과제 1: MicroSoft SMS Traffic Monitor 사용법

1. 개요

- 네트워크에서 유통되는 트래픽을 감시하여 데이터를 분석하고 프로토콜을 해석하는 네트워크 모니터의 기본 개념과 사용 방법을 익힌다.

2. 수행할 과제 내용

- 첨부된 SMS TM 설명서를 참고하여 SMS TM 을 자신의 XP 에 설치한다.
- 첨부된 SMS TM 설명서를 참고하여 SMS TM 의 사용방법을 연습한다.
- ping default gateway 로 트래픽을 발생시킨 후 SMS TM 으로 트래픽을 감시하고 감시된 트래픽을 간략히 살펴보고 각 패킷의 의미를 추정해본다.
  - default gateway 는 XP 의 명령창에서 ipconfig /all 로 확인할 것
- 네트워크 선택, 필터링 방법 등 SMS TM 의 기능을 확인해본다.

3. 과제 수행 결과 보고

- 과제 수행 결과를 한쪽 분량으로 작성한다.
- 감시한 트래픽 중 중요한 몇 가지를 캡춰한다.
- 이들을 모두 메일로 보고한다.

첨부자료: SMS TM 설명서

1. 설치 방법

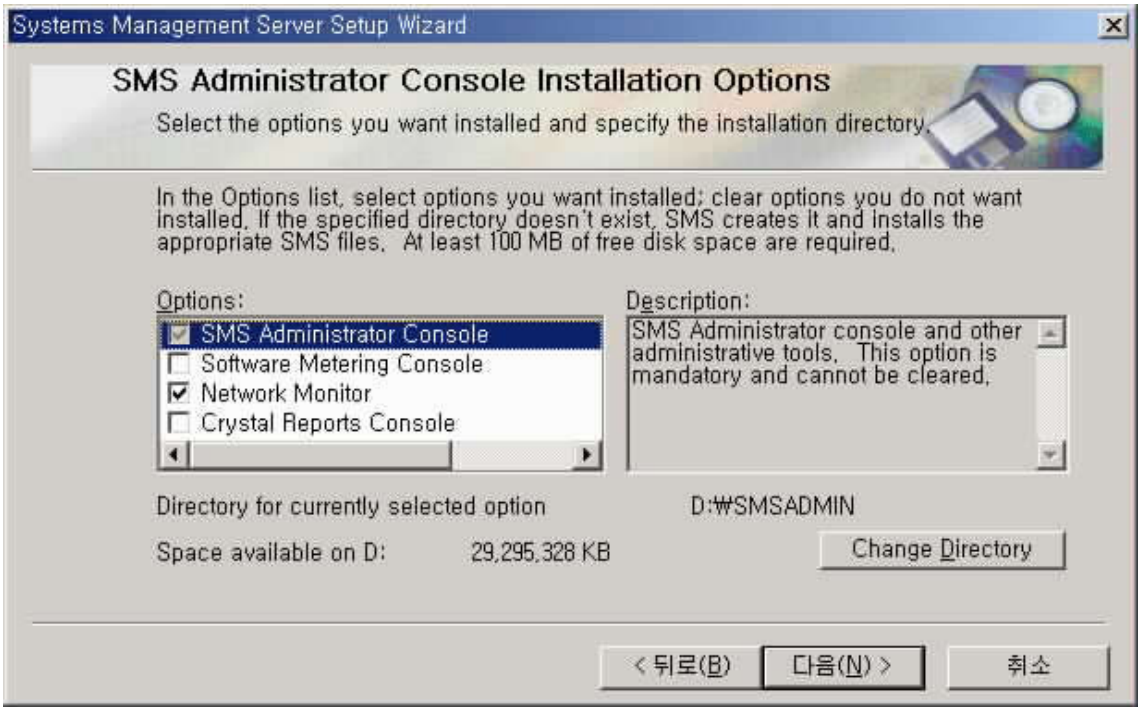
① SMS 2.0 CD-ROM을 넣으면 자동 실행되고 다음과 같은 창이 뜬다.

② "Set Up SMS2.0"을 선택하면 Setup 마법사가 나온다.

③ 설치 진행 중 "Setup Options"에서 "Install the SMS Administrator console and related tools"를 선택한다.

④ 설치 진행 중 SMS server site name에 서버이름(예로 abc0 등) 을 입력한다.

⑤ 설치 진행 중 "SMS Administrator Console Installation Options"에서 본 실습에 사용될 프로토콜 분석기인 "Network Monitor"를 반드시 체크한다.

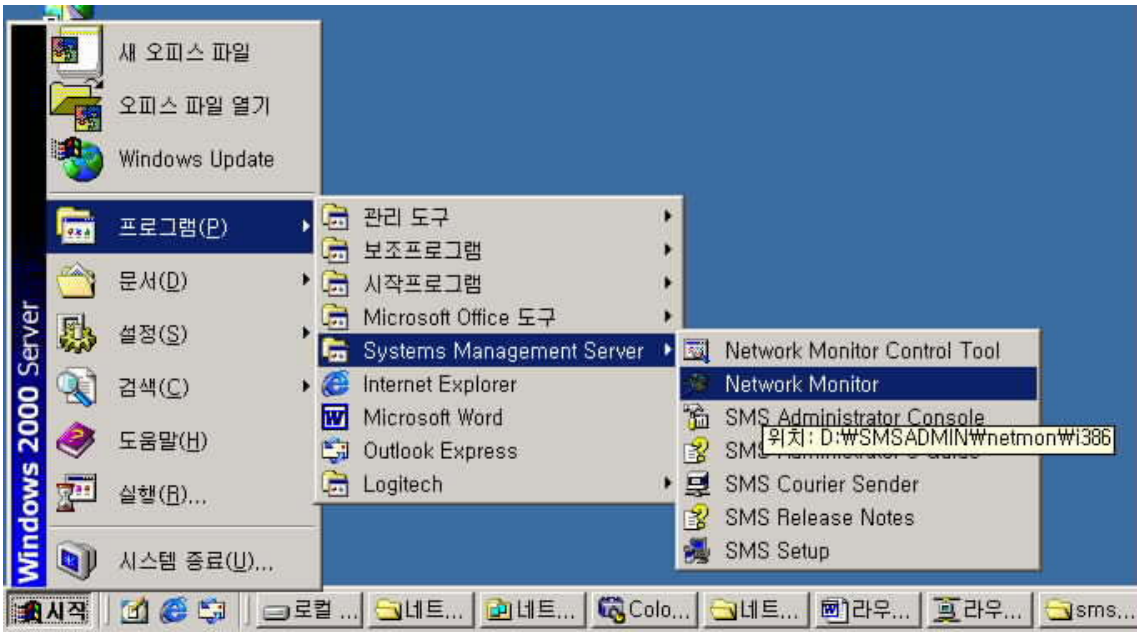


⑥ 마법사를 마치면 필요한 소프트웨어가 자동으로 설치된다.

2. 사용방법

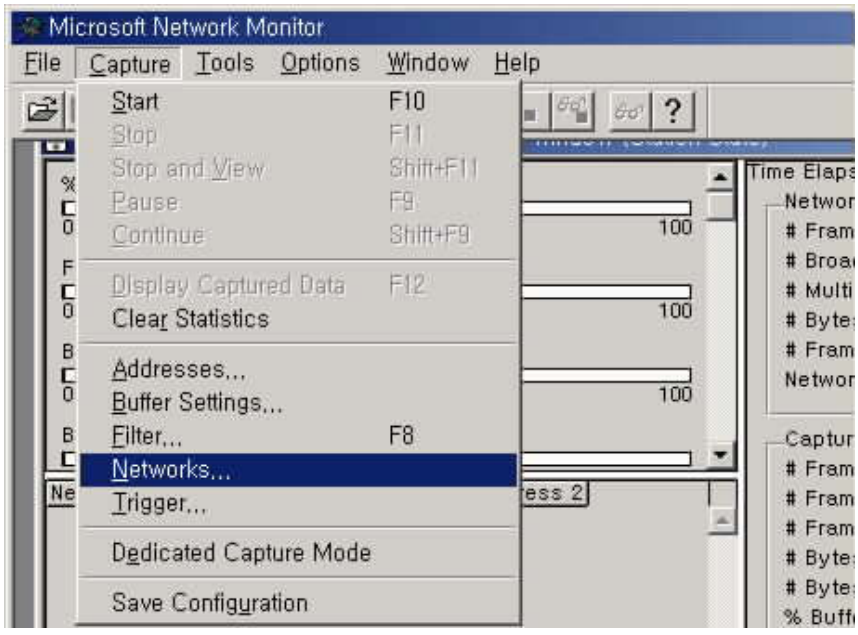
<네트워크 모니터 기동>

① [시작][프로그램][System Management Server][Network Monitor]를 클릭한다.

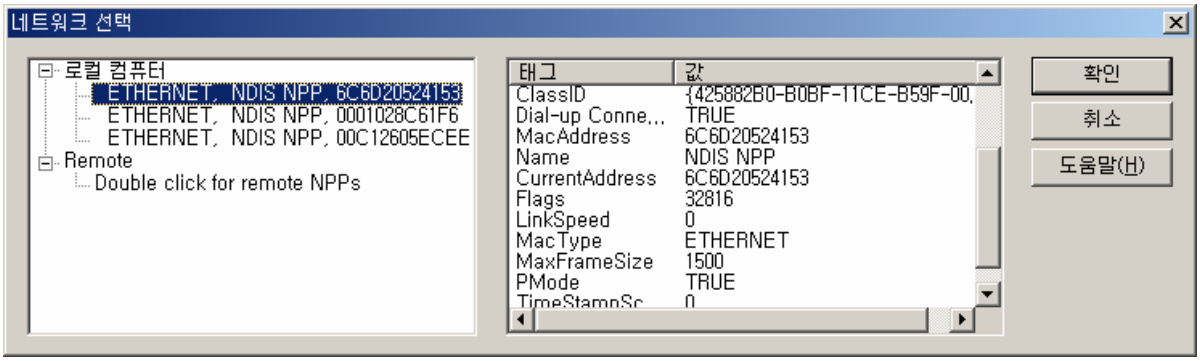


<감시할 네트워크 선택>

② 네트워크 모니터 창에서 먼저 감시할 네트워크를 선택하기 위해 [Capture][Networks]를 클릭한다.

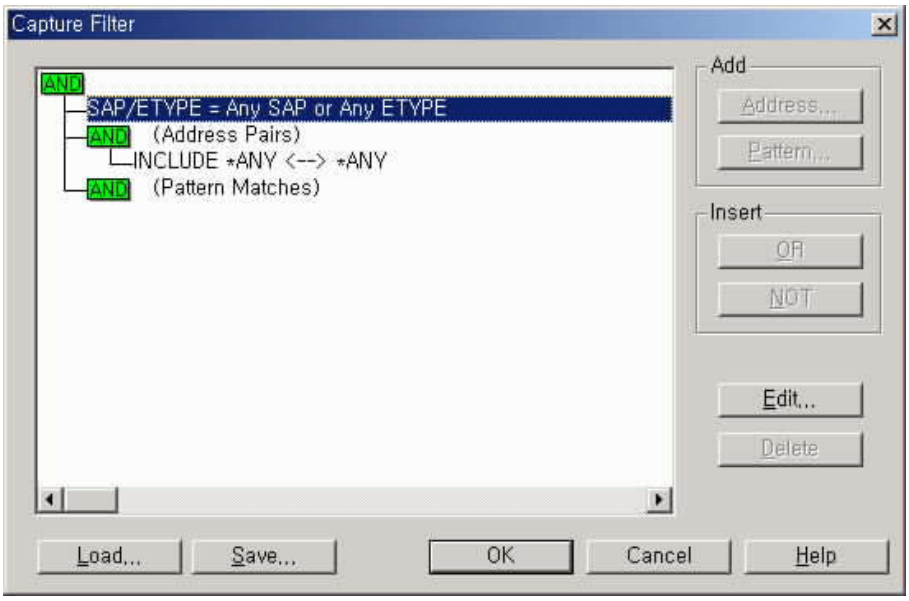


③ 그러면 다음과 같은 네트워크 선택 창이 뜨는데, 감시할 인터페이스를 찾는데, 먼저 로컬컴퓨터인지, 아니면 원격 컴퓨터인지 결정하고, 로컬컴퓨터이면 다수의 인터페이스 (예로 LAN 카드 2개, 모뎀 1개 등)가 있을 수 있는데, 감시할 네트워크에 연결된 인터페이스를 클릭하면 된다. 만약 지점외부(com) 네트워크를 감시하고자 하면 그 인터페이스의 LAN카드를 선택해야 하는데, LAN카드의 MAC 주소로 식별해야 한다. 이는 ipconfig/all 명령어로 확인할 수 있다.

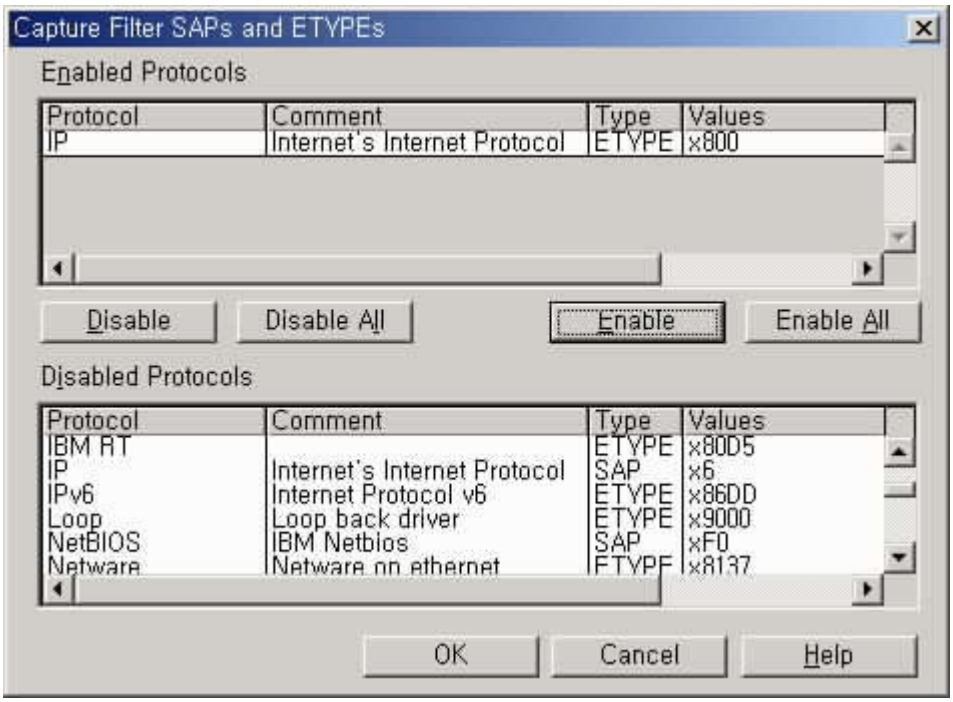


<갈무리할 데이터 필터링>

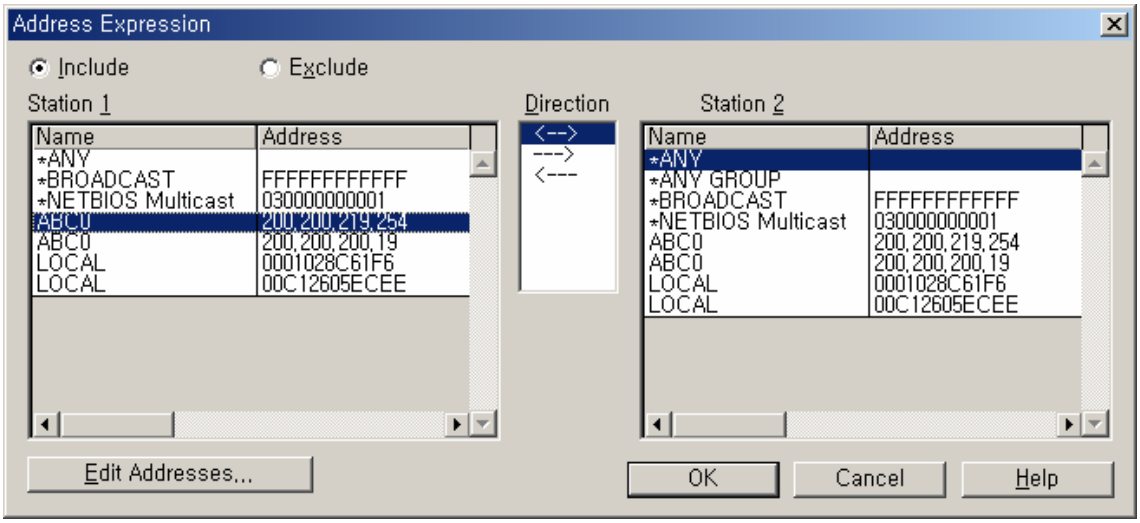
④ 다음은 갈무리할 데이터의 양을 줄이기 위해 감시할 트래픽을 제한하는 것이 좋은데, 이는 “Filter” 메뉴로 정의한다. [Capture][Filter]를 클릭하면 “Capture Filter” 창이 나온다. 제한하는 방법은 발착신지 주소, 프로토콜 유형 및 패킷내 특정 패턴의 세 가지 방법이 있다. 특정 패턴에 의한 방법은 전문가만 사용하므로 자세한 설명은 생략한다. 먼저 프로토콜 유형에 의해 감시 트래픽을 제한하기 위해 “SAP/ETYPE”를 클릭한다.



⑤ “Disable All”로 모든 프로토콜 유형을 차단한 후 원하는 프로토콜, 예로 IP 프로토콜 (Etype), 을 선택한 후 “Enable” 을 클릭하면 그 프로토콜이 “Enabled Protocols” 창에 추가된다.



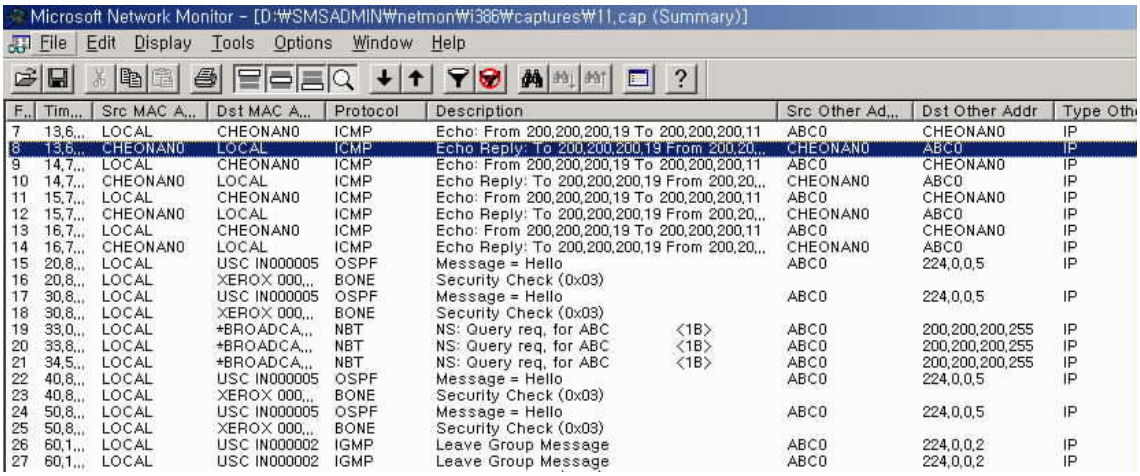
⑥ 주소에 의한 감시 트래픽의 제한은 “Capture Filter” 창에서 “Address Pairs”를 선택한 후 감시할 발.착신 컴퓨터의 이름과 주소를 찾아 선택하면 해당 조건에 부합되는 트래픽만 감시된다. 여기서 “Any”는 모든 컴퓨터를 의미하고, 이름이 등록되어 있지 않으면 좌측 하단부의 “Edit Addresses” 를 클릭하여 원하는 이름을 등록할 수 있다.



< 갈무리 시작 및 갈무리된 데이터 보기>

⑦ 감시할 네트워크와 트래픽을 정한 후 [Capture][Start]로 감시 및 갈무리를 시작한다. 진행중인 감시 및 갈무리에 대한 정보는 “Network Monitor” 창의 우측 및 하부의 창에 나타난다.

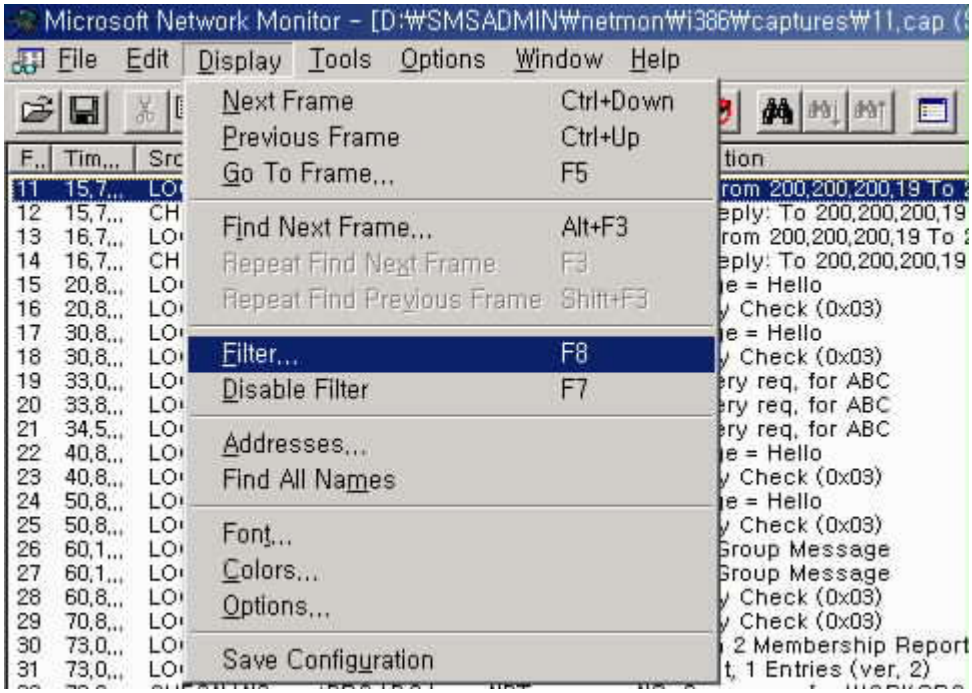
⑧ 갈무리한 트래픽을 보고자 할 경우 [Capture][Stop and View]를 클릭하면 다음과 같은 갈무리 요약 창이 뜬다. Y축은 갈무리된 프레임 순번, X축은 감시 시간, 발착신 MAC주소, 프로토콜, 설명, 다른 발착신 주소 등으로 되어 있다.



F..	Tim...	Src MAC A...	Dst MAC A...	Protocol	Description	Src Other Ad...	Dst Other Addr	Type Oth
7	13,6...	LOCAL	CHEONAN0	ICMP	Echo: From 200,200,200,19 To 200,200,200,11	ABC0	CHEONAN0	IP
8	13,6...	CHEONAN0	LOCAL	ICMP	Echo Reply: To 200,200,200,19 From 200,20...	CHEONAN0	ABC0	IP
9	14,7...	LOCAL	CHEONAN0	ICMP	Echo: From 200,200,200,19 To 200,200,200,11	ABC0	CHEONAN0	IP
10	14,7...	CHEONAN0	LOCAL	ICMP	Echo Reply: To 200,200,200,19 From 200,20...	CHEONAN0	ABC0	IP
11	15,7...	LOCAL	CHEONAN0	ICMP	Echo: From 200,200,200,19 To 200,200,200,11	ABC0	CHEONAN0	IP
12	15,7...	CHEONAN0	LOCAL	ICMP	Echo Reply: To 200,200,200,19 From 200,20...	CHEONAN0	ABC0	IP
13	16,7...	LOCAL	CHEONAN0	ICMP	Echo: From 200,200,200,19 To 200,200,200,11	ABC0	CHEONAN0	IP
14	16,7...	CHEONAN0	LOCAL	ICMP	Echo Reply: To 200,200,200,19 From 200,20...	CHEONAN0	ABC0	IP
15	20,8...	LOCAL	USC IN000005	OSPF	Message = Hello	ABC0	224,0,0,5	IP
16	20,8...	LOCAL	XEROX 000...	BONE	Security Check (0x03)			
17	30,8...	LOCAL	USC IN000005	OSPF	Message = Hello	ABC0	224,0,0,5	IP
18	30,8...	LOCAL	XEROX 000...	BONE	Security Check (0x03)			
19	33,0...	LOCAL	*BROADCA...	NBT	NS: Query req. for ABC <1B>	ABC0	200,200,200,255	IP
20	33,8...	LOCAL	*BROADCA...	NBT	NS: Query req. for ABC <1B>	ABC0	200,200,200,255	IP
21	34,5...	LOCAL	*BROADCA...	NBT	NS: Query req. for ABC <1B>	ABC0	200,200,200,255	IP
22	40,8...	LOCAL	USC IN000005	OSPF	Message = Hello	ABC0	224,0,0,5	IP
23	40,8...	LOCAL	XEROX 000...	BONE	Security Check (0x03)			
24	50,8...	LOCAL	USC IN000005	OSPF	Message = Hello	ABC0	224,0,0,5	IP
25	50,8...	LOCAL	XEROX 000...	BONE	Security Check (0x03)			
26	60,1...	LOCAL	USC IN000002	IGMP	Leave Group Message	ABC0	224,0,0,2	IP
27	60,1...	LOCAL	USC IN000002	IGMP	Leave Group Message	ABC0	224,0,0,2	IP

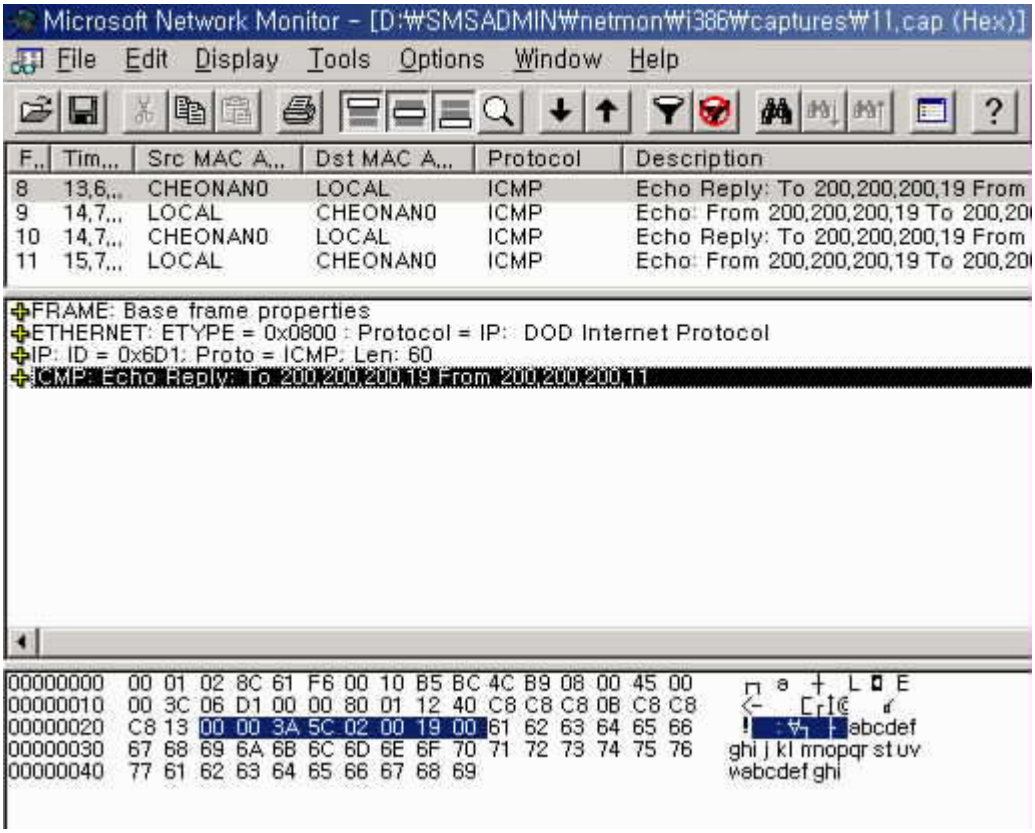
<갈무리된 데이터 필터링 >

⑨ 갈무리가 된 자료가 많을 경우 보고싶은 트래픽을 찾아보기가 어려우므로 보고싶은 트래픽만 추려낼 수 있다. 이는 [Display][Filter]를 클릭하여 프로토콜 유형과 발착신 주소로 트래픽을 추려낼 수 있다. 앞에서 살펴본 갈무리할 때의 필터링과 유사하므로 상세한 설명은 생략한다.

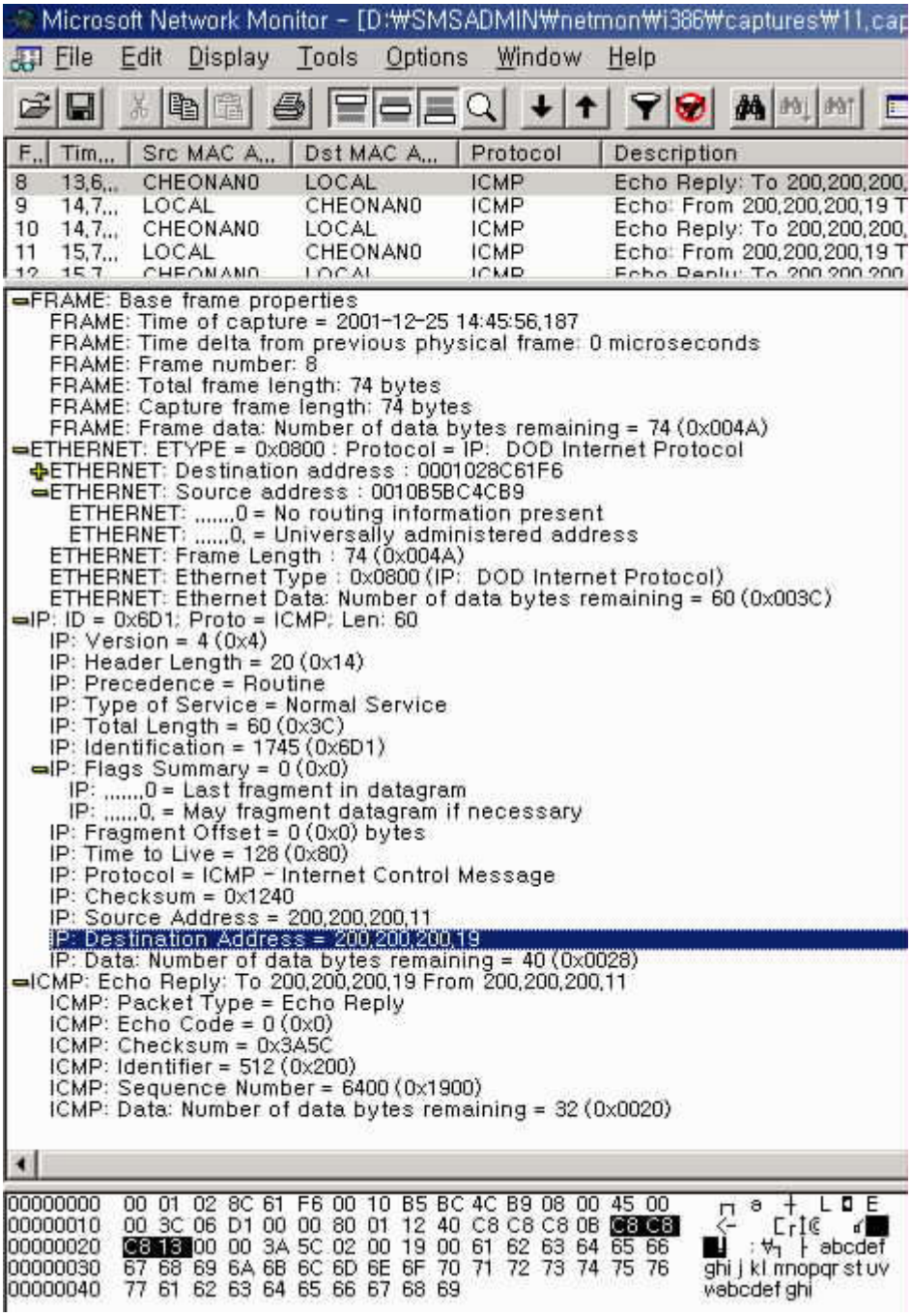


< 갈무리된 데이터 보는 방법 >

⑩ 갈무리 요약 창에서 원하는 프레임이 선택되면 이를 자세히 살펴볼 필요가 있다. 이럴 경우 선택된 프레임을 더블클릭하면 다음과 같이 3개의 창이 뜨는데, 위쪽 창은 요약 창이고, 중간에 있는 창은 프레임의 디코딩 내용, 아래쪽 창은 프레임의 엔코딩 내용을 보여준다. 여기서 엔코딩이란 바이너리 값으로 기호화 한 것을 의미하고, 디코딩이란 바이너리 값을 원래의 의미로 해석한 것을 의미한다. 디코딩 내용을 상세히 보려면 해당 라인을 클릭하면 된다.



⑪ 디코딩 창의 각 라인을 클릭하면 다음 창과 같이 프레임의 상세한 내역을 살펴볼 수 있다. 제일 위쪽의 "FRAME"란 갈무리된 프레임에 대한 간략한 정보, 예로 갈무리 시간, 데이터 크기 등을 보여주고, 그 다음부터는 프로토콜 계층구조에 따라 각각의 프로토콜에 대한 상세한 내용, 즉 각 프로토콜의 해더 내용의 세부사항과 바디 내용을 보여준다. 선택된 프로토콜의 영역에 대응되는 바이너리 값이 아래쪽 창에 선택되어 나타난다.


Microsoft Network Monitor - [D:₩SMSADMIN₩netmon₩i386₩captures₩11,cap
File Edit Display Tools Options Window Help
F.. Tim... Src MAC A... Dst MAC A... Protocol Description
8 13,6... CHEONAN0 LOCAL ICMP Echo Reply: To 200,200,200,
9 14,7... LOCAL CHEONAN0 ICMP Echo: From 200,200,200,19 T
10 14,7... CHEONAN0 LOCAL ICMP Echo Reply: To 200,200,200,
11 15,7... LOCAL CHEONAN0 ICMP Echo: From 200,200,200,19 T
FRAME: Base frame properties
FRAME: Time of capture = 2001-12-25 14:45:56,187
FRAME: Time delta from previous physical frame: 0 microseconds
FRAME: Frame number: 8
FRAME: Total frame length: 74 bytes
FRAME: Capture frame length: 74 bytes
FRAME: Frame data: Number of data bytes remaining = 74 (0x004A)
ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
ETHERNET: Destination address : 0001028C61F6
ETHERNET: Source address : 0010B5BC4CB9
ETHERNET: .....0 = No routing information present
ETHERNET: .....0. = Universally administered address
ETHERNET: Frame Length : 74 (0x004A)
ETHERNET: Ethernet Type : 0x0800 (IP: DOD Internet Protocol)
ETHERNET: Ethernet Data: Number of data bytes remaining = 60 (0x003C)
IP: ID = 0x6D1; Proto = ICMP; Len: 60
IP: Version = 4 (0x4)
IP: Header Length = 20 (0x14)
IP: Precedence = Routine
IP: Type of Service = Normal Service
IP: Total Length = 60 (0x3C)
IP: Identification = 1745 (0x6D1)
IP: Flags Summary = 0 (0x0)
IP: .....0 = Last fragment in datagram
IP: .....0. = May fragment datagram if necessary
IP: Fragment Offset = 0 (0x0) bytes
IP: Time to Live = 128 (0x80)
IP: Protocol = ICMP - Internet Control Message
IP: Checksum = 0x1240
IP: Source Address = 200,200,200,11
IP: Destination Address = 200,200,200,19
IP: Data: Number of data bytes remaining = 40 (0x0028)
ICMP: Echo Reply: To 200,200,200,19 From 200,200,200,11
ICMP: Packet Type = Echo Reply
ICMP: Echo Code = 0 (0x0)
ICMP: Checksum = 0x3A5C
ICMP: Identifier = 512 (0x200)
ICMP: Sequence Number = 6400 (0x1900)
ICMP: Data: Number of data bytes remaining = 32 (0x0020)
00000000 00 01 02 8C 61 F6 00 10 B5 BC 4C B9 08 00 45 00
00000010 00 3C 06 D1 00 00 80 01 12 40 C8 C8 C8 0B C8 C8
00000020 C8 13 00 00 3A 5C 02 00 19 00 61 62 63 64 65 66
00000030 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76
00000040 77 61 62 63 64 65 66 67 68 69