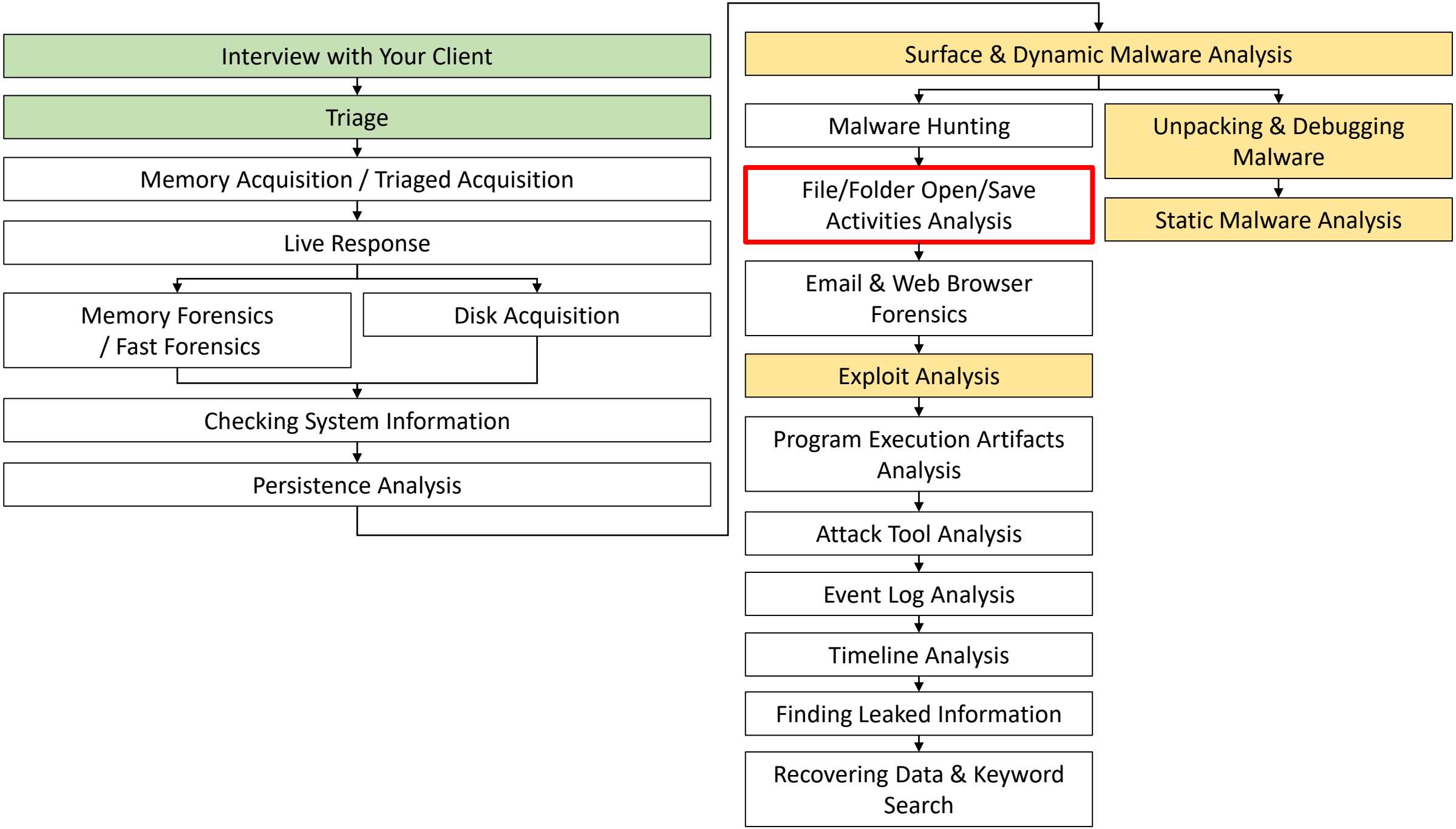
Investigating File/Folder Open/Save Activities


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

Investigating File/Folder Open/Save Activities

- When a user, regardless of whether it is legitimate or not, opens or saves a file, or creates a folder, there will be some artifacts that are recorded on the computer.
  - There are multiple artifacts for a single activity, and not all of them are human-readable.
- If an attacker tried to steal files from the infected computer, and looked around for a right file, those files could be identified from analyzing the file/folder open/save activities.
- If a legitimate user opened a file and the file caused the infection, that could be identified from analyzing the file/folder open/save activities. **This happens a lot in targeted attacks**.

The Major Root Causes (1/2)

- In order to discover the root causes of the infection, we need to check several sources.
  - E-mails
  - Web (social engineering and drive by download including watering whole attack)
  - Messengers (Skype, WhatsApp) and SNS Apps (Twitter, Facebook, …)
  - Removable disks including USB thumb drive

The Major Root Causes (2/2)

- When e-mails are used for attacks, attachments and links that look legitimate to the user is often used.
  - Technically a type of social engineering.
- When the attachments were, or links pointed to, document files, generally users open them by themselves.
  - If the file was a executables, we will do program execution artifacts forensics, which we will discuss in a later chapter.
- By examining file open/save activities, it is possible to determine which file caused the infections.

Topics Covered in This Section

- Registry Basics
  - Since many of the activities are saved in the registry, we will cover this first.
- Shellbags
- Recent docs
- Office Recent docs
- Adobe Acrobat Recent docs
- JumpLists
- LastVisitedMRU
- OpenSaveMRU

MRU

- “MRU” stands for “Most Recently Used”.
- “MRU List” is the list of the files/paths/locations/etc... that was used recently.

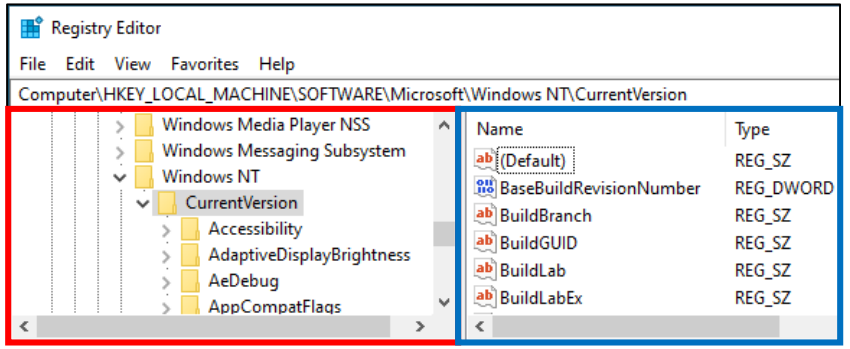
Registry Basics

Registry Basics

- Registry stores settings of Windows and other applications installed on the computer.
  - The registry “keys” and “values” are organized in tree format.
- Before registry was introduced, all settings were stored in text (.ini) files.

Keys and Values

- “Keys” are the group of registry values.
  - They are represented as a “folder” on Registry Editor.
- “Values” are individual settings.
  - They are represented as item entries on Registry Editor.
  - Each value has name, type and data. If we were to treat them as a file, consider the name as filename and the data as the file contents.
    - There are different types of values, which will be discussed in the next page.
- Keys may have child keys and values while values cannot have any kind of children.



Value Types

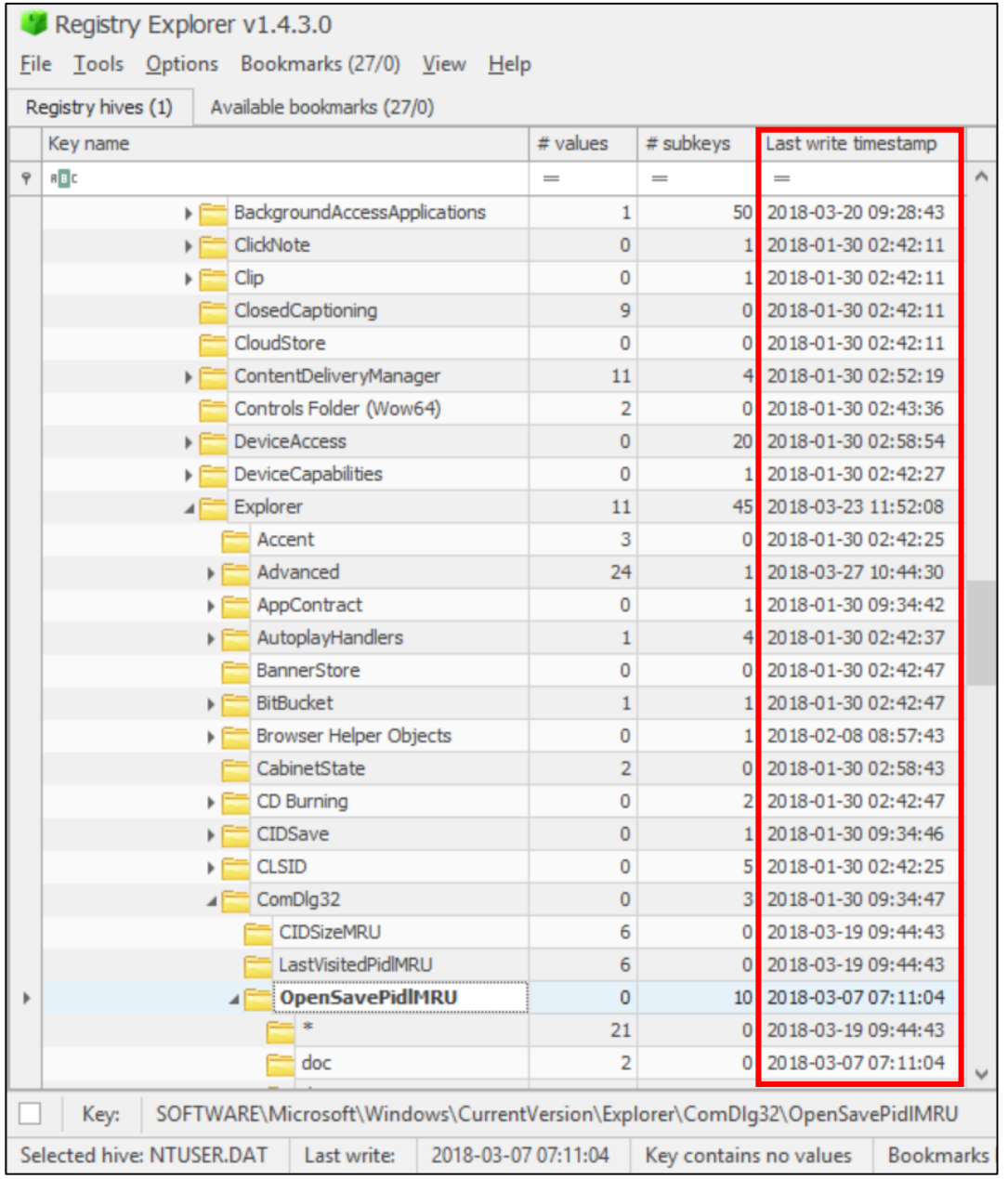
- There are six major value types on x86 Windows:

Name	Type in Registry Editor	Description
String	REG_SZ	Single-line strings
Binary	REG_BINARY	Binary data
DWORD (32-bit)	REG_DWORD	32-bit number
QWORD (64-bit)	REG_QWORD	64-bit number
Multi-String	REG_MULTI_SZ	Sequence of multiple strings
Expandable String	REG_EXPAND_SZ	String with unexpanded environment values (such as %USERPROFILE%)

- There are also some other value types specified in the development libraries, but they are designed to be used on Windows with non-x86 architectures.

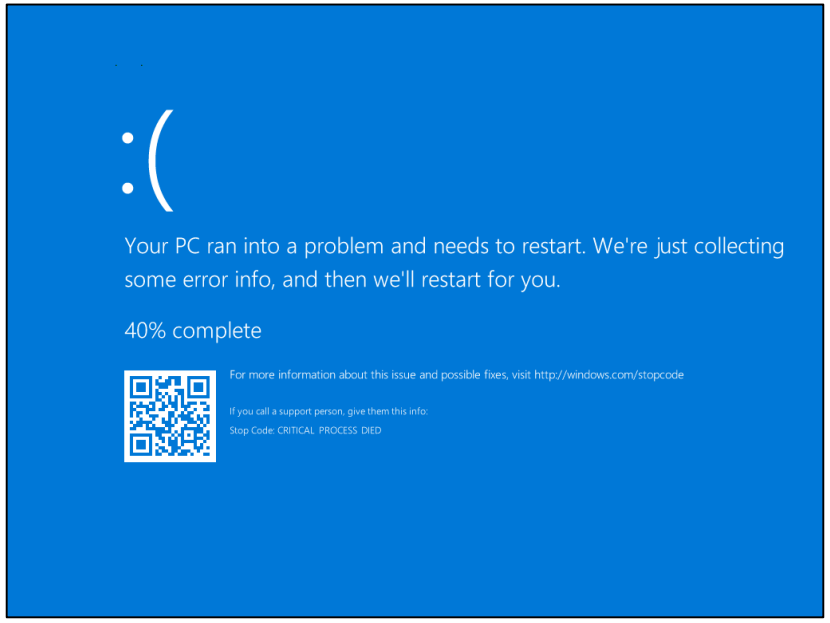
Registry Key Timestamps

- Registry keys have timestamps for the last write time.
- The timestamps do not appear on the Registry Editor. To view the timestamps, use other software that support showing them.



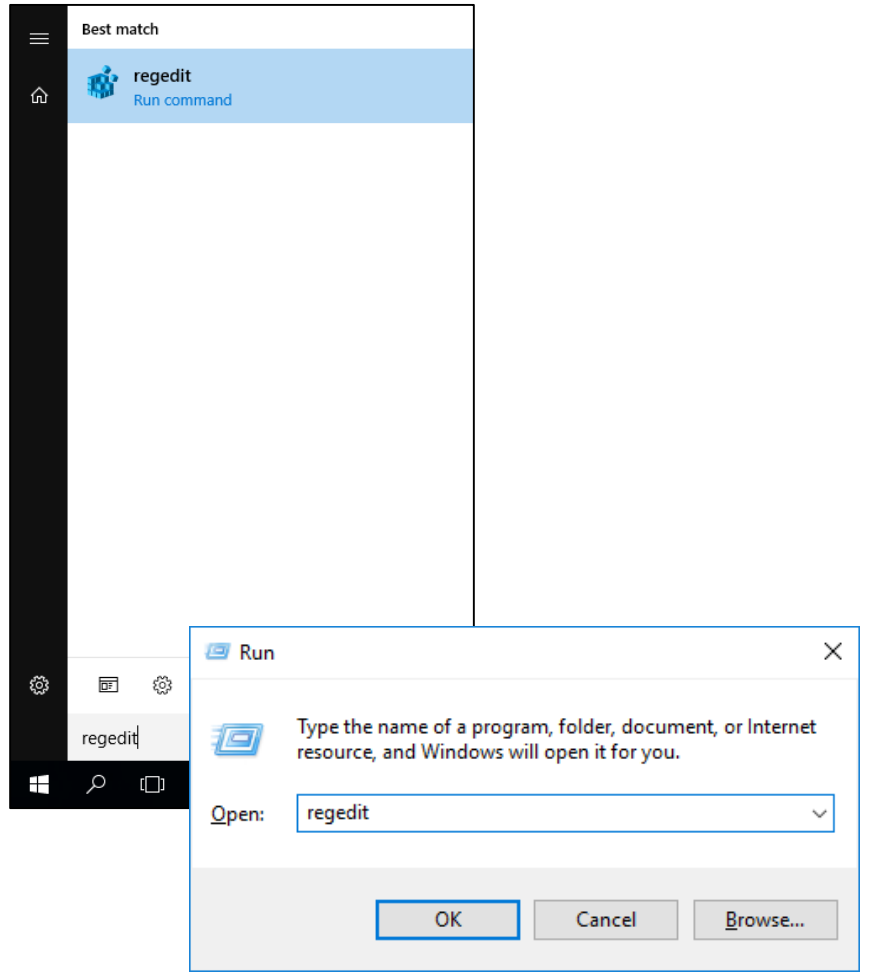
Important Things to Know About the Registry

- Registry stores Windows system settings.
- If you modify (delete or change keys and values) the registry inappropriately, the Windows may not start up again.



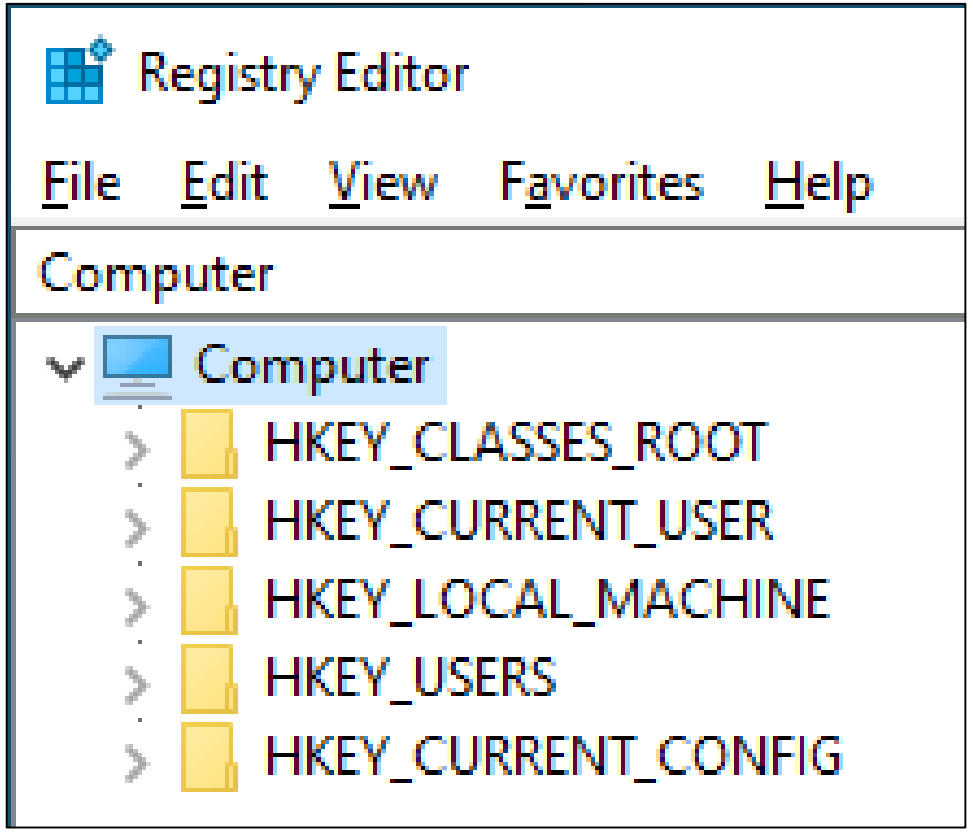
Registry Editor

- Registry Editor is a tool that is included in Windows for viewing and editing registries.
- Since it is a system tool, there are no links displayed in the Start Menu.
  - You need the administrative privilege to use it.
- To open the Registry Editor, in the Start Menu:
  - Search “regedit”, or
  - Open “Run” from “Windows System” group (or press Windows+r on the keyboard), and execute “regedit”.



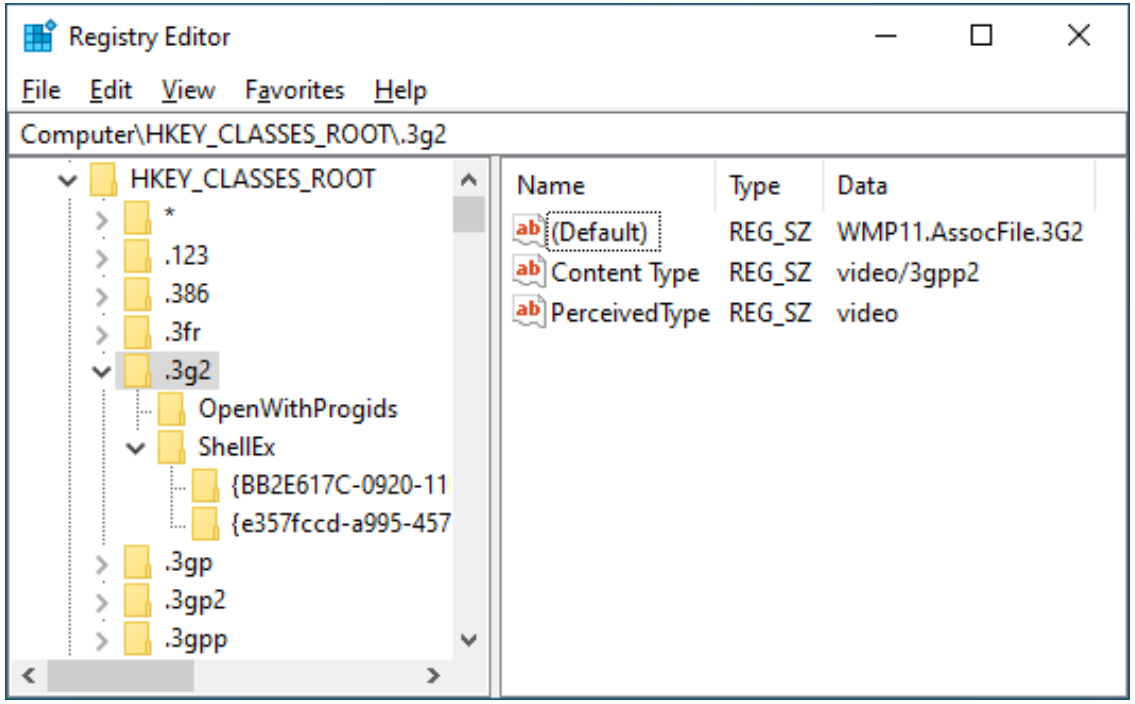
Top-Level Registry Keys

- There are five different top-level registry keys:



HKEY_CLASSES_ROOT

- It stores definitions of protocol and file types.
  - When a file was double-clicked or right-clicked on the Windows Explorer, it will run the action defined in this key.
- It is composed of system-wide classes and per-user classes.
  - “SOFTWARE\Classes” under HKEY_LOCAL_MACHINE (system) and HKEY_CURRENT_USER (per-user).
  - If the same classes are defined for both system and user, one in the user hive will be used.

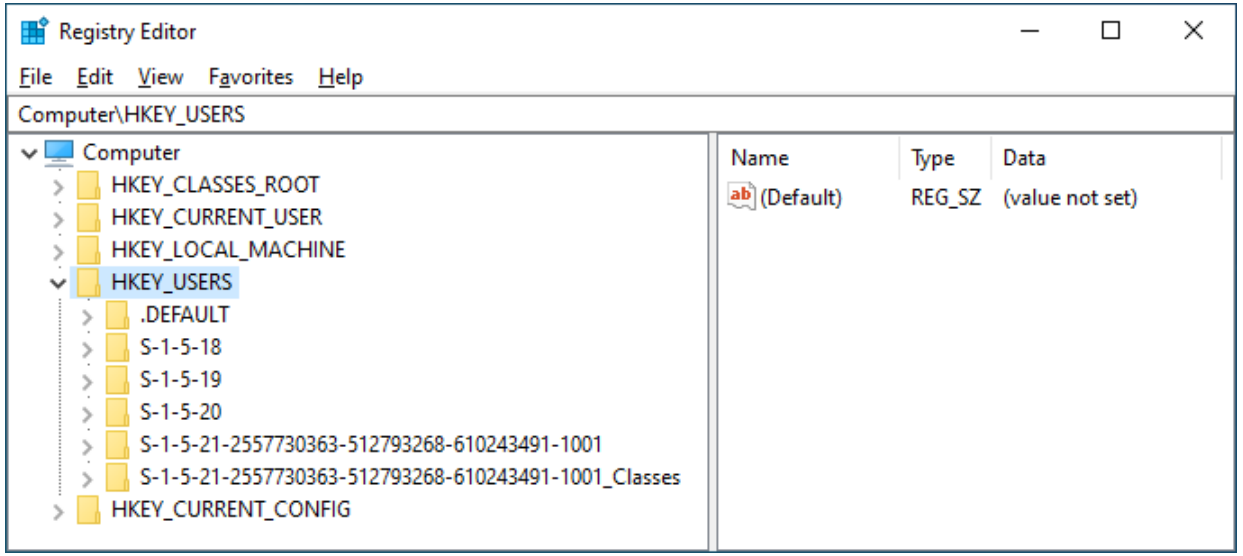


HKEY_LOCAL_MACHINE (HKLM)

- Stores system-wide settings of Windows and applications.
  - Values are applied to all users using the system.
- Three important keys:
  - SOFTWARE: settings of Windows and applications
  - SYSTEM: settings of services
  - SAM: local user and group information

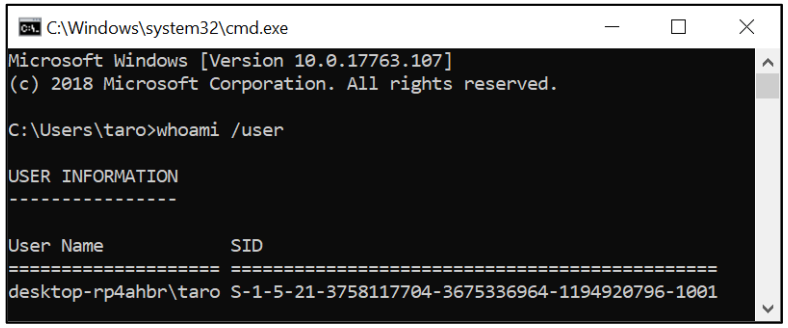
HKEY_USERS

- Stores per-user settings of Windows and applications.
  - Values are applied to each user only.
- Keys with users' SIDs are listed under the HKEY_USERS key.



Security Identifiers (SIDs)

- SIDs are IDs that indicate security principals/groups in Windows.
- SID for the current user may be obtained through “whoami /user” command on the Windows Command Prompt.
- There are some well-known SIDs.



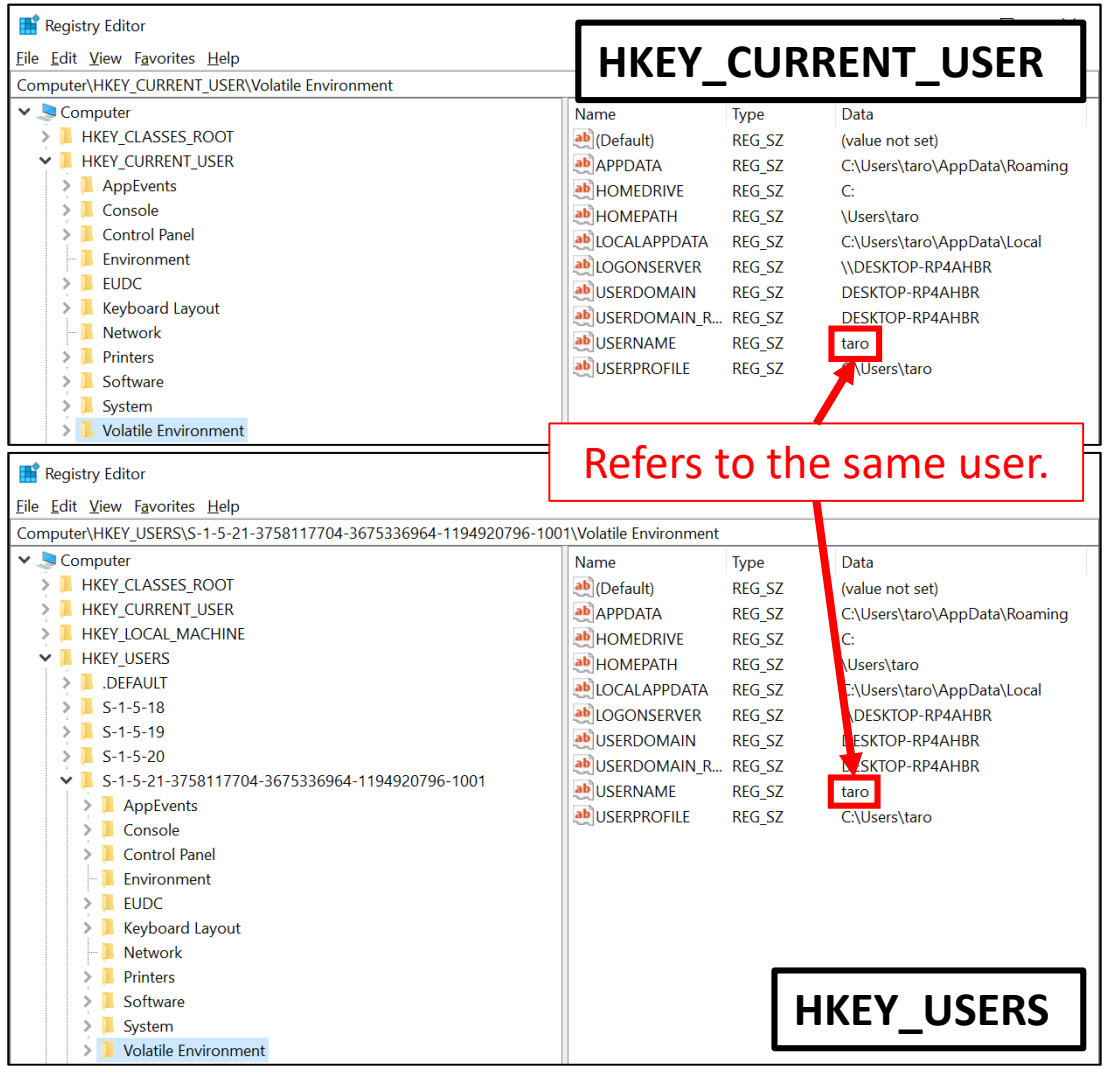
SID	Name	SID	Name
S-1-1	World Authority (e.g. S-1-1-0 as Everyone)	S-1-5-21-*domain*-500	Administrator
S-1-2	Local Authority (e.g. S-1-2-1 as Console Logon)	S-1-5-21-*domain*-512	Domain Admins
S-1-3	Creator Authority (e.g. S-1-3-0 as Creator Owner)	S-1-5-21-*domain*-515	Domain Computers
S-1-5	NT Authority	S-1-5-32-544	Administrators

Value of *domain* differs for each domain, and will be the same among all objects within the same domain.

Reference:
Microsoft, **“Well-known security identifiers in Windows operating systems”**
https://support.microsoft.com/en-us/help/243330/well-known-security-identifiers-in-windows-operating-systems

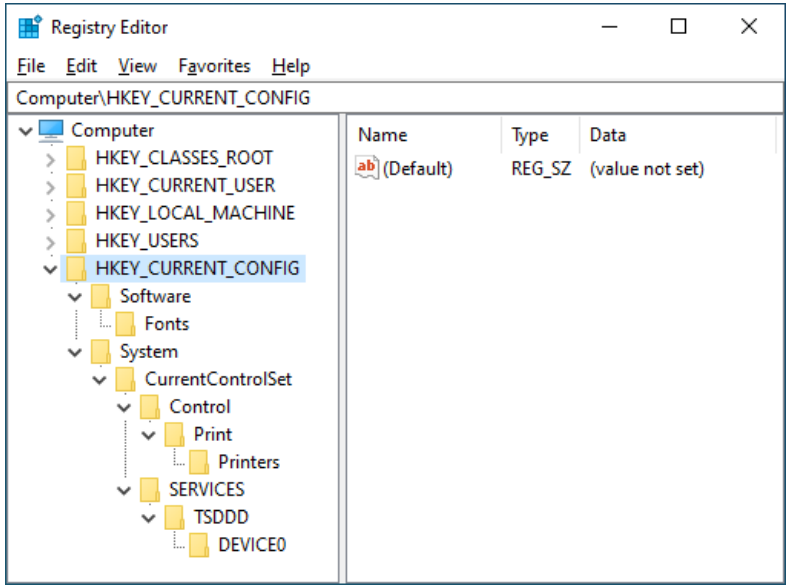
HKEY_CURRENT_USER (HKCU)

- Links to the current user's "HKEY_USERS" registry key.
  - When programs modify the registry keys and values, it normally uses HKEY_CURRENT_USER key to specify values, not "HKEY_USERS".
- When analyzing the registry offline, since there is no "current user", this key will not be available.



HKEY_CURRENT_CONFIG

- Stores settings regarding the hardware devices.
  - Not so many keys/values: only the differences from the standard hardware profile are stored in the registry.
- Links to "**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current**" registry key.



ControlSet Registry Key

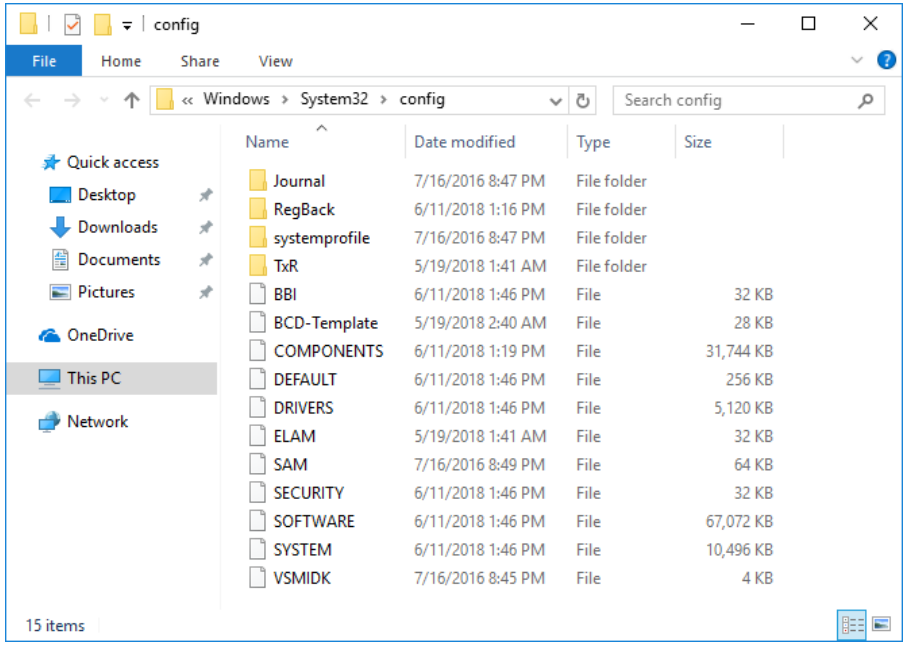
- ControlSet registry keys, found under "**SYSTEM**" key in "HKEY_LOCAL_MACHINE" and "HKEY_USERS", contains settings regarding services.
- There are registry keys such as: "**CurrentControlSet**", "**ControlSet001**", "**ControlSet002**", and so on.
  - The maximum value of "ControlSet*???*" depends on number of times the system settings were changed.
- "CurrentControlSet" is the settings that is currently running, which is an alias to "ControlSet001".
  - When analyzing an offline system, this key will not be available, like HKCU.
- "ControlSet*???*" are the settings that were used in previous Windows instances.
  - Used for restoring settings when Windows failed to start.
  - These "ControlSet*???*" might help when digging through the history of settings.

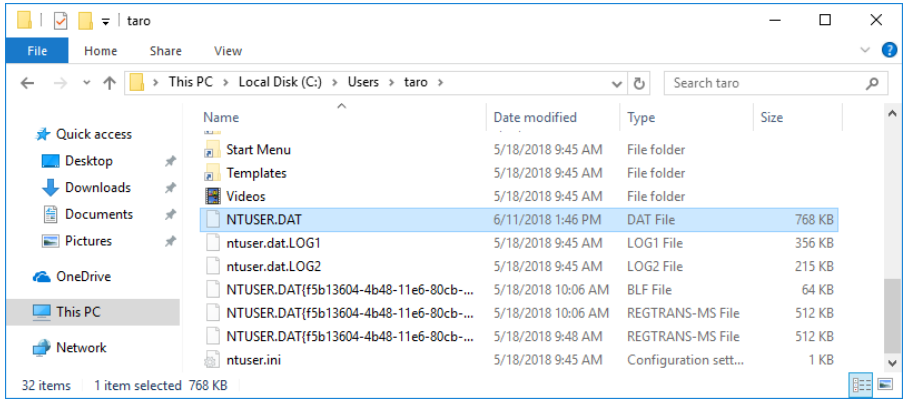
Registry Keys That Are Not Visible Through Registry Editor

- Some registry keys are not visible through Registry Editor.
  - SAM: database of Security Account Manager.
    - It includes information about users and groups in the local computer.
    - Password hashes are also included in it.
  - Amcache.hve: application compatibility database. The tree is not presented on the Registry Editor.
    - We will discuss more about this in program execution analysis chapter.
- Sometimes analysis of these keys may be necessary.
  - They can be opened by copying the registry files from an offline system, and opening them by an appropriate tool.

Registry Files

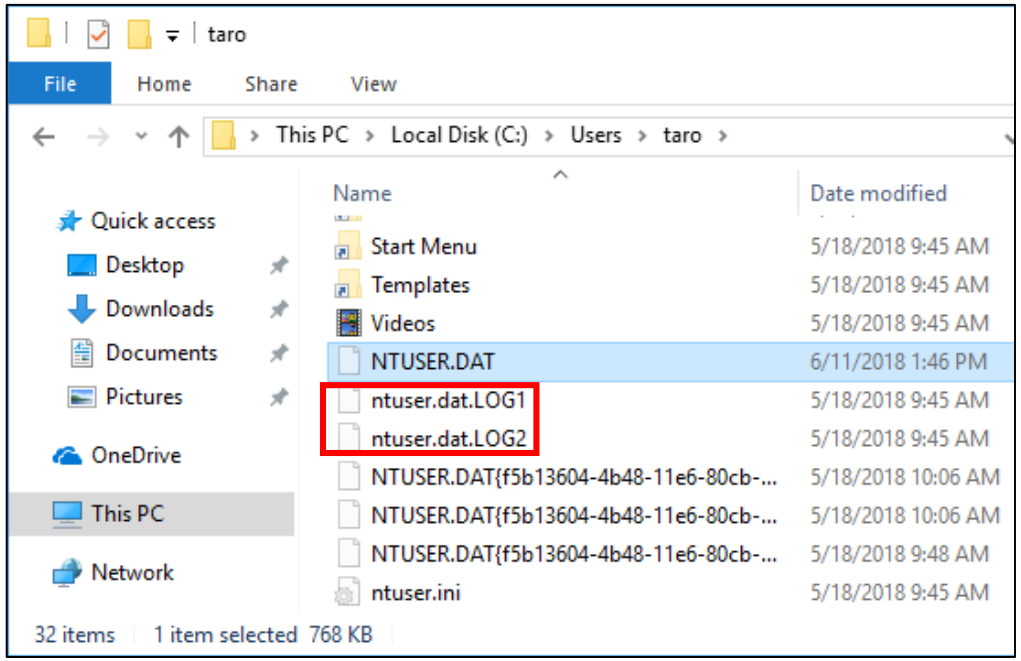
- Registry files are stored in the following locations.
  - System-wide registries: files in **C:\Windows\System32\config**
  - Per-user registry (HKCU): **%USERPROFILE%\ntuser.dat**
  - Per-user class registry (HKCU\Software\Classes): **%LocalAppData%\Microsoft\Windows\UsrClass.dat**
  - Amcache.hve: **C:\Windows\appcompat\Programs\Amcache.hve**
    - We will discuss this later in Program Execution artifacts.
- The unit of registry data is called a **hive**.





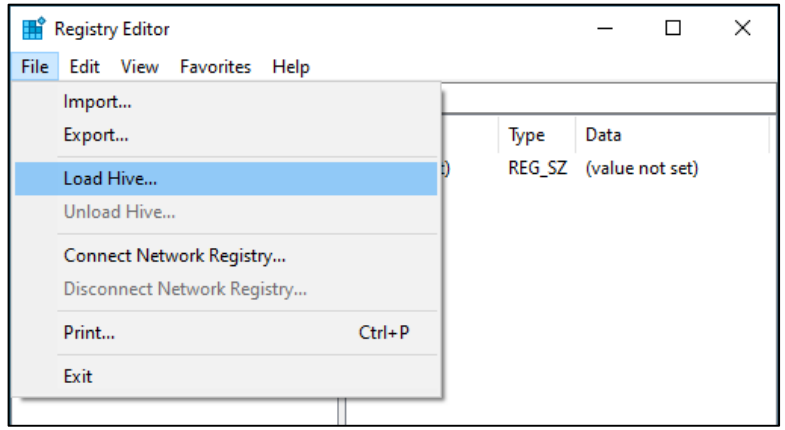
Temporary Registry Files

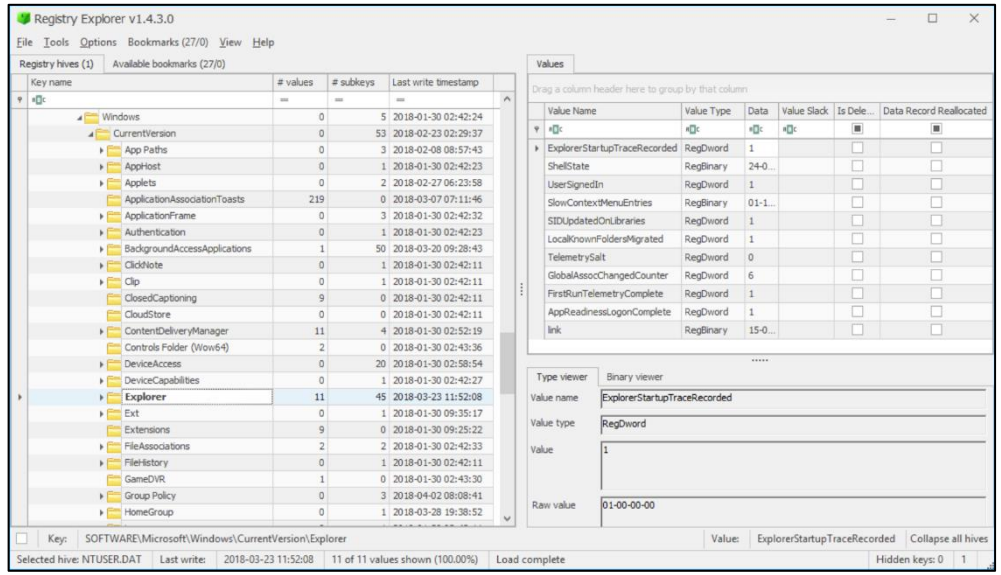
- If you look into one of the locations of registry files, you will find files that have ".LOG" in their extensions.
  - Example: ntuser.dat.LOG1
- When registry values are changed, the changes will be recorded to these LOG files first. Then, the records will be applied to each hive file.
  - Therefore, if the computer was powered off suddenly after the registry was modified, and the hive was taken to analysis without rebooting the system, those modifications may not be applied to the original hive files.



Opening Registry Files

- Registry files could be viewed using Registry Editor.
  - “Load Hive” command under the “File” menu.
  - You will have to make sure that you won’t unload wrong hives when done with the investigation.
- There are some tools that help viewing the registry files.
  - For example, Registry Explorer by Eric Zimmerman
  - https://ericzimmerman.github.io/





Tools for Looking into Registry Files

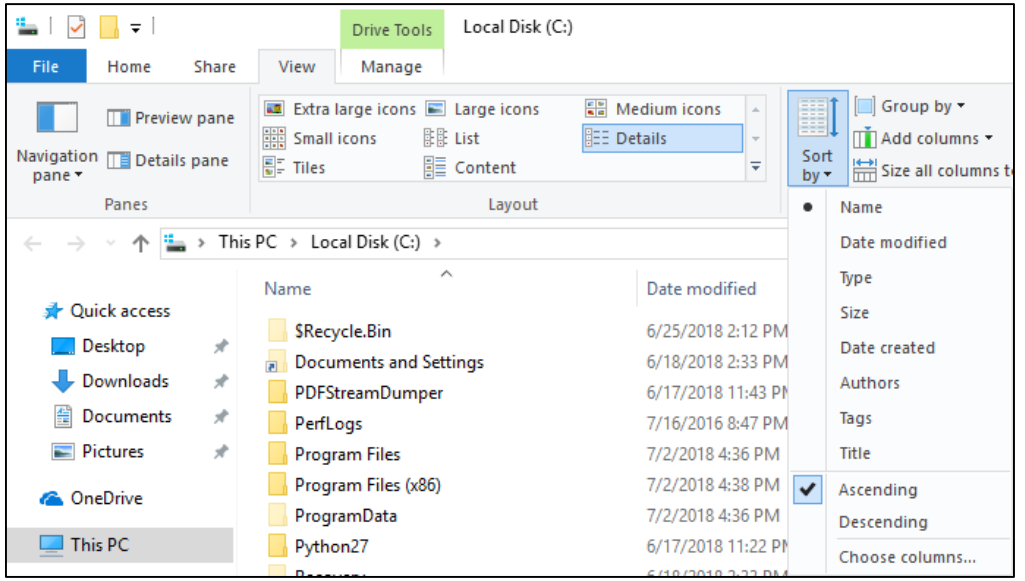
- Registry Explorer
  - Explorer-like tool to navigate the registry in trees, like the Registry Editor.
  - Includes bookmarks to some of the major registry keys.
  - Sometimes it can show deleted or missing registry keys/values.
- RegRipper
  - Parses registry contents and outputs the content to a text file.
  - Uses plugin to parse the registry contents.
- yarp (yet another registry parser)
  - Parses registry contents and outputs the content to a text file.
  - Includes tools to carve and recover the deleted or missing registry keys/values.

- These tools present some of the major registry keys in user-friendly format, rather than showing raw values.
  - For example, showing the registry contents in well-formatted tables.
- Registry Explorer and yarp can open LOG files, in addition to the hive files.

Shellbags

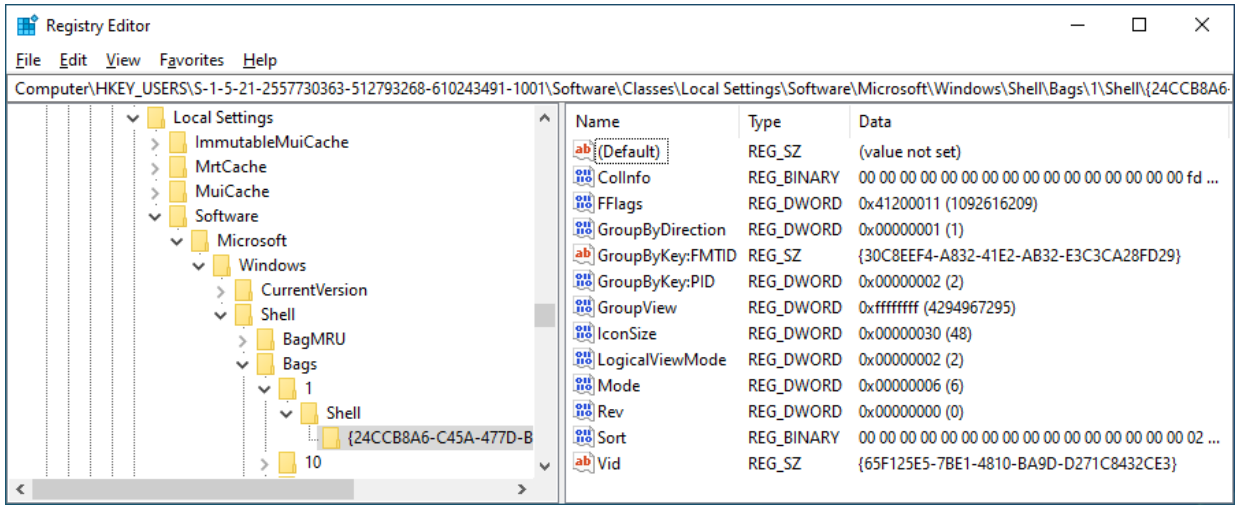
ShellBags

- Remembers how files and folders are shown when a folder was opened on the Explorer.
  - For example, icon sizes and sort orders.
  - It is stored in registry.
- Since it deals with how objects are displayed on Explorer, ShellBags will not appear when files/folders were accessed without Explorer.
  - e.g. Command Prompt



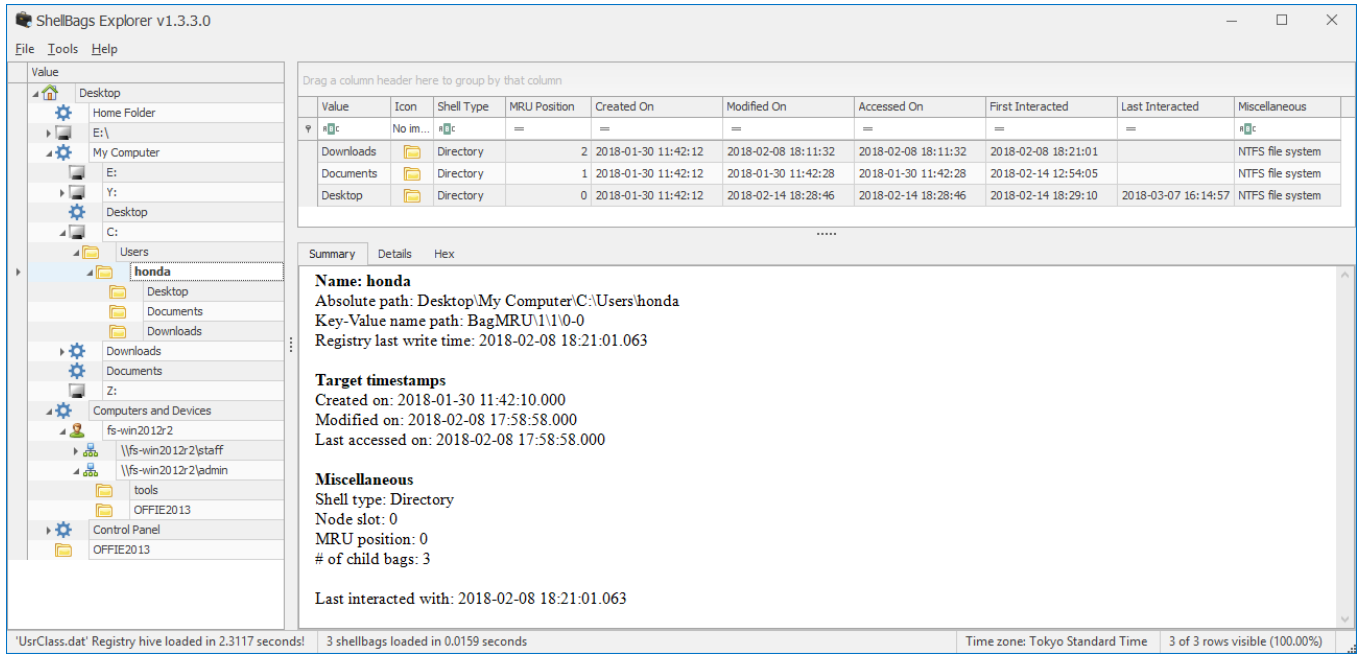
Why Parse ShellBags?

- ShellBags show the timestamps (created, modified and accessed).
- If folders were created during the attack, new ShellBags entries are created in the registry.
  - **HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\{Bags, BagMRU}**



Parsing ShellBags

- Registry entries for ShellBags are not human friendly.
- Example tool to parse them: ShellBags Explorer by Eric Zimmerman
  - Shows ShellBags entries from the currently logged on host or from a registry file.
  - https://ericzimmerman.github.io/



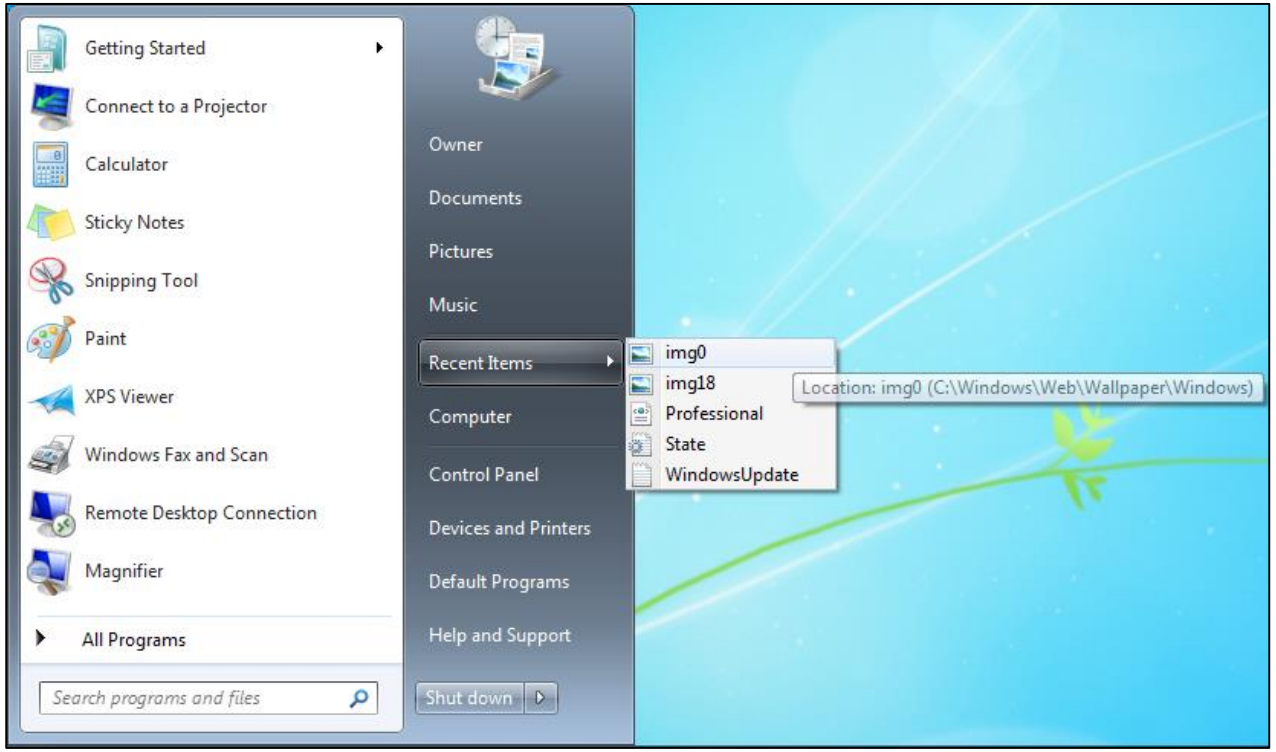
Some Notes about ShellBags

- Generally, ShellBags data are in UsrClass.dat hive.
  - %LocalAppData%\Microsoft\Windows\UsrClass.dat
- You could also find some of the ShellBags data in NTUSER.DAT hive.
  - In the scenario artifacts, you can find some histories of network share accesses.
- ShellBags data could be written if some sort of “accesses” were made to the object.
  - e.g. Viewing object properties
    - The file does not have to be opened in some cases.

Recent Documents

Recent Documents

- When a file was created or opened, it is recorded in “Recent Documents”.
- There are multiple types of the Recent Documents:
  - Files opened from Explorer
  - Files selected from File Selection Dialogs



Location of Recent Documents

- The list of Recent Documents can be found in two locations.
- In the Registry: **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs**
  - It is in binary format, and it is not human readable.
- On the file system: **%AppData%\Microsoft\Windows\Recent**
  - %AppData% is an environmental variable for “\Users\<username>\AppData\Roaming”.
  - Shortcuts (LNKs) to each file is stored in the path above.

Scenario 1 Labs:
Lab 1: Observation of Recent Documents for Client-Win10-2

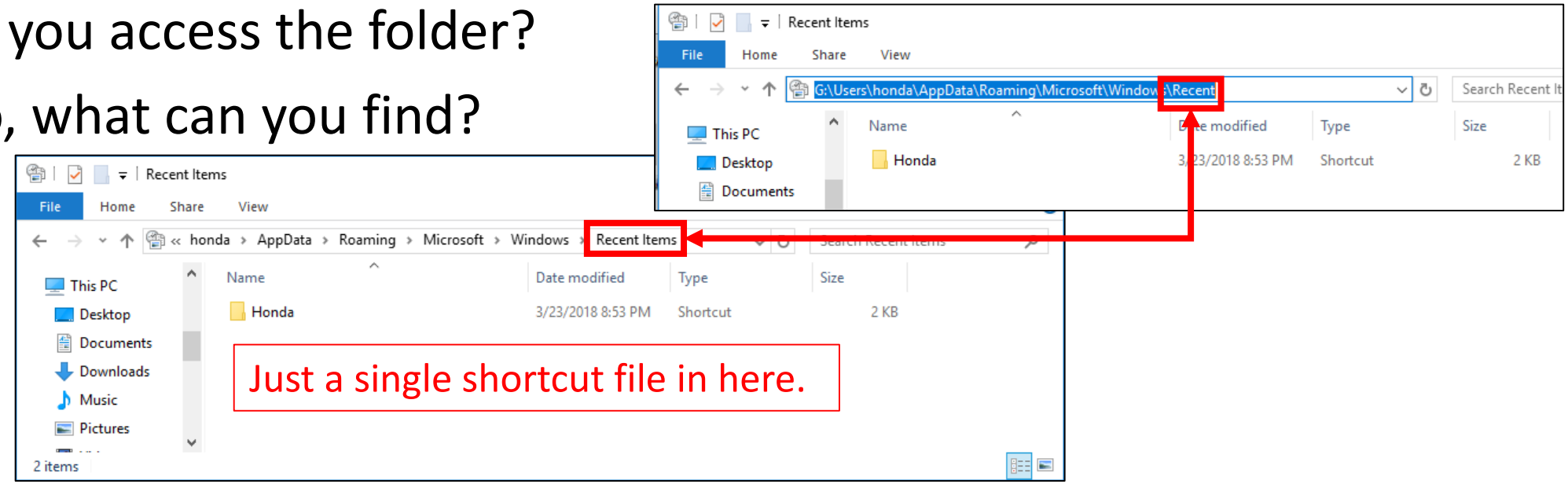
Part 1: Locating Recent Documents Shortcuts Using Windows Explorer (1/2)

- On Windows Explorer, navigate to: **G:\Users\honda\AppData\Roaming\Microsoft\Windows\Recent**

- Can you access the folder?
- If so, what can you find?

Part 1: Locating Recent Documents Shortcuts Using Windows Explorer (2/2)

- On Windows Explorer, navigate to: **G:\Users\honda\AppData\Roaming\Microsoft\Windows\Recent**
  - This is a special folder, and the location bar of the Windows Explorer will say "Recent Items" when you open it.
- Can you access the folder?
- If so, what can you find?



Part 2: Locating Recent Documents Shortcuts Using Command Prompt (1/4)

- Open Command Prompt from “tools” folder.
- Type the following command to change working directory.

```
cd /d G:\Users\honda\AppData\Roaming\Microsoft\Windows\Recent
```

- Use “**dir**” command to list contents of the folder.
  - Anything different from navigating through the Windows Explorer?

```
02/09/2018  12:24 PM             1,085 fs-win2012r2.lnk
02/08/2018  06:21 PM               565 gyoumu10.lnk
03/12/2018  03:09 PM               562 hodaka-motors (2).lnk
02/23/2018  06:56 PM             1,562 hodaka-motors.lnk
03/23/2018  08:53 PM             1,501 honda.lnk
02/08/2018  06:00 PM               172 http--jtomf4gp4jj1zevu.com-.lnk
03/07/2018  04:15 PM               541 invoice-KT20180307-2.xlsx.lnk
```

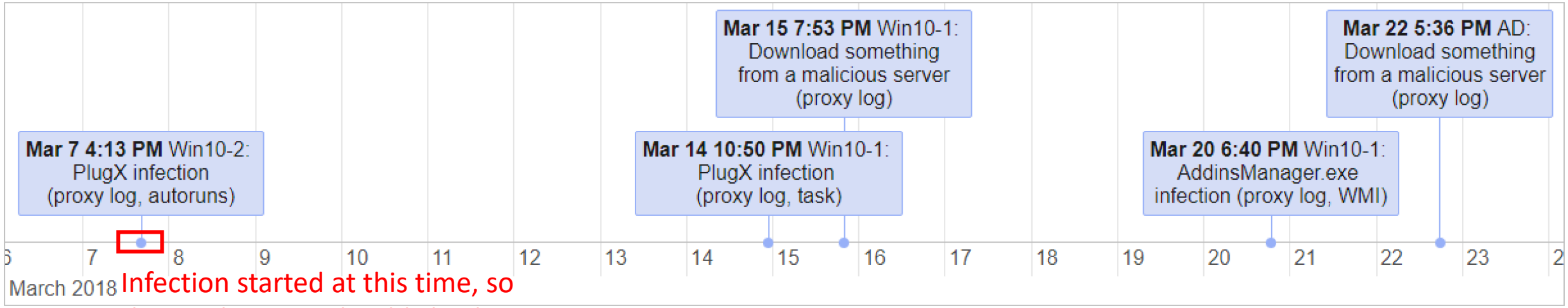
Most of these “.lnk” files were not visible on Windows Explorer.

Part 2: Locating Recent Documents Shortcuts Using Command Prompt (2/4)

- There were a lot of “.lnk” files, which are shortcuts to the recently used items.
  - We need to narrow them down.

- Since we know the date of infection, we will try to narrow it down by timestamps of those “.lnk” files.

Part 2: Locating Recent Documents Shortcuts Using Command Prompt (3/4)

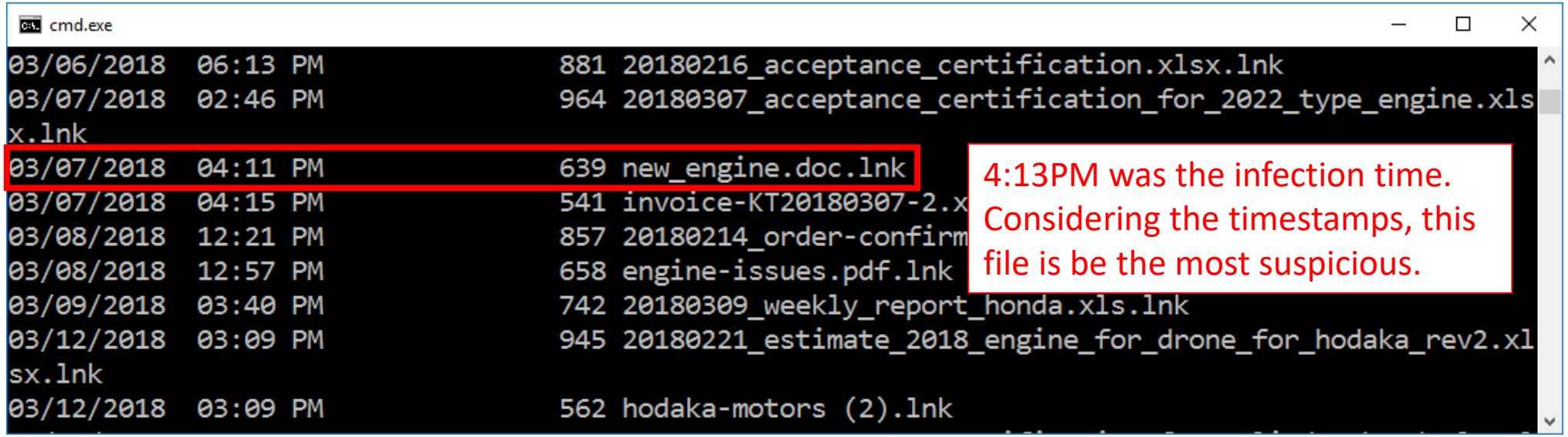


Infection started at this time, so this is where we should check.

Part 2: Locating Recent Documents Shortcuts Using Command Prompt (4/4)

- Type the following command.
  - This prints out list of files ordered by file creation timestamps.

```
dir /OD /TC
```

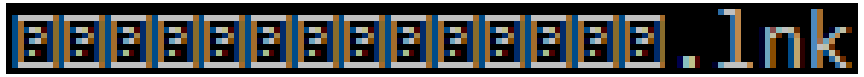


Part 3: Parsing Recent LNK Shortcuts (1/3)

- There here are tools for parsing LNK files.
  - We will be using a tool “**LECmd**” here.
- Try the following command.

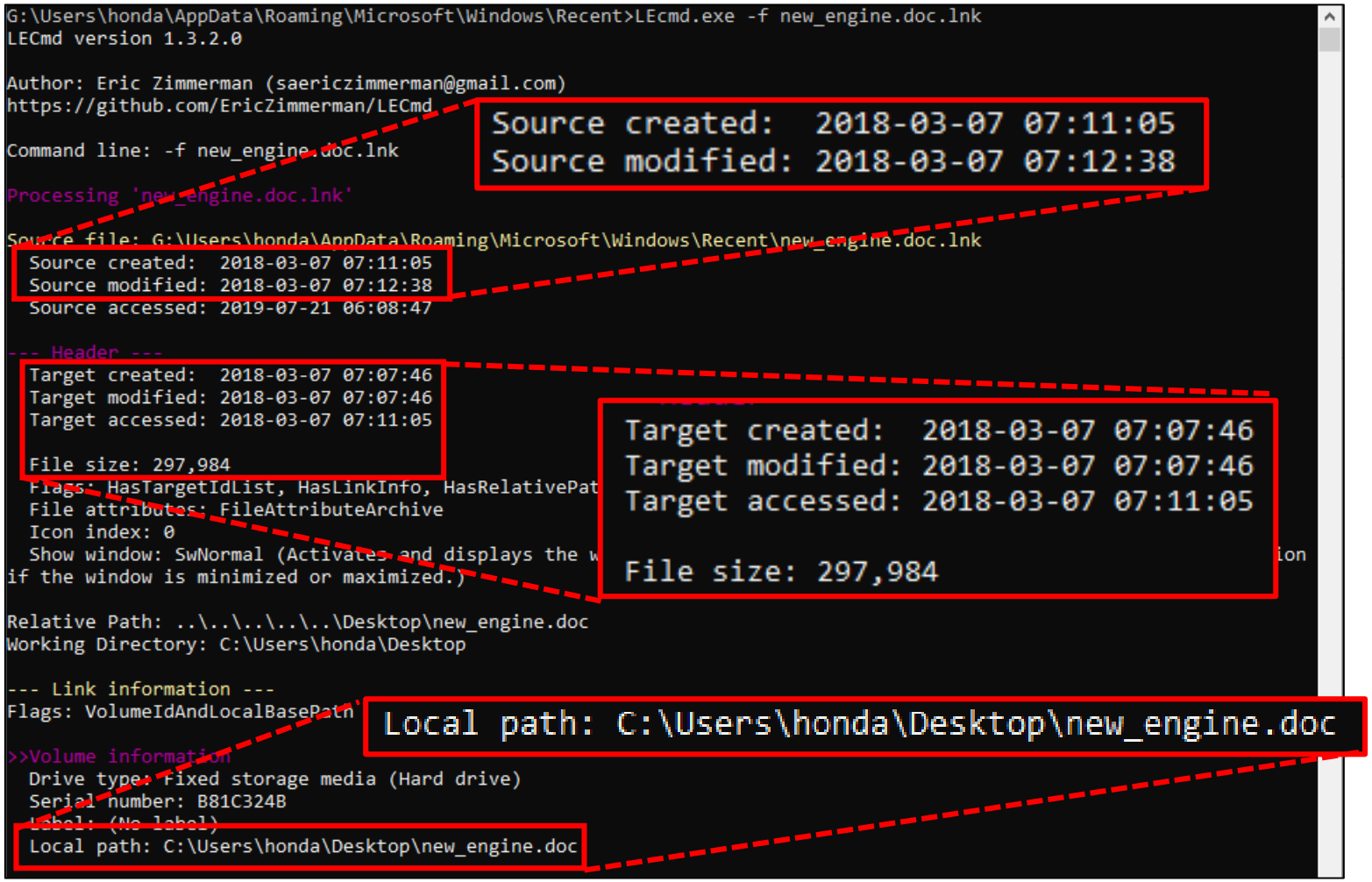
```
LECmd.exe -f new_engine.doc.lnk
```

- *Unfortunately, some files have Japanese names.*
  If you can’t read the file names, nothing is wrong in here.
  - *If you set fonts, these file names will be visible, but these files have nothing to do with the scenario.*



Part 3: Parsing Recent LNK Shortcuts (2/3)

- If you look into the output, you can find the timestamps and the location of the actual file.
  - The output implies that the user has opened a file from the Desktop.



Part 3: Parsing Recent LNK Shortcuts (3/3)

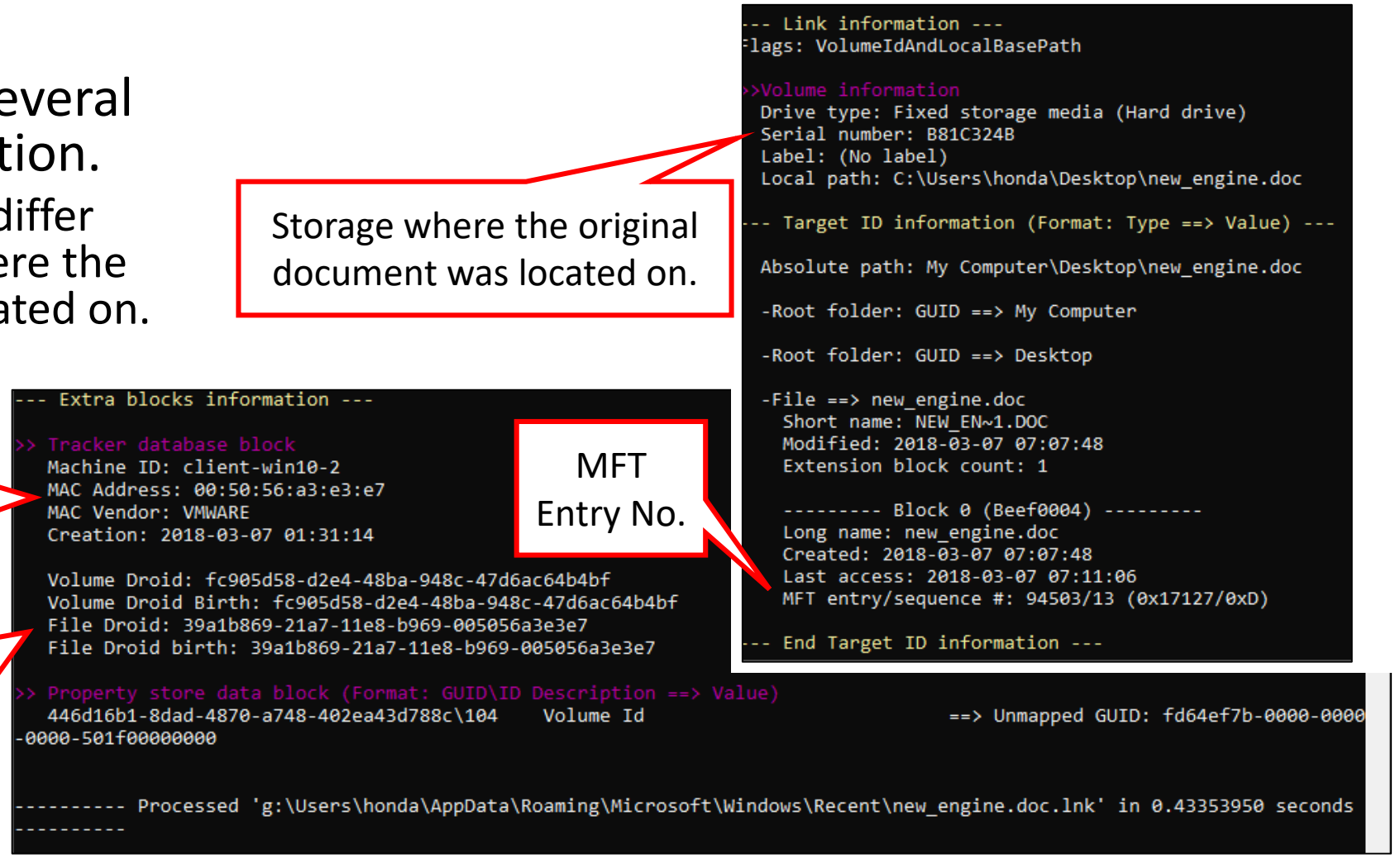
- LEcmd prints out several additional information.
  - The contents will differ depending on where the target file was located on.

Storage where the original document was located on.

Hostname & MAC address of the original machine.

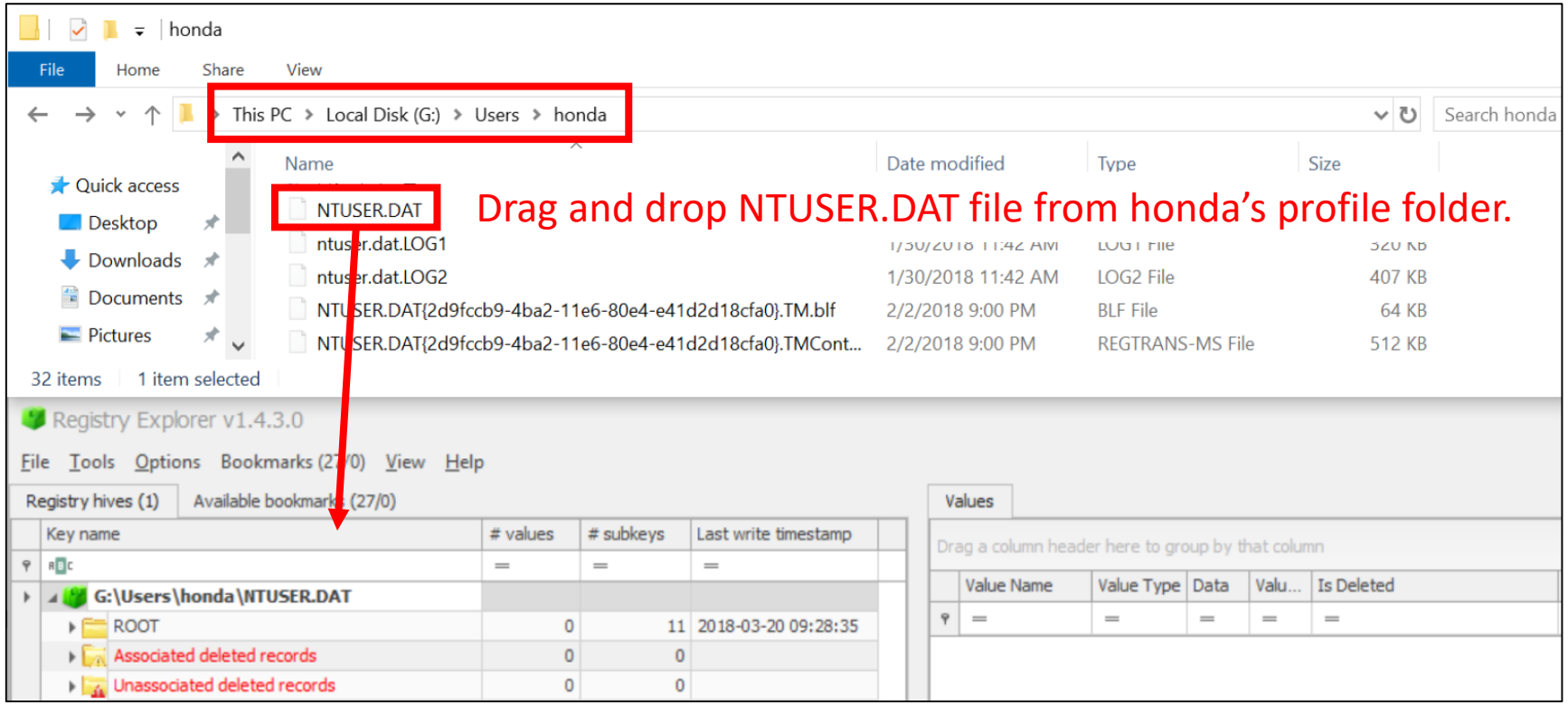
MFT Entry No.

Volumes where:
- Shortcut is located on
- Shortcut was made on
- Target file is located on
- Target file was located on



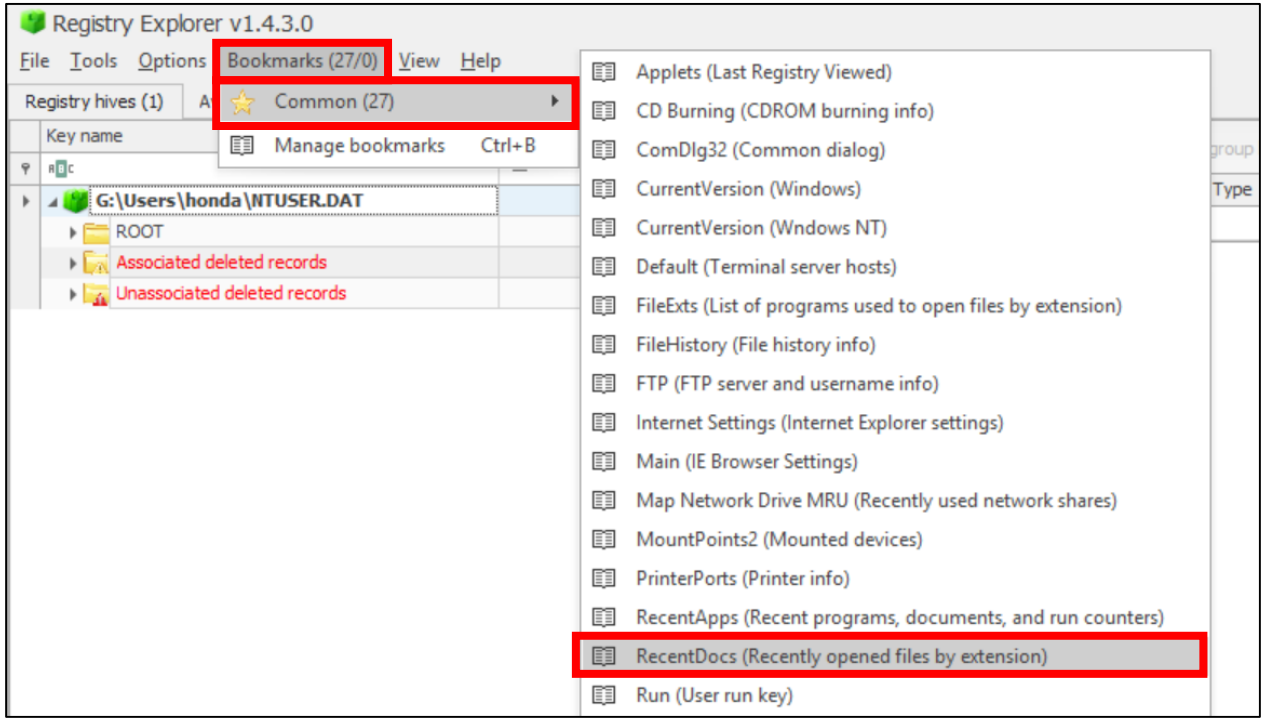
Part 4: Looking into Registry (1/6)

- In this exercise, we will use Registry Explorer.
  - Open RegistryExplorer.exe in the tools folder.



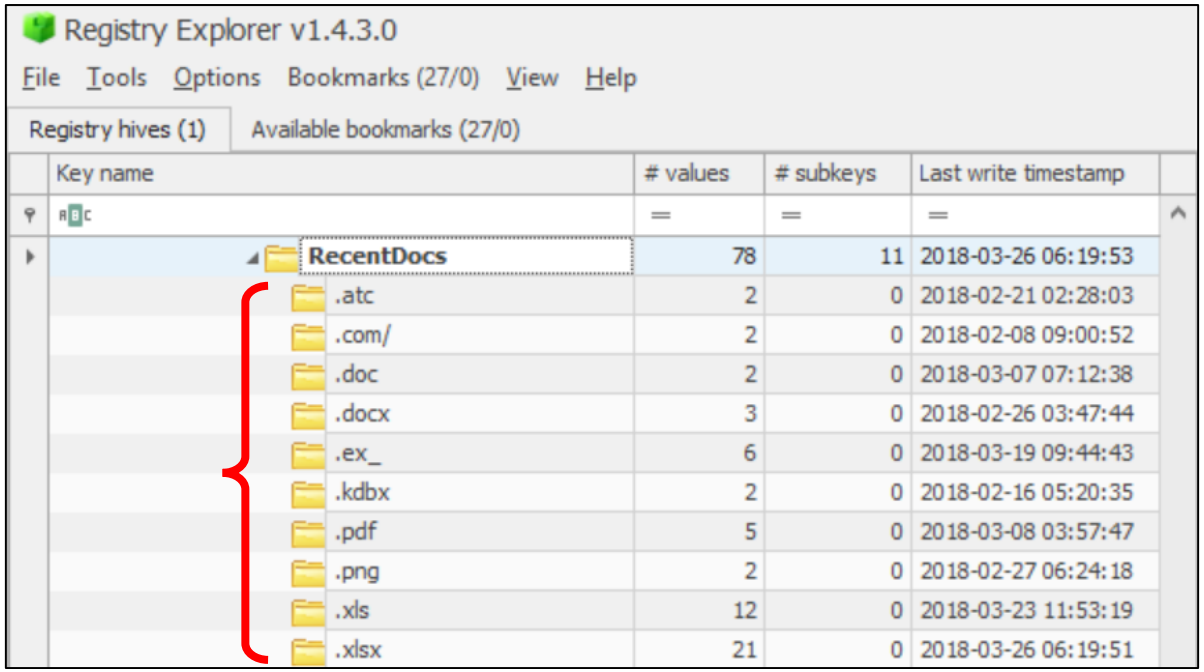
Part 4: Looking into Registry (2/6)

- Registry Explorer has bookmarks to some commonly used Registry Keys, and RecentDocs is in it.
  - From the “Bookmark” menu, select “RecentDocs”.



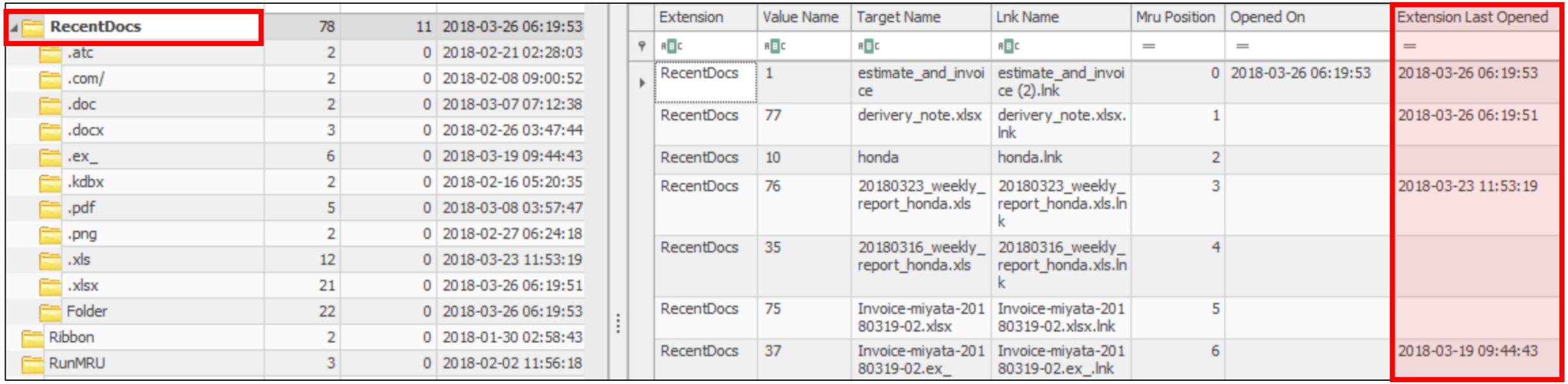
Part 4: Looking into Registry (3/6)

- List of LNK files, target paths, and the date/time when the file was opened is displayed.
- There are also subkeys for some file extensions.



Part 4: Looking into Registry (4/6)

- On Registry Explorer, when you click on the “RecentDocs” key, it shows the list of files that are in position 0 of MRU for each file extension.
- Timestamps of each files being opened (timestamps of each subkey) is shown in “Extension Last Opened” column.

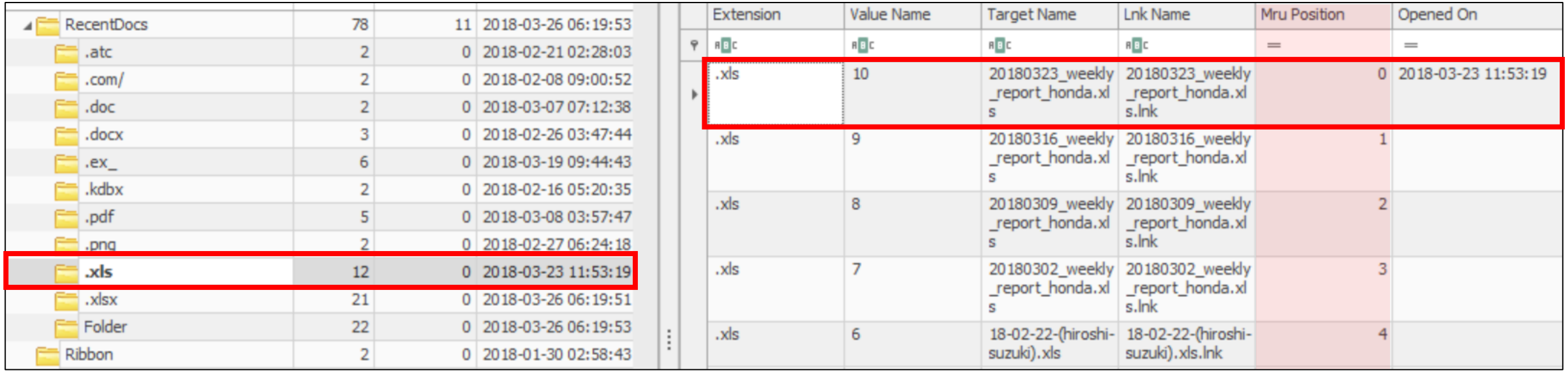


RecentDocs	78	11	2018-03-26 06:19:53
.atc	2	0	2018-02-21 02:28:03
.com/	2	0	2018-02-08 09:00:52
.doc	2	0	2018-03-07 07:12:38
.docx	3	0	2018-02-26 03:47:44
.ex_	6	0	2018-03-19 09:44:43
.kdbx	2	0	2018-02-16 05:20:35
.pdf	5	0	2018-03-08 03:57:47
.png	2	0	2018-02-27 06:24:18
.xls	12	0	2018-03-23 11:53:19
.xlsx	21	0	2018-03-26 06:19:51
Folder	22	0	2018-03-26 06:19:53
Ribbon	2	0	2018-01-30 02:58:43
RunMRU	3	0	2018-02-02 11:56:18

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
RecentDocs	1	estimate_and_invoice	estimate_and_invoice (2).lnk	0	2018-03-26 06:19:53	2018-03-26 06:19:53
RecentDocs	77	derivery_note.xlsx	derivery_note.xlsx.lnk	1		2018-03-26 06:19:51
RecentDocs	10	honda	honda.lnk	2		
RecentDocs	76	20180323_weekly_report_honda.xls	20180323_weekly_report_honda.xls.lnk	3		2018-03-23 11:53:19
RecentDocs	35	20180316_weekly_report_honda.xls	20180316_weekly_report_honda.xls.lnk	4		
RecentDocs	75	Invoice-miyata-20180319-02.xlsx	Invoice-miyata-20180319-02.xlsx.lnk	5		
RecentDocs	37	Invoice-miyata-20180319-02.ex_	Invoice-miyata-20180319-02.ex_.lnk	6		2018-03-19 09:44:43

Part 4: Looking into Registry (5/6)

- RecentDocs records the list of recently opened files for each file extension.
- The figure below shows the key for XLS file extensions. The files with the smaller MRU positions are the files that were opened more recent; the larger values are the files from the past.
- Timestamps of the files being opened is displayed based on the registry key timestamp. Therefore, only the most recent file has the “Opened On” column filled out.

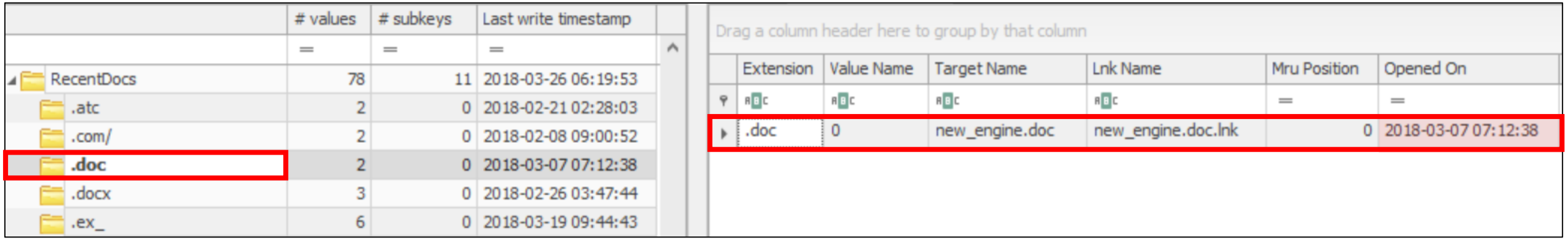


RecentDocs	78	11	2018-03-26 06:19:53
.atc	2	0	2018-02-21 02:28:03
.com/	2	0	2018-02-08 09:00:52
.doc	2	0	2018-03-07 07:12:38
.docx	3	0	2018-02-26 03:47:44
.ex_	6	0	2018-03-19 09:44:43
.kdbx	2	0	2018-02-16 05:20:35
.pdf	5	0	2018-03-08 03:57:47
.png	2	0	2018-02-27 06:24:18
.xls	12	0	2018-03-23 11:53:19
.xlsx	21	0	2018-03-26 06:19:51
Folder	22	0	2018-03-26 06:19:53
Ribbon	2	0	2018-01-30 02:58:43

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On
.xls	10	20180323_weekly_report_honda.xls	20180323_weekly_report_honda.xls.lnk	0	2018-03-23 11:53:19
.xls	9	20180316_weekly_report_honda.xls	20180316_weekly_report_honda.xls.lnk	1	
.xls	8	20180309_weekly_report_honda.xls	20180309_weekly_report_honda.xls.lnk	2	
.xls	7	20180302_weekly_report_honda.xls	20180302_weekly_report_honda.xls.lnk	3	
.xls	6	18-02-22-(hiroshi-suzuki).xls	18-02-22-(hiroshi-suzuki).xls.lnk	4	

Part 4: Looking into Registry (6/6)

- Click on ".doc" subkey.
- new_engine.doc which we have talked about is found. This indicates that no "doc" files were opened after the attack.
  - "Last write timestamp" of ".doc" subkey is March 7, 2018 at 7:12:38 (UTC), which is 4:12:38PM in JST. It is close to the infection time of client-win10-2.



	# values	# subkeys	Last write timestamp
RecentDocs	78	11	2018-03-26 06:19:53
.atc	2	0	2018-02-21 02:28:03
.com/	2	0	2018-02-08 09:00:52
.doc	2	0	2018-03-07 07:12:38
.docx	3	0	2018-02-26 03:47:44
.ex_	6	0	2018-03-19 09:44:43

Drag a column header here to group by that column

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On
.doc	0	new_engine.doc	new_engine.doc.lnk	0	2018-03-07 07:12:38

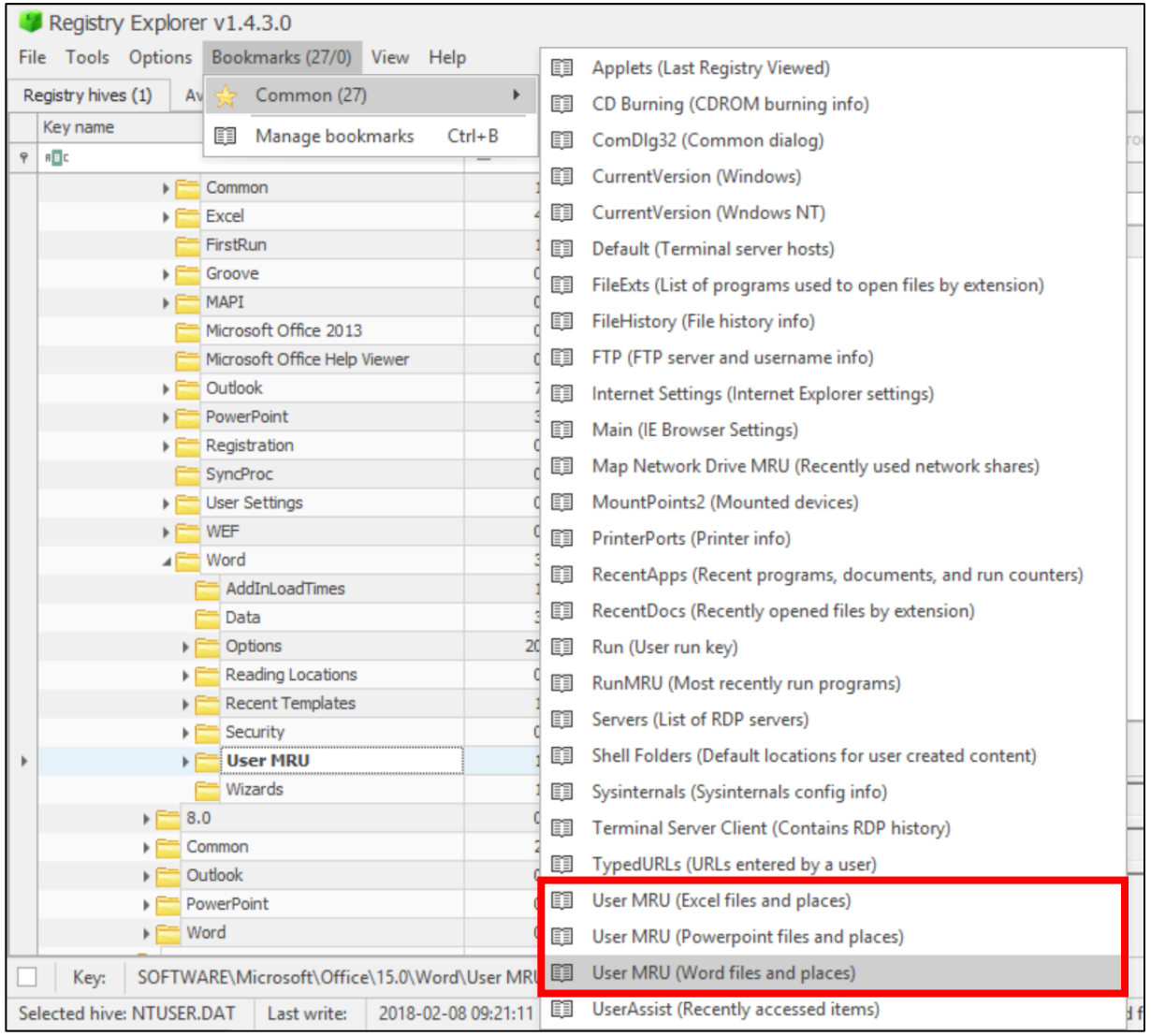
Recent Documents of Some Major Applications

Recent Documents of Microsoft Office Files

- “Recent Documents” for Microsoft Office is recorded at one of the following locations:
  - Shortcuts in **%AppData%\Microsoft\Office\Recent**
  - Registry in **HKEY_USERS\<SID>\Software\Microsoft\Office\<version>\<application>\{File, Place, User} MRU**
    - For example, list of files recently used in Word 2016 are recorded in “HKEY_USERS\<SID>\Software\Microsoft\Office\16.0\Word**File MRU**”.
    - For example, list of directories where files were recently saved/opened in Excel 2016 are recorded in “HKEY_USERS\<SID>Software\Microsoft\Office\16.0\Excel**Place MRU**”.
    - If the user has logged in using Office Accounts, the recent files are stored in “**User MRU**”.
    - Note that different versions of Office have different key structures. Since images from the scenarios used Office 2013, the keys are similar to above, but the structures of subkeys are different.

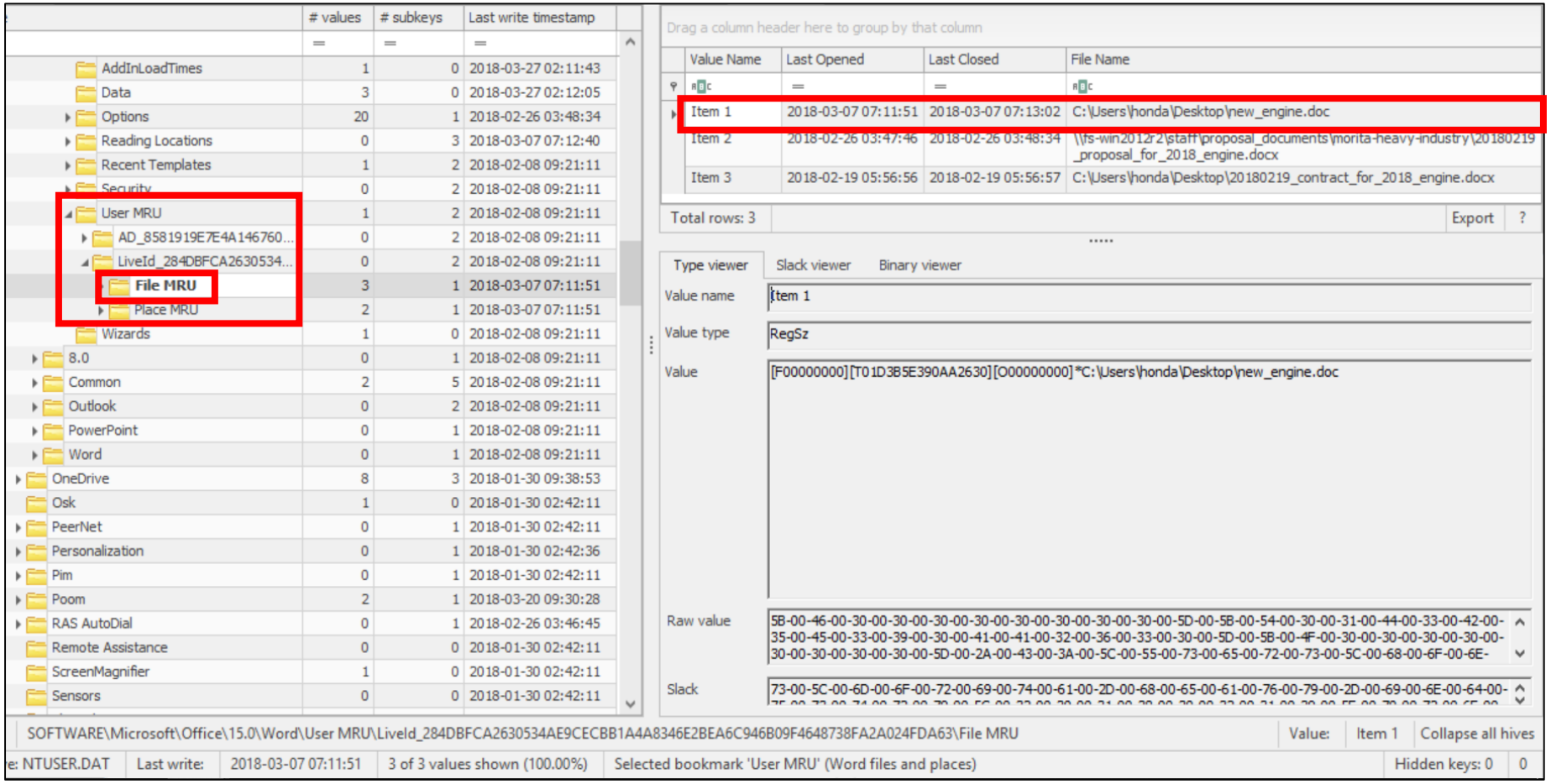
Recent Documents of Microsoft Office Files (1/2)

- Registry Explorer has shortcuts to the Word/Excel/PowerPoint MRUs.



Recent Documents of Microsoft Office Files (2/2)

- By exploring through the File and Place MRUs, you can find the history of files being opened.



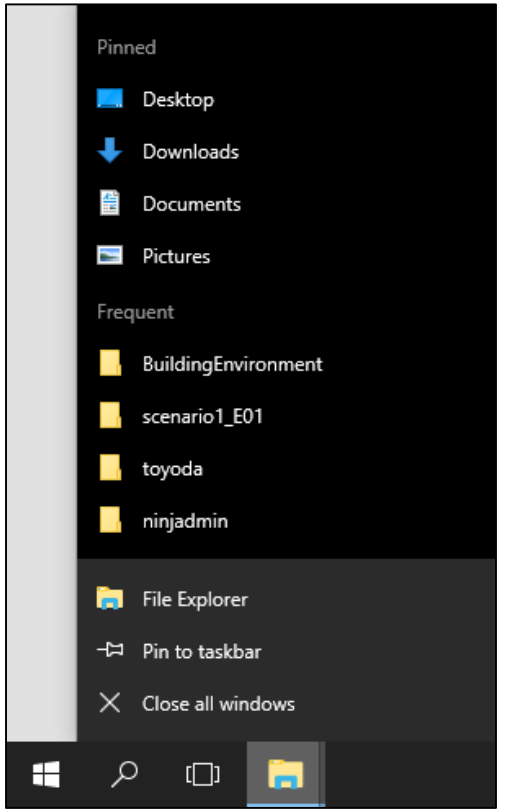
Recent Documents of Acrobat PDF Files

- When you open Adobe Acrobat/Reader, you will see a list of the recently used documents.
- The records are kept in the Registry
  - For Acrobat Reader:
    - **HKEY_USERS\<SID>\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles**
  - For Acrobat, change “Acrobat Reader” to “Adobe Acrobat”.
  - If the application is configured to not to keep file histories, this registry key will be empty.

JumpList

JumpList

- JumpLists are lists of items displayed when an icon on the taskbar is clicked.
  - Available since Windows 7.
- Some applications show list of recently used documents.
  - You could find what files were opened during the attack.
- Two types of JumpLists:
  - Automatic
  - Custom
- JumpLists are recorded as "**.{automatic,custom}Destinations-ms**" file in **%AppData%\Microsoft\Windows\Recent**



Scenario 1 Labs:
Lab 2: Observation of JumpLists for Client-Win10-2

Reading JumpLists

- Since JumpList files are in binary format, it is difficult to read them without tools.
- JumpList Explorer allows you to see the contents of the JumpList files.
- To use JumpList Explorer, you need *Destinations-ms files.
  - Since “%AppData%\Microsoft\Windows\Recent” is treated as a special folder, you cannot directly open the files through ordinal Windows Explorer and file open dialogs.
  - You will need to copy them using Command Prompt.

Copying *Destinations-ms files

- Open Command Prompt from the tools folder.
- Change working directory to Desktop.

```
cd C:\Users\taro\Desktop
```

- Create folders to store the files.

```
mkdir AutomaticDestinations CustomDestinations
```

- Copy files. Note that the following commands must be entered in a single line.

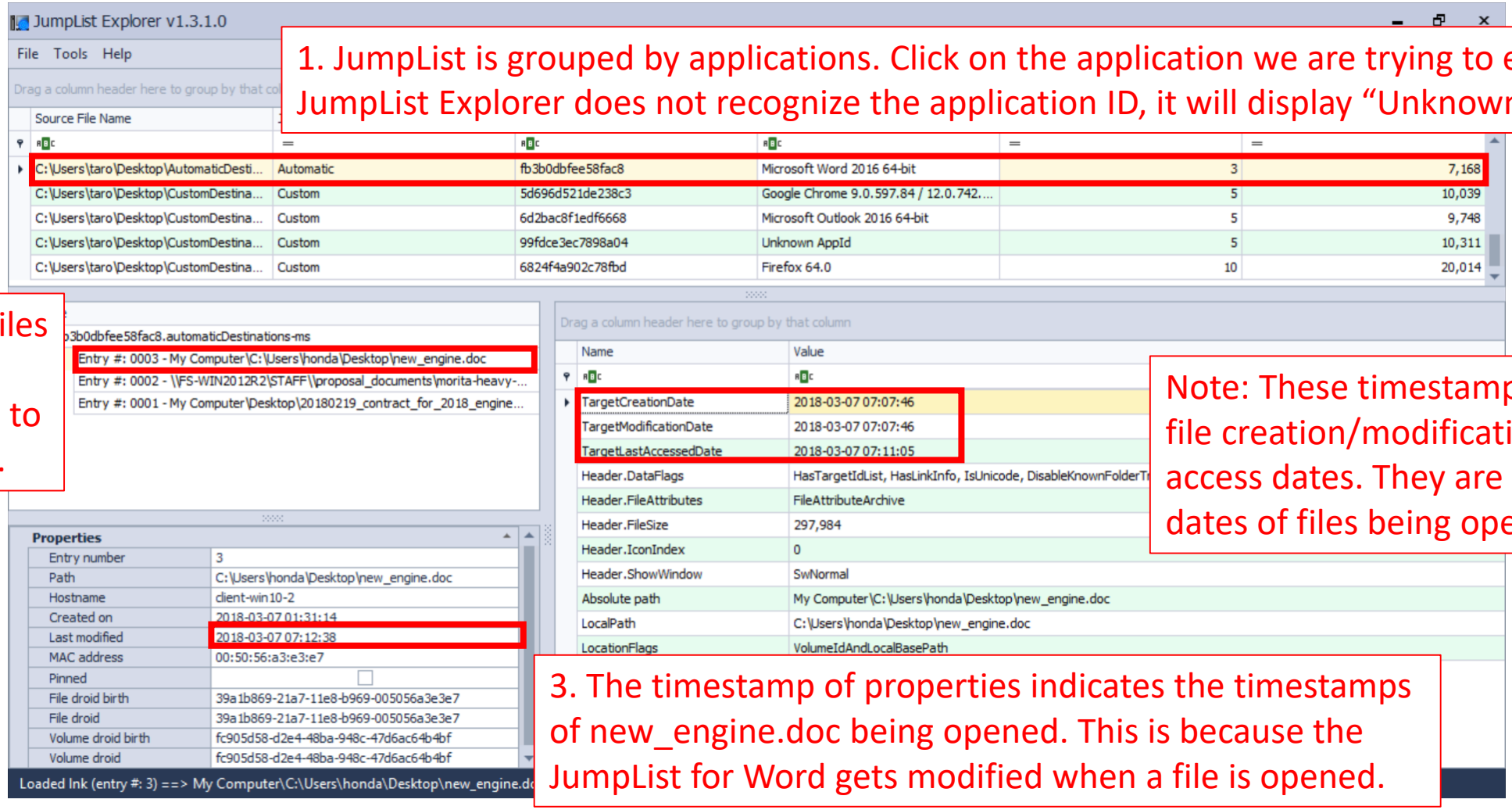
```
copy G:\Users\honda\AppData\Roaming\Microsoft\Windows\Recent
\AutomaticDestinations AutomaticDestinations
```

```
copy G:\Users\honda\AppData\Roaming\Microsoft\Windows\Recent
\CustomDestinations CustomDestinations
```

Opening JumpList Explorer

- From the tools folder, open “JumpListExplorer.exe”.
- From “File” menu, select “Load jump lists”.
- Select files copied to Automatic/Custom Destinations folders.
  - You can use Ctrl+A to select all files within the folder.
  - You can add Automatic/Custom Destinations files later.
  - You might get “Empty Jump List” errors on some of the files. When this dialog is shown, just say OK.
- See what you can find out.

Using JumpList Explorer



1. JumpList is grouped by applications. Click on the application we are trying to explore. If JumpList Explorer does not recognize the application ID, it will display “Unknown AppId”.

2. The list of files is displayed. Click on a line to see its details.

Note: These timestamps are file creation/modification/last access dates. They are **not** the dates of files being opened.

3. The timestamp of properties indicates the timestamps of new_engine.doc being opened. This is because the JumpList for Word gets modified when a file is opened.

AppIDs list

- https://github.com/4n6k/Jump_List_AppIDs/blob/master/4n6k_AppID_Master_List.md
- http://www.forensicswiki.org/wiki/List_of_Jump_List_IDs

4n6k Jump List AppID Master List

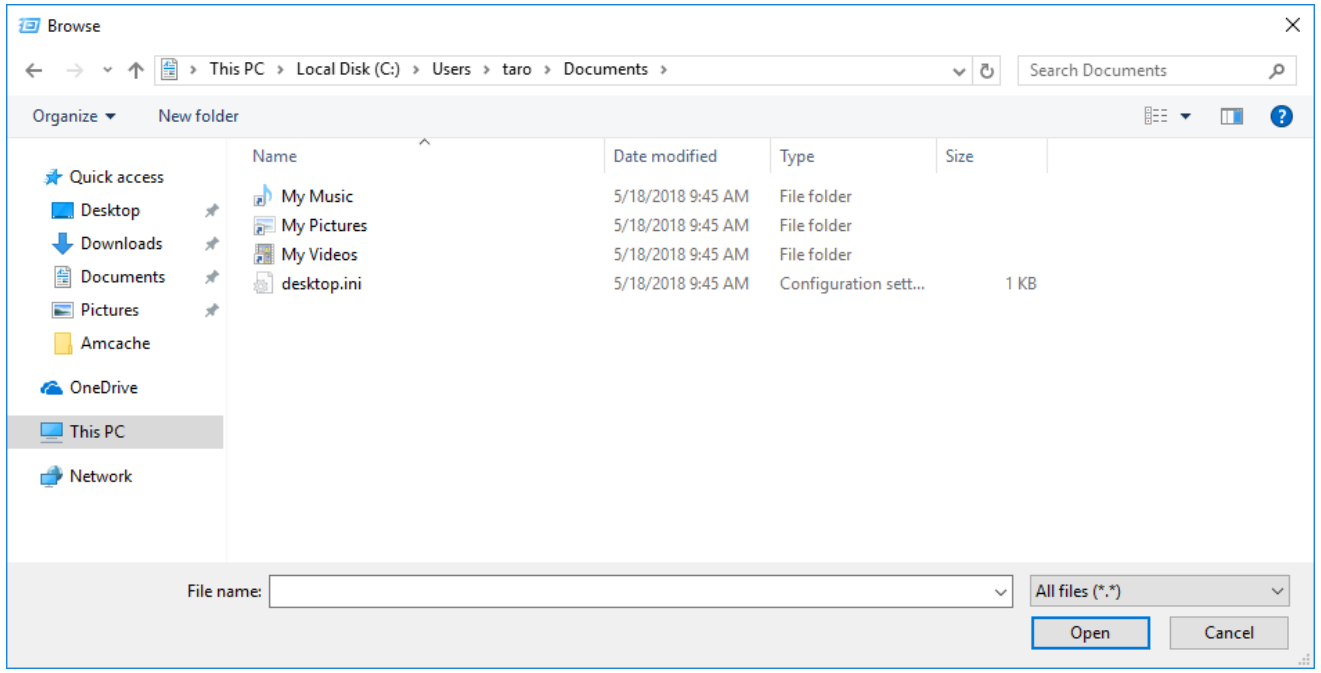
- The following is a list of Jump List AppIDs manually generated by @4n6k.
- For a full understanding of what this is, see the full blog post.
- I am making this available for free. Many forensic tools have used this and previous lists already. Please give credit where credit is due.
- Testing was done using 64-bit versions of Windows 7 and Windows 10.

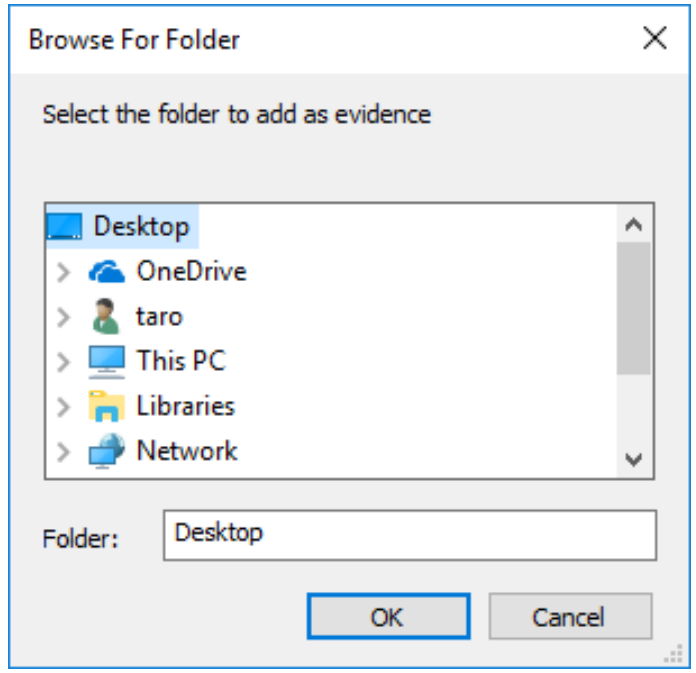
AppID	Application + Version	Date Added	Executable Path	Added By
????????????????	[i2p] i2phex 3.2.0.103.0	9/15/2011	[Default Install Location]	4n6k
f1a4c04eebef2906	[i2p] Robert 0.0.29 Preferences	9/15/2011	[Default Install Location]	4n6k
????????????????	[i2p] Rufus 0.0.4	9/15/2011	[Default Install Location]	4n6k
9ad84c52efeae190	1Password 4.6.0.604	3/8/2016	[Default Install Location] C:¥Program Files (x86)¥1Password 4¥1Password.exe	4n6k
d28ee773b2cea9b2	3D-FTP 9.0 build 7	9/15/2011	[Default Install Location]	4n6k

Common Dialog MRU

Common Dialog

- “Common Dialog” is the dialog that is prepared by the operating system developer to use system-wide.
  - Examples:





LastVisitedMRU

- LastVisitedMRU indicates the **program** that was used to open a file, and the **path** the program used at the last time.
  - When you open a file dialog within a program, the dialog starts at the same folder where the file was opened/saved previously; the LastVisitedMRU may be used to retain the previous location.

- LastVisitedMRU is recorded in "**LastVisitedPidlMRU**" key under "**HKEY_USERS\<SID>\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32**" key.

OpenSaveMRU

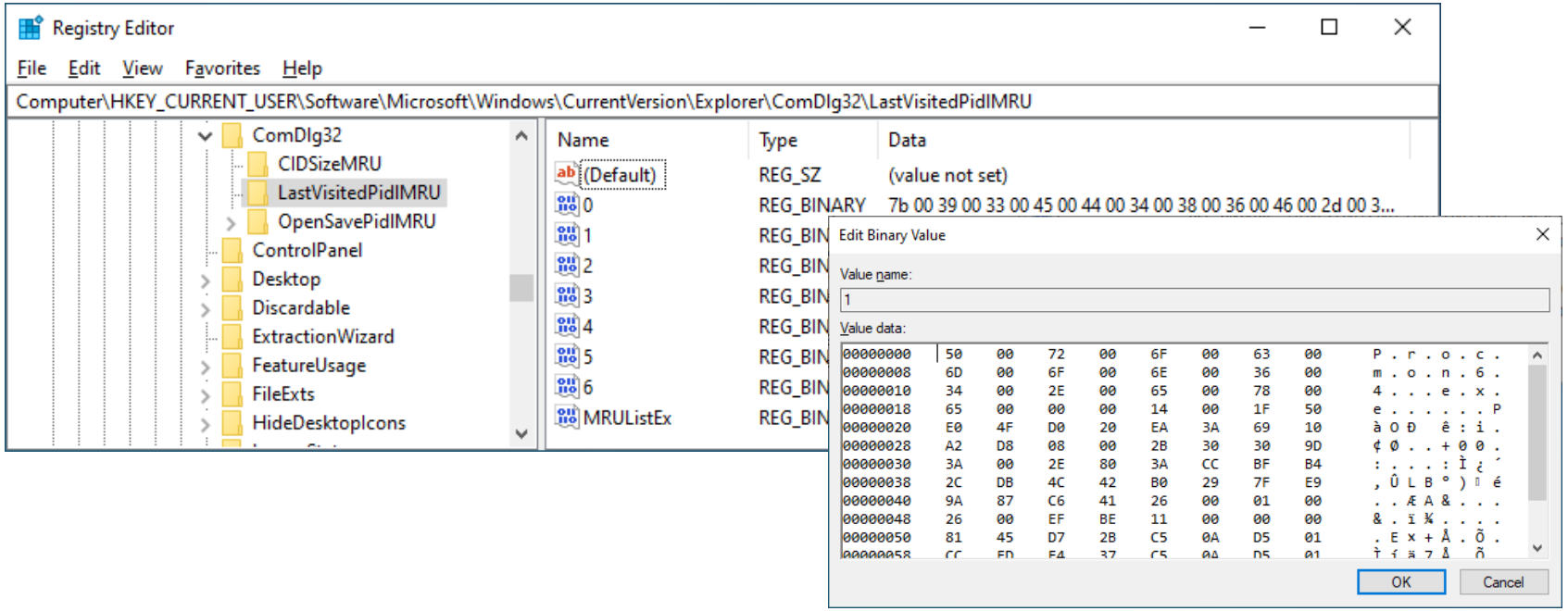
- Similar to LastVisitedMRU, the OpenSaveMRU keeps record of **files** that were recently used in file open/save dialogs.

- OpenSaveMRU is recorded in "**OpenSavePidlMRU**" key under "**HKEY_USERS\<SID>\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32**" key.

Scenario 1 Labs:
Lab 3: Observation of MRUs for Client-Win10-2

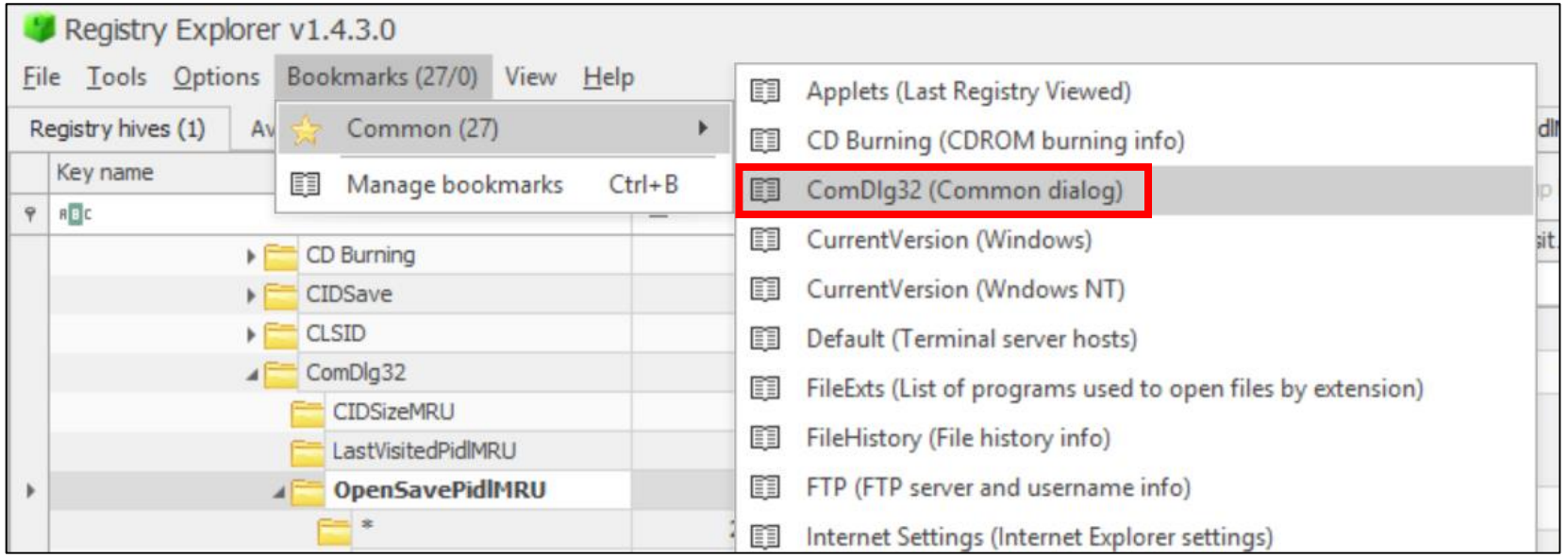
Observation of MRUs

- The MRU registry values are in binary format.
  - They are not easy for humans to read.
  - We will use a tool to read them.



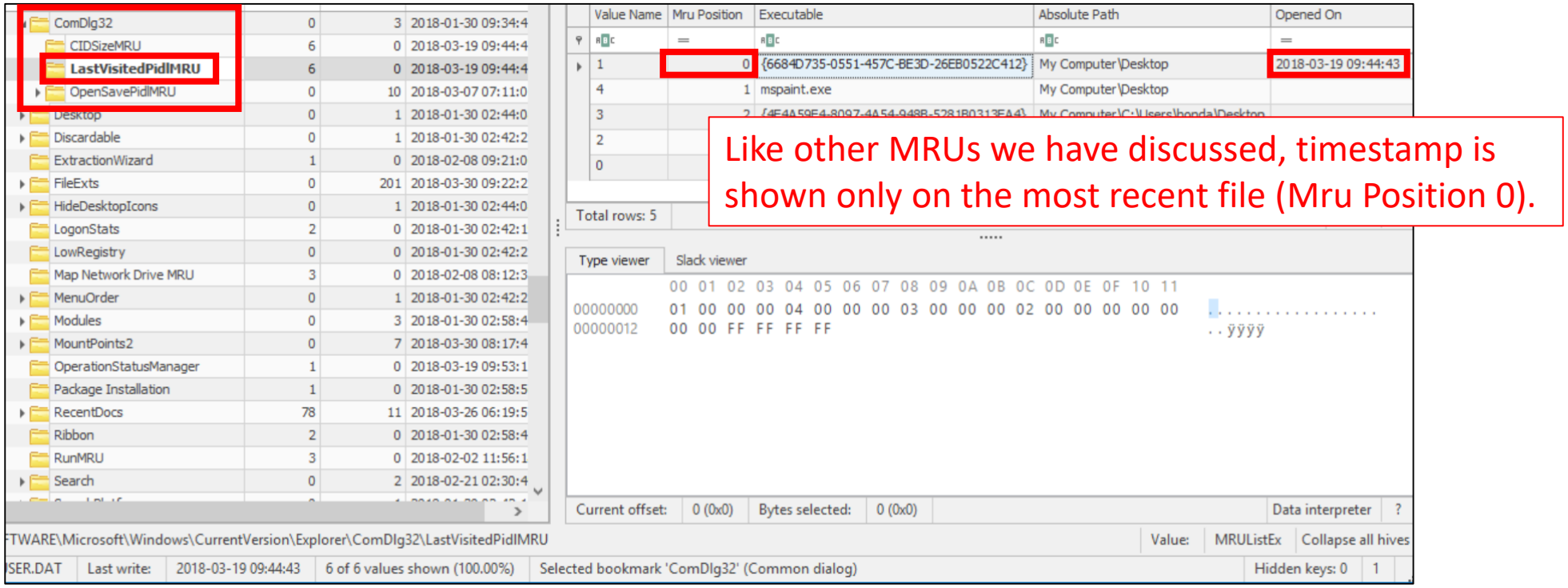
Opening Registry Hives with Registry Explorer

- We will use Registry Explorer (again) to look into MRUs.
- Open Registry Explorer, and read NTUSER.DAT for honda.
- Open "**ComDlg32 (Common dialog)**" from the bookmarks.
  - SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32



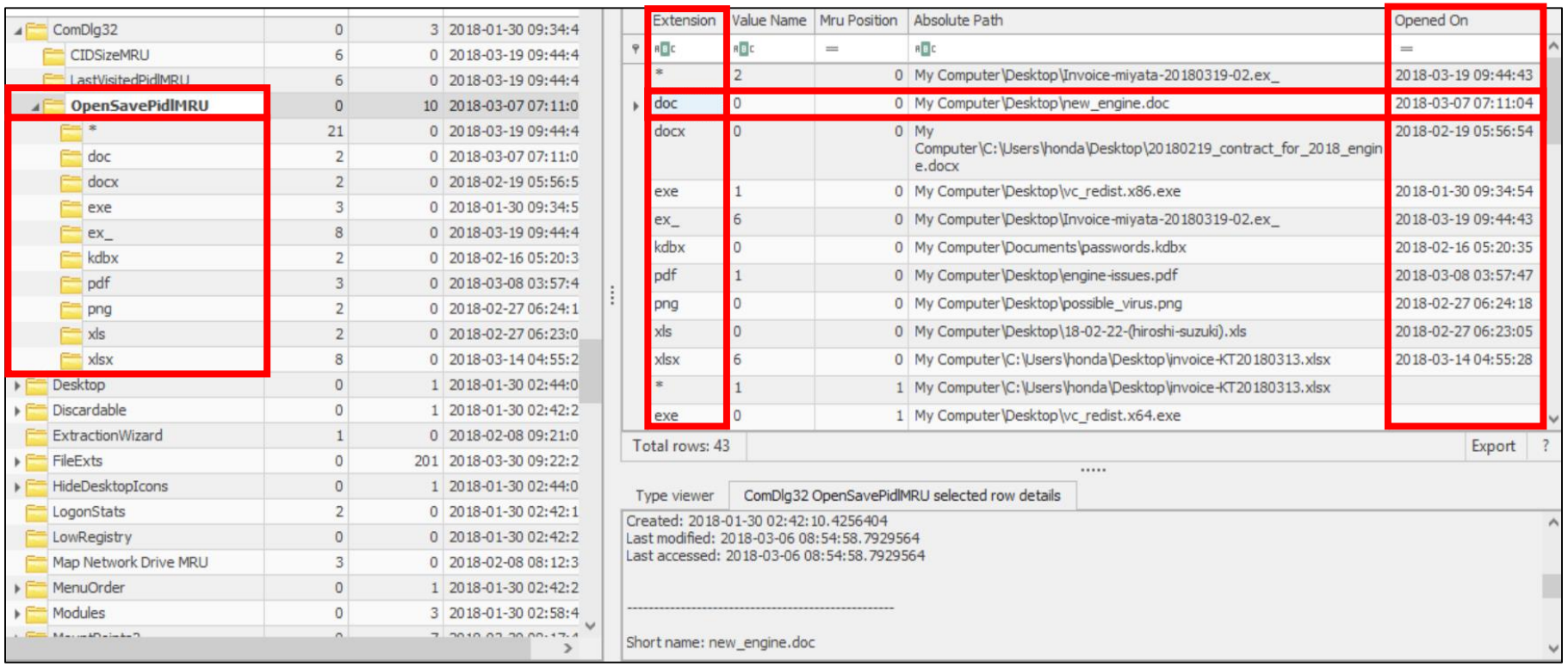
Looking Into MRU Contents (1/2)

- Expand ComDlg32 key and click “LastVisitedPidlMRU”.
  - When you look into the keys, the Registry Explorer parses them and shows the human-readable data to the right pane.



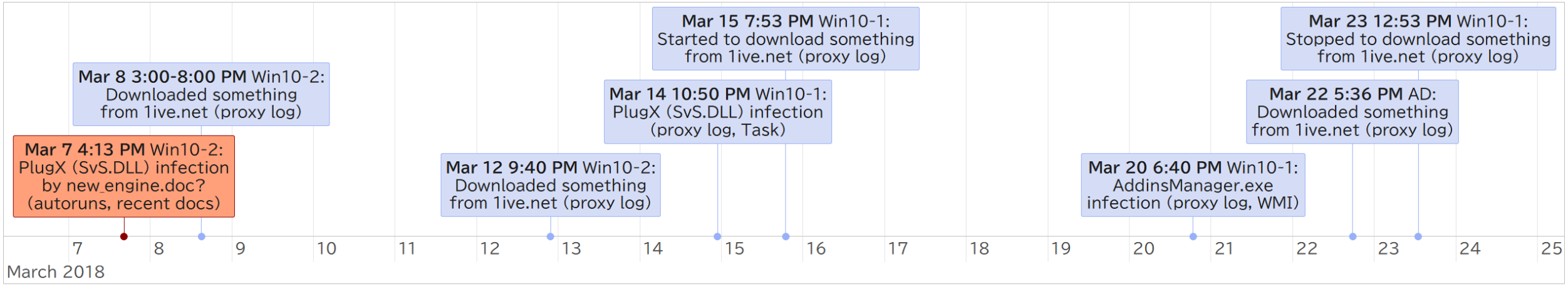
Looking Into MRU Contents (2/2)

- Navigate to “OpenSavePidlMRU”.
  - Lists MRU position 0 for each extension, like other MRUs.



Scenario 1 Labs - Summary

- From the file open activities, we found that the user honda has opened **new_engine.doc** at the time of infection.
  - No other activities were found around that time.
  - This could be the cause of infection.



Summary

Summary

- When a user, regardless of whether it is legitimate or not, opens or saves a file, or creates a folder, there will be some artifacts that are recorded on the computer.
  - Analyzing them will help investigate the incident, regardless of either those activities were done by legitimate users or attackers.
- Be careful that many of the activities are histories of Windows Explorer.
  - If non-GUI tools were used, those histories may not be available.

Tools

- Registry Explorer
  - https://ericzimmerman.github.io/
- YARP
  - https://github.com/msuhanov/yarp
- RegRipper
  - https://github.com/keydet89/RegRipper2.8
- ShellBags Explorer
  - https://ericzimmerman.github.io/
- LECmd
  - https://ericzimmerman.github.io/
- JumpList Explorer
  - https://ericzimmerman.github.io/