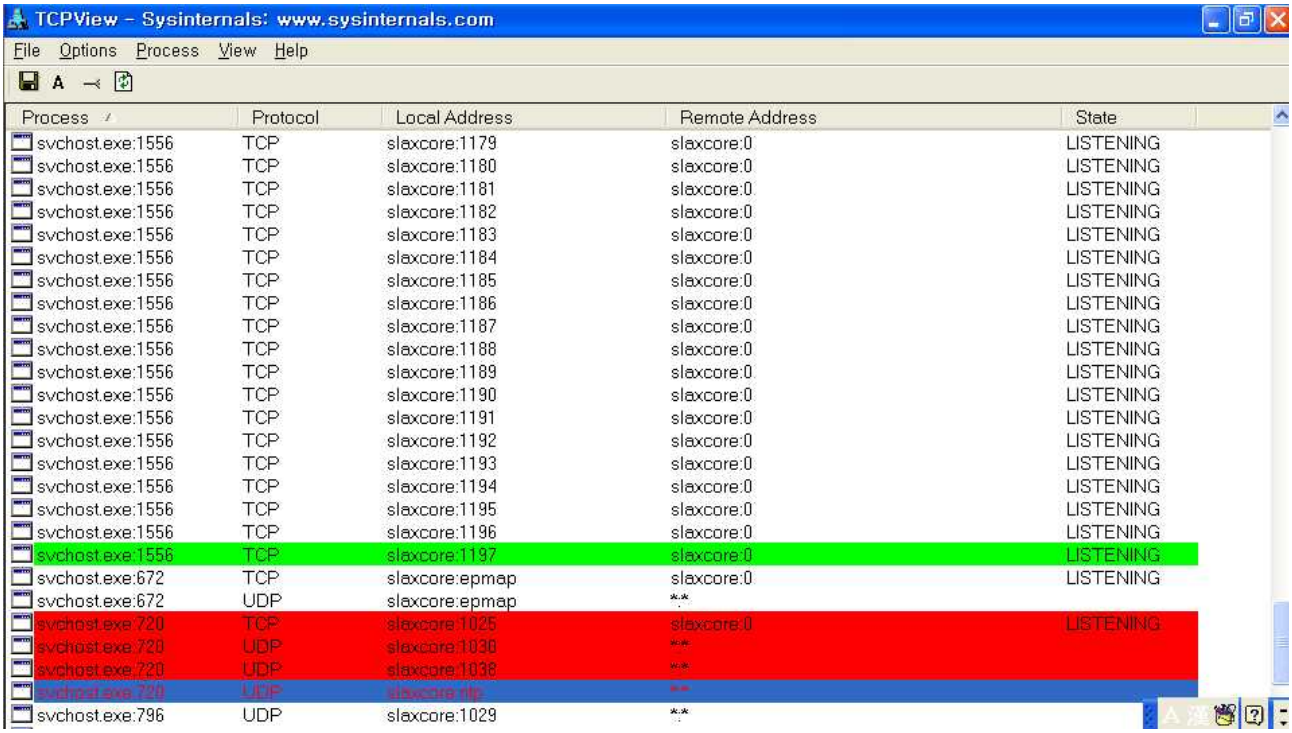
TCP View란? sysinternals이라는 제작사에서 만든 프리웨어로 로컬 및 원격 주소와 TCP 연결의 상태를 포함하여 시스템에 있는 모든 TCP와 UDP 자세한 목록이 표시됩니다. Window Server 2008, Vista, NT, 2000 및 XP에서도 TCP와 UDP를 소유하는 프로세스의 이름을 보고 합니다.
제작사의 사이트인 http://www.sysinternals.com 에서 다운로드 하면 됩니다. 따로 설치할 필요가 없으며, Tcpview.exe를 실행하시면 실행됩니다.



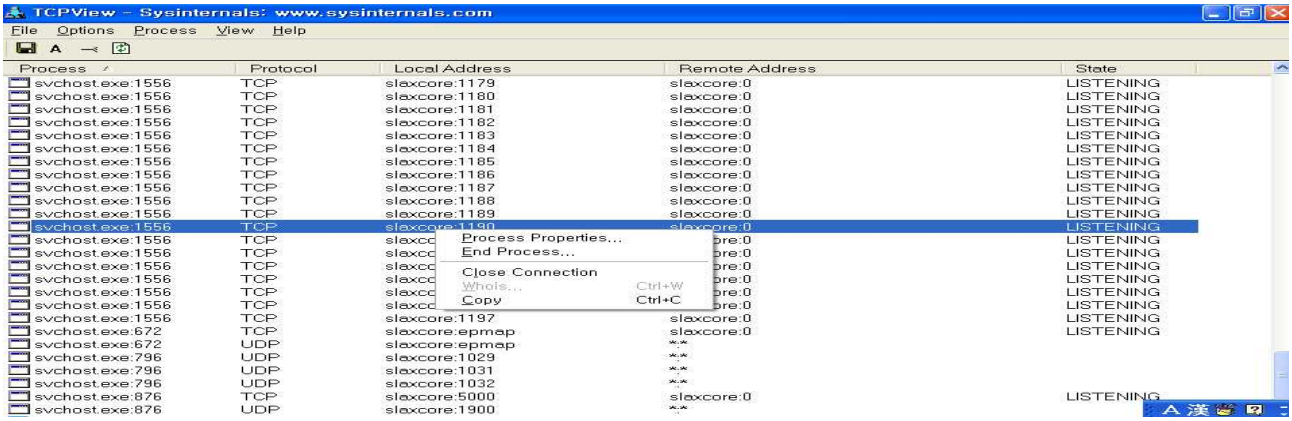
TCP View 프로그램 구동 화면

1. TCP View 프로그램 각 항목 설명

- Process : 현재 실행 중인 프로세스를 [프로세스파일명 : PID]로 표시합니다.
- Protocol : 프로토콜의 종류가 TCP(Transmission Control Protocol)인지 UDP(User Datagram Protocol)인지 표시합니다.
- Local Address : 해당 프로세스가 사용하고 있는 포트번호를 [유저이름 : 포트번호]로 표시합니다.
- Remote Address : 해당 프로세스와 연결되어 있는 외부 시스템의 IP주소 또는 도메인명과 포트번호입니다.
- State : 해당 포트의 연결 상태를 표시합니다.
  ESTABLISHED : 연결되어 있는 상태를 말합니다.
  LISTENING : 현재 시스템에서 열려있는 포트를 말합니다.
  CLOSE_WAIT : 이미 연결이 끊어진 상태를 말합니다.

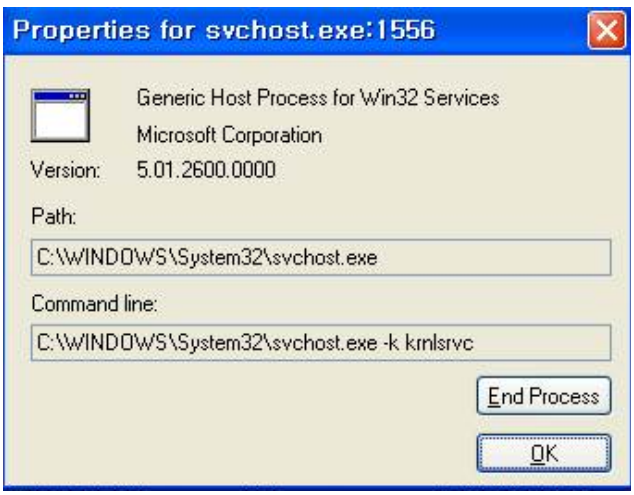
1-1. 화면을 자세히 보시면 초록색과 빨강색으로 칠해진 포트를 볼 수 있습니다. 초록색의 경우는 새로 생성되는 포트를 나타냅니다. 빨강색의 경우 종료되는 포트를 나타냅니다. 그렇다면 하얀색은 구동중인 프로세스를 나타낸다는 것을 알 수 있습니다.

2. TCP View 프로그램의 다른 기능

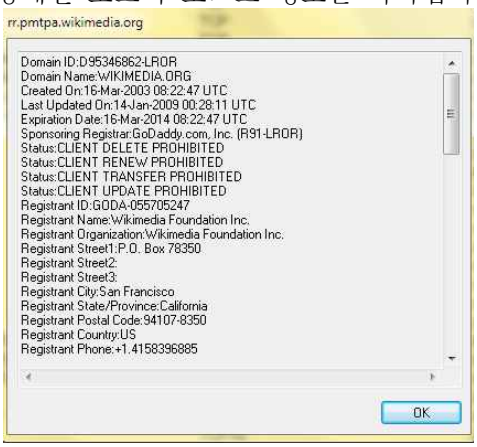


원하는 포트를 개별적으로 선택하신 후 마우스 오른쪽 버튼을 클릭하시면 그림과 같이 나옵니다.
각각의 기능에 대해 설명하겠습니다.

- Process Properties : 선택한 프로세스의 프로그램명, 버전, 프로그램의 경로 등을 표시합니다.



- End Process : 선택한 프로세스를 강제 종료합니다.
- Close Connection : 선택한 프로세스를 종료하지 않은 상태에서 현재 연결을 끊습니다.
- Whois : CLOSE_WAIT상태인 포트의 호스트 정보를 나타냅니다.



Whois에 의한 호스트 정보

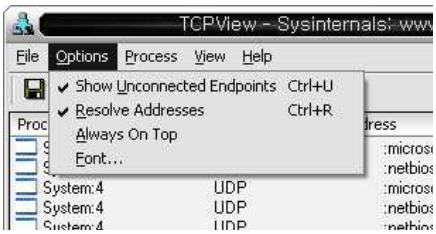
3. TCP View의 메뉴 설명

TCPView의 메뉴줄에 대해 간략하게 설명하겠습니다.

3-1. [File]

- Close Connection, Copy : 위에서 언급한 내용과 같습니다.
- Save, Save as : 현재 보이는 모든 정보를 TXT파일로 저장합니다.
- Close : TCPView를 종료합니다.

3-2. [Option]



- Show Unconnected Endpoint : 연결이 끊긴 정보도 보여줍니다. 해당 옵션을 선택하면 State가 ESTABLISHED 인 목록만 보여줍니다.
- Resolve Address : Local 및 Remote의 IP주소 대신 도메인 이름을 보여줍니다. 해당 옵션을 해제하면 숫자 IP로 보여줍니다.
- Always On Top: TCPView 창을 항상 최상위로 놓습니다.
- Font: 창의 글씨체, 크기를 선택할 수 있습니다.

3-3. [Porcess]

- Process Properties, End Process : 위에서 말한 내용과 같습니다.

3-4. [View]

- Update Speed: 프로세스 상태를 주기별로 새로고침합니다. 1초, 2초, 5초, 중지가 있습니다.
- Refresh Now: 새로고침 합니다. F5키나 아이콘을 클릭해도 됩니다.

4. 보안에서의 TCPView활용

만약 컴퓨터내에 악성 봇이나 멀웨어가 있다면, 이들 악성프로그램들은 주기적으로 자신에게 입력되어 있는 호스트에 접속을 요청하고, 강제로 포트를 개방하게 됩니다. 주기적으로 계속해서 어떠한 곳에 접속을 시도하거나 못 보던 포트가 열려있는 경우. 그 해당 포트의 프로세스를 악성프로그램으로 의심할 수 있습니다.

5. TCPView를 활용하는 법에 대해 알아보았습니다. 기타 추가적인 내용은 Help(도움말)을 통해 확인하거나 포럼에서 정보를 얻을 수 있을 것입니다.

http://forum.sysinternals.com/forum_topics.asp?FID=16

작성자 : 중부대학교 SCP회장 정혜성