Computer Networks

Assignment-1

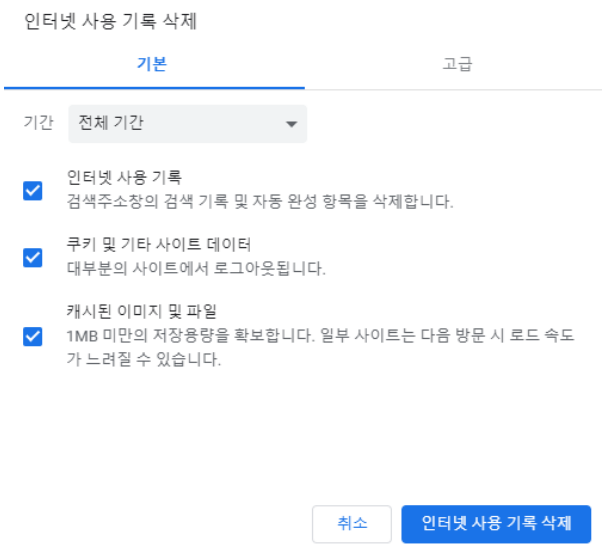
201921120 우다현

Install Wireshark, connect to any website, capture this process, analyze it, and explain the followings:
— For this purpose delete all temporary files on the internet, reboot the computer and do not perform any other network operation (stop auto login options as well).
— execute cmd(command prompt) window with administrative privileges and execute the following command sequentially

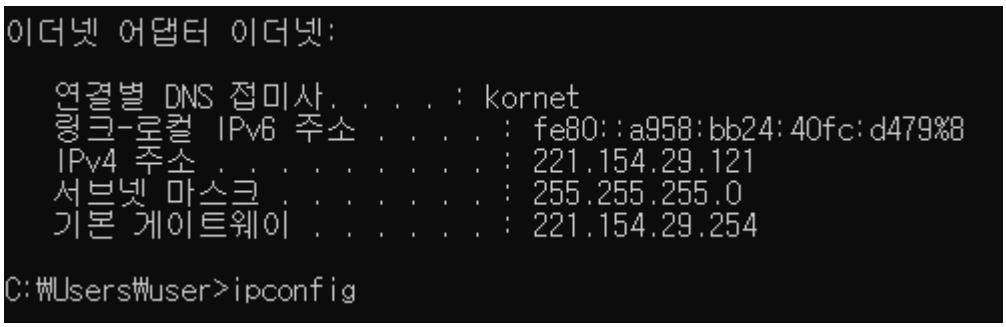
- ipconfig /flushdns
- netsh interface ip delete arpcache

0. 환경

1) 인터넷 사용정보 제거



2) cmd에서 ipconfig 명령어를 사용하여 ip 주소 확인



3)cmd에서 ipconfig /flushdns 명령어 사용 (도메인과 IP교환 과정에서 저장된 정보를 사용하지 않고 교환 과정을 자세히 보기 위해서 저장된 정보를 제거)

```
C:₩Users₩user>ipconfig /flushdns

Windows IP 구성

DNS 확인자 캐시를 플러시했습니다.
```

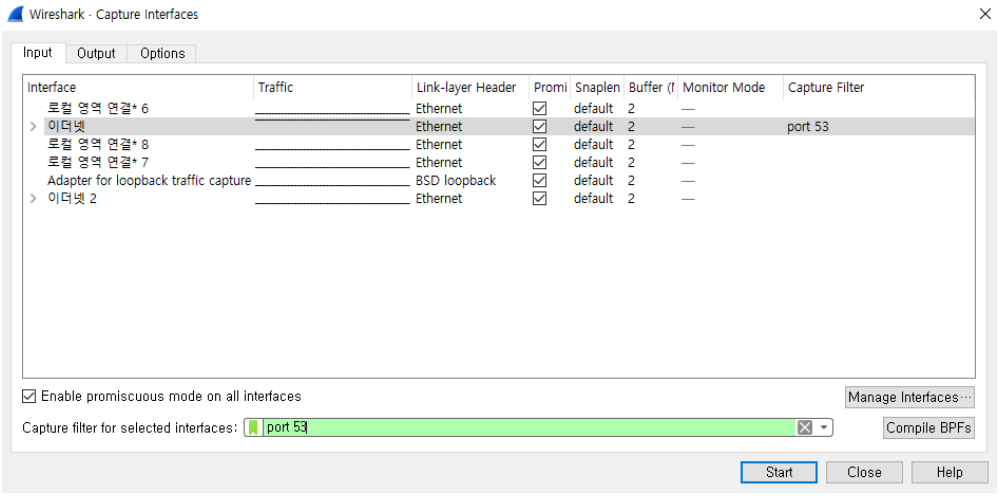
4)cmd에서 netsh interface ip delete arpcache 명령어 사용

```
C:₩Windows₩system32>netsh interface ip delete arpcache
확인됨
```

After that run Wireshark, run capture, connect to website, display all web pages, end capturing and analyze. At this time please use the filter well to see only your own. (IF you do not apply filters, other http / dos may be captured and difficult to analyze)

1. Summarize the content of DNS request response message.

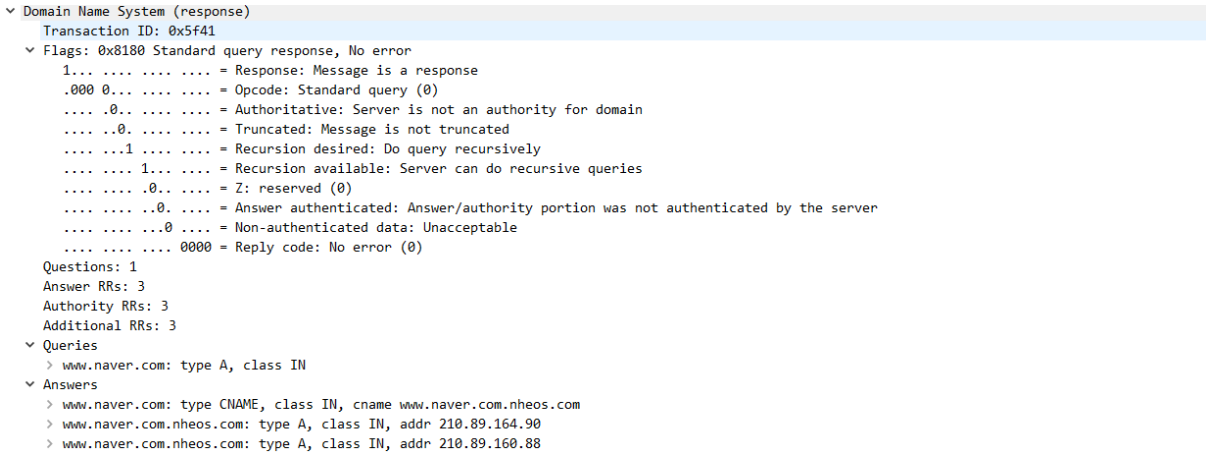
1) DNS 표준 포트인 포트53번으로 Capture filter 검색



2) DNS 요청

```
▾ Domain Name System (query)
    Transaction ID: 0x5f41
  ▾ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    › www.naver.com: type A, class IN
    [Response In: 5]
```

3) DNS 응답



Transaction ID: 0x5f41를 통해 조회에 대한 올바른 응답인 것을 확인할 수 있다.

Answers: 요청에서 물어본 네이버의 IP주소가 210.89.164.90임을 확인할 수 있다.

Transaction ID: DNS ID Number: DNS 조회와 DNS 응답을 연관시키기 위해 사용한다.

Flags

Response: QR 패킷이 DNS 조회인지 응답인지 나타내기 위해 사용한다.

Op Code

Authoritative Answer: 네임서버로부터 응답이라는 것을 나타낸다.

Truncation: 응답이 패킷에 맞추기에 너무 커서 생략됐다는 것을 나타낸다.

Recursion Desired: 네임서버가 요청된 정보를 포함하고 있지 않은 경우 DNS 클라이언트가 재귀 조회를 요청할 것인지 나타낸다.

Recursion Available: 재귀 조회를 지원한다는 것을 나타낸다.

Reserved(Z): 나중을 위해 예약된 필드로 항시 0으로 설정되어 있다.

Reply Code: 어떤 오류 발생을 나타내기 위해 DNS 응답에 사용한다.

Question Count Question : 섹션의 엔트리 수이다.

Answer Count: Section의 엔트리 수이다.

Name Server Count Authority: Section의 네임 서버 자원 레코드 수이다.

Additional Records Count: Additional Section의 수이다.

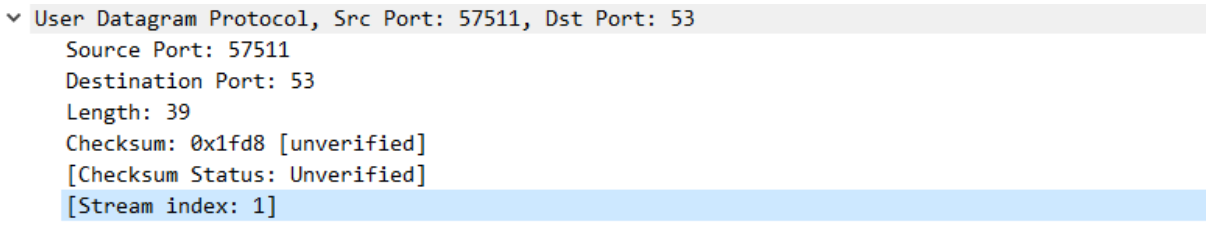
Question Section: DNS서버에 송신될 하나 이상의 정보에 대해 조회를 포함한다.

Answer Section: 조회에 응답하는 하나 이상의 리소스 레코드를 전송하는 가변 섹션이다.

Authority Section: 변환 과정을 계속하는 데 사용할 수 있는 인가된 네임 서버를 가리킨다.

Additional Information Section: 반드시 응답할 필요가 없는 조회에 관련된 부가적인 정보를 포함한다.

a) Analyze the transport layer segment to determine which transport layer to user and the port number



Source port number는 57511이고, Destination port number는 53이다.

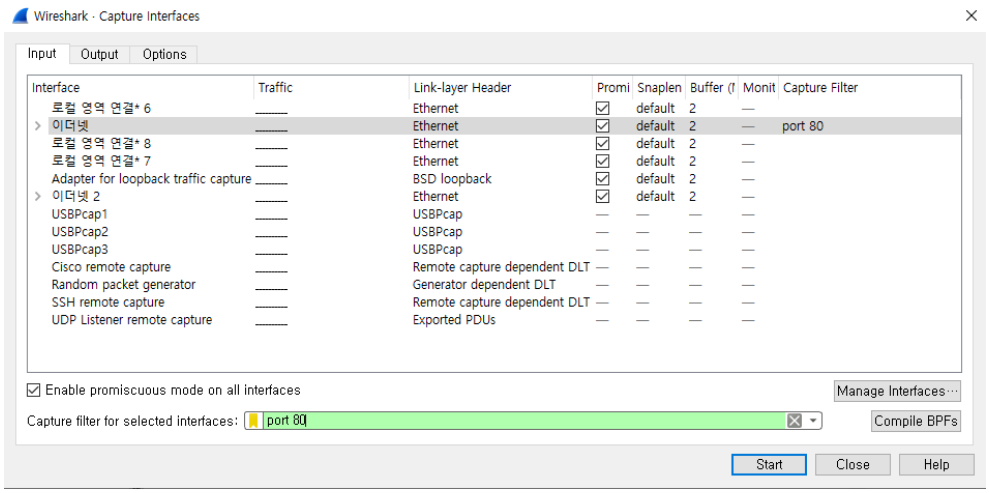
일반적인 DNS 질의 및 응답 절차를 거쳤으므로 UDP를 이용한 것을 확인할 수 있다.

아래는 DNS 메시지 시스템이다.

도메인 네임 시스템									
비트오프셋	0-15	16-31							
0	DNS ID Number	QR	OpCode	AA	TC	RD	RA	Z	RCode
32	Question Count	Answer Count							
64	Name Server Count	Additional Records Count							
96	Question Section	Answers Section							
128	Authority Section	Additional Information Section							

2. Check TCP connection setup process before HTTP.

1) HTTP를 확인하기 위해서, Capture filter port 80으로 검색 (HTTP 패킷은 TCP 상에서 HTTP 통신의 표준 포트인 서버의 80번 포트로 전달되기 때문)



2) tcp 연결

1	0.000000	221.154.29.121	211.115.106.79	TCP	54 7253 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2	0.003137	221.154.29.121	211.115.106.76	TCP	66 7293 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 WS=256 SACK_PER…
3	0.006485	211.115.106.76	221.154.29.121	TCP	66 80 → 7293 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SAC…
4	0.006746	221.154.29.121	211.115.106.76	TCP	54 7293 → 80 [ACK] Seq=1 Ack=1 Win=8704 Len=0

1	0.000000	221.154.29.121	172.217.175.68	TCP	66 10399 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_P…
2	0.000022	221.154.29.121	172.217.175.68	TCP	66 10400 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_P…
3	0.030470	172.217.175.68	221.154.29.121	TCP	66 80 → 10399 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SA…
4	0.030647	221.154.29.121	172.217.175.68	TCP	54 10399 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
5	0.030860	221.154.29.121	172.217.175.68	HTTP	696 GET / HTTP/1.1

위 두개의 사진은 모두 HTTP 이전에 TCP connection(Tree-way-Handshaking)이 이루어지는 모습이다.

[SYN] 2.초기 일련번호(Seq) 0

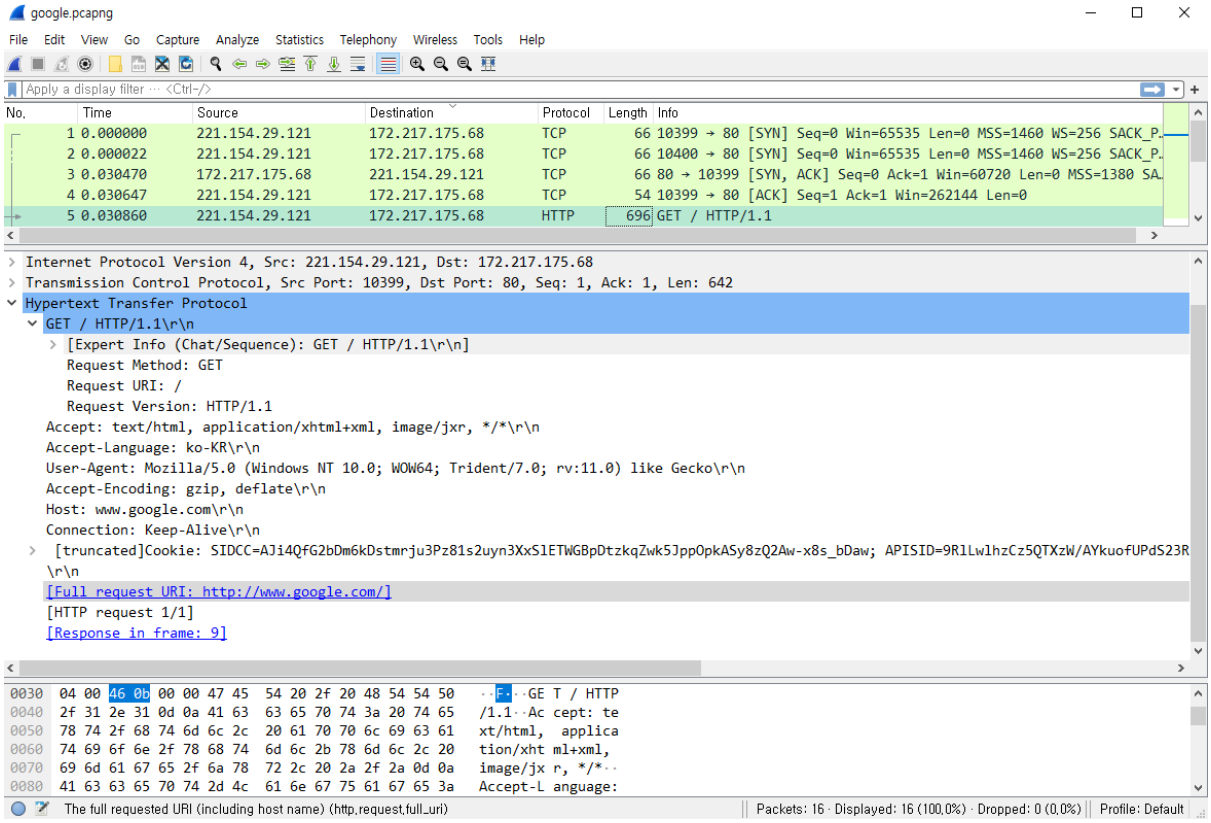
[SYN,ACK] 3.확인응답번호(Ack) 1(이전seq+1) 일련번호(Seq) 0

[SYN] 4.확인응답번호(Ack) 1(이전seq+1) 일련번호(Seq) 1

호스트가 수신할 것으로 예상되는 다음 일련번호를 지정하는데 사용되기 때문에 확인응답 번호는 이전 패킷에 포함된 일련번호보다 하나가 큰 값이다.

3. Summerize the contents and meaning for the HTTP request and response message for the first time.

1) Request message(method/URL/Version)



1-1) Method

GET method: URL로부터 확인 된 정보를 검색해서 가져온다.

POST method: Server가 Entity body를 받아들이도록 한다.

HEAD method: 서버의 응답 헤더를 요청한다. Hypertext link의 유효성, 접근 가능성, 최근 수정 사항 등을 확인하는데 사용되기도 한다.

PUT method: URL에 Entity를 저장한다.

DELETE method: URL의 자료를 제거한다.

TRACE method: Application-layer까지 도달 과정을 조사한다.

1-2) URL

Uniform Resource Locator의 두문자어로 인터넷 정보의 주소이다.

1-3) Verision

HTTP의 버전 정보이다. HTTP 1.1를 이용한다.

2) Header line

추가적인 정보를 전달한다(Web Browser 종류, 사용 언어 등.)

2-1) Accept: 처리하는 데이터의 타입을 나타낸다.

2-2) User-agent: 사용자의 Web Browser 종류 및 버전에 대한 정보이다.

2-3) Referer: URL에 대한 정보이다.

2-4) Accept-Language: 사용하는 언어에 대한 정보이다.

2-5) Connetion: 연결에 대한 정보이다.

2-6) Cookies: HTTP는 stateless 방식이기 때문에 세션을 유지하지 않고 정보를 남기지 않는다. Cookies는 사이트가 사용자의 정보를 유지할 수 있도록 허락한다.

2-7) Blank line

Header line 과 Entity Body를 구분하기 위한 공백이다.

2-8) Entity body

Request에 필요한 값들을 갖고 있다.

3) Response message

3-1) Status code:

1xx: Informational - Request received, continuing process
2xx: Success - The action was successfully received, understood, and accepted
3xx: Redirection - Further action must be taken in order to complete the request
4xx: Client Error - The request contains bad syntax or cannot be fulfilled
5xx: Server Error - The server failed to fulfill an apparently valid request

3-2) Header line

(사진에서 잘린 부분도 포함해서 설명한다.)

추가 정보

3-2-1) Date: 현재의 시간을 나타낸다.

3-2-2) Server: 웹 서버의 종류를 나타낸다.

3-2-3) Content-type: 읽을 수 있는 형태임을 나타낸다.

3-2-4) Last-modified: 마지막으로 수정된 시간을 나타낸다.

3-3) Blank line

Header line과 Entity body를 구분하기 위한 공백이다.

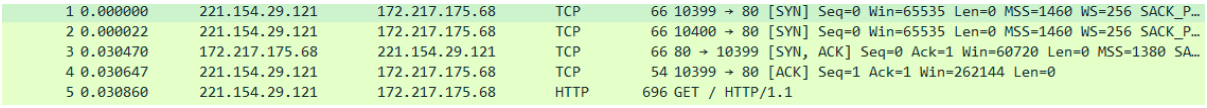
3-4) Entity body

Response에 필요한 값들을 갖고 있다.

4. Data transfer process

a) Sequence, ACK, Number

HTTP 이전에 TCP connection(Three-way-Handshaking) 과정에서 데이터 전송이 생긴다.



1	0.000000	221.154.29.121	172.217.175.68	TCP	66 10399 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_P…
2	0.000022	221.154.29.121	172.217.175.68	TCP	66 10400 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_P…
3	0.030470	172.217.175.68	221.154.29.121	TCP	66 80 → 10399 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SA…
4	0.030647	221.154.29.121	172.217.175.68	TCP	54 10399 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
5	0.030860	221.154.29.121	172.217.175.68	HTTP	696 GET / HTTP/1.1

위 사진은 http request message를 설명할 때 사용했던 사진을 다시 한 번 가져온 것이다.

[SYN] 2.초기 일련번호(Seq) 0

[SYN,ACK] 3.확인응답번호(Ack) 1(이전seq+1) 일련번호(Seq) 0

[SYN] 4.확인응답번호(Ack) 1(이전seq+1) 일련번호(Seq) 1

호스트가 수신할 것으로 예상되는 다음 일련번호를 지정하는데 사용되기 때문에 확인응답 번호는 이전 패킷에 포함된 일련번호보다 하나가 큰 값이다.

5.Analyze whether persistent or non-persistent connection.

HTTP는 Non-persistent Connections으로 연결을 매번 끊고 새로 연결하는 방식을 취하기 때문에 시간과 비용적인 측면에서 비효율적이었다. 이를 해결하기 위해 HTTP1.1부터는 Keep-Alive의 기능을 제공한다.

이 실험에서는 HTTP1.1를 사용한다. 즉, persistent connection(지속연결)이다.

6. Write what protocols other than HTTP and DNS appear.

파일 전송 프로토콜(File Transfer Protocol, FTP)이 있다. FTP는 TCP/IP 프로토콜을 가지고 서버와 클라이언트 사이의 파일 전송을 하기 위한 프로토콜이다. 파일 전송 프로토콜은 TCP/IP 프로토콜 테이블의 응용 계층에 속한다.

HTTP와는 달리 연결의 종류는 2가지가 있다:

명령 연결: 먼저 제어 포트인 서버 21번 포트로 사용자 인증, 명령을 위한 연결이 만들어지고, 여기를 통해 클라이언트에서 지시하는 명령어가 전달된다.

데이터 전송용 연결: 실제의 파일 전송은 필요할 때 새로운 연결이 만들어진다. 능동 모드(액티브 모드): 서버가 자신의 데이터 포트인 20번 포트에서부터 클라이언트가 지정한 지점으로의 데이터 연결을 만든다. 클라이언트가 지정하는 포트는 주로 1023 보다 큰 번호가 매겨진 포트이다. 클라이언트가 방화벽, NAT(IP 마스킹) 등을 사용하는 환경일 때에 잘 동작하지 않을 수 있는데, 이때 수동 모드(클라이언트가 서버가 지정한 서버 포트로 연결할 수 있게 함. 보통 양쪽 포트 모두 1023보다 큼)를 이용하면 된다.