Image Mounting and Parsing

Image Mounting and Parsing

- Disk images were created during the acquisition process.
  - There were different types of disk image formats.
- The out-of-box Windows is not capable for reading any of the formats introduced before.
  - Additional tools are necessary to read their contents.

Image Mounting Tools

- What is image mounting tools?
  - Tools that can mount a disk image as a physical drive.
    - Once mounted, files in the disk image can be accessed with Explorer and other applications.
- Example Tools
  - Arsenal Image Mounter
  - FTK Imager
  - OSFMount
  - ewfmount
    - This tool has a feature which offers EWF image as RAW image.

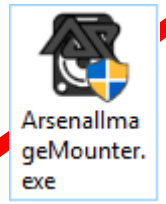
Image Parsing Tools

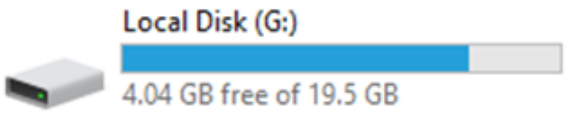
- What is image parsing tools?
  - Tools that can extract necessary data from a disk image without directly mounting them.
  - It is possible to extract data other than the original files, such as:
    - Meta files of the file system, such as $MFT, $UsrJrnl:$J, $LogFile, etc…
    - Deleted files
- Example Tools
  - The Sleuth Kit
  - FTK Imager

Difference between "Mounting" and "Parsing"

Mounting

Mount a disk image as a physical drive.





Files can be accessed using Explorer and other applications.

Parsing

```
E:\Artifacts\scenario1_E01>fls -o 1026048 Client-Win10-1_toyoda.E01 1269
d/d 31229-144-1:        All Users
d/d 1270-144-5: Default
d/d 31017-144-1:        Default User
d/d 91138-144-6:        defaultuser0
r/r 30162-128-1:        desktop.ini
d/d 95448-144-6:        ninja-master
d/d 113554-144-6:       ninja-rdp
d/d 91885-144-6:        ninjadmin
d/d 1318-144-5: Public
d/d 96037-144-5:        toyoda
```

Parsing tools directly analyze a file system.
Therefore, it is possible to access special files such as meta files, protected files by system, and deleted files.

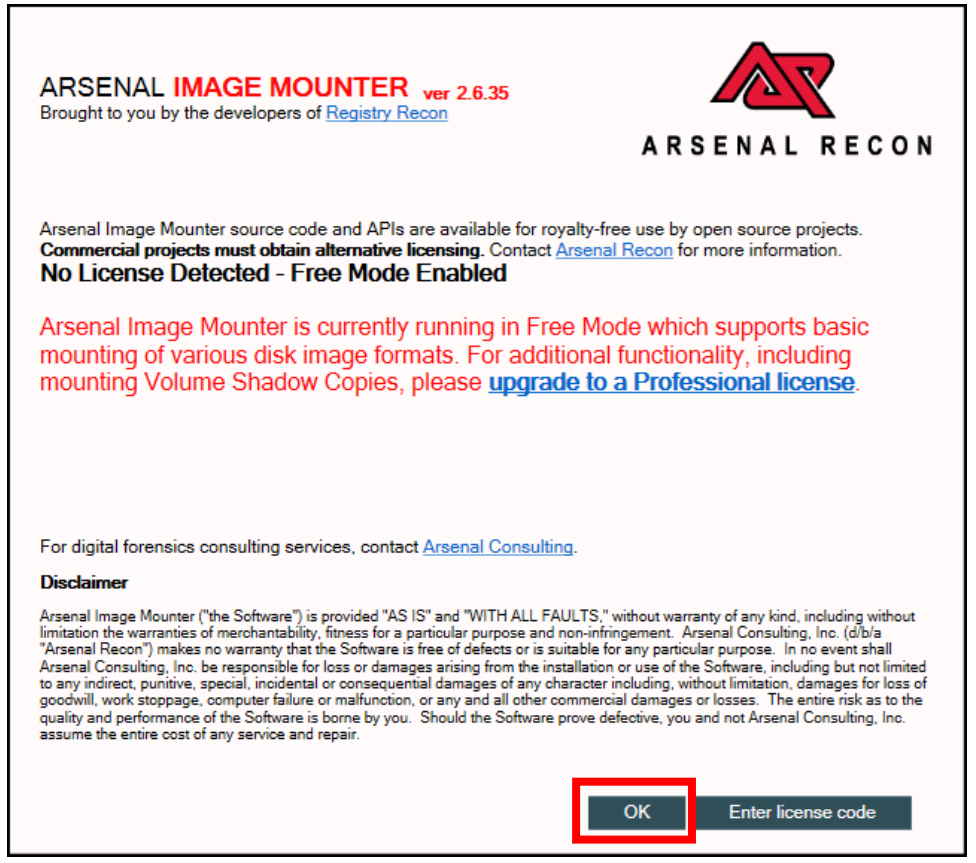
Exercise: Mounting Image File with Arsenal Image Mounter

Using Arsenal Image Mounter

- Arsenal Image Mounter mounts disk images and presents them as disks connected to the computer.
  - Not only the E01 format, but it supports multiple formats.
- We will be using Arsenal Image Mounter a lot throughout the course, so please get used to it.
- There is a shortcut for Arsenal Image Mounter in shortcuts folder.
  - **Shortcuts > 02_InitialResponse > 02_02_ImageMounting_Parsing > ArsenalImageMounter.exe**
  - You will need administrative privilege to execute it.

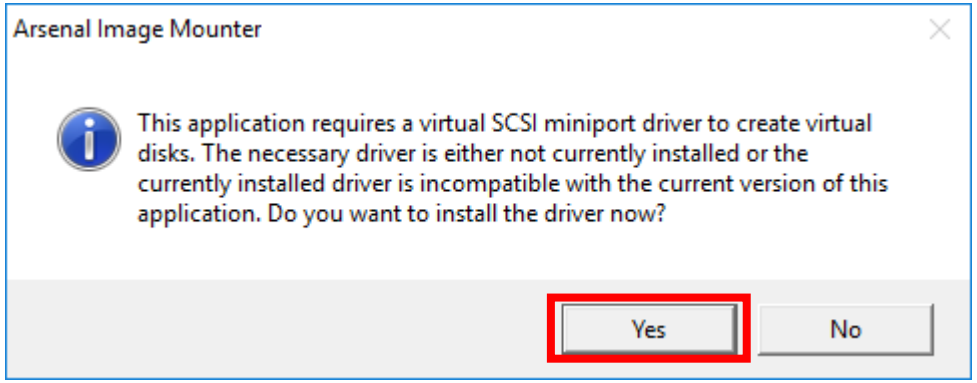
Splash Window

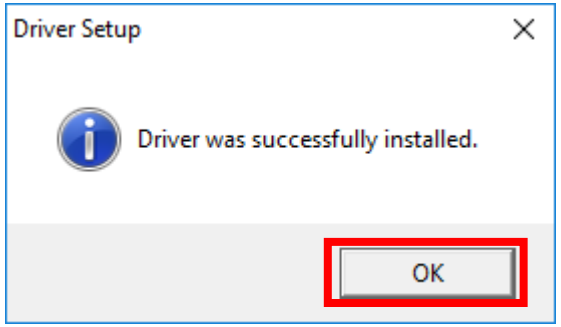
- Splash window will appear. Press “OK” to continue.



Installation of Device Drivers

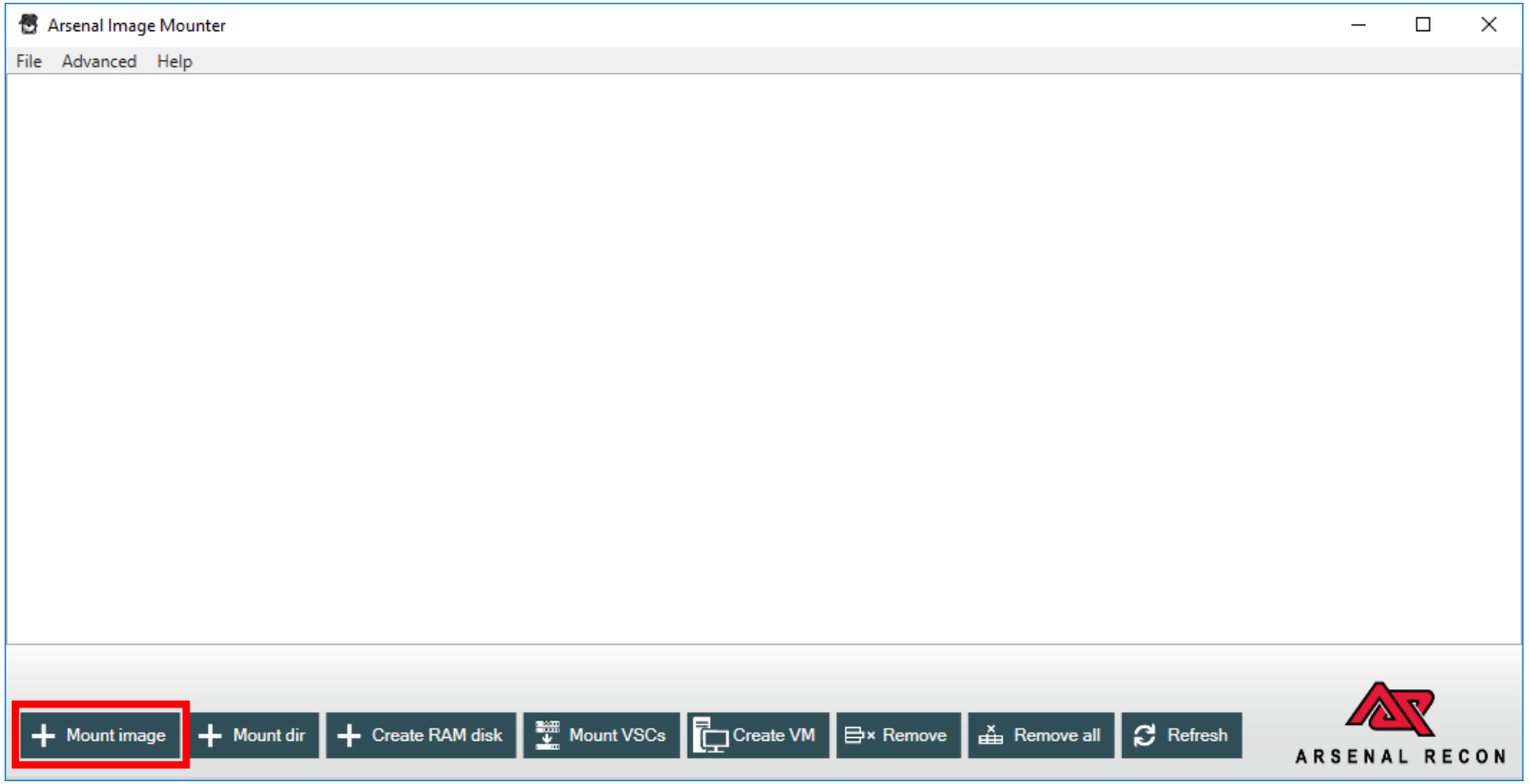
- When the Arsenal Image Mounter is executed for the first time, it will install device drivers.
  - This dialog will not appear once the driver is installed on the system.





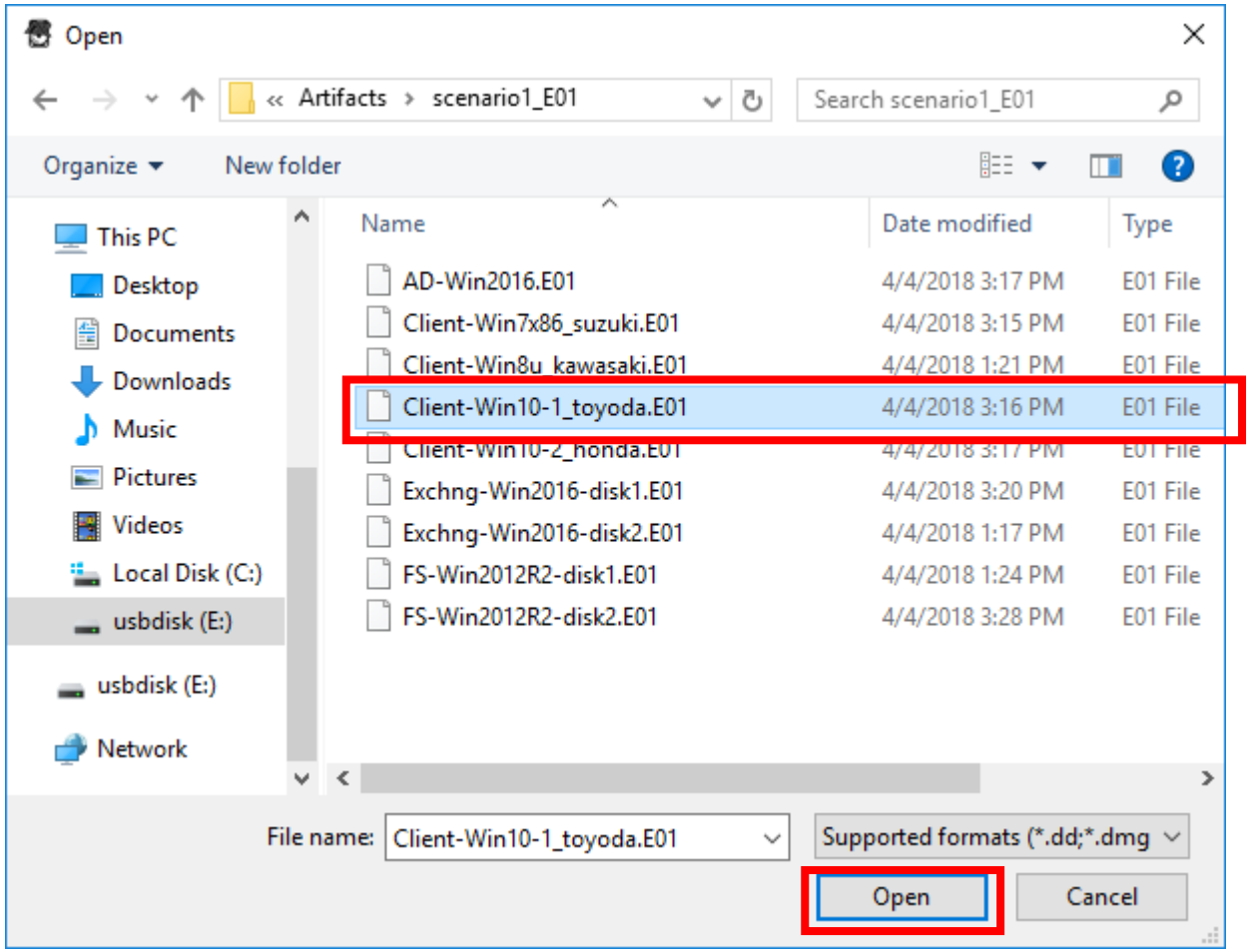
Mounting Image

- Once Arsenal Image Mounter is executed, press "Mount image" button.



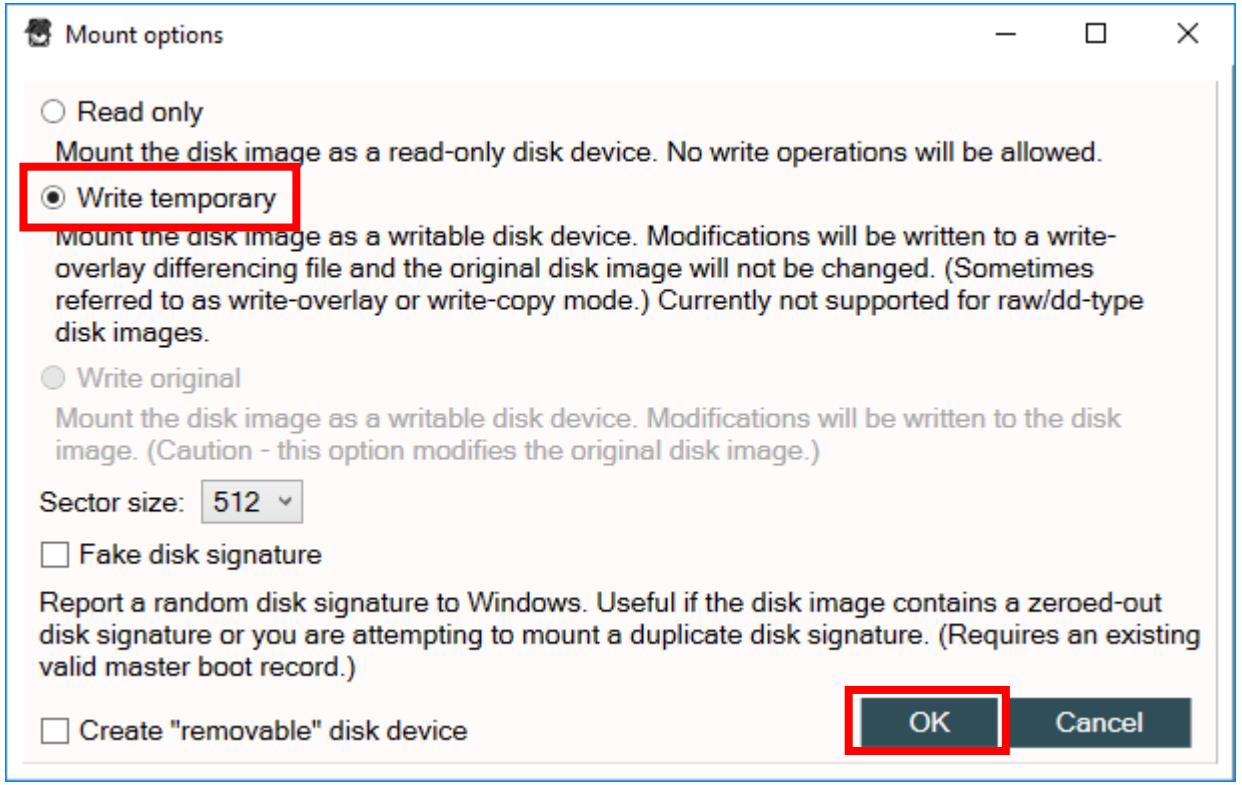
Selecting Disk Image

- Select a disk image file.
- Press “Open” when selected.



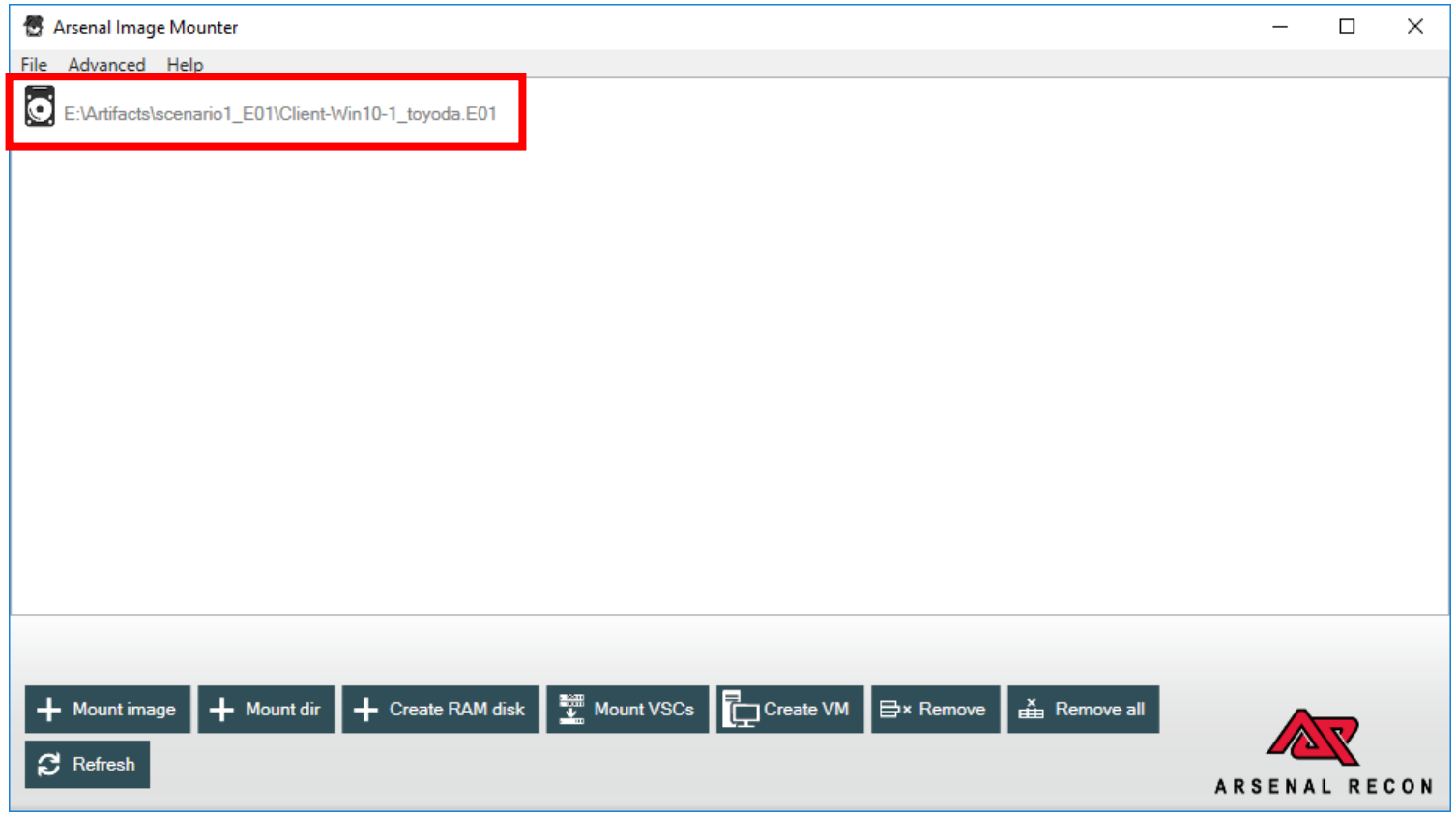
Mounting Options

- "Mount options" dialog will appear. Select "Write temporary" and press "OK" button.
  - When the option is selected, a differential file (.d01/.diff file) will be created in the same path of the E01 image file.
  - Once the .d01/.diff file is removed, the contents of the image will be reverted.



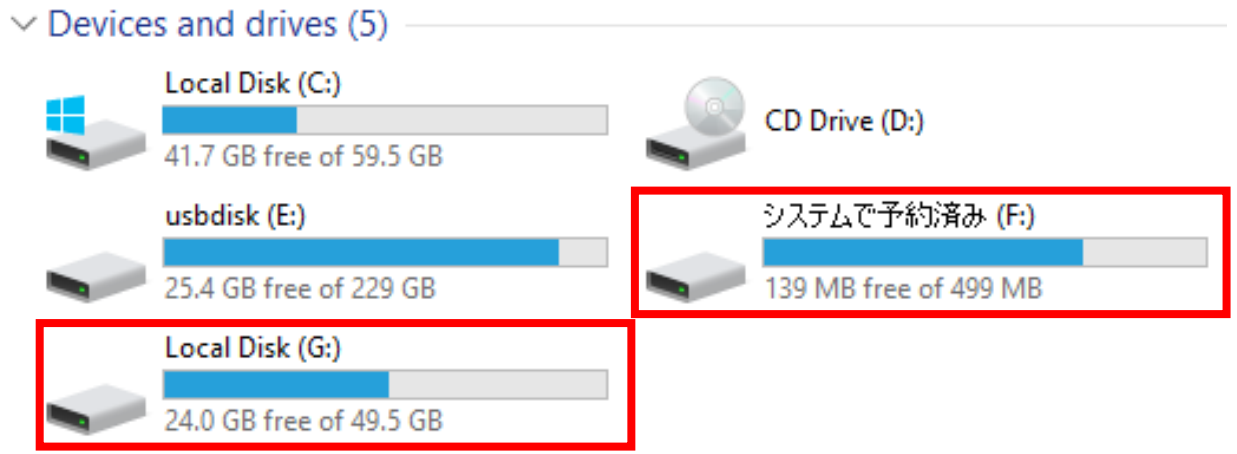
Mounted Image

- Once mounted, the image will appear in the image file list.



Accessing Image Files (This PC)

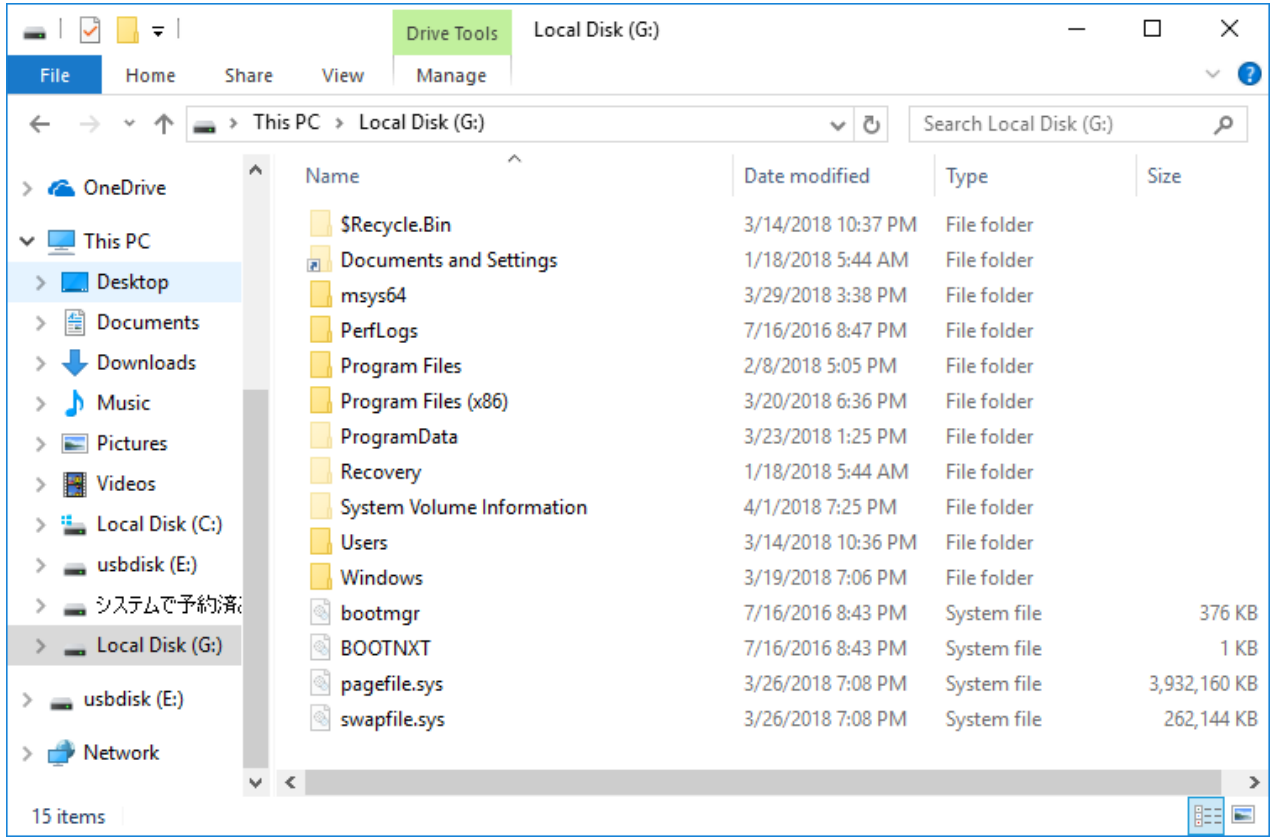
- Open Windows Explorer. You can see new two volumes, with drive letters "F:" and "G:“ assigned to them.



- The volume label of F is in Japanese, since the disk image was taken from Japanese language version of Windows 10. The name means “System Reserved”, and it contains system boot information.

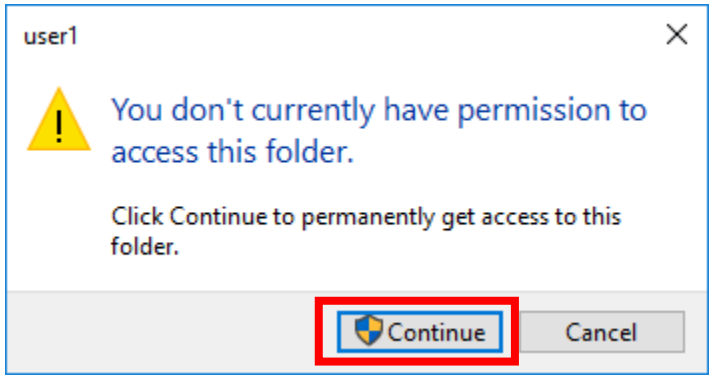
Accessing Image Files

- You can access the files in disk image via Explorer.



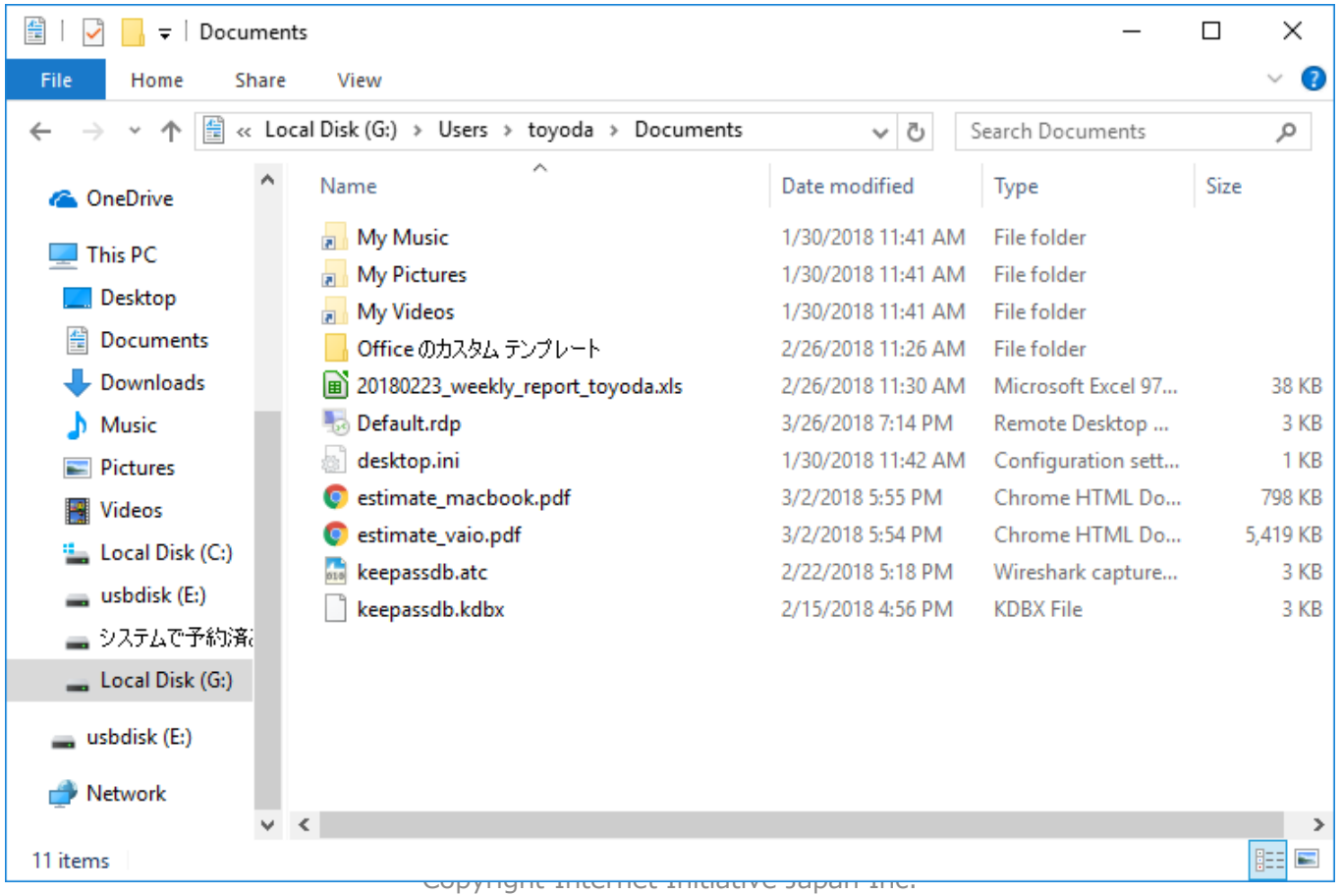
Access Permissions

- Access to "G:\Users\toyoda" folder. This will show you that you don't have a permission to access this folder.
- Press "Continue" button.
  - This will modify file access permissions of the folder.
  - Since user profile folder has many files in it, this process will take a while.



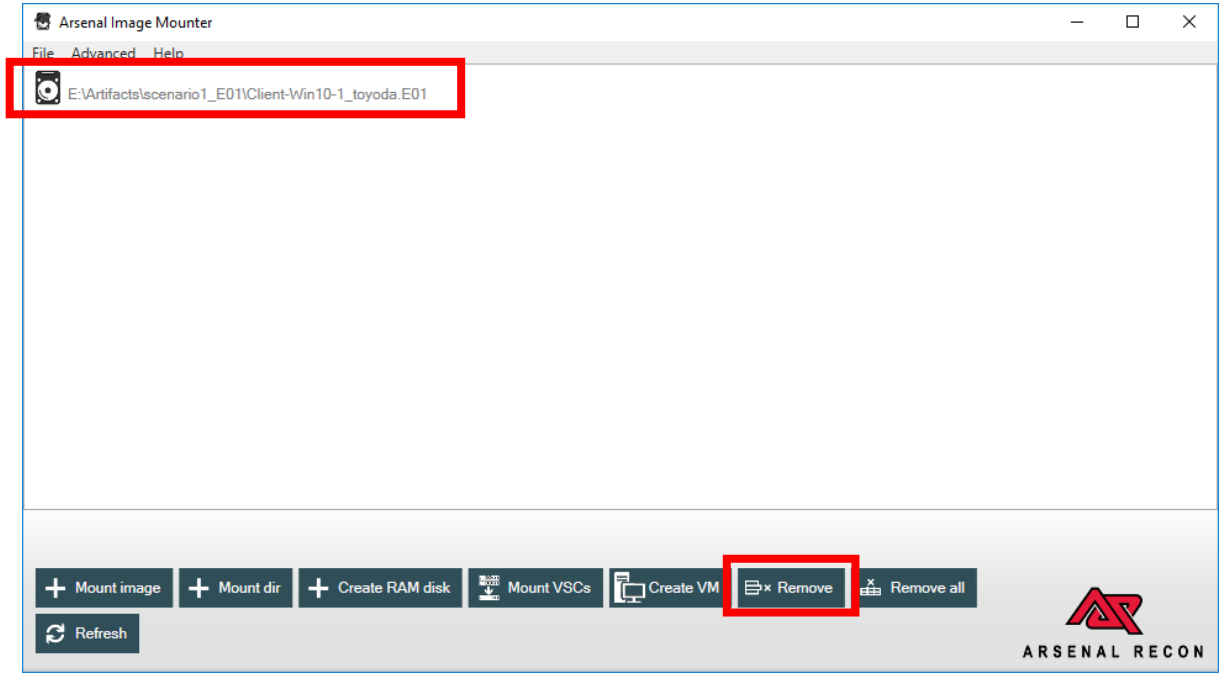
Navigating Through User Profile Folder

- Now, you can see toyoda's documents. You can also open files.



Unmounting Image

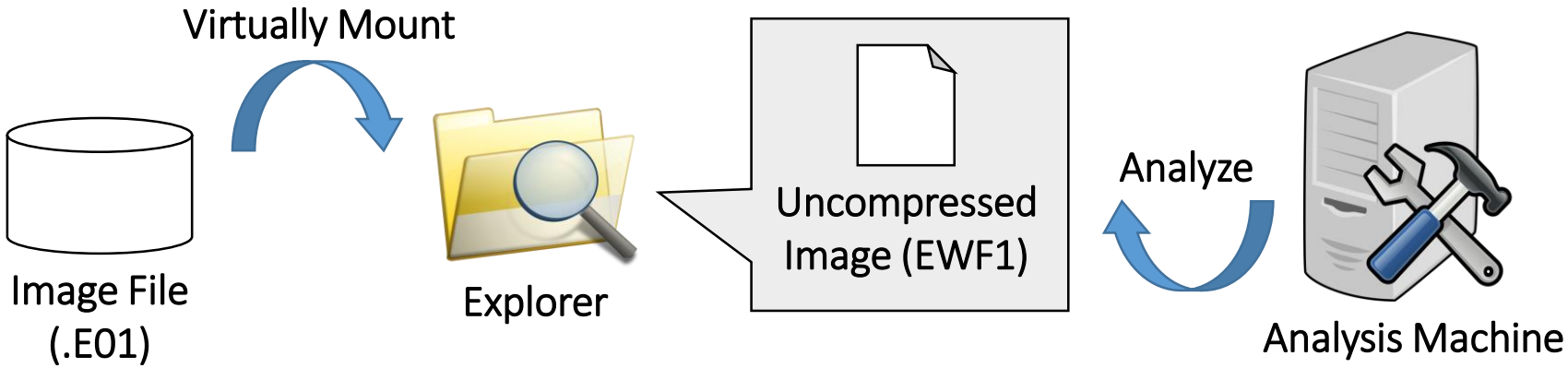
- To unmount the image, get back to the Arsenal Image Mounter, select the image, and press “Remove” button.



Exercise: Mounting Image File with ewfmount

Overview of ewfmount

- An image file in EWF format are compressed.
- ewfmount presents the image file as mounted to the explorer virtually.
  - The image file is not uncompressed.
  - ewfmount dynamically converts the necessary portion of the image.
- The “mounted” file can be analyzed using other mounting/parsing tools.



Virtually Mounting E01 Image

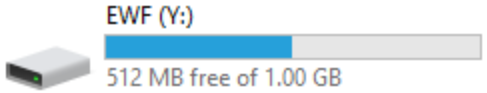
Execute "**ewfmount.exe**" as follows:
ewfmount.exe <E01_image> <drive_letter>

```
>ewfmount.exe E:\Artifacts\scenario1_E01\Client-Win10-1_toyoda.E01 Y:
```

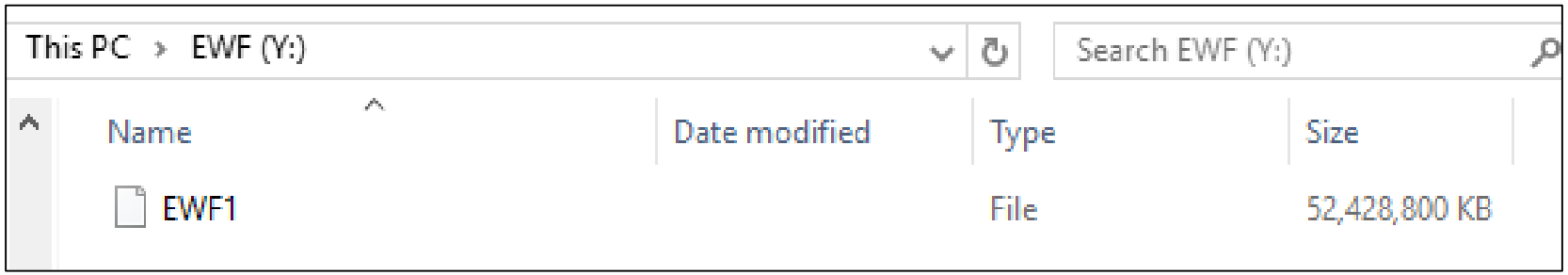
The command above virtually mounts “Client-Win10-1_toyoda.E01” to drive Y. Note that the drive letter that is not used by other disk drives must be specified.

Exploring Mounted Image

Open “PC” on Windows Explorer. You should be able to see "**EWF (Y:)**".

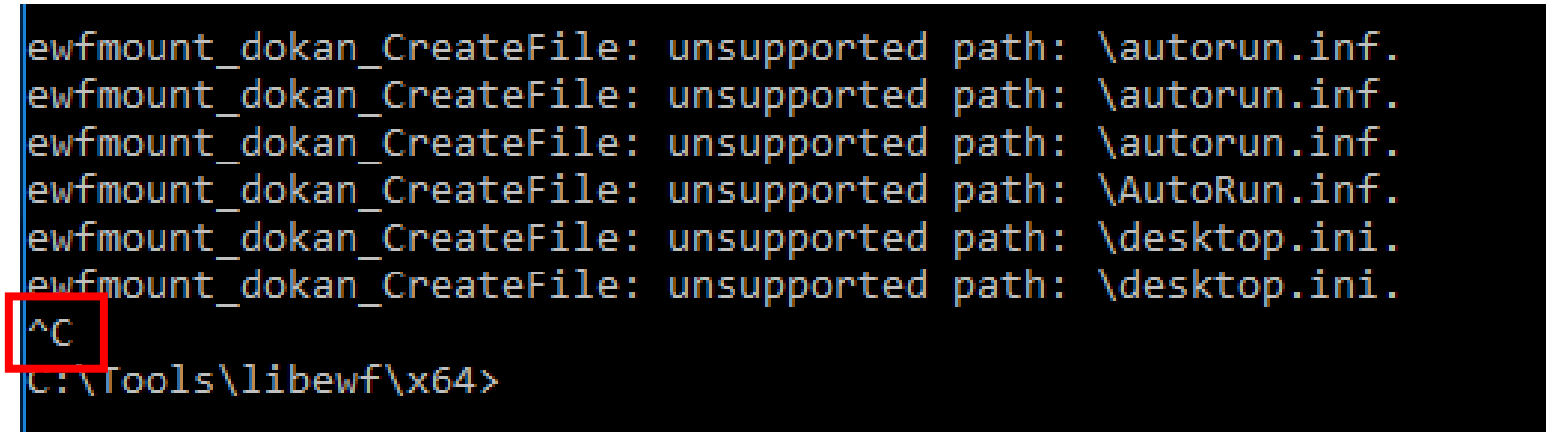


There is "**EWF1**" file on Y: drive. This is a decompressed E01 (a RAW format image). You can access data in EWF1 via forensic tools.



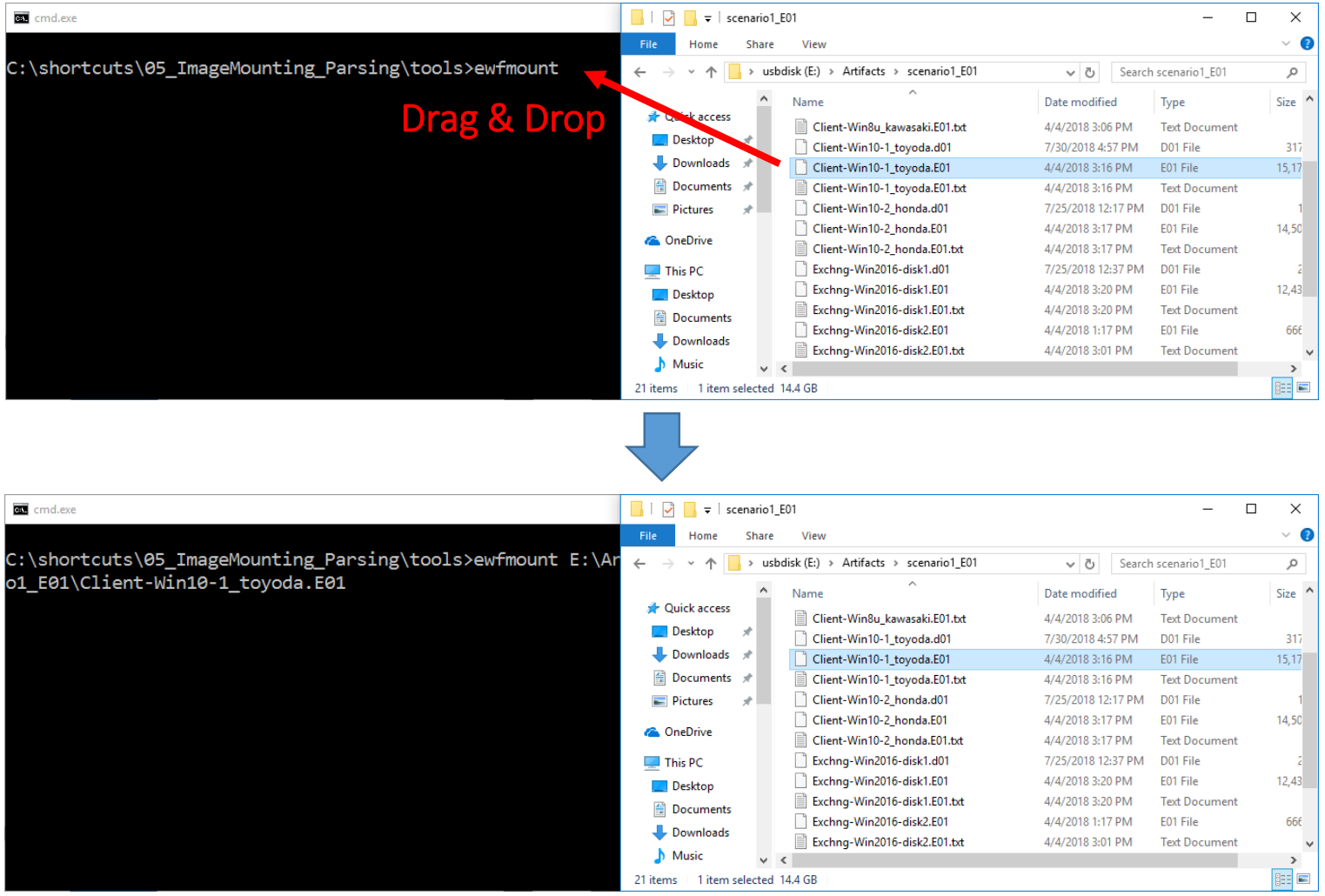
Unmounting

To terminate "ewfmount", just press "Ctrl + c" in the command prompt.
This will unmount the virtually mounted drive (Y:).



Tips: Entering Long Paths on Command Prompt

- To enter long paths (such as E:\Artifacts\scenario1_E01), you can drag and drop the file on Windows Explorer to the command line.



Exercise: Parsing Image File with The Sleuth Kit

The Sleuth Kit

- The Sleuth Kit is a set of command line tools for parsing disk images.
- Each tools has a simple feature such as showing a partition table, listing file entries, showing a file content, and so on.
- The Sleuth Kit supports file systems like below:
  - NTFS
  - FAT / exFAT
  - UFS
  - Ext
  - HFS
  - And so on

Showing a Partition Table

- mmls <disk_image_path>

```
>mmls E:\Artifacts\scenario1_E01\Client-Win10-1_toyoda.E01
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0001026047   0001024000   NTFS / exFAT (0x07)
003:  000:001   0001026048   0104855551   0103829504   NTFS / exFAT (0x07)
004:  -------   0104855552   0104857599   0000002048   Unallocated
```

You can check an offset sector (the smallest unit of data to write to disk) of each partition. You have to specify an offset when you use other TSK commands.

Drive C partition of Windows 10. Another one is a recovery partition.

Finding MFT Record Number of a Specific File

- ifind -o <partition_offset> -n <path_to_file|dir> <disk_image>

```
>ifind -o 1026048 -n /Users/toyoda/Documents E:\Artifacts\scenario1_E01\Client-Win10-1_toyoda.E01
96046
```

Unix style path (use "/", not "\")

- You can get a MFT record number of specified file.
- MFT record number is a number to identify a file or folder on Windows file system (NTFS).
- You need to specify a MFT record number to other TSK commands, if you need to extract a file or list a directory.
- We will refer to the NTFS structure later.

Showing File List

- fls -o <partition_offset> <disk_image> <mft_record_num>

```
>fls -o 1026048 E:\Artifacts\scenario1_E01\Client-Win10-1_toyoda.E01 96046
/r 95350-128-3:         20180223_weekly_report_toyoda.xls
r 99323-128-4:          Default.rdp
/r 96452-128-1:         desktop.ini
/r 103489-128-5:        estimate_macbook.pdf
r/r 163472-128-5:       estimate_vaio.pdf
r/r 112715-128-4:       keepassdb.atc
r/r 95288-128-4:        keepassdb.kdbx
d/d 96144-144-1:        My Music
96145-144-1:            My Pictures
/d 96146-144-1:         My Videos
/d 111868-144-1:        Office ????? ??????
```

You can get MFT record numbers under the specified MFT record number.

These numbers indicate attributes of the MFT entry.

MFT Entry Attributes

- Each MFT entry has attributes.
  - e.g. 128-1
- The first number is a type of the attribute.
  - Some attributes have different meanings depending on NTFS versions.
    - 1.2: Windows NT 4.0
    - 3.0: Windows 2000
  - The second number is the sequence number of attributes within the same attribute type.
    - If the entry has additional data, such as Alternate Data Stream (ADS), there will be multiple $DATA attributes within the same entry.

Type	Name
0x10 (16)	$STANDARD_INFORMATION
0x20 (32)	$ATTRIBUTE_LIST
0x30 (48)	$FILE_NAME
0x40 (64)	$VOLUME_VERSION (-NTFS v1.2) $OBJECT_ID (NTFS v3.0-)
0x50 (80)	$SECURITY_DESCRIPTOR
0x60 (96)	$VOLUME_NAME
0x70 (112)	$VOLUME_INFORMATION
0x80 (128)	$DATA
0x90 (144)	$INDEX_ROOT
0xA0 (160)	$INDEX_ALLOCATION
0xB0 (176)	$BITMAP
0xC0 (192)	$SYMBOLIC_LINK (-NTFS v1.2) $REPARSE_POINT (NTFS v3.0-)
0xD0 (208)	$EA_INFORMATION
0xE0 (224)	$EA
0xF0 (240)	$PROPERTY_SET (-NTFS v1.2)
0x100 (256)	$LOGGED_UTILITY_STREAM (NTFS v3.0-)

Reference:
Linux-NTFS Project, **“NTFS - Attributes”**
https://flatcap.org/linux-ntfs/ntfs/attributes/index.html

Display File Content

- icat -o <partition_offset> <disk_image> <mft_record_num>
  - The file content will be printed out to STDOUT.
  - The file content can be redirected to another file.

```
>icat -o 1026048 E:\Artifacts\scenario1_E01\Client-Win10-1_toyoda.E01 99323-128-4 > %USERPROFILE%\Desktop\Default.rdp
```

- The command above outputs file 99323-128-4 (C:\Users\toyoda\Documents\Default.rdp) to Desktop of the analysis machine.

Export an Unallocated Disk Space

- blkls -o <partition_offset> -A <disk_image> > <output_path>

```
>blkls -o 1026048 -A E:\Artifacts\scenario1_E01\Client-Win10-1_toyoda.E01 >
%USERPROFILE%\Desktop\unallocated.raw
```

  - -A : read data of unallocated area.
  - You have to use a redirect (">") to save a result of command; otherwise the results are printed to STDOUT.

  - You'll probably export unallocated data as a preparation for file carving.

Summary

Lesson Learned From Image Mounting and Parsing

- When you analyze disk images, you can use "Mounting" tools and "Parsing" tools.
- Difference between "Mounting" and "Parsing".
  - Mounting
    - Mount disk images as physical drives.
    - You can access files using Explorer and other applications.
  - Parsing
    - Parsing tools directly analyze file system.
    - You can access special files such as meta files, protected files by system, deleted files, and unallocated area data.

Tools (1)

- Disk Imaging Tool
  - Guymager
    - http://guymager.sourceforge.net/
- Memory Imaging Tool
  - WinPmem
    - https://github.com/google/rekall/releases
  - Comae DumpIt
    - https://www.comae.io/
  - Belkasoft Live RAM Capturer
    - https://belkasoft.com/bat
  - Magnet RAM Capture
    - https://www.magnetforensics.com/free-tool-magnet-ram-capture/
- Triaged Acquisition (Fast Forensic) Tool
  - CDIR Collector
    - https://github.com/CyberDefenseInstitute/CDIR

Tools (2)

- Disk Image Mounter
  - Arsenal Image Mounter
    - https://arsenalrecon.com/Downloads/
  - OSFMount
    - https://www.osforensics.com/tools/mount-disk-images.html
- Disk Image Parser
  - Autopsy & The Sleuth Kit
    - https://www.sleuthkit.org/
- Disk Imaging Tool / Disk Image Mounter / Parser
  - FTK Imager / FTK Imager Lite
    - https://accessdata.com/product-download