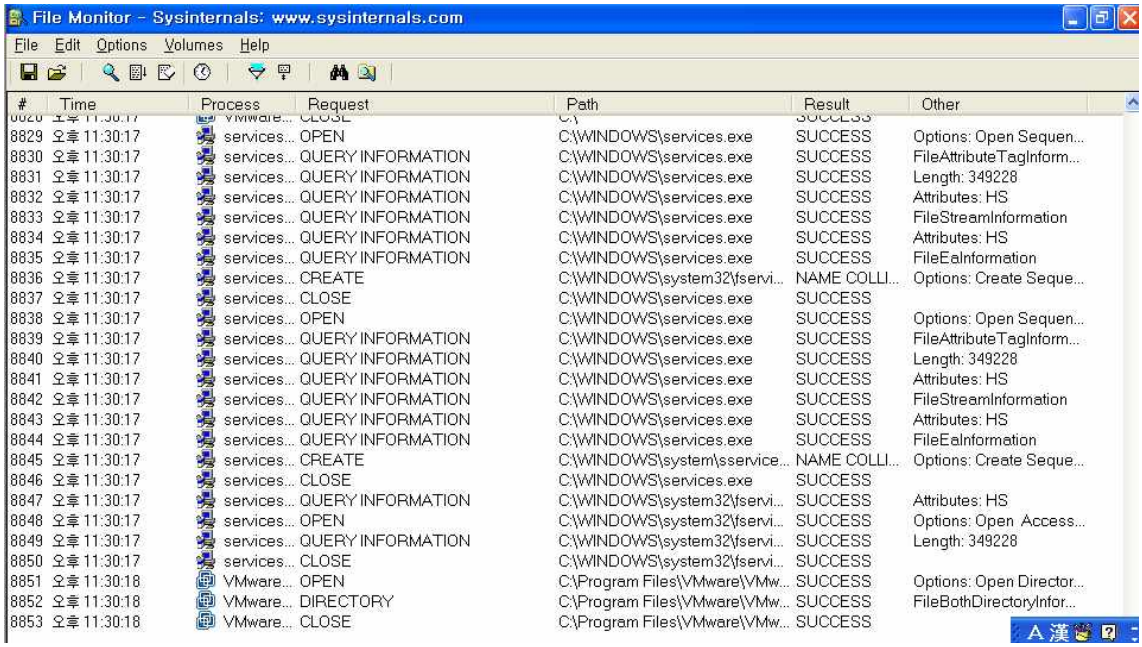
Filemon이란? sysinternals이라는 제작사에서 만든 프리웨어로 리얼타임으로 시스템에 있는 파일 시스템 활동, 프로그램의 생성, 삭제, 이동 등의 모든 이벤트를 모니터링해주는 소프트웨어입니다. 제작사의 사이트인 http://www.sysinternals.com 에서 다운로드 하면 됩니다. 따로 설치할 필요가 없으며, Filemon.exe를 실행하시면 실행됩니다.



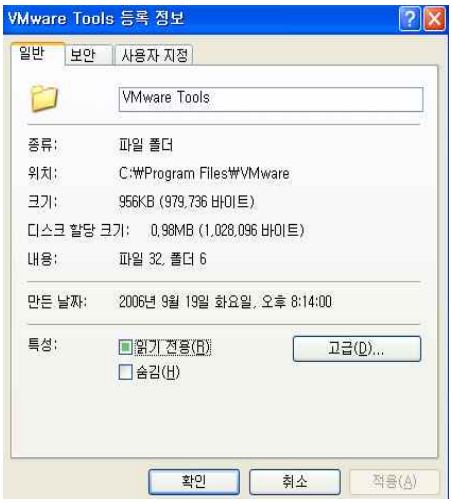
Filemon의 구동화면

1. Filemon의 메뉴구성.

Filemon의 메뉴구성에 대해 간략하게 말씀드리겠습니다.

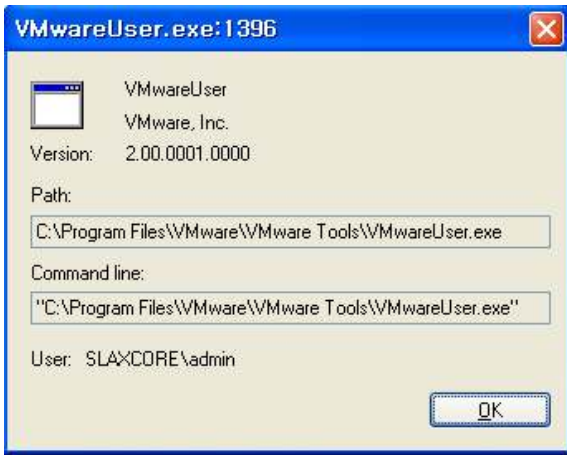
1-1. [File]

- Open : Filemon로그 파일을 엽니다.
- Save, Save as : 현재까지의 모니터링 정보를 로그파일로 저장합니다.
- Path Properties : 선택한 프로세스의 시스템 등록정보를 표시합니다.



Path Properties를 실행한 모습

- Process Properties : 선택한 프로세스의 경로와 레지스트리 값을 보여줍니다.

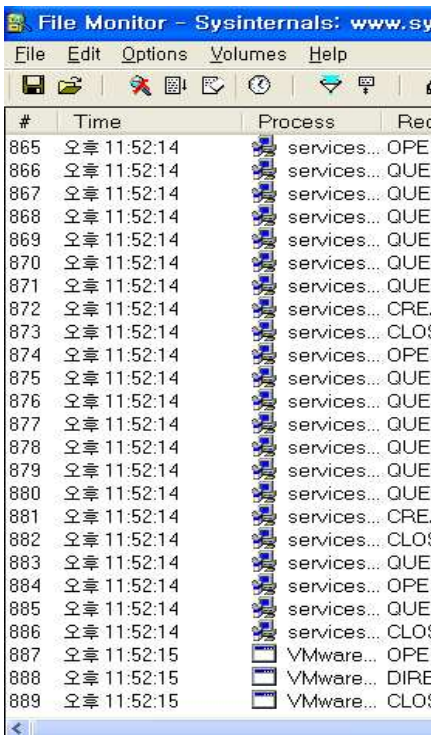


Process Properties를 실행한 모습

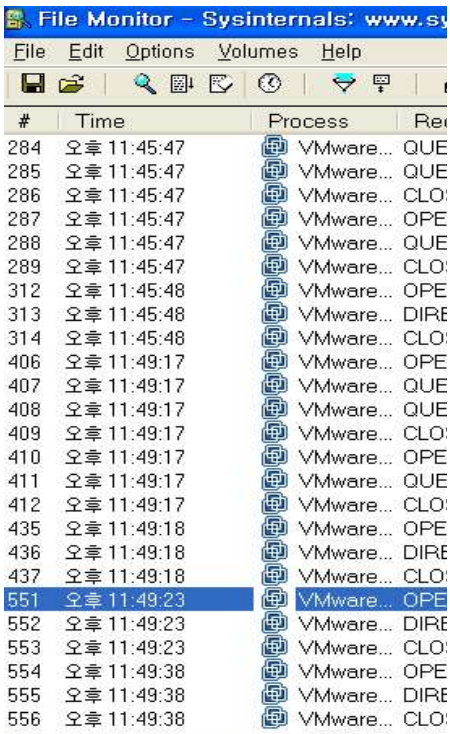
- Capture Events : 체크하면 모니터링을 실시하고, 해제하면 모니터링을 중지합니다.
- Exit : 프로그램을 종료합니다.

1-2. [Edit]

- Copy : 선택한 프로세스의 화면에 보이는 정보를 복사합니다.
- Delete : Filemon모니터링 상에서 삭제합니다.
- Include Process : 선택한 프로세스와 같은 프로세스만 화면상에 보여줍니다.

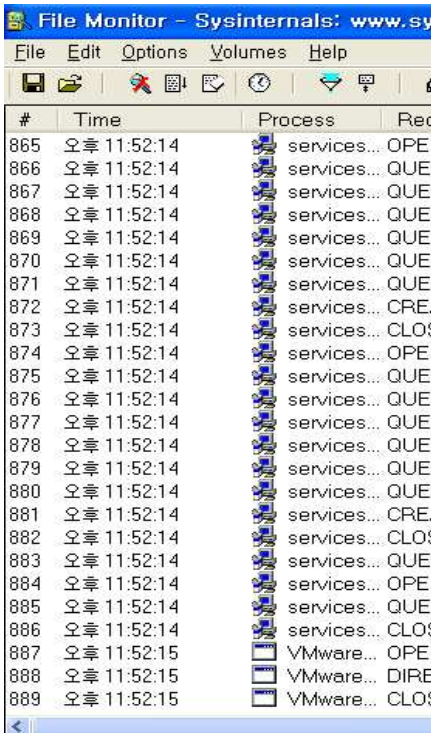


Include Process 선택 전

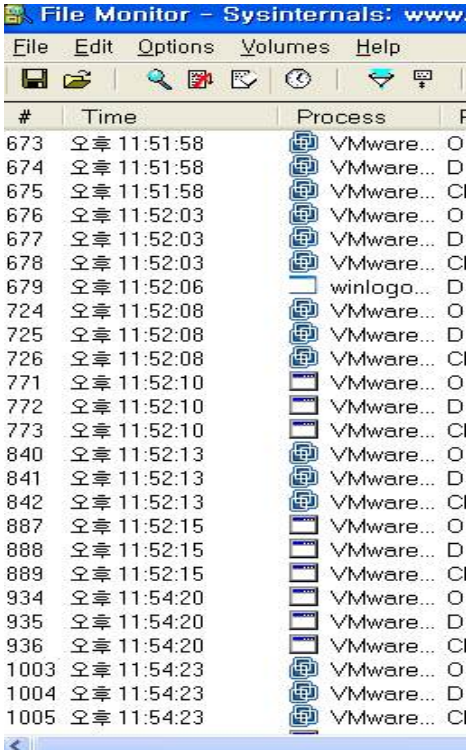


Include Process 선택 후

- Exclude Process : 선택한 프로세스와 같은 프로세스만 제외하고 화면상에 보여줍니다.

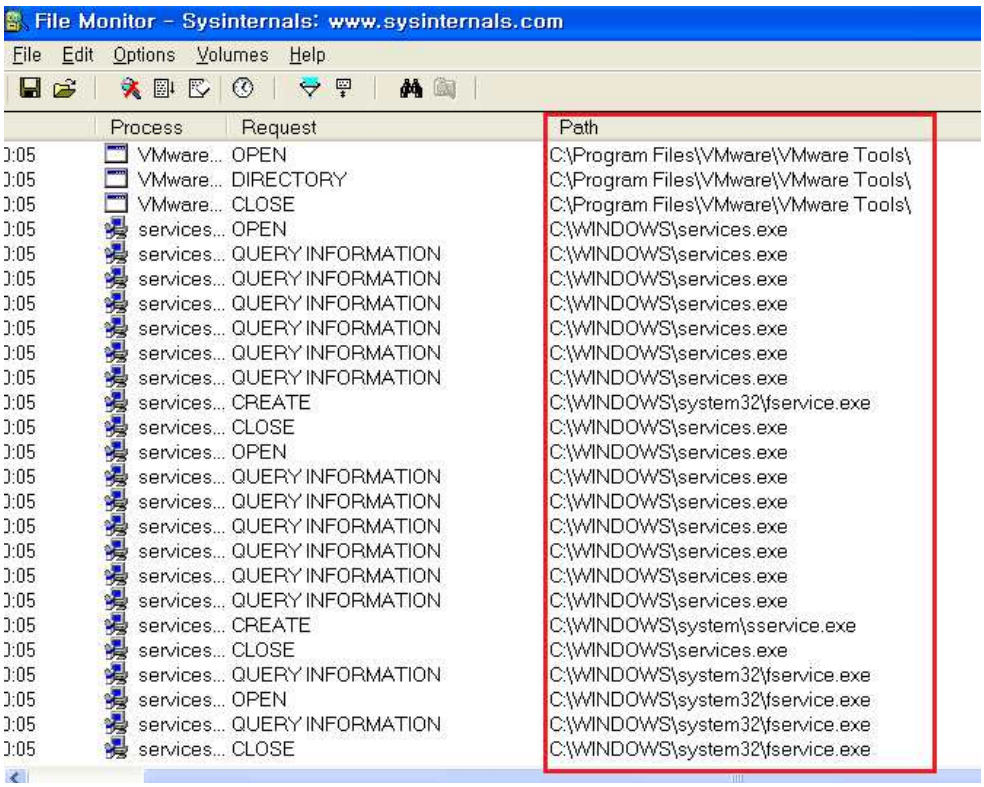


Exclude Process 선택 전

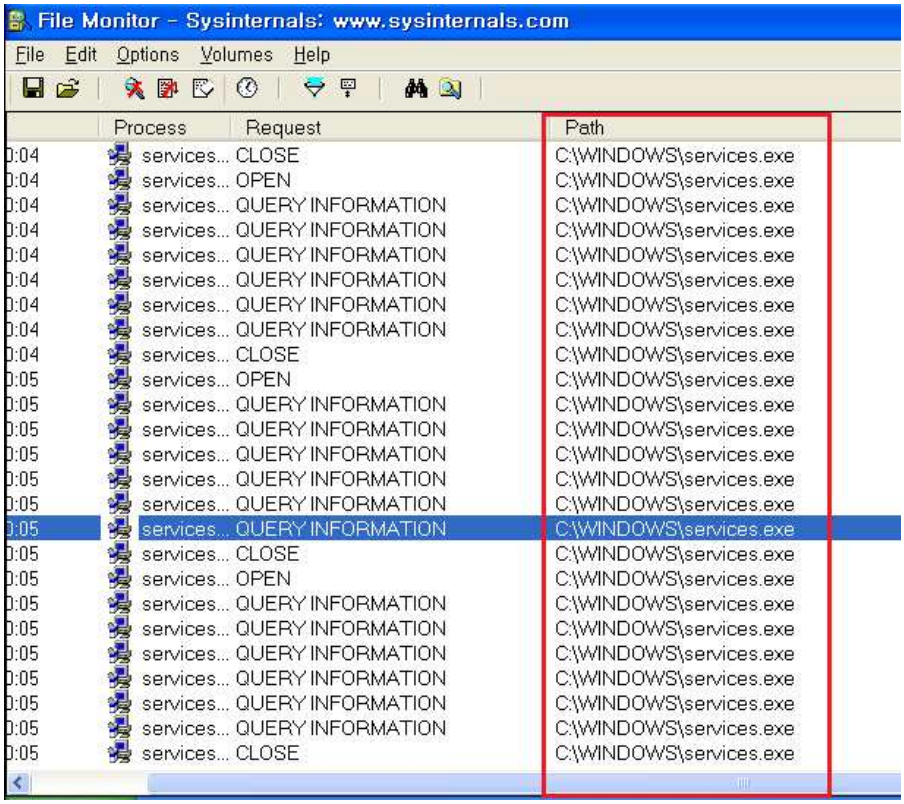


Exclude Process 선택 후

- Include Path : 선택한 프로세스와 같은 경로를 가지는 것만 화면상에 보여줍니다.

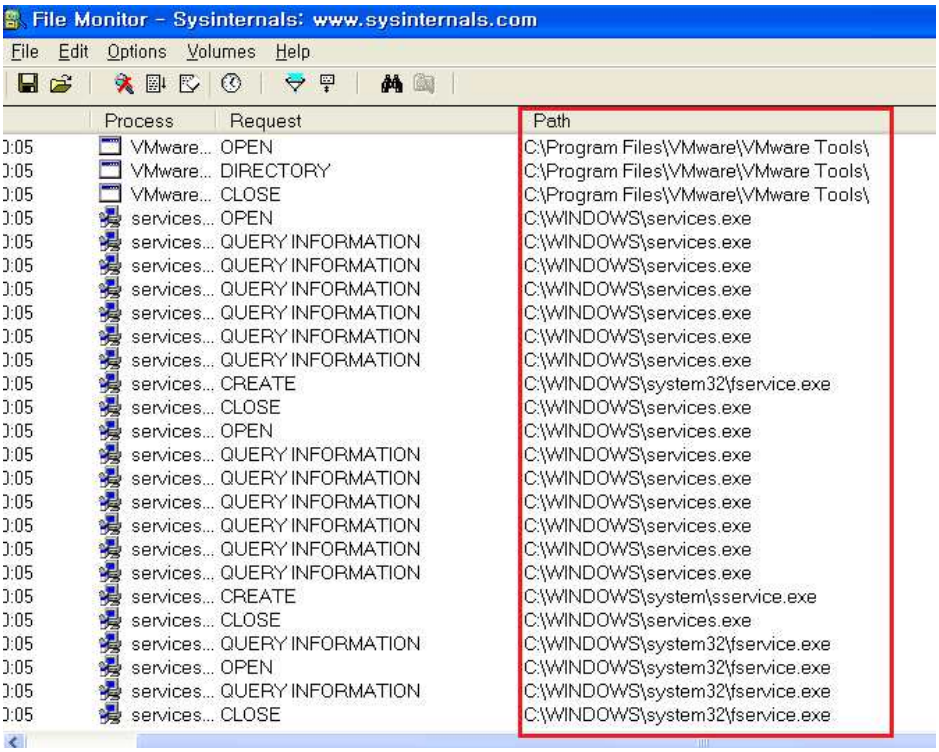


Include Path 실행 전

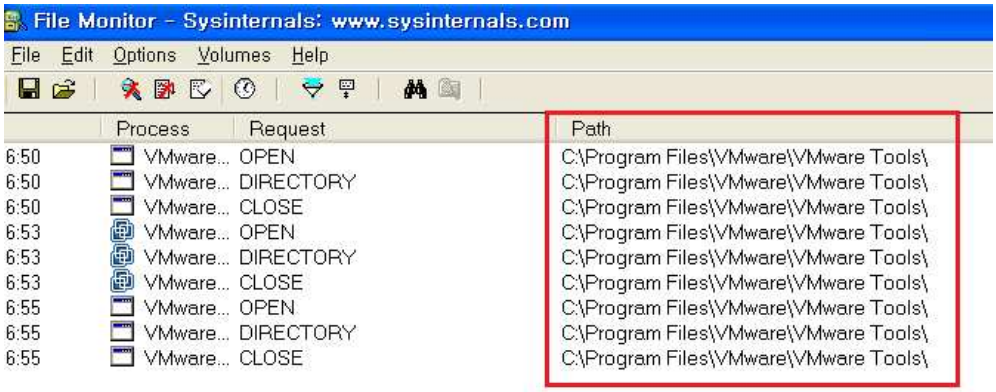


Include Path 실행 후

- Exclude Path : 선택한 프로세스와 같은 경로를 가지는 것만 제외하고 화면상에 보여줍니다.

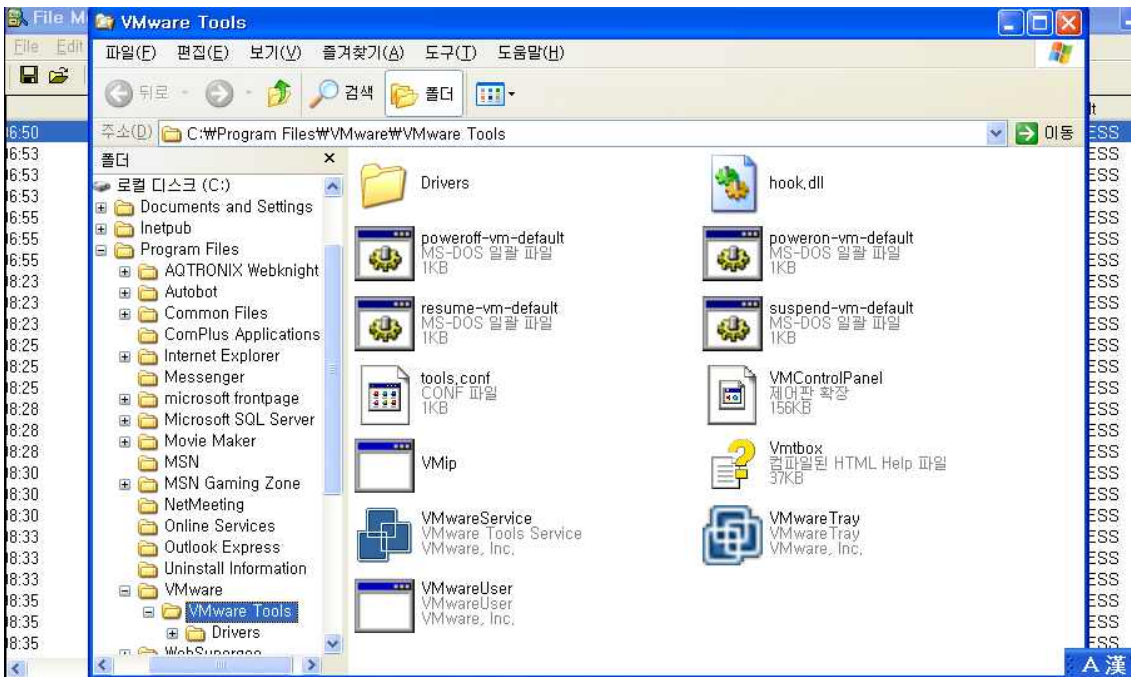


Exclude Path 실행 전



Exclude Path 실행 후

- Find : 입력 받은 키워드에 해당하는 곳을 찾아 갑니다.
- Explorer Jump : 선택한 프로세스의 폴더를 엽니다.



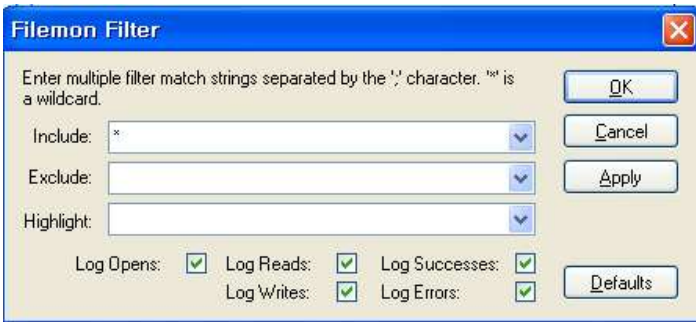
Explorer Jump를 실행한 모습

- Clear Display : 모니터링 화면을 초기화 시킵니다.

1-3. [Option]

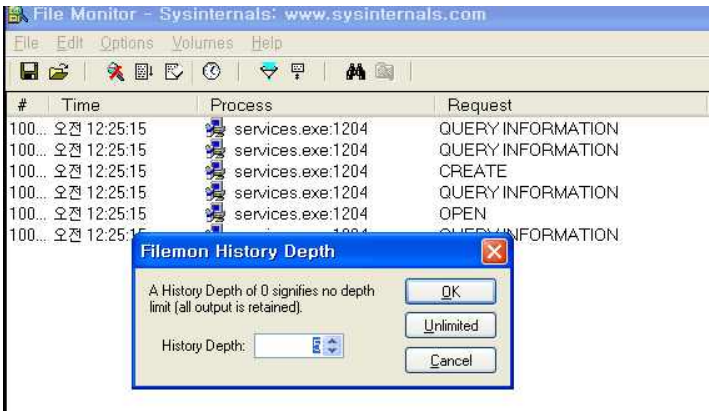
- Font : 글꼴을 수정 할 수 있습니다.
- Highlight Colors : 필터링에서 지정된 Highlight의 색을 결정할 수 있습니다.

- Filter/Highlight : 필터링과 Highlight를 설정 할 수 있습니다.
  Include는 입력된 값과 일치하는걸 보여줍니다.
  Exclude는 입력된 값과 일치하는 것은 제외합니다.
  Highlight는 입력된 값과 일치하는 것을 위에 옵션에서 설정된 색으로 보여줍니다.



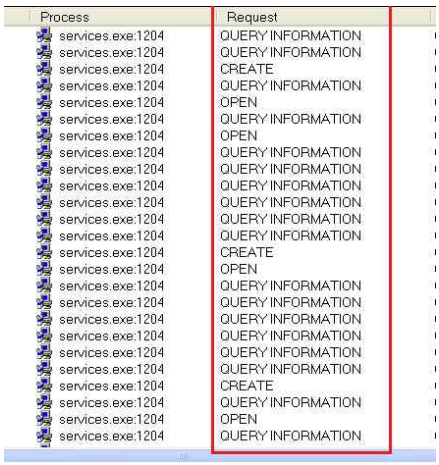
Filter/Highlight 실행화면

- History Depth : 화면에 모니터링하여 보여줄 개수를 정합니다. 입력된 숫자만큼만 보여주며, 기본설정은 0입니다. 0부터 시작하여 입력된 숫자까지의 개수만큼 보여줍니다.

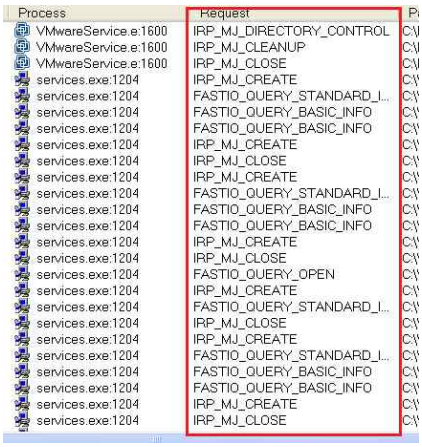


History Depth를 5로 설정한 모습

- Auto Scroll : 체크하면 스크롤을 자동으로 이동시키고, 해제하면 수동으로 이동시켜야 합니다.
- Advanced Output : 체크하면 Request를 좀 더 상세하게 보여줍니다.

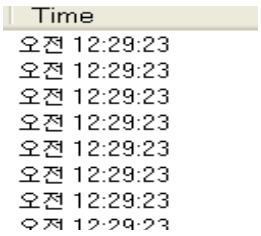


Advanced Output 체크하기 전

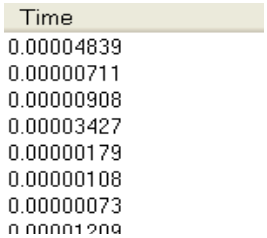


Advanced Output 체크 후

- Clock Time : 체크하면 Time항목을 시간 : 분 : 초 단위로 나타내고, 해제하면 프로그램이 실행되는데 걸린 시간을 소수점으로 나타냅니다.



Clock time 체크 전



Clock time 체크 후

- Show Milliseconds : Clock Time이 체크 되었을 경우만 체크 가능합니다. 체크할 경우 시간 항목을 밀리 초까지 표시 합니다.

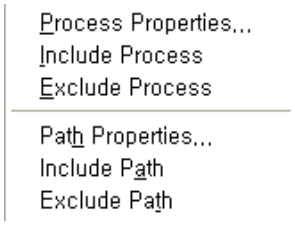
1-4. [Volume]
Volume은 모니터링을 할 것을 선택하는 메뉴입니다. Drive, Network, Mail Slot, Named Pipe 가 있습니다.

2. Filemon에서 개별선택과 화면구성

Filemon의 화면에 표시되는 항목에 대한 설명과 마우스 오른쪽 버튼을 통한 개별선택에 대해 말하겠습니다.

2-1. 화면구성
- # : 모니터링 한 것에 대한 번호입니다. 0부터 시작합니다.
- Time : 이벤트가 실행된 시간이나 실행되는데 걸리는 시간을 표시합니다.
- Process : 프로세스명과 PID을 표시합니다.
- Request : 파일이 한 행동에 대해 표시합니다.
- Path : 프로세서가 실행된 경로를 표시합니다.

2-2. 개별선택항목
프로세스를 선택하고 마우스 오른쪽 버튼을 누르면 다음과 같이 나옵니다. 나온 모든 메뉴는 위에서 언급했던 기능들과 같습니다.



3. 보안에서의 Filemon의 활용

보안에서 Filemon의 활용방법은 악성프로그램들의 대다수는 다른 프로세스와 연동하여 스스로를 계속 재생시키거나, 자기 자신을 계속하여 증식해나가는 형태를 취합니다. 이러한 프로세스가 재생되는 것과 증식해나가는 것에 대한 기록을 Filemon을 통해 알 수 있습니다. 이를 통해 서로 연동하고 있는 프로세스를 추적할 수가 있고, 증식해나가는 파일이 무엇을 매개체로해서 증식해나가는지를 알 수 있어 악성 프로그램을 추적하고 찾아내는데 용이하게 사용할 수 있습니다.

4. Filemon에 대한 활용방안과 설명이었습니다. 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