Computer Security Capstone

Project 1: DNS Reflection and Amplification Attacks

Chi-Yu Li (2022 Spring)
Computer Science Department
National Yang Ming Chiao Tung University

Goals

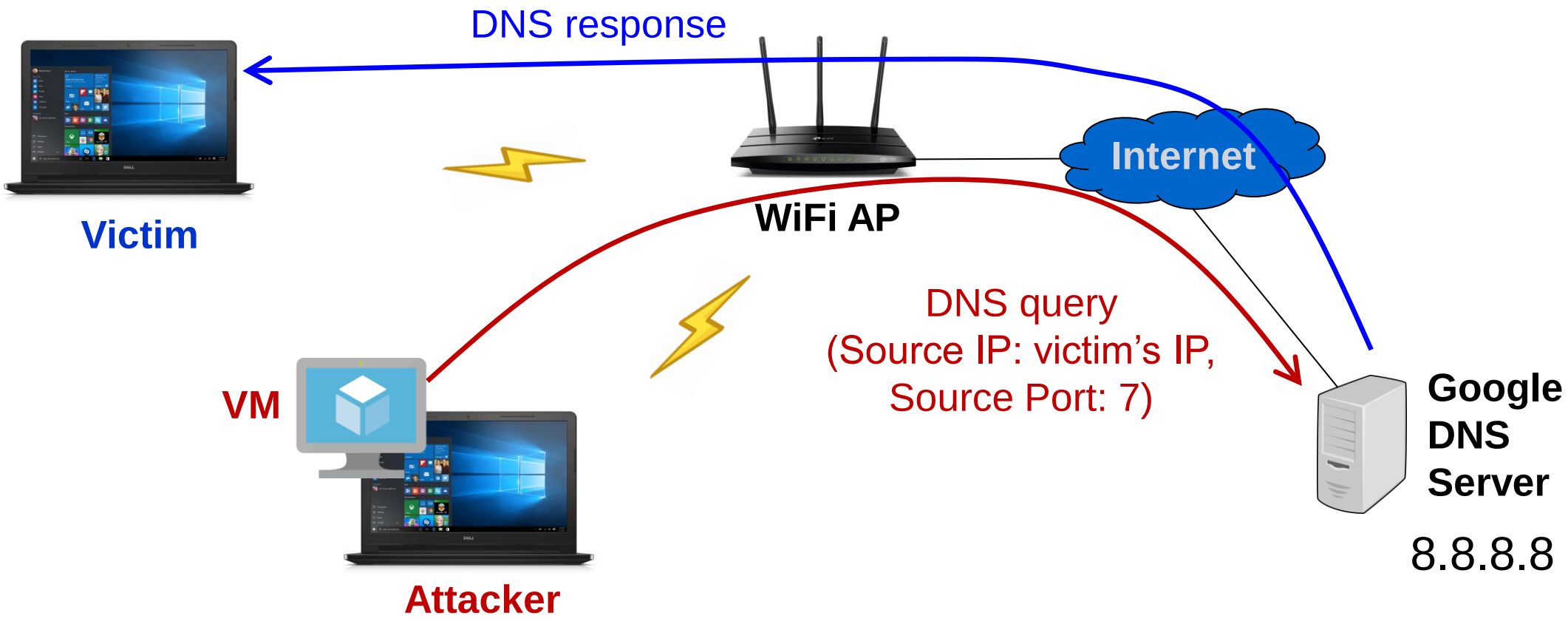
- Understand how to launch DNS reflection and amplification attacks and then defend against them

- You will learn how to
  - program with raw sockets
  - generate IP packets with spoofed IP addresses
  - trace packets using Wireshark
  - fabricate DNS query messages
  - launch DNS reflection and amplification attacks

Requirements

- You need to develop/run your program in a given virtual machine
  - VMware Workstation Player: Please download it from VMware
    - MacOS users can use VirtualBox instead of VMware
  - VM image: Please download it from Link
    - Username/password: cs2022/cs2022
- The language you use must be C/C++
- You are allowed to team up. Each team has at most 2 students
  - Teams: discussions are allowed, but no collaboration
- Please submit your source codes and report to E3

Your DNS Reflection Attack

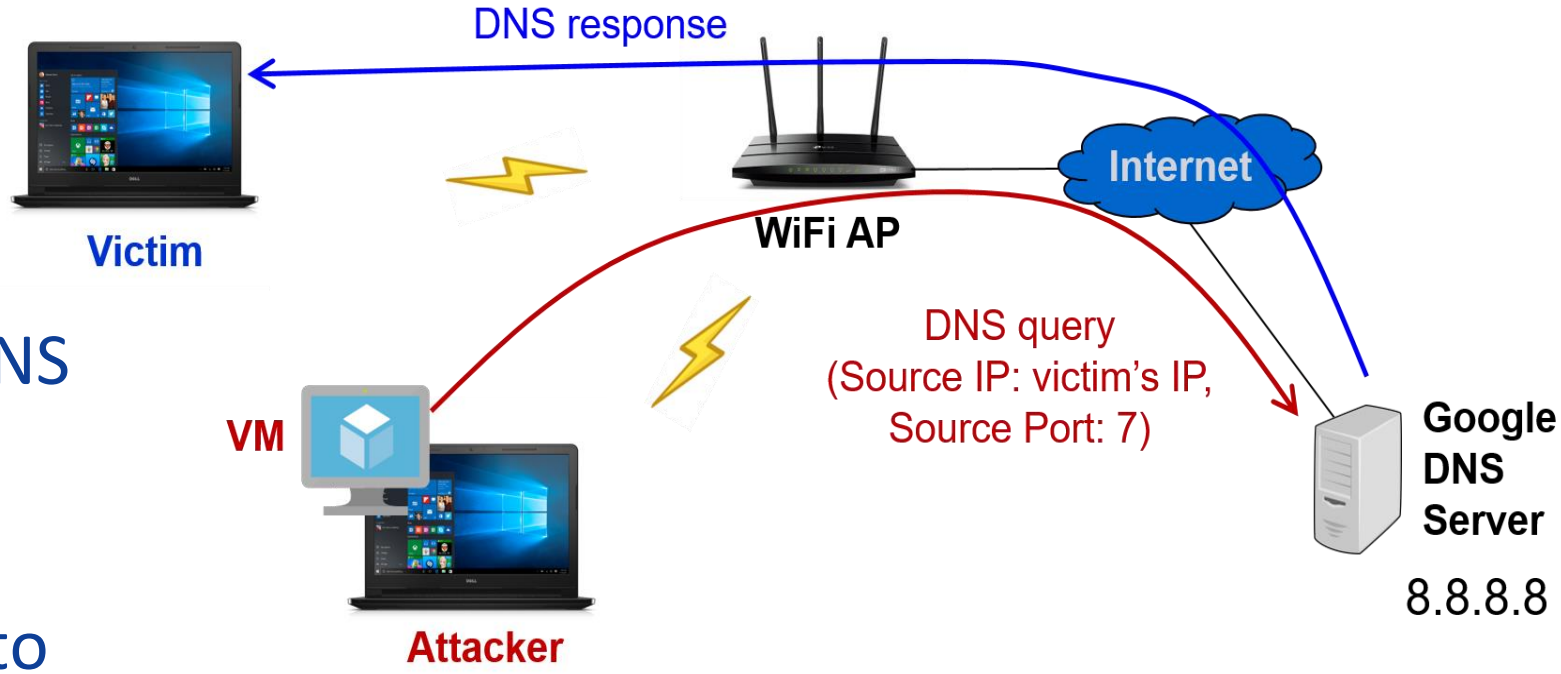


Three Tasks

- Task I: DNS reflection attack (35%)
- Task II: DNS amplification attack (35%)
  - Amplification ratio: $R = S_r / S_q$
    - S_q: the packet size of the DNS query
    - S_r: the packet size of the DNS response
  - $3 \leq R < 6$: **20%**, $6 \leq R < 10$: **25%**, $10 \leq R$: **35%**
- Task III: Report (30%)

Task I: DNS Reflection Attack

(Given a DNS server's IP and the victim's IP)

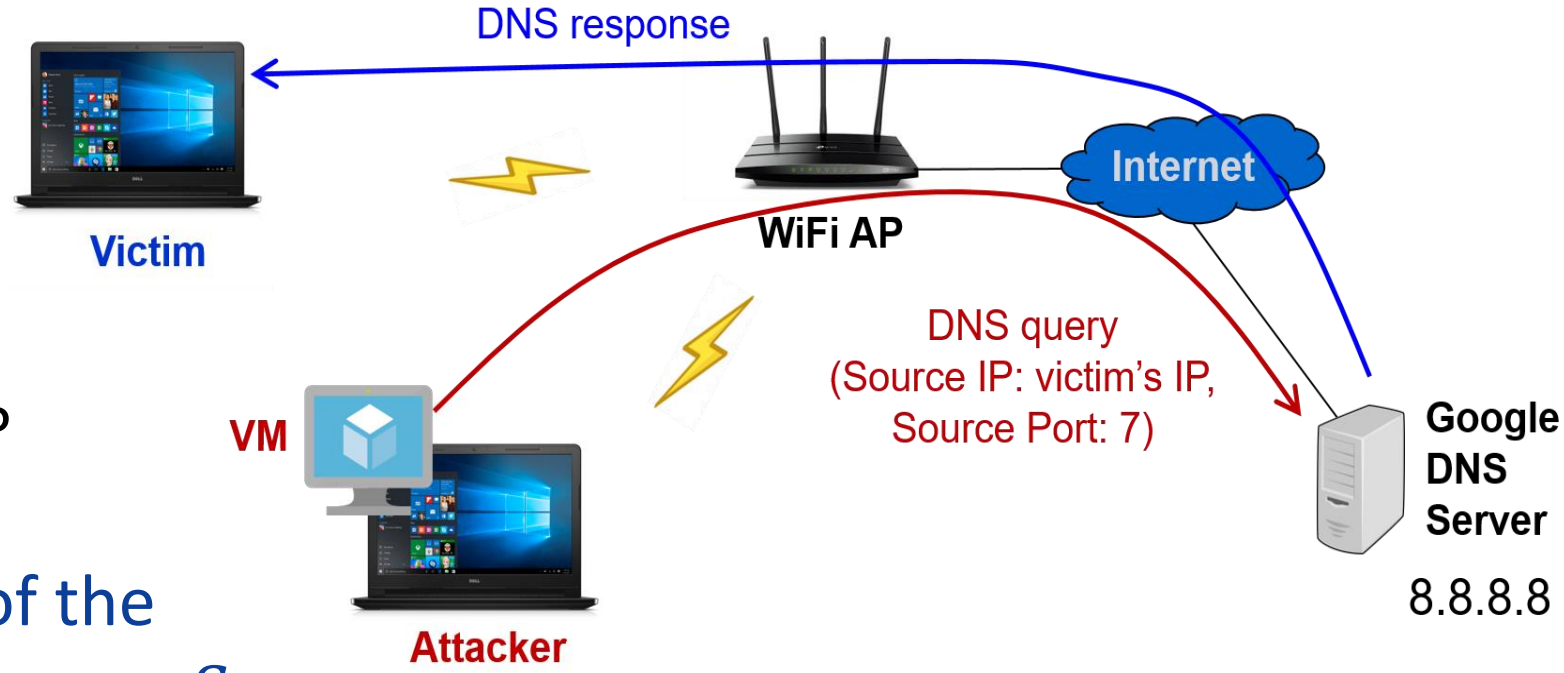


- (Attacker) Fabricate a DNS query message in a UDP packet
- (Victim) Use Wireshark to check whether a corresponding DNS response is received

Task II: DNS Amplification Attack

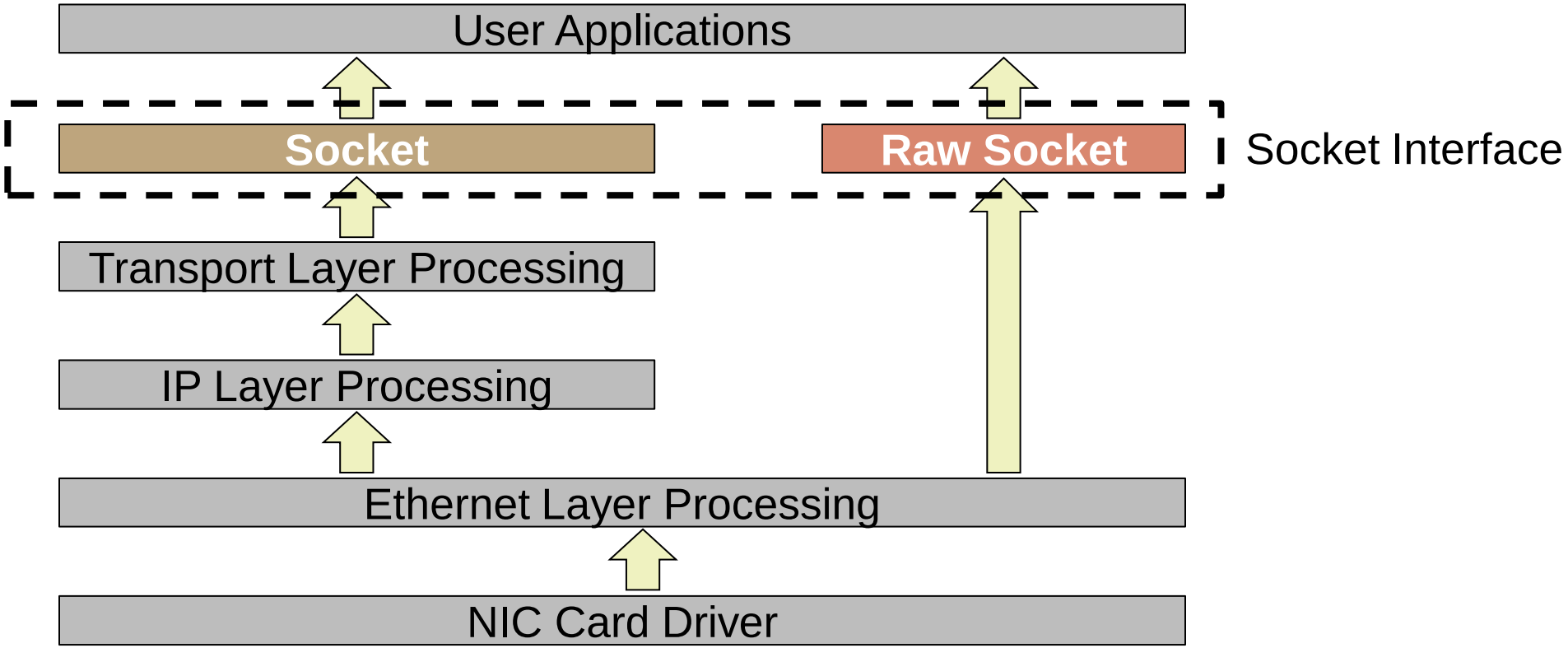
(Given a DNS server's IP and the victim's IP)

- (Attacker) Fabricate a DNS query message that can trigger a large DNS response
  - Check the size of the UDP packet: S_q
- (Victim) Check the size of the corresponding DNS response: S_r
  - Obtain the amplification ratio: $R = S_r/S_q$



Hint I: How to Create IP Spoofing Packets?

- Using Raw Socket
  - Normal network sockets vs. Raw sockets



Hint I: How to Create IP Spoofing Packets? (Cont.)

- Implementation based on raw socket
  - Create a raw socket with the UDP protocol
  - Fabricate the IP header
  - Fabricate the UDP header
  - Calculate the checksum over IP and UDP headers
  - Create DNS query in the UDP payload

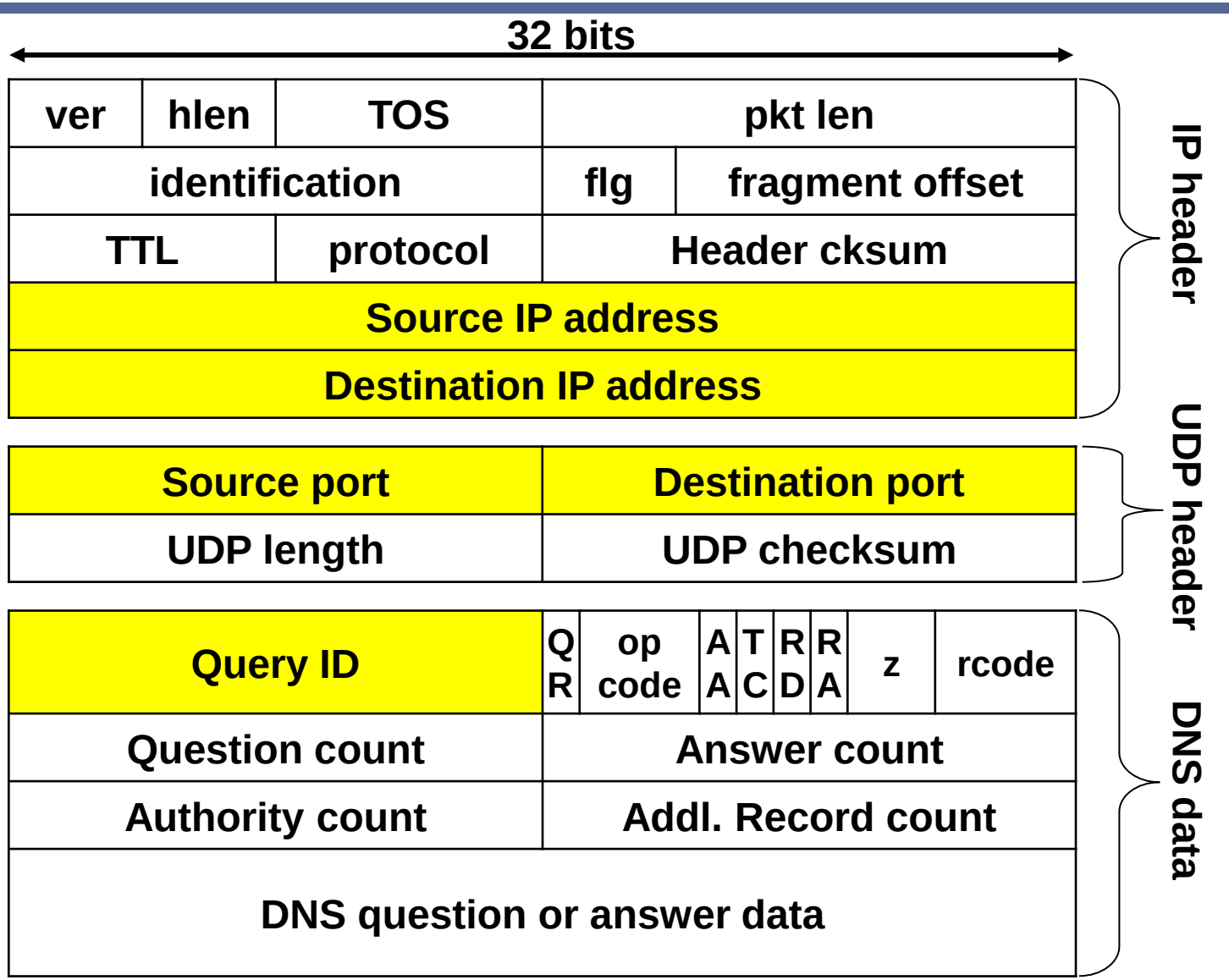
```
sd = socket(PF_INET, SOCK_RAW, IPPROTO_UDP)

struct ipheader *ip = (struct ipheader *) buffer;
ip->iph_ihl = 5;
….
ip->iph_souceip = inet_addr(arhv[1]);
….
struct udpheader *udp = …
udp->udph_srcport = htons(atoi(argv[2]));
….
```

- Reference: Tutorial

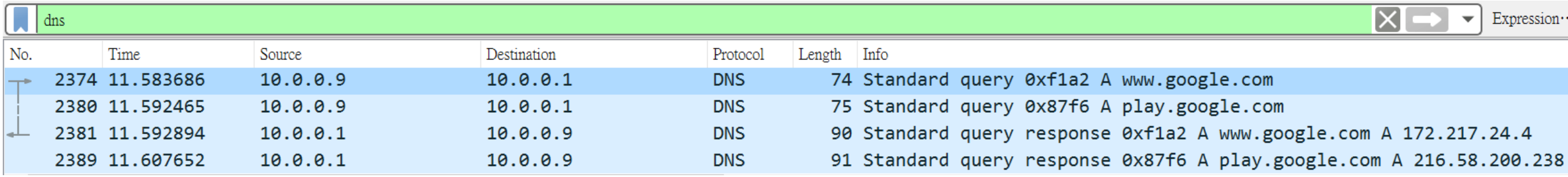
Hint I: How to Create IP Spoofing Packets? (Cont.)

- DNS/UDP/IP packet format



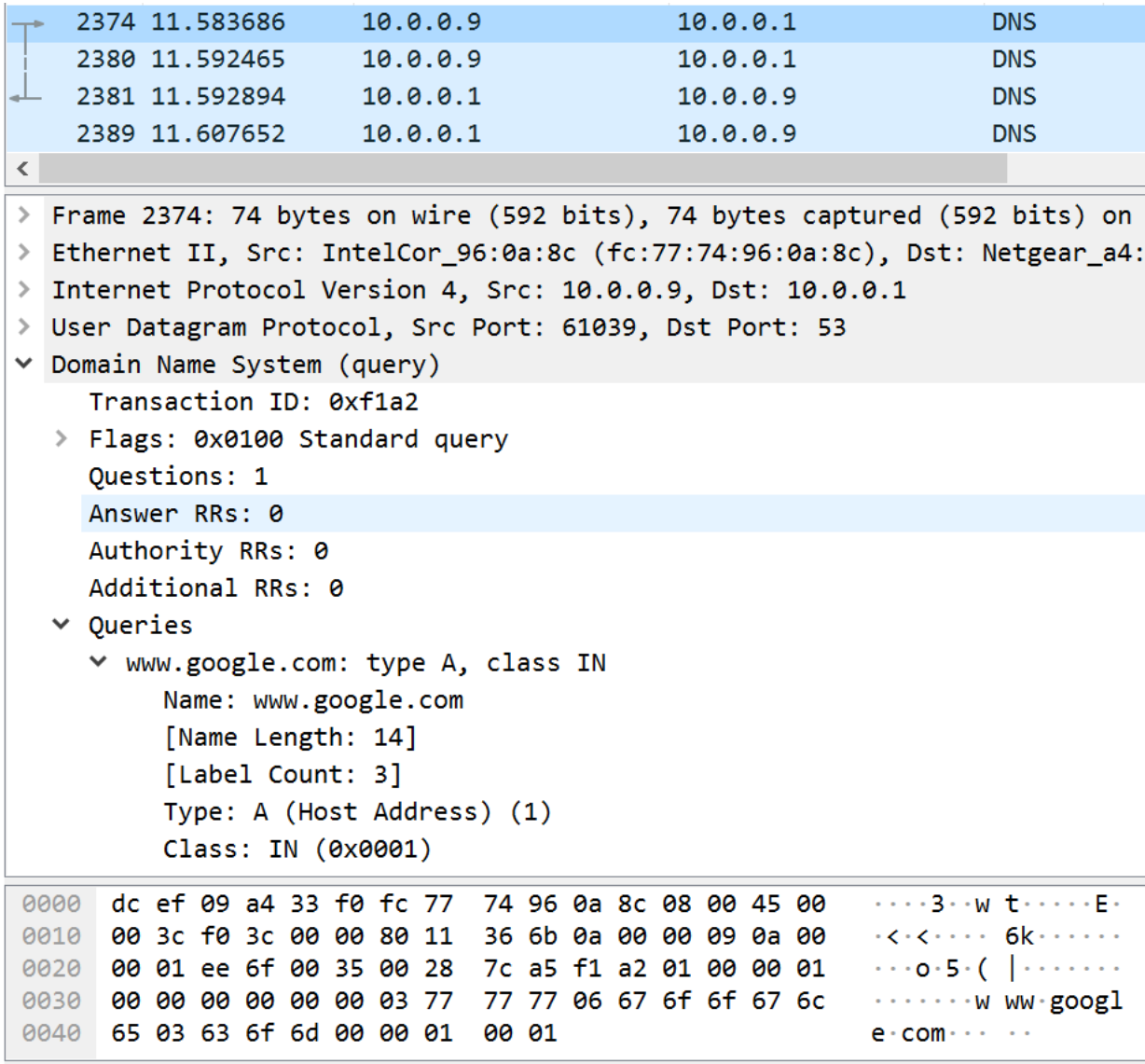
Hint 2: How to Create a DNS Query Message?

- Generate a DNS query (e.g., using ping) and then capture it using Wireshark



Hint 2: How to Create a DNS Query Message? (Cont.)

- Fill in the content of the query based on the observation from Wireshark



Important: How to Prepare Your Attack Program?

- Must provide a **Makefile** which compiles your source codes into one executable file, named **dns_attack** (Missing: -20%)
- Test requirements for the program (Missing: -10% each)
  - Must be run in the given VM without any additional tools or libraries
  - Must work for the test command: ./dns_attack <Victim IP> <UDP Source Port> <DNS Server IP>
    - E.g., ./dns_attack 10.0.0.2 7 8.8.8.8
  - After being executed, the program shall send **3** DNS queries and then terminate
  - Use the last 16 bits of your student ID in the Query ID of the DNS queries
    - Use the ID of only one member in your team
    - E.g., Student ID: 0756842 ➔ Query ID in hex: 0x8C6A

Task III: Report

- Item 1 (10%): please give evidence that you have finished Tasks I and II
  - Illustrate your results based on some snapshots
- Item 2 (10%): please explain how you amplify the DNS response
  - No more than 200 English words
- Item 3 (10%): please propose a solution that can defend against the DoS attack based on the DNS reflection
  - No more than 200 English words

- Note: the report must be written in English with font size 11 or 12 in Times New Roman. It must be submitted in one PDF file with a name “report.pdf.”

Project Submission

- Due date: 3/22 11:55pm
- Submission rules
  - Put all your files into a directory and name it using your student ID(s)
    - If your team has two members, please concatenate your IDs separated by “-”
    - Please put the student ID used for the Query ID at the beginning of the name
  - Zip the directory and upload the zip file to New E3
  - A sample of the zip file: 01212112-02121221.zip
    - Makefile
    - dns_attack.cpp
    - report.pdf
    - dns_attack.h
    - ….

Questions?