Department of Information Security, Seoul Women's University

데이터통신 및 네트워크
Instructor: Prof. Hoorin Park

Wireshark Assignment, Spring 2024
Due: April 29, 2024, 23:59:59

1. Objectives

트래픽 분석을 통한 응용 계층에서의 HTTP 이해

2. Instruction

Task 1: 자신의 네트워크에서 웹 트래픽을 측정해보기

***QUIC을 끄고 HTTP만 확인하기 위해서는 크롬사용 시 chrome://flags/ 에 접속하여 QUIC을 검색하여 disabled → relaunch로 재시작하면 됩니다.**

자신의 host 컴퓨터에서 인터넷에 연결되는 자신의 IP address에 대하여 약 30초 간 capture filter를 수행해보세요. 이 시간 동안 웹브라우저를 통해 자유롭게 웹사이트를 방문합니다. 로그인 시도 실패, 무작위 url로 잘못된 접근을 수행해보세요. 방문한 데이터를 pcapng 파일로 저장합니다. 단, 이때 pcapng 파일이 비어 있어서는 안 됩니다. 아래 지시문을 따라 작업을 진행하고 보고서로 작성합니다.

바로 패킷 캡처를 시작할 수도 있지만 외부 디바이스와 함께 연결된 네트워크의 경우에 자신의 트래픽 외에도 다른 디바이스의 트래픽이 함께 잡혀 의도하지 않은 sniffing 공격이 이루어지거나, 과도한 트래픽을 수집할 수 있습니다. 이를 피하고 자신의 트래픽만 수집하기 위해서는 capture filter에 필터 명령어를 줄 필요가 있습니다. 상단바의 톱니바퀴 모양으로 생긴 capture option 버튼을 누르거나 capture 탭의 options 메뉴로 들어가세요.

그림 1은 자신의 트래픽만 캡처를 하기위해 capture filter에 필터 명령어를 주는 화면입니다. 먼저 콘솔(win+r 키를 통해 cmd를 실행)창을 열어 ipconfig 명령어를 칩니다. 명령어의 결과를 통해 자신이 연결된 네트워크의 IP 주소를 획득합니다. 제 경우에는 이더넷이 인터넷에 연결된 메인 인터페이스이며 IPv4 주소에서 나의 주소가 211.106.***.***인 것을 확인할 수 있습니다. 이후, 그림에 초록색으로 표시된 capture filter 프롬프트에 "host 211.106.***.***" (자신의 주소)를 적고 이더넷을 더블 클릭하거나 start 버튼을 눌러 캡처를 시작합니다. 이렇게 되면 자신의 트래픽만 필터링하여 저장할 수 있게 됩니다. 캡처한 데이터에 대해 아래 간단한 지시문을 수행하기 바랍니다.

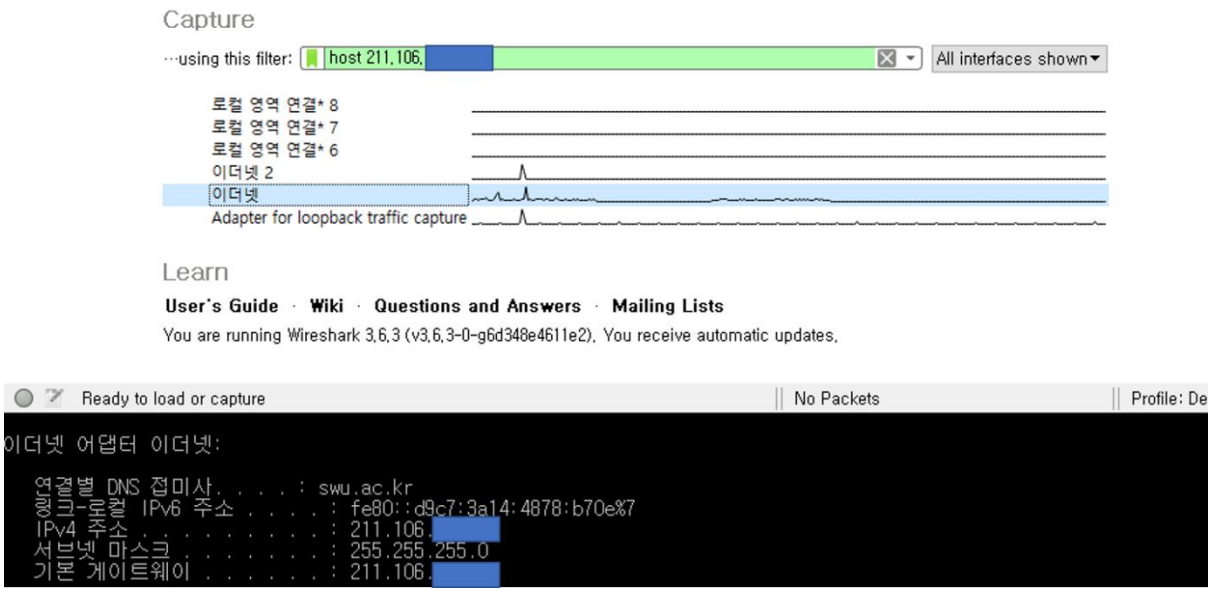

그림 1. 자신의 IP로 캡처 필터 수행

A. Display filter를 활용하여 HTTP or QUIC 패킷만 필터링해보세요.
Ethernet 또는 Wi-Fi 랜카드를 대상으로 패킷 캡처를 수행합니다.
자신의 책임 하에 있는 액세스 네트워크에서만 수행하기를 권장합니다.
(공공장소에서 캡처하지 마세요)

B. 웹 브라우저가 어떠한 HTTP (or QUIC) 버전을 사용하고 있는지 확인하세요. 어디서 정보를 찾을 수 있는지 스크린샷과 함께 제시하세요.

C. Display filter를 활용하여 HTTP status code를 필터링해보세요.
필터링을 위한 명령어와 캡처된 패킷에서 등장한 각 status code가 어떠한 의미를 갖는지 **표의 형태로 정리**해보세요. (hint: http.response.code)
*모든 http status code를 웹에서 복사하라는 이야기가 아닙니다. 본인의 파일에서 얻은 code만 살펴보면 됩니다.

Task 2: 주어진 데이터에서 패킷의 의미를 분석하기

주어진 "Wireshark_http.pcapng"를 살펴보고 아래 지시문을 따라 작업을 진행하고 보고서에 이어서 작성합니다.

A. 주어진 파일의 display filter에 "tcp"로 필터링한 후에 HTTP GET method를 갖는 패킷을 찾고 해당 패킷을 찾는 **명령어를 함께 제시**하세요. (해당 패킷을 A 패킷으로 칭함)

B. 주어진 파일에서 client와 server의 IP, port 번호를 각각 제시하세요.

C. A 패킷의 앞의 3개의 패킷은 무엇을 의미하는지 설명하세요.
   각각의 패킷을 해석하는 것이 아니라 HTTP에서 어떠한 의미를 갖는지 서술하세요.
   (hint: handshaking)

D. A 패킷의 뒤의 패킷 HTTP 200 OK까지 각각의 패킷이 어떤 의미를 갖는지 설명하세요.

3. Submission

A. 위 task를 모두 수행한 후, 보고서를 pdf 형식으로 작성하여 e-class에 제출 기한 전에 업로드합니다. "http_학번_이름.pdf"

4. Notice

A. 지각 제출은 허용하지 않습니다.

B. 시스템 상에 오류가 생겨 시간 내에 제출하지 못하는 경우 메일로 제출 가능합니다.

C. 위 task는 **본인의 machine에서만 수행**해야 합니다.

D. Task 1에서 각 지시문에 대한 대답은 본인이 wireshark에서 얻은 데이터를 기반으로 작성되어야 합니다.

E. 수행한 각 task의 지시문에 대하여 **적절한 스크린샷**과 함께 보고서가 작성되어야 합니다.