# A Comprehensive Guide to Digital Forensics for Practical Incident Response

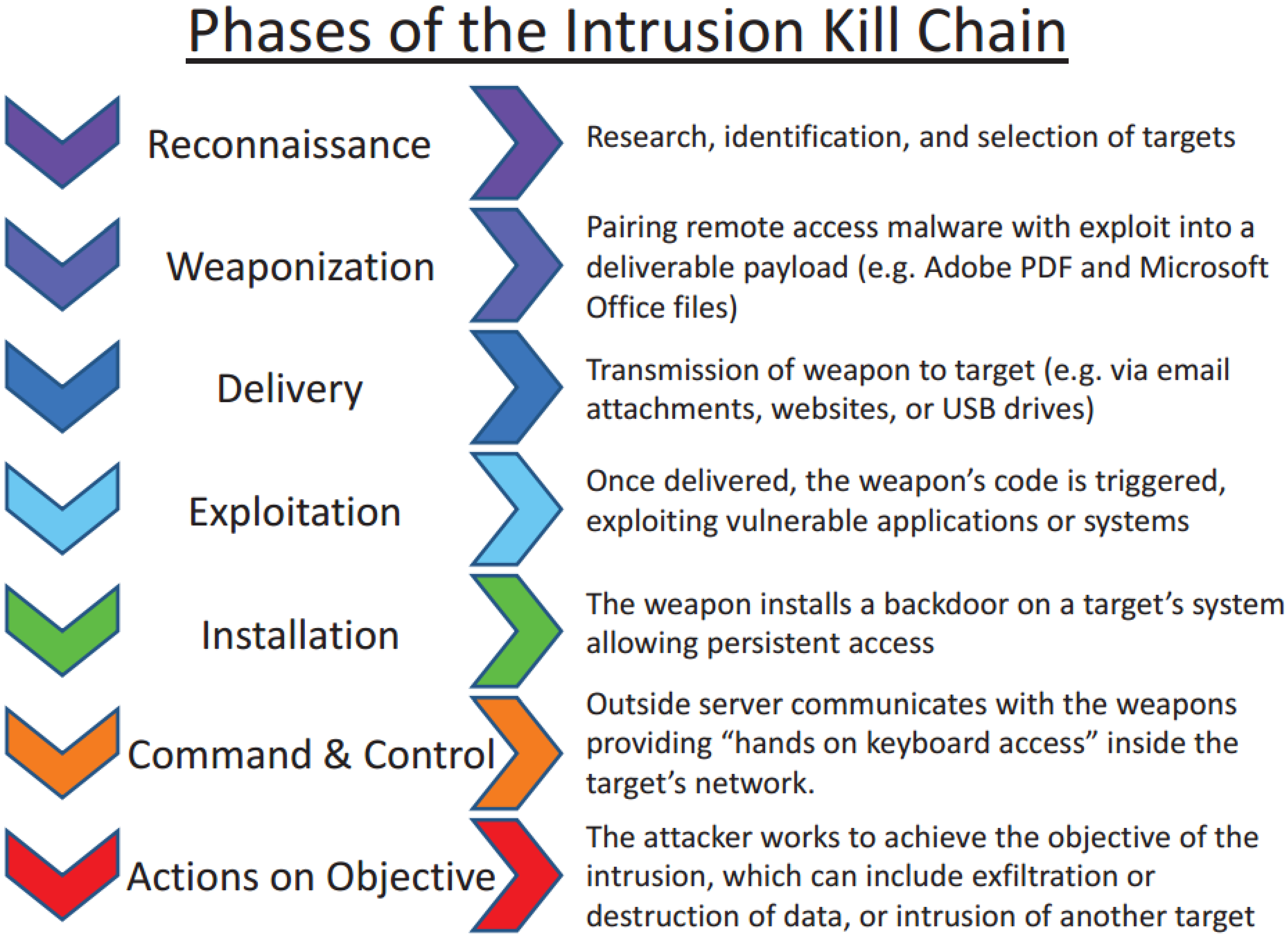
Internet Initiative Japan Inc.

Hiroshi Suzuki / Hisao Nashiwa

# The Concepts of Our Course

# The Concepts of Our Course

- We have recreated an attack scenario obtained from actual targeted attack incidents. You can learn incident response strategies and skills through the scenario.
  - In addition, you can get knowledge of other attack methods that are not included in the scenario: we have extra artifacts and disk/memory images with attacks applied.



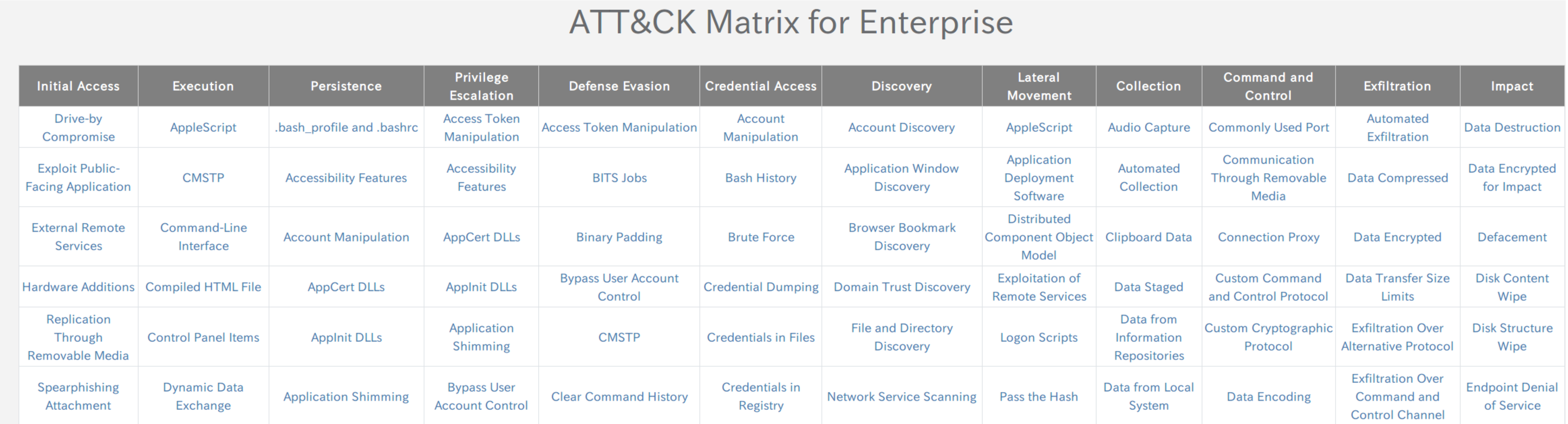
# Phases of the Intrusion Kill Chain

| | |
|---|---|
| Reconnaissance | Research, identification, and selection of targets |
| Weaponization | Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files) |
| Delivery | Transmission of weapon to target (e.g. via email attachments, websites, or USB drives) |
| Exploitation | Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems |
| Installation | The weapon installs a backdoor on a target's system allowing persistent access |
| Command & Control | Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network. |
| Actions on Objective | The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target |

https://en.wikipedia.org/wiki/File:Intrusion_Kill_Chain_-_v2.png

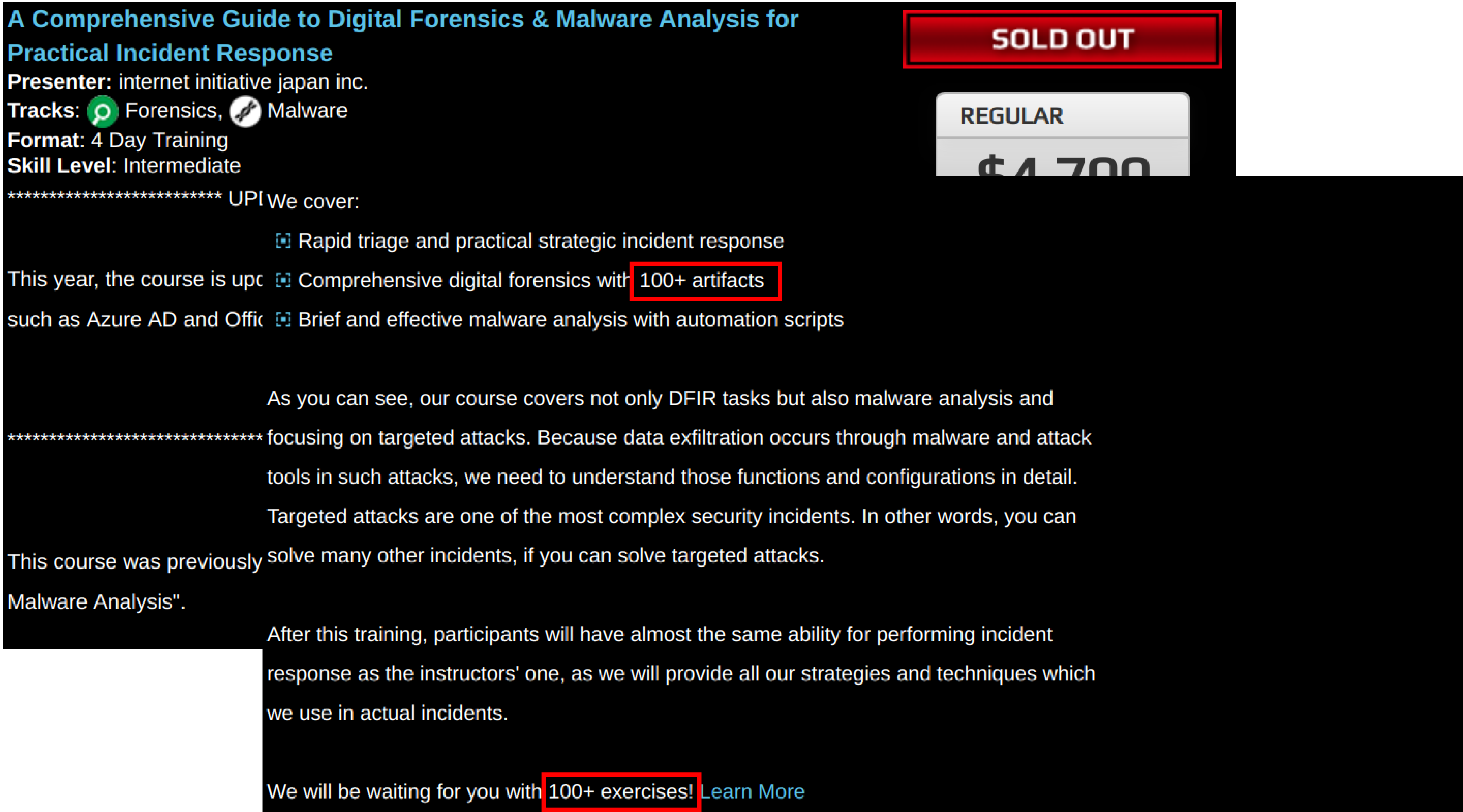
# ATT&CK

- ATT&CK Matrix for Enterprise
  - https://attack.mitre.org/matrices/enterprise/
- ATT&CK Navigator
  - https://mitre-attack.github.io/attack-navigator/enterprise/



ATT&CK Matrix for Enterprise

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Drive-by Compromise | AppleScript | .bash_profile and .bashrc | Access Token Manipulation | Access Token Manipulation | Account Manipulation | Account Discovery | AppleScript | Audio Capture | Commonly Used Port | Automated Exfiltration | Data Destruction |
| Exploit Public-Facing Application | CMSTP | Accessibility Features | Accessibility Features | BITS Jobs | Bash History | Application Window Discovery | Application Deployment Software | Automated Collection | Communication Through Removable Media | Data Compressed | Data Encrypted for Impact |
| External Remote Services | Command-Line Interface | Account Manipulation | AppCert DLLs | Binary Padding | Brute Force | Browser Bookmark Discovery | Distributed Component Object Model | Clipboard Data | Connection Proxy | Data Encrypted | Defacement |
| Hardware Additions | Compiled HTML File | AppCert DLLs | AppInit DLLs | Bypass User Account Control | Credential Dumping | Domain Trust Discovery | Exploitation of Remote Services | Data Staged | Custom Command and Control Protocol | Data Transfer Size Limits | Disk Content Wipe |
| Replication Through Removable Media | Control Panel Items | AppInit DLLs | Application Shimming | CMSTP | Credentials in Files | File and Directory Discovery | Logon Scripts | Data from Information Repositories | Custom Cryptographic Protocol | Exfiltration Over Alternative Protocol | Disk Structure Wipe |
| Spearphishing Attachment | Dynamic Data Exchange | Application Shimming | Bypass User Account Control | Clear Command History | Credentials in Registry | Network Service Scanning | Pass the Hash | Data from Local System | Data Encoding | Exfiltration Over Command and Control Channel | Endpoint Denial of Service |



## A Comprehensive Guide to Digital Forensics & Malware Analysis for Practical Incident Response

**Presenter:** internet initiative japan inc.
**Tracks**: Forensics, Malware
**Format**: 4 Day Training
**Skill Level**: Intermediate

************************** UPI

This year, the course is upc

such as Azure AD and Offic

*********************************

This course was previously

Malware Analysis".

We cover:

- Rapid triage and practical strategic incident response
- Comprehensive digital forensics with 100+ artifacts
- Brief and effective malware analysis with automation scripts

As you can see, our course covers not only DFIR tasks but also malware analysis and focusing on targeted attacks. Because data exfiltration occurs through malware and attack tools in such attacks, we need to understand those functions and configurations in detail. Targeted attacks are one of the most complex security incidents. In other words, you can solve many other incidents, if you can solve targeted attacks.

After this training, participants will have almost the same ability for performing incident response as the instructors' one, as we will provide all our strategies and techniques which we use in actual incidents.

We will be waiting for you with 100+ exercises! Learn More

# The Concepts of Our Course (Cont.)

- We will use well-prepared exercises to perform a large number of hands-on activities.
- We have prepared command outputs of processes that will take long in advance (e.g. file carving and keyword search on the entire disk images). Therefore, you will be able to get results as soon as you perform exercises.
  - Although you might be sometimes unsatisfied as you will not type commands by yourselves on some exercises, we think just doing them are not practical. Instead, we want you to spend time on performing a variety of hands-on exercises, analyzing the outputs from analysis tools, and investigating how attackers moved around in enterprise networks, as long as time permits.

# The Concepts of Our Course (Cont.)

- We do not use integrated computer forensics tools in this course, although we sometimes use them.
  - Encase (Commercial)
  - X-ways Forensics (Commercial)
  - FTK (Forensic Took Kit) (Commercial)
  - Axiom (Commercial)
  - Autopsy
  - Plaso
  - …
- We would like you to learn primitive computer forensics methods.
  - The tools might have bugs or they might be sometimes too slow for catching up the latest artifacts; this actually happened on Web Browsers artifacts in the past. If you are just using them without understanding their behaviors, it is hard to realize even when they do not show all the results.
  - In order to overcome such problems, there will be some cases where you will need to use simple dedicated tools for each artifact. Even if you own a suite software license, you should use these tools with it. And we would like you to learn primitive computer forensics techniques with these simple tools. It should help us in the future.

# Code of Conduct

# Code of Conduct for This Class

- Your neighbors are not your enemies.
- If your neighbors suffer from something what you have already understood, please help them out.
- Let's build a spirit of cooperation.

# Preparation for Our Training

# Attach USB storage to Your Physical Machine

- We will provide a USB storage that includes the whole contents for our class. DO NOT LOSE IT!!! We cannot give you extra copies.
  - You can find all documents including this document in the “Documents” folder on the storage. Please refer to it if necessary.
    - Documents\01_Introduction.pdf

# Instructions to Setup Your Environment

- Follow the instructions from next page to P.37 to setup the "AnalysisMachine". Roughly speaking, it consists of six steps.
    1. Enable Intel VT-x / AMD-V
    2. Disable Hyper-V.
    3. Start the VM.
    4. Update some contents for this training.
    5. Check to see if Fakenet-NG works well.
    6. Take a snapshot of your VM.

    - Let's do this together! If you have any questions or problems, please let us know.

# Enable Intel VT-x / AMD-V

- First, enable Intel VT-x / AMD-V.
  - You may continue to use the VM without the acceleration, but it will be slow.
    - For VirtualBox 6 users, you might not start the Analysis Machine if you don’t enable this due to a bug.
  - To modify virtualization acceleration settings, open BIOS/UEFI and configure “Intel VT-x” feature for Intel chipsets, and “AMD-V” feature for AMD chipsets.
    - To enter BIOS/UEFI, you will need to hit F2/F10/ESC key while restarting.
      - It depends on your PC vendor. Google it first if you don’t know.
  - Some PC vendors such as HP disable this feature by default.

# Disable Hyper-V To Use VMware or VirtualBox

- Before starting analysis machine, disable Hyper-V if you use Windows 10 Pro 1903 or later, or if you see a warning message about Intel VT-x or AMD-V while starting the VM.
- To do it, input the following command with administrator privilege. And reboot your machine.

```
bcdedit /set hypervisorlaunchtype off
```

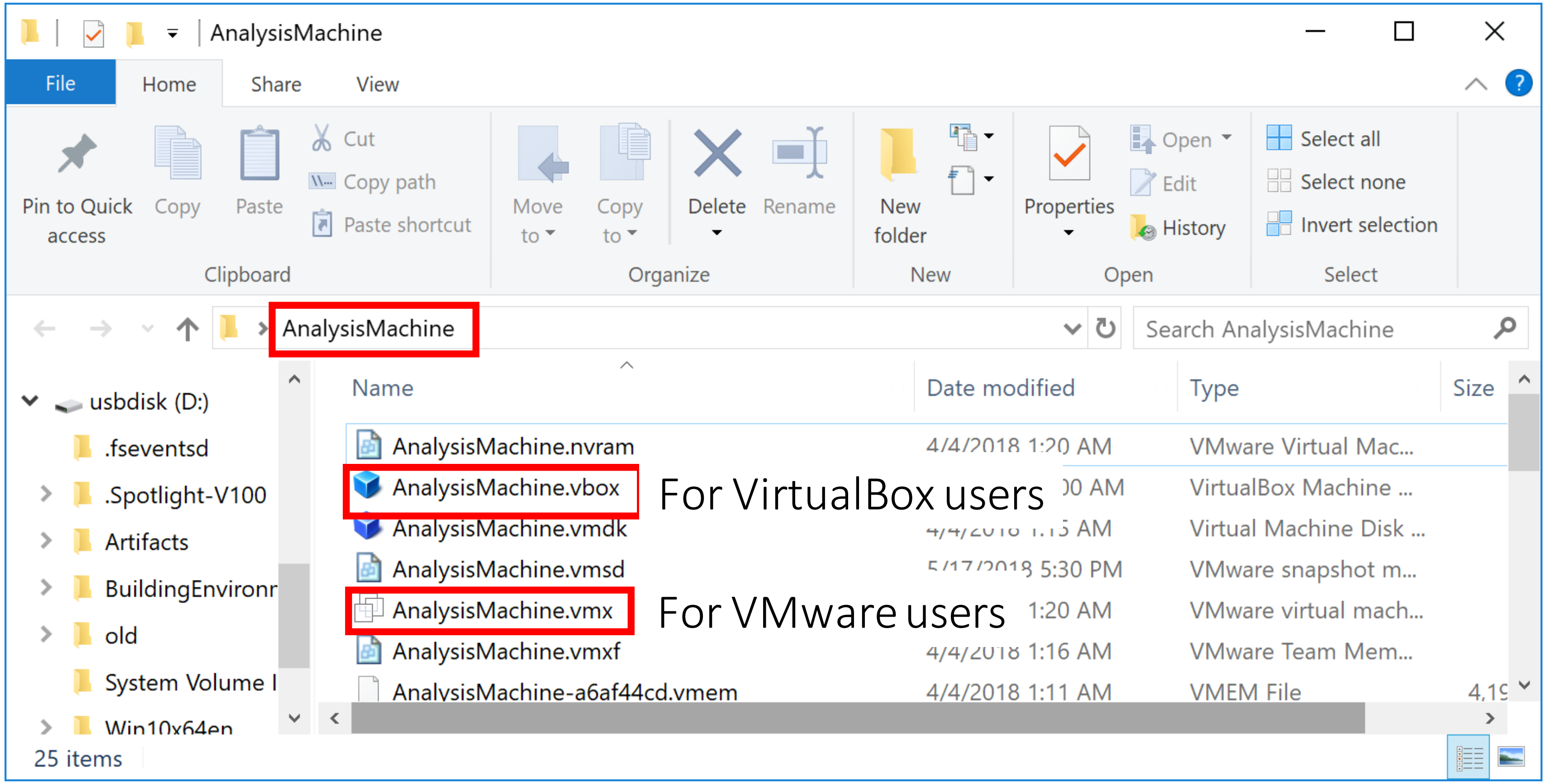
- If you want to enable it again after this training, input the command below with administrator privilege and reboot your machine.

```
bcdedit /set hypervisorlaunchtype auto
```

- You can find these batch files (disable_hyperv.bat, enable_hyperv.bat) on your USB storage that we provided.

# Start “AnalysisMachine”

- Start “AnalysisMachine” by double-clicking “AnalysisMachine.vmx” if you use VMware, or “AnalysisMachine.vbox” if you use VirtualBox.



| Name | Date modified | Type | Size |
|---|---|---|---|
| AnalysisMachine.nvram | 4/4/2018 1:20 AM | VMware Virtual Mac... | |
| AnalysisMachine.vbox | )0 AM | VirtualBox Machine ... | |
| AnalysisMachine.vmdk | 4/4/2018 1:13 AM | Virtual Machine Disk ... | |
| AnalysisMachine.vmsd | 5/17/2018 5:30 PM | VMware snapshot m... | |
| AnalysisMachine.vmx | 1:20 AM | VMware virtual mach... | |
| AnalysisMachine.vmxf | 4/4/2018 1:16 AM | VMware Team Mem... | |
| AnalysisMachine-a6af44cd.vmem | 4/4/2018 1:11 AM | VMEM File | 4,19 |

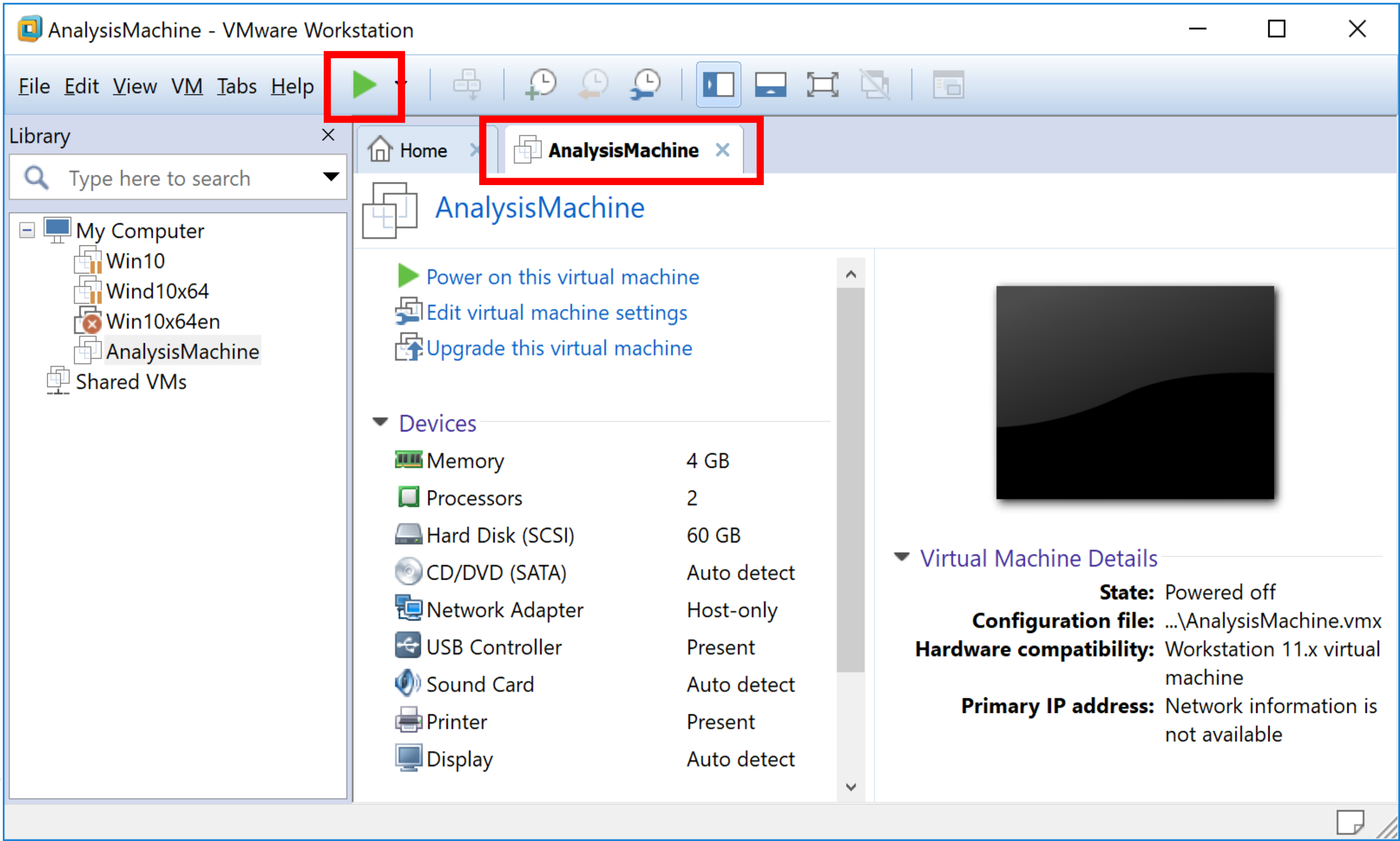
For VirtualBox users

For VMware users

# Start AnalysisMachine - for VMware users (1)

- If you are a VirtualBox user, go to page 24. If you are a VMware fusion user, go to page 21. Please follow the instructions on the slides to prepare your environment.
- For VMware user, you can see “AnalysisMachine” in the Vmware window.
  - You CANNOT use VMware Workstation Player or VMware Player because they cannot make snapshots.
  - Workstation Pro binary is in “VirtualizationSoftware” directory in your USB storage.

Co

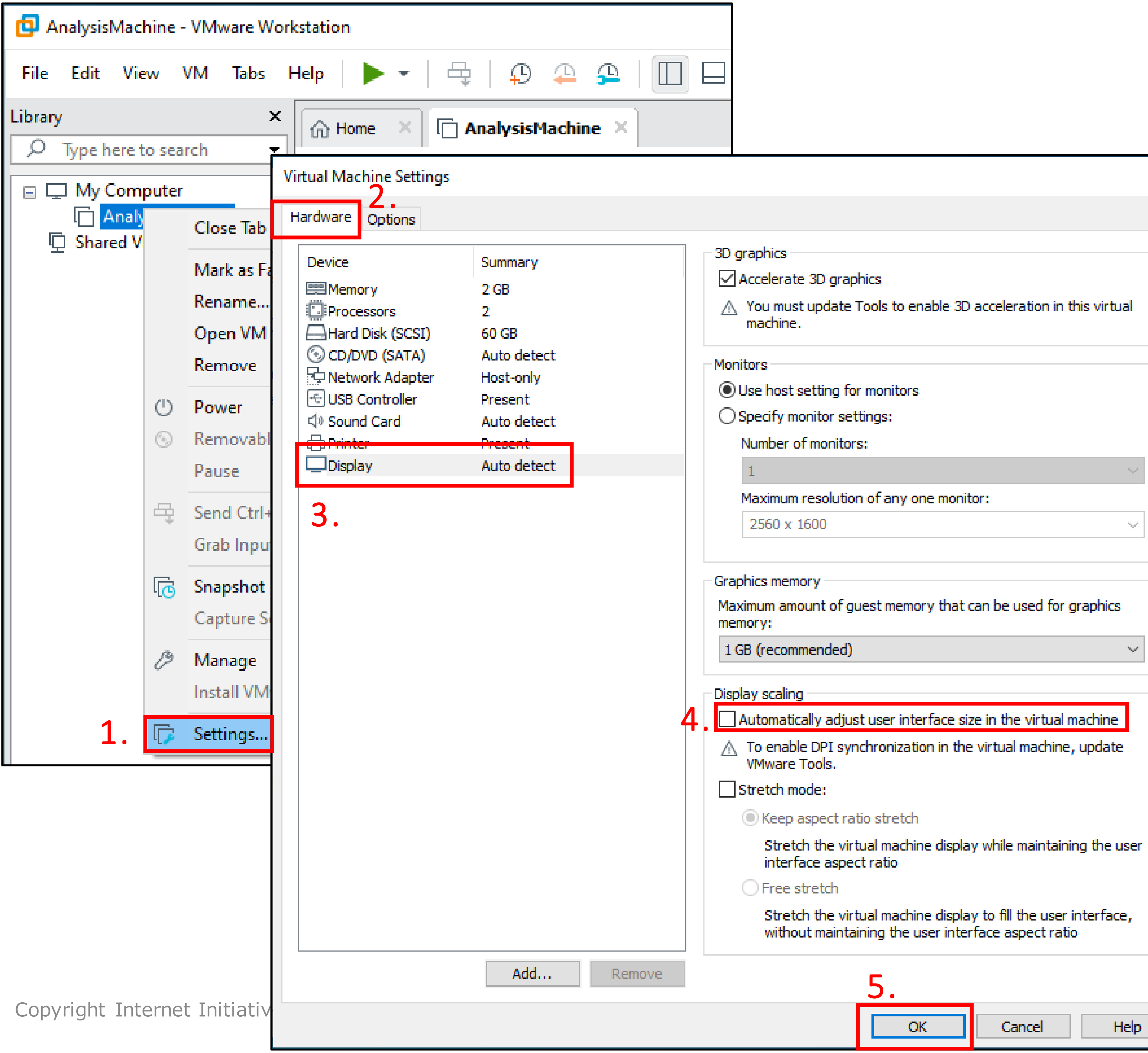


| | |
|---|---|
| Memory | 4 GB |
| Processors | 2 |
| Hard Disk (SCSI) | 60 GB |
| CD/DVD (SATA) | Auto detect |
| Network Adapter | Host-only |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |

**State:** Powered off
**Configuration file:** ...\AnalysisMachine.vmx
**Hardware compatibility:** Workstation 11.x virtual machine
**Primary IP address:** Network information is not available

# Start AnalysisMachine - for VMware users (2)

- If your laptop has high DPI display, you may want to modify the display scaling option of the VM.
- To modify the option, open VM settings.
  - You can access the settings menu by right-clicking the AnalysisMachine.
- Select “Display” from Hardware tab, and **<u>uncheck</u>** “Automatically adjust user interface size in the virtual machine” option in Display scaling option.
  - It is checked by default.



| Device | Summary |
|---|---|
| Memory | 2 GB |
| Processors | 2 |
| Hard Disk (SCSI) | 60 GB |
| CD/DVD (SATA) | Auto detect |
| Network Adapter | Host-only |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |

3D graphics

☑ Accelerate 3D graphics

⚠ You must update Tools to enable 3D acceleration in this virtual machine.

Monitors

● Use host setting for monitors

○ Specify monitor settings:

Number of monitors: 1

Maximum resolution of any one monitor: 2560 x 1600

Graphics memory

Maximum amount of guest memory that can be used for graphics memory: 1 GB (recommended)

Display scaling

□ Automatically adjust user interface size in the virtual machine

⚠ To enable DPI synchronization in the virtual machine, update VMware Tools.

□ Stretch mode:

○ Keep aspect ratio stretch

Stretch the virtual machine display while maintaining the user interface aspect ratio

○ Free stretch

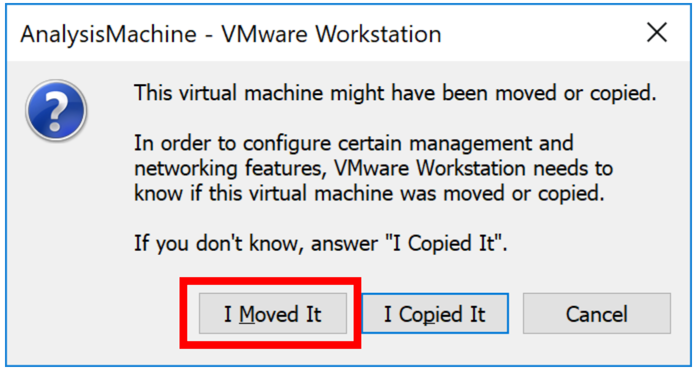
Stretch the virtual machine display to fill the user interface, without maintaining the user interface aspect ratio

# Start AnalysisMachine - for VMware users (3)

- Then click “Power On” button.

- You will see several dialogs.
- Choose “I Moved It”, “No” and “OK” for each dialog.

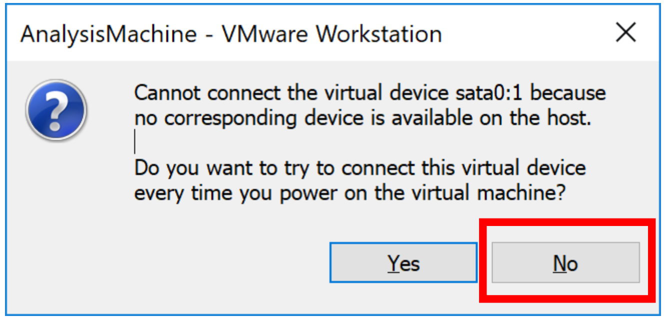
- The logon password of the guest OS is “taro”.


AnalysisMachine - VMware Workstation

This virtual machine might have been moved or copied.

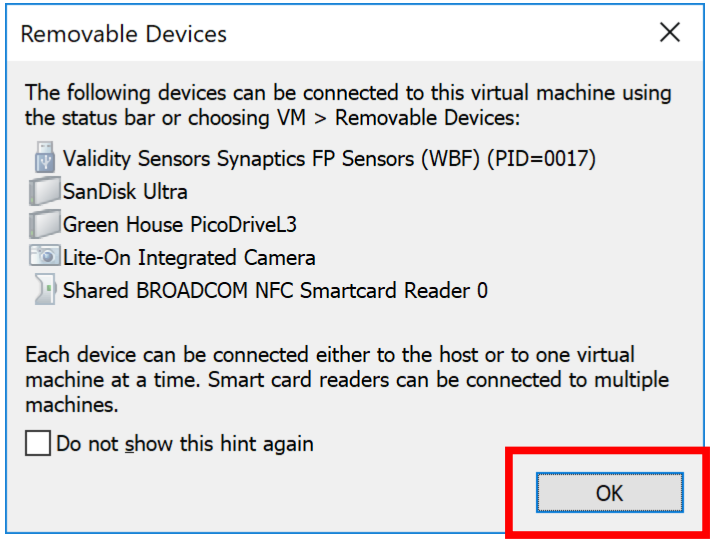
In order to configure certain management and networking features, VMware Workstation needs to know if this virtual machine was moved or copied.

If you don't know, answer "I Copied It".


AnalysisMachine - VMware Workstation

Cannot connect the virtual device sata0:1 because no corresponding device is available on the host.

Do you want to try to connect this virtual device every time you power on the virtual machine?


Removable Devices

The following devices can be connected to this virtual machine using the status bar or choosing VM > Removable Devices:

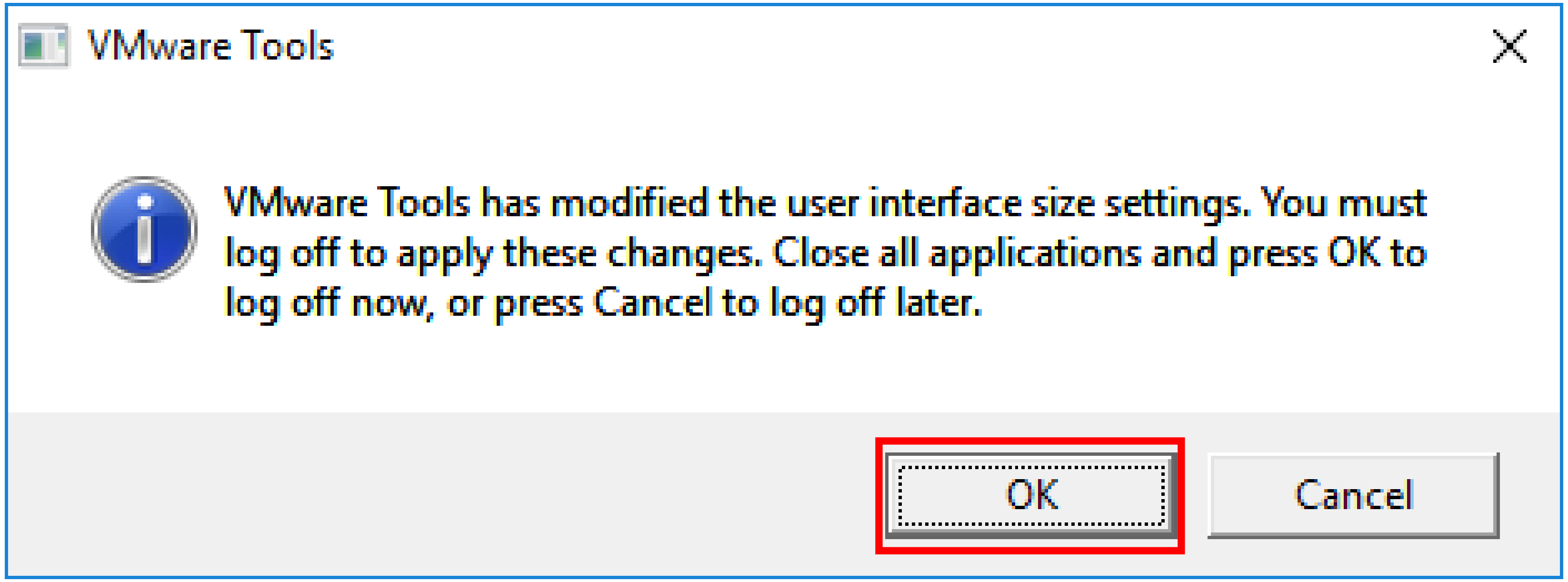
- Validity Sensors Synaptics FP Sensors (WBF) (PID=0017)
- SanDisk Ultra
- Green House PicoDriveL3
- Lite-On Integrated Camera
- Shared BROADCOM NFC Smartcard Reader 0

Each device can be connected either to the host or to one virtual machine at a time. Smart card readers can be connected to multiple machines.

☐ Do not show this hint again

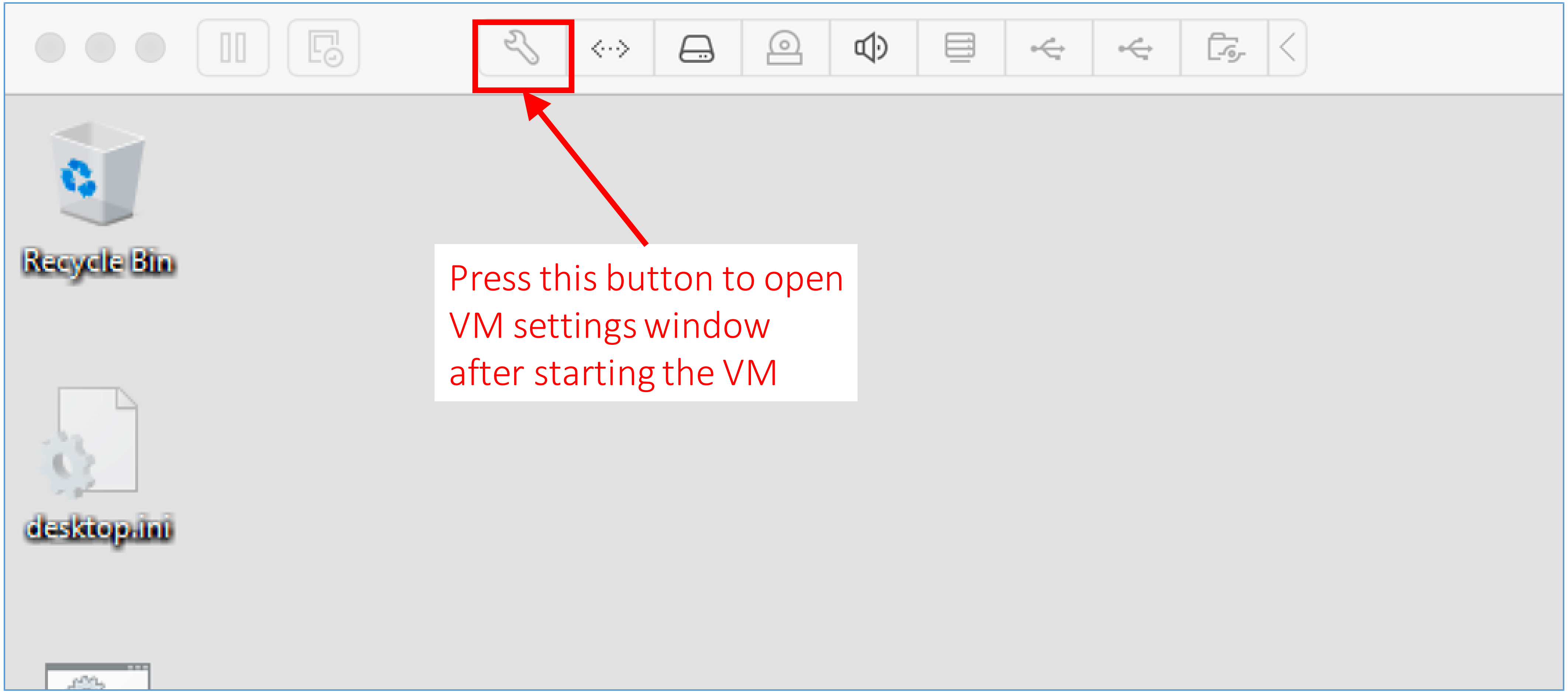
# Start AnalysisMachine - for VMware users (4)

- After the guest OS is booted, if you see the dialog below, press “OK”, and logon to the virtual machine again.



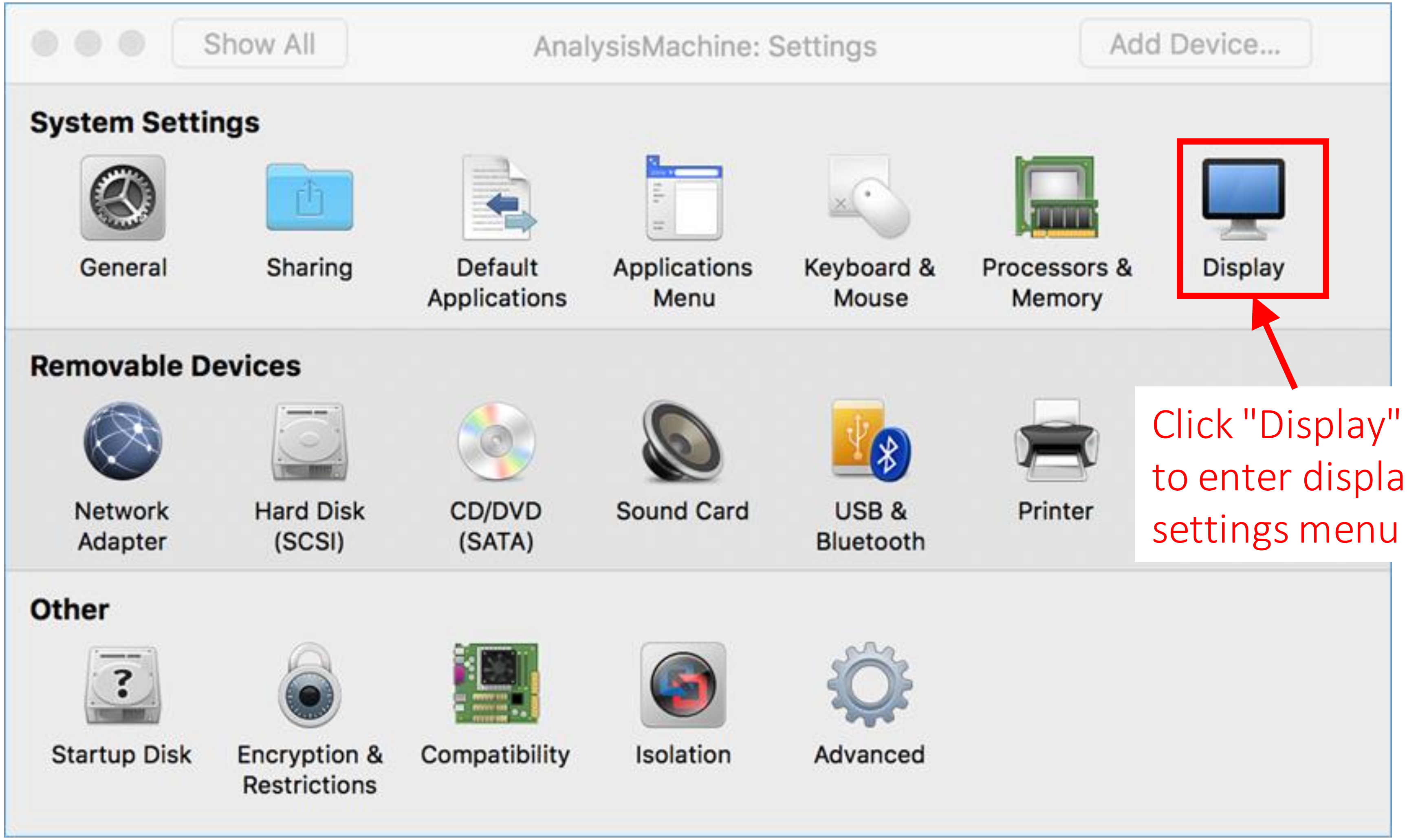
VMware Tools has modified the user interface size settings. You must log off to apply these changes. Close all applications and press OK to log off now, or press Cancel to log off later.

# Disable high resolution mode on VMware Fusion (1)



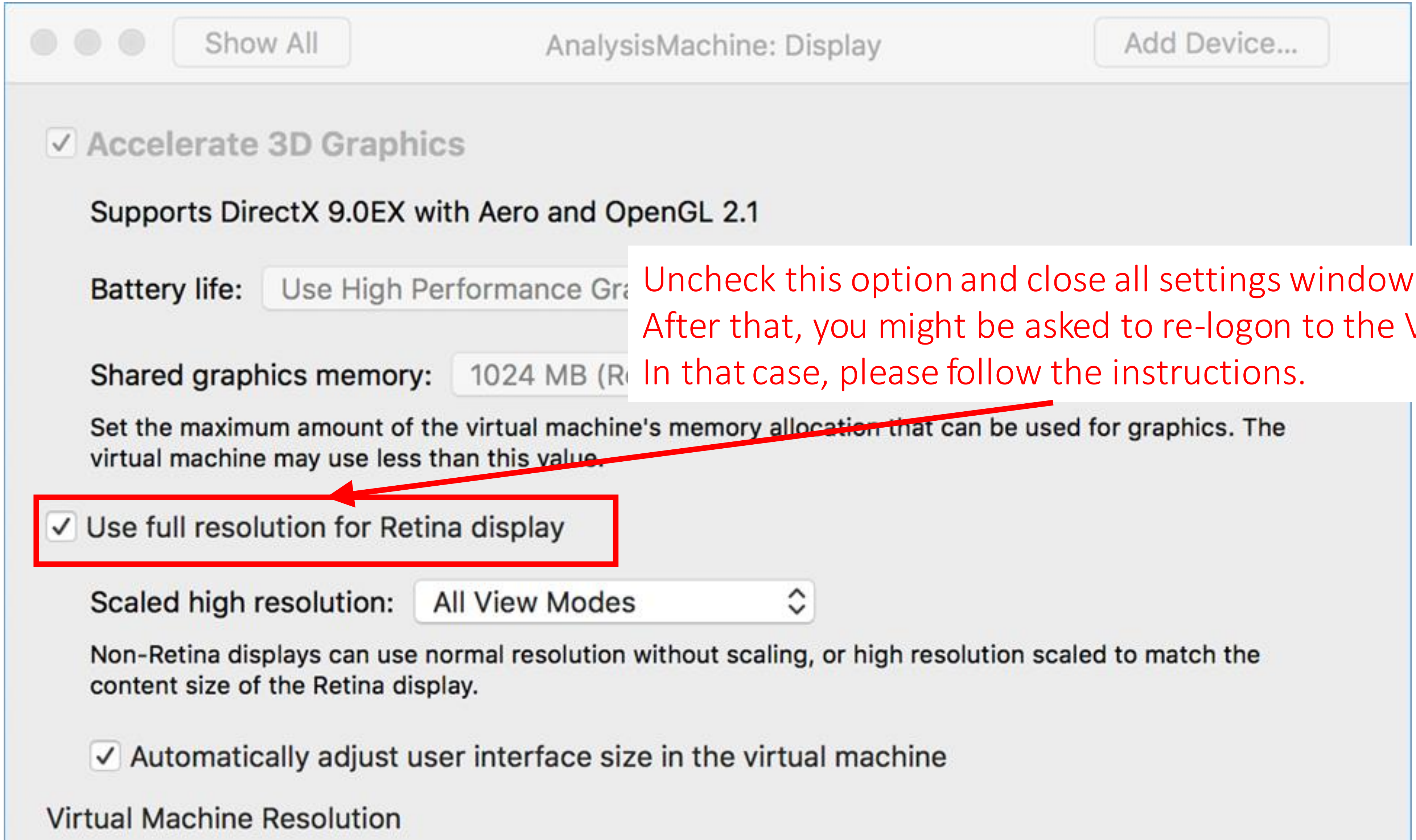
Press this button to open VM settings window after starting the VM

# Disable high resolution mode on VMware Fusion (2)



Click "Display" to enter display settings menu

# Disable high resolution mode on VMware Fusion (3)



☑ Accelerate 3D Graphics

Supports DirectX 9.0EX with Aero and OpenGL 2.1

Battery life: Use High Performance Gra

Shared graphics memory: 1024 MB (R

Set the maximum amount of the virtual machine's memory allocation that can be used for graphics. The virtual machine may use less than this value.

☑ Use full resolution for Retina display

Scaled high resolution: All View Modes

Non-Retina displays can use normal resolution without scaling, or high resolution scaled to match the content size of the Retina display.

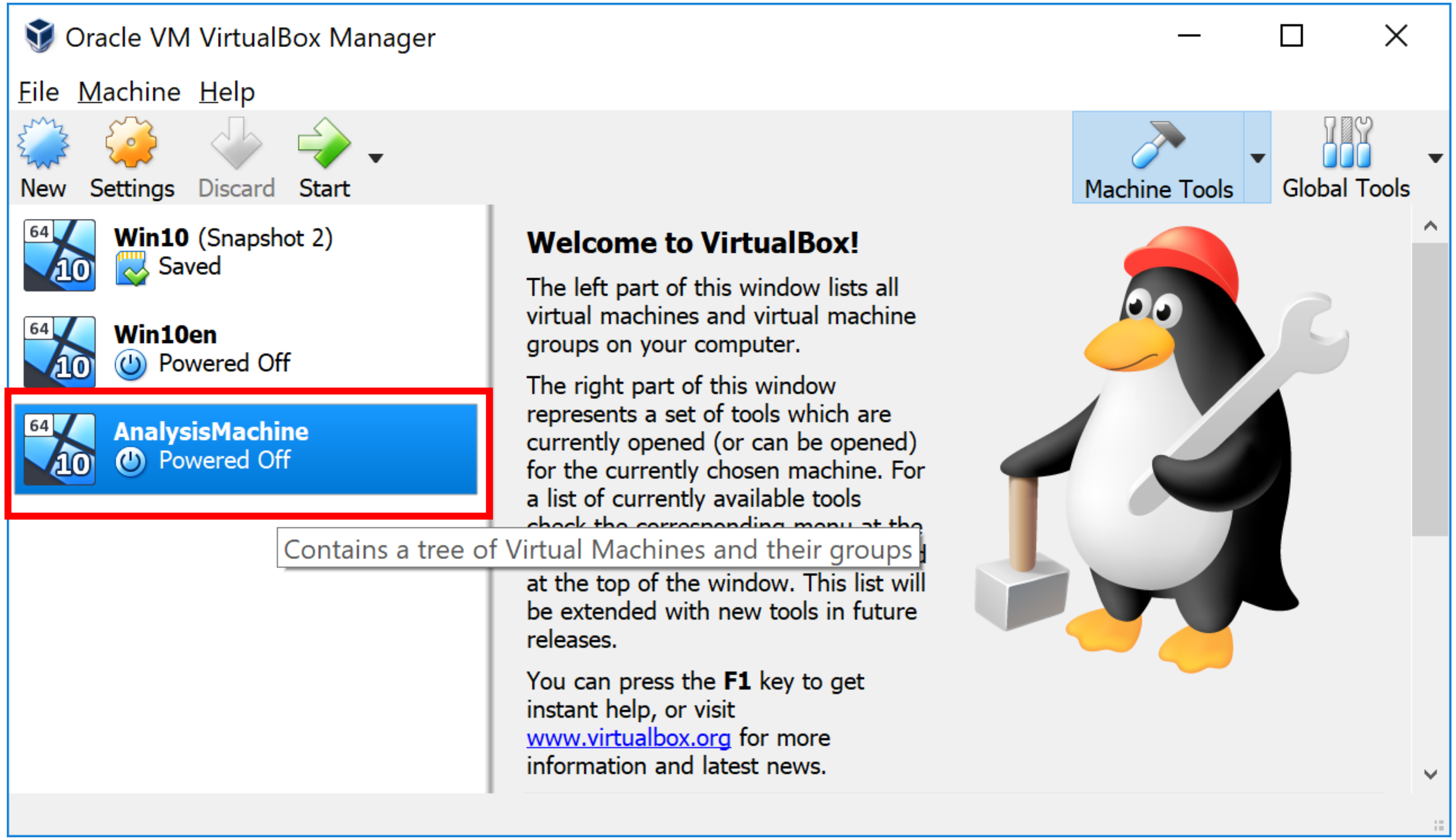
☑ Automatically adjust user interface size in the virtual machine

Virtual Machine Resolution

Uncheck this option and close all settings windows.
After that, you might be asked to re-logon to the VM.
In that case, please follow the instructions.

# Start AnalysisMachine - for VirtualBox users (1)

- Double-click “AnalysisMachine”. to start the VM.
- Password of the guest OS is “taro”.



**Welcome to VirtualBox!**

The left part of this window lists all virtual machines and virtual machine groups on your computer.

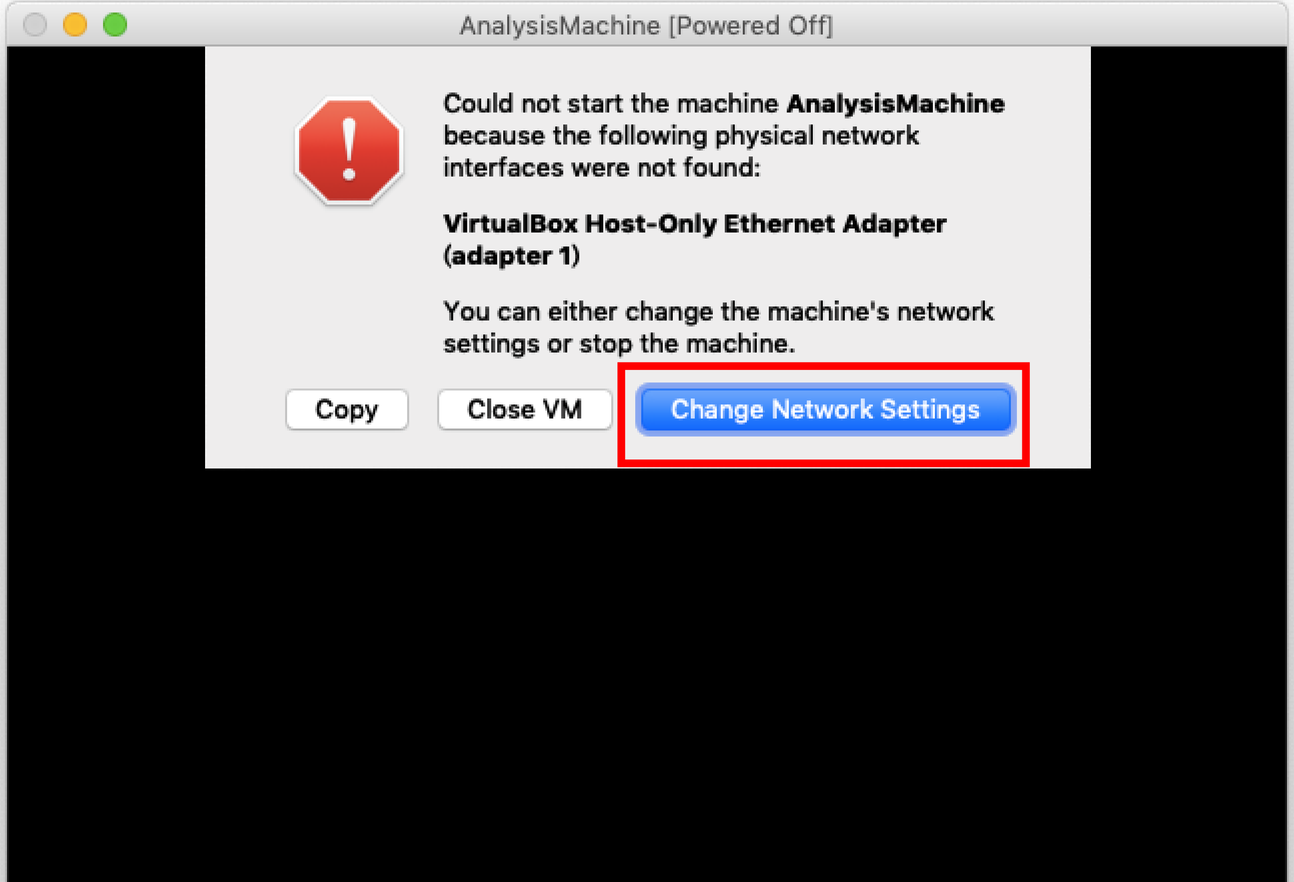
The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. For a list of currently available tools check the corresponding menu at the

at the top of the window. This list will be extended with new tools in future releases.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

# Start AnalysisMachine - for VirtualBox users (2)

- If you are a Mac user and the following dialog is displayed, press “Change Network Settings”.



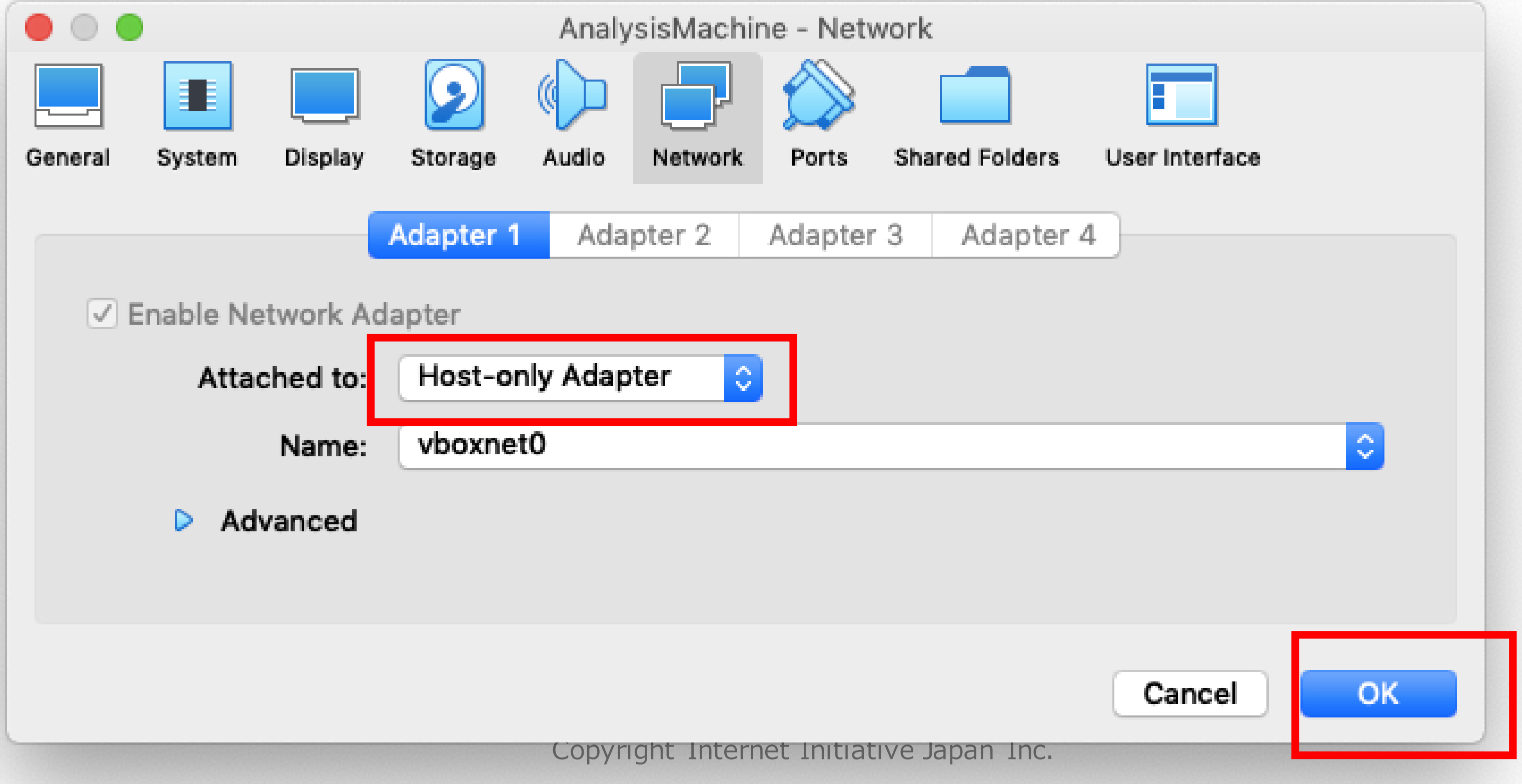
Could not start the machine **AnalysisMachine** because the following physical network interfaces were not found:

**VirtualBox Host-Only Ethernet Adapter (adapter 1)**

You can either change the machine's network settings or stop the machine.

# Start AnalysisMachine - for VirtualBox users (3)

- (Cont.) Select “Host-only Adapter” and press OK.



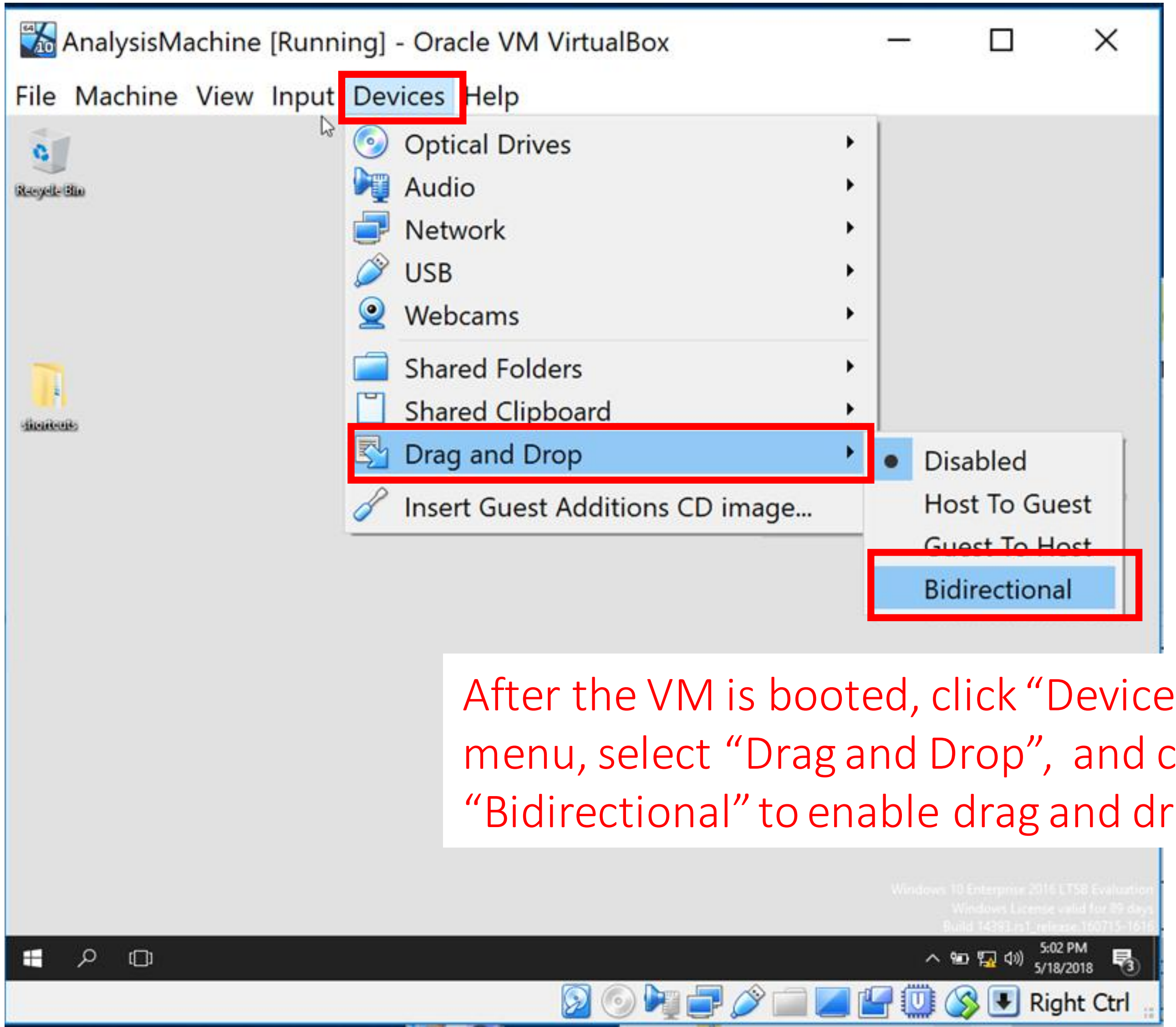
AnalysisMachine - Network

☑ Enable Network Adapter

Attached to: Host-only Adapter

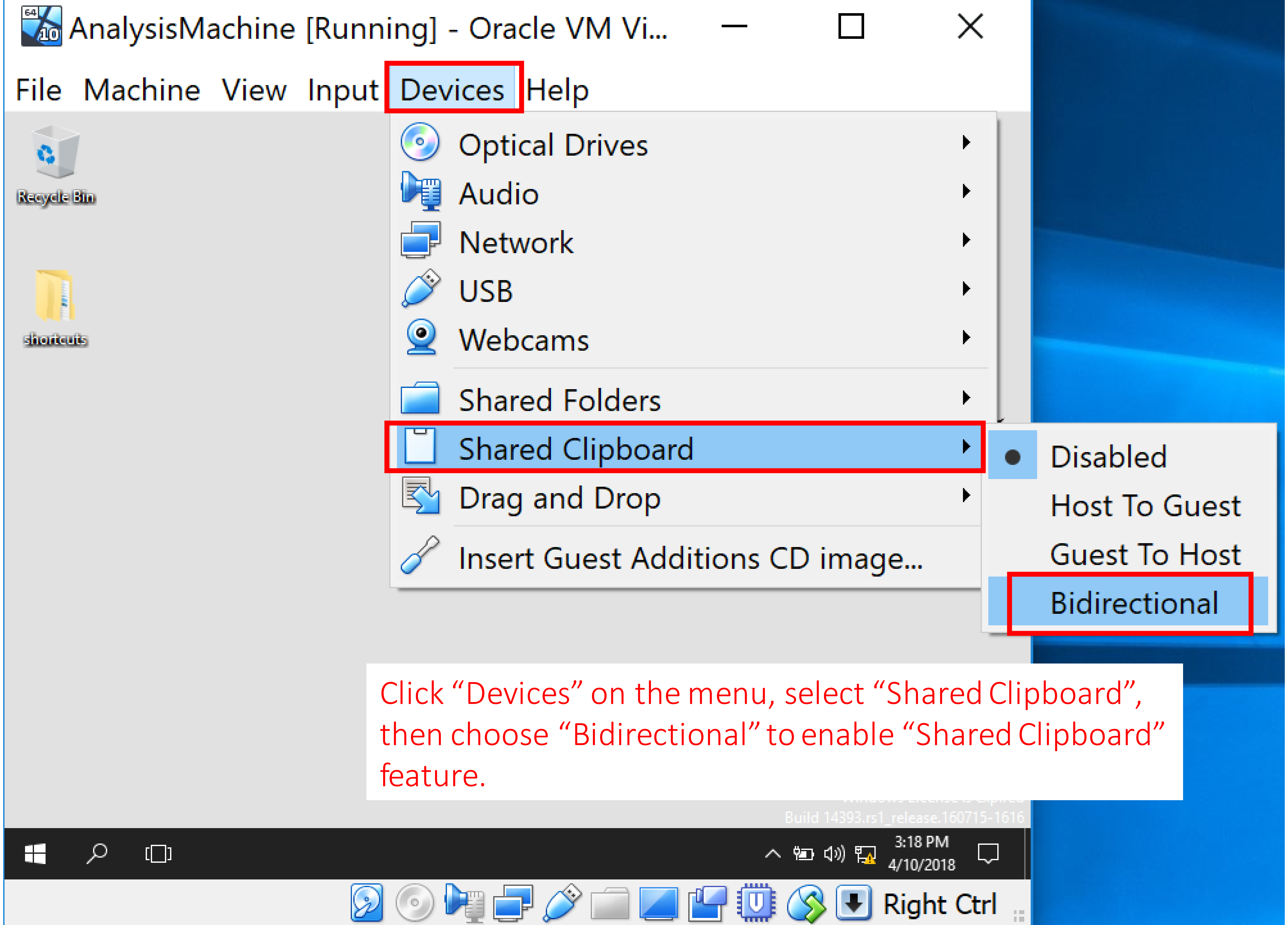
Name: vboxnet0

# Start AnalysisMachine - for VirtualBox users (4)



After the VM is booted, click “Devices” on the menu, select “Drag and Drop”, and choose “Bidirectional” to enable drag and drop feature.

St



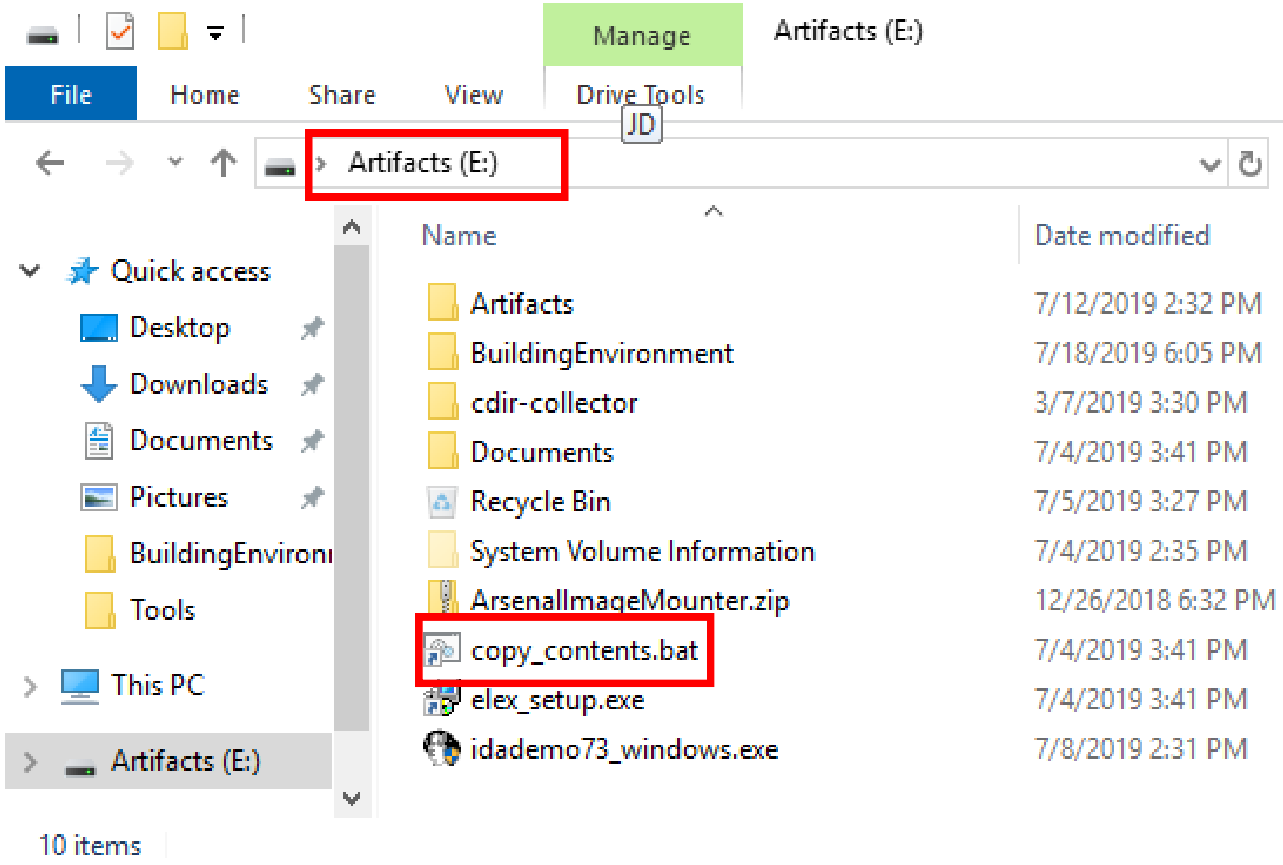
Click “Devices” on the menu, select “Shared Clipboard”, then choose “Bidirectional” to enable “Shared Clipboard” feature.

# Install Software

- For all users, if you were able to start your VM, install the software below manually on your AnalysisMachine.
  - Event Log Explorer
    - The shortcut of the binary is “elex_setup.exe” in the drive “E:”.

# Update Our Contents

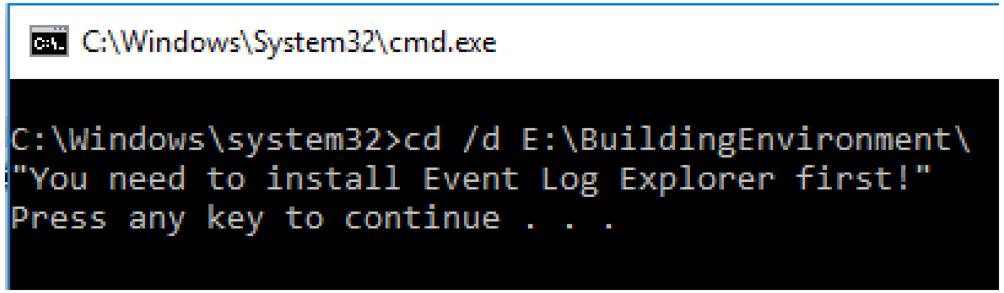
- In order to update several contents we provided, execute the shortcut of a batch file “E:\copy_contents.bat” by double-clicking it.
  - Once the script finishes, press Enter key on the window. The VM will reboot when you press the Enter key.



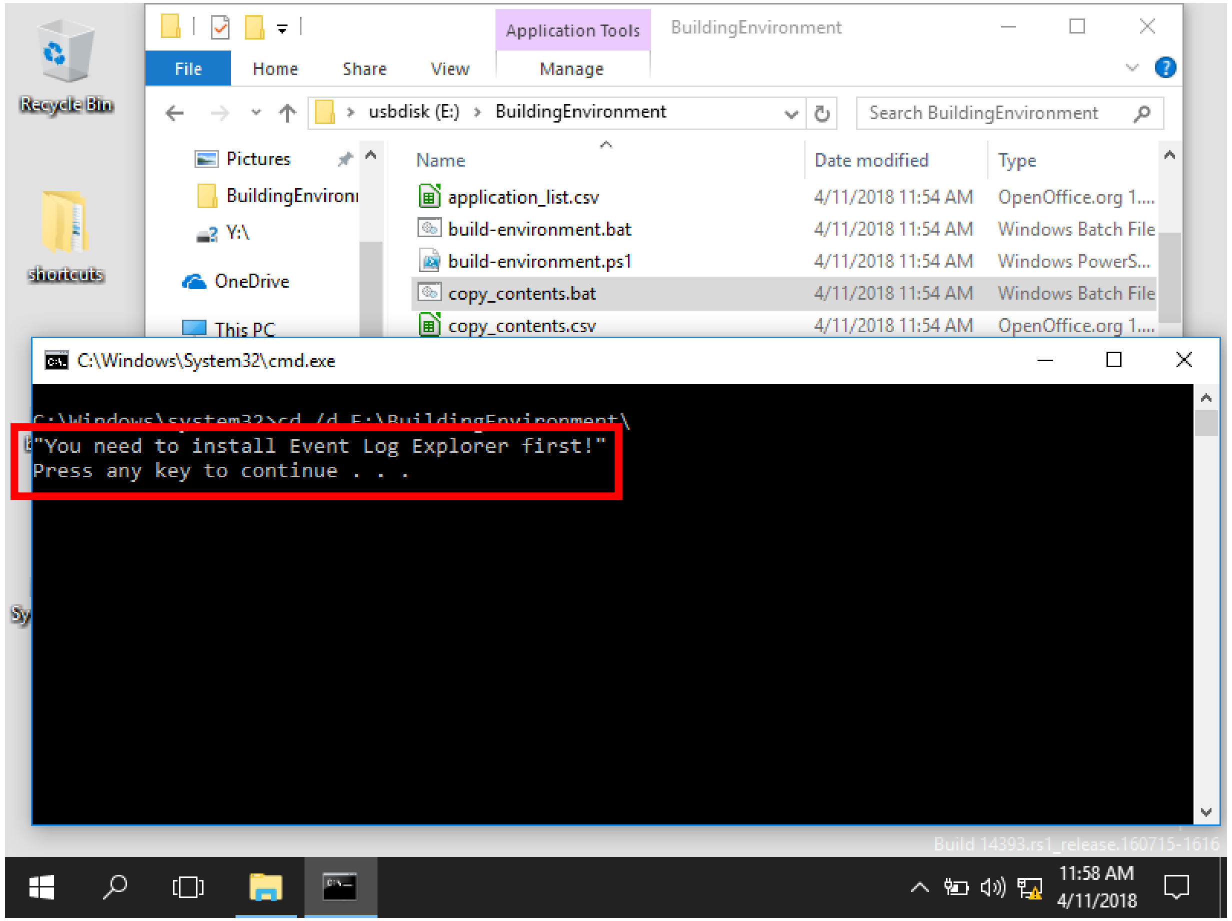
| Name | Date modified |
|---|---|
| Artifacts | 7/12/2019 2:32 PM |
| BuildingEnvironment | 7/18/2019 6:05 PM |
| cdir-collector | 3/7/2019 3:30 PM |
| Documents | 7/4/2019 3:41 PM |
| Recycle Bin | 7/5/2019 3:27 PM |
| System Volume Information | 7/4/2019 2:35 PM |
| ArsenalImageMounter.zip | 12/26/2018 6:32 PM |
| copy_contents.bat | 7/4/2019 3:41 PM |
| elex_setup.exe | 7/4/2019 3:41 PM |
| idademo73_windows.exe | 7/8/2019 2:31 PM |

# Update Our Contents

- If you got one of the messages below, you might have missed some steps. Please go back to page 29.



```
C:\Windows\system32>cd /d E:\BuildingEnvironment\
"You need to install Event Log Explorer first!"
Press any key to continue . . .
```

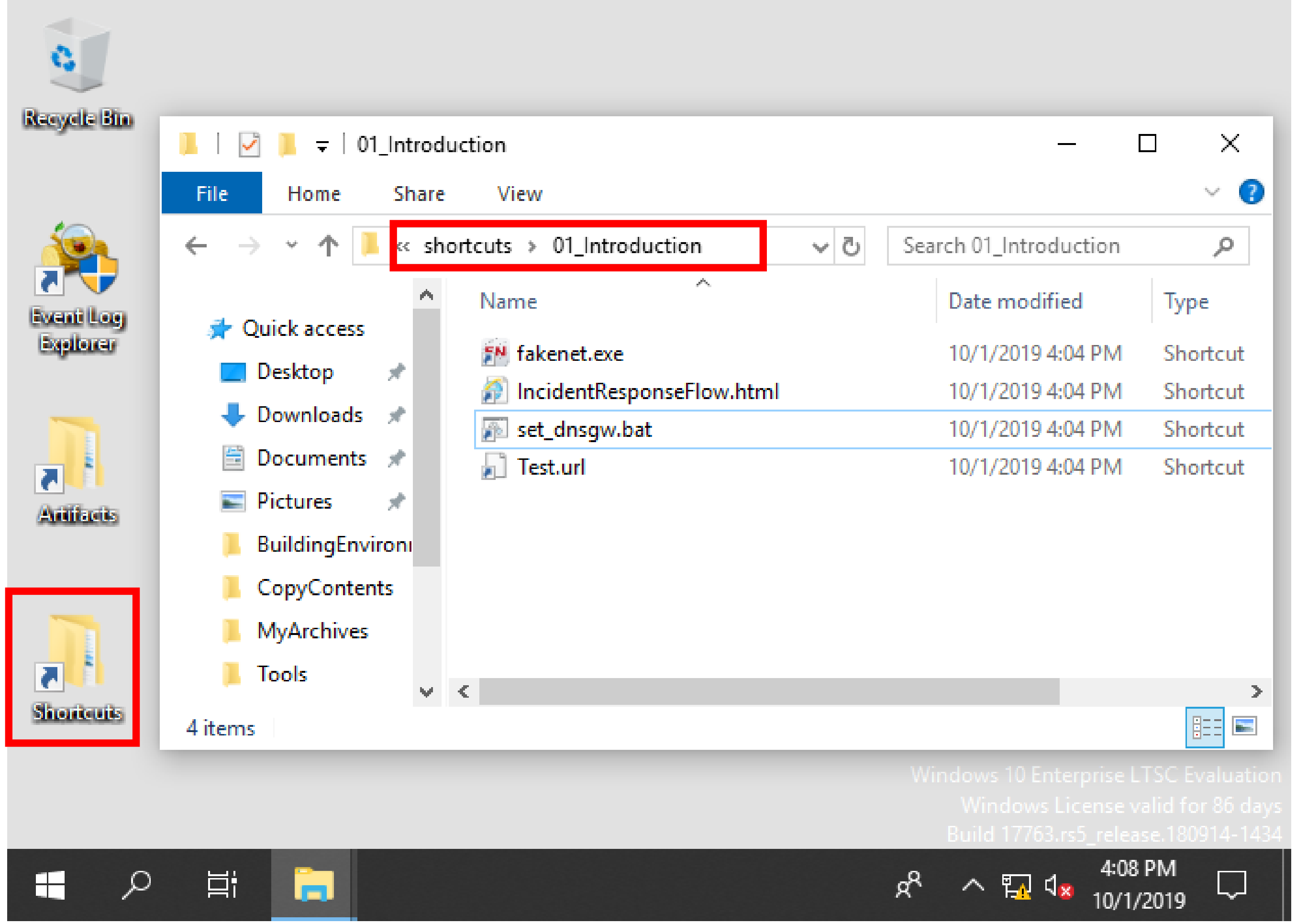


| Name | Date modified | Type |
|---|---|---|
| application_list.csv | 4/11/2018 11:54 AM | OpenOffice.org 1.... |
| build-environment.bat | 4/11/2018 11:54 AM | Windows Batch File |
| build-environment.ps1 | 4/11/2018 11:54 AM | Windows PowerS... |
| copy_contents.bat | 4/11/2018 11:54 AM | Windows Batch File |
| copy_contents.csv | 4/11/2018 11:54 AM | OpenOffice.org 1.... |

```
C:\Windows\system32>cd /d E:\BuildingEnvironment\
"You need to install Event Log Explorer first!"
Press any key to continue . . .
```

# The “Shortcuts” Folder

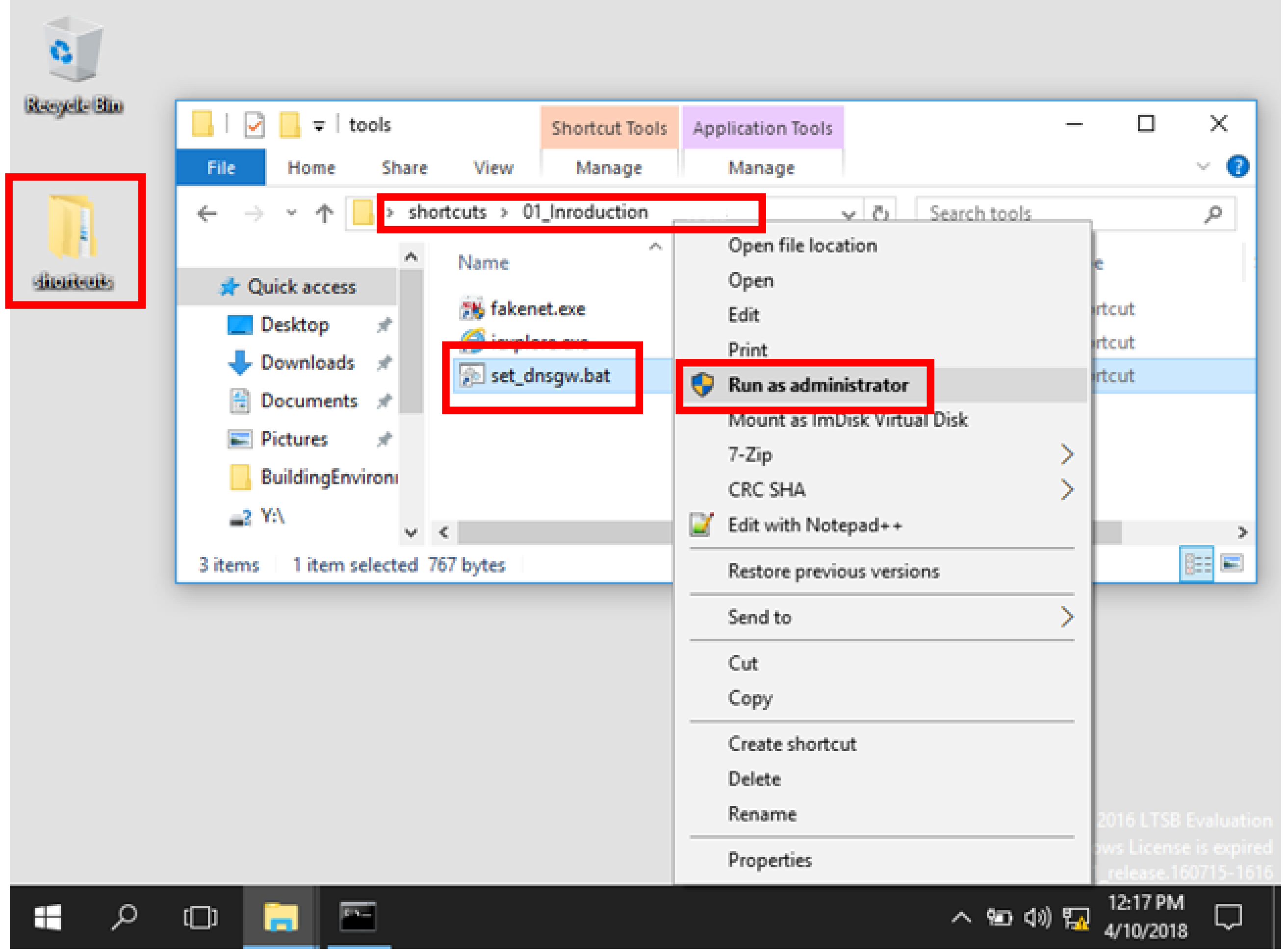
- You will find “Shortcuts” folder on the desktop of your VM.
  - This folder is important for upcoming exercises as it contains all materials as shortcuts, for example:
    - Artifacts
      - Disk/Memory images
      - Intermediate analysis results
      - Tool outputs
    - Tools
  - Please get used to it.



| Name | Date modified | Type |
|---|---|---|
| fakenet.exe | 10/1/2019 4:04 PM | Shortcut |
| IncidentResponseFlow.html | 10/1/2019 4:04 PM | Shortcut |
| set_dnsgw.bat | 10/1/2019 4:04 PM | Shortcut |
| Test.url | 10/1/2019 4:04 PM | Shortcut |

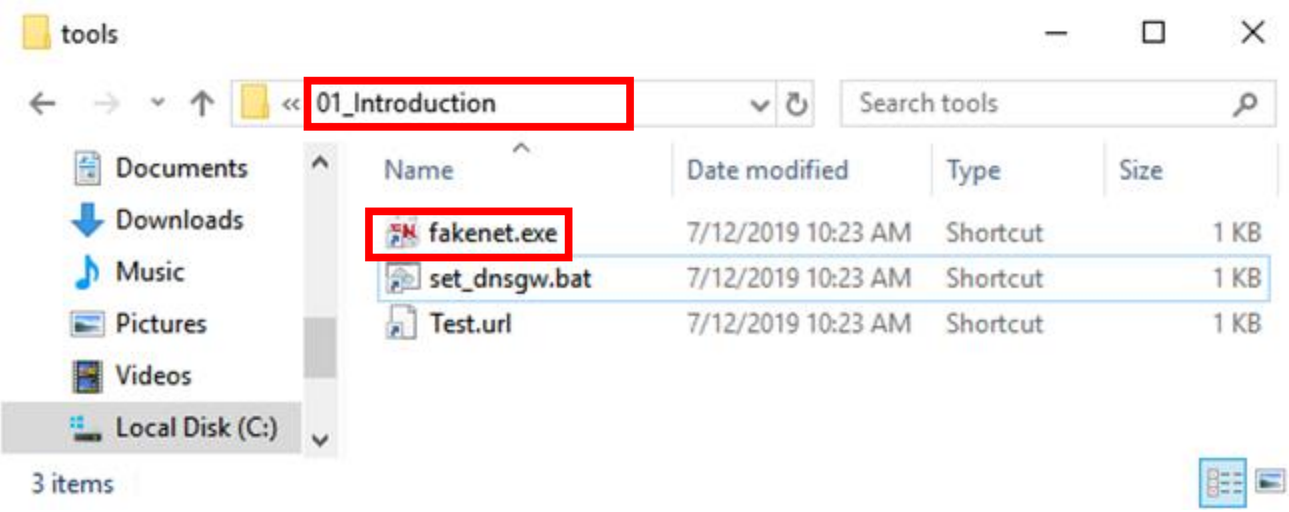
# Change Interface Settings

- Execute “set_dnsgw.bat” in “Shortcuts\01_Introduction” folder to change the network interface settings of the VM.
  - It is because the DHCP Server of VirtualBox doesn’t distribute default gateway and DNS servers settings on “Host-Only” networks.
- This is needed for executing “Fakenet-NG”, an internet simulator provided by Mandiant.



# Check Fakenet

- Double-click fakenet.exe in “Shortcuts\01_Introdcution” folder. You will see the Windows Firewall dialog when executing it. Please press “Allow Access” button.

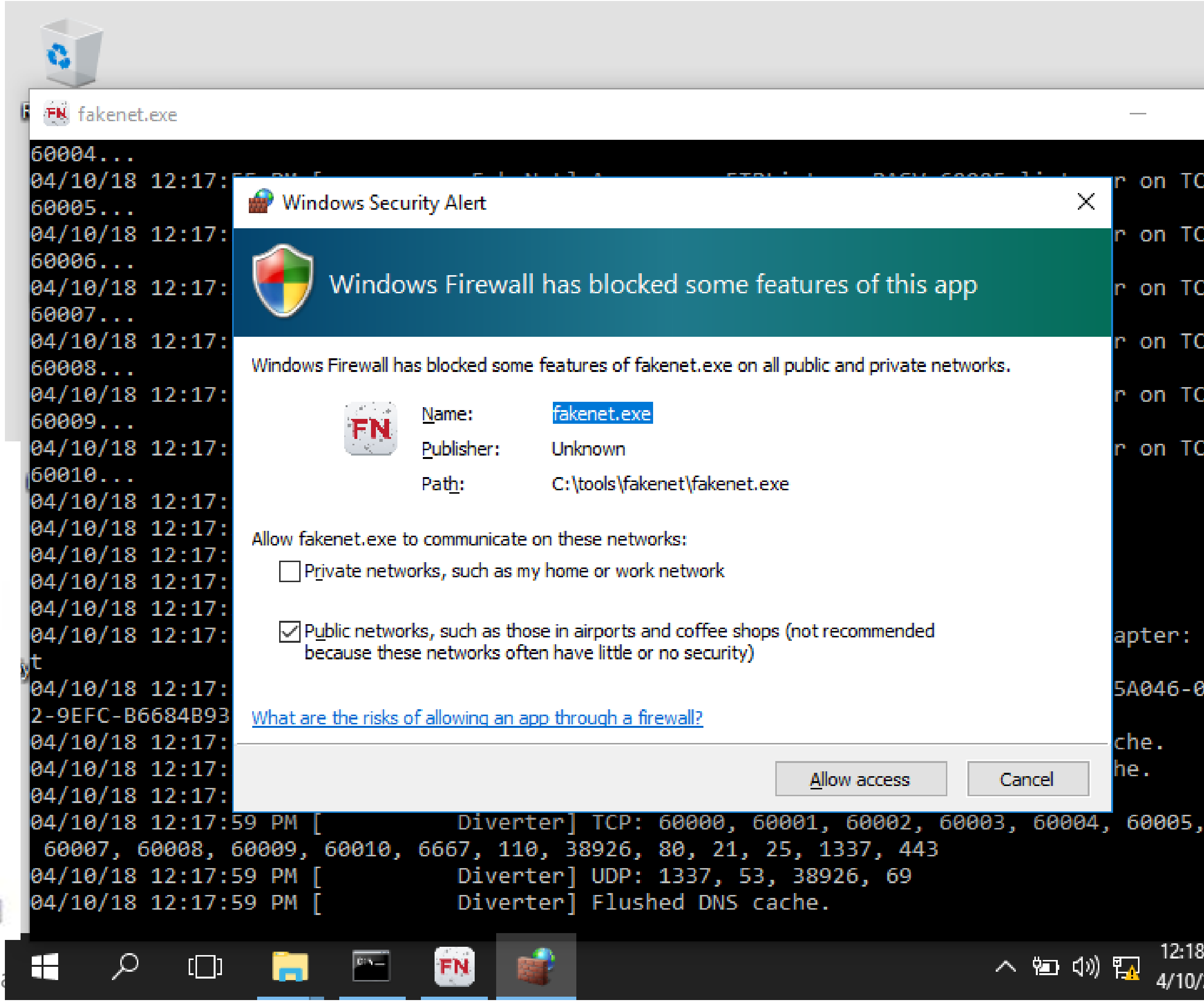


tools

01_Introduction

| Name | Date modified | Type | Size |
|---|---|---|---|
| fakenet.exe | 7/12/2019 10:23 AM | Shortcut | 1 KB |
| set_dnsgw.bat | 7/12/2019 10:23 AM | Shortcut | 1 KB |
| Test.url | 7/12/2019 10:23 AM | Shortcut | 1 KB |

3 items



fakenet.exe

```
60004...
04/10/18 12:17:                                                    r on TC
60005...
04/10/18 12:17:                                                    r on TC
60006...
04/10/18 12:17:                                                    r on TC
60007...
04/10/18 12:17:                                                    r on TC
60008...
04/10/18 12:17:                                                    r on TC
60009...
04/10/18 12:17:                                                    r on TC
60010...
04/10/18 12:17:
04/10/18 12:17:
04/10/18 12:17:
04/10/18 12:17:
04/10/18 12:17:
04/10/18 12:17:                                                    apter:
t
04/10/18 12:17:                                                    5A046-0
2-9EFC-B6684B93
04/10/18 12:17:                                                    che.
04/10/18 12:17:                                                    he.
04/10/18 12:17:
04/10/18 12:17:59 PM [         Diverter] TCP: 60000, 60001, 60002, 60003, 60004, 60005,
 60007, 60008, 60009, 60010, 6667, 110, 38926, 80, 21, 25, 1337, 443
04/10/18 12:17:59 PM [         Diverter] UDP: 1337, 53, 38926, 69
04/10/18 12:17:59 PM [         Diverter] Flushed DNS cache.
```

Windows Security Alert

Windows Firewall has blocked some features of this app

Windows Firewall has blocked some features of fakenet.exe on all public and private networks.

Name: fakenet.exe
Publisher: Unknown
Path: C:\tools\fakenet\fakenet.exe

Allow fakenet.exe to communicate on these networks:

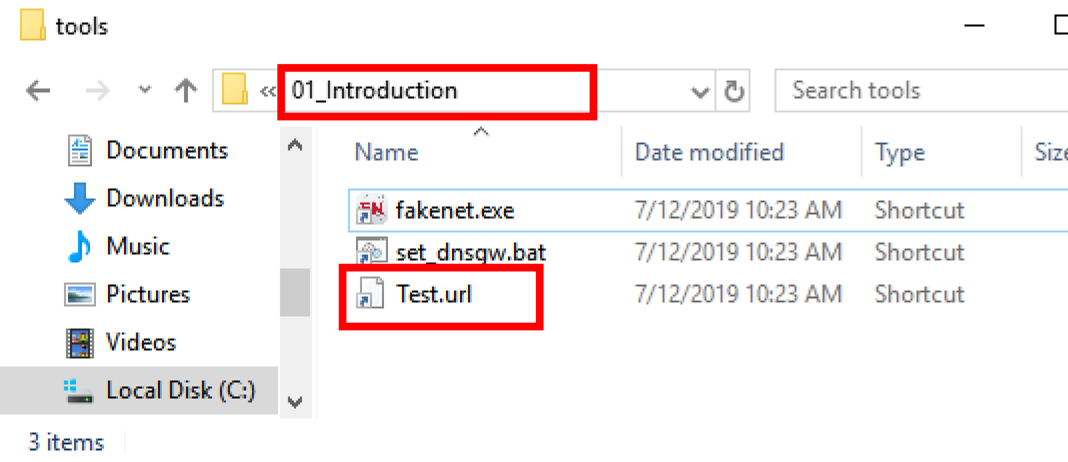
☐ Private networks, such as my home or work network

☑ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

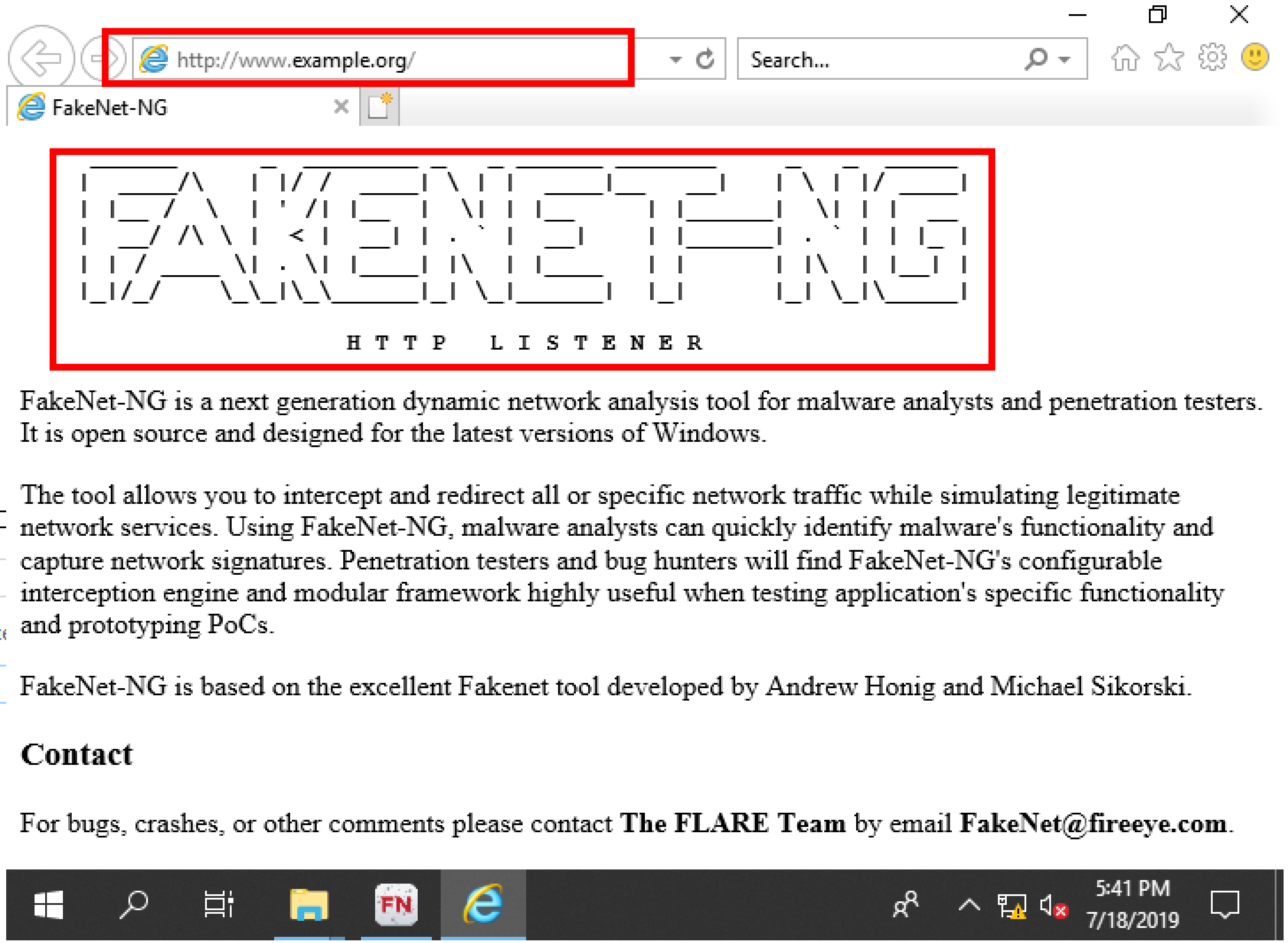
What are the risks of allowing an app through a firewall?

# Check Fakenet (Cont.)

- Then double-click “Test.url” and check if you can see the message from Fakenet like the right figure.



| Name | Date modified | Type | Size |
|---|---|---|---|
| fakenet.exe | 7/12/2019 10:23 AM | Shortcut | |
| set_dnsqw.bat | 7/12/2019 10:23 AM | Shortcut | |
| Test.url | 7/12/2019 10:23 AM | Shortcut | |



FakeNet-NG is a next generation dynamic network analysis tool for malware analysts and penetration testers. It is open source and designed for the latest versions of Windows.

The tool allows you to intercept and redirect all or specific network traffic while simulating legitimate network services. Using FakeNet-NG, malware analysts can quickly identify malware's functionality and capture network signatures. Penetration testers and bug hunters will find FakeNet-NG's configurable interception engine and modular framework highly useful when testing application's specific functionality and prototyping PoCs.

FakeNet-NG is based on the excellent Fakenet tool developed by Andrew Honig and Michael Sikorski.

## Contact

For bugs, crashes, or other comments please contact **The FLARE Team** by email **FakeNet@fireeye.com**.

# Time Zone

- Time zone of your Analysis Machine is set to JST.
    - Keep the time zone of your Analysis Machine because some tools use local time zone and they change timestamps automatically.

# Take a Snapshot for your VM

- Close Fakenet and IE windows if you saw the message from Fakenet.

- Then take a snapshot of your VM!
  - Name: “Initial state”

- Now, you are ready to perform exercises.

# Who Are We?

# Who Are We

- Hiroshi Suzuki, Hisao Nashiwa from “Internet Initiative Japan Inc.” (IIJ).
  - IIJ is a Japanese ISP (We are the first commercial ISP in Japan).
  - We belong to the CSIRT team (IIJ-SECT) of our company.
  - We are malware analysts, forensic investigators.
- We have been Briefing speakers/coauthors (USA, Europe and Asia) and Trainers (USA) in the past Black Hat events.

# Agenda

# Agenda

- Day 1
  1. Introduction
  2. Initial Response
     1. Evidence Preservation
     2. Image Mounting and Parsing
  3. Persistence Analysis
  4. Malware Analysis (Surface & Dynamic Analysis)
  5. Root Cause Analysis
     1. Malware Hunting
     2. File/Folder Open/Save Analysis

5. Root Cause Analysis (Cont.)
   3. E-mail Forensics
   4. Web Browser Forensics
   5. Exploit Analysis
6. Lateral Movements Investigation
   1. Program Execution Artifacts Analysis

# Agenda

- Day 2
  6. Lateral Movements Investigation (Cont.)
     1. Program Execution Artifacts Analysis (Cont.)
     2. Attack Tool Analysis
     3. Event Log Analysis
  7. Timeline Analysis
  8. Finding Leaked Information
  9. Recovering Data & Keyword Search
  10. Memory Forensics
  11. Wrap Up

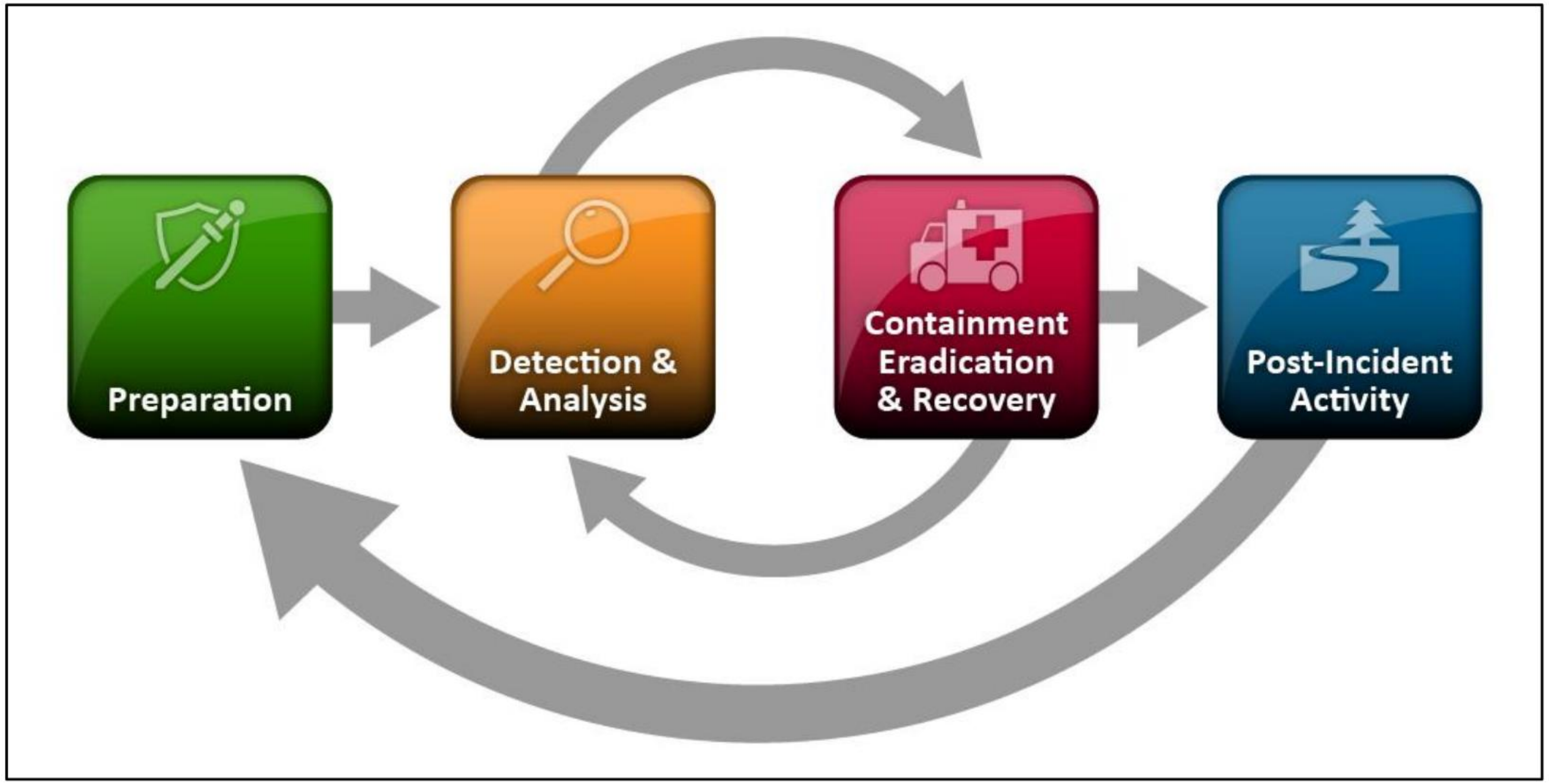
# Incident Response Basics

# What is Incident Response? (1)

- Incident response in the IT industry is a strategic approach for dealing with incidents such as data breaches or malware infections.
  - It is performed to solve incidents when they occur.
  - We also need to develop strategies that prevent incidents from recurring and enhance network protection, and then implement those strategies.
- What is incident response for targeted attacks?
  - Root cause investigation
  - Containment, eradication and prevention of damage
  - Confirmation of damage
    - Investigating data exfiltration
    - Confirming business impacts (mainly services and systems)
    - Determining its scope and scale
  - Examination of restoration methods
  - Consideration of measures to prevent recurrences
    - Review of detection methods
    - Consideration of defensive measures

# What is Incident Response? (2)

- Incident Response Steps



https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

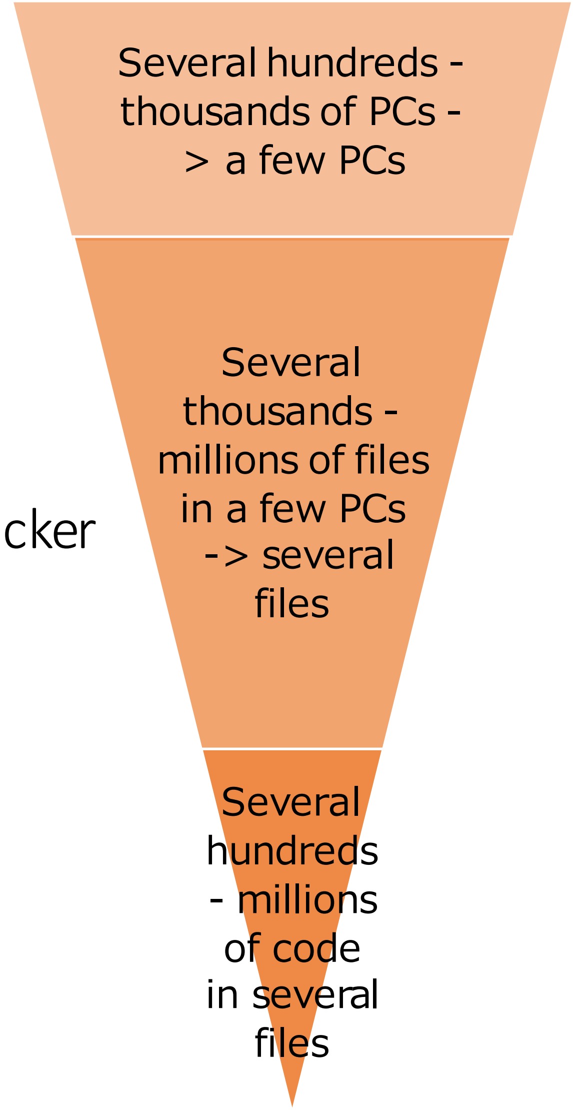
# What is Incident Response? (3)

- Other Useful IR Steps References
    - https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
    - https://www.sans.org/media/score/checklists/APT-IncidentHandling-Checklist.pdf
    - https://www.alienvault.com/blogs/security-essentials/incident-response-steps-comparison-guide
    - https://www.alienvault.com/resource-center/ebook/insider-guide-to-incident-response

# What is Incident Response? (4)

These techniques are used to perform incident responses.

- Network Forensics (from a few minutes to several hours)
  - To specify suspicious hosts by analyzing logs and packets
    - SIEM, IDPS, network devices (Firewall, Proxy, router)
- Computer Forensics (from several hours to several weeks)
  - To identify malware and files related to attacks, and to estimate attacker activities and their impacts, in suspected hosts and networks, by performing these tasks below.
    - Evidence acquisition (HDD, Memory)
    - Collecting artifacts and investigation
- Malware Analysis (from a few minutes to several months)
  - To find out other infected machines, to consider methods for preventing expansion of damage and converge the situation, by investigating malware C2 servers and its features.
    - Surface analysis, dynamic analysis and static analysis



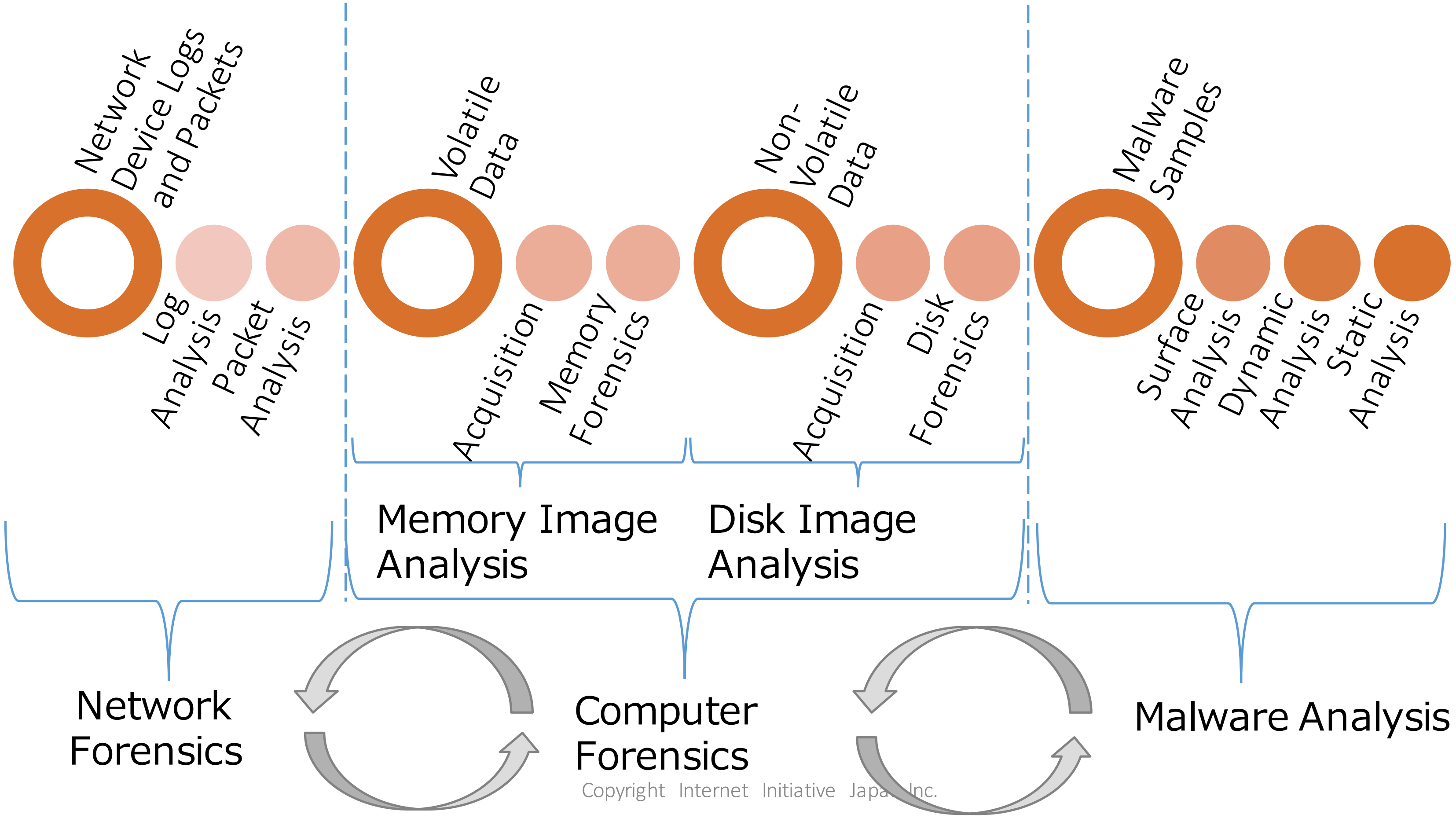
Several hundreds - thousands of PCs -> a few PCs

Several thousands - millions of files in a few PCs -> several files

Several hundreds - millions of code in several files

# What is Incident Response? (5)

- We feed back the results of analysis to each other and clarify the whole picture of the incidents.



# Network Forensics

# Network Forensics Basics

- It is a method to investigate logs of network devices and packet capture data.
    - It is necessary to prepare logs for incident response (you can’t do anything if logs are not prepared).

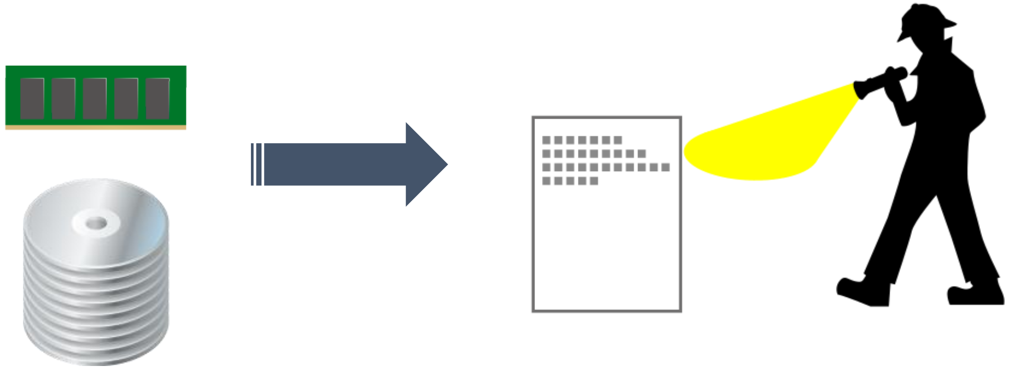
- This task will be a challenge if you don't have any suspicious IoCs (Indicator of Compromises) such as hostnames, IP addresses, or URL patterns.

- This analysis is commonly triggered by:
    - IDPS alerts
    - Anomaly detection
    - Information provided by other organizations
    - Reports from users
    - The results of DFIR task
    - Malware hunting.

# Computer Forensics

# Computer Forensics Basics (1)

- Computer forensics is a part of digital forensics steps for finding out what occurred on suspicious hosts by dumping memories or disks and analyzing them.
- We can investigate them by mounting or parsing the images and extracting data that is called **<u>artifacts</u>** with forensics tools on the images.



◆ We analyze data without any APIs on running OSes. Therefore,

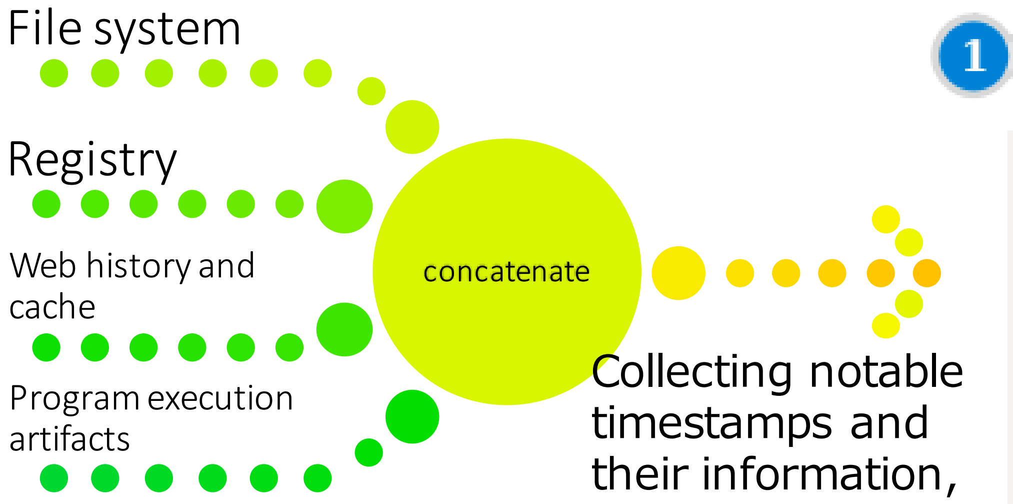
- ✓ We can analyze deleted data located in unallocated spaces.
- ✓ It is hardly affected by rootkit malware.

# Computer Forensics Basics (2) - A Variety

- There are several types of computer forensics.
  - Disk Forensics
    - This is the most fundamental method for analyzing the entire disk images.
  - Memory Forensics
    - This is a method for investigating the entire memory images.
    - This is one of the most important techniques because disk size is getting bigger these days.
  - Fast Forensics (with triaged acquisition)
    - This is an analysis method to get results rapidly by acquiring only the effective, efficient, and sufficient artifacts instead of acquiring the entire images.
  - Live Forensics / Response
    - This is to apply forensics techniques on the running machines.
    - EDR products are classified as this technique with memory forensics method.

# Computer Forensics Basics (3) - Timeline

1. We collect various remarkable timestamps in acquired memory and disk images such as file system, registry and so on, and arrange them in chronological order.
   - Time zone is very important. Whether timestamps are recorded as local time or UTC depends on each artifact. You must pay attention while analyzing them.
2. By investigating the timeline and the artifacts, we find out the evidence left by attackers.



File system

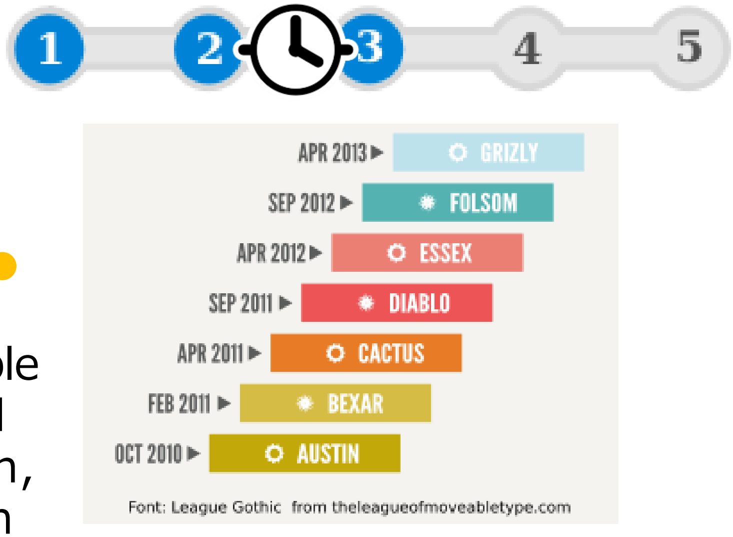
Registry

Web history and cache

Program execution artifacts

concatenate

Collecting notable timestamps and their information, and sort them in time series order



A timeline

# Computer Forensics Basics (4) - Artifacts

This is a list of some artifacts.

- File system (NTFS)
  - $MFT
  - $LogFile
  - $UsnJrnl:$J
- OS artifacts
  - Prefetch
  - Offce Recent
  - Recent
  - Jumplist
  - LNK
  - RecentFileCache.bcf
  - Amcache.hve
- Event logs
- Task Scheduler
- Registry
  - *MRU
  - Recent
  - Shellbag
  - Amcache
  - Shimcache (Application Compatibility Cache)
  - UserAssist
  - AppComatFlags
  - Legacy Registry Keys
- Web Browsers
  - Cache
  - History
  - Cookie
- E-mail
  - cache
  - Mail box

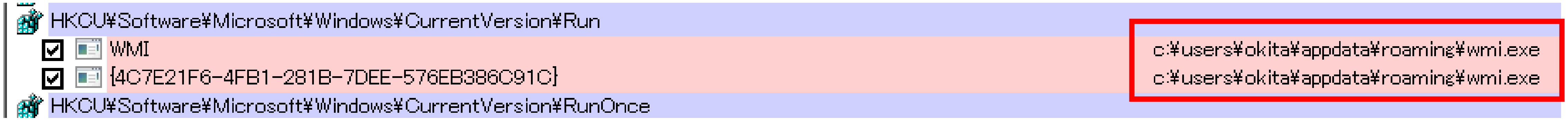
# Computer Forensics Basics (5) - Pivot Points

- Finding pivot points
  - Pivot point is a significant evidence that is a starting point of analysis.
  - For example, these artifacts could be pivot points:
    - File/Registry paths
    - Processes information
    - Hostnames or URLs information
  - If you don’t have any pivot points, we can still identify the installation date of malware as a pivot point by investigating auto-start locations.
  - If you were able to specify malware, you can trace extra activities by investigating events that were recorded at dates around the pivot point.
    - Before the date: The root cause of the infection
    - After the date: The attackers’ activities such as lateral movements

# Computer Forensics Basics (6) - Pivot Points

- Identifying malicious programs
  - Malware often starts up automatically by hiding in auto-start locations such as registry.
    - Sysinternals Autoruns can enumerate a lot of locations with the registration dates and its program locations.
    - We can use it as a pivot point.

HKEY_CURRENT_USER

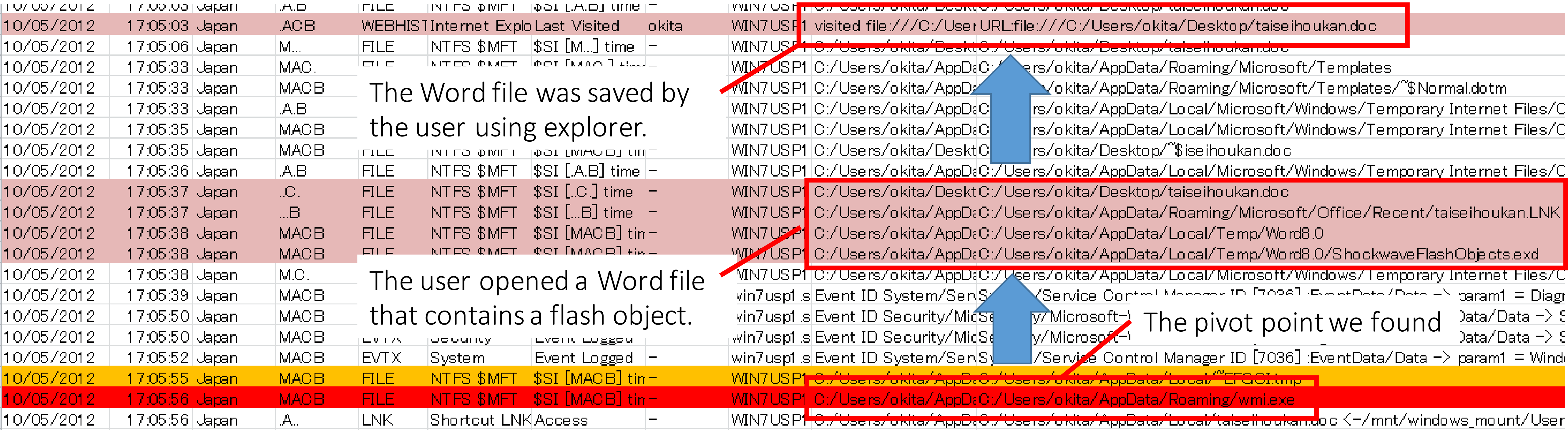


```
HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥Run
  ☑ WMI                                          c:¥users¥okita¥appdata¥roaming¥wmi.exe
  ☑ {4C7E21F6-4FB1-281B-7DEE-576EB386C91C}       c:¥users¥okita¥appdata¥roaming¥wmi.exe
HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥RunOnce
```

The result of Sysinternals Autoruns

# Computer Forensics Basics (7) - Timeline Analysis

- Timeline analysis
  - After finding a pivot point, you can find a possible root cause of the infection by investigating other artifacts such as file system metadata and registry timestamps.



| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 10/05/2012 | 17:05:03 | Japan | .A.B | FILE | NTFS $MFT | $SI [.A.B] time | - | WIN7USP1 | C:/Users/okita/Deskt | C:/Users/okita/Desktop/taiseihoukan.doc | |
| 10/05/2012 | 17:05:03 | Japan | .ACB | WEBHIST | Internet Explo | Last Visited | okita | WIN7USP1 | visited file:///C:/User | URL:file:///C:/Users/okita/Desktop/taiseihoukan.doc | |
| 10/05/2012 | 17:05:06 | Japan | M... | FILE | NTFS $MFT | $SI [M...] time | - | WIN7USP1 | C:/Users/okita/Deskt | C:/Users/okita/Desktop/taiseihoukan.doc | |
| 10/05/2012 | 17:05:33 | Japan | MAC. | FILE | NTFS $MFT | $SI [MAC.] time | - | WIN7USP1 | C:/Users/okita/AppDa | C:/Users/okita/AppData/Roaming/Microsoft/Templates | |
| 10/05/2012 | 17:05:33 | Japan | MACB | | | | | WIN7USP1 | C:/Users/okita/AppDa | C:/Users/okita/AppData/Roaming/Microsoft/Templates/~$Normal.dotm | |
| 10/05/2012 | 17:05:33 | Japan | .A.B | | | | | WIN7USP1 | C:/Users/okita/AppDa | C:/Users/okita/AppData/Local/Microsoft/Windows/Temporary Internet Files/C | |
| 10/05/2012 | 17:05:35 | Japan | MACB | | | | | WIN7USP1 | C:/Users/okita/AppDa | C:/Users/okita/AppData/Local/Microsoft/Windows/Temporary Internet Files/C | |
| 10/05/2012 | 17:05:35 | Japan | MACB | FILE | NTFS $MFT | $SI [MACB] tin | - | WIN7USP1 | C:/Users/okita/Deskt | C:/Users/okita/Desktop/~$iseihoukan.doc | |
| 10/05/2012 | 17:05:36 | Japan | .A.B | FILE | NTFS $MFT | $SI [.A.B] time | - | WIN7USP1 | C:/Users/okita/AppDa | C:/Users/okita/AppData/Local/Microsoft/Windows/Temporary Internet Files/C | |
| 10/05/2012 | 17:05:37 | Japan | ..C. | FILE | NTFS $MFT | $SI [..C.] time | - | WIN7USP1 | C:/Users/okita/Deskt | C:/Users/okita/Desktop/taiseihoukan.doc | |
| 10/05/2012 | 17:05:37 | Japan | ...B | FILE | NTFS $MFT | $SI [...B] time | - | WIN7USP1 | C:/Users/okita/AppDa | C:/Users/okita/AppData/Roaming/Microsoft/Office/Recent/taiseihoukan.LNK | |
| 10/05/2012 | 17:05:38 | Japan | MACB | FILE | NTFS $MFT | $SI [MACB] tin | - | WIN7USP1 | C:/Users/okita/AppDa | C:/Users/okita/AppData/Local/Temp/Word8.0 | |
| 10/05/2012 | 17:05:38 | Japan | MACB | FILE | NTFS $MFT | $SI [MACB] tin | - | WIN7USP1 | C:/Users/okita/AppDa | C:/Users/okita/AppData/Local/Temp/Word8.0/ShockwaveFlashObjects.exd | |
| 10/05/2012 | 17:05:38 | Japan | M.C. | | | | | WIN7USP1 | C:/Users/okita/AppDa | C:/Users/okita/AppData/Local/Microsoft/Windows/Temporary Internet Files/C | |
| 10/05/2012 | 17:05:39 | Japan | MACB | | | | | win7usp1.s | Event ID System/Ser | System/Service Control Manager ID [7036] :EventData/Data -> | param1 = Diagr |
| 10/05/2012 | 17:05:50 | Japan | MACB | | | | | win7usp1.s | Event ID Security/Mic | Security/Microsoft-\ | Data/Data -> S |
| 10/05/2012 | 17:05:50 | Japan | MACB | EVTX | Security | Event Logged | | win7usp1.s | Event ID Security/Mic | Security/Microsoft-\ | Data/Data -> S |
| 10/05/2012 | 17:05:52 | Japan | MACB | EVTX | System | Event Logged | - | win7usp1.s | Event ID System/Ser | System/Service Control Manager ID [7036] :EventData/Data -> | param1 = Windc |
| 10/05/2012 | 17:05:55 | Japan | MACB | FILE | NTFS $MFT | $SI [MACB] tin | - | WIN7USP1 | C:/Users/okita/AppDa | C:/Users/okita/AppData/Local/~EFCOI.tmp | |
| 10/05/2012 | 17:05:56 | Japan | MACB | FILE | NTFS $MFT | $SI [MACB] tin | - | WIN7USP1 | C:/Users/okita/AppDa | C:/Users/okita/AppData/Roaming/wmi.exe | |
| 10/05/2012 | 17:05:56 | Japan | .A.. | LNK | Shortcut LNK | Access | - | WIN7USP1 | C:/Users/okita/AppDa | C:/Users/okita/AppData/Local/taiseihoukan.doc <-/mnt/windows_mount/User | |

The Word file was saved by the user using explorer.

The user opened a Word file that contains a flash object.

The pivot point we found

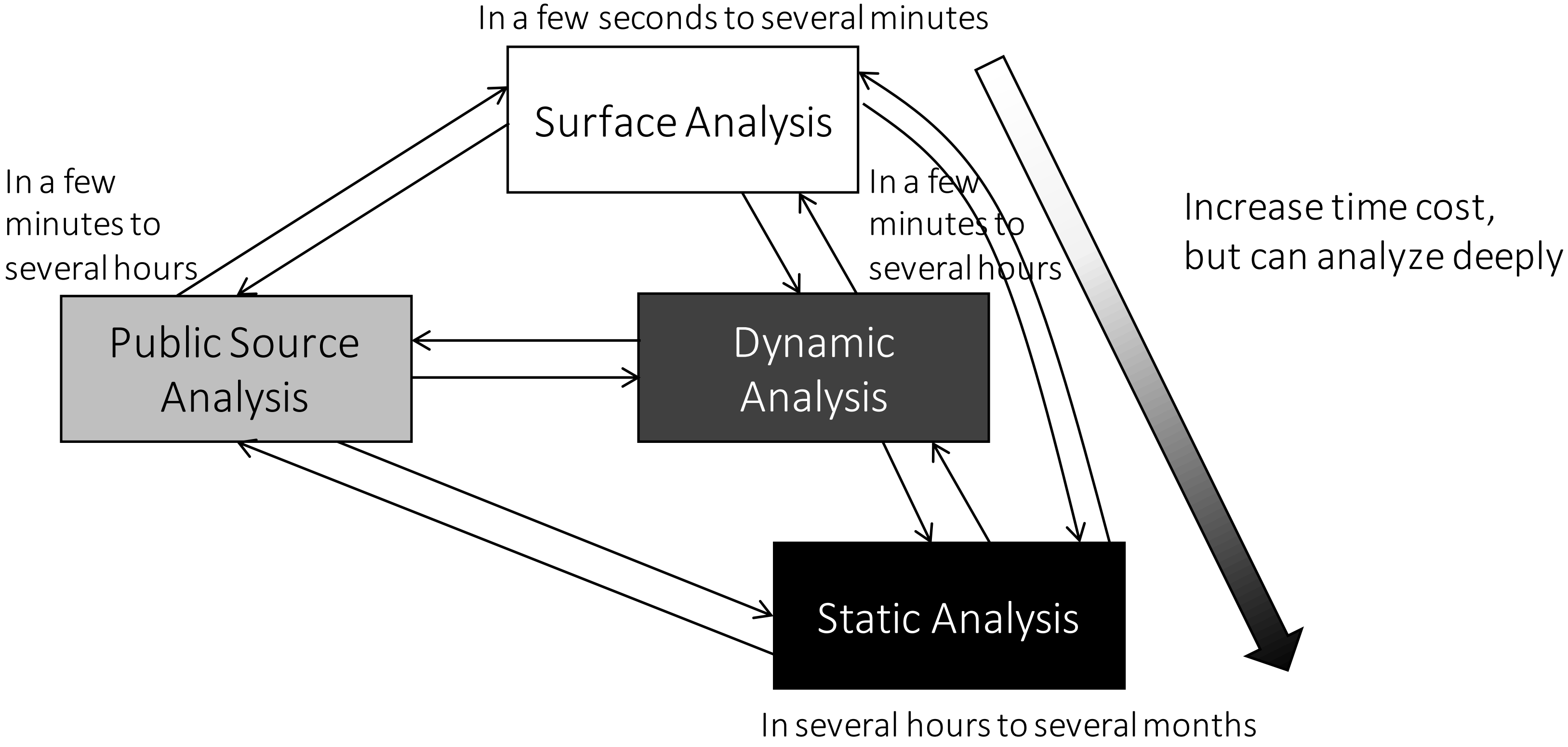
# Malware Analysis

# What is Malware Analysis?

- It is a method to reveal malware behavior by combining the methods below.
    - Surface Analysis
    - Dynamic Analysis (Runtime analysis, Black box analysis)
    - Static Analysis (White box analysis, Reverse (code) engineering, Reversing…)
        - There are other definitions; the terminologies and the definitions are not fixed.
            - Sometimes, surface analysis is included in static analysis.
        - There is “public source analysis” as well (in other words, googling ;-)).

# What is Malware Analysis? (Cont.)

- We need to feedback each analysis results to other methods.



In a few seconds to several minutes
Surface Analysis
In a few minutes to several hours
In a few minutes to several hours
Increase time cost, but can analyze deeply
Public Source Analysis
Dynamic Analysis
Static Analysis
In several hours to several months

# The Example of Response Flow

# Incident Response Flow

- How long do we perform incident response and how should we handle it?
  - Of course, it depends on incident scales. Let’s assume that it was a small incident.

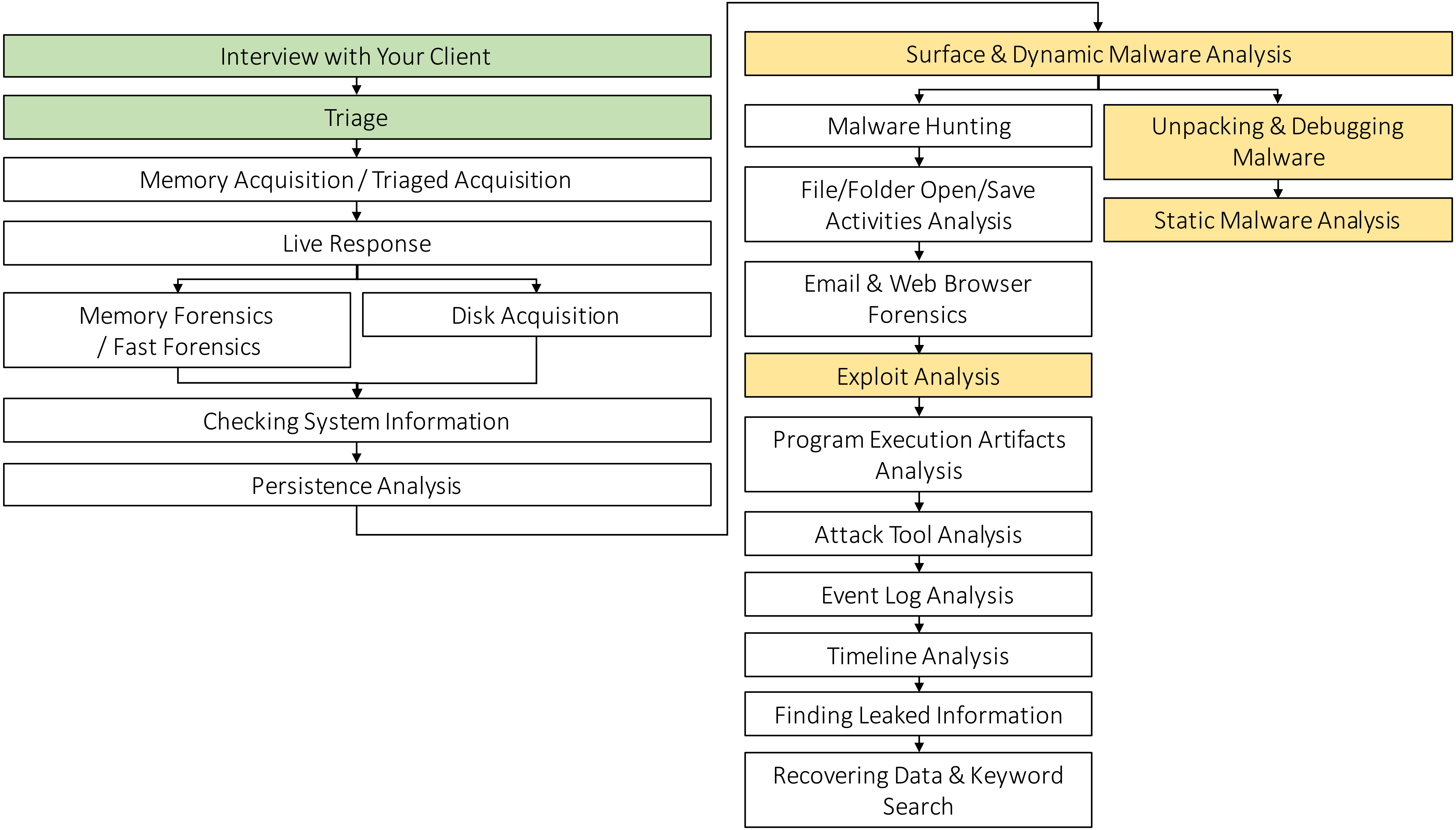
- Condition:
  - Targets are one or a few computers.
  - The targets consist of only clients, not including servers.

- We investigate the PCs and perform first response in one or two weeks.
  - The period depends on client’s budget.
  - If we have two weeks or more for the investigation, we may extend our analysis to perform static malware analysis.

- See “01_Introduction\IncidentResponseFlow.html” on the “shortcuts” folder. It shows you an example of incident response flow.

# Incident Response Flow

- When we perform a large scale incident case, for example, over a thousand computers, we will not investigate all the computers in the same way.
  - In that case, we will sample several computers that are likely to be related to an incident and investigate them first. Then, we will perform malware hunting and so on. We might investigate important servers such as active directory servers and file servers. Lastly, we will decide a plan on whether we need to take more action or not, based on the results of the incident.
  - Or, we will check all computers with EDR for example, by using collected IoCs instead of performing full course of the DFIR tasks.



Interview with Your Client

Triage

Memory Acquisition / Triaged Acquisition

Live Response

Memory Forensics / Fast Forensics

Disk Acquisition

Checking System Information

Persistence Analysis

Surface & Dynamic Malware Analysis

Malware Hunting

File/Folder Open/Save Activities Analysis

Email & Web Browser Forensics

Exploit Analysis

Program Execution Artifacts Analysis

Attack Tool Analysis

Event Log Analysis

Timeline Analysis

Finding Leaked Information

Recovering Data & Keyword Search

Unpacking & Debugging Malware

Static Malware Analysis

# About the Fictional Scenarios

# About the Fictional Scenarios

- We provide a fictional scenario.
  - Scenario 1
- See “Documents\Appendix_01_Scenario.pdf” on your USB storage.
- In this training course, we mainly perform incident response along the scenario.