이 경 호 / 김 현 진 / 여 승 철

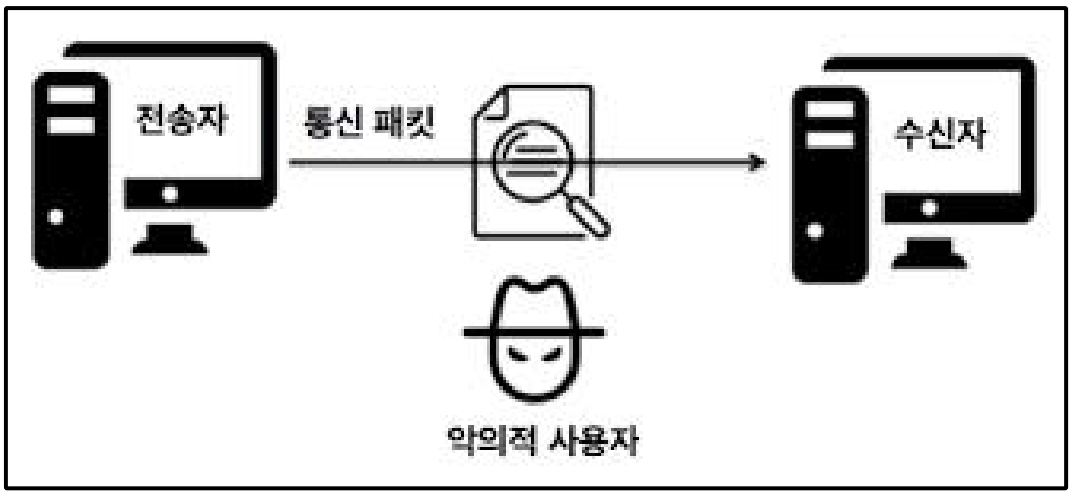
스니핑 프로그램

CONTENTS

1) 스니핑이란?

네트워크 상에서 자신이 아닌 다른 상대방의 패킷 교환을 엿듣는 것이다.

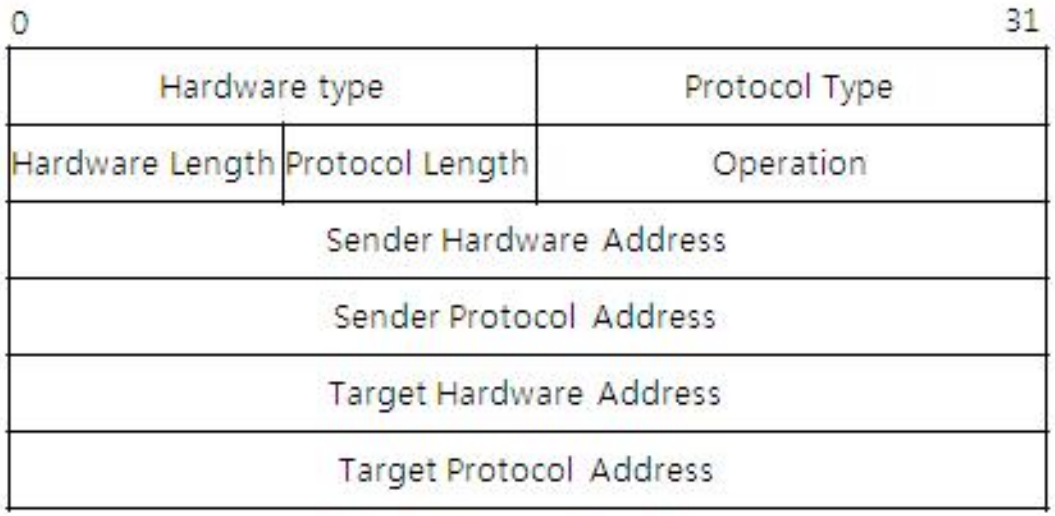
간단히 말해서 **네트워크 트래픽 도청**하는 과정을 말한다.



2) 패킷이란?

네트워크를 통해 전송하기 쉽도록 자른 데이터의 전송단위

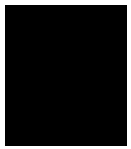
헤더 + 데이터 (구성)



ARP 패킷

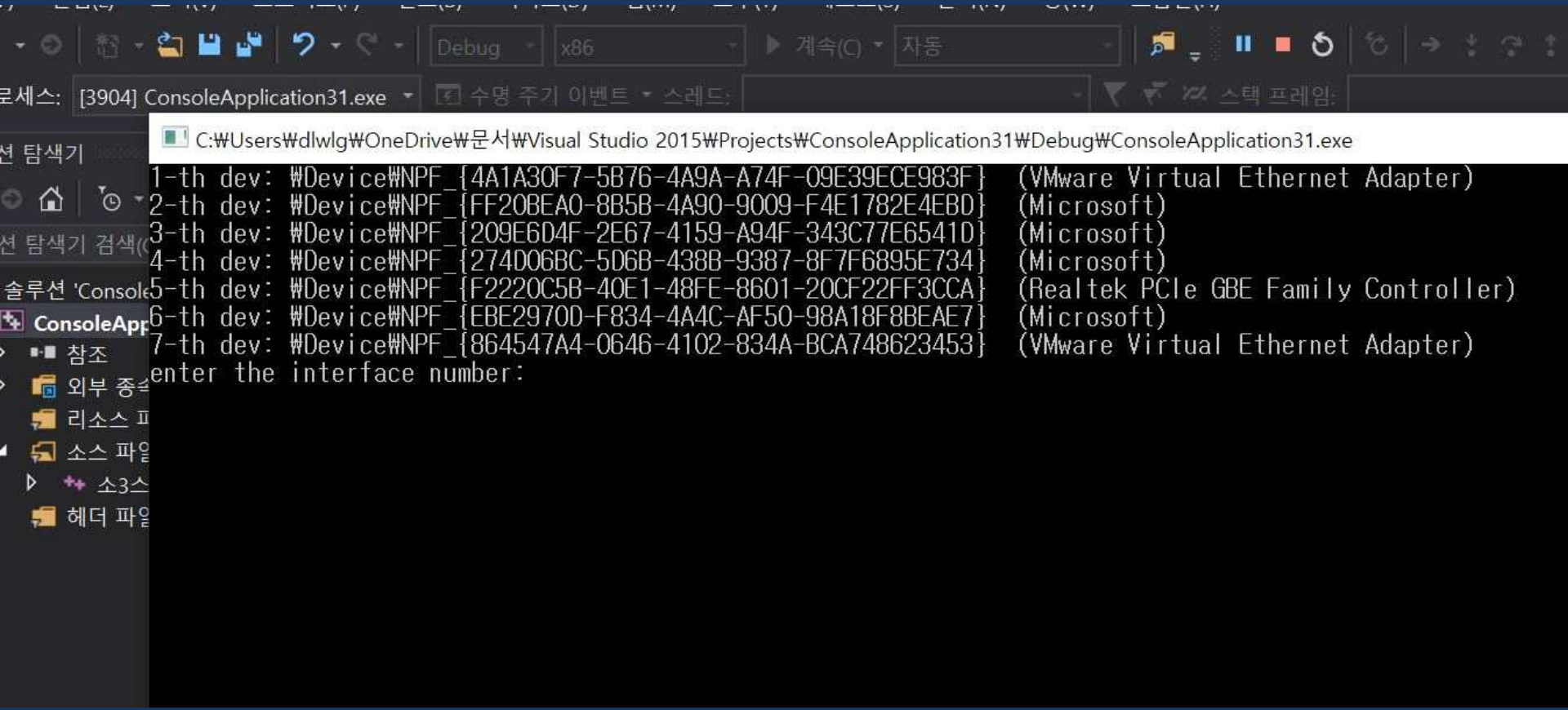
소스코드 (이경호)

: C언어로 코딩 // 윈도우에서 구현



경호sniffing.c

01


Debug
x86
계속(C)
자동
로세스: [3904] ConsoleApplication31.exe
수명 주기 이벤트
스레드:
스택 프레임:
션 탐색기
션 탐색기 검색(
솔루션 'Console
ConsoleApp
참조
외부 종
리소스 파
소스 파일
소3스
헤더 파일
C:₩Users₩dlwlg₩OneDrive₩문서₩Visual Studio 2015₩Projects₩ConsoleApplication31₩Debug₩ConsoleApplication31.exe
1-th dev: ₩Device₩NPF_{4A1A30F7-5B76-4A9A-A74F-09E39ECE983F} (VMware Virtual Ethernet Adapter)
2-th dev: ₩Device₩NPF_{FF20BEA0-8B5B-4A90-9009-F4E1782E4EBD} (Microsoft)
3-th dev: ₩Device₩NPF_{209E6D4F-2E67-4159-A94F-343C77E6541D} (Microsoft)
4-th dev: ₩Device₩NPF_{274D06BC-5D6B-438B-9387-8F7F6895E734} (Microsoft)
5-th dev: ₩Device₩NPF_{F2220C5B-40E1-48FE-8601-20CF22FF3CCA} (Realtek PCIe GBE Family Controller)
6-th dev: ₩Device₩NPF_{EBE2970D-F834-4A4C-AF50-98A18F8BEAE7} (Microsoft)
7-th dev: ₩Device₩NPF_{864547A4-0646-4102-834A-BCA748623453} (VMware Virtual Ethernet Adapter)
enter the interface number:

소스코드 (김현진)

: C언어로 코딩 // 윈도우에서 구현

snif.c

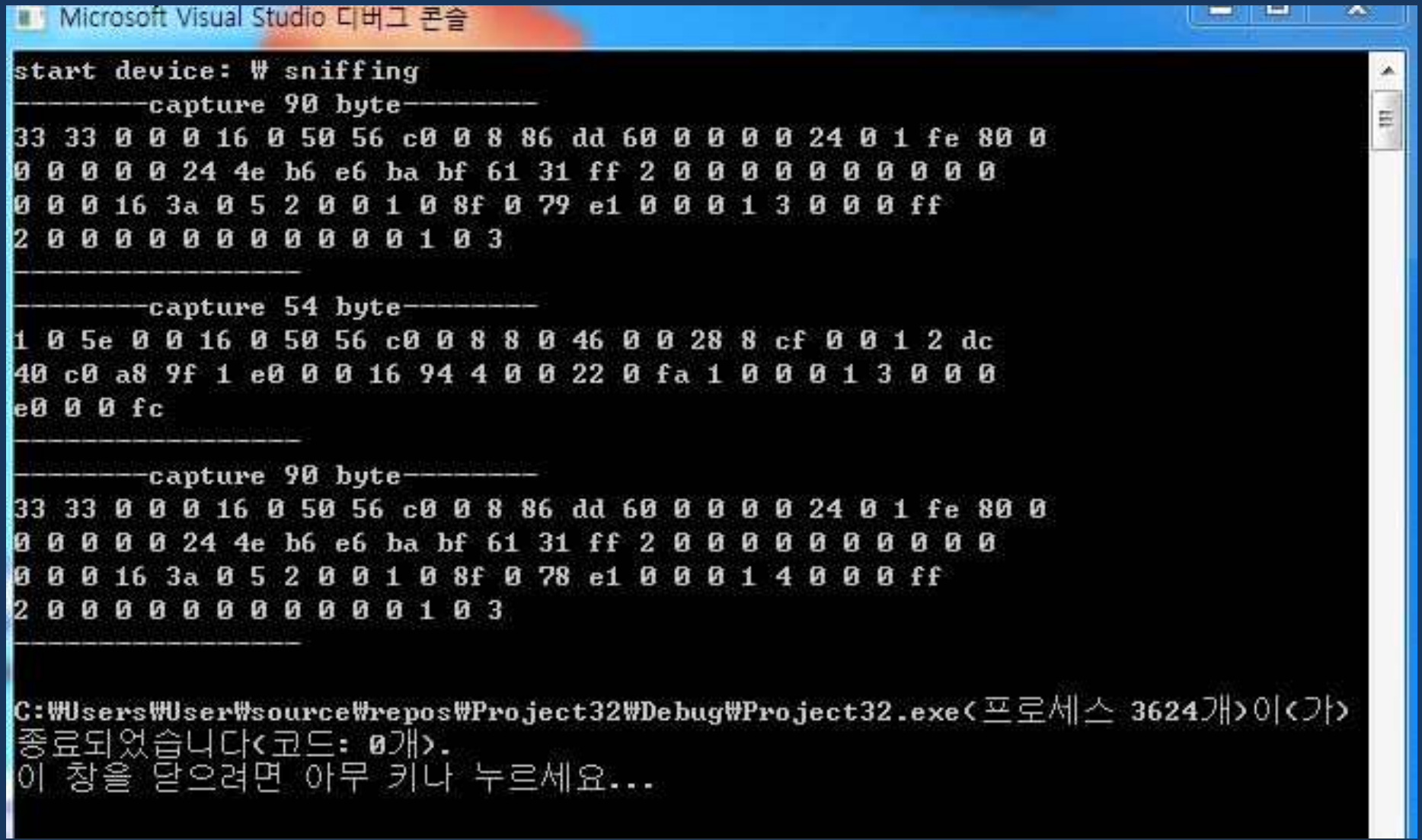
```
    <<<  패킷  >>>

보낸 MAC : 00 d0 cb 7a 41 43
받는 MAC : d0 94 66 f6 d5 ba
(TCP)Src IP : 112.161.34.224
(TCP)Des IP : 35.224.165.216
=========종료========

    <<<  패킷  >>>

보낸 MAC : 00 d0 cb 7a 41 43
받는 MAC : d0 94 66 f6 d5 ba
(TCP)Src IP : 112.161.34.224
(TCP)Des IP : 35.224.165.216
=========종료========

    <<<  패킷  >>>

보낸 MAC : 00 d0 cb 7a 41 43
받는 MAC : d0 94 66 f6 d5 ba
(TCP)Src IP : 112.161.34.224
(TCP)Des IP : 35.224.165.216
=========종료========
```

소스코드 (여승철)

: C언어로 코딩 // 윈도우에서 구현

승철 sniff.c

03


Microsoft Visual Studio 디버그 콘솔
start device: W sniffing
--------capture 90 byte--------
33 33 0 0 0 16 0 50 56 c0 0 8 86 dd 60 0 0 0 0 24 0 1 fe 80 0
0 0 0 0 0 24 4e b6 e6 ba bf 61 31 ff 2 0 0 0 0 0 0 0 0 0 0
0 0 0 16 3a 0 5 2 0 0 1 0 8f 0 79 e1 0 0 0 1 3 0 0 0 ff
2 0 0 0 0 0 0 0 0 0 0 0 1 0 3
--------capture 54 byte--------
1 0 5e 0 0 16 0 50 56 c0 0 8 8 0 46 0 0 28 8 cf 0 0 1 2 dc
40 c0 a8 9f 1 e0 0 0 16 94 4 0 0 22 0 fa 1 0 0 0 1 3 0 0 0
e0 0 0 fc
--------capture 90 byte--------
33 33 0 0 0 16 0 50 56 c0 0 8 86 dd 60 0 0 0 0 24 0 1 fe 80 0
0 0 0 0 0 24 4e b6 e6 ba bf 61 31 ff 2 0 0 0 0 0 0 0 0 0 0
0 0 0 16 3a 0 5 2 0 0 1 0 8f 0 78 e1 0 0 0 1 4 0 0 0 ff
2 0 0 0 0 0 0 0 0 0 0 0 1 0 3
C:WUsersWUserWsourceWreposWProject32WDebugWProject32.exe(프로세스 3624개)이(가)
종료되었습니다(코드: 0개).
이 창을 닫으려면 아무 키나 누르세요...

THANK YOU