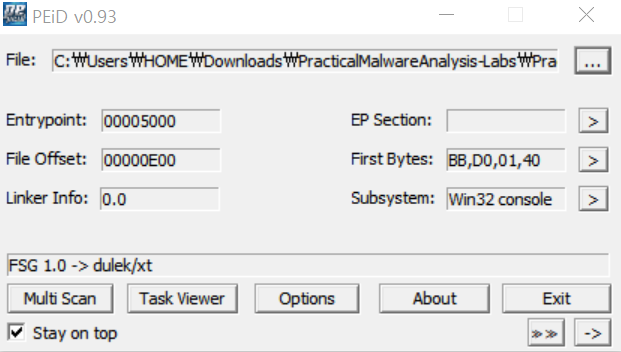
Lab01-03, Lab01-04 동적분석보고서

소프트웨어융합학과 2016111566 이나경

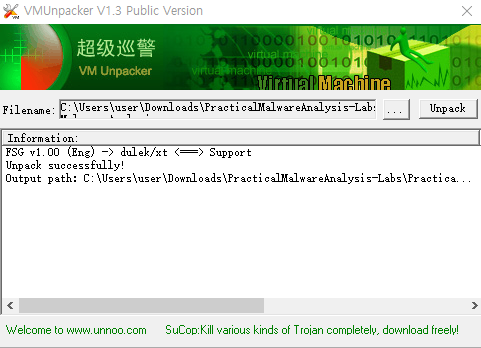
실습환경 : Windows XP(VMware 가상머신)

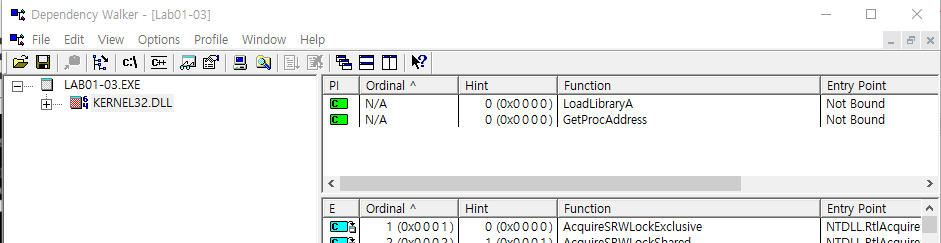
Tool : Process Monitor, Regshot, ApateDNS, wireshark 등

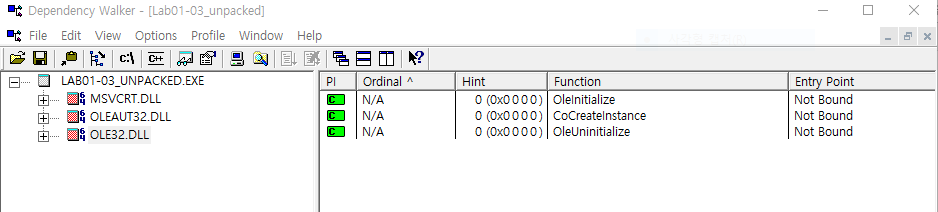
[1] Lab01-03의 정적분석결과에 따르면



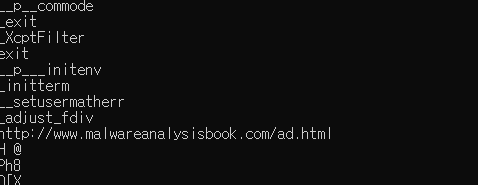
PEiD로 확인한 결과 FSG로 패킹되어있는 것을 알 수 있었다.



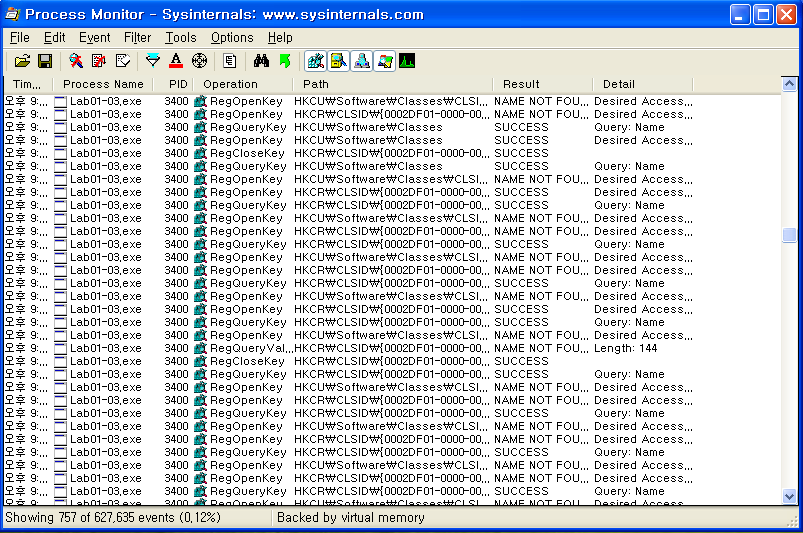




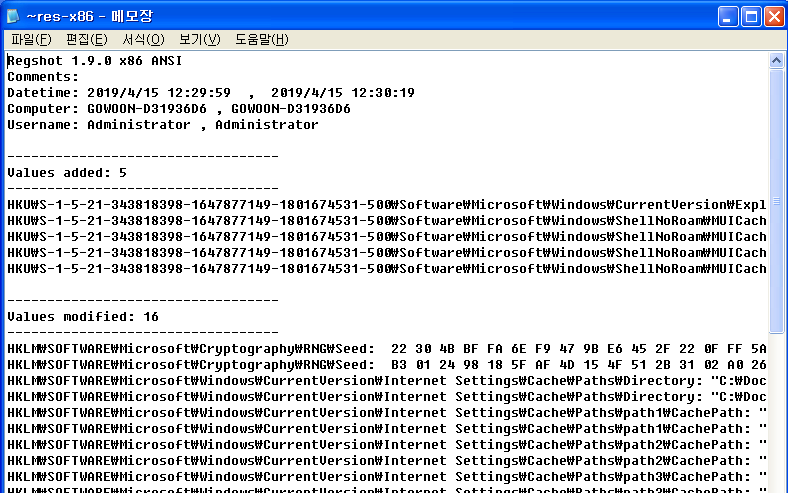
언팩하여 확인한 결과 LoadLibraryA, GetProcAddress, CoCreateInstance 등의 함수를 확인할 수 있었다.



strings로 확인한 결과 <http://www.malwareanalysisbook.com/ad.html> 라는 url을 확인할 수 있었다.



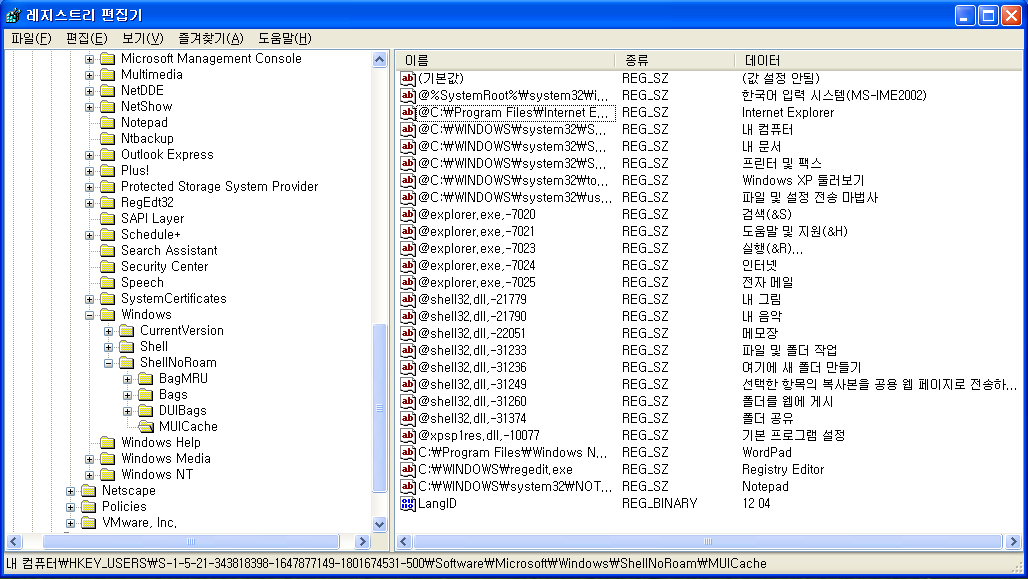
Process Monitor로 확인한 결과 레지스트리 관련된 활동이 많은 것을 확인할 수 있었다.



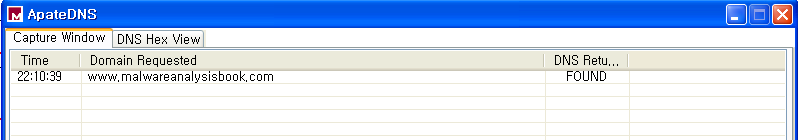
regshot으로 확인한 결과

Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Program Files\Internet Explorer\iexplore.exe: "Internet Explorer"

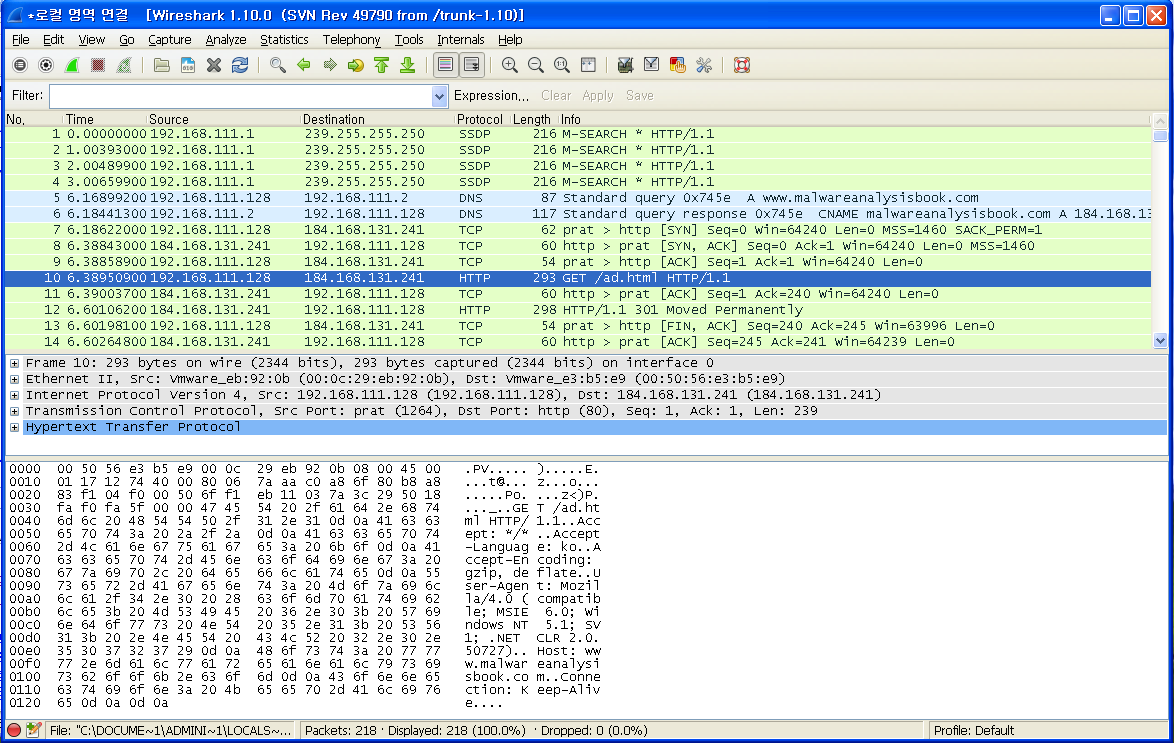
C:\WINDOWS\system32\NOTEPAD.EXE: "Notepad" 으로 등록된 것을 알 수 있다.



레지스트리편집기에서도 확인할 수 있었다.

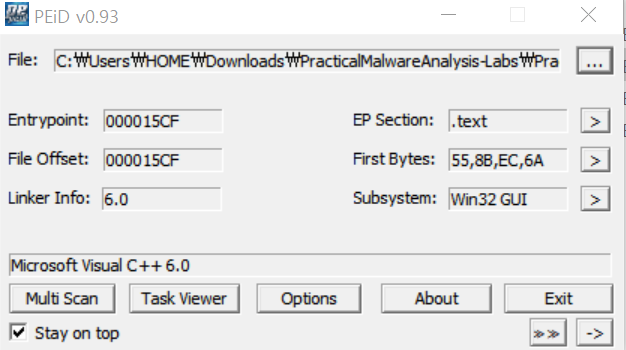


ApateDNS로 확인한 결과 [www.malwareanalysisbook.com](http://www.malwareanalysisbook.com)라는 주소에 접근하는 것을 확인할 수 있다.

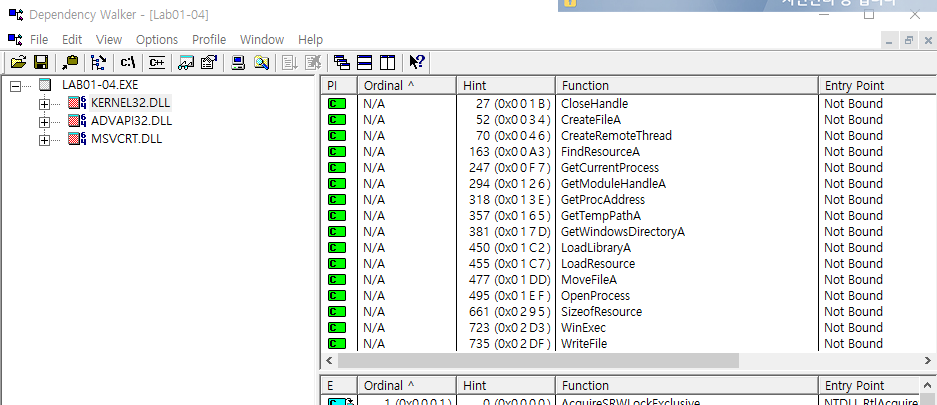


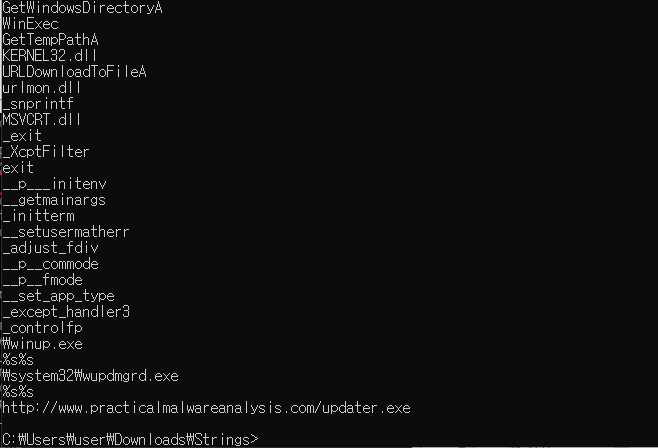
Wireshark로 확인한 결과 www.malwareanalysisbook.com 에 접속하는 것을 확인할 수 있다.

[2]Lab01-04의 정적분석결과에 따르면



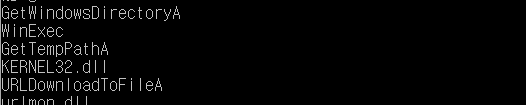
PEiD로 확인한 결과 패킹된 흔적은 없었다.

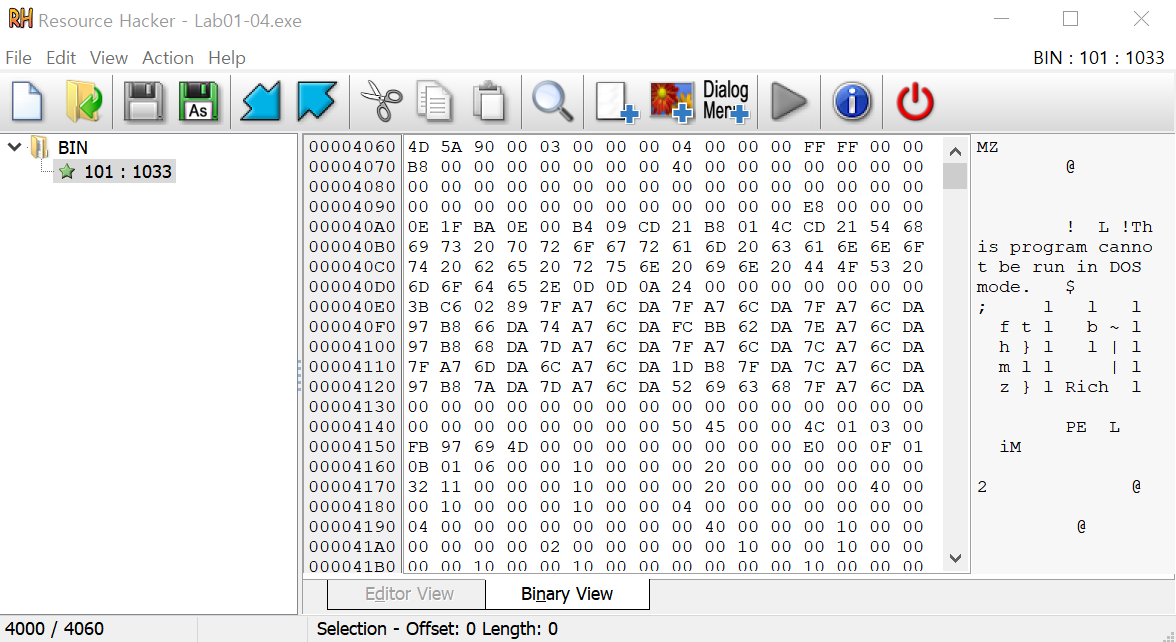




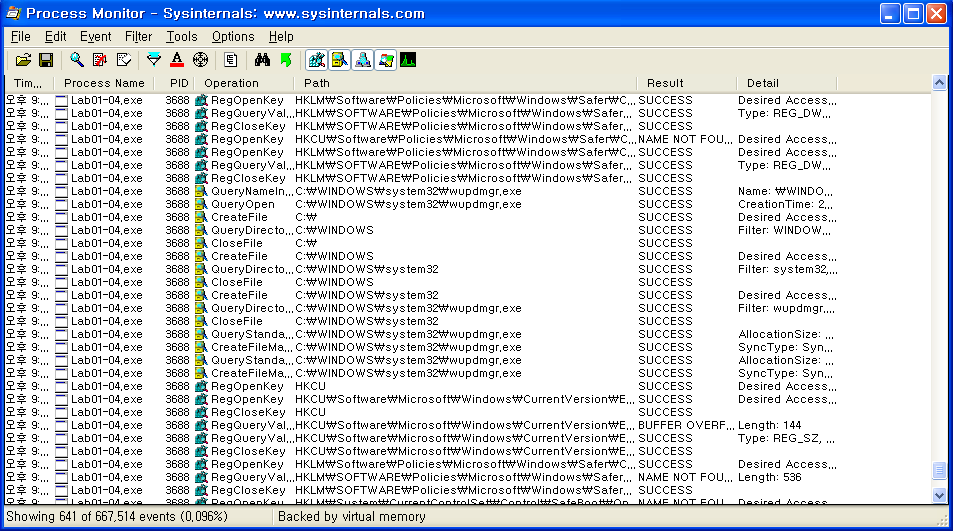
Dependency Walker와 Strings로 확인한 결과 CreateFileA, WriteFile, FindResourceA, LoadResource, WinExec 등의 함수를 확인할 수 있었다. 또한 URLDownloadToFileA라는 함수와

<http://www.practicalmalwareanalysis.com/updater.exe> 라는 url을 확인할 수 있었다.

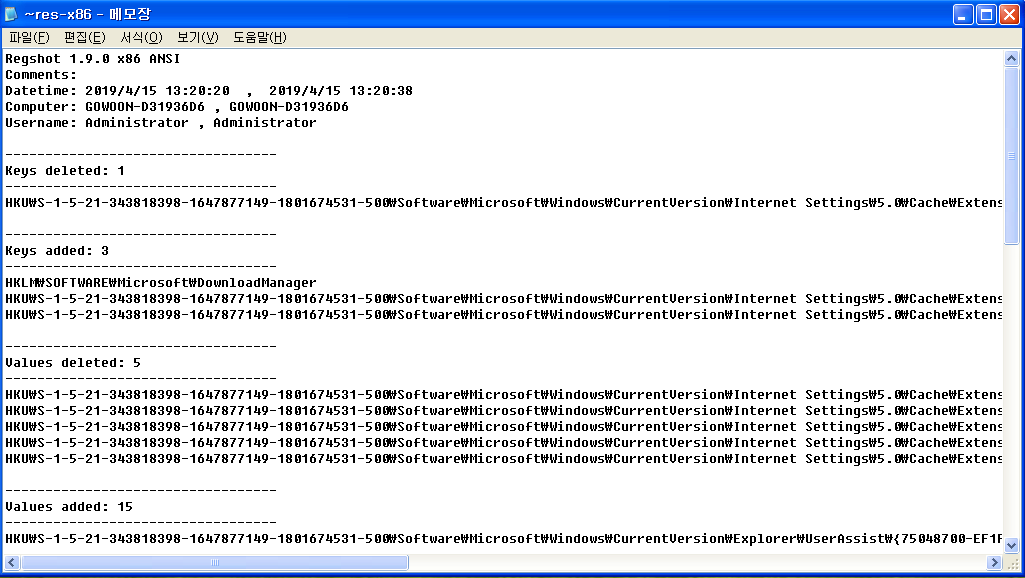




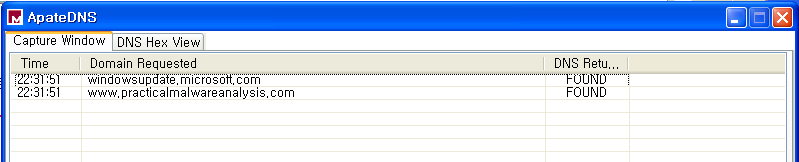
Resource Hacker를 이용해 리소스를 추출해 strings로 확인한 결과 GetWindowsDirectoryA, Get TempPathA, URLDownloadToFileA 등의 함수를 확인할 수 있었다. 이를 통해 무언가를 다운로드 하게 하는 파일임을 확인할 수 있었다.



Process Monitor을 통해 확인한 결과 \System32\wupdmgr.exe 해당 위치에 파일을 생성하거나 접근하는 것을 알 수 있다.

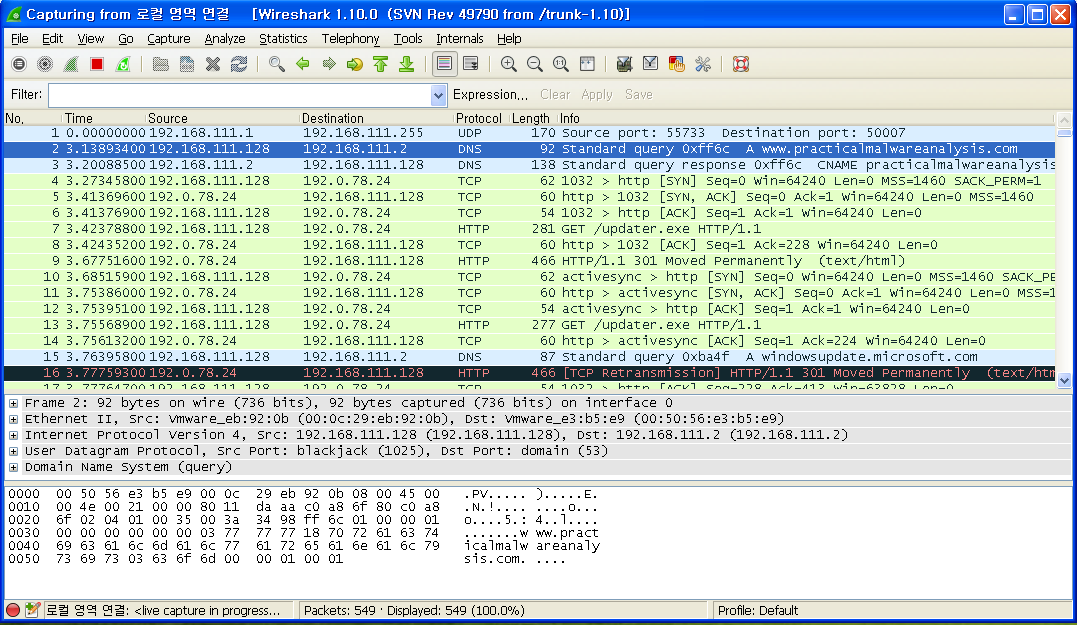


regshot으로 확인한 결과 HKLM\SOFTWARE\Microsoft 아래에 DownloadManager가 생성된 것을 알 수 있다.

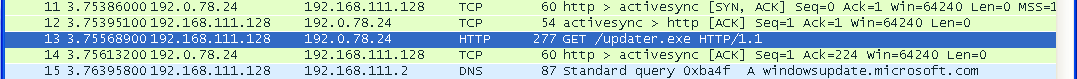


파일을 실행하면 윈도우 업데이트 서버에 접속하지만

ApateDNS로 확인한 결과 [www.practicalmalwareanalysis.com](http://www.practicalmalwareanalysis.com)라는 주소에 접근하는 것을 확인할 수 있다.



wireshark에서도 [www.practicalmalwareanalysis.com](http://www.malwareanalysisbook.com)주소에 접근하는 것을 확인할 수 있다.

그리고 이곳에서 updater.exe를 다운로드 받는것도 확인할 수 있다.

이에 대한 정보는 strings 에서도 확인이 가능하다.