TCP/IP 패킷 캡처 분석 프로그램

한국산업기술대학교(KPU) – 컴퓨터 네트워크

9조

2014154037 한승우
2016154010 김지우
2016156032 전유미
2017152049 정하림

Contents

01 과제 목표

▶과제의 목적 및 목표

네트워크 상에서 전달되는 TCP/IP 패킷을 캡쳐 하고,

대상 프로토콜의 네트워크 계층부터 응용 계층의 Payload까지

상향식 순차 분석하는 프로그램 개발

패킷 캡처에 포함될 프로토콜 3종

대상 프로토콜	링크 계층	네트워크 계층	전송 계층	응용 계층	응용 계층 페이로드
1. HTTP	Ethernet	IP	TCP	HTTP	HTTP 페이로드
2. DNS	Ethernet	IP	UDP	DNS	DNS 페이로드
3. icmp	Ethernet	IP/icmp	-	-	IP 내용 일부

02 설계 환경

VM Ware WorkStation

Wire Shark

raw socket

http://

https://

http, https, DNS, icmp

Windows PC

Web Server
210.93.48.51

DNS Server
210.93.48.196

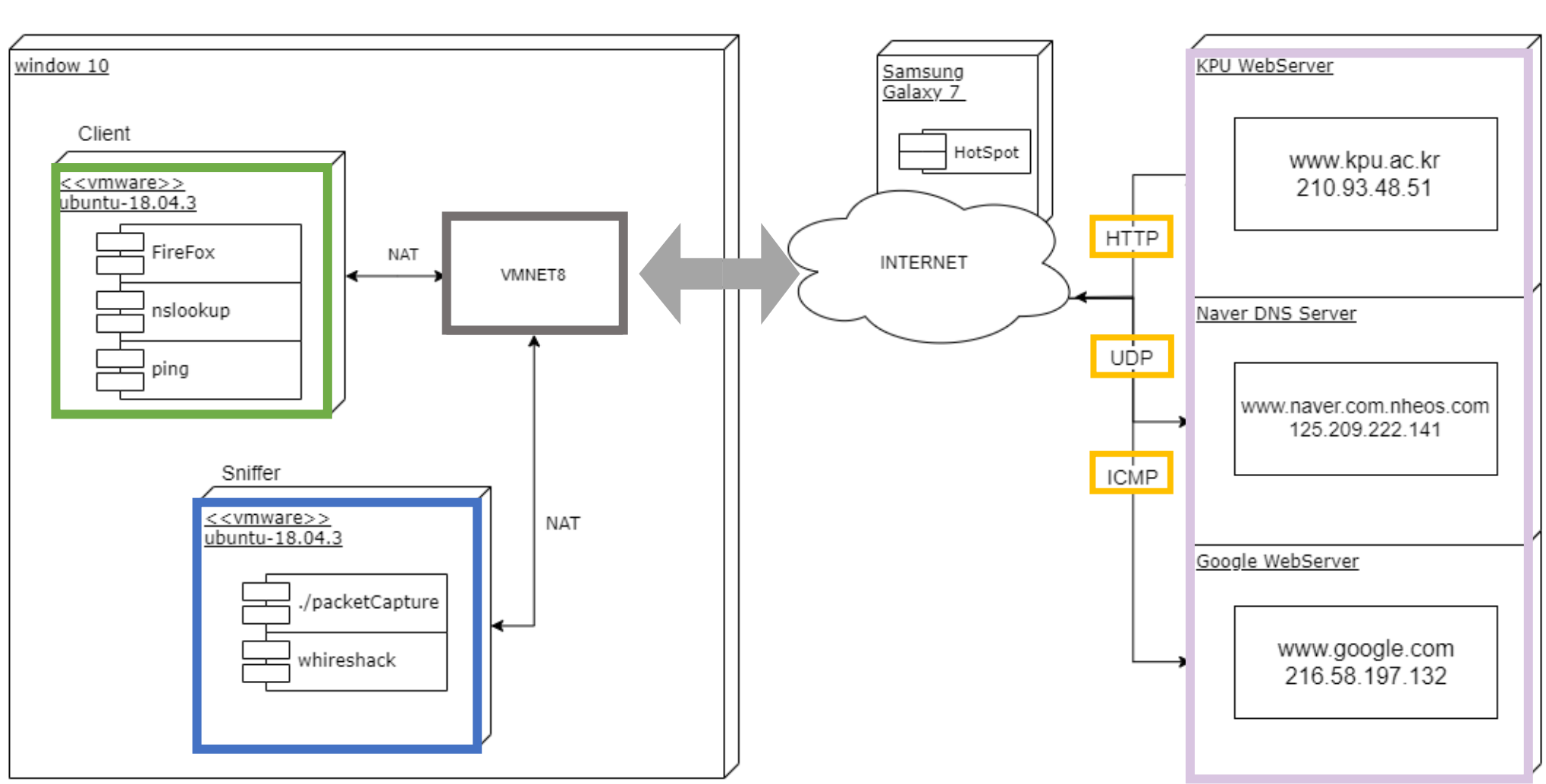
02 설계 환경

VM Ware
WorkStation
[가상 머신]

우분투
[OS]

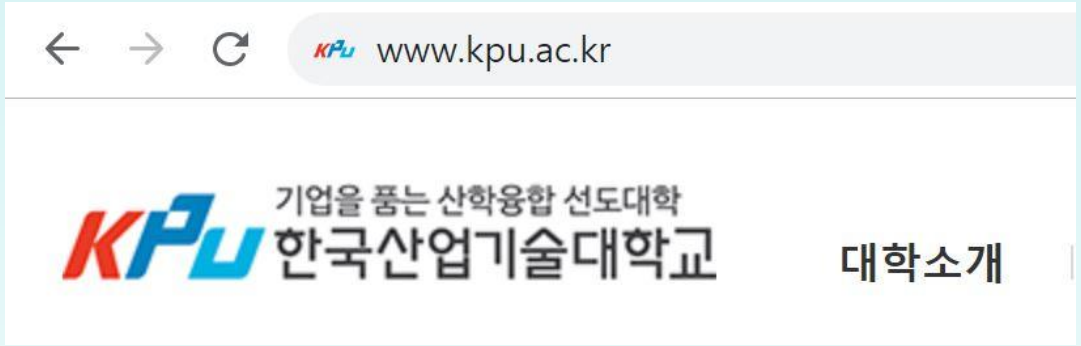
Linux gcc
[컴파일러]

03 설계 방향 – 논리적 분리(UML)



04 설계 내용

http://



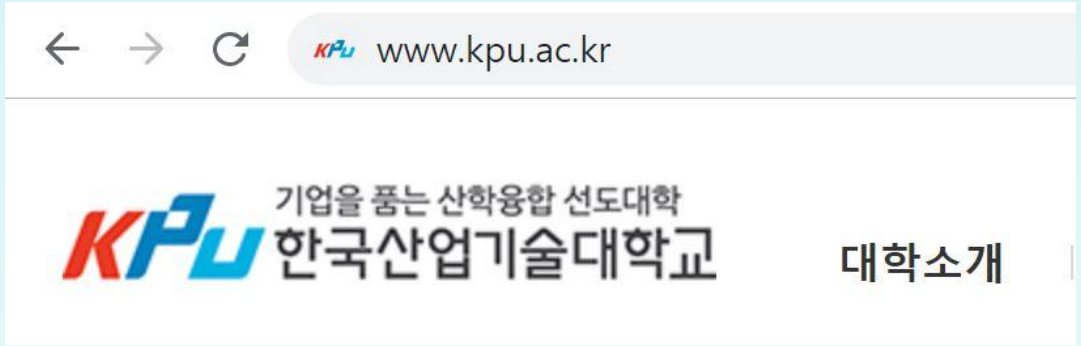
www.kpu.ac.kr 웹 서버 주소를 사용한다. (210.93.48.51)

우분투의 기본 브라우저를 사용한다. (VM Ware)

패킷 캡처 후에 IP 헤더 정보, TCP 헤더 정보, HTTP의 Payload를 분석한다.

04 설계 내용

http://



1. Raw Socket Ubuntu GCC 실행

2. HTTP 실행 후, Insert IP로 해당 IP 실행

3. Ubuntu -> 터미널 -> Raw Socket실행-> log 파일 분석
   Wireshark [필터 적용], Wireshark FlowGraph

04 결과(1)

http://

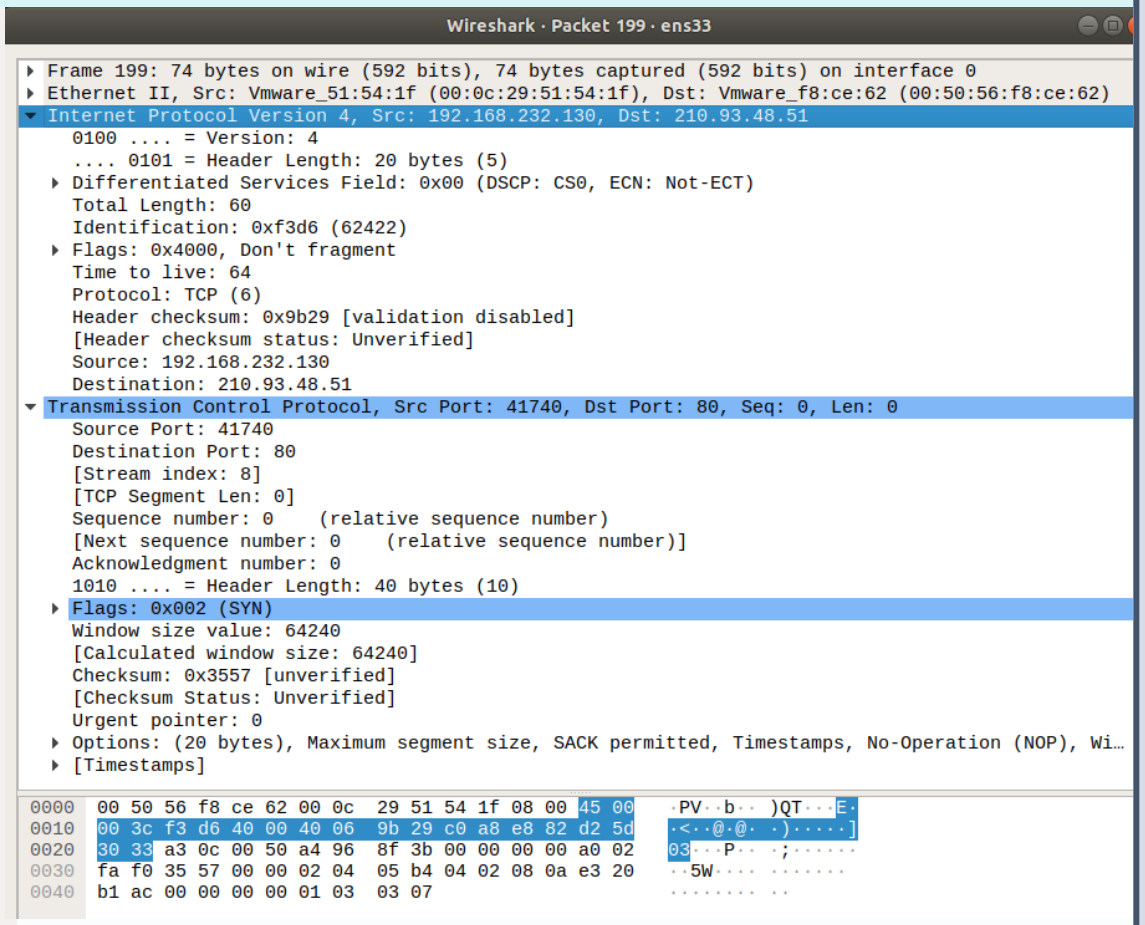
```
**********************TCP Packet*************************

IP Header
   |-IP Version        : 4
   |-IP Header Length  : 5 DWORDS or 20 Bytes
   |-Type Of Service   : 0
   |-IP Total Length   : 60  Bytes(Size of Packet)
   |-Identification    : 62422
   |-TTL      : 64
   |-Protocol : 6
   |-Checksum : 39721
   |-Source IP        : 192.168.232.130
   |-Destination IP   : 210.93.48.51

TCP Header
   |-Source Port      : 41740
   |-Destination Port : 80
   |-Sequence Number    : 2761330491
   |-Acknowledge Number : 0
   |-Header Length      : 10 DWORDS or 40 BYTES
   |-Urgent Flag          : 0
   |-Acknowledgement Flag : 0
   |-Push Flag            : 0
   |-Reset Flag           : 0
   |-Synchronise Flag     : 1
   |-Finish Flag          : 0
   |-Window         : 64240
   |-Checksum       : 13655
   |-Urgent Pointer : 0

                        DATA Dump
IP Header
    45 00 00 3C F3 D6 40 00 40 06 9B 29 C0 A8 E8 82         E..<..@.@..)....
    D2 5D 30 33                                             .]03
TCP Header
    A3 0C 00 50 A4 96 8F 3B 00 00 00 00 A0 02 FA F0         ...P...;........
    35 57 00 00 02 04 05 B4 04 02 08 0A E3 20 B1 AC         5W.......... ..
    00 00 00 00 01 03 03 07                                 ........
Data Payload

###########################################################
```



04 결과(2)

http://

```
**********************TCP Packet*************************

IP Header
   |-IP Version        : 4
   |-IP Header Length  : 5 DWORDS or 20 Bytes
   |-Type Of Service   : 0
   |-IP Total Length   : 44  Bytes(Size of Packet)
   |-Identification    : 45386
   |-TTL      : 128
   |-Protocol : 6
   |-Checksum : 56773
   |-Source IP        : 210.93.48.51
   |-Destination IP   : 192.168.232.130

TCP Header
   |-Source Port      : 80
   |-Destination Port : 41740
   |-Sequence Number    : 990782749
   |-Acknowledge Number : 2761330492
   |-Header Length      : 6 DWORDS or 24 BYTES
   |-Urgent Flag          : 0
   |-Acknowledgement Flag : 1
   |-Push Flag            : 0
   |-Reset Flag           : 0
   |-Synchronise Flag     : 1
   |-Finish Flag          : 0
   |-Window         : 64240
   |-Checksum       : 47630
   |-Urgent Pointer : 0

                        DATA Dump
IP Header
    45 00 00 2C B1 4A 00 00 80 06 DD C5 D2 5D 30 33         E..,.J..□□....]03
    C0 A8 E8 82                                             ....
TCP Header
    00 50 A3 0C 3B 0E 25 1D A4 96 8F 3C 60 12 FA F0         .P..;.%....<`...
    BA 0E 00 00 02 04 05 B4                                 ........
Data Payload
    00 00                                                   ..

############################################################
```

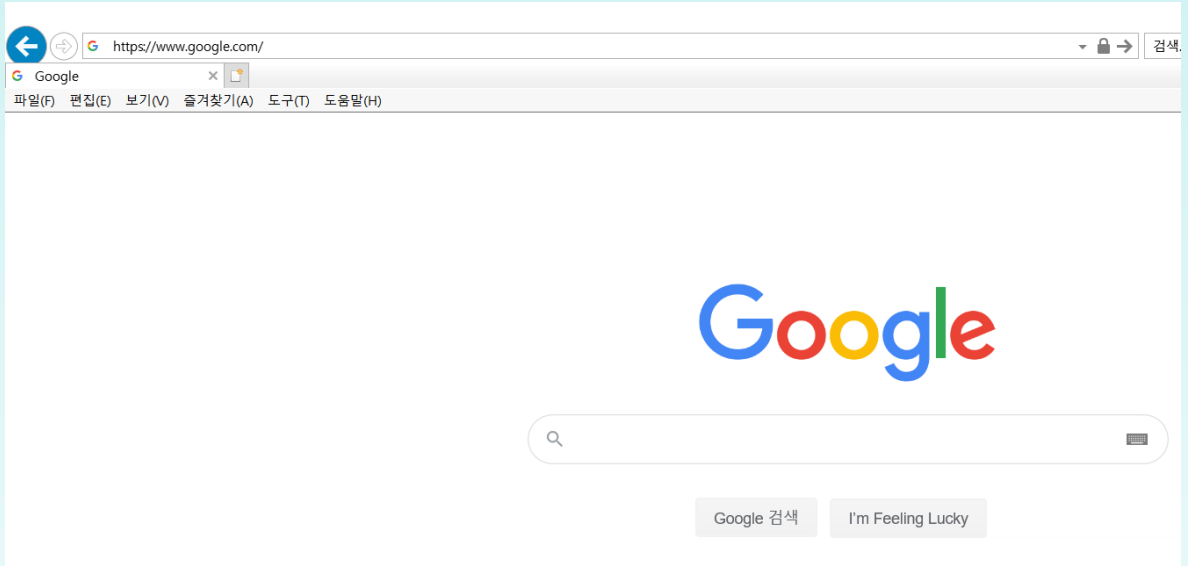
Wireshark · Packet 200 · ens33

```
▸ Frame 200: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Vmware_f8:ce:62 (00:50:56:f8:ce:62), Dst: Vmware_51:54:1f (00:0c:29:51:54:1f)
▾ Internet Protocol Version 4, Src: 210.93.48.51, Dst: 192.168.232.130
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 44
    Identification: 0xb14a (45386)
  ▸ Flags: 0x0000
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xddc5 [validation disabled]
    [Header checksum status: Unverified]
    Source: 210.93.48.51
    Destination: 192.168.232.130
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 41740, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 41740
    [Stream index: 8]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0110 .... = Header Length: 24 bytes (6)
  ▸ Flags: 0x012 (SYN, ACK)
    Window size value: 64240
    [Calculated window size: 64240]
    Checksum: 0xba0e [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (4 bytes), Maximum segment size
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]

0000  00 0c 29 51 54 1f 00 50  56 f8 ce 62 08 00 45 00    ··)QT··P V··b··E·
0010  00 2c b1 4a 00 00 80 06  dd c5 d2 5d 30 33 c0 a8    ·,·J···· ···]03··
0020  e8 82 00 50 a3 0c 3b 0e  25 1d a4 96 8f 3c 60 12    ···P··;· %····<`·
0030  fa f0 ba 0e 00 00 02 04  05 b4 00 00               ···· ···· ····
```

04 설계 내용

https://



www.google.com 웹 서버 주소를 사용한다. (172.217.26.3)

우분투의 기본 브라우저를 사용한다. (VM Ware)

패킷 캡처 후에 TCP 헤더 정보, HTTPS의 Payload를 분석한다.(443 포트 -> payload 암호화 확인)

04 결과(1)

https://

```
**********************TCP Packet*************************

IP Header
   |-IP Version        : 4
   |-IP Header Length  : 5 DWORDS or 20 Bytes
   |-Type Of Service   : 0
   |-IP Total Length   : 60  Bytes(Size of Packet)
   |-Identification    : 60926
   |-TTL      : 64
   |-Protocol : 6
   |-Checksum : 56501
   |-Source IP        : 192.168.232.130
   |-Destination IP   : 172.217.26.3

TCP Header
   |-Source Port      : 42620
   |-Destination Port : 443
   |-Sequence Number    : 1682383756
   |-Acknowledge Number : 0
   |-Header Length      : 10 DWORDS or 40 BYTES
   |-Urgent Flag          : 0
   |-Acknowledgement Flag : 0
   |-Push Flag            : 0
   |-Reset Flag           : 0
   |-Synchronise Flag     : 1
   |-Finish Flag          : 0
   |-Window         : 64240
   |-Checksum       : 22439
   |-Urgent Pointer : 0

                        DATA Dump
IP Header
    45 00 00 3C ED FE 40 00 40 06 DC B5 C0 A8 E8 82         E..<..@.@.......
    AC D9 1A 03                                             ....
TCP Header
    A6 7C 01 BB 64 47 23 8C 00 00 00 00 A0 02 FA F0         .|..dG#.........
    57 A7 00 00 02 04 05 B4 04 02 08 0A 4A 6B 0A EA         W...........Jk..
    00 00 00 00 01 03 03 07                                 ........
Data Payload

###########################################################
```

Wireshark · Packet 9 · ens33

```
▸ Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: Vmware_51:54:1f (00:0c:29:51:54:1f), Dst: Vmware_f8:ce:62 (00:50:56:f8:ce:62)
▾ Internet Protocol Version 4, Src: 192.168.232.130, Dst: 172.217.26.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xedfe (60926)
  ▸ Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xdcb5 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.232.130
    Destination: 172.217.26.3
▾ Transmission Control Protocol, Src Port: 42620, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 42620
    Destination Port: 443
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    1010 .... = Header Length: 40 bytes (10)
  ▸ Flags: 0x002 (SYN)
    Window size value: 64240
    [Calculated window size: 64240]
    Checksum: 0x57a7 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Win
  ▸ [Timestamps]

0000  00 50 56 f8 ce 62 00 0c  29 51 54 1f 08 00 45 00   ·PV··b·· )QT···E·
0010  00 3c ed fe 40 00 40 06  dc b5 c0 a8 e8 82 ac d9   ·<··@·@· ········
0020  1a 03 a6 7c 01 bb 64 47  23 8c 00 00 00 00 a0 02   ···|··dG #·······
0030  fa f0 57 a7 00 00 02 04  05 b4 04 02 08 0a 4a 6b   ··W····· ······Jk
0040  0a ea 00 00 00 00 01 03  03 07                     ········ ··
```

04 결과(2)

https://

```
**********************TCP Packet*************************

IP Header
   |-IP Version        : 4
   |-IP Header Length  : 5 DWORDS or 20 Bytes
   |-Type Of Service   : 0
   |-IP Total Length   : 145  Bytes(Size of Packet)
   |-Identification    : 55555
   |-TTL      : 64
   |-Protocol : 6
   |-Checksum : 61947
   |-Source IP        : 192.168.232.130
   |-Destination IP   : 172.217.25.99

TCP Header
   |-Source Port      : 48812
   |-Destination Port : 443
   |-Sequence Number    : 1121016244
   |-Acknowledge Number : 1890133095
   |-Header Length      : 5 DWORDS or 20 BYTES
   |-Urgent Flag          : 0
   |-Acknowledgement Flag : 1
   |-Push Flag            : 1
   |-Reset Flag           : 0
   |-Synchronise Flag     : 0
   |-Finish Flag          : 0
   |-Window         : 62780
   |-Checksum       : 49632
   |-Urgent Pointer : 0

                        DATA Dump
IP Header
    45 00 00 91 D9 03 40 00 40 06 F1 FB C0 A8 E8 82         E.....@.@.......
    AC D9 19 63                                             ...c
TCP Header
    BE AC 01 BB 42 D1 59 B4 70 A9 24 67 50 18 F5 3C         ....B.Y.p.$gP..<
    C1 E0 00 00                                             ....
Data Payload
    17 03 03 00 64 38 9A 8E A8 E1 44 8C E9 A0 FE 10         ....d8....D.....
    F2 45 3A 8C 5F 03 EC 93 AB FC 0E F5 53 B2 B3 AD         .E:._.......S...
    33 F3 D2 72 78 B3 C1 3A F9 FA BF BC 5E 91 89 87         3..rx..:....^...
    15 EF 88 4D D8 B5 2A 36 C2 EE 8A 6B 5E 42 CF 55         ...M..*6...k^B.U
    E7 26 1D C1 4F AD E6 92 B9 99 A4 FC 0A 0D 59 41         .&..O.........YA
    91 0A E9 AE ED E3 91 AB 18 69 02 66 04 2C 89 C1         .........i.f.,..
    18 7D F9 4E 75 BF 07 5D 41                              .}.Nu..]A

###########################################################
```

Wireshark · Packet 13 · ens33

```
▸ Frame 13: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface 0
▸ Ethernet II, Src: Vmware_51:54:1f (00:0c:29:51:54:1f), Dst: Vmware_f8:ce:62 (00:50:56:f8:ce
▾ Internet Protocol Version 4, Src: 192.168.232.130, Dst: 172.217.25.99
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 145
    Identification: 0xd903 (55555)
  ▸ Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xf1fb [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.232.130
    Destination: 172.217.25.99
▾ Transmission Control Protocol, Src Port: 48812, Dst Port: 443, Seq: 1, Ack: 1, Len: 105
    Source Port: 48812
    Destination Port: 443
    [Stream index: 2]
    [TCP Segment Len: 105]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 106    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 62780
    [Calculated window size: 62780]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xc1e0 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (105 bytes)
▸ Secure Sockets Layer
```

```
0000  00 50 56 f8 ce 62 00 0c  29 51 54 1f 08 00 45 00   ·PV··b·· )QT···E·
0010  00 91 d9 03 40 00 40 06  f1 fb c0 a8 e8 82 ac d9   ····@·@· ········
0020  19 63 be ac 01 bb 42 d1  59 b4 70 a9 24 67 50 18   ·c····B· Y·p·$gP·
0030  f5 3c c1 e0 00 00 17 03  03 00 64 38 9a 8e a8 e1   ·<······ ··d8····
0040  44 8c e9 a0 fe 10 f2 45  3a 8c 5f 03 ec 93 ab fc   D·····E :·_·····
0050  0e f5 53 b2 b3 ad 33 f3  d2 72 78 b3 c1 3a f9 fa   ··S···3· ·rx··:··
0060  bf bc 5e 91 89 87 15 ef  88 4d d8 b5 2a 36 c2 ee   ··^····· ·M··*6··
0070  8a 6b 5e 42 cf 55 e7 26  1d c1 4f ad e6 92 b9 99   ·k^B·U·& ··O·····
0080  a4 fc 0a 0d 59 41 91 0a  e9 ae ed e3 91 ab 18 69   ····YA·· ·······i
0090  02 66 04 2c 89 c1 18 7d  f9 4e 75 bf 07 5d 41      ·f·,···} ·Nu··]A
```

04 설계 내용

nslookup 명령어 사용, 해당 도메인 또는 IP 주소를 얻는다.

ns.kpu.ac.kr 웹 주소를 사용한다.

패킷 캡처 후에 IP 헤더 정보, UDP 헤더 정보, DNS의 Payload를 분석한다.

04 설계 내용

1. Raw Socket Ubuntu GCC 실행

2. DNS 실행 후, Insert IP로 해당 IP 실행

3. Ubuntu -> 터미널 -> Raw Socket실행-> log 파일 분석
   Wireshark [필터 적용], Wireshark FlowGraph

04 결과(1)


```
**********************UDP Packet*************************

IP Header
   |-IP Version        : 4
   |-IP Header Length  : 5 DWORDS or 20 Bytes
   |-Type Of Service   : 0
   |-IP Total Length   : 66  Bytes(Size of Packet)
   |-Identification    : 18119
   |-TTL      : 64
   |-Protocol : 17
   |-Checksum : 41485
   |-Source IP        : 192.168.232.130
   |-Destination IP   : 192.168.232.2

UDP Header
   |-Source Port      : 45053
   |-Destination Port : 53
   |-UDP Length       : 46
   |-UDP Checksum     : 62045

IP Header
    45 00 00 42 46 C7 40 00 40 11 A2 0D C0 A8 E8 82         E..BF.@.@.......
    C0 A8 E8 02                                             ....
UDP Header
    AF FD 00 35 00 2E F2 5D                                 ...5...]
Data Payload
    C1 49 01 00 00 01 00 00 00 00 00 01 03 6B 70 75         .I...........kpu
    02 61 63 02 6B 72 00 00 01 00 01 00 00 29 02 00         .ac.kr.......)..
    00 00 00 00 00 00                                       ......

############################################################
```

Wireshark · Packet 3 · ens33

```
▸ Frame 3: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
▸ Ethernet II, Src: Vmware_51:54:1f (00:0c:29:51:54:1f), Dst: Vmware_f8:ce:62 (00:50:56:f8:ce:62)
▾ Internet Protocol Version 4, Src: 192.168.232.130, Dst: 192.168.232.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 66
    Identification: 0x46c7 (18119)
  ▸ Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0xa20d [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.232.130
    Destination: 192.168.232.2
▾ User Datagram Protocol, Src Port: 45053, Dst Port: 53
    Source Port: 45053
    Destination Port: 53
    Length: 46
    Checksum: 0xf25d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
▾ Domain Name System (query)
    Transaction ID: 0xc149
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▸ Additional records
    [Response In: 4]
```

```
0000  00 50 56 f8 ce 62 00 0c  29 51 54 1f 08 00 45 00   ·PV··b·· )QT···E·
0010  00 42 46 c7 40 00 40 11  a2 0d c0 a8 e8 82 c0 a8   ·BF·@·@· ········
0020  e8 02 af fd 00 35 00 2e  f2 5d c1 49 01 00 00 01   ·····5·. ·]·I····
0030  00 00 00 00 00 01 03 6b  70 75 02 61 63 02 6b 72   ·······k pu·ac·kr
0040  00 00 01 00 01 00 00 29  02 00 00 00 00 00 00 00   ·······) ········
```

04 결과(2)


```
**********************UDP Packet*************************

IP Header
   |-IP Version        : 4
   |-IP Header Length  : 5 DWORDS or 20 Bytes
   |-Type Of Service   : 0
   |-IP Total Length   : 82  Bytes(Size of Packet)
   |-Identification    : 46094
   |-TTL      : 128
   |-Protocol : 17
   |-Checksum : 13494
   |-Source IP        : 192.168.232.2
   |-Destination IP   : 192.168.232.130

UDP Header
   |-Source Port      : 53
   |-Destination Port : 45053
   |-UDP Length       : 62
   |-UDP Checksum     : 47860

IP Header
    45 00 00 52 B4 0E 00 00 80 11 34 B6 C0 A8 E8 02         E..R....□□.4.....
    C0 A8 E8 82                                             ....
UDP Header
    00 35 AF FD 00 3E BA F4                                 .5...>..
Data Payload
    C1 49 81 80 00 01 00 01 00 00 00 01 03 6B 70 75         .I.□□.........kpu
    02 61 63 02 6B 72 00 00 01 00 01 C0 0C 00 01 00         .ac.kr..........
    01 00 00 00 05 00 04 D2 5D 30 33 00 00 29 10 00         ........]03..)..
    00 00 00 05 00 00                                       ......

###########################################################
```

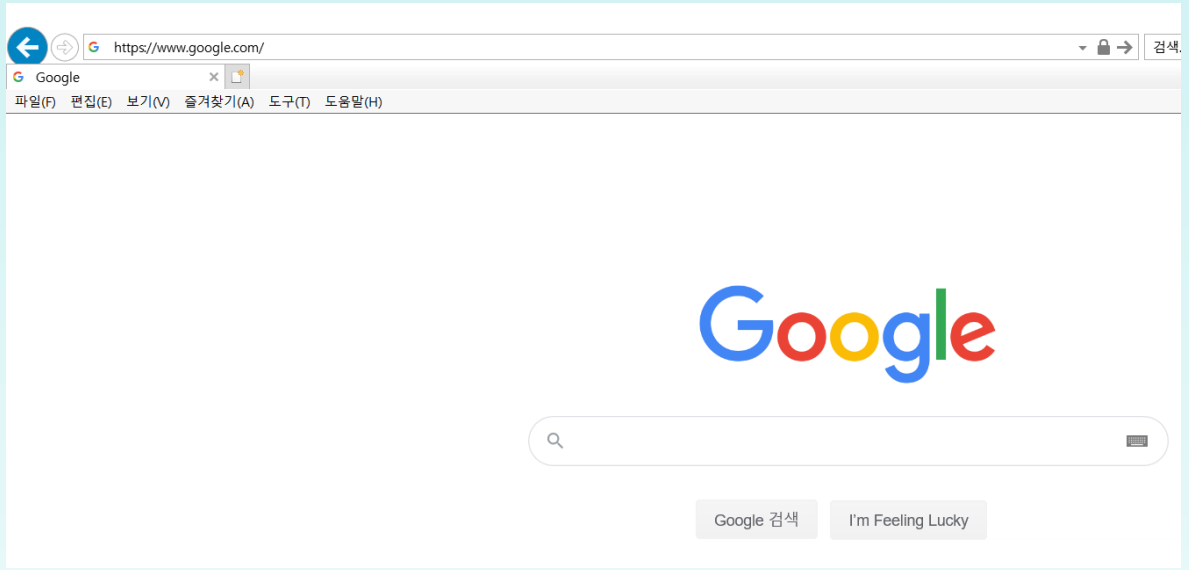
Wireshark · Packet 4 · ens33

```
▸ Frame 4: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 0
▸ Ethernet II, Src: Vmware_f8:ce:62 (00:50:56:f8:ce:62), Dst: Vmware_51:54:1f (00:0c:29:51:54:1f)
▾ Internet Protocol Version 4, Src: 192.168.232.2, Dst: 192.168.232.130
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 82
    Identification: 0xb40e (46094)
  ▸ Flags: 0x0000
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x34b6 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.232.2
    Destination: 192.168.232.130
▾ User Datagram Protocol, Src Port: 53, Dst Port: 45053
    Source Port: 53
    Destination Port: 45053
    Length: 62
    Checksum: 0xbaf4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
▾ Domain Name System (response)
    Transaction ID: 0xc149
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▸ Answers
  ▸ Additional records
    [Request In: 3]
    [Time: 0.004859958 seconds]
```

```
0000  00 0c 29 51 54 1f 00 50  56 f8 ce 62 08 00 45 00   ··)QT··P V··b··E·
0010  00 52 b4 0e 00 00 80 11  34 b6 c0 a8 e8 02 c0 a8   ·R····· 4·······
0020  e8 82 00 35 af fd 00 3e  ba f4 c1 49 81 80 00 01   ···5···> ···I····
0030  00 01 00 00 00 01 03 6b  70 75 02 61 63 02 6b 72   ·······k pu·ac·kr
0040  00 00 01 00 01 c0 0c 00  01 00 01 00 00 00 05 00   ········ ········
0050  04 d2 5d 30 33 00 00 29  10 00 00 00 00 05 00 00   ··]03··) ········
```

04 설계 내용

icmp



www.google.com 웹 주소를 사용한다. (172.217.161.78)

VM Ware에서 ping 명령어를 실행 한다.

Raw Socket 프로그램 실행 후 log 파일 분석

패킷 캡처 후에 IP 헤더 정보, ICMP 헤더 정보, IP 내용 일부를 분석후 비교 (Echo message 분석)

04 결과(1)

```
**********************ICMP Packet*************************

IP Header
   |-IP Version        : 4
   |-IP Header Length  : 5 DWORDS or 20 Bytes
   |-Type Of Service   : 0
   |-IP Total Length   : 84  Bytes(Size of Packet)
   |-Identification    : 17321
   |-TTL      : 64
   |-Protocol : 1
   |-Checksum : 65452
   |-Source IP        : 192.168.232.130
   |-Destination IP   : 172.217.161.78

ICMP Header
   |-Type : 8   |-Checksum : 15200
   |-Code : 0
   |-ID       : 2477
   |-Sequence : 1

IP Header
    45 00 00 54 43 A9 40 00 40 01 FF AC C0 A8 E8 82         E..TC.@.@.......
    AC D9 A1 4E                                             ...N
ICMP Header
    08 00 3B 60 09 AD 00 01                                 ..;`....
Data Payload
    64 BB E8 5D 00 00 00 00 9A 05 0D 00 00 00 00 00         d..]...........
    10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F         ................
    20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F          !"#$%&'()*+,-./
    30 31 32 33 34 35 36 37                                 01234567

###############################################################
```

Wireshark · Packet 18 · ens33

```
▸ Frame 18: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on inte
▸ Ethernet II, Src: Vmware_51:54:1f (00:0c:29:51:54:1f), Dst: Vmware_f8:ce:62
▾ Internet Protocol Version 4, Src: 192.168.232.130, Dst: 172.217.161.78
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x43a9 (17321)
  ▸ Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xffac [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.232.130
    Destination: 172.217.161.78
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x3b60 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2477 (0x09ad)
    Identifier (LE): 44297 (0xad09)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Response frame: 19]
    Timestamp from icmp data: Dec  5, 2019 17:10:12.000000000 KST
    [Timestamp from icmp data (relative): 0.856598632 seconds]
  ▾ Data (48 bytes)
      Data: 9a050d0000000000101112131415161718191a1b1c1d1e1f...
      [Length: 48]

0000  00 50 56 f8 ce 62 00 0c  29 51 54 1f 08 00 45 00   ·PV··b·· )QT···E·
0010  00 54 43 a9 40 00 40 01  ff ac c0 a8 e8 82 ac d9   ·TC·@·@· ........
0020  a1 4e 08 00 3b 60 09 ad  00 01 64 bb e8 5d 00 00   ·N··;`·· ··d··]··
0030  00 00 9a 05 0d 00 00 00  00 00 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                             67
```

04 결과(2)


```
**********************ICMP Packet*************************

IP Header
   |-IP Version        : 4
   |-IP Header Length  : 5 DWORDS or 20 Bytes
   |-Type Of Service   : 0
   |-IP Total Length   : 84  Bytes(Size of Packet)
   |-Identification    : 46110
   |-TTL      : 128
   |-Protocol : 1
   |-Checksum : 36663
   |-Source IP        : 172.217.161.78
   |-Destination IP   : 192.168.232.130

ICMP Header
   |-Type : 0  (ICMP Echo Reply)
   |-Checksum : 17248
   |-Code : 0
   |-ID       : 2477
   |-Sequence : 1

IP Header
    45 00 00 54 B4 1E 00 00 80 01 8F 37 AC D9 A1 4E         E..T....[..]..7...N
    C0 A8 E8 82                                          ....
ICMP Header
    00 00 43 60 09 AD 00 01                              ..C`....
Data Payload
    64 BB E8 5D 00 00 00 00 9A 05 0D 00 00 00 00 00      d..]..............
    10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F      ................
    20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F       !"#$%&'()*+,-./
    30 31 32 33 34 35 36 37                              01234567

###############################################################
```

Wireshark · Packet 19 · ens33

```
▸ Frame 19: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on inte
▸ Ethernet II, Src: Vmware_f8:ce:62 (00:50:56:f8:ce:62), Dst: Vmware_51:54:1f
▾ Internet Protocol Version 4, Src: 172.217.161.78, Dst: 192.168.232.130
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xb41e (46110)
  ▸ Flags: 0x0000
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x8f37 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.217.161.78
    Destination: 192.168.232.130
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x4360 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2477 (0x09ad)
    Identifier (LE): 44297 (0xad09)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Request frame: 18]
    [Response time: 40.432 ms]
    Timestamp from icmp data: Dec  5, 2019 17:10:12.000000000 KST
    [Timestamp from icmp data (relative): 0.897030645 seconds]
  ▾ Data (48 bytes)
      Data: 9a050d0000000000101112131415161718191a1b1c1d1e1f...
      [Length: 48]
```

```
0000  00 0c 29 51 54 1f 00 50  56 f8 ce 62 08 00 45 00   ··)QT··P V··b··E·
0010  00 54 b4 1e 00 00 80 01  8f 37 ac d9 a1 4e c0 a8   ·T······ ·7···N··
0020  e8 82 00 00 43 60 09 ad  00 01 64 bb e8 5d 00 00   ····C`·· ··d··]··
0030  00 00 9a 05 0d 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                             67
```

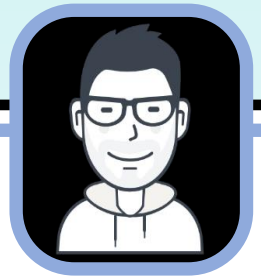
05 실적

월 / 일정	10월	11월	12월
1주차		Wireshark 설치 및 실행 방법 공부(그룹 스터디)	프로그램 결과 확인 및 PPT 작성
2주차		개발 및 시연 환경 구축	최종 발표 준비
3주차		캡쳐 프로그램 자료 수집 및 실행 해보기 2차 발표 준비 및 PPT 작성	
4주차		2차 발표 캡쳐 분석 프로그램 개발	
5주차	팀원 구성	캡쳐 분석 프로그램 개발 리눅스 환경에서 구동 및 오류 검사	

06 역할 분장

한승우

회의 일정 조율
PPT 작성
패킷 캡쳐 분석 프로
그램 개발
최종 발표



김지우

설계 환경 구축
패킷 캡쳐 분석 프로
그램 개발
시연

전유미

PPT 작성
패킷 캡쳐 분석 프로
그램 코드 수집
패킷 캡쳐 분석 프로
그램 개발

정하림

설계 환경 구축
패킷 캡쳐 분석 프로
그램 개발
중간 발표

07 문제점과 해결책

- ✓ 캡쳐 프로그램 개발을 하는 데에 애를 먹었음 -> 여러 코드들을 수집하여 수정 및 개발
- ✓ 조원의 노트북 사양에 따른 시연/설계 환경 구축 -> 팀원들 중 가장 사양이 좋은 컴퓨터에서 시연하기로 결정
- ✓ Wire shark 작동법 미숙 -> 조원들 간의 그룹 스터디로 문제 해결
- ✓ 패킷 분석에 대한 이해력 부족으로 많은 학습이 필요

08 교훈

- ✓ 처음에는 어렵게 느껴졌던 패킷 분석이 공부를 하면서 이해가 되었고, 네트워크 보안 쪽에 조금 관심이 생겼다.
- ✓ 나도 모르게 네트워크상에 흐르던 수많은 패킷들을 직접 캡쳐 해보며 수업시간에 배운 내용이 실제로는 어떤 흐름을 가지는지 확인할 수 있어 유익했다.
- ✓ 패킷을 직접 분석하면서 TCP 원리에 대해 더 잘 이해할 수 있게 되었고, 우리가 사용하는 네트워크에 대해 더 깊이 있게 공부할 수 있었다.
- ✓ Wireshark를 처음 만지며 네트워크라는 분야에 한발짝 다가갈 수 있었고, 다양한 프로토콜을 다루며 실제 동작하는 내용을 살펴볼 수 있어 어렵지만 큰 배움의 시간이었다.

시연

Q&A

감사합니다☺