# 시스템, 네트워크 모니터링을 통한 보안 강화

네트워크의 미래를 제시하는 세미나 **NetFocus 2003 :**
**IT** 관리자를 위한 네트워크 보안 방법론

on the NET
Network Intelligence for Leading Networkers

㈜피지피넷 / 팀장
나 병 윤
dewymoon@pgpnet.com

# 주요 내용

시스템 모니터링

- 패킷 크기와 장비의 **CPU** 및 **Memory** 사용량
- **SNMP**를 장비의 상태 관찰

비 정상적인 트래픽 모니터링

- **Packet** 분석기의 다양한 트래픽 모니터링 도구를 이용한 비 정상적인 트래픽 관찰
- **Traffic Gauge, Host** 트래픽, **Matrix** 트래픽 등등

비 정상적인 패킷 분석

- 비 정상적인 트래픽을 유발 시키는 패킷 캡처
- 패킷 패턴 분석
- 보안 침투 및 바이러스 발생지 추적

# 시스템 모니터링

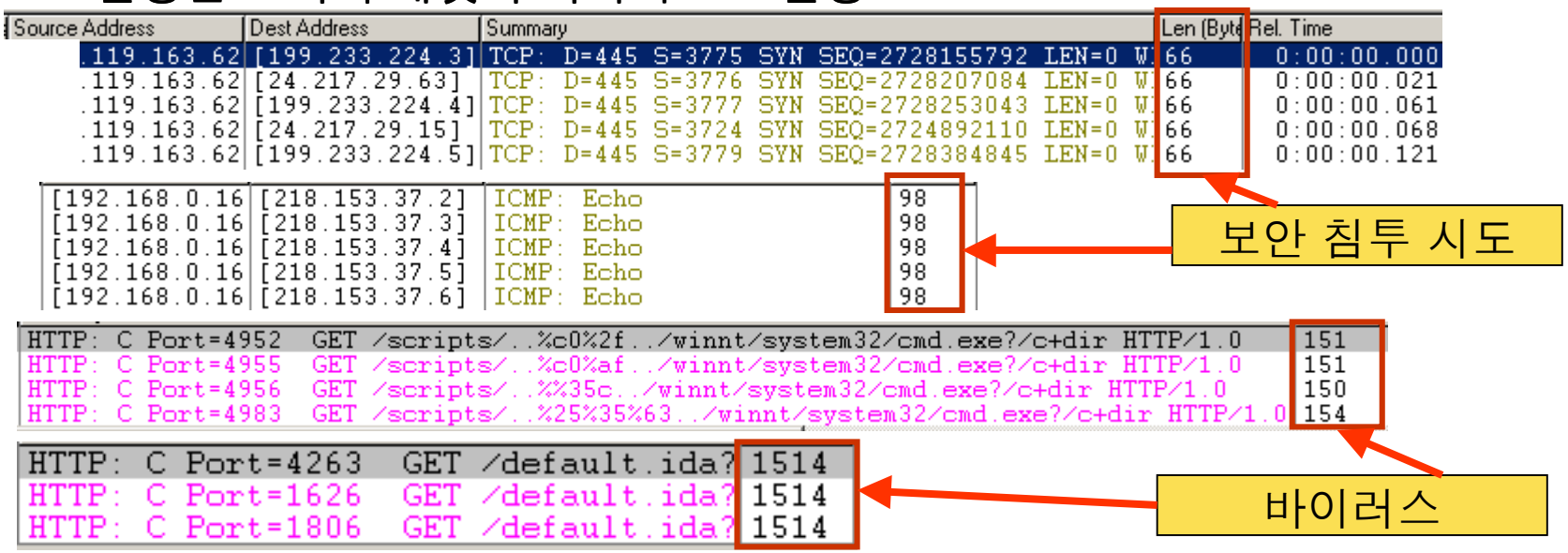
## 패킷 크기별 최대 전송속도

- 최대 전송량 및 최소 패킷 크기
  - ⇢ 100Mbps 네트워크 : 12,500,000 bytes/s
- 최소 패킷 크기
  - ⇢ 최소 데이터 프레임 : 64 bytes
    - ➨ DLC header + IP header + TCP/UDP header + CRC
  - ⇢ Frame gap : 12 bytes, Preamble : 8 bytes
  - ⇢ 최소 패킷 크기 : 64 + 12 + 8 = 84 bytes
  - ⇢ 가능한 전송 속도 : 100Mbps -> 148,800 packets/sec
- 최대 패킷 크기
  - ⇢ 최대 데이터 프레임 : 1518 bytes
  - ⇢ 최대 패킷 크기 : 1518 + 12 + 8 = 1538 bytes
  - ⇢ 가능한 전송 속도 : 8,127 packets/sec
- 대역폭 효율성
  - 64 bytes : 64 / 84 = 0.76 따라서 76%
  - 1518 bytes : 1518/1538 = 0.986 따라서 약 98%

# 시스템 모니터링

보안 침투 및 바이러스에 의한 패킷 특징

- 일정한 크기의 패킷이 지속적으로 발생




패킷 크기와 장비에 대한 영향

- 작은 패킷**(64~128)**이 많은 경우

  ⇢ CPU 과부하 유발 : Layer 2 장비 < Layer 3 장비 < Layer 4 장비 …

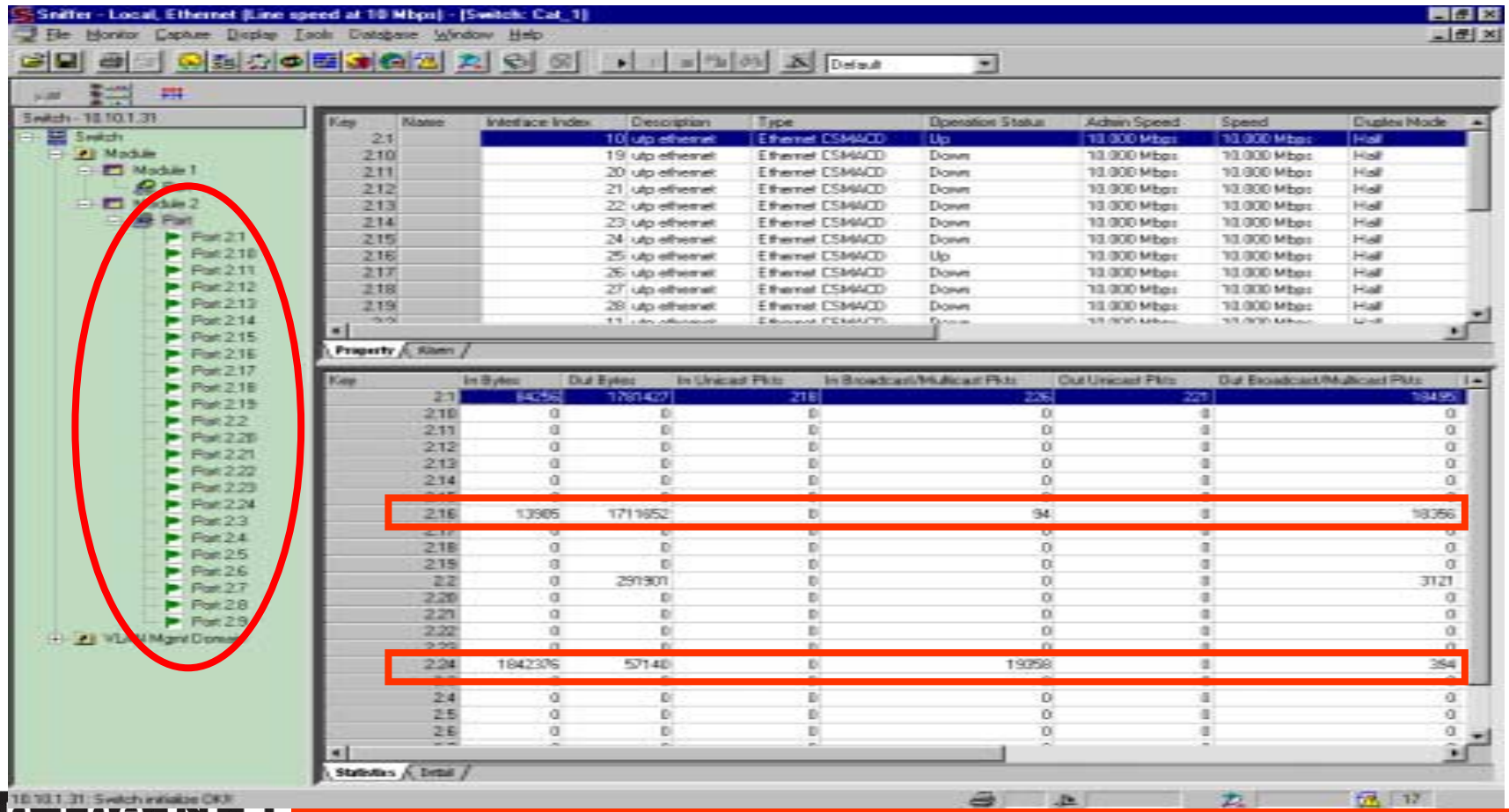
- 큰 패킷**(1024 ~)**이 많은 경우

  ⇢ Memory 처리 용량 초과 및 대역폭 Full

# 시스템 모니터링

**SNMP**를 이용한 장비의 상태 관찰

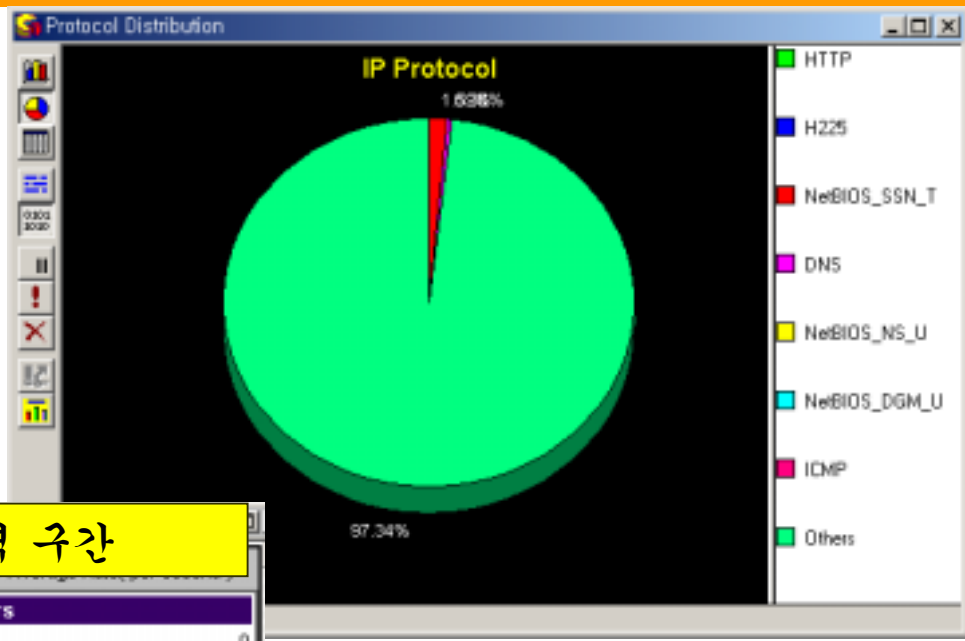
- **CPU** 및 **Memory** 사용량 수시 관찰
- 장비의 포트 트래픽 상태 관찰 **(**패킷 수와 바이트 수 비교 관찰**)**



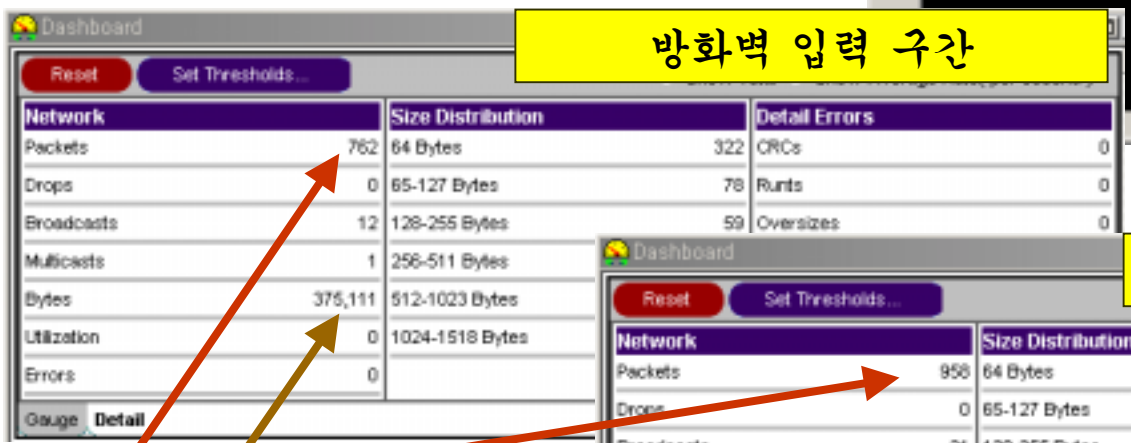
# 시스템 모니터링

## 파이어월 트래픽

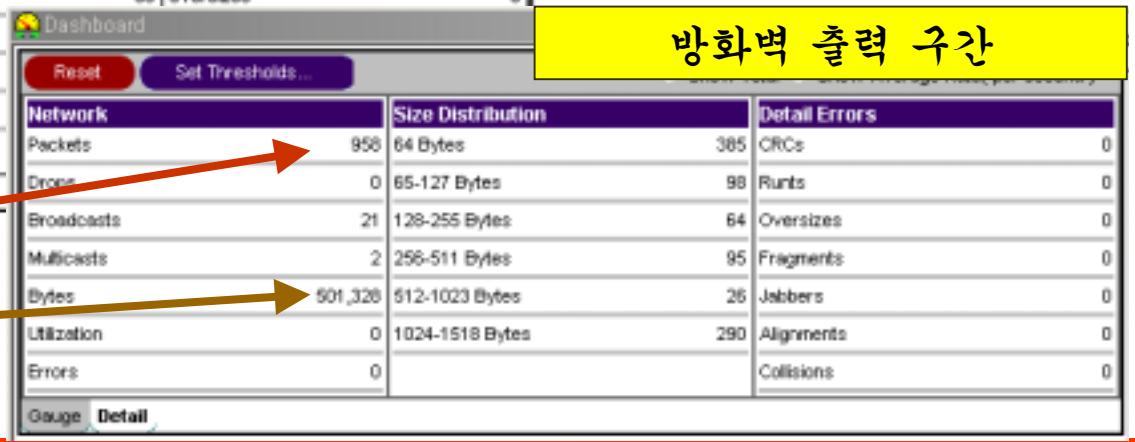
- 트래픽 차단 상태 관찰
  - 포트별 트래픽 량 및 패킷 개수 관찰
- 어플리케이션 포트 차단 상태 관찰
  - 관측되는 어플리케이션 프로토콜 현황




방화벽 입력 구간



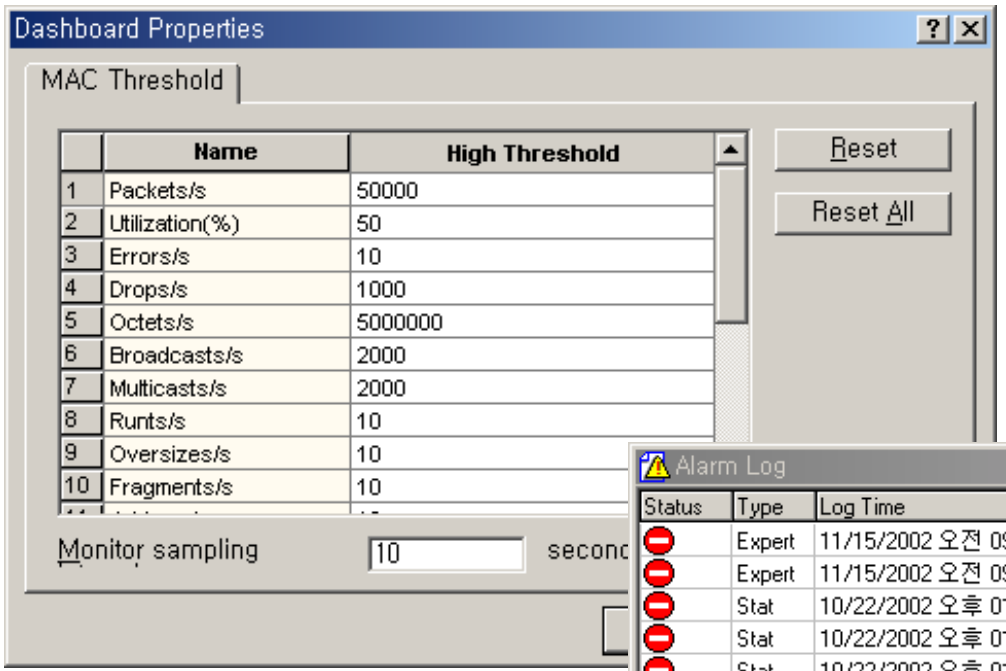

방화벽 출력 구간

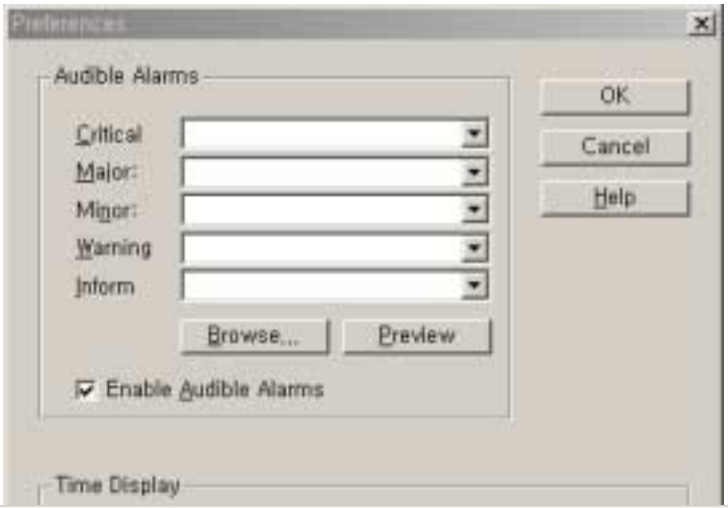


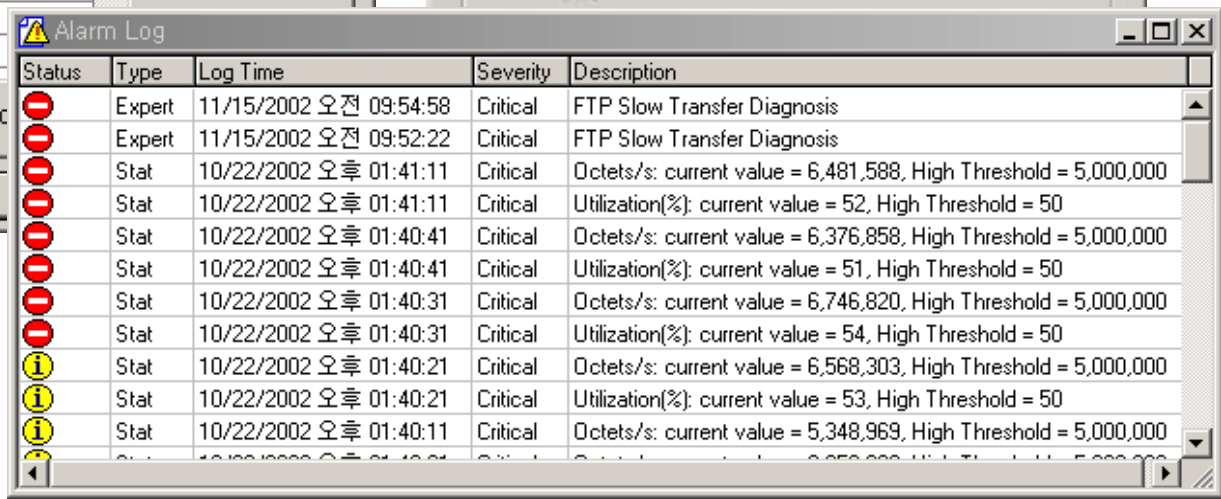
# 비정상적인 트래픽 모니터링

다양한 알람 기능 활용

- 알람 임계 값**(threshold)**을 자신의 네트워크 상황에 맞게 수정
- 알람의 중요도에 따라서 다양한 소리 설정

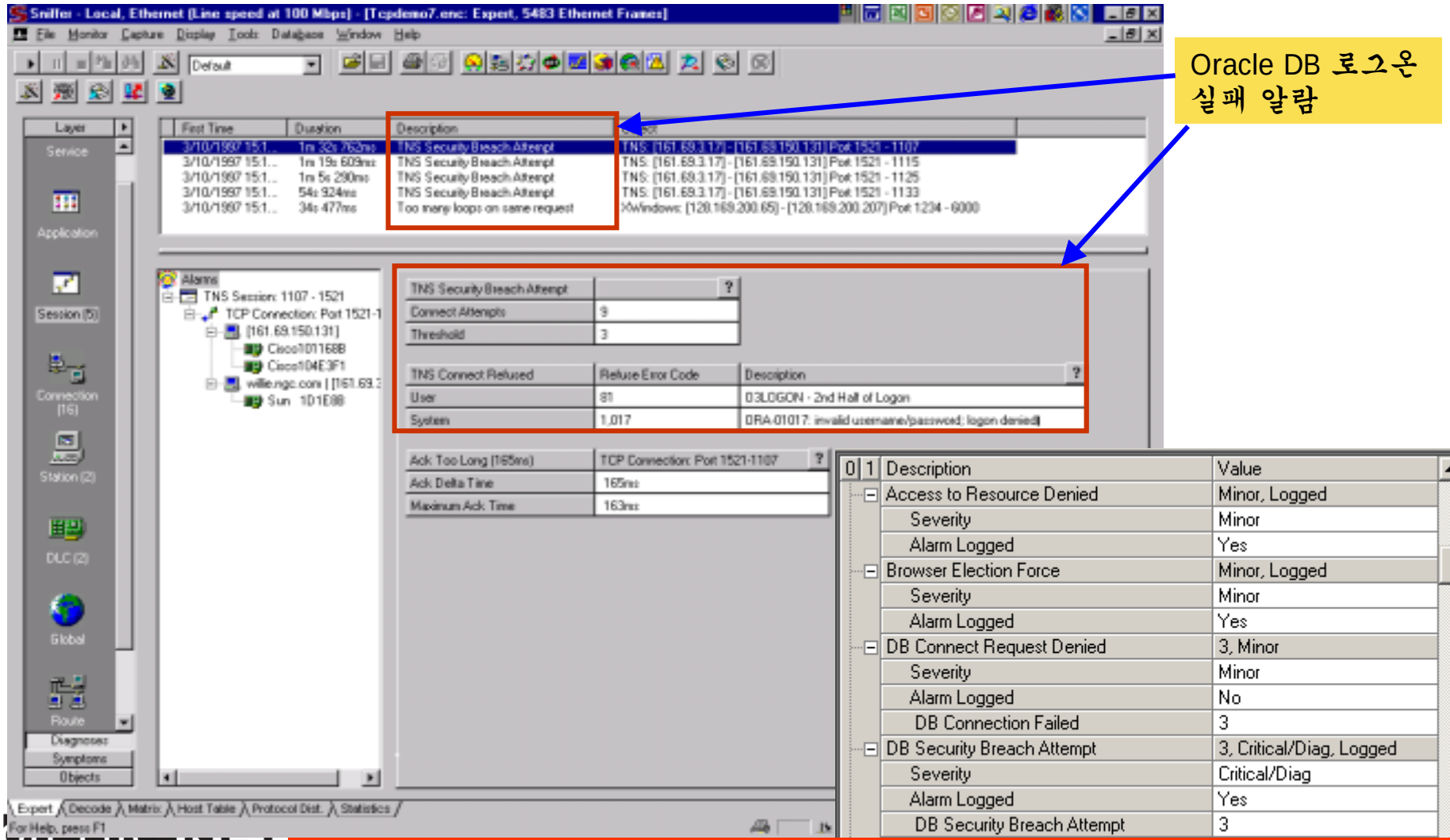


# 비정상적인 트래픽 모니터링

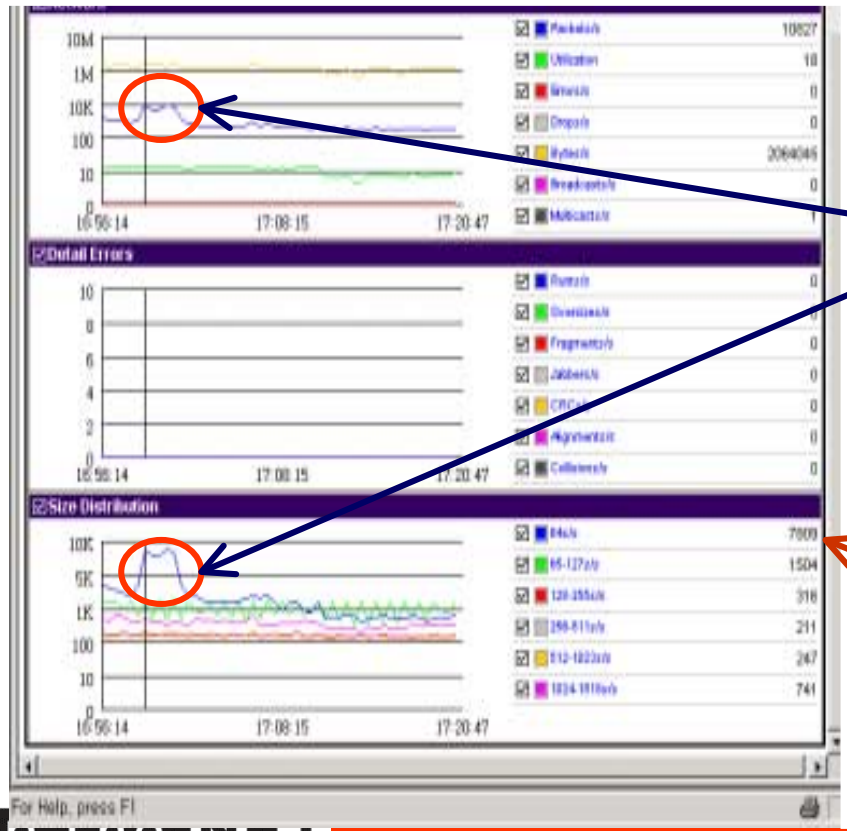
패킷 분석 시스템



# 비정상적인 트래픽 모니터링

## 전체 트래픽 및 특정 시스템의 트래픽 관찰

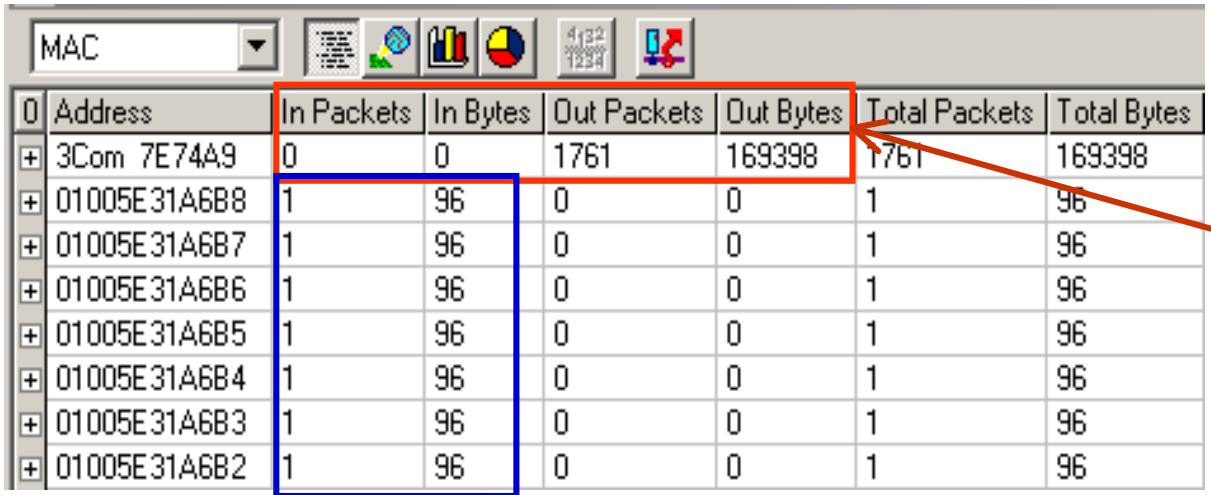
- 보안 침투 시도 및 바이러스 활동 확인
  - ⇢ 크기가 127Bytes 이하인 패킷이 많이 발생하는 경우
  - ⇢ 한 MAC 주소가 알 수 없는 많은 MAC 주소로 패킷을 전달만 하는 경우(순차적 진행)
  - ⇢ 한 IP 주소가 알 수 없는 또는 내부 모든 IP 대역으로 동일한 크기의 패킷을 전달 하는 경우




보안 침투 시도 또는 바이러스 활동 시간

총 **10827**개의 패킷 가운데 **64 bytes** 패킷이 **7809**개 발생**??**

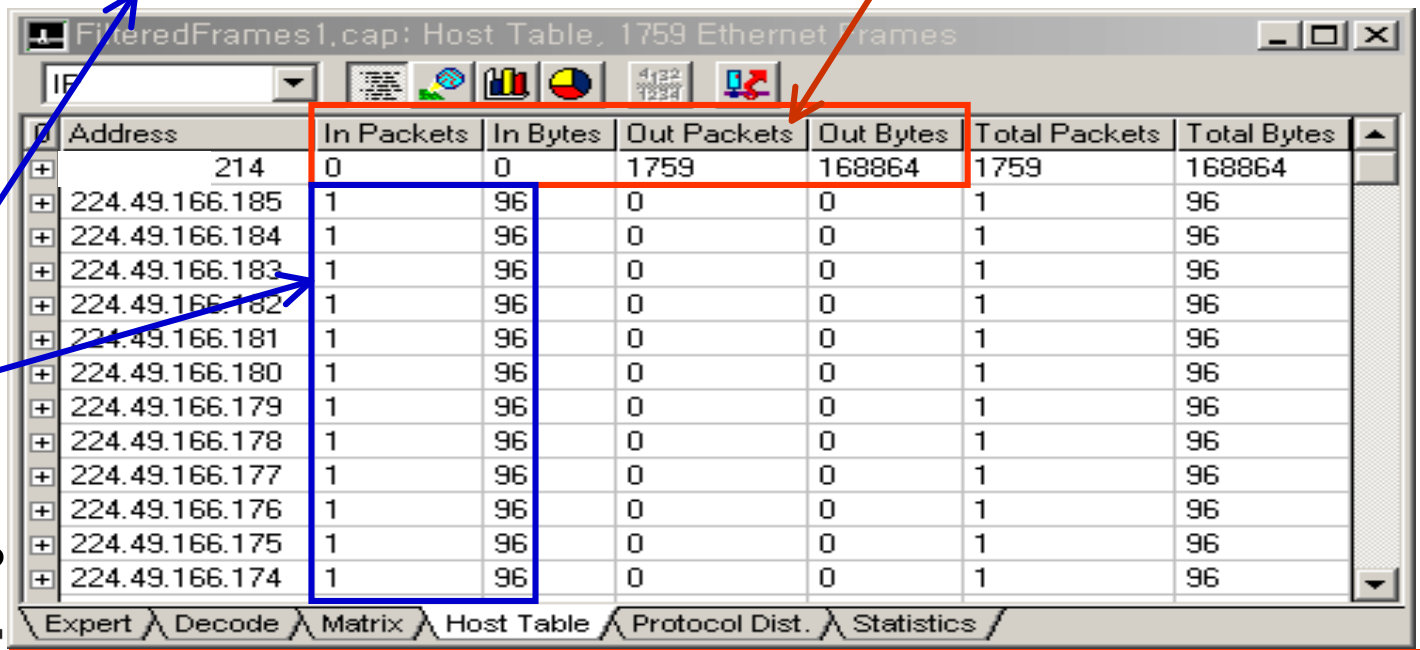
# 비정상적인 트래픽 모니터링




Out Packets or In Packets 으로 정렬(sorting)

송신되는 패킷만 있고 수신되는 패킷은 없다?

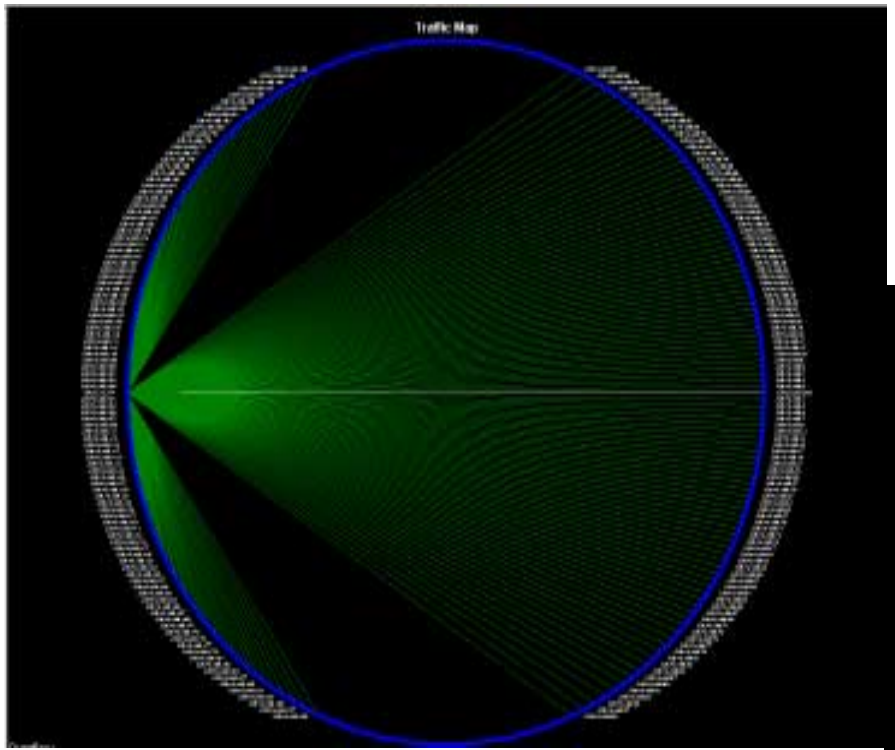
발생지 확인



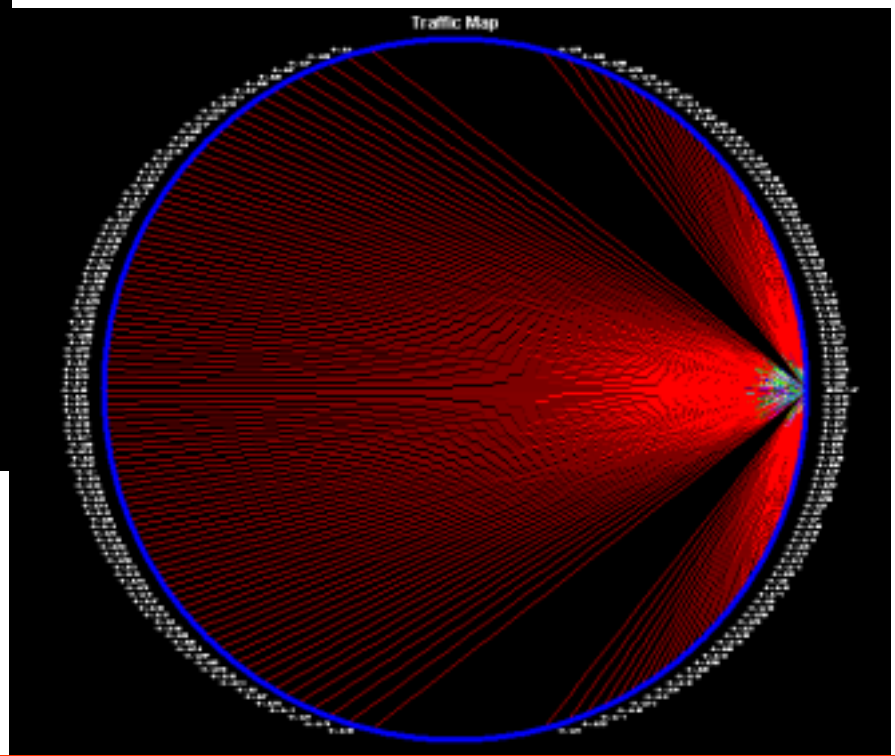

수신되는 패킷만 있고 송신되는 패킷은 없다?

# 비정상적인 트래픽 모니터링

## 두 시스템간의 트래픽 관찰




- Source MAC 주소 및 Destination MAC 주소는 1개
- Source IP 주소가 N개 이고 Destination IP 주소는 1개




- Source MAC, IP 주소는 1개, Destination MAC, IP 주소는 N개 인 경우

# 비정상적인 트래픽 모니터링

MAC

| 0 | Host 1 | Packets | Bytes | Bytes | Packets | Host 2 | Total Pkts | Total Bytes |
|---|---|---|---|---|---|---|---|---|
| + | 7E74A9 | 2 | 534 | 0 | 0 | Broadcast | 2 | 534 |
| + | 7E74A9 | 1 | 96 | 0 | 0 | 01005E31A6B9 | 1 | 96 |
| + | 7E74A9 | 1 | 96 | 0 | 0 | 01005E31A6B8 | 1 | 96 |
| + | 7E74A9 | 1 | 96 | 0 | 0 | 01005E31A6B7 | 1 | 96 |
| + | 7E74A9 | 1 | 96 | 0 | 0 | 01005E31A6B6 | 1 | 96 |
| + | 7E74A9 | 1 | 96 | 0 | 0 | 01005E31A6B5 | 1 | 96 |
| + | 7E74A9 | 1 | 96 | 0 | 0 | 01005E31A6B4 | 1 | 96 |
| + | 7E74A9 | 1 | 96 | 0 | 0 | 01005E31A6B3 | 1 | 96 |
| + | 7E74A9 | 1 | 96 | 0 | 0 | 01005E31A6B2 | 1 | 96 |

• Source MAC, IP 주소는 1개, Destination MAC, IP 주소는 N개 인 경우

IP

| 0 | Host 1 | Packets | Bytes | Bytes | Packets | Host 2 | Total Pkts | Total Bytes |
|---|---|---|---|---|---|---|---|---|
| + | 22.12.214 | 1 | 96 | 0 | 0 | 224.49.166.185 | 1 | 96 |
| + | 22.12.214 | 1 | 96 | 0 | 0 | 224.49.166.184 | 1 | 96 |
| + | 22.12.214 | 1 | 96 | 0 | 0 | 224.49.166.183 | 1 | 96 |
| + | 22.12.214 | 1 | 96 | 0 | 0 | 224.49.166.182 | 1 | 96 |
| + | 22.12.214 | 1 | 96 | 0 | 0 | 224.49.166.181 | 1 | 96 |
| + | 22.12.214 | 1 | 96 | 0 | 0 | 224.49.166.180 | 1 | 96 |
| + | 22.12.214 | 1 | 96 | 0 | 0 | 224.49.166.179 | 1 | 96 |
| + | 22.12.214 | 1 | 96 | 0 | 0 | 224.49.166.178 | 1 | 96 |
| + | 22.12.214 | 1 | 96 | 0 | 0 | 224.49.166.177 | 1 | 96 |

MAC

| 0 | Host 1 | Packets | Bytes | Bytes | Packets | Host 2 | Total Pkts | Total Bytes |
|---|---|---|---|---|---|---|---|---|
| + | RealtkE7989D | 67805 | 5288790 | 0 | 0 | FutSys841649 | 67805 | 5288790 |

• Source MAC 주소 및 Destination MAC 주소는 1개

• Source IP 주소가 N개이고 Destination IP 주소는 1개

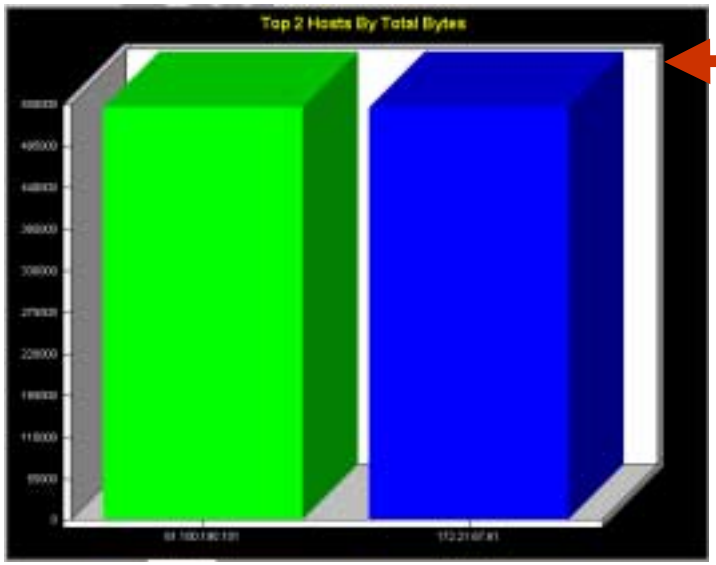
IP

| 0 | Host 1 | Packets | Bytes | Bytes | Packets | Host 2 | Total Pkts | Total Bytes |
|---|---|---|---|---|---|---|---|---|
| + | 1.0.101 | 305 | 23790 | 0 | 0 | 169.204.171.67 | 305 | 23790 |
| + | 1.0.135 | 304 | 23712 | 0 | 0 | 169.204.171.67 | 304 | 23712 |
| + | 1.0.86 | 304 | 23712 | 0 | 0 | 169.204.171.67 | 304 | 23712 |
| + | 1.0.217 | 300 | 23400 | 0 | 0 | 169.204.171.67 | 300 | 23400 |
| + | 1.0.108 | 300 | 23400 | 0 | 0 | 169.204.171.67 | 300 | 23400 |
| + | 1.0.242 | 299 | 23322 | 0 | 0 | 169.204.171.67 | 299 | 23322 |
| + | 1.0.105 | 298 | 23244 | 0 | 0 | 169.204.171.67 | 298 | 23244 |
| + | 1.0.114 | 298 | 23244 | 0 | 0 | 169.204.171.67 | 298 | 23244 |
| + | 1.0.183 | 298 | 23244 | 0 | 0 | 169.204.171.67 | 298 | 23244 |
| + | 1.0.14 | 296 | 23088 | 0 | 0 | 169.204.171.67 | 296 | 23088 |
| + | 1.0.251 | 296 | 23088 | 0 | 0 | 169.204.171.67 | 296 | 23088 |
| + | 1.0.155 | 295 | 23010 | 0 | 0 | 169.204.171.67 | 295 | 23010 |
| + | 1.0.143 | 293 | 22854 | 0 | 0 | 169.204.171.67 | 293 | 22854 |
| + | 1.0.126 | 293 | 22854 | 0 | 0 | 169.204.171.67 | 293 | 22854 |

# 비정상적인 트래픽 모니터링

두 시스템 간의 트래픽 양이 거의 일치 하는 경우

- 실시간 관찰: Host Table, Matrix의 MAC 또는 IP 계층 테이블
- 패킷 캡처 후 분석




| 0 | Address | In Packets | In Bytes | Out Packets | Out Bytes | Total Packets | Total Bytes |
|---|---|---|---|---|---|---|---|
| + | 61.100.190.101 | 4273 | 273472 | 4268 | 273152 | 8541 | 546624 |
| + | 172.21.67.61 | 4268 | 273152 | 4273 | 273472 | 8541 | 546624 |

| 0 | Host 1 | Packets | Bytes | Bytes | Packets | Host 2 | Total Pkts | Total Bytes |
|---|---|---|---|---|---|---|---|---|
| + | 61.100.190.101 | 4268 | 273152 | 273472 | 4273 | 172.21.67.61 | 8541 | 546624 |

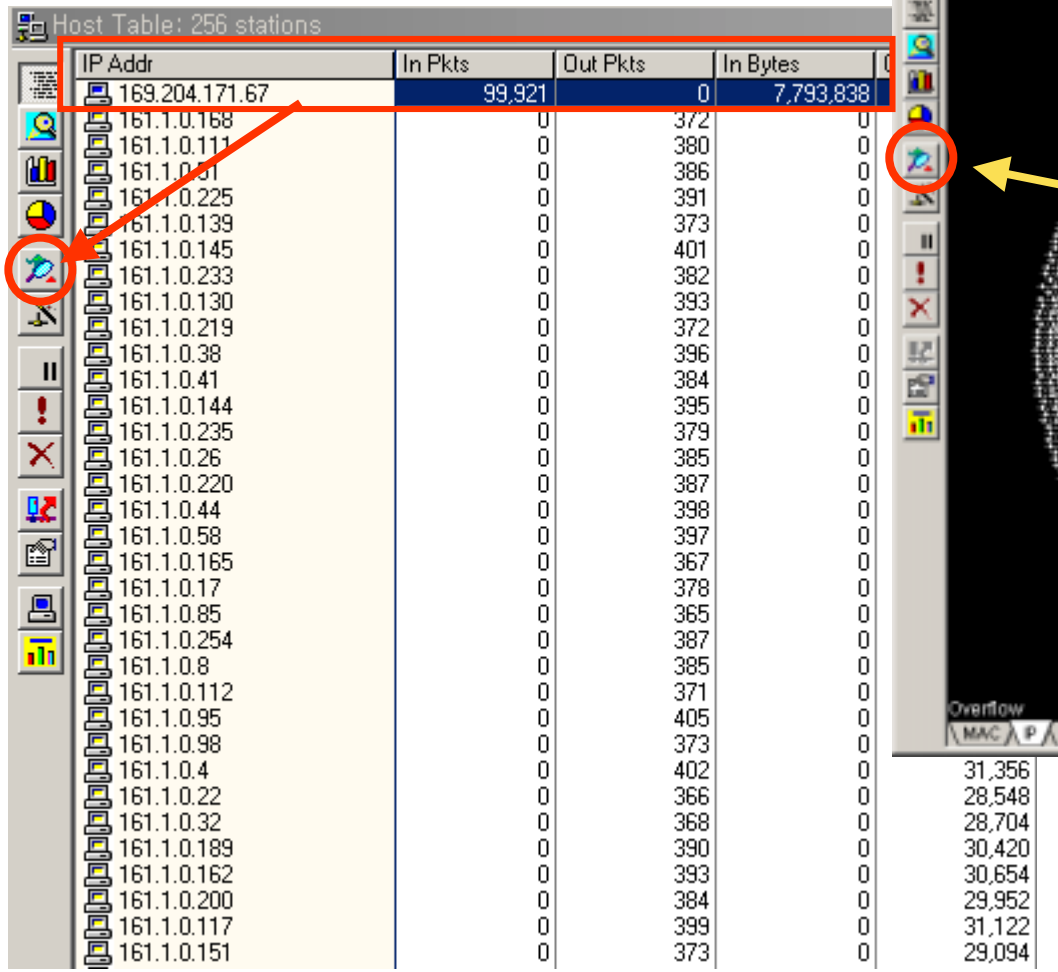
In, Out Packet (Tx, Rx Frames)이 비슷하다??

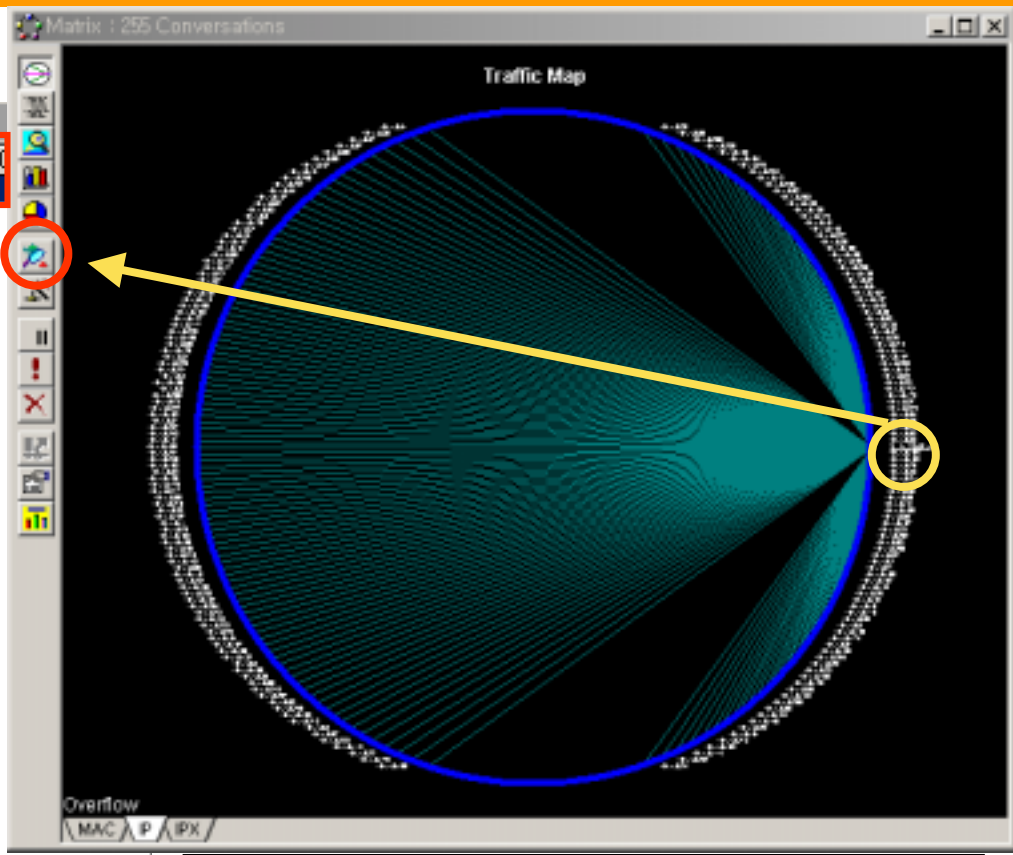
| Layer | Diagnoses | Symptoms | Objects |
|---|---|---|---|
| Service | 0 | 0 | 0 |
| Application | 0 | 0 | 0 |
| Session | 0 | 0 | 0 |
| Connection (1) | 0 | 0 | 1 |
| Station (2) | 0 | 0 | 2 |
| DLC (2) | 0 | 0 | 2 |
| Global (1) | 0 | 0 | 1 |
| Route | 0 | 0 | 0 |
| Subnet (1) | 0 | 0 | 1 |

| Net Station | DLC Station | Rx Frames | Tx Frames | Rx Bytes | Tx Bytes |
|---|---|---|---|---|---|
| [61,100,190,101] | ArwPnt00E3B7 | 4,273 | 4,268 | 171K | 171K |
| [172,21,67,61] | Cisco C8CA09 | 4,268 | 4,273 | 171K | 171K |

# 비 정상적인 패킷 분석

패킷 캡처

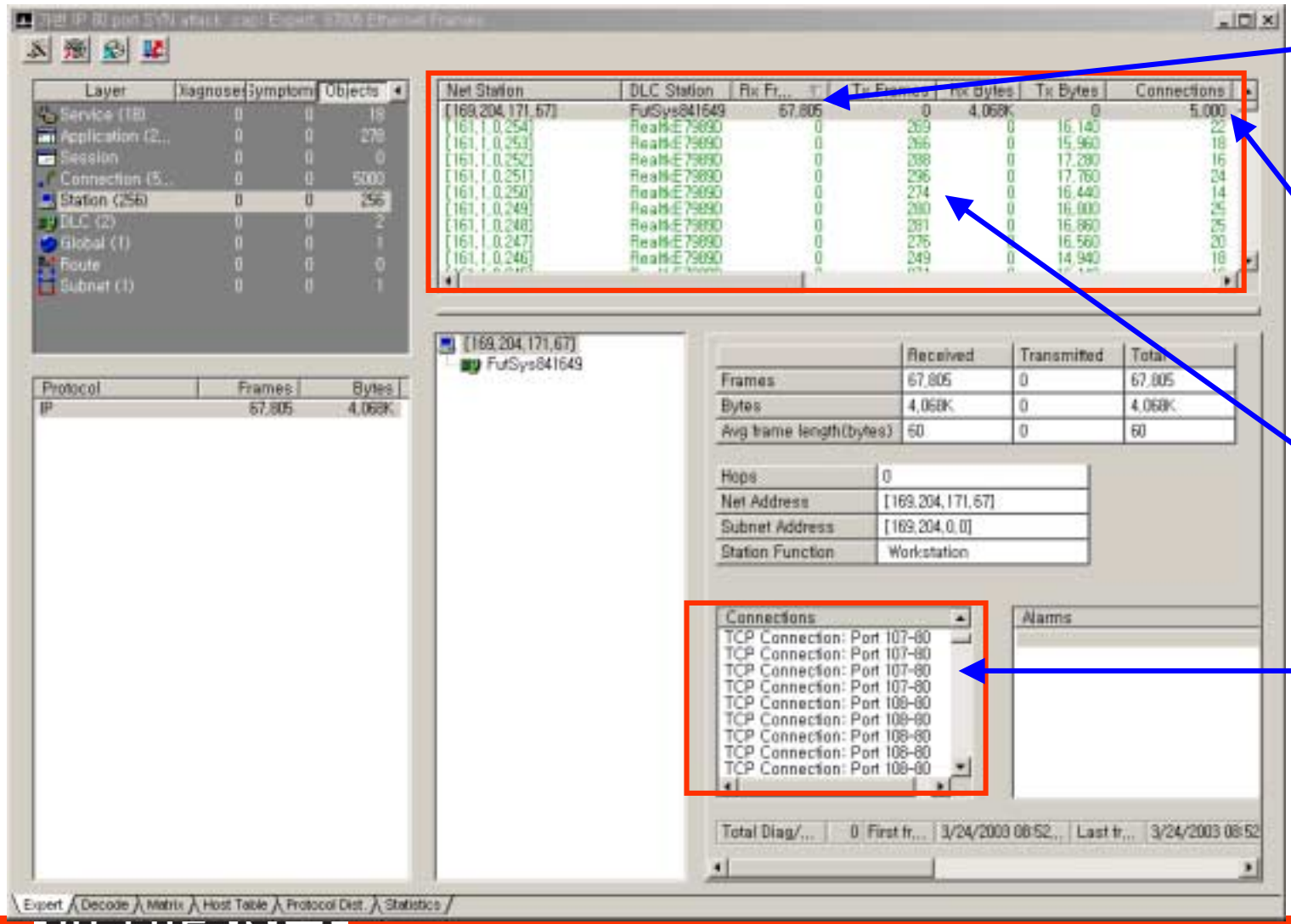



In 또는 Out packets으로 정렬하여 이상 트래픽이 발생하는 경우, Source 또는 Destination이 되는 스테이션을 선택하여 실시간으로 패킷 캡처

# 비 정상적인 패킷 분석

패킷 분석 시스템 활용




Tx는 없는데 Rx만 있다?

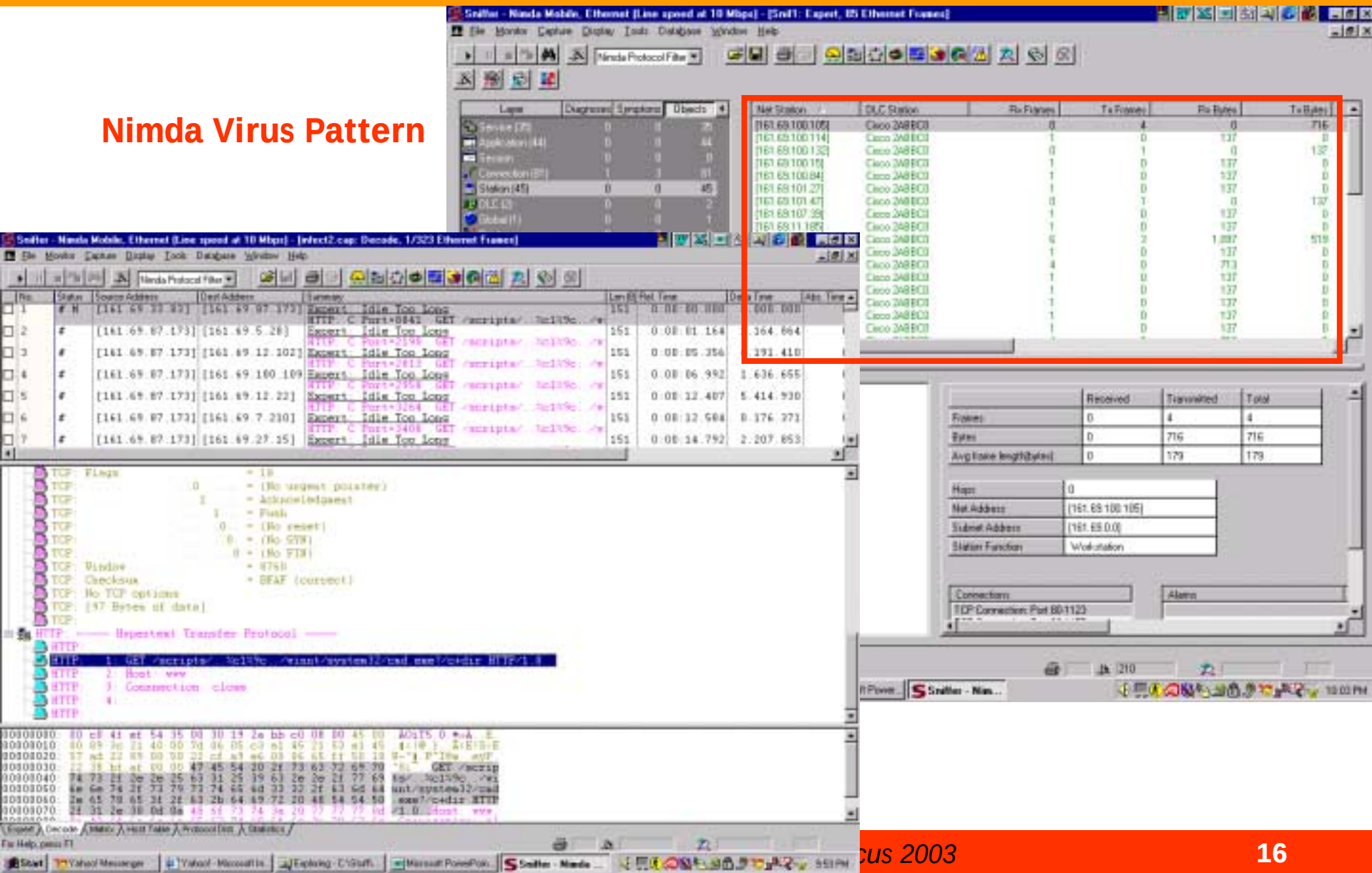
순간적으로 5000번의 접속이 시도되었다?

Tx는 있는데 Rx만 있다?

Source의 포트가 순차적으로 증가한다?

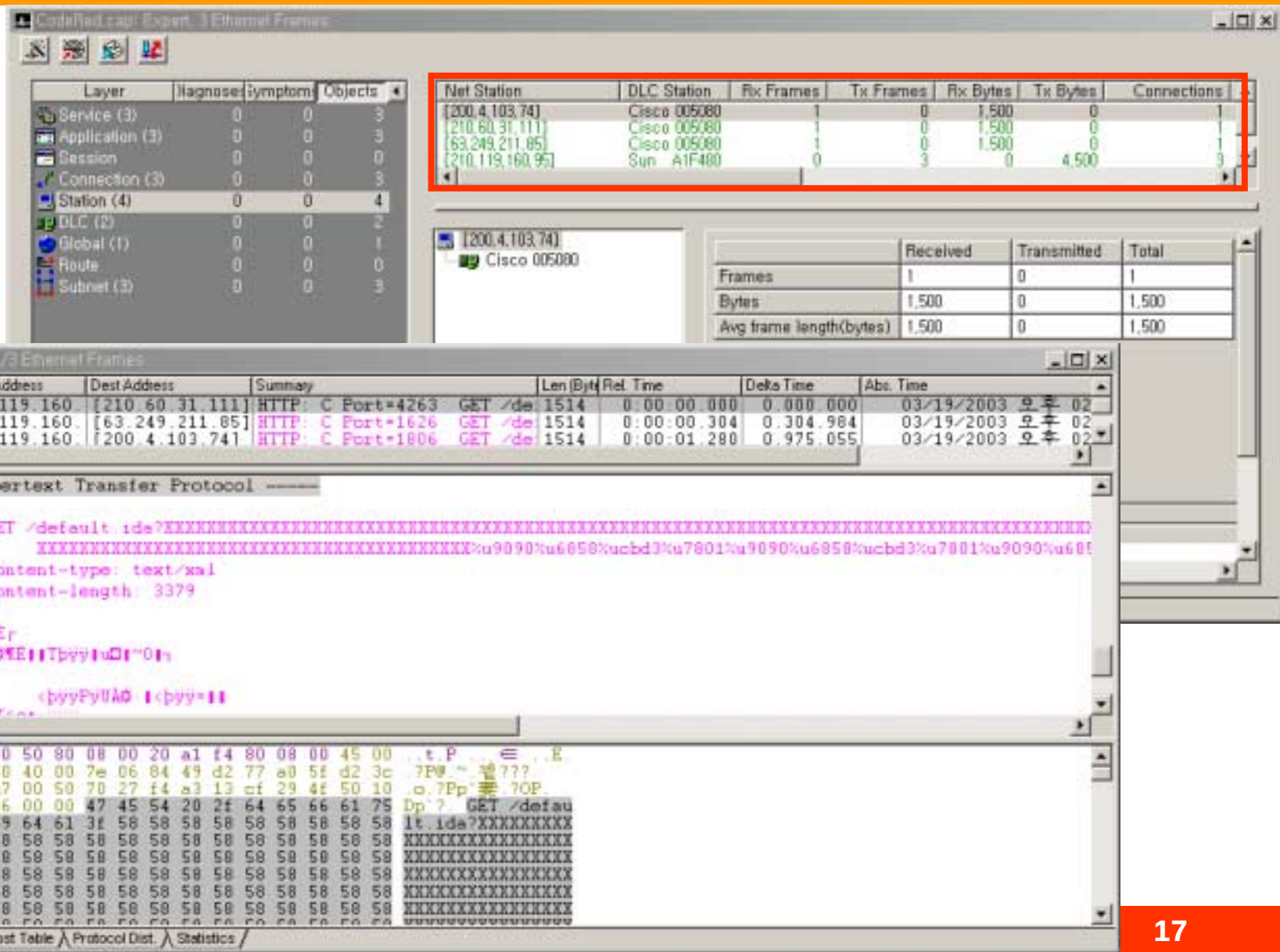
# 비 정상적인 패킷 분석

**Nimda Virus Pattern**



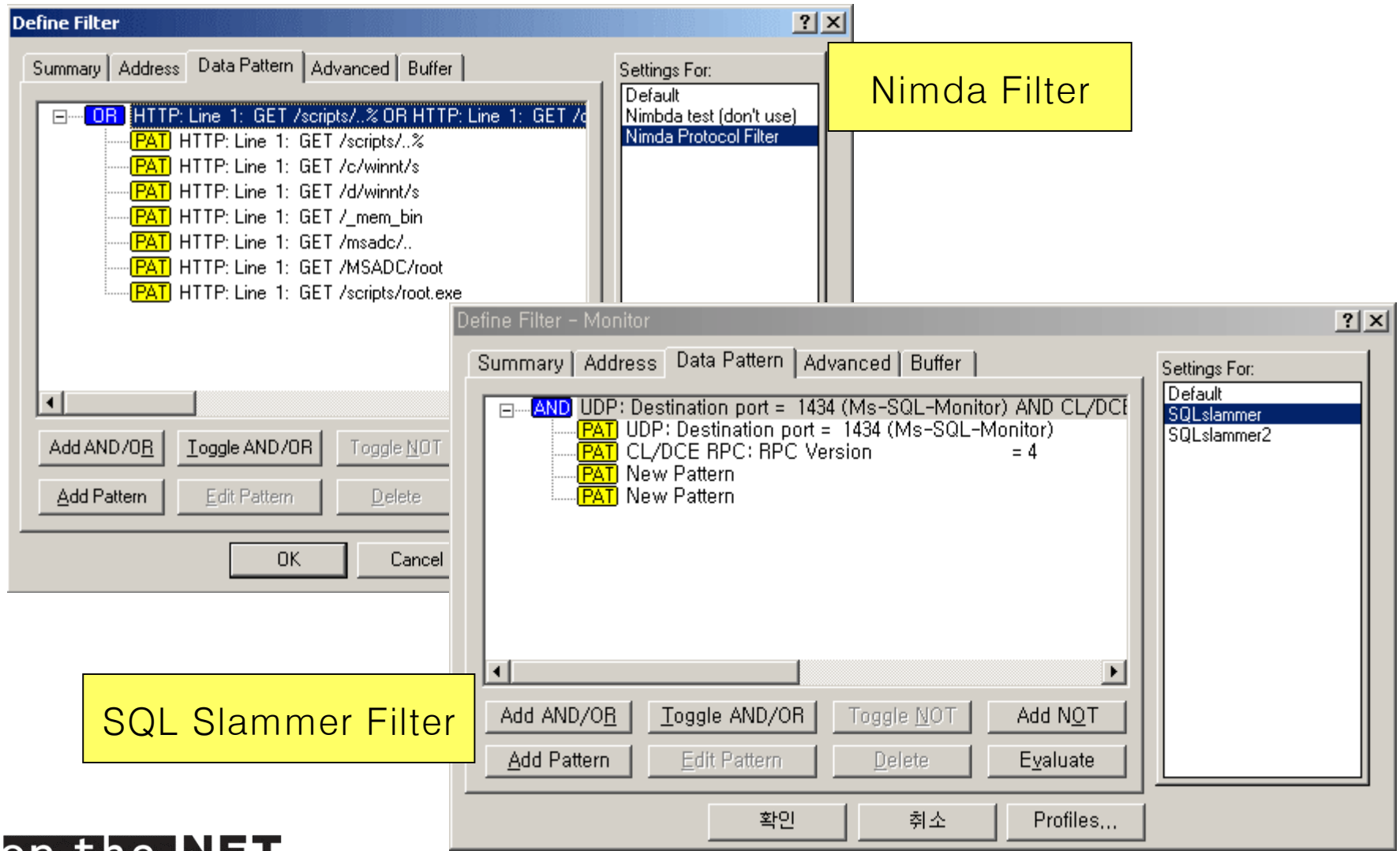
# 비 정상적인 패킷 분석

**Code Red**



# 비 정상적인 패킷 분석

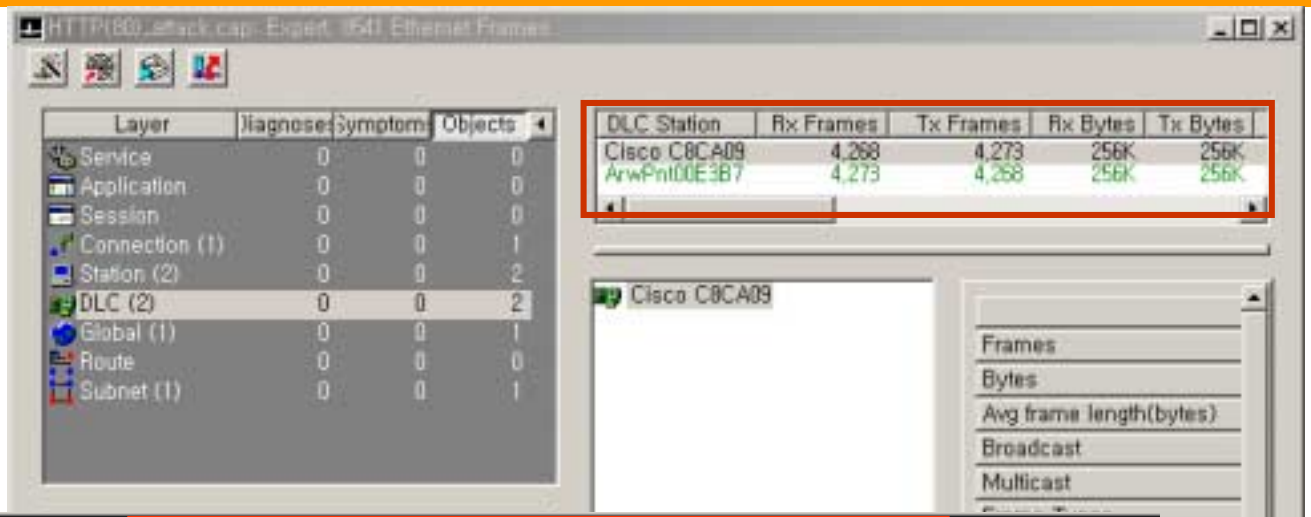
**Filters**



# 비 정상적인 패킷 분석

## Ack Attack

- 당 약 **2000**개 이상의 **60 bytes** 패킷
- 동일한 **Seq.** 및 **ACK** 번호
- 비슷한 개수의 **Tx, Rx** 프레임




| No. | Status | Source Address | Dest Address | Summary | Len (Byte | Rel. Time |
|---|---|---|---|---|---|---|
| 1370 | | 00105800E3B7 | 00049AC8CA09 | TCP: D=1058 S=80 FIN ACK=128747 SEQ=18973883 | 60 | 0:00:00.991 |
| 1371 | | 00049AC8CA09 | 00105800E3B7 | TCP: D=80 S=1058 ACK=1897388498 WIN=8440 | 60 | 0:00:00.994 |
| 1372 | | 00049AC8CA09 | 00105800E3B7 | TCP: D=80 S=1058 ACK=1897388498 WIN=8440 | 60 | 0:00:00.995 |
| 1373 | | 00105800E3B7 | 00049AC8CA09 | TCP: D=1058 S=80 FIN ACK=128747 SEQ=18973883 | 60 | 0:00:00.997 |
| 1374 | | 00105800E3B7 | 00049AC8CA09 | TCP: D=1058 S=80 FIN ACK=128747 SEQ=18973883 | 60 | 0:00:00.997 |
| 1375 | | 00049AC8CA09 | 00105800E3B7 | TCP: D=80 S=1058 ACK=1897388498 WIN=8440 | 60 | 0:00:00.998 |
| 1376 | | 00049AC8CA09 | 00105800E3B7 | TCP: D=80 S=1058 ACK=1897388498 WIN=8440 | 60 | 0:00:00.999 |
| 1377 | | 00105800E3B7 | 00049AC8CA09 | TCP: D=1058 S=80 FIN ACK=128747 SEQ=18973883 | 60 | 0:00:00.999 |
| 1378 | | 00105800E3B7 | 00049AC8CA09 | TCP: D=1058 S=80 FIN ACK=128747 SEQ=18973883 | 60 | 0:00:00.999 |
| 1379 | | 00049AC8CA09 | 00105800E3B7 | TCP: D=80 S=1058 ACK=1897388498 WIN=8440 | 60 | 0:00:01.000 |
| 1380 | | 00049AC8CA09 | 00105800E3B7 | TCP: D=80 S=1058 ACK=1897388498 WIN=8440 | 60 | 0:00:01.000 |
| 1381 | | 00049AC8CA09 | 00105800E3B7 | TCP: D=80 S=1058 ACK=1897388498 WIN=8440 | 60 | 0:00:01.001 |
| 1382 | | 00105800E3B7 | 00049AC8CA09 | TCP: D=1058 S=80 FIN ACK=128747 SEQ=18973883 | 60 | 0:00:01.001 |
| 1383 | | 00049AC8CA09 | 00105800E3B7 | TCP: D=80 S=1058 ACK=1897388498 WIN=8440 | 60 | 0:00:01.002 |
| 1384 | | 00049AC8CA09 | 00105800E3B7 | TCP: D=80 S=1058 ACK=1897388498 WIN=8440 | 60 | 0:00:01.003 |
| 1385 | | 00105800E3B7 | 00049AC8CA09 | TCP: D=1058 S=80 FIN ACK=128747 SEQ=18973883 | 60 | 0:00:01.004 |
| 1386 | | 00105800E3B7 | 00049AC8CA09 | TCP: D=1058 S=80 FIN ACK=128747 SEQ=18973883 | 60 | 0:00:01.004 |
| 1387 | | 00105800E3B7 | 00049AC8CA09 | TCP: D=1058 S=80 FIN ACK=128747 SEQ=18973883 | 60 | 0:00:01.004 |
| 1388 | | 00049AC8CA09 | 00105800E3B7 | TCP: D=80 S=1058 ACK=1897388498 WIN=8440 | 60 | 0:00:01.006 |

네트워크 침투 방법 및 패턴은 다양해도 결국 불필요한 트래픽을 유발

# 비 정상적인 패킷 분석

특정 포트로의 **TCP SYN Scan - Tx >> Rx**

| Source Address | Dest Address | Summary | Len (Byte | Rel. Time |
|---|---|---|---|---|
| .119.163.62 | [199.233.224.3] | TCP: D=445 S=3775 SYN SEQ=2728155792 LEN=0 W | 66 | 0:00:00.000 |
| .119.163.62 | [24.217.29.63] | TCP: D=445 S=3776 SYN SEQ=2728207084 LEN=0 W | 66 | 0:00:00.021 |
| .119.163.62 | [199.233.224.4] | TCP: D=445 S=3777 SYN SEQ=2728253043 LEN=0 W | 66 | 0:00:00.061 |
| .119.163.62 | [24.217.29.15] | TCP: D=445 S=3724 SYN SEQ=2724892110 LEN=0 W | 66 | 0:00:00.068 |
| .119.163.62 | [199.233.224.5] | TCP: D=445 S=3779 SYN SEQ=2728384845 LEN=0 W | 66 | 0:00:00.121 |

**TCP SYN Attack - 50,000~60,000 frames/ sec (Only Tx)**

| Source Address | Dest Address | Summary | Len (Byte | Rel. Time | Delta Time |
|---|---|---|---|---|---|
| [10.1.0.2] | [10.1.0.1] | TCP: D=34 S=2360 SYN SEQ=277351 LEN=0 WIN=8192 | 78 | 0:00:00.000 | 0.000.000 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=38 S=2368 SYN SEQ=277393 LEN=0 WIN=8192 | 78 | 0:00:00.000 | 0.000.041 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=42 S=2376 SYN SEQ=277418 LEN=0 WIN=8192 | 78 | 0:00:00.000 | 0.000.019 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=35 S=2362 SYN SEQ=277366 LEN=0 WIN=8192 | 78 | 0:00:00.000 | 0.000.017 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=39 S=2370 SYN SEQ=277399 LEN=0 WIN=8192 | 78 | 0:00:00.000 | 0.000.017 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=43 S=2378 SYN SEQ=277426 LEN=0 WIN=8192 | 78 | 0:00:00.000 | 0.000.017 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=36 S=2364 SYN SEQ=277372 LEN=0 WIN=8192 | 78 | 0:00:00.000 | 0.000.017 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=40 S=2372 SYN SEQ=277405 LEN=0 WIN=8192 | 78 | 0:00:00.000 | 0.000.017 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=44 S=2380 SYN SEQ=277432 LEN=0 WIN=8192 | 78 | 0:00:00.000 | 0.000.018 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=37 S=2366 SYN SEQ=277378 LEN=0 WIN=8192 | 78 | 0:00:00.000 | 0.000.016 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=41 S=2374 SYN SEQ=277411 LEN=0 WIN=8192 | 78 | 0:00:00.000 | 0.000.017 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=45 S=2382 SYN SEQ=277437 LEN=0 WIN=8192 | 78 | 0:00:00.000 | 0.000.016 |

**IP Scan - Tx >> Rx**

| Source Address | Dest Address | Summary | Len (Byte | Rel. Time |
|---|---|---|---|---|
| [192.168.0.16 | .37.2 | ICMP: Echo | 98 | 0:00:02.264 |
| [192.168.0.16 | .37.3 | ICMP: Echo | 98 | 0:00:02.265 |
| [192.168.0.16 | .37.4 | ICMP: Echo | 98 | 0:00:02.266 |
| [192.168.0.16 | .37.5 | ICMP: Echo | 98 | 0:00:02.268 |
| [192.168.0.16 | .37.6 | ICMP: Echo | 98 | 0:00:02.269 |
| [192.168.0.16 | .37.7 | ICMP: Echo | 98 | 0:00:02.270 |
| [192.168.0.16 | .37.8 | ICMP: Echo | 98 | 0:00:02.272 |
| [192.168.0.16 | .37.9 | ICMP: Echo | 98 | 0:00:02.273 |
| [192.168.0.16 | .37.1 | ICMP: Echo | 98 | 0:00:02.274 |

# 비 정상적인 패킷 분석

**Port Scan - Tx = Rx**

| Net Station 1 | Net Station 2 | Protocol | Frames | Bytes |
|---|---|---|---|---|
| [10.1.0.1] | [10.1.0.2] | TCP | 2 | 64 |
| [10.1.0.1] | [10.1.0.2] | TCP | 2 | 64 |
| [10.1.0.1] | [10.1.0.2] | TCP | 2 | 64 |
| [10.1.0.1] | [10.1.0.2] | TCP | 2 | 64 |
| [10.1.0.1] | [10.1.0.2] | TCP | 2 | 64 |
| [10.1.0.1] | [10.1.0.2] | TCP | 2 | 64 |
| [10.1.0.1] | [10.1.0.2] | TCP | 3 | 88 |
| [10.1.0.1] | [10.1.0.2] | TCP | 2 | 64 |
| [10.1.0.1] | [10.1.0.2] | TCP | 3 | 88 |
| [10.1.0.1] | [10.1.0.2] | TCP | 2 | 64 |
| [10.1.0.1] | [10.1.0.2] | TCP | 2 | 64 |
| [10.1.0.1] | [10.1.0.2] | TCP | 2 | 64 |
| [10.1.0.1] | [10.1.0.2] | TCP | 1 | 44 |
| [10.1.0.1] | [10.1.0.2] | TCP | 1 | 44 |

특징:

- Destination Port가 순차적으로 증가
- 접속이 불가능한 포트에 대해서 SYN와 RST 패킷이 반복적으로 발생
- Source 시스템의 SEQ 번호 증가율이 균일함
- 접속 가능한 포트 (7, 9 번 포트)

  (SYN – SYN ACK – ACK)

특징:

- 두 스테이션의 Connection 각각에 대해서 송수신된 패킷이 전체적으로 너무 적고, 개수도 비슷함

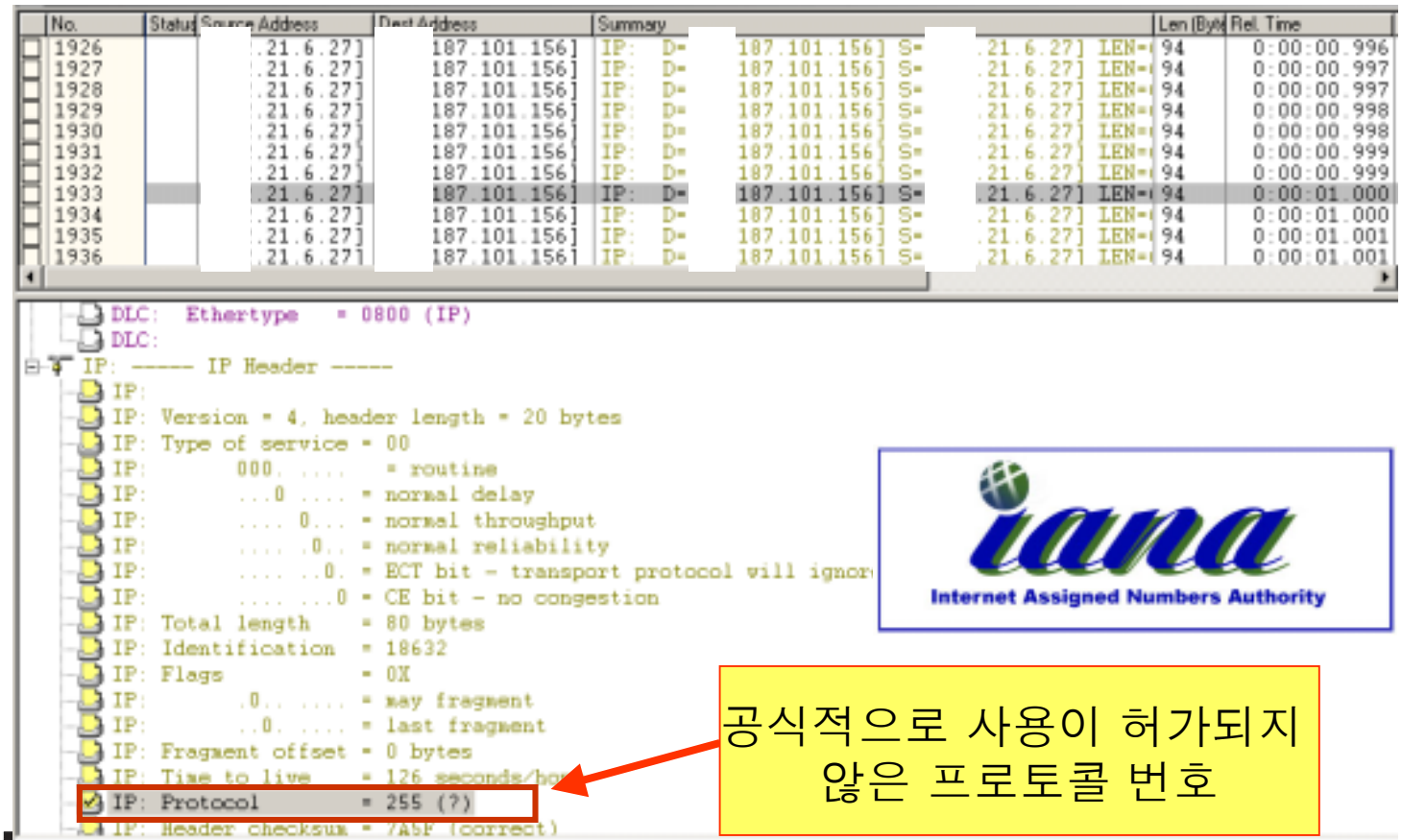
| Source Address | Dest Address | Summary | Len (Byte |
|---|---|---|---|
| [10.1.0.2] | [10.1.0.1] | TCP: D=1 S=2294 SYN SEQ=277138 LEN=0 WIN=8192 | 78 |
| [10.1.0.1] | [10.1.0.2] | TCP: D=2294 S=1 RST ACK=277139 WIN=0 | 60 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=2 S=2296 SYN SEQ=277145 LEN=0 WIN=8192 | 78 |
| [10.1.0.1] | [10.1.0.2] | TCP: D=2296 S=2 RST ACK=277146 WIN=0 | 60 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=3 S=2298 SYN SEQ=277151 LEN=0 WIN=8192 | 78 |
| [10.1.0.1] | [10.1.0.2] | TCP: D=2298 S=3 RST ACK=277152 WIN=0 | 60 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=4 S=2300 SYN SEQ=277156 LEN=0 WIN=8192 | 78 |
| [10.1.0.1] | [10.1.0.2] | TCP: D=2300 S=4 RST ACK=277157 WIN=0 | 60 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=5 S=2302 SYN SEQ=277161 LEN=0 WIN=8192 | 78 |
| [10.1.0.1] | [10.1.0.2] | TCP: D=2302 S=5 RST ACK=277162 WIN=0 | 60 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=6 S=2304 SYN SEQ=277166 LEN=0 WIN=8192 | 78 |
| [10.1.0.1] | [10.1.0.2] | TCP: D=2304 S=6 RST ACK=277167 WIN=0 | 60 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=7 S=2306 SYN SEQ=277172 LEN=0 WIN=8192 | 78 |
| [10.1.0.1] | [10.1.0.2] | TCP: D=2306 S=7 SYN ACK=277173 SEQ=352903520 LEN | 60 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=7 S=2306 ACK=352903521 WIN=8760 | 60 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=8 S=2308 SYN SEQ=277177 LEN=0 WIN=8192 | 78 |
| [10.1.0.1] | [10.1.0.2] | TCP: D=2308 S=8 RST ACK=277178 WIN=0 | 60 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=9 S=2310 SYN SEQ=277182 LEN=0 WIN=8192 | 78 |
| [10.1.0.1] | [10.1.0.2] | TCP: D=2310 S=9 SYN ACK=277183 SEQ=352903520 LEN | 60 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=9 S=2310 ACK=352903521 WIN=8760 | 60 |
| [10.1.0.2] | [10.1.0.1] | TCP: D=10 S=2312 SYN SEQ=277188 LEN=0 WIN=8192 | 78 |
| [10.1.0.1] | [10.1.0.2] | TCP: D=2312 S=10 RST ACK=277189 WIN=0 | 60 |

# 비 정상적인 패킷 분석

**IP Protocol number = 255 (Only Tx)**

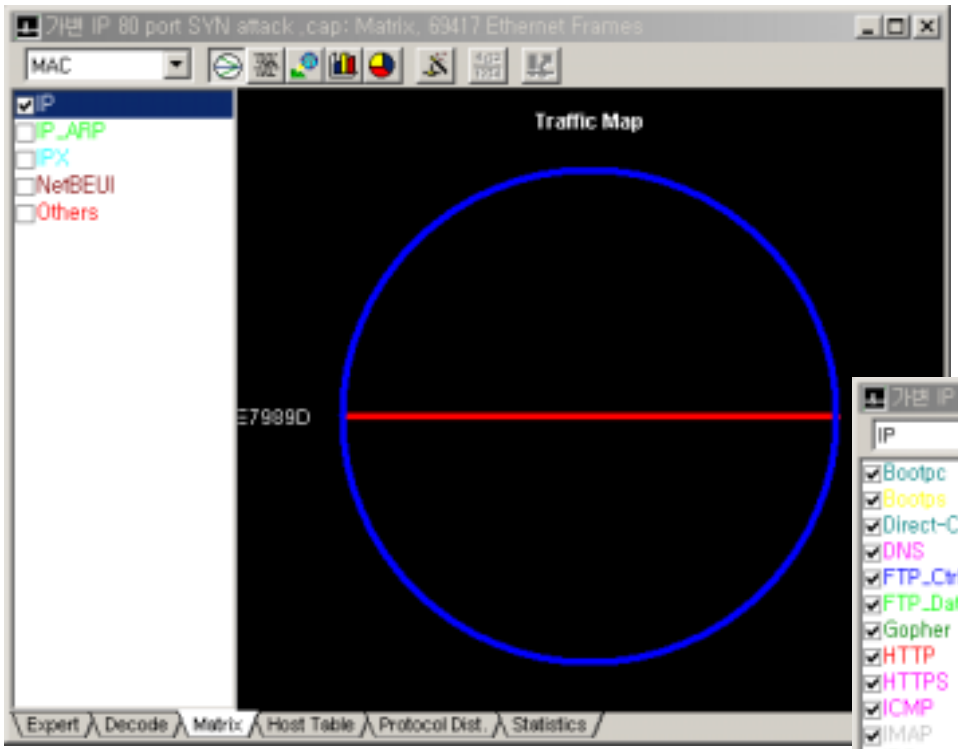
- irc bot ip potocol 255 – **DDOS Attack?**

| DLC Station | Rx Frames | Tx Frames | Rx Bytes | Tx Bytes |
|---|---|---|---|---|
| Cisco BD4C01 | 0 | 10,768 | 0 | 1,012K |
| 0009B766364A | 10,768 | 0 | 1,012K | 0 |



# 비 정상적인 패킷 분석

특정 스테이션의 **IP** 및 어플리케이션 포트 **SCAN (Multi-IP Only Tx)**

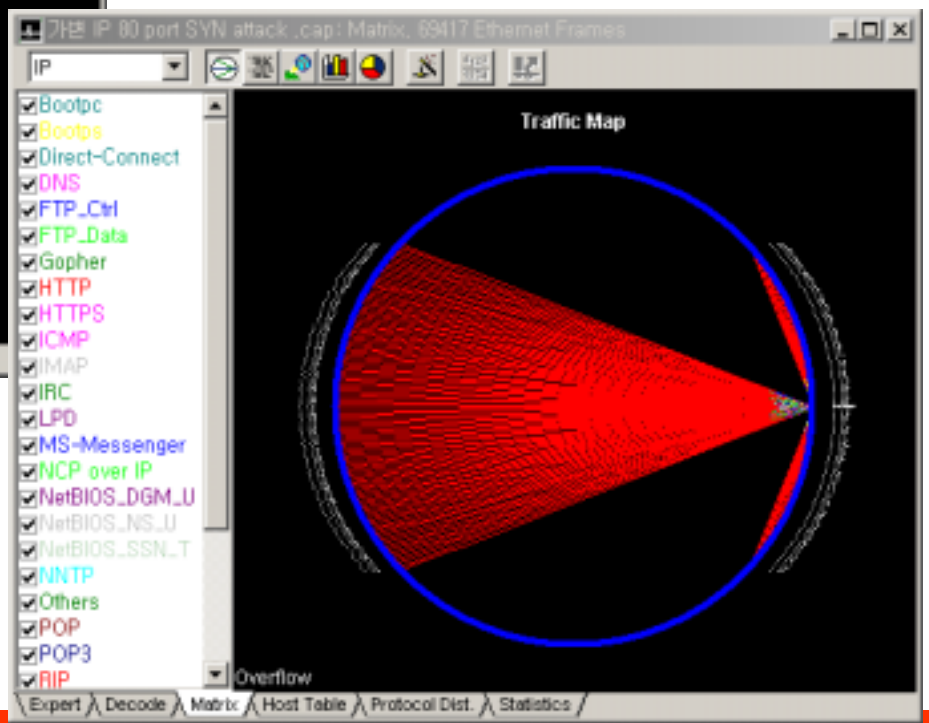



Source MAC: 1

Destination MAC: 1

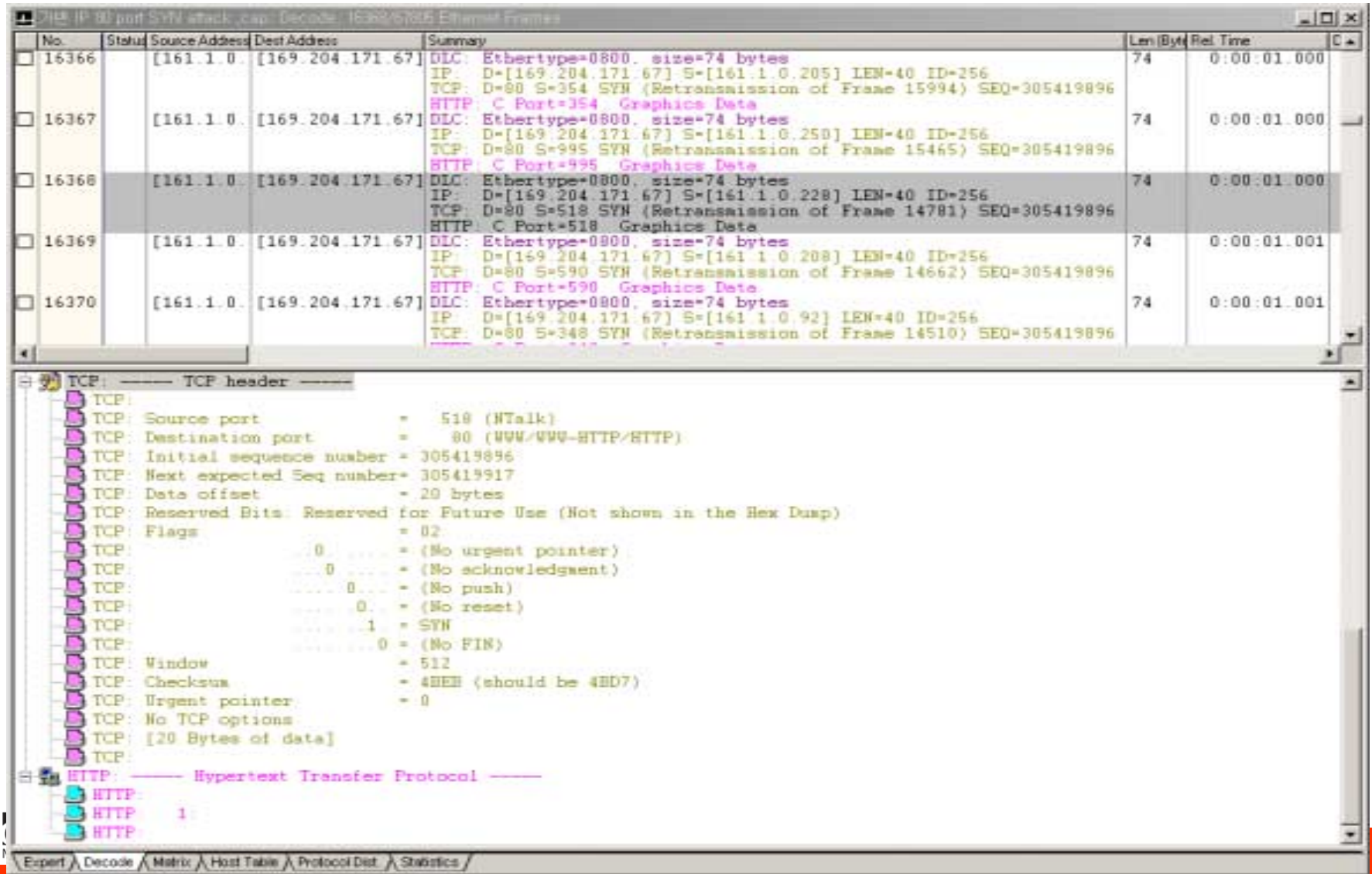
Source IP : N

Destination IP: 1



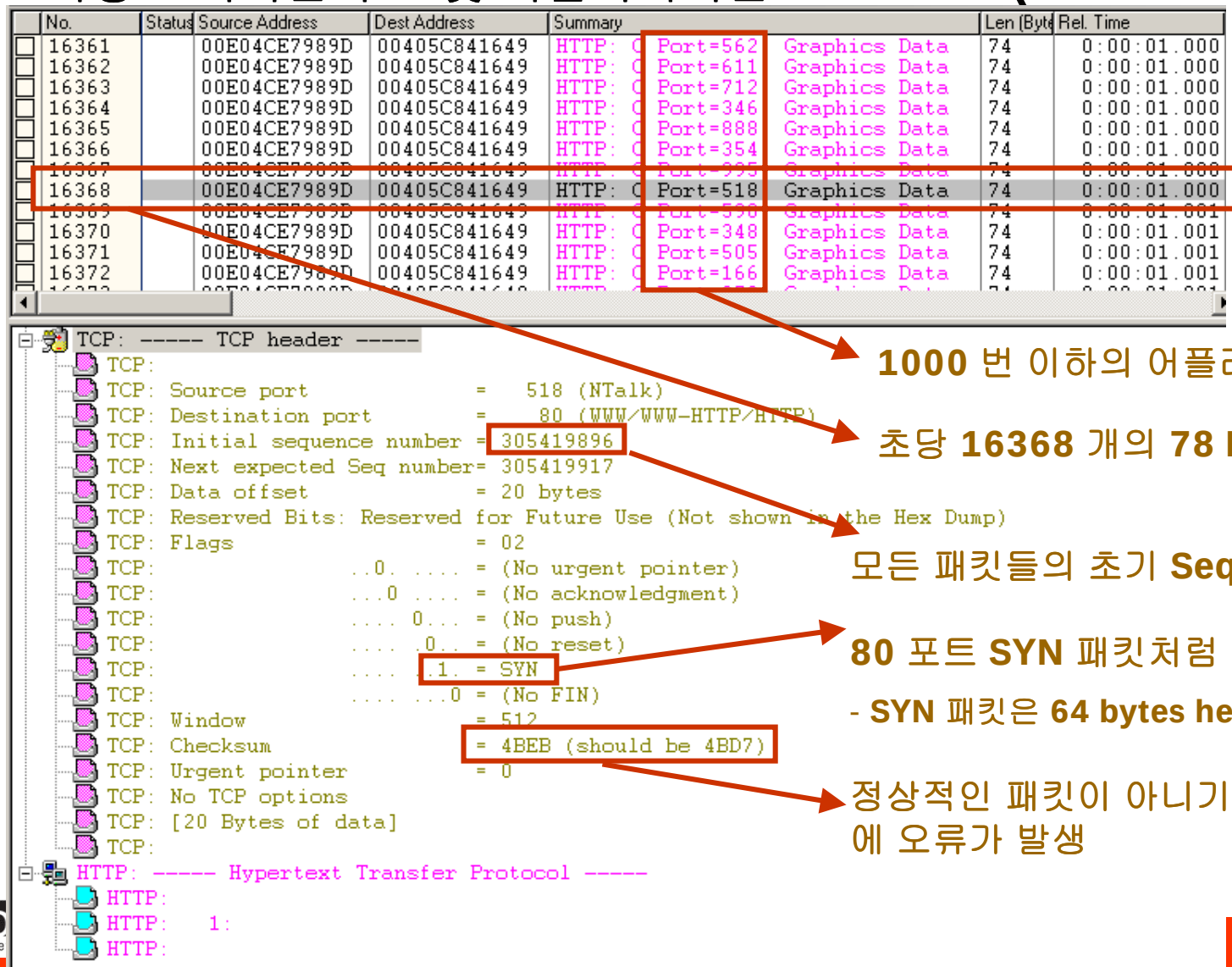
# 비 정상적인 패킷 분석

특정 스테이션의 **IP** 및 어플리케이션 포트 **SCAN (Multi-IP Only Tx)**



# 비 정상적인 패킷 분석

특정 스테이션의 **IP** 및 어플리케이션 포트 **SCAN (Multi-IP Only Tx)**




**1000** 번 이하의 어플리케이션 포트

초당 **16368** 개의 **78 Bytes** 패킷들

모든 패킷들의 초기 **Seq.** 번호가 동일

**80** 포트 **SYN** 패킷처럼 위장

- **SYN** 패킷은 **64 bytes header**만 포함

정상적인 패킷이 아니기 때문에 헤더에 오류가 발생