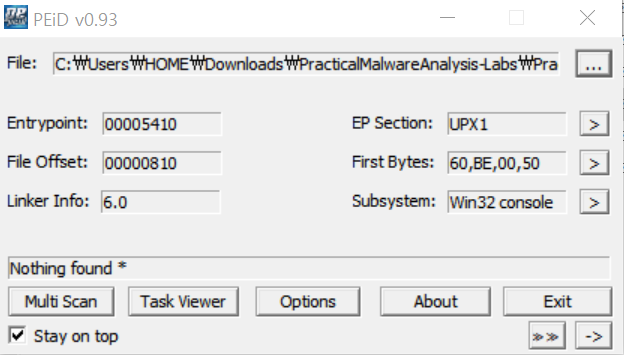
실습보고서5 2016111566 이나경

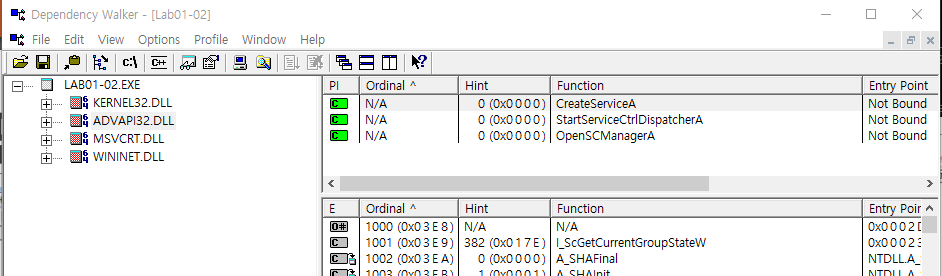
실습환경 : Windows XP(VMware 가상머신)

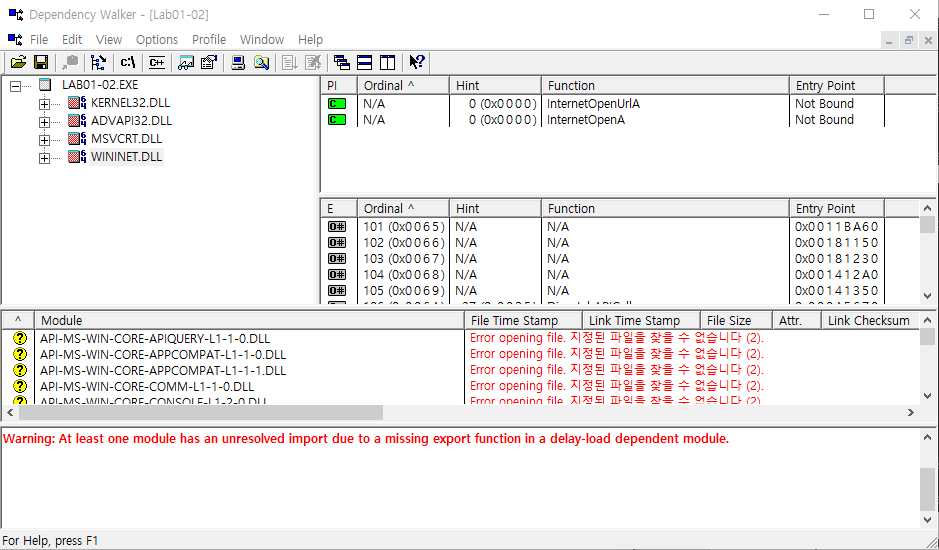
Tool : Process Monitor, Regshot, ApateDNS, wireshark 등

정적분석결과에 따르면



패킹되어있는 것을 알 수 있었고

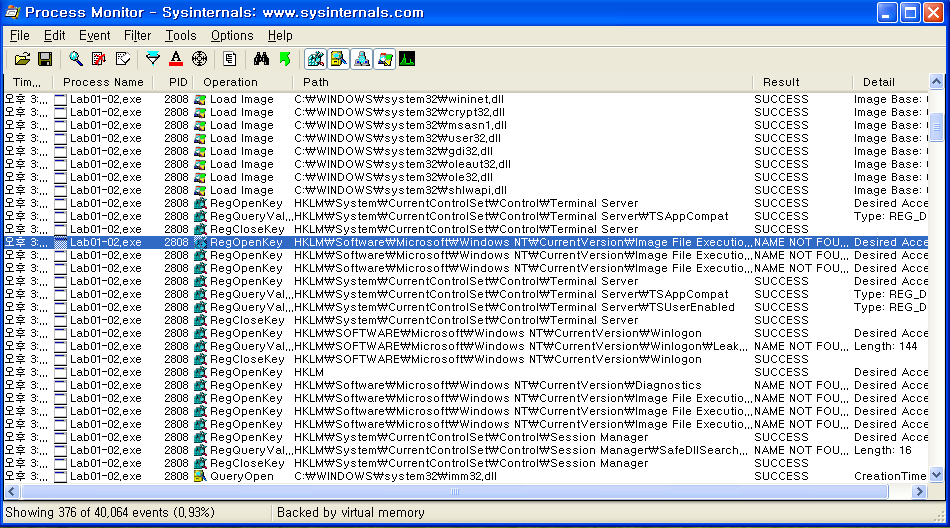




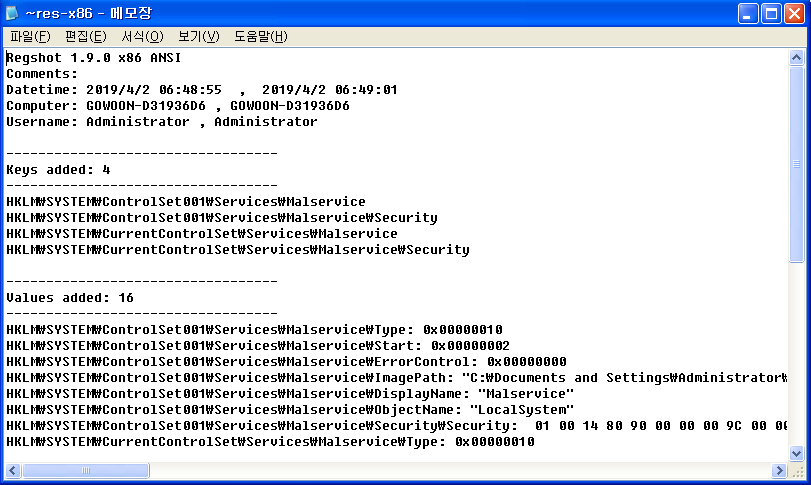
Dependency Walker에서 CreateServiceA, InternetOpenUrlA, InternetOpenA 등의 함수를 확인할 수 있었다.



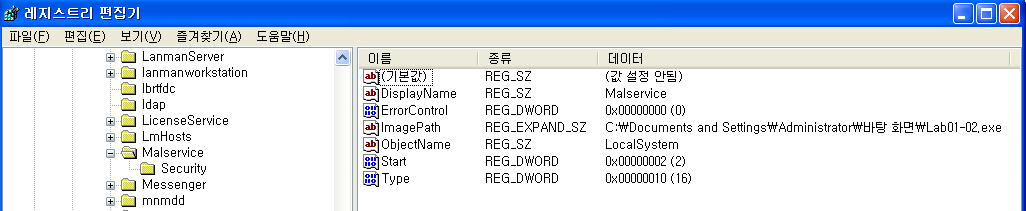
또한 언패킹 후 문자열을 확인한 결과 <http://www.malwareanalysisbook.com>라는 주소를 확인할 수 있었다. 따라서 네트워크상에서 더 깊이 분석해보기 위해 동적분석을 실시하였다.



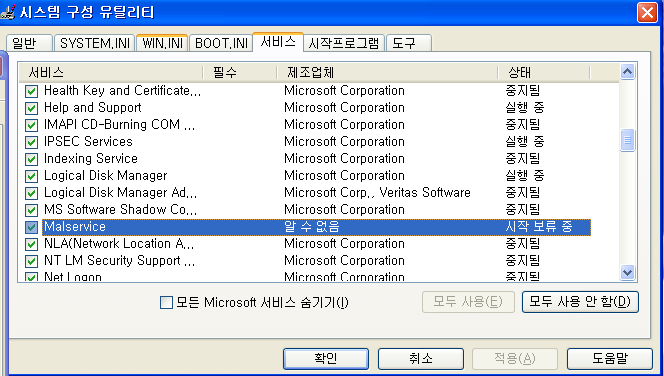
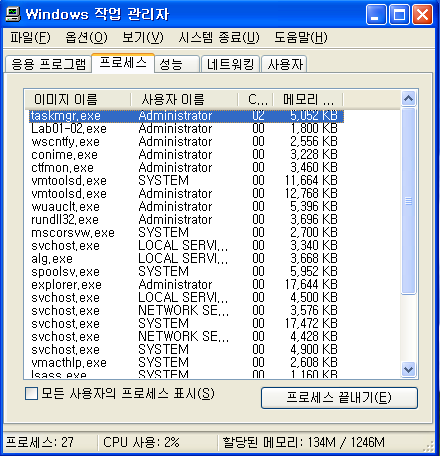
Process Monitor로 확인한 결과 레지스트리 관련된 활동이 많은 것을 확인할 수 있었다.



regshot으로 확인한 결과 SYSTEM\ControlSet001\Services 아래에 Malservice가 등록되었다는 것을 알 수 있다.



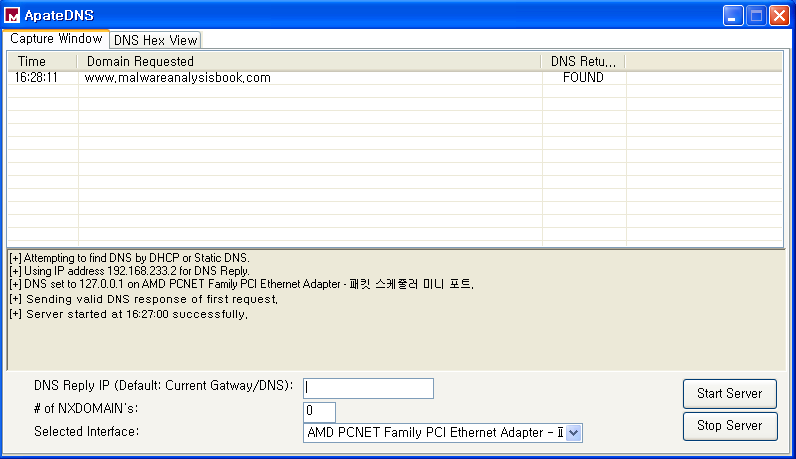
레지스트리 편집기에서 직접 확인한 결과 Lab01-02.exe에 의해 생성된 것임을 확인할 수 있다.



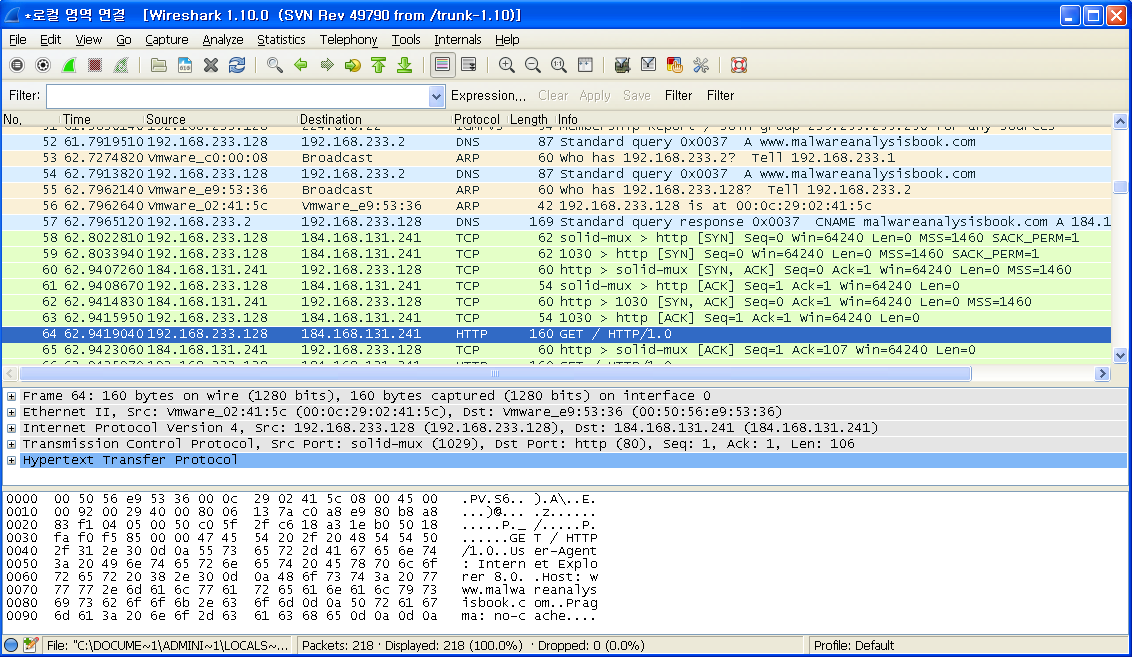
리부팅 후에 자동으로 재실행되는데

작업관리자 – 프로세스에서 Lab01-02.exe와

시스템 구성 유틸리티 – 서비스에서 시작 보류 중인 Malservice를 찾아볼 수 있다.



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



Wireshark로 확인한 결과 [www.malwareanalysisbook.com](http://www.malwareanalysisbook.com) 에 접속하는 것을 확인할 수 있다.

결론:

Lab01-02.exe는 패킹되었으나 일반실행이 가능하다.

Regshot과 regedit으로 확인한 결과 레지스트리에 Malservice가 등록된다.

리부팅 후에 자동실행된다.

ApateDNS와 wireshark로 확인한 결과 [www.malwareanalysisbook.com](http://www.malwareanalysisbook.com)라는 주소에 접근한다.