



Malware Analysis

Sang YOUNG CISSP CISA CIFI CHFI CEH CFSA ACE

Program Committee
ws.young@pisa.org.hk



Topics

- ① Essential Requirement for Forensic Analysis
- ② Malware Identification Process
- ③ Freeware Tools



Forensic Analysis Requirements

- Backup the system
 - Forensic Backup
- Minimize the changes to the system
- Don't run command on the victim system
 - We need Incident Response Toolkits



Forensic Backup

- Creating Bit-stream Copies
 - Including contents of deleted files, unallocated space, bad sectors
- Verify with Cryptographic Checksum
 - md5, sha1

Incident Response Toolkits

- Contains the tools & utilities
- Operating System Tools/Commands
 - cmd.exe, netstat.exe, nbtstat.exe, arp.exe, ipconfig.exe
 - Static Binary (Unix, Linux)
- From 3rd parties
 - Foundstone : fport
 - Sysinternals : Autoruns, Process Explorer
- Others : netcat, md5sum



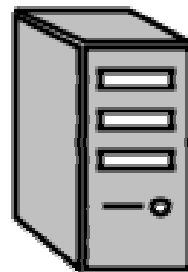
Analysis Procedures

- Backup the Disk
- Rebuild it to Virtual Environment
- Boot the Virtual Environment
- Identify Rogue Listening Port
- Identify Rogue Process which creating ports
- Identify the Startup Methods

Forensic Copy

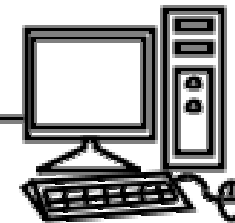
- Live Disk Cloning

Victim System



Forensic WorkStation

192.168.1.100

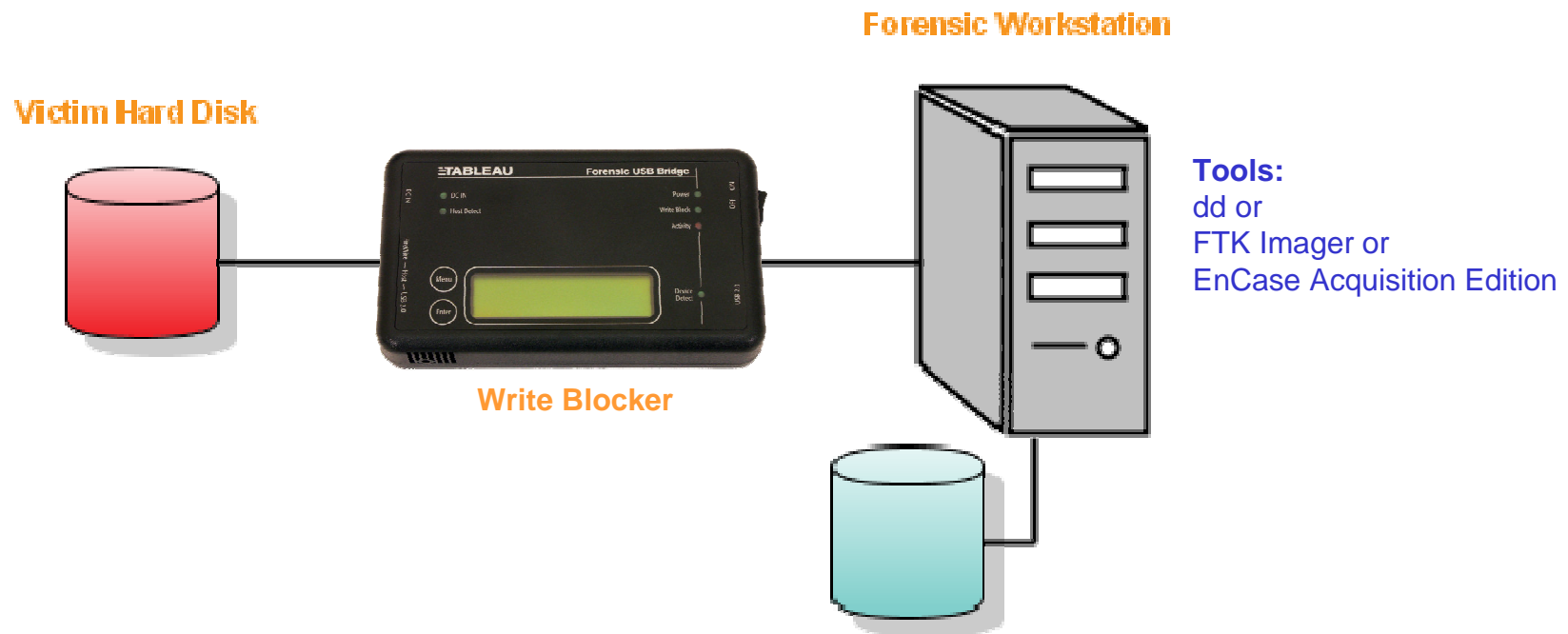


D:\>dd if=\\.\PhysicalDrive0 | nc 192.168.1.100 9000

C:\>nc -l 9000 > image.dd

Forensic Copy

- Offline Cloning

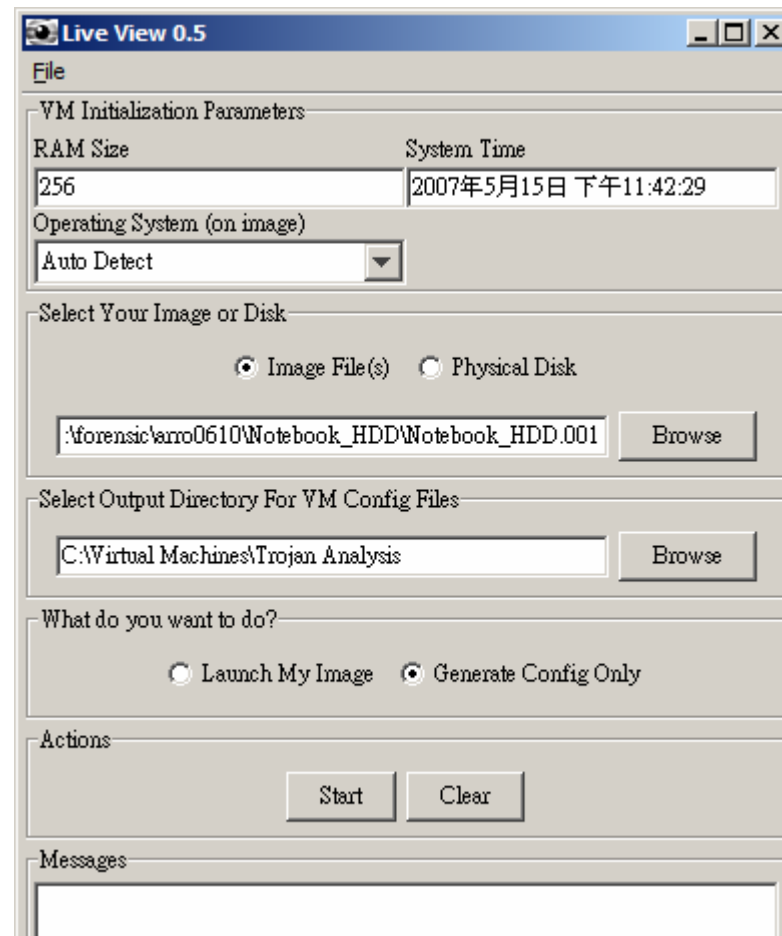




Convert to Virtual Environment

- Tools
 - Convert disk image (raw) to VMware
<http://liveview.sourceforge.net>
 - Run it in the VMware environment
<http://www.vmware.com>

Liveview Example





Using IRT #1

- Finding rogue listening port
 - netstat –an
- Finding the process of opening the rogue port
 - fport -p

Using IRT #2

- Kill the process
 - pskill #
- Locate the trojan executable file
 - dir <<path of the trojan image >>
 - dir /a <<path of the trojan image >>
- Remove the file
- Reboot the Computer
- Verify Again



Using IRT #3

- Identify the auto start methods for the Trojan
 - Autoruns
- Optional
 - Process Explorer

Manual Removing Trojans

- Suspend the processes
- Kill all the processes
- Delete the trojans files
 - move is required in some cases
- Delete the registry key
 - Using regdelnull from www.sysinternals.com
e.g. regdelnull hklm\software
- Reboot to verify
- Monitor using Process/File/Registry Mon



IR & Forensic CD

- Helix
 - <http://www.e-fense.com/helix>



Other References

- www.sysinternals.com
 - autoruns, procexp, pslist, pskill
- www.foundstone.com
 - fport



About PISA

- A not-for-profit organization for local information security professionals.
- Focus on developing the local information security market with a global presence in the industry



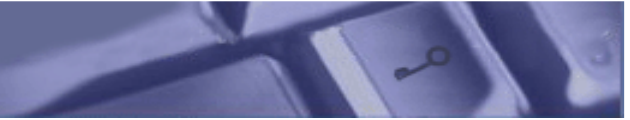
Mission

- to facilitate knowledge and information sharing among the PISA members
- to promote the highest quality of technical and ethical standards to the information security profession,
- to promote best-practices in information security control,
- to promote security awareness to the IT industry and general public in Hong Kong



Contact PISA

- Web Site:
 - <http://www.pisa.org.hk>
- Membership Information:
 - <http://www.pisa.org.hk/membership/member.htm>



Thank you for listening