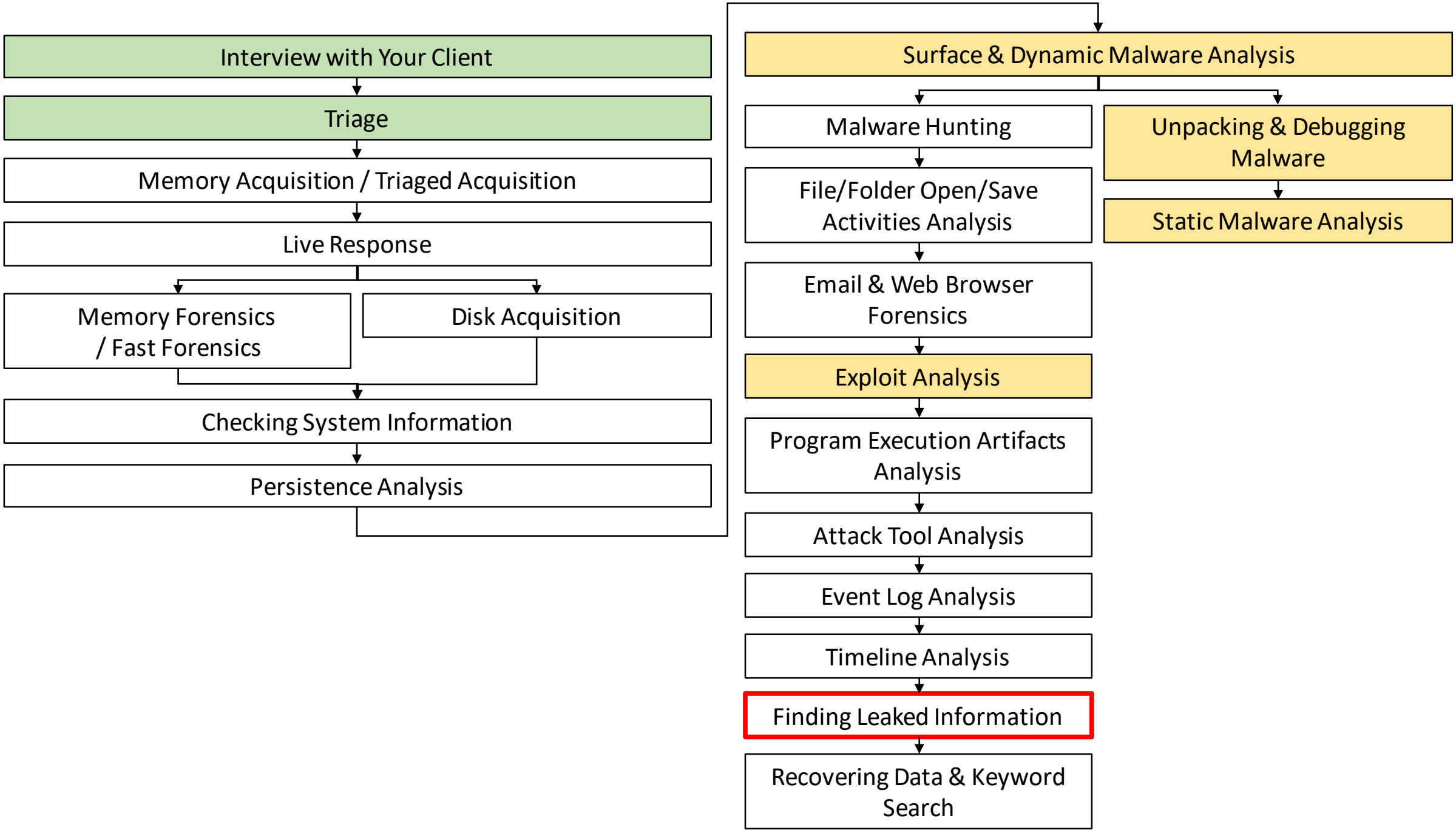
Finding Leaked Information


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

Finding Leaked Information

- One of the major objectives for the attackers to intrude into an enterprise network would be to steal files from the network.
  - Identifying the files the attackers accessed during the intrusion becomes necessary in forensics.
- When a file was accessed on the system, some file access related artifacts will be recorded.
  - Just like we have taken a look at open and save histories for files and folders, the file access histories would be helpful for illustrating the activities that occurred during the attack.

Topics Covered In This Section

- File Access Events
- MountPoints2
- Volume Shadow Copies
- USB Related Artifacts

File Access Events

File Access Events

- The timestamps may help us figure out what files the attackers created or modified.
  - We also would like to know which files the attackers accessed during the attack.
- NTFS has MACB timestamps.

  M = Modification, A = Access, C = Change, B = Birth
- Timestamp of “Access” is not recorded on Windows Vista and later by default.
  - Use of audit logs is essential for recording the file access events.
  - Windows 10 1803 or later may record it under certain conditions.

Auditing File Access Events

- When files are accessed on the local file system or over the network, these actions are logged on the audit Event Logs in Security.evtx.
  - For local accesses, event 4656, 4660, 4663 or 4690 might be helpful.
  - For network accesses, events such as 5140 or 5145 might be helpful.
  - Unfortunately, these IDs are not enabled by default.

File Sharing Related Events

- Why is this event important?
  - If attackers steal important documents from remote file servers, you could be able to find those evidences.

- Important events
  - Security.evtx

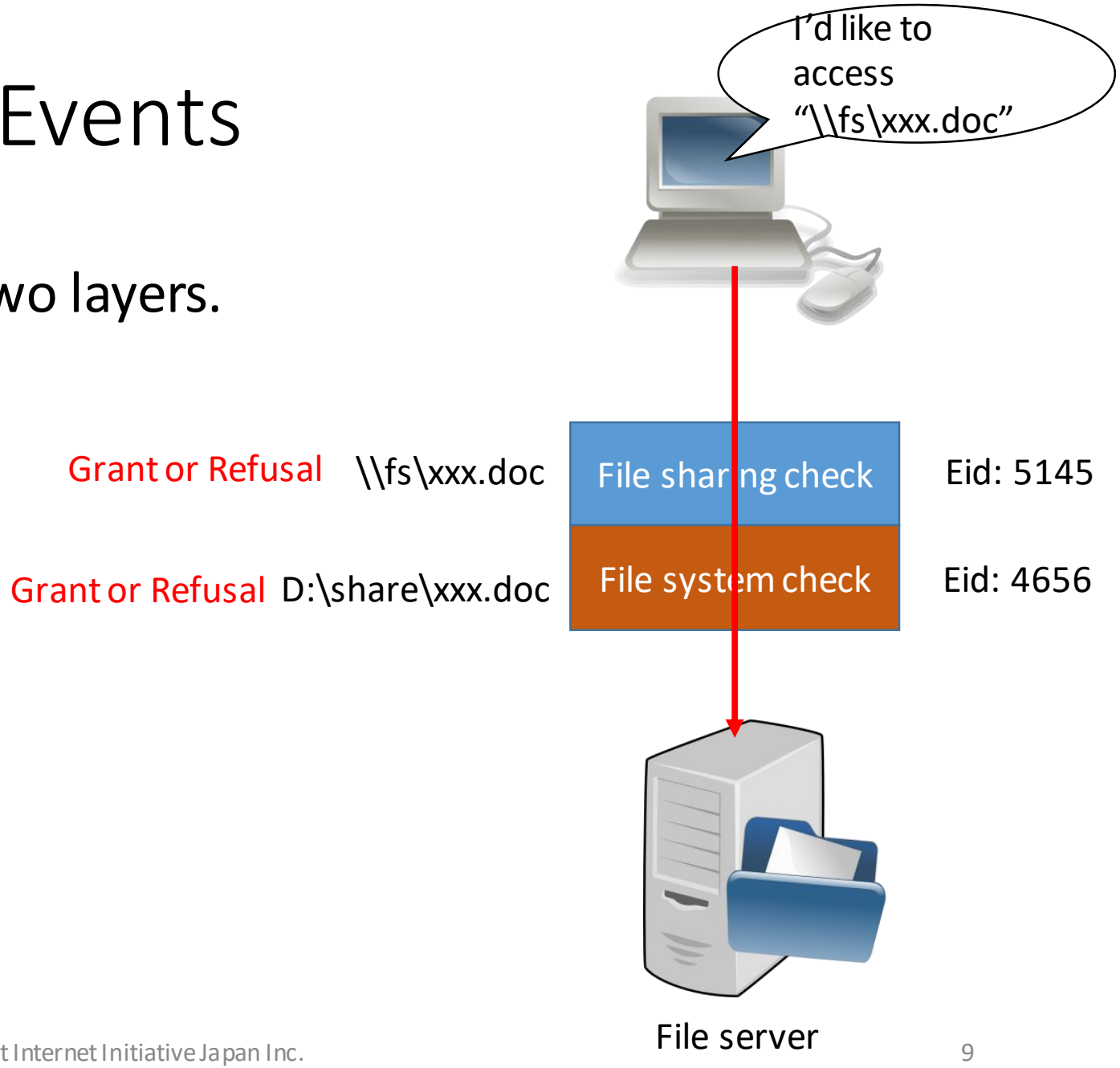
Note that these are NOT enabled by default, but let's assume you have enabled these events.

File sharing (SMB) events
- 5140: A network share object was accessed.
- 5145: A network share object was checked to see whether client can be granted desired access.

File system events
- 4656: A handle to an object was requested.
- 4663: An attempt was made to access an object.
- 4660: An object was deleted.
- 4690: An attempt was made to duplicate a handle to an object.

File Sharing Related Events

- We need to check logs from two layers.
  - Event ID 5145:
    - ACLs on file shares.
  - Event ID 4656:
    - ACLs on file systems.



File Sharing Related Events

- Let's assume these conditions are given.
  - Important files are located in “D:\share\secret” directory on the file server.
    - This directory is only for “ishikawa” account, and even domain administrators are restricted to access the directory.
  - Another important files are these files on the file sever.
    - D:\share\public\docs\20170706_daikan_meeting\20170706_daikan_meeting.docx
    - D:\share\public\reports\iir_vol32.pdf
    - According to this organization, this directory is supposed to be accessed with “dkato” account only.
  - Are those files accessed by someone who is unexpected?

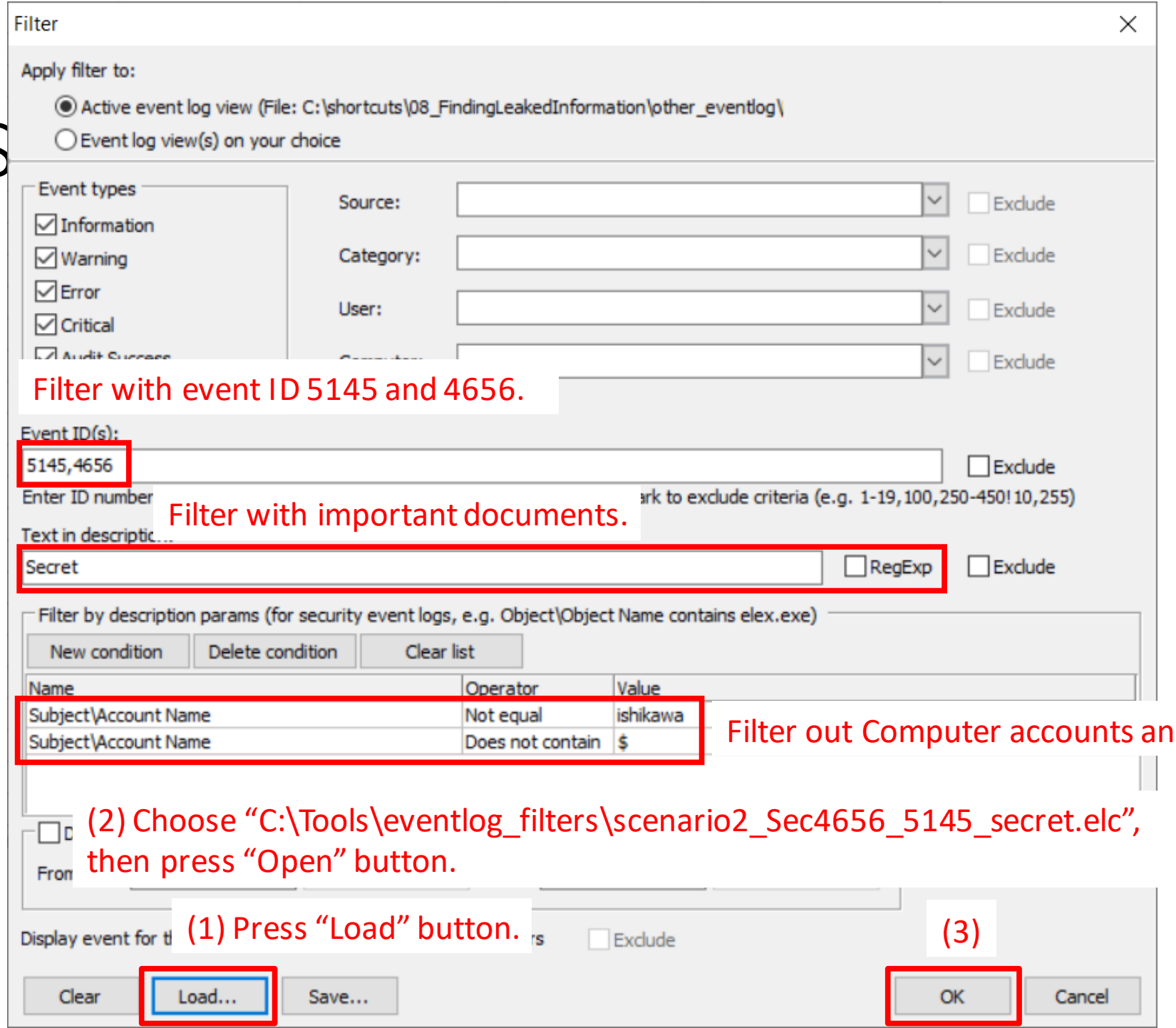
File Sharing Related Events

- Open the log below with Event Log Explorer, and press “Filter Events” button.
  - E:\Artifacts\other_eventlog\FileEvt_Security.evtx
    - Original file: Security.evtx

Notice:

You can **drag** the log file **and drop** it to Event Log Explorer.

File S


Filter
Apply filter to:
Active event log view (File: C:\shortcuts\08_FindingLeakedInformation\other_eventlog\
Event log view(s) on your choice
Event types
Information
Warning
Error
Critical
Source:
Category:
User:
Exclude
Filter with event ID 5145 and 4656.
Event ID(s):
5145,4656
Exclude
Enter ID number
ark to exclude criteria (e.g. 1-19,100,250-450!10,255)
Filter with important documents.
Text in descriptio
Secret
RegExp
Exclude
Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)
New condition
Delete condition
Clear list
Name
Operator
Value
Subject\Account Name
Not equal
ishikawa
Subject\Account Name
Does not contain
$
Filter out Computer accounts and the legitimate user.
(2) Choose “C:\Tools\eventlog_filters\scenario2_Sec4656_5145_secret.elc”, then press “Open” button.
From
Display event for t
(1) Press “Load” button.
rs
Exclude
(3)
Clear
Load...
Save...
OK
Cancel

File Sh

Type	Date	Time	Event	Source
Audit Success	7/20/2017	6:39:05 PM	5145	Microsoft-Windows

Description

A network share object was checked to see whether client can be granted desired access.

Subject:
- Security ID: S-1-5-21-1546390377-3790665809-845109970-500
- Account Name: Administrator
- Account Domain: DFIR-NINJA
- Logon ID: 0x18db77d

Network Information:
- Object Type: File
- Source Address: 192.168.52.40
- Source Port: 49725

Share Information:
- Share Name: *\share
- Share Path: \??\D:\share
- Relative Target Name: secret

Access Request Information:
- Access Mask: 0x100081
- Accesses: SYNCHRONIZE
  ReadData (or ListDirectory)

It seems that access to a secret folder was granted…,

Access Check Results:
- SYNCHRONIZE
- : Granted by D:(A;;FA;;;WD)
- ReadData (or ListDirectory)
- : Granted by D:(A;;FA;;;WD)
- ReadAttributes
- : Granted by D:(A;;FA;;;WD)

Description | Data

Events: 37811 Displayed: 6 Selected: 1

File S

Type	Date	Time	Event	Source
Audit Failure	7/20/2017	6:39:05 PM	4656	Microsoft-Windo

Description

A handle to an object was requested.

Subject:

Security ID: S-1-5-21-1546390377-3790665809-845109970-500
Account Name: Administrator
Account Domain: DFIR-NINJA
Logon ID: 0x18db77d

Object:

Object Server: Security
Object Type: File
Object Name: D:\share\secret
Handle ID: 0x0
Resource Attributes:

Process Information:

Process ID: 0x4
Process Name:

Access Request Information:

Transaction ID: {00000000-0000-0000-0000-000000000000}

but Administrator account could not access secret directory because it was denied by file system ACL.

Access Reasons: SYNCHRONIZE
: Not granted

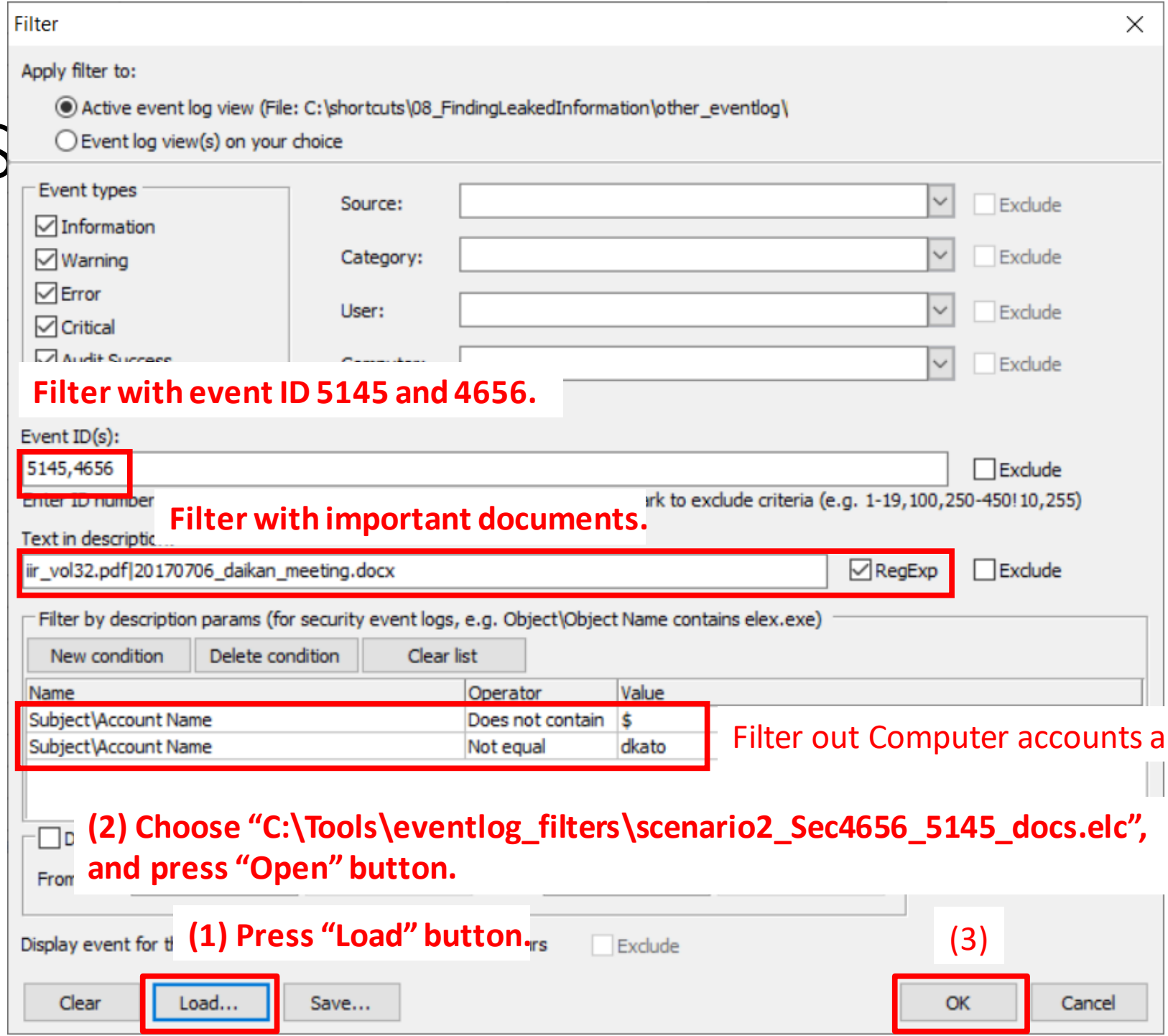
ReadData (or ListDirectory)
: Not granted

ReadAttributes
: Granted by ACE on parent folder
D:(A;OICI;0x1301bf;;;DU)

Access Mask: 0x100081

Description Data

File S


Filter
Apply filter to:
Active event log view (File: C:\shortcuts\08_FindingLeakedInformation\other_eventlog\
Event log view(s) on your choice
Event types
Information
Warning
Error
Critical
Source:
Category:
User:
Exclude
Filter with event ID 5145 and 4656.
Event ID(s):
5145,4656
Filter with important documents.
Text in descriptio
iir_vol32.pdf|20170706_daikan_meeting.docx
RegExp
Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)
New condition
Delete condition
Clear list
Name
Operator
Value
Subject\Account Name
Does not contain
$
Subject\Account Name
Not equal
dkato
Filter out Computer accounts and the legitimate user.
(2) Choose "C:\Tools\eventlog_filters\scenario2_Sec4656_5145_docs.elc", and press "Open" button.
(1) Press "Load" button.
(3)
Clear
Load...
Save...
OK
Cancel

Type	Date	Time	Event	Source
Audit Success	7/20/2017	6:45:56 PM	4656	Microsoft-Windo
Audit Success	7/20/2017	6:45:56 PM	5145	Microsoft-Windo

Description

A network share object was checked to see whether client can be granted desired access.

Subject:
- Security ID: S-1-5-21-1546390377-3790665809-845109970-500
- Account Name: Administrator
- Account Domain: DFIR-NINJA
- Logon ID: 0x18db77d

Network Information:
- Object Type: File
- Source Address: 192.168.52.40
- Source Port: 51244

Share Information:
- Share Name: *\share
- Share Path: \??\D:\share
- Relative Target Name: public\reports\iir_vol32.pdf

Access Request Information:
- Access Mask: 0x120089

Description Data

Events: 37811 Displayed: 4 Selected: 1

Type	Date	Time	Event
Audit Success	7/20/2017	6:45:56 PM	4656
Audit Success	7/20/2017	6:45:56 PM	5145

Description

- Relative Target Name: public\reports\iir_vol32.pdf

Access Request Information:
- Access Mask: 0x120089
- Accesses: READ_CONTROL
  SYNCHRONIZE
  ReadData (or ListDirectory)
  ReadEA
  ReadAttributes

Access Check Results:
- READ_CONTROL
  : Granted by Ownership
- SYNCHRONIZE
  : Granted by D:(A;;FA;;;WD)
- ReadData (or ListDirectory)
  : Granted by D:(A;;FA;;;WD)

The Built-in Administrator account was granted the rights to read “iir_vol32.pdf” via SMB from “192.168.52.40”.

Type	Date	Time	Event	Source
Audit Success	7/20/2017	6:45:56 PM	4656	Microsoft-Windo
Audit Success	7/20/2017	6:45:56 PM	5145	Microsoft-Windo

Description

A handle to an object was requested.

Subject:

Security ID: S-1-5-21-1546390377-3790665809-845109970-500

Account Name: Administrator

Account Domain: DFIR-NINJA

Logon ID: 0x18db77d

Object:

Object Server: Security

Object Type: File

Object Name: D:\share\public\reports\iir_vol32.pdf

Handle ID: 0xb38

Resource Attributes: -

Process Information:

Process ID: 0x4

Process Name:

Access Request Information:

Transaction ID: {00000000-0000-0000-0000-000000000000}

Accesses: READ_CONTROL
SYNCHRONIZE
ReadData (or ListDirectory)
ReadEA

Description Data

Type	Date	Time	Event
Audit Success	7/20/2017	6:45:56 PM	4656
Audit Success	7/20/2017	6:45:56 PM	5145

Description

ReadEA
ReadAttributes

Access Reasons: READ_CONTROL
: Granted by Ownership
SYNCHRONIZE
: Granted by
D:(A;ID;0x1301bf;;;DU)
ReadData (or ListDirectory)
: Granted by
D:(A;ID;0x1301bf;;;DU)
ReadEA
: Granted by
D:(A;ID;0x1301bf;;;DU)
ReadAttributes
: Granted by
D:(A;ID;0x1301bf;;;DU)

Access Mask: 0x120089

Privileges Used for Access Check: -

Restricted SID Count: 0

Description Data

The Built-in Administrator account was also “granted” the rights to read the data of “iir_vol32.pdf”. It means, this file is likely to be stolen by the attackers.

Type	Date	Time	Event	Source
Audit Success	7/20/2017	6:45:56 PM	4656	Microsoft-Windo
Audit Success	7/20/2017	6:45:56 PM	5145	Microsoft-Windo

Description

A handle to an object was requested.

Subject:
- Security ID: S-1-5-21-1546390377-3790665809-845109970-500
- Account Name: Administrator
- Account Domain: DFIR-NINJA
- Logon ID: 0x18db77d

Object:
- Object Server: Security
- Object Type: File
- Object Name: D:\share\public\reports\ir_vol32.pdf
- Handle ID: 0xb38
- Resource Attributes: -

Process Information:
- Process ID: 0x4
- Process Name:

Access Request Information:
- Transaction ID: {00000000-0000-0000-0000-000000000000}
- Accesses: READ_CONTROL
  SYNCHRONIZE
  ReadData (or ListDirectory)
- ReadEA

Description | Data

Type	Date	Time	Event	S
Audit Success	7/20/2017	6:37:07 PM	4624	M

Description

New Logon:
- Security ID: S-1-5-21-1546390377-3790665809-845
- Account Name: Administrator
- Account Domain: DFIR-NINJA
- Logon ID: 0x18db77d
- Linked Logon ID: (null)
- Network Account Name: (null)
- Network Account Domain: (null)
- Logon GUID: {9392082C-C942-264F-6832-22B1621C

Process Information:
- Process ID: 0x0
- Process Name: -

Network Information:
- Workstation Name:
- Source Network Address: 192.168.52.40
- Source Port: 49725

Detailed Authentication Information:

Audit Success	7/20/2017	6:45:56 PM	4663	M
Audit Success	7/20/2017	6:45:56 PM	4663	M

Description

An attempt was made to access an object.

Subject:
- Security ID: S-1-5-21-1546390377-3790665809-845
- Account Name: Administrator
- Account Domain: DFIR-NINJA
- Logon ID: 0x18db77d

Object:
- Object Server: Security
- Object Type: File
- Object Name: D:\share\public\reports\ir_vol32.pdf
- Handle ID: 0xb38
- Resource Attributes: S:AI

Process Information:
- Process ID: 0x4
- Process Name:

Access Request Information:
- Accesses: ReadData (or ListDirectory)

Even if you don't record file sharing events, you can still get source address information by linking logon ID with 4656 and 4624.

You can also confirm actual activities of the attackers by linking logon ID and handle ID with 4656 and 4663.

MountPoints2

Mounting Storage Devices

- When accessing a storage device on an operating system, you will need to mount the storage device.
  - Just like we do using the Arsenal Image Mounter.
- When a storage device is mounted, there will be an artifact that will remain on the computer.

MountPoints2

- If paths (local or network) were mounted, the histories may be recorded at "**SOFTWARE\Microsoft\Windows \CurrentVersion\Explorer\MountPoints2**" in the user's registry hive.
- "Mount" can happen when:
  - A drive letter (e.g. **C**) was assigned to a storage partition.
    - The device could be both local and network shares; you can assign a drive letter to a network share, and treat it like a partition on the local computer.
  - A removal media (e.g. CD-ROM) was inserted to a removal drive.
    - These are managed with UUID under the registry.
- Mountpoints2 keys are recorded when the mounting took place on Windows Explorer.
  - They will not be created when the mounting took place on other tools.
  - And, often attacks do not take place on Windows Explorer.

Volume Shadow Copies

Volume Shadow Copies

- A Volume Shadow Copy is a snapshot of volume that was taken at a certain point of time.
  - Often called as “VSS”, which came from “Volume Shadow Copy Service”.
- Even if files were modified or deleted during the attack, it may be possible to recover them from the VSS snapshots.
  - We will discuss about file recoveries from VSS snapshots in “Recovering Deleted Data” chapter.

USB Related Artifacts

When a Device is Connected…

- When a device is connected to a computer, device drivers are installed.
  - When devices are installed, driver files may be copied to the Windows system folder.
- Windows has device structures in the registry.
  - **HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses**

USB Device Registries

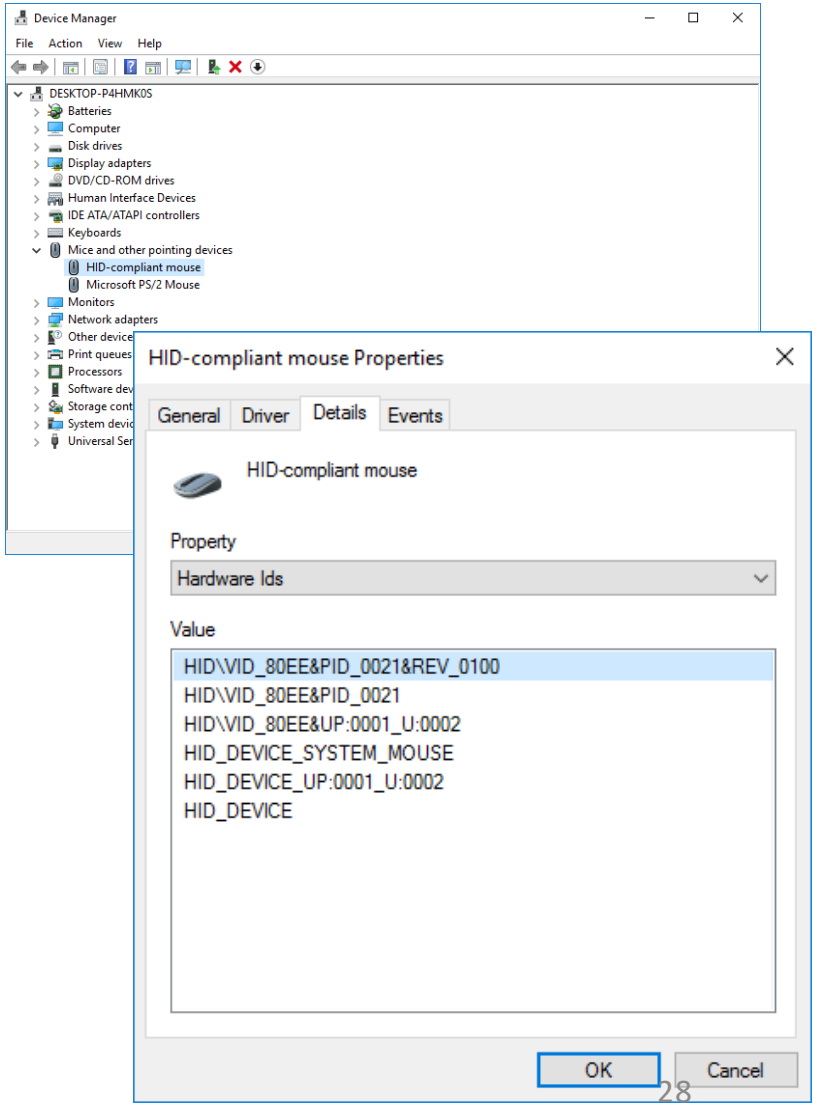
- When the connected device is a USB device, the following registries entries are modified.
  - **HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB**
- Under this key, properties of the devices are organized in their identification numbers.

Identification of Devices

- Each device has its own Vendor ID (VID) and Product ID (PID).
  - If there are two hardware that are **exactly** same, their VID and PID will be same.
  - If the product names are same, if the hardware revisions are different, different components (e.g. controllers) might be used.
    - In that case, the VID and PID might change.
- You can look for VID and PID from the Device Manager.

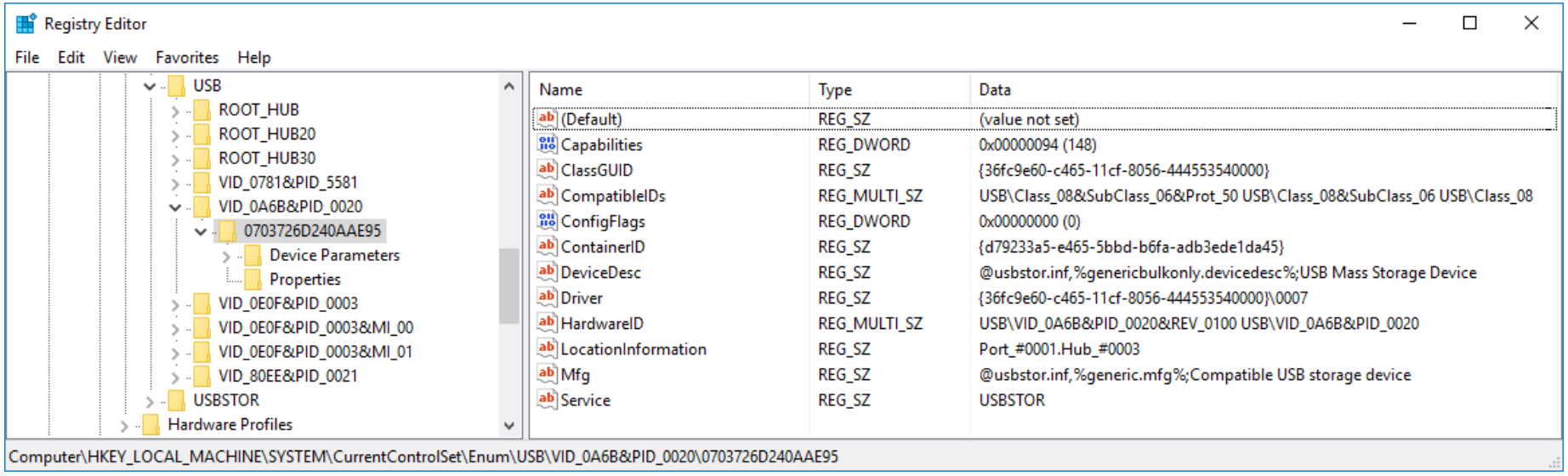
Looking for VID and PID

- One method to check the VID and PID is to use the Device Manager.
  - The Device Manager may be opened from the Control Panel.
    - It also can be searched from the Start Menu, and it can be started by calling “devmgmt.msc” from the “Run” menu.
- Double click on a device, and navigate to the “Details” tab. From the “Property” drop-down box, select “Hardware Ids” to see the device VID and PID.



Looking into USB Registries

- If you look into one of the keys in "**HKEY_LOCAL_MACHINE \SYSTEM\ControlSet001\Enum\USB**", you will notice that there is another subkey under the VID&PID key.
- This is the device **Instance ID**.



Device Instances

- When you connect a same device to a different port, the devices are considered as different **instances** of the devices.
- When the device instances are different, the devices are considered as a different device.
  - If you connect a USB mouse to a USB port, disconnect it and connect it to another port, it might take some time (at least longer than re-connecting it to the same port) for the mouse to start working.
  - This is because when the mouse is connected to another port, the device has to be re-installed.

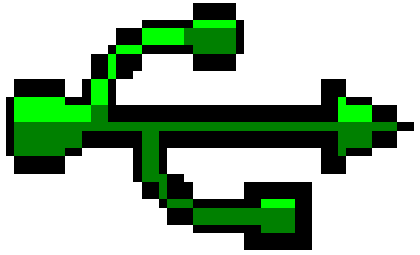
USB Device Histories

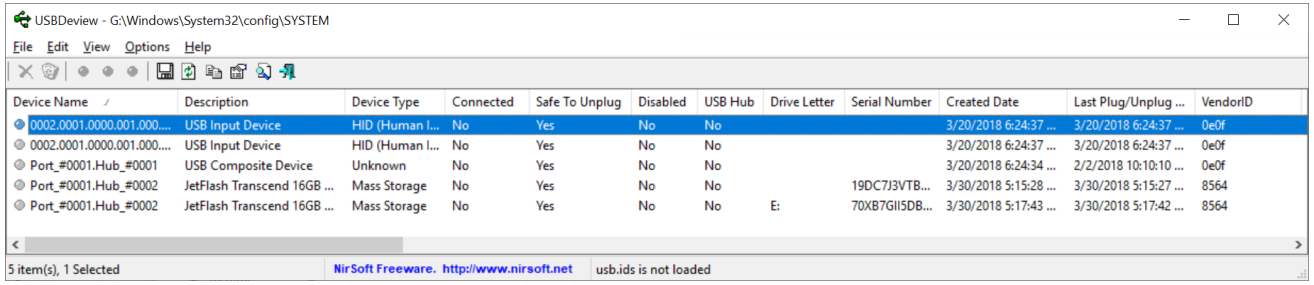
- If USB devices were used, the registry entry will be created.
- Even if the device was removed, unless the device was completely "uninstalled", the registry entry will remain.
- If the registry key exists, and the device **does not** exist on the Device Manager (or other device lists), that means the device was connected and then disconnected from the computer.

Tools for Viewing List of USB Devices

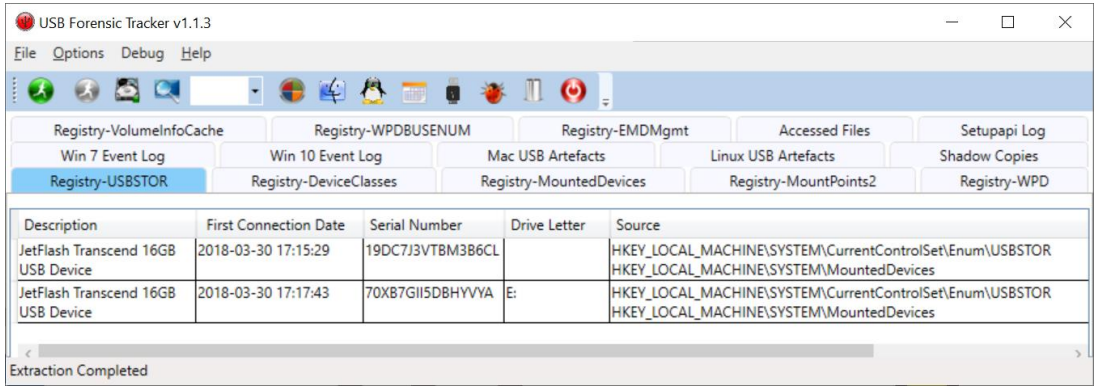
- There are several tools that show us the list of USB devices.

USBDeview





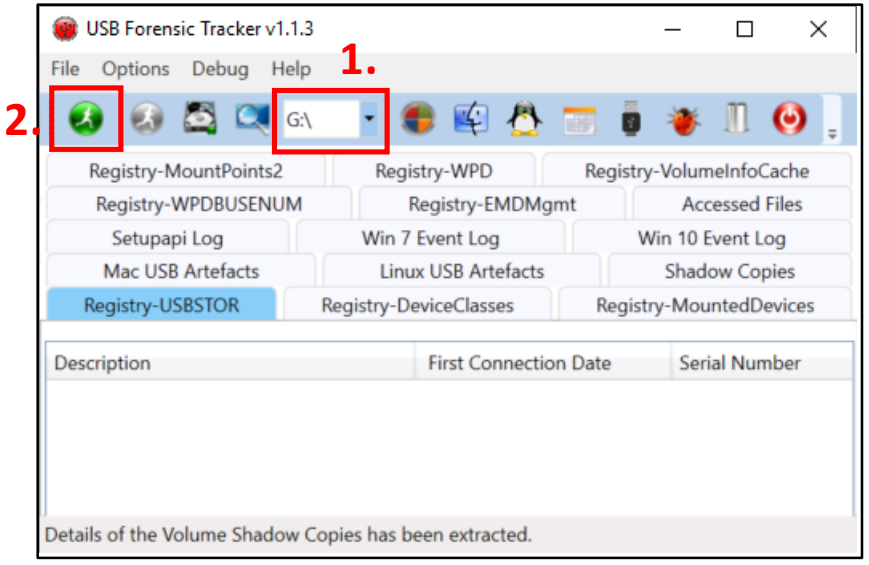
USB Forensic Tracker



Exercise:
Using USB Forensic Tracker

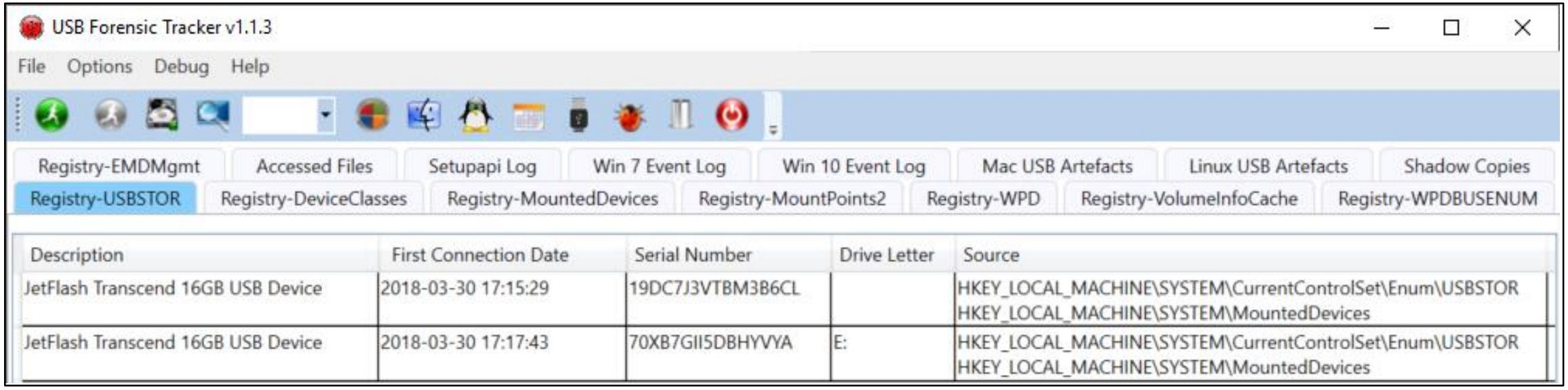
USB Forensic Tracker

- USB Forensic Tracker can gather the information related to USB and some other artifacts.
- From the tools folder, open **USBFT64.exe**.
  - Accept UAC when prompted.
- Once USB Forensic Tracker opens:
  1. Select drive “G” from the dropdown list.
     - We will continue using **Client-Win10-2_honda.E01** image. Please mount it if you have unmounted it.
  2. Press “Run” on the toolbar.



Exploring USB Forensic Tracker

- Once parsed, the list of USB devices and their information, such as partitions and device IDs, are displayed in tables.
  - You can also find some other parameters, such as Mountpoints2 registry contents.



Other Possible Findings

- We have been talking about registry, but there are also some other places we can look for the device artifacts.
- The examples include:
  - Event Log
    - Event ID 20001 and 20003 in “System” log
      - Indicates installation of a new device.
    - Audit Event ID 6416 in “Security” log (disabled by default)
      - When a USB device is connected, it is recorded.
  - Device driver files
    - When a device driver is installed, if the device driver did not exist on the system, the driver files might be copied to “**C:\Windows\System32\drivers**” folder. This could be identified with file audits and other methods.

Summary

Summary

- When a file was accessed on the system, some file access related artifacts will be recorded.
- The possible artifacts to look for in Windows are:
  - File access audits
  - Mount points
  - Volume Shadow Copies
  - USB devices