4. TCP
5. dst 3163 scr: 53
6.

128.238.38.160, the same

7. Type A t's a type A Standard Query and it doesn't contain any answers

8. There were 2 answers containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address.

Answers
www.ietf.org: type A, class IN, addr 209.173.57.180
Name:
www.ietf.org
Type: A (Host address) Class:
IN (0x0001)
Time to live: 30 minutes
Data length: 4
Addr: 209.173.57.180
www.ietf.org: type A, class IN, addr 209.173.53.180
Name:
www.ietf.org
Type: A (Host address) Class:
IN (0x0001)
Time to live: 30 minutes
Data length: 4
Addr: 209.173.53.180

9. Yes
10. No
11. Destination Port: 53 (query message) ; response message source: 53

11. What is the destination port for the DNS query message? What is the source port of DNS response message? The destination port of the DNS query is 53 and the source port of the DNS response is 53.

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? It's sent to 192.168.1.1 which as we can see from the ipconfig –all screenshot, is the default local DNS server.

13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? The query is of type A and it doesn't contain any answers.

14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain? The response DNS message contains one answer containing the name of the host, the type of address, the class, and the IP address.

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? It was sent to 128.238.29.22 which is my default DNS server.

17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? It's a type NS DNS query that doesn't contain any answers.

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 nameservers? The nameservers are bitsy, strawb and w20ns. We can find their IP addresses if we expand the Additional records field in Wireshark as seen below.

Answers
mit.edu: type NS, class inet, ns bitsy.mit.edu
mit.edu: type NS, class inet, ns strawb.mit.edu
mit.edu: type NS, class inet, ns w20ns.mit.edu
Additional records
bitsy.mit.edu: type A, class inet, addr 18.72.0.3
strawb.mit.edu: type A, class inet, addr 18.71.0.151
w20ns.mit.edu: type A, class inet, addr 18.70.0.160

20. To what 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? The query is sent to 18.72.0.3 which corresponds to bitsy.mit.edu.

21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? It's a standard type A query that doesn't contain any answers.

22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain? One answer is provided in the DNS response message. It contains the following:

Answers
www.aiit.or.kr: type A, class inet, addr 222.106.36.102
Name: www.aiit.or.kr
Type: Host address
Class: inet
Time to live: 1 hour
Data length: 4
Addr: 222.106.36.102