**Ethernet**

**1. 실험**

1) Internet Explorer의 캐쉬를 비운다.

- 도구 🡪 인터넷옵션 🡪 (검색기록) 삭제: 모두 삭제할 것

2) Wireshark 실행하고 Capture 준비

3) Wireshark에서 capture 시작하자마자, Internet Explorer로 <http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>에 접속

4) 웹사이트의 내용이 보이자마자, Wireshark의 capture 중단

**2. 참고사항**

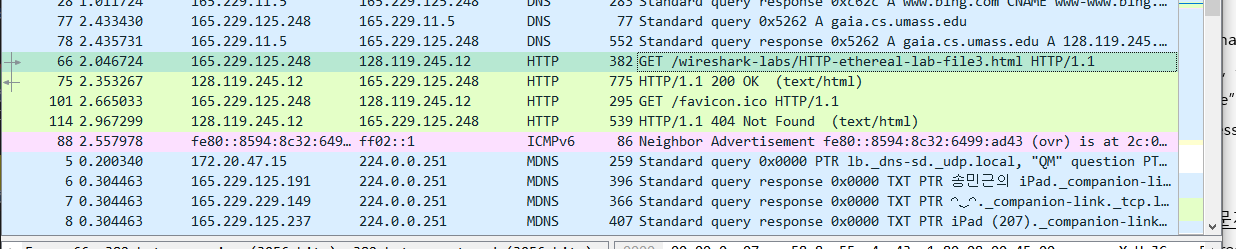
1) Ethernet (version II) frame의 구조는 아래와 같다. 대부분의 Ethernet card는 Preamble과 FCS는 하드웨어에서 제거하므로, Wireshark가 볼 수 있는 부분은 아래의 녹색 부분이다.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Preamble | Destination MAC address | Source  MAC address | Frame Type | User Data | Frame Check Sequence (FCS) |
| 8 | 6 | 6 | 2 | 46 - 1500 | 4 |

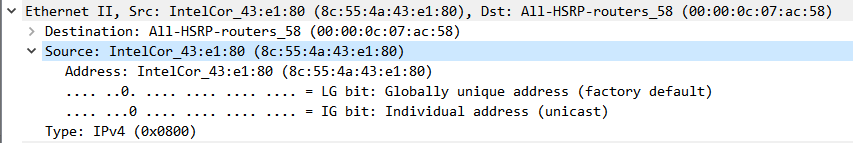
2) 웹서비스는 Application layer protocol인 HTTP를 사용하여 정보를 주고 받으며, 웹페이지를 요청하는 HTTP packet에는 “GET”이라는 문자열이 포함되어 있고, 해당 웹페이지를 가져오는 HTTP packet에는 “OK”라는 문자열이 포함되어 있다. HTTP packet은 Transport layer protocol로서 TCP를, Network layer protocol로서 IP를 사용하며, Link/Physical layer protocol로는 (현재) Ethernet을 사용하고 있다.

**3. 문제**

Capture된 packets 중에서 “GET”이라는 문자열이 포함된 HTTP packet을 찾아, 화면 캡쳐하라.

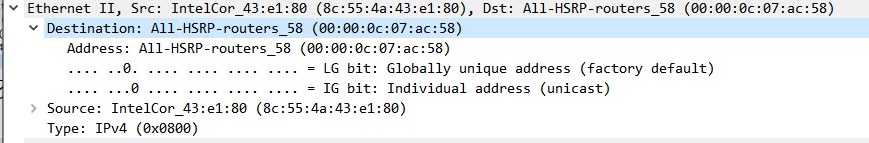


Q1) 그 packet의 Ethernet source address는 무엇인가? 해당 Ethernet address는 누구의 것이라고생각하는가?



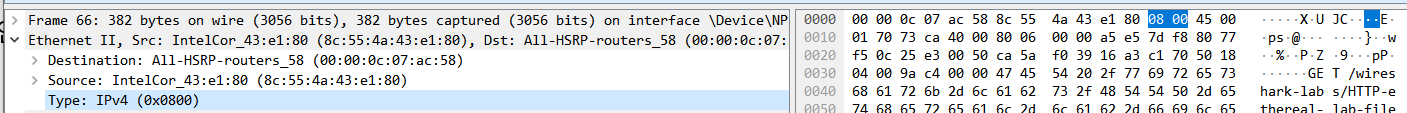
사용자의 컴퓨터.

Q2) 그 packet의 Ethernet destination address는 무엇인가? 해당 Ethernet address는 gaia.cs.umass.edu의 것인가? 아니라면, 누구의 것이라고 생각하는가?



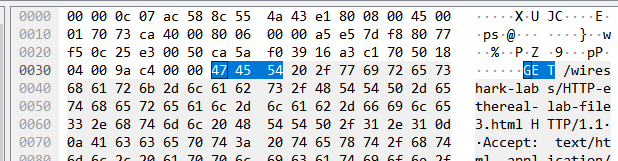
아니다. 사용자의 컴퓨터와 가장 가까운 라우터의 mac주소 . (default gateway)

Q3) 그 packet의 Ethernet “Frame Type” field 값은? 해당 “Frame Type”이 의미하는 바는?



상위계층이 IPv4라는 것을 의미

Q4) Ethernet “Destination MAC address” field의 시작을 “첫 번째” 바이트라고 할 때, “GET”의 “G”는 몇 번째 바이트인가?

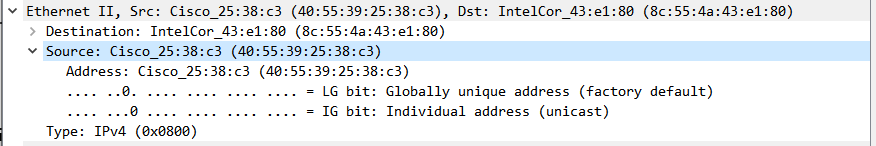


55번째 바이트.

Capture된 packets 중에서 “OK”라는 문자열이 포함된 HTTP packet을 찾아, 화면 캡쳐하라.

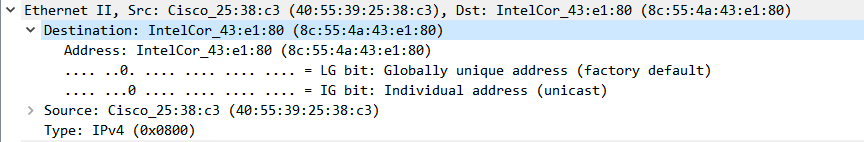


Q5) 그 packet의 Ethernet source address는 무엇인가? 해당 Ethernet address는 gaia.cs.umass.edu의 것인가? 아니라면, 누구의 것이라고 생각하는가?



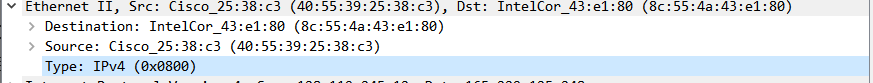
사용자의 컴퓨터와 가장 가까운 라우터의 mac 주소

Q6) 그 packet의 Ethernet destination address는 무엇인가? 해당 Ethernet address는 누구의 것이라고 생각하는가?



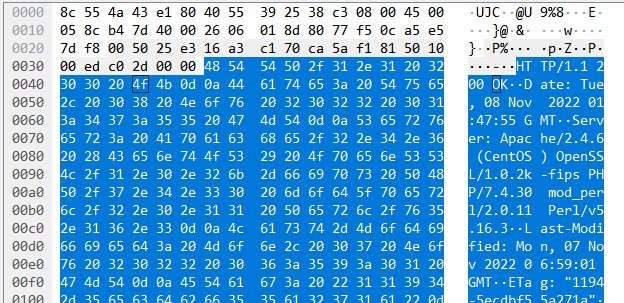
사용자의 컴퓨터

Q7) 그 packet의 Ethernet “Frame Type” field 값은? 해당 “Frame Type”이 의미하는 바는?



상위계층이 IPv4라는 것을 의미

Q8) Ethernet “Destination MAC address” field의 시작을 “첫 번째” 바이트라고 할 때, “OK”의 “O”는 몇 번째 바이트인가?



68번째 바이트