Discussion Questions: Case Study on DDoS

1. Please briefly explains what happened in the DDoS attack.

2. Why 100Gbps becomes the magic ceiling in most DDoS attacks?

3. On average Google processes 40,000 searches per second, and the average page size is 300KB. Can you calculate the average Google search traffic per second (in Gbps)? Compare the calculation result with 300Gbps attack.

Hints: 1byte = 8bits; KB is kilo bytes; Gbps is giga bit per second

4. How did the attackers amplify the attacking traffic by misuse open DNS resolvers?

5. How to create a packet with spoofed IP address?

6. How to make a packet with spoofed IP address routable on the Internet?

7. What is anycast, and how is anycast used to defeat DDoS attack (with help of mirror servers and cache servers)?

8. How to use packet filtering and rate limiting to defeat DDoS attack?

9. What is Akamai? How to use Akamai to defeat DDoS attack?

10. The peak of DDoS attack is around 2000 to 2009. You don’t see a lot of DDoS attacks making the headline news nowadays. Why is that?