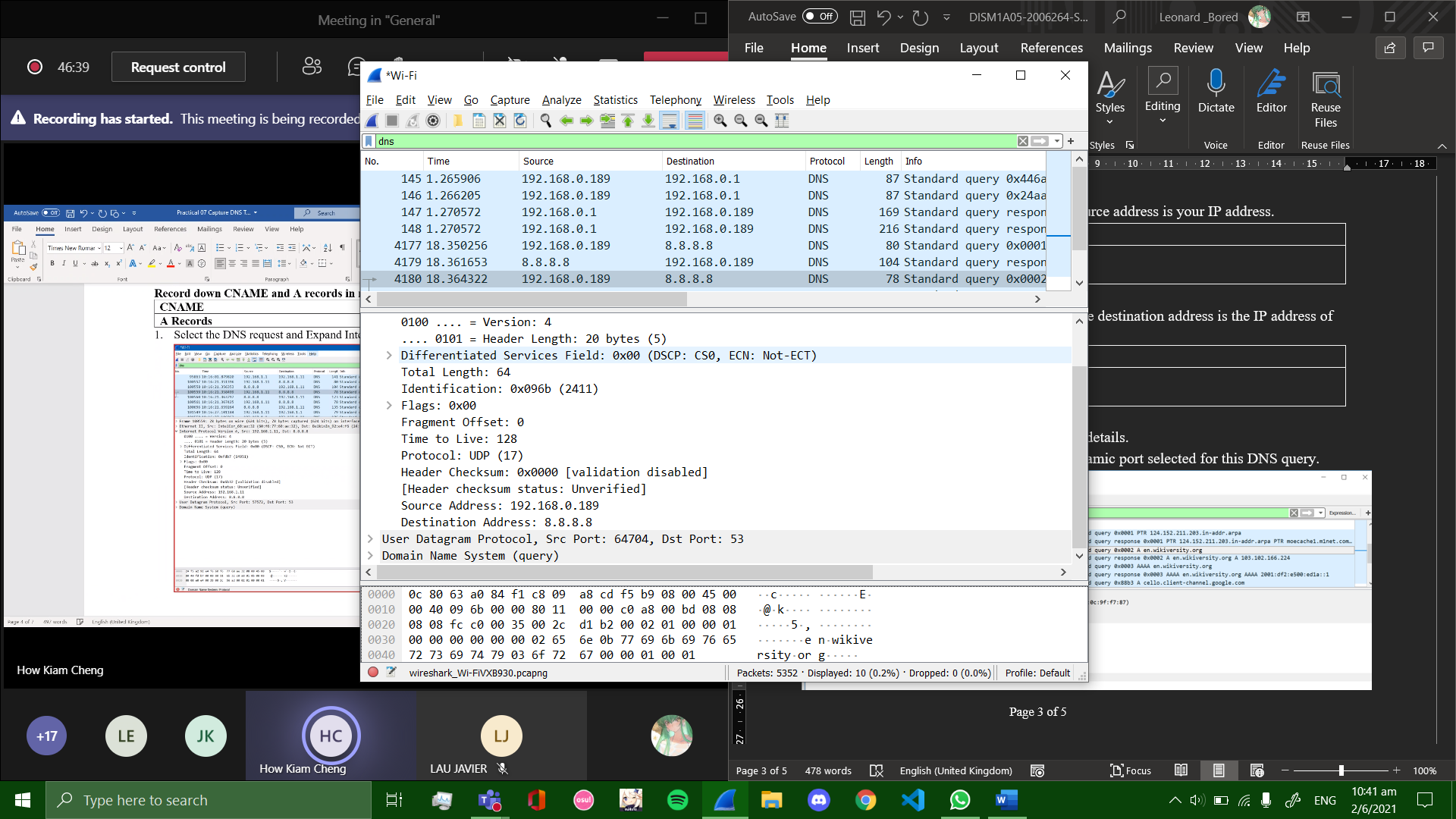
1. Select the DNS request and Expand Internet Protocol Version 4 to view IP details.
2. 
3. Observe the Source address. Notice that the source address is your IP address.

|  |  |
| --- | --- |
| Source IP address | 192.168.0.189 |
| Is the source IP address your Own IP address? (true or false) | true |

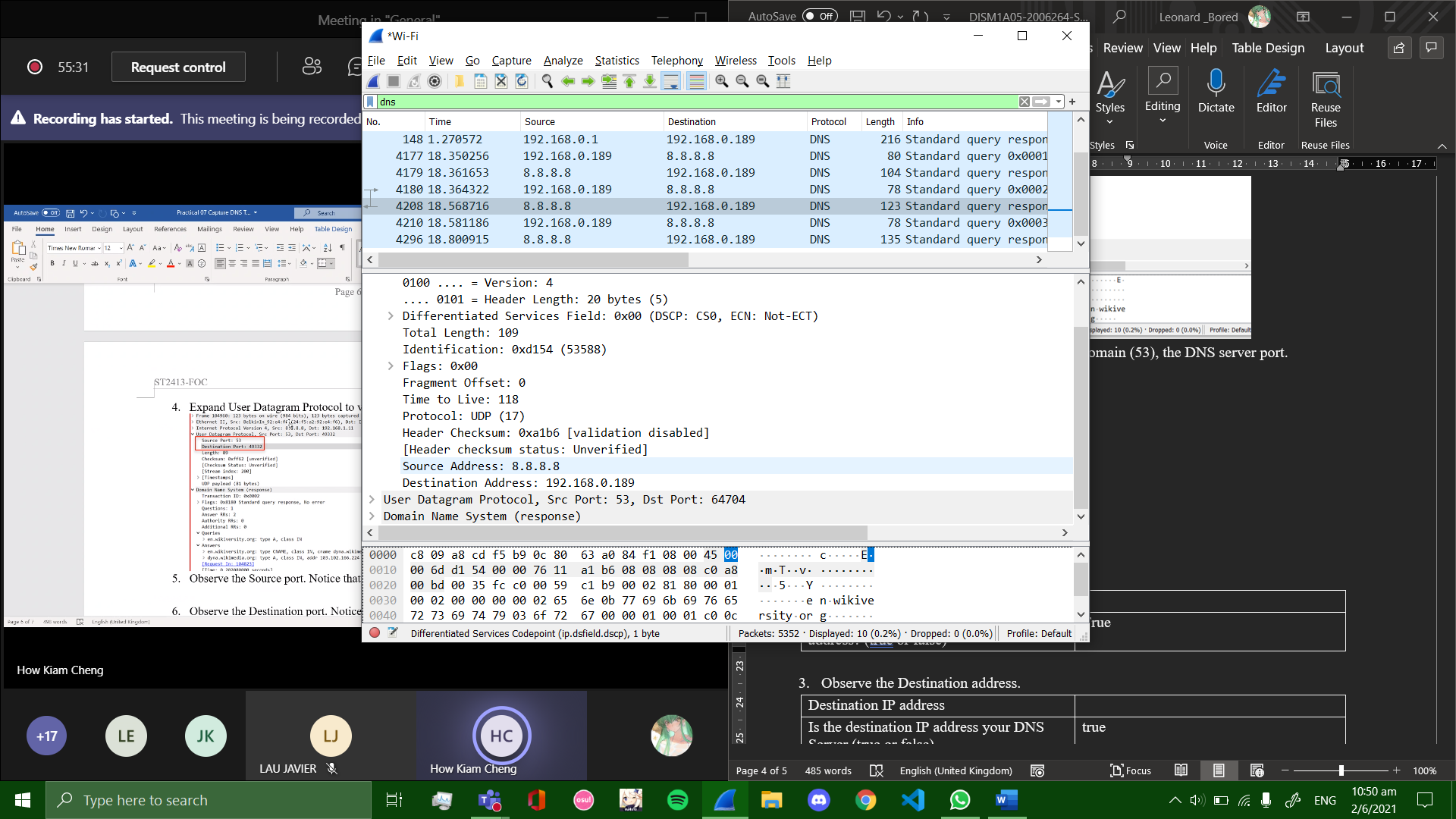
1. Observe the Destination address. Notice that the destination address is the IP address of the DNS server.

|  |  |
| --- | --- |
| Destination IP address | 8.8.8.8 |
| Is the destination IP address your DNS Server (true or false) | true |

1. Expand User Datagram Protocol to view UDP details.
2. Observe the Source port. Notice that it is a dynamic port selected for this DNS query.



1. Observe the Destination port. Notice that it is domain (53), the DNS server port.
2. **Analyze DNS Response Traffic**
3. Select DNS Response Traffic.



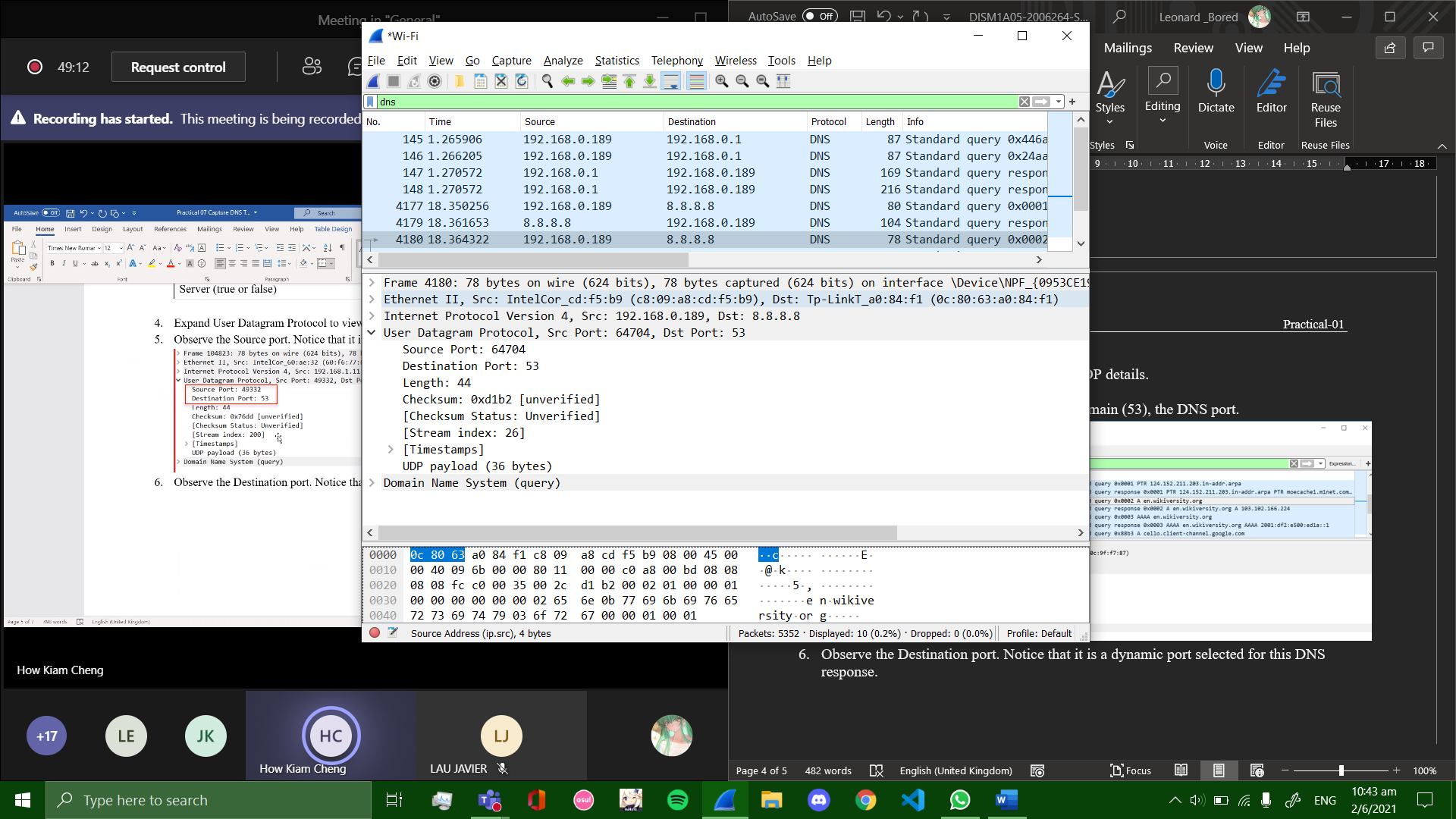
1. Observe the Source address.

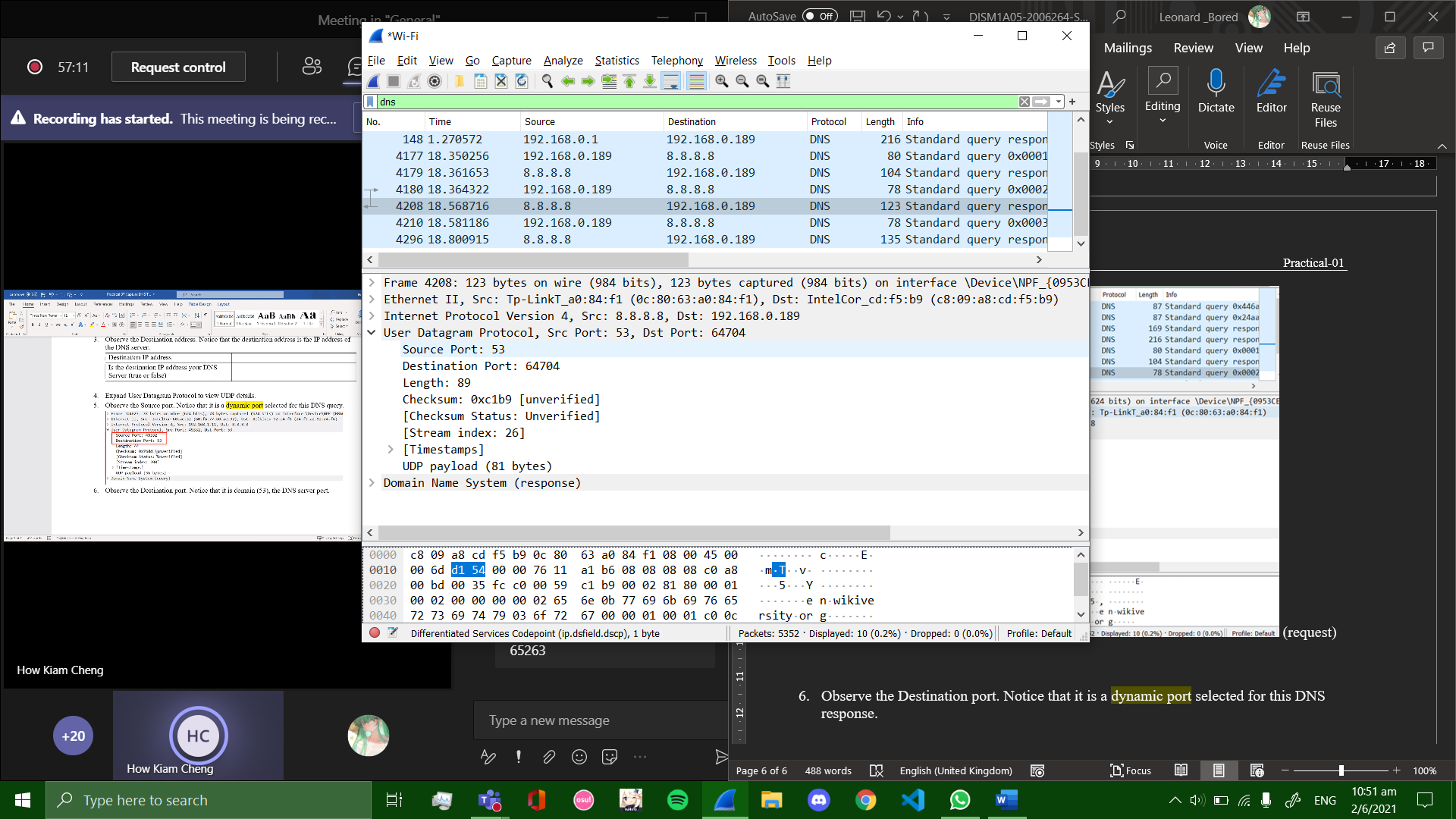
|  |  |
| --- | --- |
| Source IP address | 8.8.8.8 |
| Is the source IP address your Own IP address? (true or false) | True |

1. Observe the Destination address.

|  |  |
| --- | --- |
| Destination IP address | 192.168.0.189 |
| Is the destination IP address your DNS Server (true or false) | true |

1. Expand User Datagram Protocol to view UDP details.
2. Observe the Source port. Notice that it is domain (53), the DNS port.

 (request)

(response)

1. Observe the Destination port. Notice that it is a dynamic port selected for this DNS response.

Both source port and destination port in request is swapped for the response.

1. What have you learnt?

Today, I have learned how computers interact with DNS servers to fetch basic information such as ip addresses of websites in order to process a request from a user to visit a website. When typing the website name into the search bar of any web browser, the computer sends a request to the DNS server in which it will get a reply back confirming the ip address of the website.

1. Difficulties encountered and how you solved the problems?

Overall, I found this activity really manageable as my teacher’s instructions were clear and thorough. I think by paying attention in class and following instructions one step at a time, I was never lost throughout this practical.

*End of Practical*