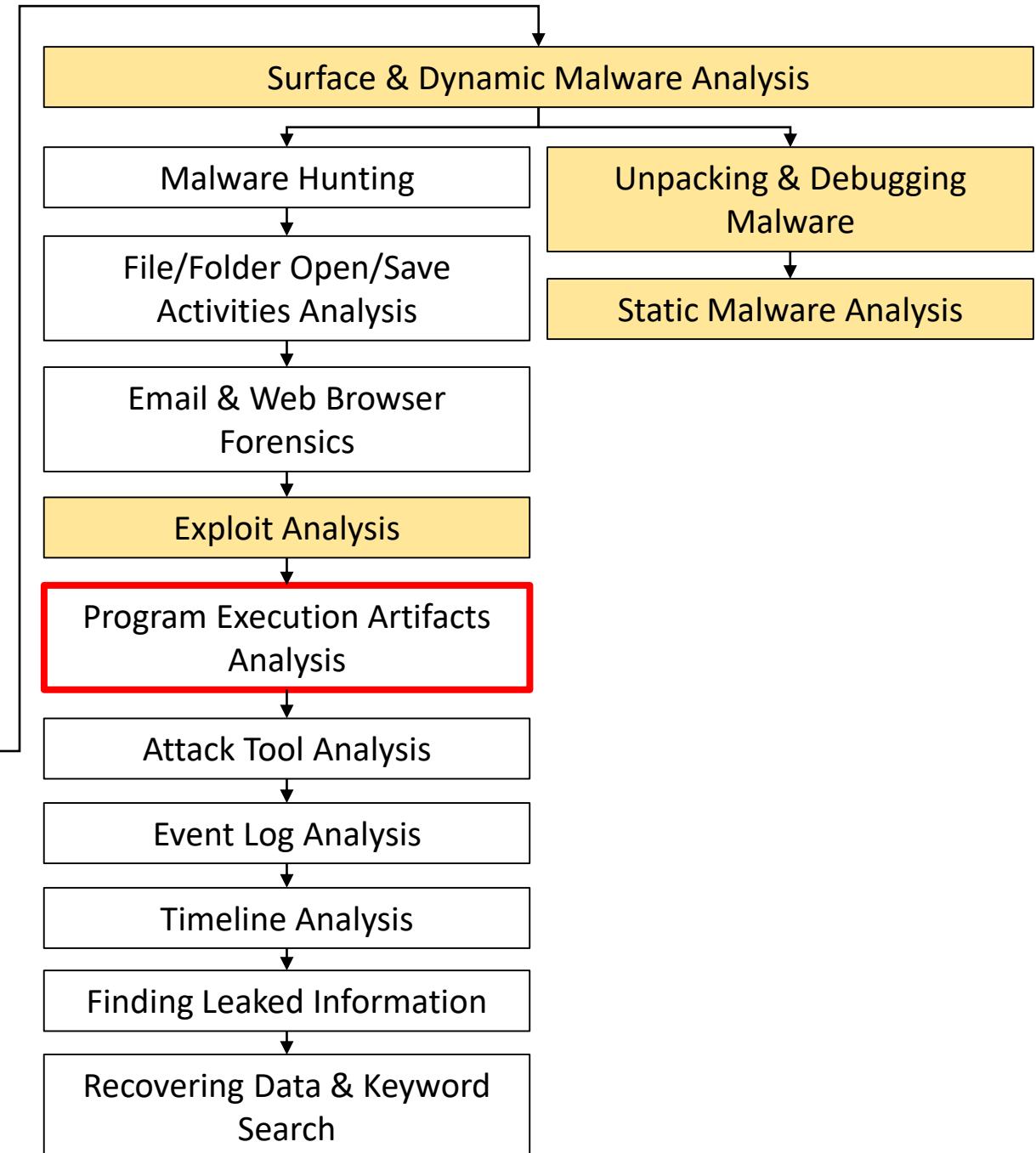
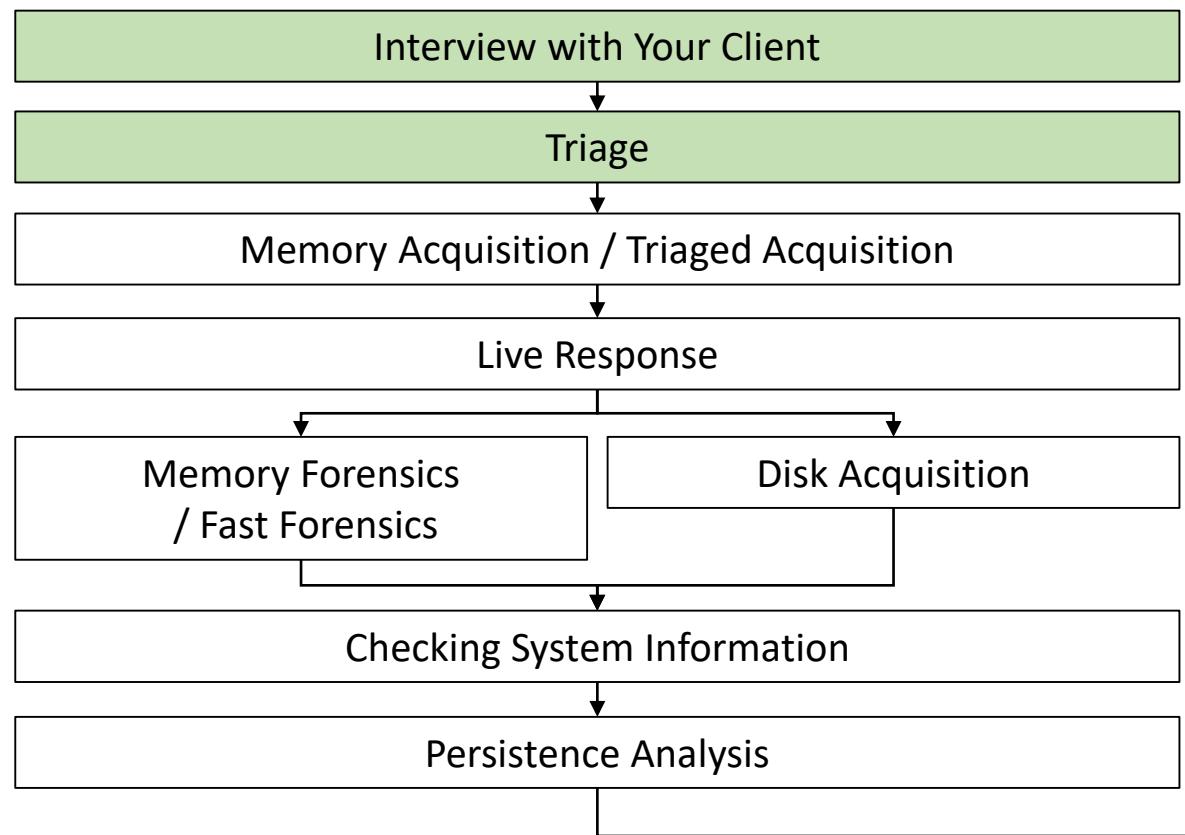


# Program Execution Artifacts Analysis



# Program Execution Artifacts

- When programs are executed on Windows, several “records” of execution remains on the computer.
- By examining the “records”, it may be possible to track the programs that were executed during the intrusion.

# A Variety of Program Execution Artifacts

- There is a variety of program execution artifacts.
- The following URL can help you know what execution artifacts are in your OS.

Artifact	Prefetch	ShimCache	MUICache	Amcache	RecentFileCache.bcf	Syscache.hve	Microsoft-Windows-TaskScheduler (200/201)	LEGACY_* Registry Keys	Microsoft-Windows-Application-Experience Program-Inventory	Microsoft-Windows-Application-Experience Program-Telemetry	Application Experience Program Telemetry
Windows 10	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	TBC
Windows 8.1	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	TBC
Windows 8	Yes	Yes	Yes	Yes	No	TBC	Yes	No	Yes	Yes	TBC
Windows 7	Yes	Yes	Yes	KB2952664+	Yes	Yes	Yes	TBC	Yes	Yes	TBC
Windows Vista	Yes	Yes	Yes	No	No	No	No	TBC	No	No	TBC
Windows XP	Yes	Yes*	Yes	No	No	No	No	Yes	No	No	TBC
Windows Server 2019	If Enabled	Yes	TBC	Yes	TBC	No	TBC	TBC	TBC	TBC	TBC
Windows Server 2016	If Enabled	Yes	Yes	Yes	No	No	Yes	No	TBC	TBC	TBC
Windows Server 2012 R2	If Enabled	Yes	Yes	Yes	No	No	Yes	No	TBC	TBC	TBC
Windows Server 2012	If Enabled	Yes	Yes	Yes	No	No	Yes	No	TBC	TBC	TBC
Windows Server 2008 R2	If Enabled	Yes	Yes	TBC	Yes	Yes	Yes	TBC	TBC	TBC	Yes
Windows Server 2008	If Enabled	Yes	Yes	No	No	TBC	TBC	TBC	TBC	TBC	TBC
Windows Server 2003 R2	If Enabled	Yes	Yes	No	No	No	TBC	Yes	TBC	TBC	TBC
Windows Server 2003	If Enabled	Yes	Yes	No	No	No	TBC	Yes	TBC	TBC	TBC

<https://blog.1234n6.com/2018/10/available-artifacts-evidence-of.html>

[https://1234n6-my.sharepoint.com/:x/p/adam/EU3Fk3ec6NdPsSQx1eA1sfwB\\_R\\_fRa4tJ4c1FR6WJlWIEA?rtime=w3w-xg\\_o1kg](https://1234n6-my.sharepoint.com/:x/p/adam/EU3Fk3ec6NdPsSQx1eA1sfwB_R_fRa4tJ4c1FR6WJlWIEA?rtime=w3w-xg_o1kg)

# What We Will Learn in This Section

- In this course, we will mainly learn several useful program execution artifacts which you are able to know about attackers' post-exploitation activities such as Prefetch, Shimcache, SRUM and so on. You will learn a few artifacts for identifying legitimate user's activities.

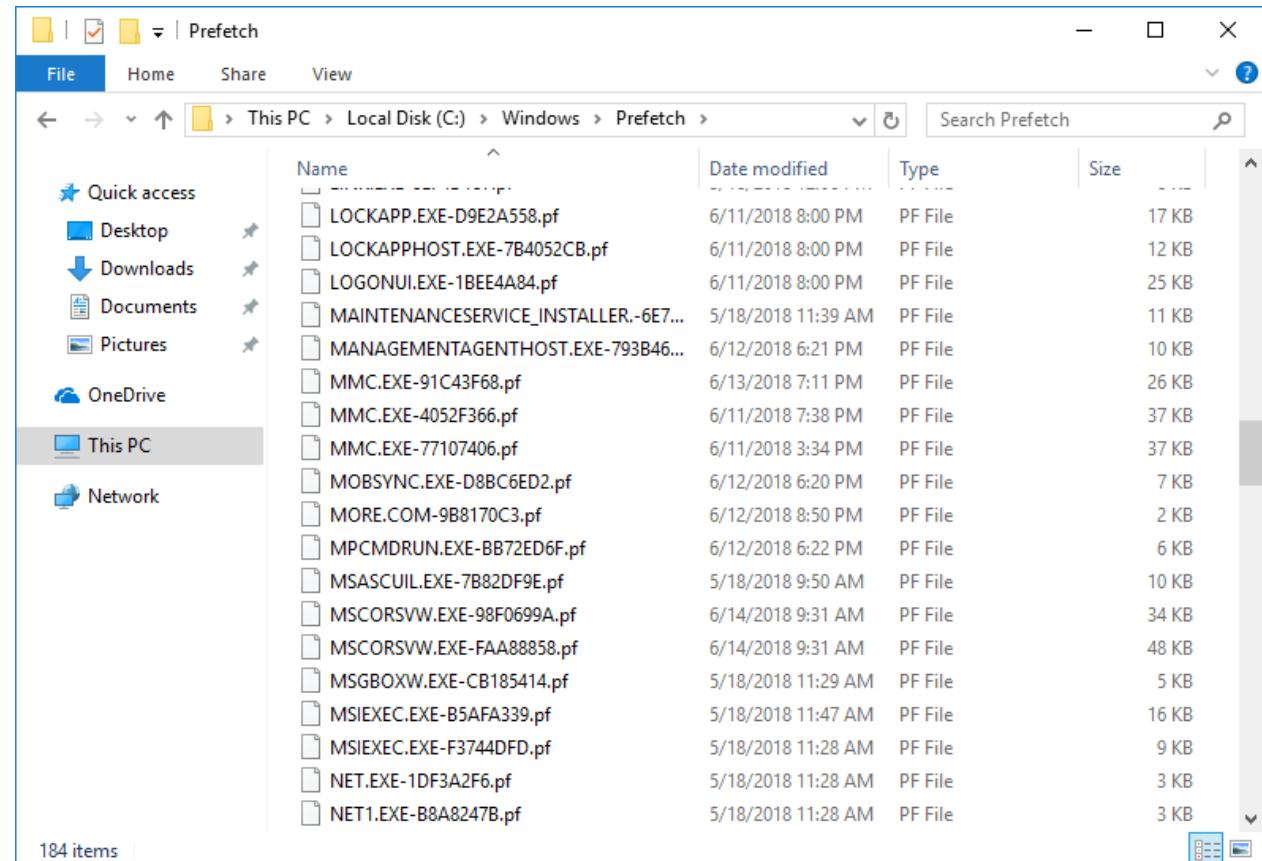
# Prefetch

# Prefetch

- A Windows function for diagnosing user behaviors and creating a list of necessary library files to improve the application execution performances.
- Prefetch was first introduced on Windows XP, and is still available on Windows 10.
- Prefetch is not always enabled: to use the feature, it may be necessary for users to manually enable it.
  - When the host is running a Windows Server OS.
  - In some cases, when the host is running on a virtual machine.

# Prefetch Files

- Prefetch files are created in “Prefetch” folder under “Windows”.
  - File extension is “.pf”.
  - If none of those files exists, prefetch is not enabled on the system.
- Prefetch files are created when the program was executed for the first time.
  - The .pf files will be updated after each program execution.
  - They may be deleted automatically in some cases.
    - E.g. when the number of prefetch files reached the maximum.



# Characteristics of Prefetch (1/2)

- Number of prefetch entries are as follows.
  - Up to 128 files for Windows 7 and older.
  - Up to 256 files for Windows 8 and newer.
    - Even when the number of prefetch entries reached these limits, files are not deleted instantaneously. They will be removed at a certain timing.
  - The number of prefetch files may be configured with the following registry value.
    - Key: "HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Prefetcher"
    - Value: MaxPrefetchFiles
- Each prefetch file stores 8 execution histories for Windows 8 and newer.
  - 1 execution history is stored on older Windows.

# Characteristics of Prefetch (2/2)

- Since prefetch files are updated every time the program is being executed, file system timestamps of the .pf files can be considered as a program execution history record.
  - Creation timestamp as the first execution time.
  - Modification timestamp as the last execution time.
  - However, note that a prefetch file is created or modified at the earlier one of: 10 seconds after the program was executed, or program was terminated. Therefore, there might be a maximum of 10 seconds of difference between the file timestamps and the actual execution time.
- Unlike other histories, prefetch is recorded when the programs were not executed from the Explorer process.
  - However, non-existence of prefetch files does not tell that the program has not been executed. For example, there are cases where the .pf files are not generated when the program was executed with SYSTEM privileges.

Filename	Created Time	Modified Time	File Size
7Z.EXE-3ED84250(pf	5/28/2019 3:52:2...	5/28/2019 4:20:5...	11,652
7Z.EXE-E3EC114E(pf	5/28/2019 3:52:2...	6/1/2019 12:33:0...	101,052

# Contents of the Prefetch Files

- What you can find from a Prefetch file includes:
  1. Name and path of the executable file and the process
  2. Number of times the program was executed
  3. Date/time when the program was last executed
    - For Windows 8 and newer, up to eight histories are recorded.
  4. Files and their paths the program is referring to, such as DLL, EXE and other read files
  5. Index of the files the program is referring to in the order of files being called from the program

1 Filename	Created Time	Modified Time	File Size	1 Process EXE	1 Process Path	2 Run Counter	3 Last Run Time
7Z.EXE-3ED84250(pf)	5/28/2019 3:52:2...	5/28/2019 4:20:5...	11,652	7Z.EXE	\VOLUME{0000000000000000-c6d20b19}\B...	2	5/28/2019 4:20:56 PM, 5/28/2019 3:52:2...
7Z.EXE-E3EC114E(pf)	5/28/2019 3:52:2...	6/1/2019 12:33:0...	101,052	7Z.EXE	C:\PROGRAM FILES\7-Zip\7z.exe	16	6/1/2019 12:33:01 AM, 5/28/2019 3:52:2...
7Z.C.FVE.0F0C4001.fve	5/1/2019 12:45:2...	5/1/2019 12:45:2...	20,054	7Z.C.FVE	C:\PROGRAM FILES\7-Zip\7z.c.fve	1	5/1/2019 12:45:22 AM

4 Filename	4 Full Path	4 Device Path	5 Index
7-ZIP.CHM	C:\PROGRAM FILES\7-Zip\7-zip.chm	\VOLUME{01d5159874530c4d-7e748e...}	38
7-ZIP.DLL	C:\PROGRAM FILES\7-Zip\7-zip.dll	\VOLUME{01d5159874530c4d-7e748e...}	134
7-ZIP.DLL.TMP	C:\PROGRAM FILES\7-ZIP\7-ZIP.DLL....	\VOLUME{01d5159874530c4d-7e748e...}	135
7-ZIP32.DLL	C:\PROGRAM FILES\7-Zip\7-zip32.dll	\VOLUME{01d5159874530c4d-7e748e...}	136
7Z.BIN	C:\PROGRAM FILES\7-Zip\7z.b...	\VOLUME{01d5159874530c4d-7e748e...}	137

# Multiple Prefetch Files

- There may be multiple Prefetch files for the same program name.

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Cou
 IEXPLORE.EXE-1B894AFB(pf)	6/11/2018 9:41:10 PM	6/11/2018 9:41:10 PM	15,846	IEXPLORE.EXE	C:\PROGRAM FILES\INTERNET EXPLORER\iexplore.exe	1
 IEXPLORE.EXE-F6A52C88(pf)	6/11/2018 9:41:10 PM	6/11/2018 9:41:13 PM	20,367	IEXPLORE.EXE	C:\PROGRAM FILES (X86)\INTERNET EXPLORER\iexplore.exe	2

- If program(s) with a same name was executed in different paths, multiple Prefetch files would be created.

# Viewing Prefetch Files (1/2)

- Prefetch files are binary files.
  - Tools are necessary to see their contents.
- WinPrefetchView: software available on NirSoft website.
  - [https://www.nirsoft.net/utils/win\\_prefetch\\_view.html](https://www.nirsoft.net/utils/win_prefetch_view.html)
  - Note that the timestamps shown on the tool is the local time of the analysis machine by default.

The screenshot shows the WinPrefetchView application interface. It has a menu bar with File, Edit, View, Options, and Help. Below the menu is a toolbar with icons for opening files, saving, and other functions. The main area contains two tables of data.

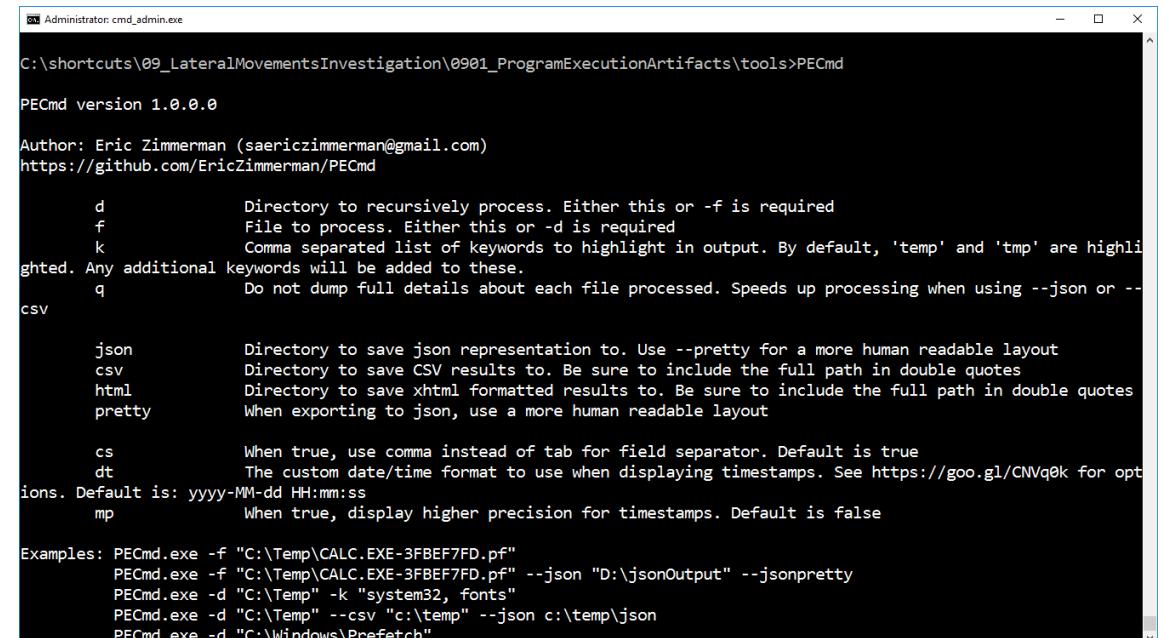
Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counter	Last Run Time	Missing Pr...
C:\Windows\SysWOW64\cmd.exe	5/18/2018 9:46:53...	5/18/2018 11:28:34...	3,388	CMD.EXE	C:\Windows\SysWOW64\cmd.exe	6	5/18/2018 11:28:34 AM, 5/18/2018 9:46:57 A...	No
C:\Windows\System32\COMPATTELRUNN...	6/12/2018 11:49:...	6/13/2018 1:57:1...	8,000	COMPATTELRUNN...	C:\Windows\System32\COMPATTELRUNN...	4	6/13/2018 1:57:10 PM, 6/13/2018 1:57:11 P...	No
C:\Windows\System32\conhost.exe	5/18/2018 9:47:...	6/13/2018 8:59:...	4,173	CONHOST.EXE	C:\Windows\System32\conhost.exe	309	6/13/2018 8:59:24 PM, 6/13/2018 8:54:23 P...	No
C:\Windows\System32\consent.exe	5/18/2018 9:47:3...	6/13/2018 8:23:...	11,036	CONSENT.EXE	C:\Windows\System32\consent.exe	19	6/13/2018 8:22:32 PM, 6/13/2018 7:11:25 P...	No
C:\Windows\MICROSOFT.NET.FRAMEWO...	5/18/2018 11:17:...	5/18/2018 12:29:...	9,279	CSC.EXE	C:\Windows\MICROSOFT.NET.FRAMEWO...	6	5/18/2018 12:29:23 PM, 5/18/2018 12:27:29 ...	No
C:\Windows\MICROSOFT.NET.FRAMEWO...	5/18/2018 11:17:...	5/18/2018 12:29:...	3,299	CVTRES.EXE	C:\Windows\MICROSOFT.NET.FRAMEWO...	6	5/18/2018 12:29:23 PM, 5/18/2018 12:27:30 ...	No
C:\Windows\System32\dllhost.exe	5/18/2018 10:05:...	6/13/2018 7:11:1...	3,719	DLLHOST.EXE	C:\Windows\System32\dllhost.exe	11	6/13/2018 7:11:12 PM, 6/12/2018 6:19:55 P...	No

Filename	Full Path	Device Path	Index
ADVAPI32.DLL	C:\Windows\System32\advapi32.dll	\VOLUME\01d3ecc73f14a3e-8274ca45\WINDOWS\SYSTEM32\ADVAPI32.DLL	7
CMD.EXE	C:\Windows\System32\cmd.exe	\VOLUME\01d3ecc73f14a3e-8274ca45\WINDOWS\SYSTEM32\CMD.EXE	1
CMDEXT.DLL	C:\Windows\System32\cmdex.dll	\VOLUME\01d3ecc73f14a3e-8274ca45\WINDOWS\SYSTEM32\CMDEXT.DLL	6
IS-LISTENER-RUNNING...	C:\PROGRAMDATA\VMware\VMWARE CAF\pm\scripts\IS-LISTENER-RUNNING.BAT	\VOLUME\01d3ecc73f14a3e-8274ca45\PROGRAMDATA\VMWARE\VMWARE CAF\PM\SCRIPTS\IS-LISTEN...	10
KERNEL32.DLL	C:\Windows\System32\kernel32.dll	\VOLUME\01d3ecc73f14a3e-8274ca45\WINDOWS\SYSTEM32\KERNEL32.DLL	2
KERNELBASE.DLL	C:\Windows\System32\kernelbase.dll	\VOLUME\01d3ecc73f14a3e-8274ca45\WINDOWS\SYSTEM32\KERNELBASE.DLL	3
LOCALE.NLS	C:\Windows\System32\locale.nls	\VOLUME\01d3ecc73f14a3e-8274ca45\WINDOWS\SYSTEM32\LOCALE.NLS	4
MSVCR7.DLL	C:\Windows\System32\msvcr7.dll	\VOLUME\01d3ecc73f14a3e-8274ca45\WINDOWS\SYSTEM32\MSVCR7.DLL	5
NTDLL.DLL	C:\Windows\System32\ntdll.dll	\VOLUME\01d3ecc73f14a3e-8274ca45\WINDOWS\SYSTEM32\NTDLL.DLL	0
RPCRT4.DLL	C:\Windows\System32\rpcrt4.dll	\VOLUME\01d3ecc73f14a3e-8274ca45\WINDOWS\SYSTEM32\RPCRT4.DLL	9
SECHOST.DLL	C:\Windows\System32\sechost.dll	\VOLUME\01d3ecc73f14a3e-8274ca45\WINDOWS\SYSTEM32\SECHOST.DLL	8
SORTDEFAULT.NLS	C:\Windows\GLOBALIZATION\Sorting\SORTDEFAULT.NLS	\VOLUME\01d3ecc73f14a3e-8274ca45\WINDOWS\GLOBALIZATION\SORTING\SORTDEFAULT.NLS	11

# Viewing Prefetch Files (2/2)

- PEcmd
  - Command line tool that can parse prefetch files.
    - <https://ericzimmerman.github.io/>
  - WinPrefetchView shows all the “Last Run Time” in a single column, but PEcmd can split them.
  - PEcmd sometimes fails to resolve full paths because it uses a file name based on a “.pf” file to resolve a path, not an actual file name in a record, while WinPrefetchView can succeed. In that case, you should also check the result of WinPrefetchView.
  - Note that the default time zone will be UTC.



```
C:\shortcuts\09_LateralMovementsInvestigation\0901_ProgramExecutionArtifacts>PEcmd
PEcmd version 1.0.0.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PEcmd

d          Directory to recursively process. Either this or -f is required
f          File to process. Either this or -d is required
k          Comma separated list of keywords to highlight in output. By default, 'temp' and 'tmp' are highlighted. Any additional keywords will be added to these.
q          Do not dump full details about each file processed. Speeds up processing when using --json or --csv

json        Directory to save json representation to. Use --pretty for a more human readable layout
csv         Directory to save CSV results to. Be sure to include the full path in double quotes
html        Directory to save xhtml formatted results to. Be sure to include the full path in double quotes
pretty      When exporting to json, use a more human readable layout

cs          When true, use comma instead of tab for field separator. Default is true
dt          The custom date/time format to use when displaying timestamps. See https://goo.gl/CNVq0k for options. Default is: yyyy-MM-dd HH:mm:ss
mp          When true, display higher precision for timestamps. Default is false

Examples: PEcmd.exe -f "C:\Temp\CALC.EXE-3FBEF7FD.pf"
          PEcmd.exe -f "C:\Temp\CALC.EXE-3FBEF7FD.pf" --json "D:\jsonOutput" --jsonpretty
          PEcmd.exe -d "C:\Temp" -k "system32, fonts"
          PEcmd.exe -d "C:\Temp" --csv "c:\temp" --json c:\temp\json
          PEcmd.exe -d "C:\Windows\Prefetch"
```

# Tips for Analyzing Prefetch (1/3)

Step 1: Start the analysis using WinPrefetchView:

## 1. Sort by Created Time

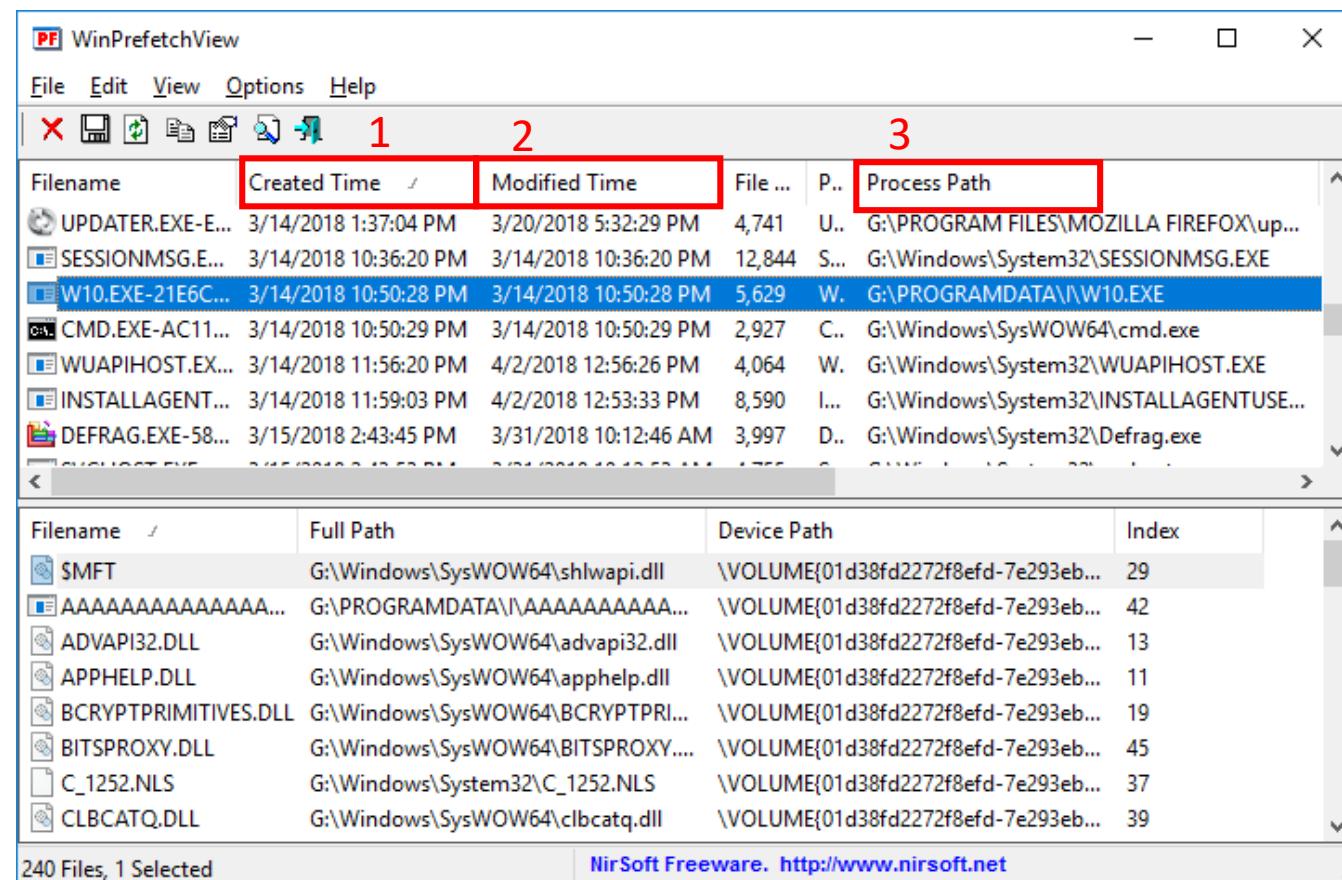
- Timeline of the initial execution can be found.

## 2. Sort by Modified Time

- Timeline of the last program execution can be found.

## 3. Sort by Process Path

- File paths that do not exist on the original state of the environment may be found.
- Even if the files are legitimate Windows executables, if the path is under “SysWOW64” folder, the program was 32-bit, not 64-bit.



Filename	Created Time	Modified Time	File ...	P...	Process Path
UPDATER.EXE-E...	3/14/2018 1:37:04 PM	3/20/2018 5:32:29 PM	4,741	U...	G:\PROGRAM FILES\MOZILLA FIREFOX\up...
SESSIONMSG.E...	3/14/2018 10:36:20 PM	3/14/2018 10:36:20 PM	12,844	S...	G:\Windows\System32\SESSIONMSG.EXE
W10.EXE-21E6C...	3/14/2018 10:50:28 PM	3/14/2018 10:50:28 PM	5,629	W...	G:\PROGRAMDATA\W10.EXE
CMD.EXE-AC11...	3/14/2018 10:50:29 PM	3/14/2018 10:50:29 PM	2,927	C...	G:\Windows\SysWOW64\cmd.exe
WUAPIHOST.EX...	3/14/2018 11:56:20 PM	4/2/2018 12:56:26 PM	4,064	W...	G:\Windows\System32\WUAPIHOST.EXE
INSTALLAGENT...	3/14/2018 11:59:03 PM	4/2/2018 12:53:33 PM	8,590	I...	G:\Windows\System32\INSTALLAGENTUSE...
DEFRAG.EXE-58...	3/15/2018 2:43:45 PM	3/31/2018 10:12:46 AM	3,997	D...	G:\Windows\System32\Defrag.exe
SMFT					
AAAAAAAAAAAAAA...					
ADVAPI32.DLL					
APPHHELP.DLL					
BCRYPTPRIMITIVES.DLL					
BITSPROXY.DLL					
C_1252.NLS					
CLBCATQ.DLL					

240 Files, 1 Selected      NirSoft Freeware. <http://www.nirsoft.net>

Note that SysWoW64 is NOT a directory for 64 bit, but for 32 bit.

It stands for the **System** directory for **Windows 32 bit On Windows 64 bit**.

# Tips for Analyzing Prefetch (2/3)

Step 2: When a suspicious entry is found, use the bottom pane to confirm the files used by the program.

## 1. Sort by Full Path (or Device Path)

- File paths that do not exist on the original state of the environment may be found.
- Even if the files are legitimate Windows files, if the path is under “SysWOW64” folder, the program was 32-bit, not 64-bit.

## 2. Sort by Index

- Presents the order of files that were read from the program.

The screenshot shows the WinPrefetchView application interface. The top pane displays a list of prefetch entries with columns for Filename, Created Time, Modified Time, File Size, Process Type, and Process Path. One entry, 'W10.EXE-21E6C...', is selected and highlighted in blue. The bottom pane shows a detailed view of the selected file's dependencies, with columns for Filename, Full Path, Device Path, and Index. The 'Full Path' and 'Device Path' columns are highlighted with red boxes and numbered '1', while the 'Index' column is also highlighted with a red box and numbered '2'. The status bar at the bottom indicates '240 Files, 1 Selected' and the source 'NirSoft Freeware. http://www.nirsoft.net'.

Filename	Created Time	Modified Time	File ...	P...	Process Path
UPDATER.EXE-E...	3/14/2018 1:37:04 PM	3/20/2018 5:32:29 PM	4,741	U..	G:\PROGRAM FILES\MOZILLA FIREFOX\up...
SESSIONMSG.E...	3/14/2018 10:36:20 PM	3/14/2018 10:36:20 PM	12,844	S...	G:\Windows\System32\SESSIONMSG.EXE
W10.EXE-21E6C...	3/14/2018 10:50:28 PM	3/14/2018 10:50:28 PM	5,629	W..	G:\PROGRAMDATA\W10.EXE
C:\CMD.EXE-AC11...	3/14/2018 10:50:29 PM	3/14/2018 10:50:29 PM	2,927	C..	G:\Windows\SysWOW64\cmd.exe
C:\WUAPIHOST.EX...	3/14/2018 11:56:20 PM	4/2/2018 12:56:26 PM	4,064	W..	G:\Windows\System32\WUAPIHOST.EXE
C:\INSTALLAGENT...	3/14/2018 11:59:03 PM	4/2/2018 12:53:33 PM	8,590	I...	G:\Windows\System32\INSTALLAGENTUSE...
C:\DEFFRAG.EXE-58...	3/15/2018 2:43:45 PM	3/31/2018 10:12:46 AM	3,997	D..	G:\Windows\System32\Defrag.exe
SYSCON.FVE	3/14/2018 10:50:28 PM	3/21/2018 10:12:53 AM	175	S...	G:\Windows\System32\syscon.fve

Filename	Full Path	Device Path	Index
SMFT	G:\Windows\SysWOW64\shlwapi.dll	\VOLUME{01d38fd2272f8efd-7e293eb...}	29
AAAAAAAAAAAAAAA...	G:\PROGRAMDATA\AAAAAAAAAAA...	\VOLUME{01d38fd2272f8efd-7e293eb...}	42
ADVAPI32.DLL	G:\Windows\SysWOW64\advapi32.dll	\VOLUME{01d38fd2272f8efd-7e293eb...}	13
APPHHELP.DLL	G:\Windows\SysWOW64\apphelp.dll	\VOLUME{01d38fd2272f8efd-7e293eb...}	11
BCRYPTPRIMITIVES.DLL	G:\Windows\SysWOW64\BCRYPTPRI...	\VOLUME{01d38fd2272f8efd-7e293eb...}	19
BITSPROXY.DLL	G:\Windows\SysWOW64\BITSPROXY....	\VOLUME{01d38fd2272f8efd-7e293eb...}	45
C_1252.NLS	G:\Windows\System32\C_1252.NLS	\VOLUME{01d38fd2272f8efd-7e293eb...}	37
CLBCATQ.DLL	G:\Windows\SysWOW64\clbcatq.dll	\VOLUME{01d38fd2272f8efd-7e293eb...}	39

# Tips for Analyzing Prefetch (3/3)

- When looking into the “Last Run Time”, WinPrefetchView cannot treat each history independently.
- PECmd can split those Last Run Time entries.
- You can just do it like the following command.
- You will get two files and the file ends with “\_Timeline.csv” is the file which is split by Last Run Time.

20180731144858_PECmd_Output_Timeline.csv - LibreOffice Calc	
A331	File Edit View Insert Format Styles Sheet Data Tools Window Help
	Liberation Sans 10 <b>a a a</b> <b>A B</b> <b>% 0.0</b> <b>0.0</b>
	2018-03-07 13:40:21
A	B
309	2018-03-07 06:04:03 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSTEM32\DLLHOST.EXE
310	2018-03-07 07:10:19 \VOLUME{01d396231a3999ae-b81c324b}\PROGRAM FILES\MICROSOFT OFFICE 15\ROOT\OFFICE15\WINWORD.EXE
311	2018-03-07 07:11:46 \VOLUME{01d396231a3999ae-b81c324b}\PROGRAM FILES\MICROSOFT OFFICE 15\ROOT\OFFICE15\WINWORD.EXE
312	2018-03-07 07:11:49 \VOLUME{01d396231a3999ae-b81c324b}\PROGRAM FILES\MICROSOFT OFFICE 15\ROOT\OFFICE15\WINWORD.EXE
313	2018-03-07 07:13:00 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\CERTUTIL.EXE
314	2018-03-07 07:13:01 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\EXPLORER.EXE
315	2018-03-07 07:13:01 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\REG.EXE
316	2018-03-07 07:13:02 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\RUNDLL32.EXE
317	2018-03-07 07:13:06 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\RPCCONFIG.EXE
318	2018-03-07 07:13:29 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
319	2018-03-07 07:13:40 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\SYSTEMINFO.EXE
320	2018-03-07 07:13:44 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\WBEM\WMIPRVS.EXE
321	2018-03-07 07:13:47 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
322	2018-03-07 07:13:56 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSTEM32\MSIEXEC.EXE
323	2018-03-07 07:14:02 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\REG.EXE
324	2018-03-07 07:14:03 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\FIND.EXE
325	2018-03-07 07:14:03 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\FIND.EXE
326	2018-03-07 07:14:03 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\FIND.EXE
327	2018-03-07 07:14:03 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\REG.EXE
328	2018-03-07 07:14:03 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\REG.EXE
329	2018-03-07 07:14:21 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\RPCCONFIG.EXE
330	2018-03-07 07:14:21 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\NET.EXE
331	2018-03-07 07:14:21 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\NET1.EXE
332	2018-03-07 07:14:21 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\NET1.EXE
333	2018-03-07 07:14:21 \VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\NETSTAT.EXE
334	2018-03-08 03:19:35 \VOLUME{01d396231a3999ae-b81c324b}\PROGRAM FILES\VMWARE\VMWARE TOOLS\VMWARERESOLUTIONSET.EXE

```
PECmd.exe -d PATH_TO_PREFETCH_FOLDER --csv PATH_TO_OUTPUT_FOLDER
```

 20190601042926\_PECmd\_Output.csv

6/1/2019 1:29 PM OpenOffice.org 1.... 1,804 KB

 20190601042926\_PECmd\_Output\_Timeline.csv

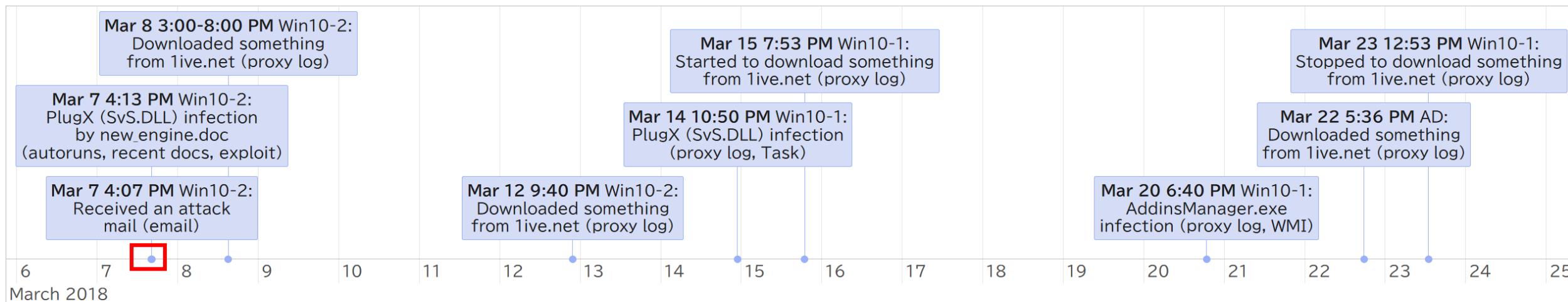
6/1/2019 1:29 PM OpenOffice.org 1.... 84 KB

# Scenario 1 Labs:

## Lab 1: Looking into Prefetch Files for Client-Win10-2

# Looking into Prefetch Files

- The goal of this exercise is to look into Prefetch files, find execution histories, and information regarding related files.
  - This helps us to find the programs used in attacks.
- Since we know the infection date/time, we will look around that time.

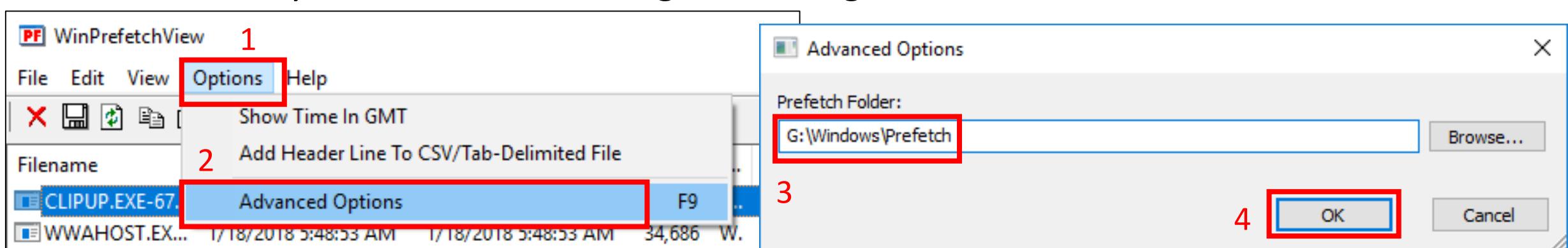
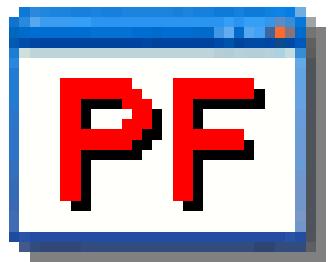


# Mounting E01 File

- In this exercise, we will be looking inside the E01 images.
- As we have done, open Arsenal Image Mounter from Shortcuts folder.
  - Shortcuts > 06\_LateralMovementsInvestigation > 0601\_ProgramExecutionArtifacts > ArsenallImageMounter.exe
  - Accept UAC when prompted.
- Say “OK” to the Arsenal Image Mounter splash screen.
- Mount **Client-Win10-2\_honda.E01** file with “**Write Temporary**” option.
  - The “\*.pf” files are in **%WinDir%\Prefetch** folder, where permission is necessary for opening.

# Using WinPrefetchView

- From the tools folder, open winprefetchview.exe.
- Once opened, the Prefetch contents for the running machine (Analysis Machine) is displayed. Select “Advanced Options” from “Options” menu.
  - Change the Prefetch Folder to G:\Windows\Prefetch.
  - See if you can find something interesting.



# Finding Suspicious Activities with WinPrefetchView

PF	WinPrefetchView	File	Edit	View	Options	Help	
Filename	Created Time	Modified Time	Size	Type	Path	Count	Last Run
CERTUTIL.EXE-4AEA2570(pf)	3/7/2018 4:13:00 PM	3/7/2018 4:13:	4,105	CERTUTIL.EXE	G:\Windows\SysWOW64\certutil.exe	1	3/7/2018 4:13:00 PM
EXPAND.EXE-CFADC4F4(pf)	3/7/2018 4:13:01 PM	3/7/2018 4:13:01 PM	4,105	EXPAND.EXE	G:\Windows\SysWOW64\expand.exe	1	3/7/2018 4:13:01 PM
REG.EXE-4978446A(pf)	3/7/2018 4:13:01 PM	3/7/2018 10:40:13 PM	2,723	REG.EXE	G:\Windows\SysWOW64\reg.exe	4	3/7/2018 10:40:13 PM
CMD.EXE-AC113AA8(pf)	3/7/2018 4:13:03 PM	3/23/2018 1:16:34 PM	4,510	CMD.EXE	G:\Windows\SysWOW64\cmd.exe	6	3/23/2018 1:16:34 PM
RUNDLL32.EXE-8592AB45(pf)	3/7/2018 4:13:12 PM	3/7/2018 4:13:12 PM	5,798	RUNDLL32.EXE	G:\Windows\SysWOW64\rundll32.exe	1	3/7/2018 4:13:12 PM
IPCONFIG.EXE-E1E46F7F(pf)	3/7/2018 10:36:07 PM	3/23/2018 12:50:13 PM	3,396	IPCONFIG.EXE	G:\Windows\SysWOW64\ipconfig.exe	50	3/23/2018 12:50:13 PM
POWERSHELL.EXE-767FB1AE(...)	3/7/2018 10:38:39 PM	3/7/2018 10:39:57 PM	29,459	POWERSHELL.EXE	G:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	2	3/7/2018 10:39:57 PM
SYSTEMINFO.EXE-254F8281(pf)	3/7/2018 10:39:47 PM	3/7/2018 10:39:47 PM	4,970	SYSTEMINFO.EXE	G:\Windows\SysWOW64\systeminfo.exe	1	3/7/2018 10:39:47 PM
WMIPRVSE.EXE-6768A320(pf)	3/7/2018 10:39:55 PM	3/7/2018 10:39:55 PM	3,036	WMIPRVSE.EXE	G:\Windows\SysWOW64\wmiprvse.exe	1	3/7/2018 10:39:55 PM
FIND.EXE-9AAADDA11(pf)	3/7/2018 10:40:13 PM	3/7/2018 10:40:13 PM	3,036	FIND.EXE	G:\Windows\SysWOW64\find.exe	1	3/7/2018 10:40:13 PM
NET.EXE-40D48057(pf)	3/7/2018 10:40:13 PM	3/20/2018 6:05:16	3,036	NET.EXE	G:\Windows\SysWOW64\net.exe	1	3/20/2018 6:05:16
NET1.EXE-3D280034(pf)	3/7/2018 10:40:19 PM	3/20/2018 6:05:16	3,036	NET1.EXE	G:\Windows\SysWOW64\net1.exe	1	3/20/2018 6:05:16
NETSTAT.EXE-981F3B53(pf)	3/7/2018 10:40:21 PM	3/7/2018 10:40:21 PM	3,036	NETSTAT.EXE	G:\Windows\SysWOW64\netstat.exe	1	3/7/2018 10:40:21 PM
WHOAMI.EXE-8229429D(pf)	3/8/2018 2:44:08 PM	3/8/2018 2:44:08 PM	3,036	WHOAMI.EXE	G:\Windows\SysWOW64\whoami.exe	1	3/8/2018 2:44:08 PM
NSLOOKUP.EXE-8DBC12C3(pf)	3/8/2018 2:44:43 PM	3/8/2018 2:44:43 PM	3,056	NSLOOKUP.EXE	G:\Windows\SysWOW64\nslookup.exe	1	3/8/2018 2:44:43 PM
W10.EXE-8C03A848(pf)	3/8/2018 2:49:48 PM	3/23/2018 1:16:34 PM	6,026	W10.EXE	G:\PROGRAMDATA\S\W10.EXE	8	3/23/2018 1:16:34 PM
SCHTASKS.EXE-AD598958(pf)	3/8/2018 2:49:48 PM	3/23/2018 1:06:25 PM	3,981	SCHTASKS.EXE	G:\Windows\SysWOW64\schtasks.exe	4	3/23/2018 1:06:25 PM

Start by sorting with “Created Time”, and look histories around the infection time (Mar 7 2018, 4:13 PM). As we have seen in the exploit analysis chapter, certutil.exe was used to decode the archive, expand.exe was used to expand the cab file, and rundll32.exe was executed from cmd.exe.

Few hours later, commands to obtain system information were executed.

Next day, a suspicious program “W10.exe” was executed. The path includes a folder with a single letter, and it was executed from ProgramData, which is not a common folder to execute a program from. This needs to be inspected.

# Windows Commands Abused by Attackers – JPCERT/CC

- One of the studies shows that legitimate Windows commands were often used by attackers.
  - Many of the commands you can find in the WinPrefetchView are also listed.

Table 1: Initial Investigation (Top 10 commands)

Ranking	Command	Times executed
1	tasklist	155
2	ver	95
3	ipconfig	76
4	systeminfo	40
5	net time	31
6	netstat	27
7	whoami	22
8	net start	16
9	qprocess	15
10	query	14

Table 2: Reconnaissance (Top 10 commands)

Ranking	Command	Times executed
1	dir	976
2	net view	236
3	ping	200
4	net use	194
5	type	120
6	net user	95
7	net localgroup	39
8	net group	20
9	net config	16
10	net share	11

<https://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html>

# Finding Programs in Unusual Paths

- Sort by “Process Path” to find unusual paths.
- ProgramData is not a typical path to install programs
- However, in addition to W10.exe, “DQ.EXE” and “L.EXE” were executed from the folder.

PF WinPrefetchView						
File	Edit	View	Options	Help		
Filename	Created Time	Modified Time	File Size	P..	Process Path	Run Counter
SETUP.EXE-58C5970D.pf	2/8/2018 5:56:21 PM	2/8/2018 5:56:21 PM	7,076	S..	G:\PROGRAMDATA\Adobe\Setup\{AC76BA86-...	1
L.EXE-38698459.pf	3/23/2018 1:17:33 PM	3/23/2018 1:18:13 PM	6,216	L..	G:\PROGRAMDATA\L.EXE	3
MPENGINE.EXE-F1D867B7.pf	1/29/2018 9:13:19 PM	1/29/2018 9:13:19 PM	1,964	M..	G:\PROGRAMDATA\MICROSOFT\WINDOWS D...	1
DQ.EXE-DB61C8B1.pf	3/14/2018 10:19:24 ...	3/14/2018 10:20:26 P...	7,612	D..	G:\PROGRAMDATA\S\DQ.EXE	2
W10.EXE-8C03A848.pf	3/8/2018 2:49:48 PM	3/23/2018 1:16:34 PM	6,026	W..	G:\PROGRAMDATA\S\W10.EXE	8
EVERNOTE.EXE-4B97C7E9.pf	2/8/2018 5:59:08 PM	2/19/2018 2:49:54 PM	31,894	E..	G:\Users\honda\AppData\Local\Apps\Evernote...	2
SOFTWARE_REPORTER_TOO...	3/9/2018 3:06:54 PM	3/9/2018 3:07:47 PM	6,286	S..	G:\USERS\HONDA\APPDATA\LOCAL\GOOGLE...	4
ONEDRIVE.EXE-03653C7F.pf	2/26/2018 12:12:15 ...	3/20/2018 6:30:09 PM	15,531	O..	G:\Users\honda\AppData\Local\MICROSOFT...	4
ATCS3230.TMP-44459076.pf	2/8/2018 5:56:02 PM	2/8/2018 5:56:02 PM	11,186	A..	G:\USERS\HONDA\APPDATA\LOCAL\TEMP\IS...	1
KEEPASS-2.38-SETUP.TMP-F...	2/8/2018 5:58:35 PM	2/8/2018 5:58:35 PM	10,581	K..	G:\USERS\HONDA\APPDATA\LOCAL\TEMP\IS...	1
VC_REDIST.X86.EXE-728D1F5...	1/30/2018 6:35:58 PM	1/30/2018 6:35:58 PM	12,066	V..	G:\USERS\HONDA\APPDATA\LOCAL\TEMP\{7...	1
VC_REDIST.X64.EXE-4B5E250...	1/30/2018 6:35:41 PM	1/30/2018 6:35:41 PM	13,058	V..	G:\USERS\HONDA\APPDATA\LOCAL\TEMP\{E...	1
INVOICE-MIYATA-20180319-...	3/19/2018 6:46:12 PM	3/19/2018 6:46:12 PM	17,449	I..	G:\USERS\HONDA\Desktop\INVOICE-MIYATA...	1
ORDERCONFIRMATION-MIY...	2/22/2018 11:13:42 ...	2/22/2018 11:13:42 A...	19,780	O..	G:\USERS\HONDA\Desktop\ORDERCONFIRM...	1
ORDERCONFIRMATION-MIY...	3/6/2018 5:54:07 PM	3/6/2018 5:54:07 PM	21,006	O..	G:\USERS\HONDA\Desktop\ORDERCONFIRM...	1
ORDERCONFIRMATION-MIY...	3/6/2018 5:15:49 PM	3/6/2018 5:15:49 PM	16,855	O..	G:\USERS\HONDA\Desktop\ORDERCONFIRM...	1
VC_REDIST.X64.EXE-407E6F90...	1/30/2018 6:35:34 PM	1/30/2018 6:35:34 PM	12,576	V..	G:\USERS\HONDA\Desktop\VC_REDIST.X64.EXE	1
Filename	Full Path	Device Path				
\$MFT	G:\Windows\System32\locale.nls	\VOLUME{01d396231a3999ae-b81c324b}\\$MFT				
AAAAAAAAAAAAAA...	G:\PROGRAMDATA\S\AAAAAAAAAAAAAAA...	\VOLUME{01d396231a3999ae-b81c324b}\PROGRAMDA...				
ADVAPI32.DLL	G:\Windows\SysWOW64\advapi32.dll	\VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SY...				
APPHHELP.DLL	G:\Windows\SysWOW64\apphelp.dll	\VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SY...				
BCRYPTPRIMITIVES.DLL	G:\Windows\SysWOW64\BCRYPTPRIMITIVES.DLL	\VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SY...				
BITSPROXY.DLL	G:\Windows\SysWOW64\BITSPROXY.DLL	\VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SY...				

# Findings from Prefetch File Contents

- Prefetch of L.EXE recorded several interesting files.
  - Refers to other EXE and BAT files in ProgramData folder.
  - “AAAAAAA...” file.

WinPrefetchView									
File	Edit	View	Options	Help					
File	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counter	Last Run Time	Missing Pr...	
L.EXE-38698459.pf	3/23/2018 1:17:33 PM	3/23/2018 1:18:13 PM	6,216	L.EXE	G:\PROGRAMDATA\L.EXE	3	3/23/2018 1:18:12 PM, 3/23/2018 1:17:47 PM...	Yes	
LAUNCHTM.EXE-56CAE1...	2/23/2018 11:29:35 AM	3/19/2018 6:53:17 PM	7,905	LAUNCHTM.EXE	G:\Windows\System32\LaunchTM.exe	4	3/19/2018 6:53:17 PM, 3/19/2018 6:52:47 PM...	No	
LOGONUI.EXE-09140401.pf	1/26/2018 6:49:47 AM	4/2/2018 5:08:25 PM	34,112	LOGONUI.EXE	G:\Windows\System32\LogonUI.exe	28	4/2/2018 5:08:14 PM, 3/20/2018 6:18:58 PM...	No	
MAVINJECT32.EXE-9364A...	2/8/2018 6:21:11 PM	3/23/2018 8:53:22 PM	4,062	MAVINJECT32.EXE	G:\PROGRAM FILES\MICROSOFT OFFICE 15\CLIENTX64\MAVINJE...	52	3/23/2018 8:53:22 PM, 3/22/2018 6:52:49 PM...	No	
MICROSOFTEDGE.EXE-53...	1/30/2018 6:34:30 PM	3/22/2018 4:38:55 PM	56,923	MICROSOFTEDGE...	G:\Windows\SYSTEMMAPPS\MICROSOFT.MICROSOFTEDGE_8WEK...	24	3/22/2018 4:38:45 PM, 3/20/2018 6:15:31 P...	No	
MICROSOFTEDGECP.EXE-...	1/30/2018 6:34:32 PM	3/23/2018 12:27:09 ...	81,281	MICROSOFTEDGE...	G:\Windows\SYSTEMMAPPS\MICROSOFT.MICROSOFTEDGE_8WEK...	88	3/23/2018 12:26:51 PM, 3/22/2018 6:51:02 P...	No	
MOBSYNC.EXE-C5E2284F...	1/26/2018 6:53:03 AM	3/20/2018 6:29:45 PM	7,081	MOBSYNC.EXE	G:\Windows\System32\mobsync.exe	17	3/20/2018 6:29:32 PM, 3/20/2018 6:02:03 P...	No	
File	Full Path	Device Path	Index						
\$MET	G:\PROGRAMDATA\WINDOWS\SYSTEM32\TAPI2.DLL	\VOLUME(01d396231a3999ae-b81c324b)\\$MET	43						
7.EXE	G:\PROGRAMDATA\S\7.EXE	\VOLUME(01d396231a3999ae-b81c324b)\PROGRAMDATA\S\7.EXE	44						
AAAAAAAAAAAAAAAAAAAAAA	G:\PROGRAMDATA\S\AAAAAAAAAAAAAAAAAAAAAA	\VOLUME(01d396231a3999ae-b81c324b)\PROGRAMDATA\S\AAAAAAAAAAAAAAAAAAAAAA	45						
AD.BAT	G:\PROGRAMDATA\S\AD.BAT	\VOLUME(01d396231a3999ae-b81c324b)\PROGRAMDATA\S\AD.BAT	46						
ADVAPI32.DLL	G:\Windows\SYSWOW64\advapi32.dll	\VOLUME(01d396231a3999ae-b81c324b)\WINDOWS\SYSWOW64\ADVAPI32.DLL	31						
APP	G:\PROGRAMDATA\S\7.EXE	\VOLUME(01d396231a3999ae-b81c324b)\PROGRAMDATA\S\7.EXE							
BCR	G:\PROGRAMDATA\S\AAAAAAAAAAAAAA	\VOLUME(01d396231a3999ae-b81c324b)\PROGRAMDATA\S\AAAAAAAAAAAAAA							
BCR	G:\PROGRAMDATA\S\AD.BAT	\VOLUME(01d396231a3999ae-b81c324b)\PROGRAMDATA\S\AD.BAT							
C_12									
CFG									
CON									
COM									
COMLOG32.VCL	G:\Windows\SYSWOW64\comargs32.dll	\VOLUME(01d396231a3999ae-b81c324b)\WINDOWS\SYSWOW64\COMLOG32.VCL							
CRYPTBASE.DLL	G:\Windows\SYSWOW64\CRYPTBASE.DLL	\VOLUME(01d396231a3999ae-b81c324b)\WINDOWS\SYSWOW64\CRYPTBASE.DLL							
CRYPTSP.DLL	G:\Windows\SysWOW64\cryptsp.dll	\VOLUME(01d396231a3999ae-b81c324b)\WINDOWS\SysWOW64\cryptsp.dll							
DQ.EXE	G:\PROGRAMDATA\S\DQ.EXE	\VOLUME(01d396231a3999ae-b81c324b)\PROGRAMDATA\S\DQ.EXE							
G.BAT	G:\PROGRAMDATA\S\G.BAT	\VOLUME(01d396231a3999ae-b81c324b)\PROGRAMDATA\S\G.BAT							
G.LOG	G:\PROGRAMDATA\S\G.LOG	\VOLUME(01d396231a3999ae-b81c324b)\PROGRAMDATA\S\G.LOG							
GD32.DLL	G:\Windows\SYSWOW64\gd32.dll	\VOLUME(01d396231a3999ae-b81c324b)\WINDOWS\SYSWOW64\gd32.dll							
GD32FULL.DLL	G:\Windows\SysWOW64\gd32full.dll	\VOLUME(01d396231a3999ae-b81c324b)\WINDOWS\SysWOW64\gd32full.dll							
IMM32.DLL	G:\Windows\SysWOW64\imm32.dll	\VOLUME(01d396231a3999ae-b81c324b)\WINDOWS\SysWOW64\imm32.dll							
KERNELAPPCORE.DLL	G:\Windows\SysWOW64\KERNELAPPCORE.DLL	\VOLUME(01d396231a3999ae-b81c324b)\WINDOWS\SysWOW64\KERNELAPPCORE.DLL							
KERNEL32.DLL	G:\Windows\System32\kernel32.dll	\VOLUME(01d396231a3999ae-b81c324b)\WINDOWS\System32\kernel32.dll							
KERNEL32.DLL	G:\Windows\SysWOW64\kernel32.dll	\VOLUME(01d396231a3999ae-b81c324b)\WINDOWS\SYSWOW64\kernel32.dll							
KERNELBASE.DLL	G:\Windows\SysWOW64\kernelbase.dll	\VOLUME(01d396231a3999ae-b81c324b)\WINDOWS\SysWOW64\kernelbase.dll							
L.EXE	G:\PROGRAMDATA\L.EXE	\VOLUME(01d396231a3999ae-b81c324b)\PROGRAMDATA\L.EXE							

# Findings From the Prefetch

- Infection occurred around 4:13 PM on March 7.
- Legitimate Windows commands for retrieving system information were executed starting at 10:36 PM on March 7, and also on March 8.
- Some activities were also found on March 14 and 23.
- Suspicious files existed in paths such as “ProgramData” and “ProgramData\s”
  - L.exe, W10.exe, 7.exe, G.bat, G.log, DQ.exe, AD.BAT, AAAAAAAAAAAAAAAA...

# Quick Demo: Looking into Prefetch Files for Client-Win10-1

# Quick Demo: Looking into Prefetch Files for Client-Win10-1

- Next, we will check Prefetch contents of **Client-Win10-1\_toyoda.E01** file.

# Findings from Prefetch Files

- Similar to client-win10-2, the following points may be found.
  - A folder with single letter.
  - An executable file residing under ProgramData, which can be modified by non-privileged users.
    - “ProgramData\I” in here.
  - Suspicious reference to “AAAAAAAAAAA...” file
  - Since legitimate Windows commands were executed from SysWOW64, a 32-bit program must have executed them.

The screenshot shows the WinPrefetchView application interface. It consists of two vertically stacked tables. The top table has columns for Filename, Created Time, Modified Time, File Size, Process ID, and Process Path. The bottom table has columns for Filename, Full Path, Device Path, and Index. Both tables show various system files and executables. In the bottom table, the row for 'AAAAAAAAAAA...' is highlighted with a red box.

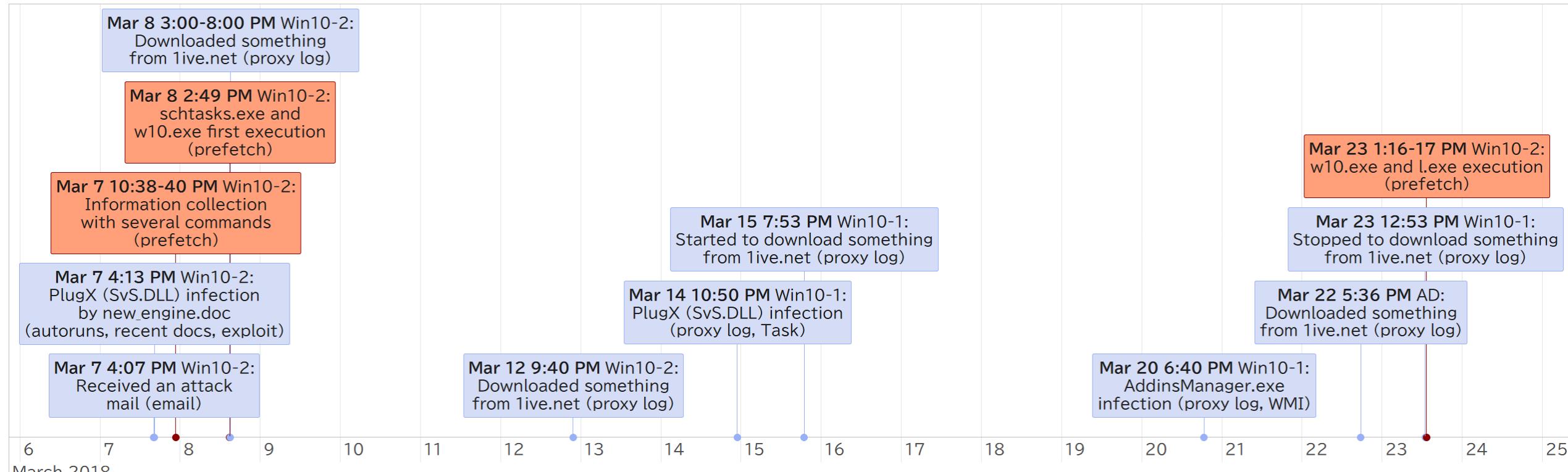
Filename	Created Time	Modified Time	File ...	P...	Process Path
UPDATER.EXE-E...	3/14/2018 1:37:04 PM	3/20/2018 5:32:29 PM	4,741	U...	G:\PROGRAM FILES\MOZILLA FIREFOX\up...
SESSIONMSG.E...	3/14/2018 10:36:20 PM	3/14/2018 10:36:20 PM	12,844	S...	G:\Windows\System32\SESSIONMSG.EXE
W10.EXE-21E6C...	3/14/2018 10:50:28 PM	3/14/2018 10:50:28 PM	5,629	W...	G:\PROGRAMDATA\I\W10.EXE
CMD.EXE-AC11...	3/14/2018 10:50:29 PM	3/14/2018 10:50:29 PM	2,927	C...	G:\Windows\SysWOW64\cmd.exe
WUAPIHOST.EX...	3/14/2018 11:56:20 PM	4/2/2018 12:56:26 PM	4,064	W...	G:\Windows\System32\WUAPIHOST.EXE
INSTALLAGENT...	3/14/2018 11:59:03 PM	4/2/2018 12:53:33 PM	8,590	I...	G:\Windows\System32\INSTALLAGENTUSE...
DEFRAG.EXE-58...	3/15/2018 2:43:45 PM	3/31/2018 10:12:46 AM	3,997	D...	G:\Windows\System32\Defrag.exe

Filename	Full Path	Device Path	Index
SMFT	G:\Windows\SysWOW64\shlwapi.dll	\VOLUME{01d38fd2272f8efd-7e293eb...}	29
AAAAAAAAAAA...	G:\PROGRAMDATA\I\AAAAAAAAAAA...	\VOLUME{01d38fd2272f8efd-7e293eb...}	42
ADVAPI32.DLL	G:\Windows\SysWOW64\advapi32.dll	\VOLUME{01d38fd2272f8efd-7e293eb...}	13
APPHelp.dll	G:\Windows\SysWOW64\apphelp.dll	\VOLUME{01d38fd2272f8efd-7e293eb...}	11
BCRYPTPRIMITIVES.DLL	G:\Windows\SysWOW64\BCRYPTPRI...	\VOLUME{01d38fd2272f8efd-7e293eb...}	19
BITSPROXY.DLL	G:\Windows\SysWOW64\BITSPROXY....	\VOLUME{01d38fd2272f8efd-7e293eb...}	45
C_1252.NLS	G:\Windows\System32\C_1252.NLS	\VOLUME{01d38fd2272f8efd-7e293eb...}	37
CLBCATQ.DLL	G:\Windows\SysWOW64\clbcatq.dll	\VOLUME{01d38fd2272f8efd-7e293eb...}	39

# Information Obtained from Prefetch

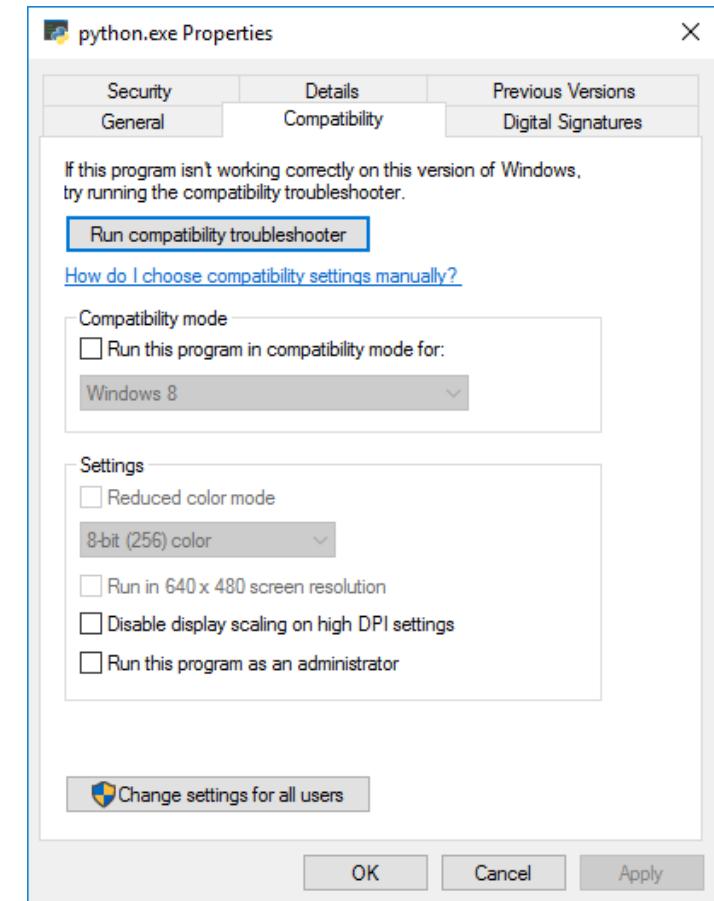
- Execution of various commands and executable files were found on Client-Win10-2.
- Execution of some commands on Client-Win10-1 can be also confirmed from the Prefetch.



# Shimcache

# Shimcache

- Since Windows XP, Windows has “application compatibility” feature.
- Shimcache is stored in registry as a binary value “AppCompatCache” under **“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache” key.**
  - To get the Shimcache, you will need to extract the “SYSTEM” registry hive.



# Contents of Shimcache

- What you can find from a record of Shimcache includes:
  1. Path of the program
  2. Last **modified** timestamp of the program
    - Note that this is not the execution time.
  3. Flag whether the program has been executed or not (Windows Vista+ have this flag, but the flag is always false on Windows 10)
- Shimcache remains even if the original EXE was deleted.

ControlSet	CacheEntryPosition	Path	LastModifiedTimeUTC	Executed
● 1	18	C:\Bitnami\redmine-3.4.4-2\apps\redmine\scripts\winserv.exe	2017-02-27 09:04:34	NA
● 1	19	C:\Windows\system32\chcp.com	2016-07-16 11:42:45	NA
● 1	20	C:\Windows\SysWOW64\chcp.com	2016-07-16 11:42:45	NA
● 1	21	C:\Bitnami\REDMIN~1.4-2\mysql\bin\mysql.exe	2017-12-09 07:50:20	NA
● 1	22	C:\Bitnami\REDMIN~1.4-2\ruby\bin\ruby.exe	2016-12-02 19:03:48	NA
● 1	23	C:\Bitnami\redmine-3.4.4-2\ruby\bin\ruby.exe	2016-12-02 19:03:48	NA

# Characteristics of ShimCache

- We cannot tell program execution dates, but they are registered by reverse order of program execution.
- Programs executed with SYSTEM privilege are also recorded.
- Execution of BAT files may also be recorded in some conditions.
- If the machine was shut down inappropriately, ShimCache would not be flushed to the registry HIVE like other registry data, but it's only written to the journal LOG files.
  - In that case, tools that can parse the LOG files become necessary.
    - Yarp
    - Registry Explorer

# Characteristics of ShimCache (Cont.)

- A Shimcache entry for a certain binary that is already stored on Shimcache will be inserted again after the binary is modified and then executed. Otherwise, it won't happen again.
- Note that Shimcache may record not executed binaries at the following case.

*Simply viewing the directory in the GUI that the extracted but not executed executable was in was enough to get it added to the shimcache*

<https://www.hecfblog.com/2018/11/daily-blog-544-forensic-lunch-test.html>

# Tips for Analyzing ShimCache

- Order of the records is important.
  - Do not sort them with timestamps or other columns.
  - Timestamps are “Modified Time”, and NOT the “Execution Time”.
  - Newer entries are recorded first, and the oldest are the last.
    - You can reverse the sort order to see it in chronological order.
  - You can also sort them with file paths to find suspicious paths.
- We should use other artifacts that have timestamps, such as Prefetch, UserAssist, AmCache or file system metadata of the command, to point out the exact time or the time range of execution timeframe.
- You may be able to trust the timestamps in ShimCache in a few cases.
  - If a program is executed from a temporary folder, it may be an installer program. In this case, the file execution time may become equal to the modification time.
    - Entries between such programs were executed at some time within that time frame.
  - Or when a BAT file created and executed repeatedly and periodically.
    - You could estimate the program execution times by observing ShimCache of those programs.

# Comparing with Prefetch

- Pros:
  - Shimcache is able to record entries even when programs were executed as SYSTEM privilege while Prefetch may not be able to record.
  - Both Prefetch and Shimcache can record executables that are not executed from the Explorer process.
  - Shimcache can record entries even where corresponding executables are located in external SMB servers while Prefetch doesn't.
  - Execution of BAT files may also be recorded while Prefetch doesn't.
- Cons:
  - Shimcache doesn't have the exact execution timestamps while Prefetch has multiple timestamps.
  - Shimcache doesn't tell the number of times which the programs were executed while Prefetch stores the number of times.

# Viewing Shimcache

- Since Shimcache is in binary format, it is difficult for the ordinary humans to read it without a parser.
- Many parsers are included in the analysis environment:
  - AppCompatCache Parser by Eric Zimmerman
  - ShimCacheParser.py
    - The tool does not run with Python 3.x
  - RegRipper
  - Registry Explorer
  - ...
- In this exercise, we will use AppCompatCache Parser.

# Scenario 1 Labs:

## Lab 2: Looking into ShimCache for Client-Win10-2

# Looking into ShimCache

- Looking into ShimCache may give us information about the programs that were executed, and the programs that were already deleted from the computer.
- The goal of the exercise is to find those artifacts.
  - Try to find something that was not found in Prefetch.
- We will assume that you are still mounting client-win10-2 onto drive G of the analysis machine.
  - If you have unmounted it since the previous exercise, please remount it.

# Running AppCompatCache Parser

- Execute Command Prompt as administrator.
  - SYSTEM hive on the mounted image is not readable due to permissions.
    - Workarounds: open the folder once using Windows Explorer and obtain permissions, or copy the SYSTEM hive to somewhere the analyzing user can read (e.g. Desktop).
    - To make it easier, we will run the tool as administrator.
- Run AppCompatCache Parser. Enter the following in a single line:

```
AppCompatCacheParser.exe -f G:\Windows\System32\config\SYSTEM  
--csv %USERPROFILE%\Desktop
```
- This parses SYSTEM hive from G:\Windows\System32\config and creates output file to the user's Desktop.

# Preparation for Shimcache Analysis

- Open the AppCompatCachParser's result with CSVFileView or your favorite CSV viewer. Then reverse sort with CacheEntryPosition by clicking the header of the column **twice** so that you can look the result as chronological order.

ControlSet	CacheEntryPosition	Path	LastModifiedTi...	Executed
1	459	C:\Windows\s...	2016-07-16 11:...	NA
1	458	C:\Windows\s...	2016-07-16 11:...	NA
1	457	C:\Windows\s...	2016-07-16 11:...	NA
1	456	C:\Windows\s...	2016-07-16 11:...	NA
1	455	C:\Windows\s...	2016-07-16 11:...	NA

- Then, press “Ctrl + F” and search “systeminfo”.

# Running PEcmd to Compare

- Execute Command Prompt as administrator.
  - To compare the AppComaptCacheParser's result with Prefetch, execute PEcmd.

```
PECmd.exe -d G:\Windows\Prefetch --csv %USERPROFILE%\Desktop
```

- This parses Prefetch folder on G drive and creates output file to the user's Desktop.
  - -d: An option to specify Prefetch folder
  - --csv: the output folder for the result as a csv format

# The Output of PEcmd

- After execution, you can find the result files in the current folder, which was specified with --csv option.

 20190601042926_PECmd_Output.csv	6/1/2019 1:29 PM	OpenOffice.org 1....	1,804 KB
 20190601042926_PECmd_Output_Timeline.csv	6/1/2019 1:29 PM	OpenOffice.org 1....	84 KB

- Let's open the file ending with "\_Timeline.csv" with CSVFileView or your favorite csv viewer. In this file, Last Run Time entries are split into each line.
- Another file is an output for parsed records of prefetch files. It is similar to the one of WinPrefetchView.

# Preparation for This Exercise

- Click “RunTime” once to sort by executed date. And press “Ctrl + F”, then search “systeminfo”.

RunTime	ExecutableName
2018-03-07 13:38:29	\VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\WINDOWSPOWERSHE...
2018-03-07 13:39:40	\VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\SYSTEMINFO.EXE
2018-03-07 13:39:44	\VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\WBEM\WMIPRVSE.EXE
2018-03-07 13:39:47	\VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\WINDOWSPOWERSHE...
2018-03-07 13:39:56	\VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSTEM32\MSIEXEC.EXE
2018-03-07 13:40:12	\VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\REG.EXE
2018-03-07 13:40:13	\VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\REG.EXE
2018-03-07 13:40:13	\VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\REG.EXE
2018-03-07 13:40:13	\VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\FIND.EXE
2018-03-07 13:40:13	\VOLUME{01d396231a3999ae-b81c324b}\WINDOWS\SYSWOW64\FIND.EXE

Path	LastModifiedTime...			
77 C:\Windows\SysW... ShimCache	2016-07-16 11:42:49	2018-03-07 07:13:02	\W	Prefetch(PECmd) EXE
76 C:\Windows\SysW...	2016-07-16 11:42:49	2018-03-07 13:36:07	\W	EXE
75 C:\Windows\system32\systeminfo.exe	2016-07-16 11:43:04	2018-03-07 13:38:29	\WINDOWS\SYSWOW64\WINDOWSPOWERSHELL\V1	
74 C:\Windows\SysWoW64\systeminfo.exe	2016-07-16 11:43:04	2018-03-07 13:39:40	\WINDOWS\SYSWOW64\SYSTEMINFO.EXE	
73 C:\Windows\sysWOW64\wbem\wmiprvse.e...	2016-07-16 11:42:56	2018-03-07 13:39:44	\WINDOWS\SYSWOW64\WBEM\WMIPRVSE.EXE	
72 C:\Windows\system32\find.exe	2016-07-16 11:42:45	2018-03-07 13:39:47	\WINDOWS\SYSWOW64\WINDOWSPOWERSHELL\V1	
71 C:\Windows\SysWoW64\find.exe	2016-07-16 11:42:45	2018-03-07 13:39:56	\WINDOWS\SYSTEM32\MSIEXEC.EXE	
70 C:\Windows\system32\net.exe	2016-07-16 11:42:49	2018-03-07 13:40:12	\WINDOWS\SYSWOW64\REG.EXE	
69 C:\Windows\SysWoW64\net.exe	2016-07-16 11:42:49	2018-03-07 13:40:13	\WINDOWS\SYSWOW64\FIND.EXE	
68 C:\Windows\system32\net1.exe	2016-07-16 11:42:49	2018-03-07 13:40:13	\WINDOWS\SYSWOW64\FIND.EXE	
67 C:\Windows\SysWoW64\net1.exe	2016-07-16 11:42:49	2018-03-07 13:40:13	\WINDOWS\SYSWOW64\FIND.EXE	
66 C:\Windows\system32\NETSTAT.EXE	2016-07-16 11:42:49	2018-03-07 13:40:13	\WINDOWS\SYSWOW64\REG.EXE	
65 C:\Windows\SysWoW64\NETSTAT.EXE	2016-07-16 11:42:49	2018-03-07 13:40:13	\WINDOWS\SYSWOW64\REG.EXE	
64 C:\Windows\system32\whoami.exe	2016-07-16 11:42:46	2018-03-07 13:40:21	\WINDOWS\SYSWOW64\IPCONFIG.EXE	
63 C:\Windows\SysWoW64\whoami.exe	2016-07-16 11:42:46	2018-03-07 13:40:21	\WINDOWS\SYSWOW64\NET.EXE	
62 C:\Windows\system32\nslookup.exe	2016-07-16 11:42:46	2018-03-07 13:40:21	\WINDOWS\SYSWOW64\NET1.EXE	
61 C:\Windows\SysWoW64\nslookup.exe	2016-07-16 11:42:46	2018-03-07 13:40:21	\WINDOWS\SYSWOW64\NET1.EXE	
60 C:\ProgramData\s\w10.exe	2018-02-05 05:31:46	2018-03-07 13:40:21	\WINDOWS\SYSWOW64\NET1.EXE	
59 C:\Windows\system32\cscript.exe	2016-07-16 11:42:37	2018-03-07 13:40:21	\WINDOWS\SYSWOW64\NETSTAT.EXE	
		2018-03-08 03:19:35	\PROGRAM FILES\VMWARE\VMWARE TOOLS\VMWA	
		2018-03-08 03:33:19	\WINDOWS\SYSTEM32\SVCHOST.EXE	
		2018-03-08 03:33:19	\WINDOWS\SYSTEM32\WERFAULT.EXE	
		2018-03-08 03:52:03	\PROGRAM FILES\MICROSOFT OFFICE 15\ROOT\OF	
		2018-03-08 03:57:31	\PROGRAM FILES (X86)\ADOBE\ACROBAT READER I	
		2018-03-08 03:57:31	\WINDOWS\SYSWOW64\PREVHOST.EXE	
		2018-03-08 03:57:32	\PROGRAM FILES (X86)\ADOBE\ACROBAT READER I	
		2018-03-08 05:44:08	\WINDOWS\SYSWOW64\WHOAMI.EXE	
		2018-03-08 05:44:33	\WINDOWS\SYSWOW64\NSLOOKUP.EXE	
		2018-03-08 05:49:47	\PROGRAMDATA\S\W10.EXE	
		2018-03-08 05:49:48	\WINDOWS\SYSWOW64\SCHTASKS.EXE	
		2018-03-08 05:49:48	\PROGRAMDATA\S\W10.EXE	
		2018-03-08 05:56:40	\WINDOWS\SYSTEM32\DEFRAG.EXE	

Let's start analysis based on the line of systeminfo. From the ShimCache, it seems that cscript.exe was executed after W10.EXE was executed on client-win10-2.

## ShimCache

61	C:\Windows\SysWoW64\nslookup.exe	2016-07-16 11:42:4
60	C:\ProgramData\s\w10.exe	2018-02-05 05:31:4
59	C:\Windows\system32\cscript.exe	2016-07-16 11:42:3
58	C:\Users\honda\AppData\Local\Google\Chrome\User Data\SwReporter\25.141.202\software_reporter_tool.exe	2018-01-31 04:49:5
57	C:\Program Files (x86)\Google\Update\1.3.33.7\GoogleUpdateBroker.exe	2018-02-08 08:58:2
56	C:\Program Files (x86)\Google\Update\Install\{C2B0CB92-7DE6-4F7C-8963-242408D085FF}\65.0.3325.146_64.0.3282.18...	2018-03-06 10:32:4
55	C:\Program Files (x86)\Google\Update\Install\{C2B0CB92-7DE6-4F7C-8963-242408D085FF}\65.0.3325.146_64.0.3282.18...	2018-03-07 04:24:2

We found that cscript.exe was executed in between  
Mar 8 2:49 PM in JST (UTC+9:00) and Mar 9 3:06 PM  
by combining with the Prefetch result.

## Prefetch(PECmd)

	WS\SYSWOW64\NSLOOKUP.EXE	
2018-03-08 05:49:47	\PROGRAMDATA\SW10.EXE	
2018-03-08 05:49:48	\WINDOWS\SYSWOW64\SCHTASKS.EXE	
2018-03-08 05:49:48	\PROGRAMDATA\SW10.EXE	
2018-03-08 05:56:40	\WINDOWS\SYSTEM32\DEFRAG.EXE	
2018-03-08 06:00:08	\WINDOWS\SYSTEM32\WINDOWSPowershell\v1.0\POWERSHELL.EXE	
2018-03-08 07:00:01	\WINDOWS\SYSTEM32\WINDOWSPowershell\v1.0\POWERSHELL.EXE	
2018-03-08 08:00:01	\WINDOWS\SYSTEM32\WINDOWSPowershell\v1.0\POWERSHELL.EXE	
2018-03-08 09:00:02	\WINDOWS\SYSTEM32\WINDOWSPowershell\v1.0\POWERSHELL.EXE	
2018-03-08 10:00:00	\WINDOWS\SYSTEM32\WINDOWSPowershell\v1.0\POWERSHELL.EXE	
2018-03-08 11:00:00	\WINDOWS\SYSTEM32\CMD.EXE	
	(snip)	
2018-03-09 06:06:21	\PROGRAMDATA\MOZILLA FIREFOX\FIREFOX.EXE	
2018-03-09 06:06:40	\USERS\HONDA\APPDATA\LOCAL\GOOGLE\CHROME\USER DATA\SWREPORTER\25.141.202\SOFTWARE REPORTER	
2018-03-09 06:06:43	\USERS\HONDA\APPDATA\LOCAL\GOOGLE\CHROME\USER DATA\SWREPORTER\25.141.202\SOFTWARE_REPORTER	
2018-03-09 06:06:50	\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE	
2018-03-09 06:06:55	\PROGRAM FILES (X86)\GOOGLE\UPDATE\1.3.33.7\GOOGLEUPDATEBROKER.EXE	

# ShimCache

61	C:\Windows\SysWoW64\nslookup.exe	2016-07-16 11:42:4
60	C:\ProgramData\s\w10.exe	2018-02-05 05:31:4
59	C:\Windows\system32\cscript.exe	2016-07-16 11:42:3
58	C:\Users\honda\AppData\Local\Google\Chrome\User Data\SwReporter\25.141.202\software_reporter_tool.exe	2018-01-31 04:49:5
57	C:\Program Files (x86)\Google\Update\1.3.33.7\GoogleUpdateBroker.exe	2018-02-08 08:58:2
56	C:\Program Files (x86)\Google\Update\Install\{C2B0CB92-7DE6-4F7C-8963-242408D085FF}\65.0.3325.146_64.0.3282.18...	2018-03-06 10:32:4
55	C:\Program Files (x86)\Google\Update\Install\{C2B0CB92-7DE6-4F7C-8963-242408D085FF}\65.0.3325.146_64.0.3282.18...	2018-03-07 04:04:2

## Prefetch(PECmd)

	WS\SYSWOW64\NSLOOKUP.EXE
2018-03-08 05:49:47	\PROGRAMDATA\SW10.EXE
2018-03-08 05:49:48	\WINDOWS\SYSWOW64\SCHTASKS.EXE
2018-03-08 05:49:48	\PROGRAMDATA\SW10.EXE
2018-03-08 05:56:40	\WINDOWS\SYSTEM32\DEFFRAG.EXE
2018-03-08 06:00:08	\WINDOWS\SYSTEM32\WINDOWSPowershell\v1.0\POWERSHELL.EXE
2018-03-08 07:00:01	\WINDOWS\SYSTEM32\WINDOWSPowershell\v1.0\POWERSHELL.EXE
2018-03-08 08:00:01	\WINDOWS\SYSTEM32\WINDOWSPowershell\v1.0\POWERSHELL.EXE
2018-03-08 09:00:02	\WINDOWS\SYSTEM32\WINDOWSPowershell\v1.0\POWERSHELL.EXE
2018-03-08 10:00:00	\WINDOWS\SYSTEM32\WINDOWSPowershell\v1.0\POWERSHELL.EXE
2018-03-08 11:00:00	\WINDOWS\SYSTEM32\CMD.EXE

w10.exe executed scbtasks.exe and w10.exe itself. And then, powershell.exe was executed every hour until 7:00 PM by Task Scheduler. And cscript.exe was related to the activities. It means that cscript was executed via Powershell by Task Scheduler. In order to confirm it, you should check Windows Event logs.

# The Result of ShimCache Analysis for Client-Win10-2

- cscript.exe was executed after W10.EXE
  - cscript.exe is a program used for executing VBScript and Jscript with SYSTEM privilege in between **Mar 8 2:49 PM** in JST (UTC+9:00) and **Mar 9 3:06 PM**.
  - However, the cscript.exe isn't 32-bit binary, but 64-bit. It is likely that the file was executed by task scheduler with SYSTEM privilege or by chance at that moment.
- If we could find the script along with W10.EXE, we may be able to investigate more details.

# Scenario 1 Labs:

## Lab 3: Looking into ShimCache for Client-Win10-1

# Looking into ShimCache for Client-Win10-1

- We will assume that the OS volume of client-win10-1 is mounted to drive I.
  - If you unmounted it after the previous exercise, please remount it.
- We will compare ShimCache with Prefetch to see if entries that did not remain in Prefetch are remaining.

# Running AppCompatCache Parser

- Run AppCompatCache Parser. Enter the following in a single line:

```
AppCompatCacheParser.exe -f I:\Windows\System32\config\SYSTEM  
--csv %USERPROFILE%\Desktop
```

- This parses SYSTEM hive from I:\Windows\System32\config and creates an output file to the user's Desktop.
  - f: An option to specify the SYSTEM HIVE
  - csv: the output folder for the result as a csv format

# Running PEcmd to Compare

- Execute Command Prompt as administrator.
  - To compare the AppComaptCacheParser's result with Prefetch, execute PEcmd.

```
PEcmd.exe -d I:\Windows\Prefetch --csv %USERPROFILE%\Desktop
```

- This parses Prefetch folder on I drive and creates output file to the user's Desktop.
  - -d: An option to specify Prefetch folder
  - --csv: the output folder for the result as a csv format

# Preparation for the Analysis

- The same way as the previous exercise, let's open the output file of the PEcmd ending with "\_Timeline.csv" and sort by RunTime.
- Open the output file of the AppCompatCache Parser and reverse-sort by the CacheEntryPosition.
- Then, search w10.exe.

# Findings from ShimCache

- 32-bit cmd.exe, ipconfig.exe, and whoami.exe are recorded.
- From the prefetch results, w10.exe and cmd.exe were executed at March 14 10:50 PM (in JST:UTC+9:00) and atbroker.exe was executed at March 15 6:21 PM (in JST:UTC+9:00).
- Some temporary files were executed at March 19, 2018 on 7:04 PM (in JST:UTC+9:00). Therefore, ipconfig.exe and whoami.exe should be executed in between March 15 6:21 PM and March 19, 2018 on 7:04 PM.

	Path	ShimCache	LastModifiedTime...	ExecutionTime...	Prefetch(PECmd)	File Path
39	C:\Users\ninja-rdp\AppData\Local\Microsoft\OneDri...		2018-03-14 13:39:20	2018-03-14 13:50:26	\PROGRAMDATA\\W10.EXE	M32\BACKGROUNDDA
38	C:\ProgramData\w10.exe		2018-02-05 07:21:48	2018-03-14 13:50:28	\WINDOWS\SYSWOW64\CMD.EXE	
37	C:\Windows\SysWoW64\cmd.exe		2016-07-16 11:43:01	2018-03-14 13:50:28	\PROGRAMDATA\\W10.EXE	
36	C:\Windows\system32\atbroker.exe		2016-07-16 11:42:20	2018-03-14 13:52:42	\WINDOWS\SYSTEM32\DLLHOST.EXE	
35	C:\Windows\SysWoW64\ipconfig.exe		2016-07-16 11:42:49	2018-03-14 13:52:51	\WINDOWS\SYSTEM32\LOGONUI.EXE	
34	C:\Windows\SysWoW64\whoami.exe		2016-07-16 11:42:46	2018-03-15 05:43:43	\WINDOWS\SYSTEM32\DEFrag.EXE	
33	C:\Users\toyoda\Downloads\python-3.6.4-amd64.exe		2018-03-19 10:04:10	2018-03-15 09:21:23	\WINDOWS\SYSTEM32\SVCHOST.EXE	
32	C:\Users\toyoda\AppData\Local\Temp\{9EBE94CA-7...		2018-03-19 10:04:12	2018-03-15 09:21:25	\WINDOWS\SYSTEM32\DLLHOST.EXE	
						PROGRAM FILES\WINDOWS DEFENDER

# Estimating Execution Time from Nearby Entries

- AddinsManager.exe is malware that was found on client-win10-1. This is recorded in WMI, but the following output suggests that mofcomp command was used for registering the malware.
- We already know that AddinsManager.exe infected the client March 20, 2018 on 6:40 PM. Therefore, WMI must have been registered sometime between March 20, 2018 on 6:22 PM (in JST:UTC+9:00) and March 20, 2018 on 6:40 PM.

	Path	LastModifiedTime...	Executed
25	C:\Users\toyoda\Downloads\TerminalsSetup_4.0.1.msi	2018-03-20 09:22:38	NA
24	C:\Program Files (x86)\Terminals\Terminals.exe	2017-06-24 00:00:24	NA
23	C:\Windows\System32\Wbem\mofcomp.exe	2016-07-15 11:42:56	NA
22	C:\Windows\SysWoW64\Wbem\mofcomp.exe	2016-07-15 11:42:56	NA
21	C:\Windows\addons\AddinsManager.exe	2016-06-13 05:41:28	NA
20	C:\Progr AddinsManager.exe infected the client March 20, 2018 on 6:40 PM		
19	C:\Program Files (x86)\Google\Chrome\Application\...	2018-03-13 19:46:20	NA
18	C:\Windows\TEMP\CR_CAC90.tmp\setup.exe	2018-03-21 07:46:07	NA

# Findings from ShimCache

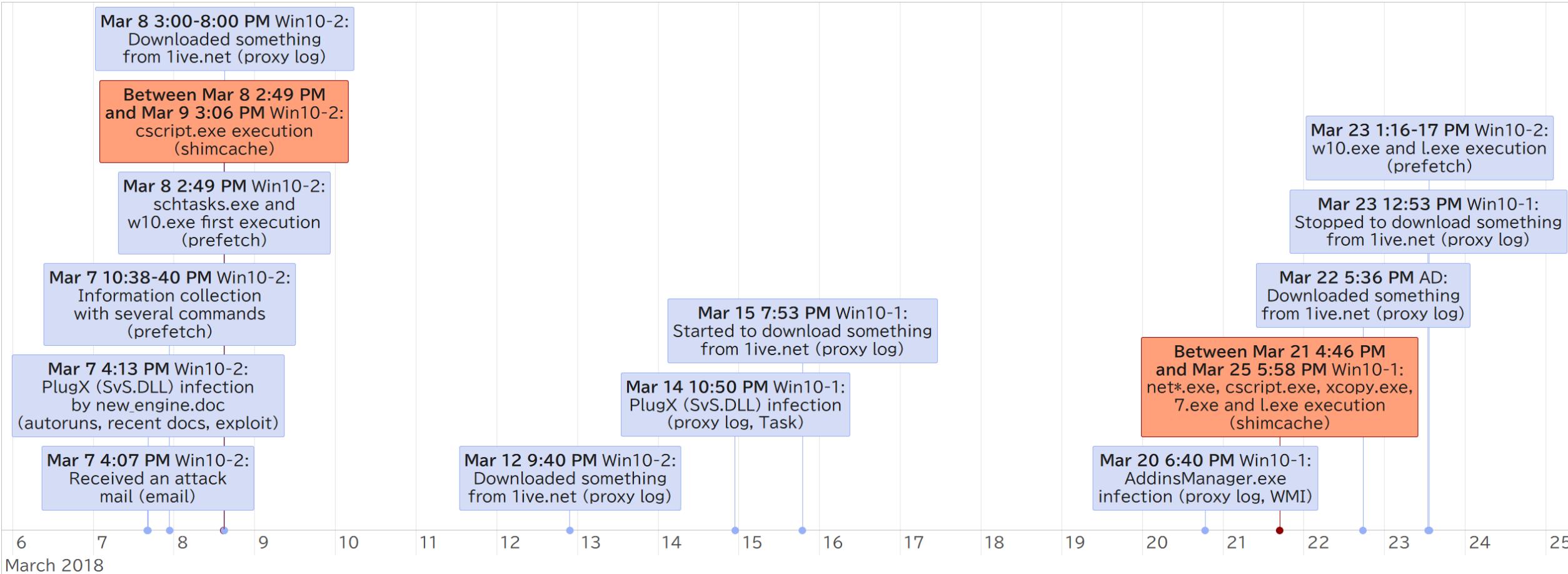
- 32-bit net\*.exe, cscript.exe, and xcopy.exe are recorded.
  - Something may have been copied from the computer.
- Programs named with a single letter, such as 7.exe and l.exe, are recorded right after that.
  - Might be related to the attacks.
- Temporary files indicate that the programs were executed at some time between March 21, 2018 on 4:46 PM (in JST:UTC+9:00) and March 25, 2018 on 5:58 PM.

	Path	LastModifiedTime...	Executed
19	C:\Program Files (x86)\Google\Chrome\Application\...	2018-03-13 19:46:20	NA
18	C:\Windows\TEMP\CR_CAC90.tmp\setup.exe	2018-03-21 07:46:07	NA
17	C:\Windows\SysWoW64\net.exe	2016-07-16 11:42:49	NA
16	C:\Windows\SysWoW64\net1.exe	2016-07-16 11:42:49	NA
15	C:\Windows\SysWoW64\cscript.exe	2016-07-16 11:43:02	NA
14	C:\Windows\SysWoW64\xcopy.exe	2016-07-16 11:42:49	NA
13	C:\ProgramData\s\7.exe	2016-10-04 15:12:28	NA
12	C:\ProgramData\l.exe	2017-06-30 03:47:22	NA
11	C:\Windows\Installer\MSI398C.tmp	2018-03-25 08:58:10	NA
10	C:\Windows\SysWoW64\werfault.exe	2016-07-16 11:42:56	NA

# The Result of ShimCache Analysis

- In persistence chapter, we have found that WMI was used on client-win10-1. From the ShimCache, we found that the registration was done using mofcomp.exe.
- After W10.EXE was executed, ipconfig.exe and whoami.exe, which did not appear on Prefetch, were executed.
- net\*.exe, cscript.exe, xcopy.exe, 7.exe, l.exe were executed at some time in between March 21 and 25. We should pay a close attention to the executables with a single letter.

# Scenario 1 Incident Timeline After ShimCache Analysis



# SRUM

# SRUM

- Stands for “System Resource Usage Monitor”.
  - Monitors system resource performances.
- SRUM records the CPU time and other operations, and the disk and network I/Os.
  - If an executable file appears in the SRUM, the program must have been executed.
- First introduced in Windows 8.
- It is recorded in a file “**C:\Windows\System32\sru\SRUDB.dat**”.

# Contents of SRUM

- SRUM has several sections. The contents of SRUM include:
  - Network usage: application, user SID, interface, bytes sent/received/total
  - Application resource usage: application, user SID, CPU time in foreground/background, context switches, bytes read/written, number of read/write operations, etc...
  - Energy usage
  - ...
- Each SRUM entry has a timestamp of when the SRUM entry was created.
  - It records statistics once an hour or when the system shutdowns.
  - You can see information of processes that was running at that moment, like a snapshot.

# Parsing SRUM

- SRUM is not a human-readable file; it needs to be converted.
- It is written in the ESEDB format, which is used in a lot of places such as Active Directory, IE/Edge, and so on. You can parse:
  - ESEDatabaseView by Nirsoft
  - libesedb by libyal project
- However, you will need to join some tables and resolve names such as interface name. You can use a libesedb based python script called “srum-dump”.
  - <https://github.com/MarkBaggett/srum-dump>
- “srum-dump” can parse SRUDB.dat file, join tables and resolve names, and output to a XLSX file or several CSV files.

# Note About SRUM

- SRUM is updated once an hour or at the system shutdown.
- SRUM does not record executable files which started after a polling occurred and ended before the next polling is occurred.
- Be careful that timestamp in SRUM **does not tell exactly** when the program was first executed.

# Why This Artifact is so Important?

- We may be able to find RAT/BOT by analyzing this artifact because it has CPU usage, network I/O and disk I/O statistics every hour.
  - You can find processes that were kept executing for a long time.
  - You can find network communication spikes of suspicious processes.

# Scenario 1 Labs:

## Lab 4: Analyzing SRUM on Client-Win10-2

# Creating the Result of srum-dump

- You can use srum-dump

```
cd srum-dump
```

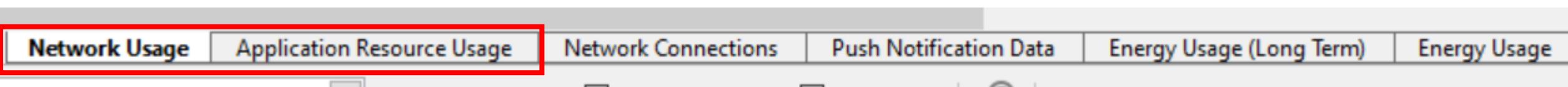
```
srum_dump -i G:\Windows\System32\sru\SRUDB.dat -r  
G:\Windows\System32\config\SOFTWARE -o %USERPROFILE%\Desktop\SRUDB.dat.xlsx
```

Note that this command takes a long time! We have already prepared the command result.  
The entire command needs to be entered in a single line.

- -i: Input file. You need to specify the path to a SRUDB.dat
  - The default path of SRUDB.dat is **C:\Windows\System32\sru\SRUDB.dat**
- -r: You can specify a HKLM\SOFTWARE hive to resolve WLAN's interface name.
  - The default path of SOFTWARE hive is **C:\Windows\System32\Config\SOFTWARE**
- -o: Output file. You can specify the output file path.

# Opening the output XLSX of srum-dump

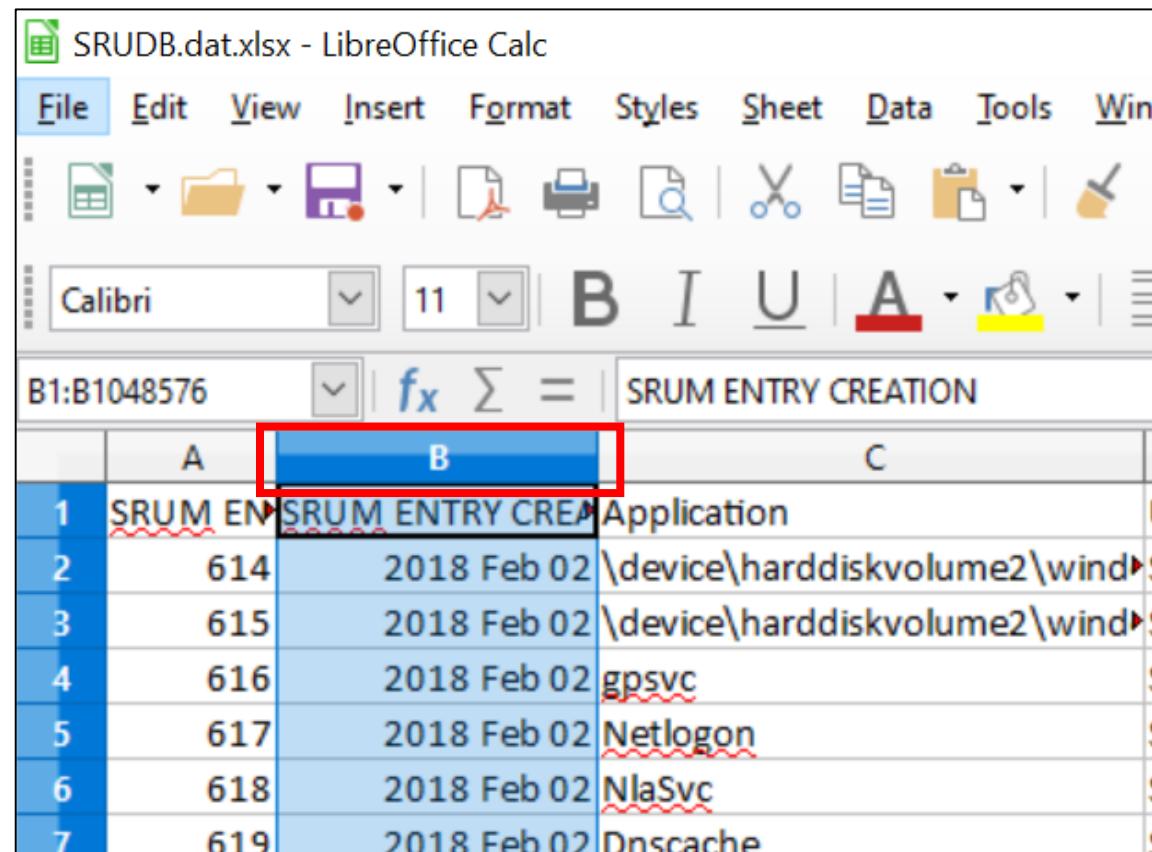
- You can find six sheets in the output XLSX.



- There are two important sheets in it.
  - Network Usage
  - Application Resource Usage
- Let's see “Network Usage” tab first.

# Change Columns Format (1)

- Before starting analyzing, let's change columns format first.
- Click "Column B".
- Then press "Ctrl + 1".
- You will see "format cells" dialog.



The screenshot shows a LibreOffice Calc spreadsheet titled "SRUDB.dat.xlsx - LibreOffice Calc". The menu bar includes File, Edit, View, Insert, Format, Styles, Sheet, Data, Tools, and Window. The toolbar below has icons for file operations, print, and search. The formula bar shows "B1:B1048576" and "SRUM ENTRY CREATION". The main table has columns A, B, and C. Row 1 contains "SRUM ENTR" and "SRUM ENTRY CREA" with "Application" in column C. Rows 2 through 7 show various entries with dates like "2018 Feb 02" and paths like "\device\harddiskvolume2\wind". Column B is highlighted with a red box. The formula bar also shows "fx", "Σ", and "=".

	A	B	C
1	SRUM ENTR	SRUM ENTRY CREA	Application
2	614	2018 Feb 02	\device\harddiskvolume2\wind
3	615	2018 Feb 02	\device\harddiskvolume2\wind
4	616	2018 Feb 02	gpsvc
5	617	2018 Feb 02	Netlogon
6	618	2018 Feb 02	NlaSvc
7	619	2018 Feb 02	Dnscache

# Change Date Format

Format Cells



Numbers Font Font Effects Alignment Borders Background Cell Protection

Category

All  
User-defined  
Number  
Percent  
Currency

1

Date

Time  
Scientific  
Fraction  
Boolean Value  
Text

Format

Fri Tevet 22 5760  
Fri 22 Tevet 5760  
22 Tevet 5760  
Tevet 22 5760  
22 Tevet  
Tevet 22  
Tevet 5760  
Tevet  
1999 Dec 31  
31 13:37:46

12/31/99 01:37 PM  
12/31/1999 13:37:46  
1999-12-31 13:37:46

Language

Default - English (USA)

2. Click one of these to get hour and minute units.

SRUM ENTRY CREATION

Options

Decimal places:

Negative numbers red

Leading zeroes:

Thousands separator

Format code

YYYY-MM-DD HH:MM:SS

3

Help

Reset

OK

Cancel

# Change Columns Format (3)

The screenshot shows the LibreOffice Calc interface with the title bar "SRUDB.dat.xlsx - LibreOffice Calc". The menu bar includes File, Edit, View, Insert, Format, Styles, Sheet, Data (which is highlighted with a red box and labeled "2"), Tools, Window, and Help. A context menu is open over a table, with the "Data" menu option also highlighted with a red box and labeled "2". The submenu contains "Sort...", "Sort Ascending", "Sort Descending", "AutoFilter" (which is highlighted with a red box and labeled "3"), "More Filters", "Define Range...", and "Select Range...". The main Calc interface shows a table with columns A and B, and rows 1 through 3. The first row has "SRUM ENTRY" in column A and "SRUM ENTRY CRE" in column B. The second row has "614" in column A and "2018 Feb 02 \device\harddi" in column B. The third row has "615" in column A and "2018 Feb 02 \device\harddi" in column B.

	A	B
1	SRUM ENTRY	SRUM ENTRY CRE
2	614	2018 Feb 02 \device\harddi
3	615	2018 Feb 02 \device\harddi

# Change Columns Format (4)

The screenshot shows a spreadsheet interface with several rows of data. Column H has been highlighted with a red border, indicating it is selected for movement. Red text annotations provide instructions:

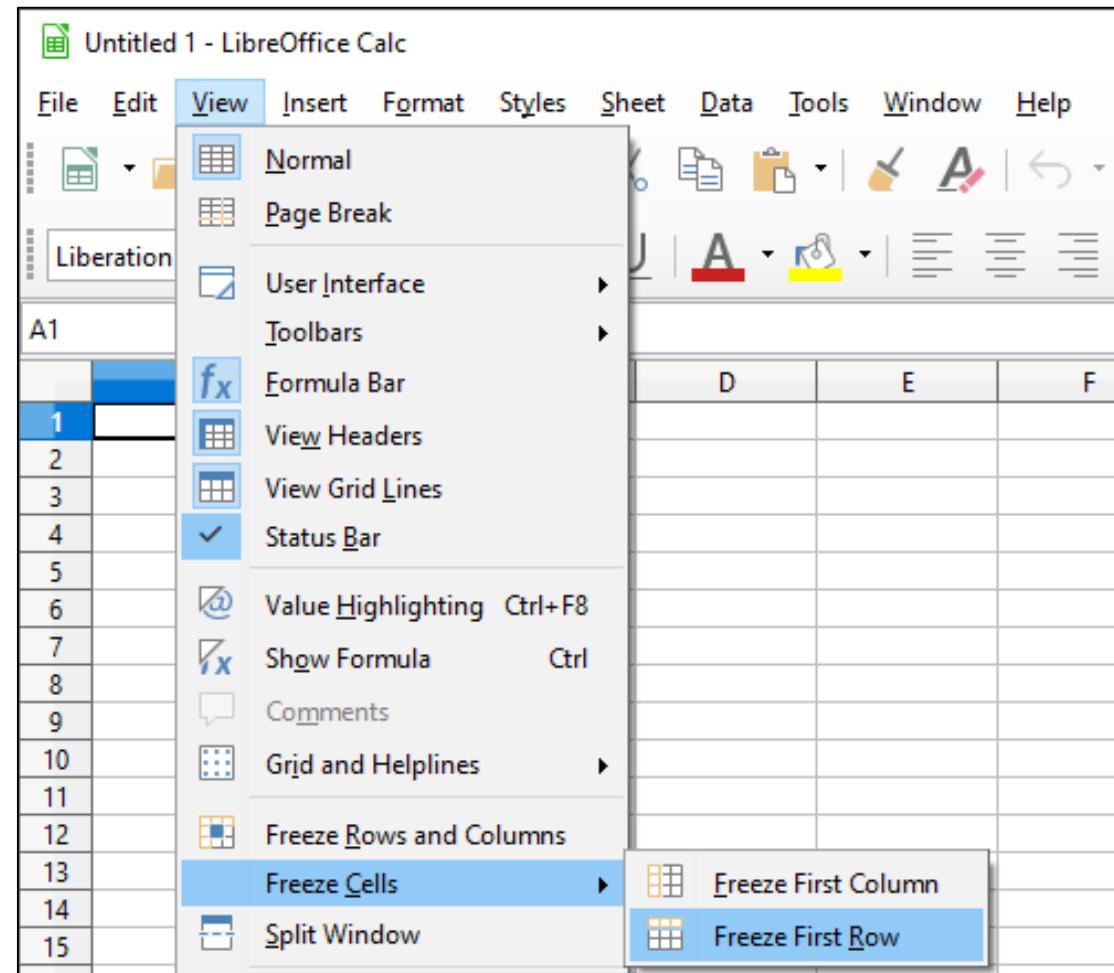
1. Drag Column H to J.
2. Click "Format as a Number" button once.
3. Click "Delete Decimal Place" button twice.

The top ribbon bar shows various icons for sorting, filtering, and data manipulation. The number format buttons are highlighted with red boxes. The data table includes columns for SID, Interface, Profile, Bytes Sent, Bytes Received, and Total Bytes.

SID	Interface	Profile	Bytes Sent	Bytes Received	Total Bytes
-18 ( Local System)	IF_TYPE_ETHERNET	0	96162	98103	194265
-18 ( Local System)	IF_TYPE_ETHERNET	0	26213	16660	42873
-18 ( Local System)	IF_TYPE_ETHERNET	0	133048	273997	407045
-18 ( Local System)	IF_TYPE_ETHERNET	0	5029	4386	9415
-20 ( NT Authority)	IF_TYPE_ETHERNET	0	824	5662	6486

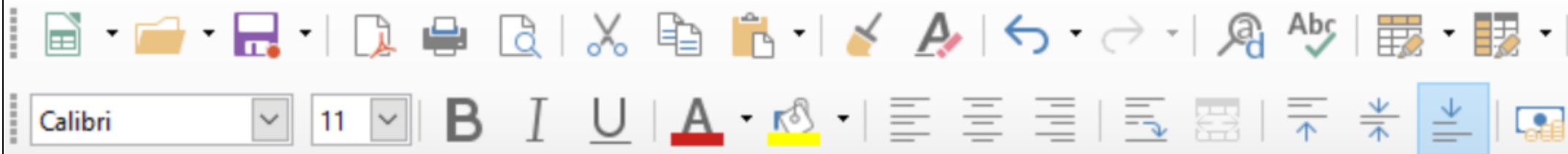
# Freeze First Row

- Use “Freeze First Row” option to keep the title row visible even when you scroll the worksheet.
- You can also apply the same option to column if there is a title column.



# The Strategy of Analyzing srum-dump Results

- We shouldn't look each line one by one because the number of the records are huge.
- We have several pivot points that:
  - The malware process that was found from this host is “rundll32.dll (SvS.DLL)”.
  - The malware is for 32-bit environment. Therefore, program execution records of standard command-line executables which are located in the “SysWOW64” folder are suspicious because if a 32-bit program spawns another program, it should run on 32-bit environment as well.
  - The attacker used “ProgramData” and “ProgramData\s” folders as the foothold folders.
- You can also check around the timestamps of the pivot points that we found so far.
- Let's filter with these keywords and take a look at around the timestamps.



C2      fx    Σ   =    NlaSvc

	A	B	C
1	SRUM	SRUM ENTRY CREATI	Application
2	494	2018-02-02 12:24:00	NlaSvc
3	495	2018-02-02 12:24:00	\device\harddiskvolum
4	496	2018-02-02 12:24:00	gpsvc
5	497	2018-02-02 12:24:00	Dnscache
6	498	2018-02-02 12:24:00	Dhcp
7	499	2018-02-02 12:24:00	W32Time
8	500	2018-02-02 12:24:00	Netlogon
9	501	2018-02-02 12:24:00	None
10	502	2018-02-02 12:24:00	gpsvc
11	503	2018-02-02 12:24:00	\device\harddiskvolum
12	504	2018-02-02 12:24:00	SENS
13	505	2018-02-02 12:24:00	System\IPv6 Control M
14	506	2018-02-02 12:24:00	System
15	507	2018-02-02 12:24:00	SENS

1. Click the triangle button on the Application column.

Sort Ascending

Sort Descending

Top 10

Empty

Not Empty

Standard Filter...

2. Input "rundll32"

rundll32

 \device\harddiskvolume2\wind3. Then you will see  
only one binary.

The binary was started to be recorded at March 07 4:37 PM.

Note that the timestamps are recorded in UTC. You should add nine hours for converting into JST. Since SRUM records statistics every hour, the malware was executed in around 15:37 to 16:37 for the first time. You have already known it happened at 4:13 PM though.

You can get the SID of the user that the malware executed.

	A	B	C	D	E
1	SRUM	SRUM ENTRY CREATE	Application	User SID	Internet
9127	9619	2018-03-07 07:37:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1110	IF_
9130	9622	2018-03-07 08:37:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1110	IF_
9146	9638	2018-03-07 09:37:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1110	IF_
9162	9654	2018-03-07 10:38:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1110	IF_
9174	9666	2018-03-07 11:39:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1110	IF_
9190	9682	2018-03-07 12:40:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1110	IF_
9205	9697	2018-03-07 13:40:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1110	IF_
9219	9711	2018-03-07 13:40:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1110	IF_
9223	9715	2018-03-07 14:41:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1110	IF_
9245	9737	2018-03-07 15:41:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1110	IF_
9258	9750	2018-03-07 16:42:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1110	IF_
9270	9762	2018-03-07 17:52:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1110	IF_

Malware seems to continue to run because it was recorded every hour.

You can see sent and received bytes that malware did in an hour.

	A	B	C	D	E	F	G	H	I	J
1	SRU	SRUM ENTRY CREAT	Application	▼	▼	▼	▼	Bytes Sent	Bytes Recei	Total B
9127	9619	2018-03-07 07:37:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF	0	15,672		5,048		20,720
9130	9622	2018-03-07 08:37:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF	0	34,745		12,354		47,099
9146	9638	2018-03-07 09:37:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF	0	34,771		12,354		47,125
9162	9654	2018-03-07 10:38:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF	0	35,976		12,780		48,756
9174	9666	2018-03-07 11:39:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF	0	35,378		12,567		47,945
9190	9682	2018-03-07 12:40:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF	0	35,374		12,567		47,941
9205	9697	2018-03-07 13:40:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF	0	50,405		481,753		532,158
9219	9711	2018-03-07 13:40:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	9 IF	0	4,929		9,322		14,251
9223	9715	2018-03-07 14:41:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF	0	65,408		19,268		84,676
9245	9737	2018-03-07 15:41:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF	0	34,691		12,354		47,045
9258	9750	2018-03-07 16:42:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF	0	35,852		12,780		48,632

You can see malware communicates relatively a lot around this time.

In order to filter entries with “Total Bytes” values, open Standard Filter window.

	D	E	F	G	H	I	J	K	L
	U	Imp	Prv	Prv	Bytes Sent	Bytes Recd	Total Bytes		
syswow64\rundll32.exe	S+IF_TYP>	0	15,672	5,048					
syswow64\rundll32.exe	S+IF_TYP>	0	34,745	12,354					
syswow64\rundll32.exe	S+IF_TYP>	0	34,771	12,354					
syswow64\rundll32.exe	S+IF_TYP>	0	35,976	12,780					
syswow64\rundll32.exe	S+IF_TYP>	0	35,378	12,567					
syswow64\rundll32.exe	S+IF_TYP>	0	35,374	12,567					
syswow64\rundll32.exe	S+IF_TYP>	0	50,405	481,753					
\SysWOW64\rundll32.exe	S+IF_TYP>	0	4,929	9,322					
syswow64\rundll32.exe	S+IF_TYP>	0	65,408	19,268					
syswow64\rundll32.exe	S+IF_TYP>	0	34,691	12,354					
syswow64\rundll32.exe	S+IF_TYP>	0	35,852	12,780					
syswow64\rundll32.exe	S+IF_TYP>	0	38,272	14,214					

Sort Ascending  
Sort Descending  
Top 10  
Empty  
Not Empty  
**Standard Filter...**

Search items...  
 B210

Then, set the filter as the below figure.

### Standard Filter

#### Filter Criteria

In this case, we try to apply the filter with the "Total Bytes" values greater equal than 100,000 first.

Operator	Field name	Condition	Value
Application	Contains	rundll32	
AND	Total Bytes	>=	100000
	- none -	=	
	- none -	=	

+ Options

Help

OK

Cancel

There are few entries having the “Total Bytes” value greater than 100000.

SRUM ENTRY CREAT	Application	Up	Inf	Prv	Pst	Bytes Sent	Bytes Rec	Total Bytes
2018-03-07 13:40:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>	IF_	TY>	0	50,405	481,753	532,158
2018-03-09 06:06:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>	IF_	TY>	0	88,798	18,062	106,860
2018-03-12 12:34:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>	IF_	TY>	0	86,125	14,214	100,339
2018-03-12 13:35:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>	IF_	TY>	0	110,178	20,513	130,691
2018-03-14 13:03:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>	IF_	TY>	0	190,827	36,817	227,644
2018-03-14 14:04:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>	IF_	TY>	0	141,900,642	16,798,753	158,699,395
2018-03-23 04:16:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>	IF_	TY>	0	77,141	25,684	102,825

Standard Filter

Filter Criteria

Operator	Field name	Condition	Value
AND	Application	Contains	rundll32
	Total Bytes	>=	80000
	- none -	=	
	- none -	=	

Then, apply filter again with smaller value.  
In this case, use 80000 as the threshold .

+ Options

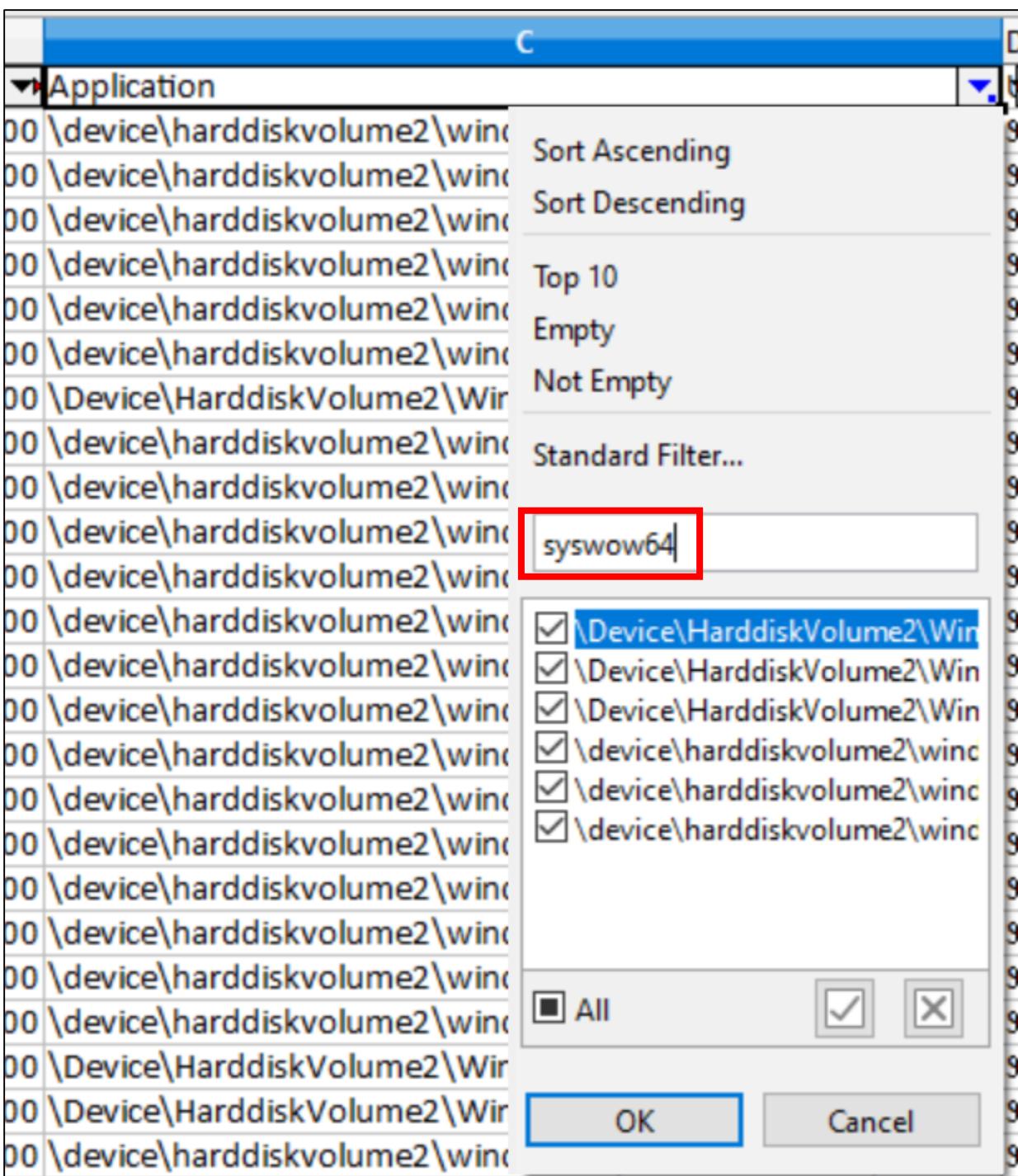
Help OK Cancel

SRU	SRUM ENTRY CREAT	Application	S	I	P	P	Bytes Sent	Bytes Rec	Total Bytes
9697	2018-03-07 13:40:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>IF_TY>	0			50,405	481,753	532,158
9715	2018-03-07 14:41:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>IF_TY>	0			65,408	19,268	84,676
9951	2018-03-08 05:57:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>IF_TY>	0			65,799	26,401	92,200
10305	2018-03-09 06:06:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>IF_TY>	0			88,798	18,062	106,860
11682	2018-03-12 12:34:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>IF_TY>	0			86,125	14,214	100,339
11699	2018-03-12 13:35:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>IF_TY>	0			110,178	20,513	130,691
12556	2018-03-14 13:03:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>IF_TY>	0			190,827	36,817	227,644
12575	2018-03-14 14:04:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>IF_TY>	0			141,900,642	16,798,753	158,699,395
15733	2018-03-23 04:16:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>IF_TY>	0			77,141	25,684	102,825
15752	2018-03-23 05:16:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S>IF_TY>	0			65,494	18,368	83,862

There are several spikes of the communications for the malware process.

The attacker might have had something activities around these time periods.

- March 7 9:40 PM - 11:41 PM (in JST: UTC+9:00)
- March 8 1:56 PM - 2:57 PM
- March 9 2:06 PM - 3:06 PM
- March 12 8:33 PM - 10:35 PM
- March 14 9:02 PM - 11:04 PM
- March 23 12:16 PM - 2:16 PM



When you filter with  
"syswow64"...,

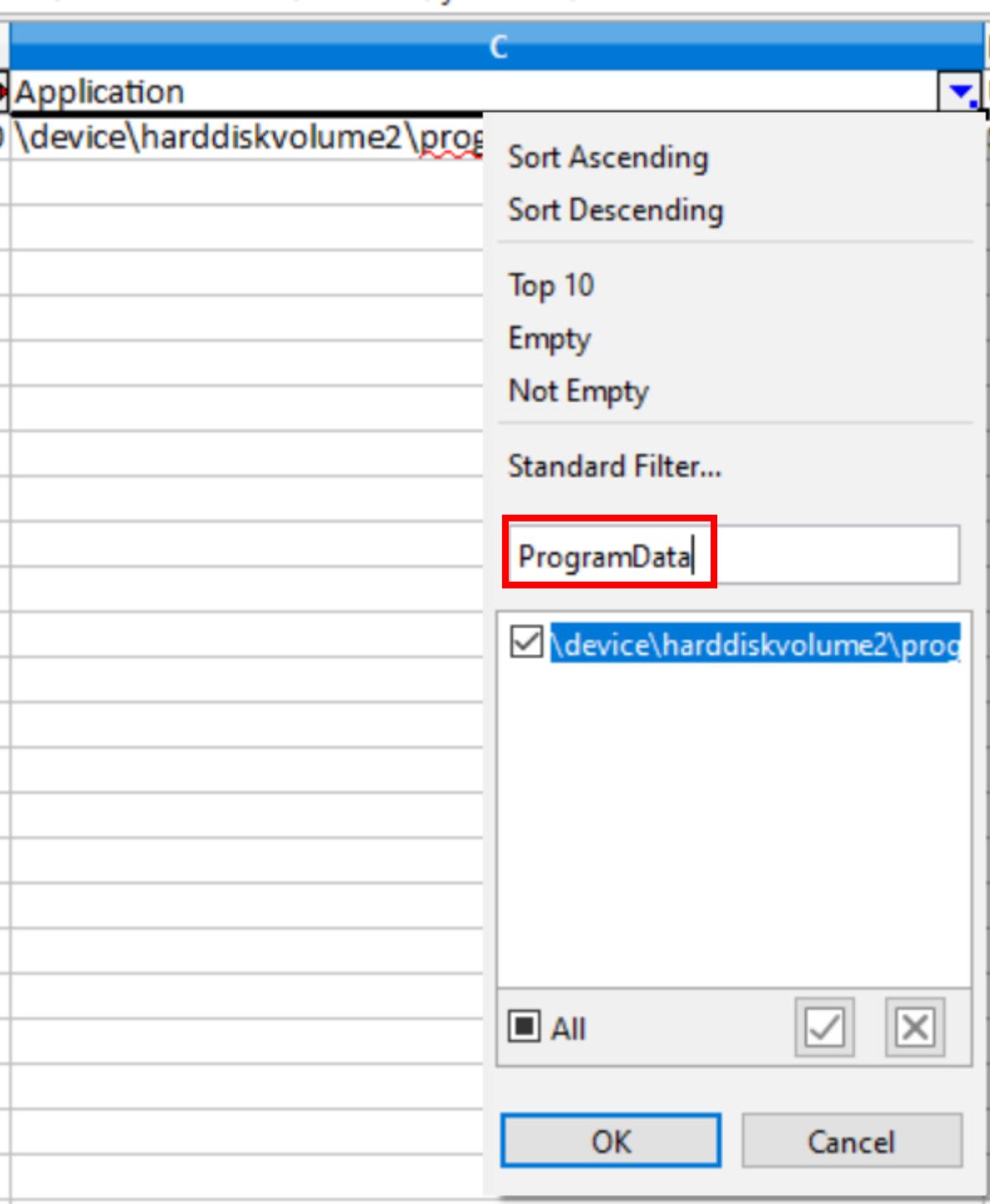
9682	2018-03-07 12:40:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF_ ▶ 0	35,374	12,567	47
9697	2018-03-07 13:40:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF_ ▶ 0	50,405	481,753	532
9711	2018-03-07 13:40:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	9 IF_ ▶ 0	4,929	9,322	14
9715	2018-03-07 14:41:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF_ ▶ 0	65,408	19,268	84
9722	2018-03-07 14:41:00	\Device\HarddiskVolume2\Windows\SysWOW64\net1.exe	9 IF_ ▶ 0	18,886	26,741	45
9727	2018-03-07 15:41:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF_ ▶ 0	24,691	12,254	47

We can find net1.exe and nslookup.exe at the same time as the malware's spikes on the communications.

9911	2018-03-08 03:55:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF_ ▶ 0	58,747	12,554	51
9934	2018-03-08 04:56:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF_ ▶ 0	42,335	12,654	54
9951	2018-03-08 05:57:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF_ ▶ 0	65,799	26,401	92
9965	2018-03-08 05:57:00	\device\harddiskvolume2\windows\syswow64\nslookup.exe	9 IF_ ▶ 0	255	530	
9966	2018-03-08 05:57:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	9 IF_ ▶ 0	1,946	5,016	6,
9968	2018-03-08 06:58:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF_ ▶ 0	47,905	15,654	63,
9991	2018-03-08 07:58:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF_ ▶ 0	42,542	12,567	55,

Note that these binaries are false positive and they are not related to this incident because of the dates.

- searchprotocolhost.exe
- msieexec.exe
- IMEWDBLD.EXE

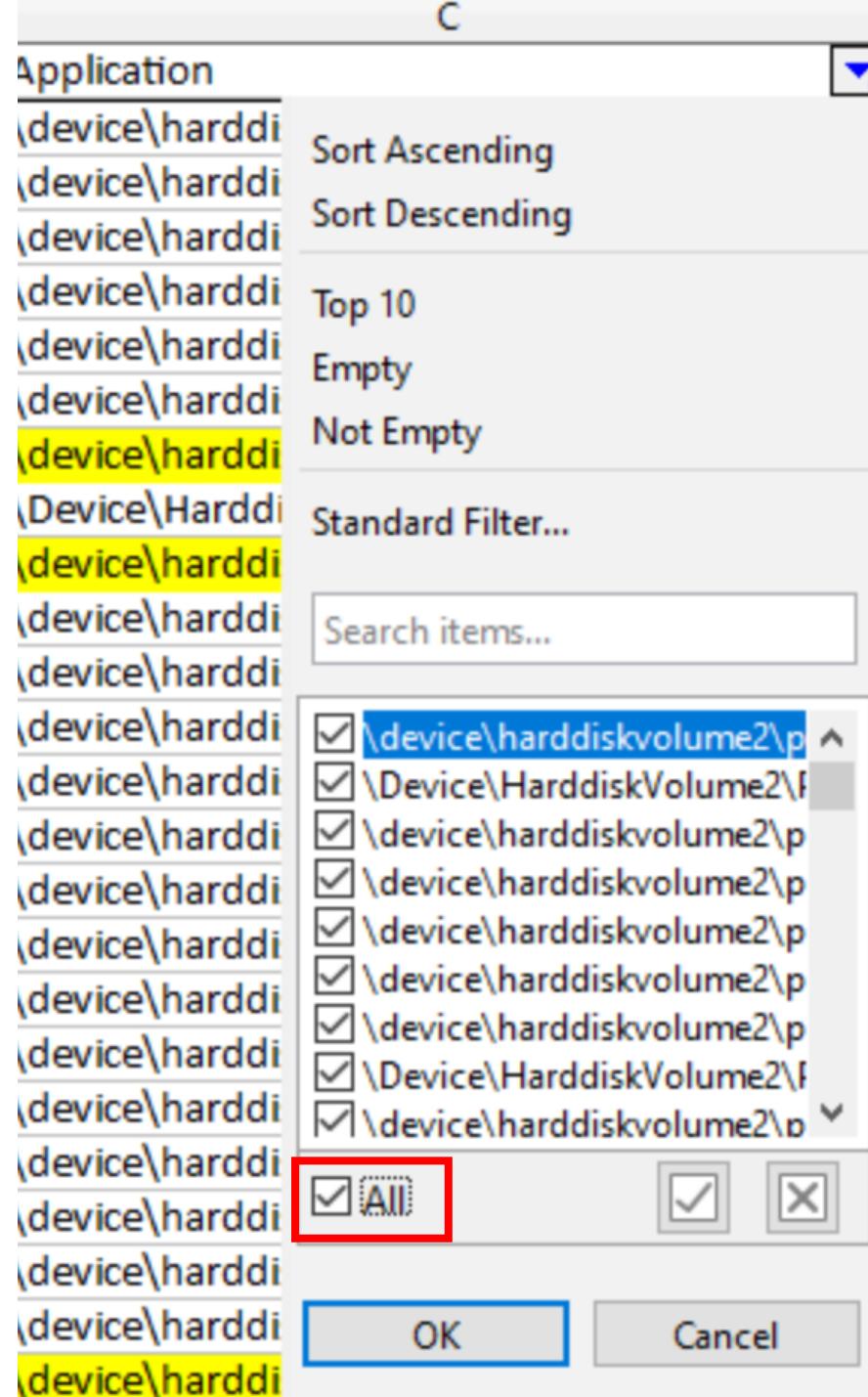


When you filter with  
“ProgramData”...,

12541	2018-03-14 12:02:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF_ ▶ 0	40,412	12,780	53
12556	2018-03-14 13:03:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF_ ▶ 0	190,827	36,817	227
12569	2018-03-14 13:03:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	9 IF_ ▶ 0	1,346	2,936	4
12579	2018-03-14 14:04:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	9 IF_ ▶ 0	141,900,642	16,798,753	

We can also find dq.exe at the same time as the malware's spikes on a communication.

A	B	C	D	E	F	G	H	I	J
SRUJ	SRUM ENTRY CREATI	Application	▼	▼	▼	▼	Bytes Sent	Bytes Recei	Total
12584	2018-03-14 14:04:00	\device\harddiskvolume2\programdata\s\dq.exe	9 IF_ ▶ 0				5,941	9,274	15,



Finally, check records having the same time as the malware's spikes on a communication.

2018-03-07 12:40:00	\device\harddiskvolume2\windows\system32\browser_broker.exe	S-1>IF_TYP	0	560	4,48
2018-03-07 13:40:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S-1>IF_TYP	0	50,405	481,75
2018-03-07 13:40:00	\device\harddiskvolume2\program files\microsoft office 15\root\office	S-1>IF_TYP	0	23,644	18,36
2018-03-07 13:40:00	\device\harddiskvolume2\windows\system32\wbern\wmiprvse.exe	S-1>IF_TYP	0	14,025	13,32
2018-03-07 13:40:00	\device\harddiskvolume2\windows\system32\wmiprvse.exe	S-1>IF_TYP	0	1,254	6,75
2018-03-07 14:41:00	\device\harddiskvolume2\windows\system32\wmiprvse.exe	wmiprvse.exe processes imply WMI related activities.			
2018-03-07 14:41:00	Dnscache				
2018-03-07 14:41:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S-1>IF_TYP	0	65,408	19,26
2018-03-07 14:41:00	System\SMB	S-1>IF_TYP	0	76,146	71,38
2018-03-07 14:41:00	\device\harddiskvolume2\program files\microsoft office 15\root\office	S-1>IF_TYP	0	23,944	18,30
2018-03-07 14:41:00	\device\harddiskvolume2\windows\system32\wbern\wmiprvse.exe	S-1>IF_TYP	0	3,360	21,20
2018-03-12 13:35:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S-1>IF_TYP	0	110,	
2018-03-12 13:35:00	\d	These powershell.exe and cscript.exe might have been called by the attacker via the malware.			
2018-03-12 13:35:00	\Device\HarddiskVolume2\Windows\System32\powershell.exe	S-1>IF_TYP	0	19,	
2018-03-12 13:35:00	\Device\HarddiskVolume2\Windows\System32\cscript.exe	S-1>IF_TYP	0		
2018-03-14 14:04:00	\device\harddiskvolume2\windows\syswow64\rundll32.exe	S-1>IF_TYP	0	141,900,642	16,79
2018-03-14 14:04:00	System\SMB	S-1>IF_TYP	0	82,015	7
2018-03-14 14:04:00	mstsc.exe is the remote desktop client. It might be related to the attacker's lateral movement activity.				
2018-03-14 14:04:00	\device\harddiskvolume2\windows\system32\lsass.exe	S-1>IF_TYP	0	3,897	
2018-03-14 14:04:00	\device\harddiskvolume2\windows\system32\mstsc.exe	S-1>IF_TYP	0	695,983	3,63

- Next, let's take a look at “Application Resource Usage” tab.
- If you filter with “syswow64”...,

You have already known these periods are suspicious.

- March 7 9:40 PM - 11:41 PM (in JST: UTC+9:00)
- March 8 1:56 PM - 2:57 PM
- March 9 2:06 PM - 3:06 PM
- March 12 8:33 PM - 10:35 PM
- March 14 9:02 PM - 11:04 PM
- March 23 12:16 PM - 2:16 PM

44406	2018-03-07 07:37:00	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe
44407	2018-03-07 07:37:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
44464	2018-03-07 08:37:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
44521	2018-03-07 09:37:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
44576	2018-03-07 10:38:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
44632	2018-03-07 11:39:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
44686	2018-03-07 12:40:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
44726	2018-03-07 13:40:00	\Device\HarddiskVolume2\Windows\SysWOW64\wbem\WmiPrvSE.exe
44745	2018-03-07 13:40:00	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe
44746	2018-03-07 13:40:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
44747	2018-03-07 13:40:00	\Device\HarddiskVolume2\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
44790	2018-03-07 14:41:00	\Device\HarddiskVolume2\Windows\SysWOW64\wbem\WmiPrvSE.exe
44810	2018-03-07 14:41:00	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe
44811	2018-03-07 14:41:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe

These are close to the infection date.

These are close to the information collection date.

- Although, we couldn't find cmd.exe, powershell.exe and WmiPrvSE.exe on Network Usage tab, we did in Application Resource Usage tab!

42102	45083	2018-03-08 05:57:00	\Device\HarddiskVolume2\Windows\SysWOW64\SearchProtocolHost.exe
42107	45688	2018-03-08 05:57:00	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe
42108	45689	2018-03-08 05:57:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
42109	45690	2018-03-08 05:57:00	\Device\HarddiskVolume2\Windows\SysWOW64\prevhost.exe
42169	45750	2018-03-08 06:58:00	\Device\HarddiskVolume2\Windows\SysWOW64\SearchProtocolHost.exe
42175	45756	2018-03-08 06:58:00	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe
42176	45757	2018-03-08 06:58:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
42231	45812	2018-03-08 07:58:00	\Device\HarddiskVolume2\Windows\SysWOW64\SearchProtocolHost.exe
42237	45818	2018-03-08 07:58:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
49160	52741	2018-03-12 12:34:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
49231	52812	2018-03-12 13:35:00	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe
49232	52813	2018-03-12 13:35:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
49301	52882	2018-03-12 14:36:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
52522	56103	2018-03-14 12:02:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
52596	56177	2018-03-14 13:03:00	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe
52597	56178	2018-03-14 13:03:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
52677	56258	2018-03-14 14:04:00	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe
52678	56259	2018-03-14 14:04:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
52752	56333	2018-03-14 15:04:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
65582	69163	2018-03-23 04:16:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
65584	69165	2018-03-23 04:16:00	\Device\HarddiskVolume2\Windows\SysWOW64\SearchProtocolHost.exe
65595	69176	2018-03-23 04:16:00	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe
65652	69233	2018-03-23 05:16:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe
65654	69235	2018-03-23 05:16:00	\Device\HarddiskVolume2\Windows\SysWOW64\SearchProtocolHost.exe
65659	69240	2018-03-23 05:16:00	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe

- There is no interesting result for filtering with “ProgramData”.

SRUDB.dat.xlsx - LibreOffice Calc

	A	B	C
1	Srum ID	Srum Entry Creation	Application
2977	6558	2018 Feb 08	\Device\HarddiskVolume2\ProgramData\Adobe\Setup\{AC76BA86-7AD7-1041-7B44-AC0F074E41\AdobeSetup.exe
32573	36154	2018 Feb 28	\Device\HarddiskVolume2\ProgramData\Adobe\ARM\S\17684\AdobeARMHelper.exe
79213			
79214			

# Summary for This Lab

- You was able to find several suspicious spiked communications from malware.

Date Range (in JST: UTC+9:00)	Assumed Activities	Sent/Recv Bytes
March 7 9:40 PM - 11:41 PM	Information Collection	50,405/481,753
March 8 1:56 PM - 2:57 PM	SchedTasks and W10 execution	65,799/26,401
March 9 2:06 PM - 3:06 PM	??? (w/o cmd.exe)	88,798/18,062
March 12 8:33 PM - 10:35 PM	??? (w/ cmd.exe)	110,178/20,513
March 14 9:02 PM - 11:04 PM	Lateral Movement Occurred? (Client-Win10-1 was infected around this date)	141,900,642/16,798,753
March 23 12:16 PM - 2:16 PM	l.exe execution	77,141/25,684



We got a possible new activity by the attacker.

# Scenario 1 Labs:

## Lab 5: Analyzing SRUM on Client-Win10-1

# Creating the Result of srum-dump

- You can use srum-dump

```
cd C:\tools\srum-dump\
```

```
srum_dump -i E:\Artifacts\scenario1_srum\Client-Win10-1_toyoda\SRUDB.dat -r  
E:\Artifacts\scenario1_srum\Client-Win10-1_toyoda\SOFTWARE -o  
E:\Artifacts\scenario1_srum\Client-Win10-1_toyoda\SRUDB.dat.xlsx
```

Note that this command takes a long time! We have already prepared the command result.  
This is one line. Don't start a new line.

- -i: Input file. You need to specify the path to a SRUDB.dat
  - The default path of SRUDB.dat is **C:\Windows\System32\sru\SRUDB.dat**
- -r: You can specify a HKLM\SOFTWARE hive to resolve WLAN's interface name.
  - The default path of SOFTWARE hive is **C:\Windows\System32\Config\SOFTWARE**
- -o: Output file. You can specify the output file path.

# The Strategy of Analyzing srum-dump Results

- We shouldn't look each line one by one because the number of the records are huge.
- We have several pivot points that:
  - Malware processes that were found from this host are “rundll32.dll (SvS.DLL)” and “AddinsManager.exe”.
  - Both of the malware are for 32-bit environment. Therefore, program execution records of standard command-line executables which are located in the “SysWow64” folder are suspicious.
  - The attacker used “ProgramData” and “ProgramData\s” folders as the foothold folders.
- You can also check around the timestamps of the pivot points that we found so far.
- Let's filter with these keywords and take a look at around the timestamps.

# Preparation for This Exercise

- First, let's open the path below.
  - E:\Artifacts\scenario1\_srum\Client-Win10-1\_toyoda\SRUDB.dat.xlsx
- And change columns format as we mentioned in the previous exercise.

1. Click the triangle button on the Application column.

	A	B	C
1	SRUM	SRUM ENTRY CREATION	Application
2	614	2018-02-02 12:05:00 \device\harddiskvolume2>window	<input type="button" value="▼"/>
3	615	2018-02-02 12:05:00 \device\harddiskvolume2>window	Sort Ascending
4	616	2018-02-02 12:05:00 gpsvc	Sort Descending
5	617	2018-02-02 12:05:00 Netlogon	Top 10
6	618	2018-02-02 12:05:00 NlaSvc	Empty
7	619	2018-02-02 12:05:00 Dnscache	Not Empty
8	620	2018-02-02 12:05:00 WinRM	Standard Filter...
9	621	2018-02-02 12:05:00 None	<input type="text" value="rundll"/>
10	622	2018-02-02 12:05:00 Spooler	2. Input "rundll" to analyze SvS.DLL malware communications.
11	623	2018-02-02 12:05:00 gpsvc	
12	624	2018-02-02 12:05:00 SENS	
13	625	2018-02-02 12:05:00 Dhcp	
14	626	2018-02-02 12:05:00 SENS	
15	627	2018-02-02 12:05:00 SSDPSRV	
16	628	2018-02-02 12:05:00 System	
17	629	2018-02-02 12:05:00 System\IPv6 Control Message	
18	630	2018-02-02 12:05:00 SENS	
19	631	2018-02-02 12:05:00 Microsoft.Windows.Cortana_1.7.0	
20	632	2018-02-02 12:05:00 wlidsvc	
21	633	2018-02-02 12:05:00 OneSyncSvc_36dcc	
22	634	2018-02-02 12:05:00 \device\harddiskvolume2\program	
23	635	2018-02-02 12:05:00 \device\harddiskvolume2\users\t	
24	636	2018-02-02 12:05:00 DoSvc	
25	637	2018-02-02 12:05:00 \device\harddiskvolume2>window	

1. Click the triangle button on the Application column.

	A	B	C
1	SRUM	SRUM ENTRY CREATION	Application
2	614	2018-02-02 12:05:00	\device\harddiskvolume2\window
3	615	2018-02-02 12:05:00	\device\harddiskvolume2\window
4	616	2018-02-02 12:05:00	gpsvc
5	617	2018-02-02 12:05:00	Netlogon
6	618	2018-02-02 12:05:00	NlaSvc
7	619	2018-02-02 12:05:00	Dnscache
8	620	2018-02-02 12:05:00	WinRM
9	621	2018-02-02 12:05:00	None
10	622	2018-02-02 12:05:00	Spooler
11	623	2018-02-02 12:05:00	gpsvc
12	624	2018-02-02 12:05:00	SENS
13	625	2018-02-02 12:05:00	Dhcp
14	626	2018-02-02 12:05:00	SENS
15	627	2018-02-02 12:05:00	SSDPSRV
16	628	2018-02-02 12:05:00	System
17	629	2018-02-02 12:05:00	System\IPv6 Control Message
18	630	2018-02-02 12:05:00	SENS
19	631	2018-02-02 12:05:00	Microsoft.Windows.Cortana_1.7.0
20	632	2018-02-02 12:05:00	wlidsvc
21	633	2018-02-02 12:05:00	OneSyncSvc_36dcc
22	634	2018-02-02 12:05:00	\device\harddiskvolume2\program
23	635	2018-02-02 12:05:00	\device\harddiskvolume2\users\t
24	636	2018-02-02 12:05:00	DoSvc
25	637	2018-02-02 12:05:00	\device\harddiskvolume2\window

Sort Ascending

Sort Descending

Top 10

Empty

Not Empty

Standard Filter...

Addin

2. Input "Addin" to get entries  
for "AddinsManager.exe"

3. But there is no  
process at this time.

All



OK

Cancel

# Note of SRUM's Network Usage

- We couldn't get the results for both malware processes due to some reasons at this time. Unfortunately, it seems that SRUM sometimes doesn't record some of the communications...
- Let's continue the analysis. Next, let's check binaries in the syswow64 directory.

These are no related to this incidents because of the date.

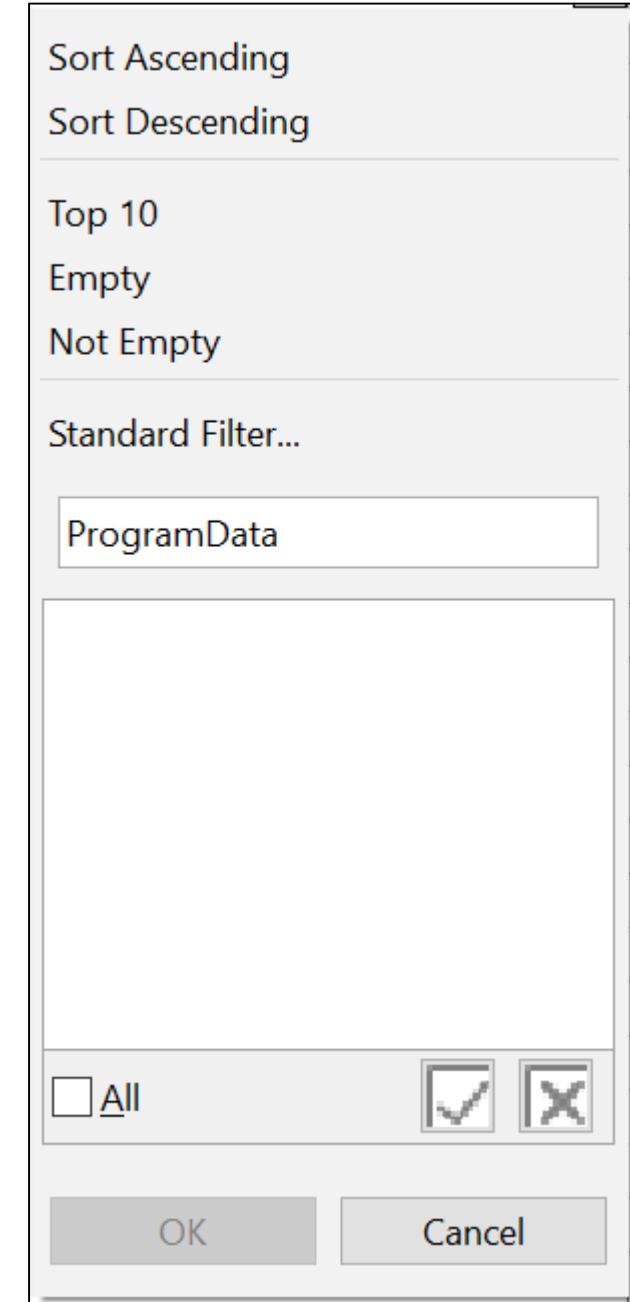
These binaries imply the attacker might have used NET USER/GROUP command to get accounts information or NET USE command to mount network share with SMB.

The attacker used certain scripts written in JScript or VBScript.

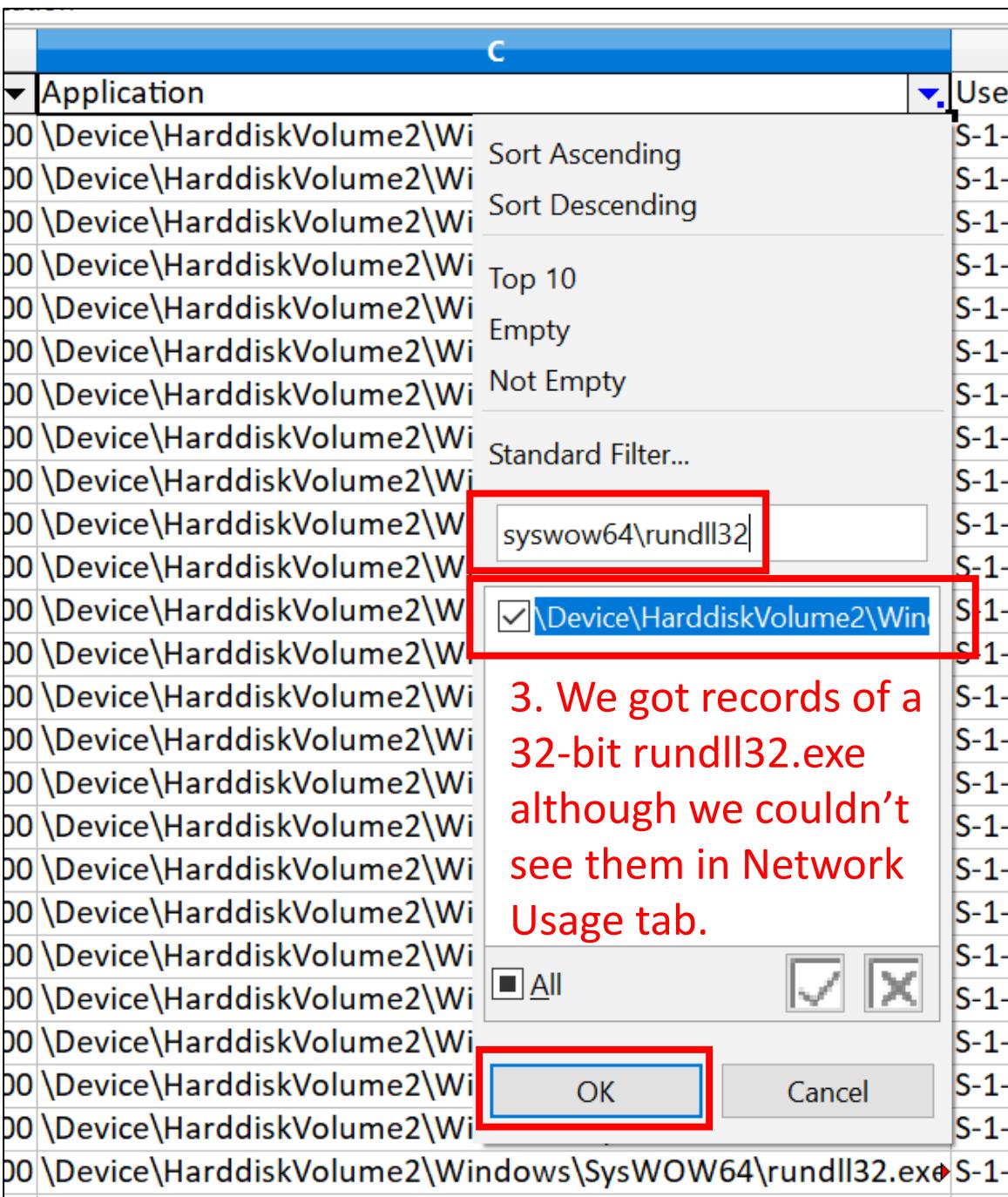
A	B	C	D	E	F	G	H	I
			User SID	HTTP Bytes	HTTP Bytes Received			
SRU	SPLUM ENTRY CREA	Application	S-1-5-21-3671970501-39	Un# 0	0			
1394	2018-02-08 07:54:00	\Device\HarddiskVolume2\Windows\SysWOW64\msiexec.exe	S-1-5-21-3671970501-39	Un# 0	0			
1430	2018-02-08 08:38:00	\Device\harddiskvolume2\windows\syswow64\msiexec.exe	S-1-5-21-3671970501-39	IF# 454	4,494			
1432	2018-02-08 08:38:00	\Device\HarddiskVolume2\Windows\SysWOW64\msiexec.exe	S-1-5-21-3671970501-39	Un# 0	0			
6	14158	2018-03-22 09:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\net1.exe	S-1-5-18 ( Local System)	Un# 16,192	13,449			
8	14160	2018-03-22 09:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\net.exe	S-1-5-18 ( Local System)	Un# 4,038	3,493			
9	14161	2018-03-22 09:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\cscript.exe	S-1-5-18 ( Local System)	Un# 8,976	6,727			
3	14165	2018-03-22 09:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe	S-1-5-18 ( Local System)	Un# 15,552	27,196			
5	14167	2018-03-22 10:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe	S-1-5-18 ( Local System)	Un# 41,196	90,164			
6	14168	2018-03-22 10:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\xcopy.exe	S-1-5-18 ( Local System)	Un# 330,941	64,173,558			
9	14171	2018-03-22 10:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\net.exe	S-1-5-18 ( Local System)	Un# 0	0			
0	14172	2018-03-22 10:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\cscript.exe	S-1-5-18 ( Local System)	Un# 3,814	4,360			
5	14227	2018-03-23 04:20:00 \Device\HarddiskVolume2\Windows\SysWOW64\cscript.exe	S-1-5-18 ( Local System)	Un# 2,289	2,554			
6	14228	2018-03-23 04:20:00 \Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe	S-1-5-18 ( Local System)	Un# 8,601	16,616			
7	14229	2018-03-23 04:20:00 \Device\HarddiskVolume2\Windows\SysWOW64\xcopy.exe	S-1-5-18 ( Local System)	Un# 46,219	32,670,032			

The attacker used xcopy.exe at least twice. And the first one is likely that the attacker mounted a remote file system with SMB and copy data from the system. For the second one, the attacker also used xcopy command to get data from a remote host because this record is in the Network Usage tab. The traffic were approximately 64 MB and 33 MB.

- There is no entry when you filter with “ProgramData”.
- But we was able to find remote file copy operation by the attacker.
- Next, let's check Application Resource Usage tab.



1. Click the triangle button on the Application column.



2. Input “syswow64\rundll32” to get entries for “SvS.DLL”.

3. We got records of a 32-bit rundll32.exe although we couldn't see them in Network Usage tab.

1. Click the triangle button on the Application column.

B	C
Srum Entry Creatio	Application ▾
1 2018-03-14 14:08:00	\Device\HarddiskVolume2\Wi
9 2018-03-14 14:08:00	\Device\HarddiskVolume2\Wi
2 2018-03-14 14:08:00	\Device\HarddiskVolume2\Wi
0 2018-03-14 15:08:00	\Device\HarddiskVolume2\Wi
9 2018-03-14 15:08:00	\Device\HarddiskVolume2\Wi
9 2018-03-14 16:09:00	\Device\HarddiskVolume2\Wi
1 2018-03-14 16:09:00	\Device\HarddiskVolume2\Wi
1 2018-03-14 17:09:00	\Device\HarddiskVolume2\Wi
3 2018-03-14 17:09:00	\Device\HarddiskVolume2\Wi
5 2018-03-14 18:09:00	\Device\HarddiskVolume2\Wi
8 2018-03-14 18:09:00	\Device\HarddiskVolume2\Wi
0 2018-03-14 19:10:00	\Device\HarddiskVolume2\Wi
4 2018-03-14 19:10:00	\Device\HarddiskVolume2\Wi
4 2018-03-14 20:10:00	\Device\HarddiskVolume2\Wi
6 2018-03-14 20:10:00	\Device\HarddiskVolume2\Wi
6 2018-03-14 21:11:00	\Device\HarddiskVolume2\Wi
0 2018-03-14 21:11:00	\Device\HarddiskVolume2\Wi
0 2018-03-14 22:11:00	\Device\HarddiskVolume2\Wi
2 2018-03-14 22:11:00	\Device\HarddiskVolume2\Wi
2 2018-03-14 23:12:00	\Device\HarddiskVolume2\Wi
6 2018-03-14 23:12:00	\Device\HarddiskVolume2\Wi
6 2018-03-15 00:12:00	\Device\HarddiskVolume2\Wi
0 2018-03-15 00:12:00	\Device\HarddiskVolume2\Wi
0 2018-03-15 01:12:00	\Device\HarddiskVolume2\Wi

2. Input “Addins” to get entries for “AddinsManager.exe”.

3. We also got records of AddinsManager.exe although we couldn't see them in Network Usage tab.

# Malware run on Local System account.

52103	57302	2018-03-15 09:15:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)
52203	57336	2018-03-15 09:19:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728
52248	57381	2018-03-15 10:20:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)
52250	57383	2018-03-15 10:20:00	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe	S-1-5-18 ( Local System)
52287	57420	2018-03-15 10:20:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728
52217	57450	2018-03-15 11:20:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)

Rundll32.exe with cmd.exe at these timestamps.  
 The attacker is like to have been doing something.

58074	63207	2018-03-19 09:02:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728
58103	63236	2018-03-19 10:03:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)
58104	63237	2018-03-19 10:03:00	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe	S-1-5-18 ( Local System)
58141	63274	2018-03-19 10:03:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728
58174	63307	2018-03-19 11:03:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)
58175	63308	2018-03-19 11:03:00	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe	S-1-5-18 ( Local System)
58214	63347	2018-03-19 11:03:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728

59597	64730	2018-03-20 09:38:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728
59630	64763	2018-03-20 10:41:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)
59656	64789	2018-03-20 10:41:00	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe	S-1-5-18 ( Local System)
59676	64809	2018-03-20 10:41:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728

## The attacker might have mounted a network drive, and execute JScrips or VBScripts.

2018-03-22 08:06:00 \Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)	6.91E+09
2018-03-22 08:06:00 \Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe	S-1-5-18 ( Local System)	27107134
2018-03-22 08:06:00 \Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1106	4.93E+08
2018-03-22 09:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)	7.09E+09
2018-03-22 09:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe	S-1-5-18 ( Local System)	7.35E+08
2018-03-22 09:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\cscript.exe	S-1-5-18 ( Local System)	7.7E+08
2018-03-22 09:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\net.exe	S-1-5-18 ( Local System)	56454596
2018-03-22 09:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1106	4.58E+08
2018-03-22 10:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)	7.21E+09
2018-03-22 10:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe	S-1-5-18 ( Local System)	7.64E+08
2018-03-22 10:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\xcopy.exe	S-1-5-18 ( Local System)	4.47E+08
2018-03-22 10:07:00 \Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1106	5.85E+08
2018-03-22 11:08:00 \Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)	9.51E+09
2018-03-22 11:08:00 \Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe	S-1-5-18 ( Local System)	74524422
2018-03-22 11:08:00 \Device\HarddiskVolume2\Windows\SysWOW64\xcopy.exe	S-1-5-18 ( Local System)	0
2018-03-22 11:08:00 \Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1106	1.1E+09
2018-03-22 12:08:00 \Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)	6.92E+09
2018-03-22 12:08:00 \Device\HarddiskVolume2\Windows\SysWOW64\xcopy.exe	S-1-5-18 ( Local System)	0
2018-03-22 12:08:00 \Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1106	5.17E+08
2018-03-22 13:09:00 \Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)	6.92E+09
2018-03-22 13:09:00 \Device\HarddiskVolume2\Windows\SysWOW64\xcopy.exe	S-1-5-18 ( Local System)	0

xcopy is recorded repeatedly, but CPU wasn't used at all here. It might have been a zombie process or have remained for some reasons.

As we have already seen these activities before, xcopy was executed for a relatively long time and they copied data from external hosts.

W64\xcopy.exe	S-1-5-18 ( Local System)	0
W64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1106	1.1E+09
W64\rundll32.exe	S-1-5-18 ( Local System)	6.92E+09
W64\xcopy.exe	S-1-5-18 ( Local System)	0
W64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1106	5.17E+08
W64\rundll32.exe	S-1-5-18 ( Local System)	6.92E+09
W64\xcopy.exe	S-1-5-18 ( Local System)	0

When you filter with “Syswow64”, you can find several rundll32 with cmd.exe. The attacker was doing something.

2018-03-23 03:19:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)	6.38E+09
2018-03-23 03:19:00	\Device\HarddiskVolume2\Windows\SysWOW64\xcopy.exe	S-1-5-18 ( Local System)	0
2018-03-23 03:19:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1106	5.36E+08
2018-03-23 04:20:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)	1.16E+10
2018-03-23 04:20:00	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe	S-1-5-18 ( Local System)	7.06E+08
2018-03-23 04:20:00	\Device\HarddiskVolume2\Windows\SysWOW64\xcopy.exe	S-1-5-18 ( Local System)	1.81E+08
2018-03-23 04:20:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1106	2.61E+09
2018-03-23 05:20:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)	6.97E+09
2018-03-23 05:20:00	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe	S-1-5-18 ( Local System)	1.3E+08
2018-03-23 05:20:00	\Device\HarddiskVolume2\Windows\SysWOW64\xcopy.exe	S-1-5-18 ( Local System)	0
2018-03-23 05:20:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1106	5.74E+08
2018-03-23 06:21:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)	7.71E+09
2018-03-23 06:21:00	\Device\HarddiskVolume2\Windows\SysWOW64\xcopy.exe	S-1-5-18 ( Local System)	0
2018-03-23 06:21:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-21-3671970501-3975728774-4289435121-1106	7.85E+08
2018-03-23 07:22:00	\Device\HarddiskVolume2\Windows\SysWOW64\rundll32.exe	S-1-5-18 ( Local System)	7.88E+09
2018-03-23 07:22:00	\Device\HarddiskVolume2\Windows\SysWOW64\xcopy.exe	S-1-5-18 ( Local System)	0

When you filter with “ProgramData”, you can find execution of 7.exe and l.exe  
the activities happened at the same time as the above activities.

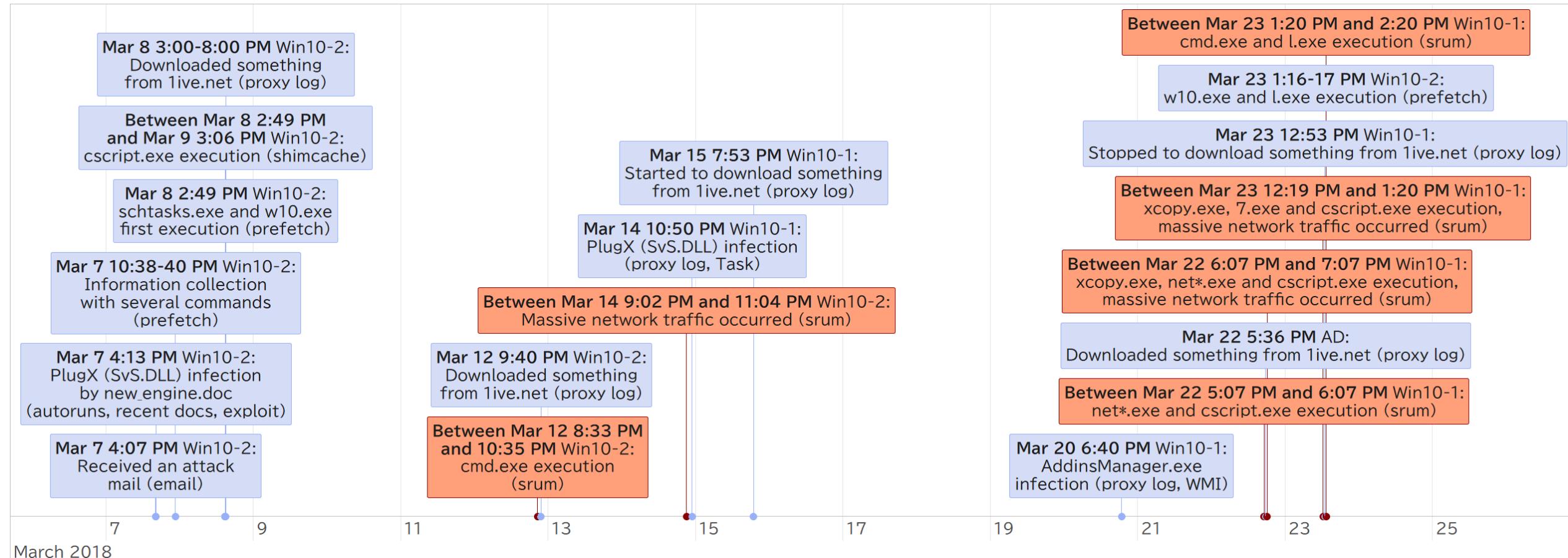
	Event ID	Source	Event Type	User SID
3	2018-02-08 07:54:00	\Device\HarddiskVolume2\ProgramData\Adobe\Setup\{AC76BA86-7A	Information	S-1-5-21-3671970501-3975728774-4289435121-1106
7	2018-03-23 04:20:00	\Device\HarddiskVolume2\ProgramData\s\7.exe	Information	S-1-5-18 ( Local System)
8	2018-03-23 05:20:00	\Device\HarddiskVolume2\ProgramData\l.exe	Information	S-1-5-18 ( Local System)

# Summary for This Lab

- You was able to find several attacker's activities.

Date Range (in JST: UTC+9:00)	Assumed Activities	Sent/Recv Bytes	
Mar 15 6:19 PM - 7:20 PM	rundll32 w/ cmd		→ We got attacker's new activities.
Mar 19 6:02 PM - 8:03 PM	rundll32 w/ cmd		
Mar 20 6:38 PM - 7:41 PM	rundll32 w/ cmd		
Mar 22 5:07 PM - 6:07 PM	rundll32 w/ net, cscript		
Mar 22 6:07 PM - 7:07 PM	rundll32 w/ xcopy, net, cscript	330,942/64,173,558	→ We were able to narrow down these attacker's activities rather than shimcache analysis and we got the exact number of the traffic volume.
Mar 23 12:19 PM - 1:20 PM	rundll32 w/ xcopy, cscript, 7.exe	46,219/32,670,032	
Mar 23 1:20 PM - 2:20 PM	rundll32 w/ cmd, l.exe		

# Scenario 1 Incident Timeline After SRUM Analysis



# UserAssist

# UserAssist

- Keeps track of frequently used applications.
  - The data contains path to the EXE file, number of times the program was executed, and timestamp the UserAssist entry was modified.
    - When the entry is updated, the timestamp will change; timestamp can be interpreted as the last time the program was executed.
- The UserAssist is recorded in registry under “HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist” key.
  - Each entry name is “ROT13” of the EXE file path.
  - Each data is in binary.

# ROT13

- ROT13 means to rotate the alphabet for 13 letters.
  - Numbers and symbols remain unchanged.

<b>First 13 Letters</b>	A	B	C	D	E	F	G	H	I	J	K	L	M
<b>Later 13 Letters</b>	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

- For example, “P:\Hfref\gneb” refers to...?



C:\Users\taro

# Characteristics of UserAssist

- Only the programs executed from Windows Explorer are recorded in UserAssist.
- Therefore, it is useful for investigating legitimate user activities.
  - For example, malware infection with social engineering, or internal attacks triggered by the user.
- If the attacker used GUI, the UserAssist may be recorded.
- Or if malware used Startup as a persistence, the evidence would be recorded in UserAssist.
  - In that case, runcount would be kept to be zero and the timestamp would be 1601/01/01.
- A researcher claimed that it can also record Scheduled Task's activities in a certain condition, although we couldn't reproduce it.
  - [https://medium.com/@forensic\\_matt/no-run-counts-in-userassist-4f2a78cb9e2c](https://medium.com/@forensic_matt/no-run-counts-in-userassist-4f2a78cb9e2c)

# Parsing UserAssist

- It will be easier to use the tool to read the UserAssist data.
  - To read the name of UserAssist entries, it is necessary to calculate ROT13.
  - The contents of UserAssist data are in binary format.
- Registry Explorer by Eric Zimmerman
  - It can parse UserAssist both online and offline.
- UserAssistView by NirSoft
  - Useful for parsing UserAssist of the running machine.
  - Since it cannot read contents of the offline hosts, one way is to use the Registry Explorer for viewing them.

The screenshot shows the Registry Explorer interface with the 'UserAssist' key selected. The left pane displays a tree view of registry keys under 'UserAssist', including 'Count', 'VirtualDesktops', 'VisualEffects', 'Wallpapers', 'Ext', 'FileAssociations', 'FileHistory', 'GameDVR', 'Group Policy', 'GrpConv', and several GUID entries. The right pane shows a table of UserAssist entries with columns: Program Name, Run ..., Foc..., Focus Time, and Last Executed. An entry for 'WindowsPowerShell\v1.0\powershell.exe' is highlighted. The bottom status bar shows 'Selected hive: NTUSER.DAT' and 'Last write: 2019-06-14 03:52:07'.

The screenshot shows the UserAssistView application window. The main table lists UserAssist entries with columns: Item Name, Index, Count, Modified Time, and ClassID. The entries are identical to those shown in the Registry Explorer. The bottom status bar shows '67 item(s), 1 Selected' and 'NirSoft Freeware. http://www.nirsoft.net'.

Item Name	Index	Count	Modified Time	ClassID
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe	11	4	6/14/2018 6:24:12 PM	(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA)
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mmc.exe	27	2	6/11/2018 7:38:05 PM	(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA)
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\msdt.exe	45	0		(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA)
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe	3	8	5/18/2018 9:44:09 AM	(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA)
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe	4	21	6/14/2018 4:52:27 PM	(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA)
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\oobe\FirstLogonAnim.exe	5	0		(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA)
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe	15	0		(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA)
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Usoclient.exe	1	14	5/18/2018 9:44:09 AM	(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA)
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WindowsPowerShell\v1.0\p... 29	30	0		(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA)
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WindowsPowerShell\v1.0\p... 12	32	3	5/18/2018 12:51:10 PM	(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA)
{6D809377-6A0F-444B-8957-A3773F02200E}\Internet Explorer\iexplore.exe	1	1	6/11/2018 9:41:00 PM	(CEBFF5CD-ACE2-4F4F-9178-9926F41749EA)

# Scenario 1 Labs:

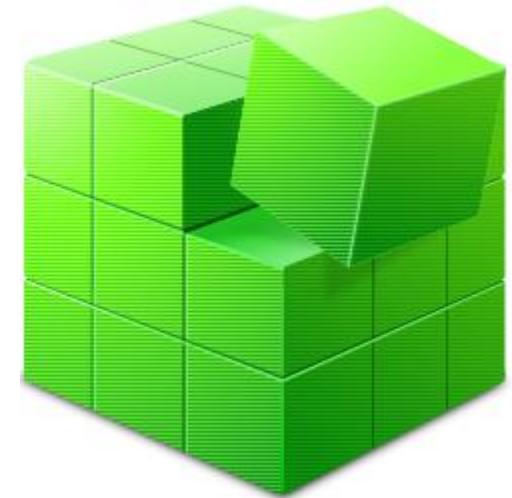
## Lab 6: Parsing UserAssist for Client-Win10-2

# Parsing UserAssist

- The goal is to look into UserAssist to see if any interesting data is remaining.

# Opening Per-User Hive

- Since UserAssist resides in per-user registry hive, we will use Registry Explorer to see the data.
- When Registry Explorer is opened, select “Load offline hive” under “File” menu.
- Open **G:\Users\honda\NTUSER.DAT** hive.
  - If the disk image is not mounted as “G”, modify the drive letter.
  - When you open “honda” folder, you will be asked to obtain permission.
- There is a bookmark for UserAssist in Registry Explorer.



Registry Explorer v1.4.2.0

File Tools Options Bookmarks (19/0) View Help

Registry hives (1) A Common (19)

Manage bookmarks Ctrl+B

UserAssist {9E04CAB2-CC14-11DF-BB8C-A2F1DED72085} {A3D53349-6E61-4557-8FC7-0028EDCEEBF6} Count {B267E3AD-A825-4A09-82B9-EEC22AA3B847} {BCB48336-4DDD-48FF-BB0B-D3190DACB3E2} {CAA59E3C-4792-41A5-9909-6A6A8D32490E} {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA} Count {F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442} {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F} Count {FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BD} VirtualDesktops VisualEffects Wallpapers Ext FileAssociations FileHistory GameDVR Group Policy

7-Zip (7-Zip history and config)  
Applets (Last Registry Viewed)  
CD Burning (CDROM burning info)  
ComDlg32 (Common dialog)  
CurrentVersion (Windows)  
CurrentVersion (Windows NT)  
FileExts (List of programs used to open files by extension)  
FileHistory (File history info)  
FTP (FTP server and username info)  
Internet Settings (Internet Explorer settings)  
Main (IE Browser Settings)  
MountPoints2 (Mounted devices)  
PrinterPorts (Printer info)  
RecentDocs (Recently opened files by extension)  
Run (User run key)  
RunMRU (Most recently run programs)  
Shell Folders (Default locations for user created content)  
TypedURLs (URLs entered by a user)  
UserAssist (Recently accessed items)

Time	Last Executed
=	
0h, 00m, 00s	
0h, 07m, 00s	2019-05-28 05:23:46
6h, 33m, 00s	
0h, 07m, 00s	2019-06-14 02:20:19
0h, 57m, 58s	2019-06-12 08:39:33
0h, 00m, 52s	
1h, 49m, 16s	
0h, 50m, 40s	
0h, 00m, 47s	
0h, 00m, 19s	
0h, 00m, 03s	
0h, 10m, 05s	2019-05-28 07:01:24

Export ?

Current offset: 0 (0x0) Bytes selected: 0 (0x0) Data interpreter ?

Key: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}

Selected hive: NTUSER.DAT Last write: 2019-06-14 03:52:07 37 of 37 values shown (100.00%) Copied path to clipboard Hidden keys: 0 7

# Observing UserAssist

- When you look into the UserAssist, you can see that the “Value Name” and the “Program Name” columns are in ROT13 relations.
- You can also see the parameters such as Run Counter, Focus Count, Focus Time and the Last Executed date/time.

The screenshot shows three windows from the Registry Explorer application (v1.4.3.0) illustrating the UserAssist registry keys and their values.

**Left Window:** Shows the registry tree under the key `Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist`. The tree includes StreamMRU, Streams, StudRects3, Taskband, TVWinUI, TypedPaths, User Shell Folders, and various UserAssist entries. Each entry has subkeys like Count and a timestamp.

**Middle Window:** Shows the details for a specific UserAssist entry. The "Values" tab is selected, displaying a table with columns: Value Name, Value Type, Data, Value Size, Is Deleted, and Data Rec... . The data shows various ROT13 encoded strings corresponding to the UserAssist key names.

Value Name	Type	Data	Value Size	Is Deleted	Data Rec...
(7)SN40RS-N050-40SP-874N-P052R0095N8R\pbzzba Svyrf\Ngbor\NEZ\1.0\NgborNEZ.rkr	RegBinary	00...	0C-00-00-00	□	□
(Q5232100-0251-4857-N4PR-N8R7P6N7Q27)QJWIA.RKR	RegBinary	00...	0C-00-00-00	□	□
(S3805404-1Q41-4252-9305-67Q0028SP23)\Vgrafalccf\Vpebfbsg.Jvaqbjf.Pbegnan_pj5a1u2gkdrj\frnepuhV.rkr	RegBinary	00...	10-8F-04-00	□	□
R:\pove-phyyrgpbe\pove-phyyrgpbe.rkr	RegBinary	00...	20-00-53-00	□	□
(6Q809377-6N50-44HO-8957-N3733S0220R)\Vpebfbsg_Bssvr_15\Bbbg\Bssvr15\RKPRY.RKR	RegBinary	00...	28-F9-0E-00	□	□
\V\jva2012e2\pova\gbby\W\Criff-2.38.Frgh.rkr	RegBinary	00...	2D-32-00-00	□	□
(1NP1-4R77-0287-RSQ-0744-201NRS19807)\fvircp.rkr	RegBinary	00...	30-00-36-00	□	□
\V\jva2012e2\pova\gbby\W\ngp03230.rkr	RegBinary	00...	36-00-30-00	□	□
\V\jva2012e2\pova\gbby\W\pebEeqP1800920044_yvn_WC.rkr	RegBinary	00...	38-00-77-00	□	□
Zpebfbsg_Jvaqbjf.EzdgzQrhgbc	RegBinary	00...	45-00-20-00	□	□
P:\V\fre\fu\baap\Q\rfxgb\be\qr\pasevezngvba-z\ngn-20180221-09.rkr	RegBinary	00...	61-74-65-00	□	□
(7)SN40RS-N050-40SP-874N-P052R0095N8R\NggnprnPrf3\NggnprnPrf.rkr	RegBinary	00...	65-00-21-00	□	□
Zpebfbsg_Bssvr_JVAJBECK.RKR.15	RegBinary	00...	66-00-39-00	□	□
(1NP1-4R77-0287-RSQ-0744-201NRS19807)\H\pby\yrag.rkr	RegBinary	00...	68-58-0E-00	□	□
Zpebfbsg_NhgbTrarengq.(97880R4R-9653-3CN7-990P-Q245R15652R)	RegBinary	00...	70-00-70-00	□	□
P:\V\fre\fu\baap\Q\rfxgb\be\qr\pasevezngvba-z\ngn-20180302-02 (2).rkr	RegBinary	00...	70-39-12-00	□	□
Zpebfbsg_Bssvr_15.PypvgGdha	RegBinary	00...	72-00-61-00	□	□
(6Q809377-6N50-44HO-8957-N3733S0220R)\V\zner\Zjner_Gbby\rgbbyfq.rkr	RegBinary	00...	73-68-00-00	□	□

**Right Window:** Shows the details for a specific UserAssist entry. The "Program Name" tab is selected, displaying a table with columns: Program Name, Run Counter, Focus Count, Focus Time, and Last Executed.

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
UEME_CTLCUCount:ctor	0	0	0d, 0h, 00m, 00s	
Microsoft.Getstarted_8wekyb3d8bbwe!App	14	23	0d, 0h, 07m, 08s	2018-01-30 02:40:43
UEME_CTLSESSION	265	1046	0d, 17h, 06m, 51s	
Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe!App	13	19	0d, 0h, 06m, 15s	2018-01-30 02:40:43
Microsoft.WindowsMaps_8wekyb3d8bbwe!App	12	17	0d, 0h, 05m, 30s	2018-01-30 02:40:43
Microsoft.People_8wekyb3d8bbwe!x4c7a3b7dy2188y46d4ya362y19ac5a5805e5x	11	15	0d, 0h, 04m, 45s	2018-01-30 02:40:43
Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe!App	10	13	0d, 0h, 04m, 00s	2018-01-30 02:40:43
(System32)\snippingTool.exe	9	11	0d, 0h, 03m, 15s	2018-01-30 02:40:43
Microsoft.WindowsCalculator_8wekyb3d8bbwe!App	8	9	0d, 0h, 02m, 30s	2018-01-30 02:40:43
(System32)\mspaint.exe	8	8	0d, 0h, 02m, 05s	2018-02-27 06:23:57
(System32)\notepad.exe	8	12	0d, 0h, 01m, 54s	2018-03-06 08:17:01
Microsoft.Windows.Explorer	17	261	0d, 2h, 41m, 11s	2018-03-23 11:52:08
Microsoft.Windows.Shell.RunDialog	0	0	0d, 0h, 00m, 03s	
(System32)\cmd.exe	3	9	0d, 0h, 06m, 57s	2018-02-26 03:16:29

# Observing EXE UserAssist for User honda

- UserAssist mainly consists of keys that record EXE files and LNK files.
  - {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA} : for EXE
  - {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F} : for LNK (shortcuts)
- The figure below shows EXE records in NTUSER.DAT, for user honda on client-win10-2.
- If you sort it with “Last Executed” column, it can be viewed in chronological order.
- Since UserAsisst is recorded when the programs were executed from the Windows Explorer, CLI operations over RAT will not be recorded in it.

The screenshot shows a Windows Registry Editor window with two panes. The left pane displays a tree view of registry keys under 'Key name'. The right pane shows a grid of records with columns: Program Name, Run Counter, Focus Count, Focus Time, and Last Executed. The 'Last Executed' column is sorted chronologically, showing various applications like AttachéCase.exe, Microsoft.RemoteDesktop, Microsoft.PowerPoint, Adobe Acrobat Reader, Chrome, KeePass Password Safe, and Microsoft Word.

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
{Program Files x86}\AttachéCase\AttachéCase.exe	3	15	0d, 0h, 03m, 55s	2018-03-15 09:36:40
Microsoft.Windows.RemoteDesktop	1	1	0d, 0h, 14m, 49s	2018-03-14 13:33:45
Microsoft.Office.POWERPNT.EXE.15	5	3	0d, 0h, 00m, 29s	2018-03-14 04:54:05
{Program Files x86}\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	5	10	0d, 0h, 01m, 28s	2018-03-12 05:50:48
Chrome	5	35	0d, 0h, 30m, 31s	2018-03-12 05:50:43
{Program Files x86}\KeePass Password Safe 2\KeePass.exe	3	24	0d, 0h, 09m, 04s	2018-03-09 06:04:34
{Program Files X64}\Microsoft Office 15\Root\Office15\WINWORD.EXE	2	0	0d, 0h, 00m, 00s	2018-03-07 07:11:46

# Observing LNK UserAssist for User honda

- The image below is UserAssist of LNK on client-win10-2.
- On March 14 at 10:50 PM (JST:UTC+9:00), when infection of client-win10-1 occurred, execution of Remote Desktop Connection is recorded.
  - We should figure out if the user happened to run the Remote Desktop client at this time, or it was opened by the attackers.

The screenshot shows two windows side-by-side. The left window is a file explorer displaying a list of LNK files in a folder structure. The right window is the UserAssist tool showing a detailed list of executed programs. A red box highlights the 'Last Executed' column in the UserAssist table, which shows the date and time of the most recent execution. Another red box highlights the date and time 'March 14 at 10:33 PM (JST)'.

Program Name	Run Counter	Focus...	Focus Time	Last Executed
{Common Programs}\Accessories\Remote Desktop Connection.lnk	1	0	0d, 0h, 00m, 00s	2018-03-14 13:33:45
{User Pinned}\TaskBar\PowerPoint 2013.lnk	5	0	0d, 0h, 00m, 00s	2018-03-14 04:54:05
C:\Users\Public\Desktop\Acrobat Reader DC.lnk	5	0	0d, 0h, 00m, 00s	2018-03-12 05:50:48
C:\Users\Public\Desktop\Google Chrome.lnk				
C:\Users\honda\Desktop\KeePass 2.lnk				
{Programs}\Accessories\Notepad.lnk	8	0	0d, 0h, 00m, 00s	2018-03-06 08:17:01

# Amcache.hve

# Amcache.hve

- Amcache.hve is another application compatibility feature that was introduced in Windows 8.
  - In Windows Vista and 7, another feature “RecentFile.bcf” was used.
  - Amcache.hve was later added to Windows 7.
- It is recorded in **%WinDir%\AppCompat\Programs\Amcache.hve** file.
  - Requires Administrative privilege to open the path.
  - The file cannot be copied while Windows is running.
  - %WinDir% is typically mapped to C:\Windows.
- The file is in Registry (hive) format.

# Contents of the Amcache.hve

- What you can find from Amcache.hve include:
  - The list of program EXE files, with their path, size, sha-1 hash and other application properties.
  - The list of device driver files, with their properties.
- You can regard each key of the last written time as the last execution times.

# Value Names

- In Amcache.hve, value names are numbers; without knowing their meanings, it is difficult to determine which item is important and which one is not.

Number	Contents
0	Product Name
1	Company Name
2	File Version
3	Language Code
4	SwitchBackContext
5	File Version
6	File Size
7	PE Header Field: SizeOfImage
8	Hash of PE Header
9	PE Header Field: Checksum

Number	Contents
c	File Description
F	Build Timestamp
11	Last Modified Timestamp
12	Created Timestamp
15	Full path to the File
17	Last Modified Timestamp 2
100	Program ID
101	SHA1 hash of the File
<i>a,b,d,10,16</i>	<i>Unknown</i>

# Tools for Amcache.hve

- Amcache Parser by Eric Zimmerman
  - <https://github.com/EricZimmerman/AmcacheParser>

```
Amcacheparser -f PATH_TO_AMCACHE --csv PATH_TO_OUTPUT_FOLDER
```

- Python-registry (amcache.py)
  - <https://github.com/williballenthin/python-registry>

```
py amcache.py PATH_TO_AMCACHE > PATH_TO_OUTPUT_FILE
```

# Note for Amcache.hve

- Note that different Amcache versions have different features. For example:
  - Amcache on Windows 10 records related to drivers. However, it no longer records non-GUI applications while former version record them. Therefore, we might not be able to get attackers' activities with it on Windows 10.
  - You can see the detail analysis of Amcache at the following URL.
    - [http://www.ssi.gouv.fr/uploads/2019/01/anssi-coriin\\_2019-analysis\\_amcache.pdf](http://www.ssi.gouv.fr/uploads/2019/01/anssi-coriin_2019-analysis_amcache.pdf)
- David Cowen said:

*Amcache added the executable we left on the desktop but did not execute on Friday at 5am UTC saturday, the process event log showed it was a background task manager.*

<https://www.hecfblog.com/2018/11/daily-blog-550-forensic-lunch-test.html>

<https://www.hecfblog.com/2018/11/daily-blog-551-forensic-lunch-test.html>

<https://www.hecfblog.com/2018/11/daily-blog-552-forensic-lunch-test.html>

# SuperFetch

# SuperFetch

- SuperFetch is an addition to Prefetch for performance improvements.
  - First introduced in Windows Vista.
- Prefetch primarily focused on boot and application startup. The SuperFetch focuses on historical information and memory management.
- SuperFetch data is stored in the following database files under “C:\Windows\Prefetch”: AgAppLaunch.db, AgGIFaultHistory.db, AgGIFgAppHistory.db, AgGIGlobalHistory.db, AgGIUAD\_P\_<SID>.db, AgGIUAD\_<SID>.db and AgRobust.db.
  - Need Administrative privileges to see them.

# Tools for Analyzing SuperFetch

- CrowdResponse by CrowdStrike
  - <https://www.crowdstrike.com/resources/community-tools/crowdresponse/>
- rewolf-superfetch-dumper
  - <https://github.com/rwfpl/rewolf-superfetch-dumper>
- libagdb by libyal
  - <https://github.com/libyal/libagdb>

# Analyzing Superfetch by CrowdResponse

- For example, you can use it with these two commands to get outputs on 64 bit environment.

```
CrowdResponse64.exe @SuperFetch -6s "F:\Windows\Prefetch" > superfetch_cr.xml  
CRconvert.exe -s -t -f superfetch_cr.xml -o output_dir
```

	A	B	C	D
1	process	launchcount	fgcount	path
2	CONHOST.EXE	4	209	? CONHOST.EXE
3	GPUPDATE.EXE	22	241	? GPUPDATE.EXE
4	MPCMDRUN.EXE	15	152	? MPCMDRUN.EXE
5	?	0	231	? CDIR-COLLECTOR.EXE
6	CONSENT.EXE	18	163	? CONSENT.EXE
7	DSMUSERTASK	2	63	? DSMUSERTASK.EXE
8	FIREFOX.EXE	0	151	? FIREFOX.EXE
9	OUTLOOK.EXE	0	219	? OUTLOOK.EXE

	A	B	C
1	timestamp	period	path
2	2018-01-26T16:56:36Z	Weekday 12 to 6AM	? MPCMDRUN.EXE
3	2018-01-27T14:07:24Z	Weekday 12 to 6AM	? MPCMDRUN.EXE
4	2018-01-27T14:08:48Z	Weekday 12 to 6AM	? SIHOST.EXE
5	2018-01-27T14:08:48Z	Weekday 12 to 6AM	? EXPLORER.EXE
6	2018-01-27T14:08:48Z	Weekday 12 to 6AM	?
7	2018-01-27T14:08:48Z	Weekday 12 to 6AM	?
8	2018-01-27T14:08:49Z	Weekday 12 to 6AM	? OUTLOOK.EXE
9	2018-01-27T14:08:54Z	Weekday 12 to 6AM	?

# BAM

# BAM

- Stands for “Background Activity Moderator”
  - We are not talking about “Business Activity Monitoring” in this class.
- BAM resides in registry under  
“HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\bam\Use  
rSettings” key.
- This is relatively new feature that was introduced in Windows 10  
version 1709, and we have confirmed to exist at least until on 1903.
  - The service does not exist in Windows 8.1 and older, and earlier versions of  
Windows 10.

# BAM Contents

- BAM also has list of applications, last executed timestamps, and some other data.
- Since BAM is relatively new, some history cleaning tools may not be aware of the BAM.
  - Could be one of the locations where the histories may remain even when other artifacts were cleared.

Name	Type	Data
Default	REG_SZ	(value not set)
\Device\HarddiskVolume4\Windows\explorer.exe	REG_BINARY	17 f0 38 71 b1 19 d4 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
\Device\HarddiskVolume4\Windows\regedit.exe	REG_BINARY	3e 4c d5 98 b1 19 d4 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
\Device\HarddiskVolume4\Windows\System32\oobe\FirstLogonAnim.exe	REG_BINARY	f0 e7 28 c2 51 04 d4 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
\Device\HarddiskVolume4\Windows\System32\rundll32.exe	REG_BINARY	92 c6 25 a6 b1 19 d4 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
CanonicalGroupLimited.UbuntuonWindows_79rhkp1fndgsc	REG_BINARY	65 85 3f 6b 2c f3 d3 01 00 00 00 00 00 00 01 00 00 02 00 00 00
Microsoft.LockApp_cw5n1h2byewy	REG_BINARY	b7 5c cc dc 52 04 d4 01 00 00 00 00 00 00 01 00 00 02 00 00 00
Microsoft.MicrosoftEdge_8wekyb3d8bbwe	REG_BINARY	3a 0a ee 17 b9 f1 d3 01 00 00 00 00 00 00 01 00 00 02 00 00 00
Microsoft.WinDbg_8wekyb3d8bbwe	REG_BINARY	c1 be 5a 63 b9 f1 d3 01 00 00 00 00 00 00 01 00 00 02 00 00 00
Microsoft.Windows.Cortana_cw5n1h2byewy	REG_BINARY	42 51 20 72 b1 19 d4 01 00 00 00 00 00 00 01 00 00 02 00 00 00
Microsoft.Windows.SecHealthUI_cw5n1h2byewy	REG_BINARY	41 8f f6 fb 9d db d3 01 00 00 00 00 00 01 00 00 02 00 00 00
Microsoft.Windows.ShellExperienceHost_cw5n1h2byewy	REG_BINARY	3b 98 4a 70 b1 19 d4 01 00 00 00 00 00 00 01 00 00 02 00 00 00
Microsoft.WindowsStore_8wekyb3d8bbwe	REG_BINARY	3f d9 9a 01 4a 04 d4 01 00 00 00 00 00 00 01 00 00 02 00 00 00
SequenceNumber	REG_DWORD	0x0000000b (11)
Version	REG_DWORD	0x00000001 (1)
windows.immersivecontrolpanel_cw5n1h2byewy	REG_BINARY	cd 8f 57 c2 45 04 d4 01 00 00 00 00 00 00 01 00 00 02 00 00 00

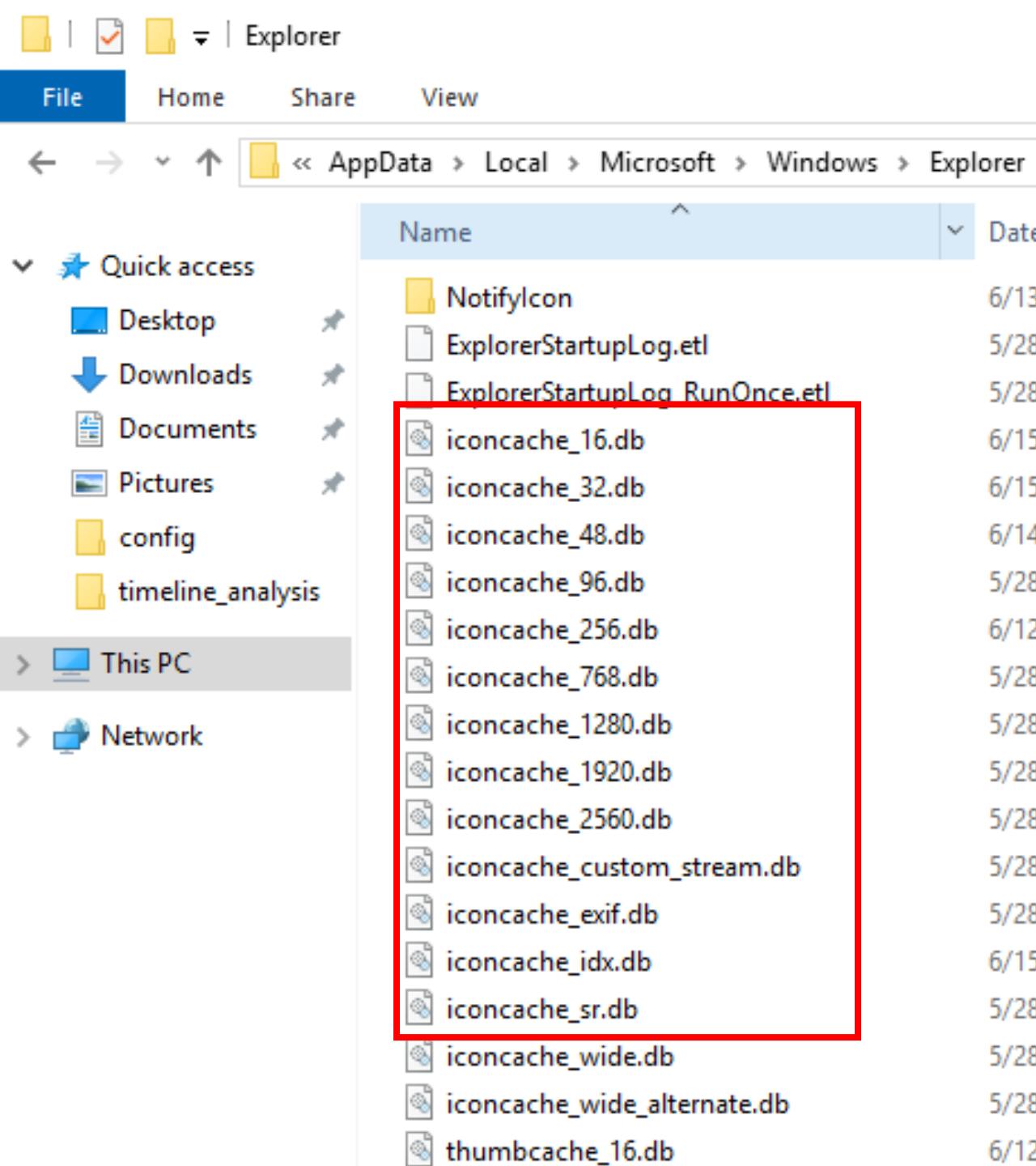
# IconCache.db

# IconCache.db (1)

- Strictly speaking, This artifact isn't for confirming program execution. However, you might be able to find unknown executable names and their icons which a user displayed executables in the Explorer process by analyzing IconCache.db.
- You can find it in the following path.
  - Windows 7 or later
    - C:\Users\<user\_name>\AppData\Local
      - You can get file paths of executables by analyzing it.
    - Windows 8 and 10
      - C:\Users\<user\_name>\AppData\Local\Microsoft\Windows\Explorer
        - You can get icons of executables by analyzing them.

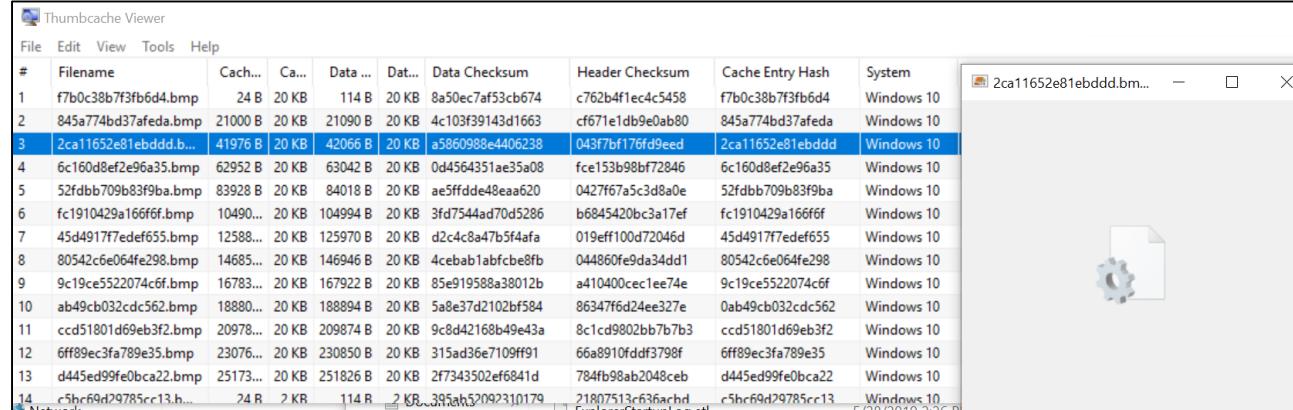
# IconCache.db (2)

- There is a variety of IconCache.db files in Windows 8 and later.



# Tools for IconCache.db

- You will need different tools for different paths because the file formats are different.
  - C:\Users\<user\_name>\AppData\Local\IconCache.db
    - strings
      - We are not sure the file format. However, the paths strings are stored as UTF-16-LE. You can use strings command.
  - C:\Users\<user\_name>\AppData\Local\Microsoft\Windows\Explorer\IconCache\*.db
    - libwtcdb by libyal (<= Win 8.1)
      - <https://github.com/libyal/libwtcdb>
    - Thumbcache Viewer
      - <https://thumbcacheviewer.github.io/>
      - The file format is the same as thumbnailcache.



#	Filename	Cach...	Ca...	Data ...	Dat...	Data Checksum	Header Checksum	Cache Entry Hash	System
1	f7b0c38b7f3fb6d4.bmp	24 B	20 KB	114 B	20 KB	8a50ec7af53cb674	c762b4f1ec4c5458	f7b0c38b7f3fb6d4	Windows 10
2	845a774bd37afeda.bmp	21000 B	20 KB	21090 B	20 KB	4c103f39143d1663	cf671e1db9e0ab80	845a774bd37afeda	Windows 10
3	2ca11652e81ebddd.bmp...	41976 B	20 KB	42066 B	20 KB	a5860988e4406238	043f7bf176fd9eed	2ca11652e81ebddd	Windows 10
4	6c160d8ef2e96a35.bmp	62952 B	20 KB	63042 B	20 KB	0d456431ae35a08	fce153b98bf72846	6c160d8ef2e96a35	Windows 10
5	52fdbb709b83f9ba.bmp	83928 B	20 KB	84018 B	20 KB	ae5ffdde48eaa620	0427f67a5c3d8a0e	52fdbb709b83f9ba	Windows 10
6	fc1910429a166f6f.bmp	10490...	20 KB	104994 B	20 KB	3fd7544ad70d5286	b6845420bc3a17ef	fc1910429a166f6f	Windows 10
7	45d4917f7edef655.bmp	12588...	20 KB	125970 B	20 KB	d2c4c8a47b5f4afa	019eff100d72046d	45d4917f7edef655	Windows 10
8	80542c6e064fe298.bmp	14685...	20 KB	146946 B	20 KB	4cebabb1bfccbe8fb	044860fe9da34d1	80542c6e064fe298	Windows 10
9	9c19ce5522074c6f.bmp	16783...	20 KB	167922 B	20 KB	85e919588a38012b	a410400cec1ee74e	9c19ce5522074c6f	Windows 10
10	ab49cb032cdc562.bmp	18880...	20 KB	188894 B	20 KB	5a8e37d2102bf58a	86347f6d24ee327e	0ab49cb032cdc562	Windows 10
11	cc5d1801d69eb3f2.bmp	20978...	20 KB	209874 B	20 KB	9c8d42168b49e43a	8c1cd9802bb7b7b3	cc5d1801d69eb3f2	Windows 10
12	6ff89ec3fa789e35.bmp	23076...	20 KB	230850 B	20 KB	315ad36e7109ff91	66a8910fdfd3798f	6ff89ec3fa789e35	Windows 10
13	d445ed99fe0bca22.bmp	25173...	20 KB	251826 B	20 KB	2f7343502ef6841d	784fb98ab2048ceb	d445ed99fe0bca22	Windows 10
14	c5hc69d29785cc13.h...	24 R	2 KR	114 R	2 KR	395ah52092310179	21807513-f36achd	c5hc69d29785cc13	Windows 10
	Network								5/28/2019 2:26 PM

# Syscache

# SysCache

- SysCache is a program execution artifact only on Windows 7 and Windows Server 2008 R2.
  - <https://dfir.ru/2018/12/02/the-cit-database-and-the-syscache-hive/>
  - <https://dfir.ru/2019/01/04/what-writes-to-the-syscache-hive/>
  - <https://www.hecfblog.com/2018/12/daily-blog-563-forensic-lunch-test.html>
- Tools
  - Syscache is a HIVE. You can parse it with registry parsers such as Registry Explorer and yarp. However, you will need to parse data on your own.
- File Path:
  - C:\System Volume Information\Syscache.hve

The screenshot shows a software interface for analyzing the SysCache hive. On the left, a tree view displays the structure of the hive, starting with 'C:\Users\taro\Desktop...' and its subkeys like 'DefaultObjectStore', 'IndexTable', 'LruList', and 'ObjectTable'. Each key has associated '# values' and '# subkeys'. On the right, a large data viewer pane shows a table of data records. The columns include 'Key name', 'Data', and 'Data Record'. Below the table, there are two viewers: 'Type viewer' and 'Slack viewer', which show binary data in hex and ASCII formats respectively. At the bottom, status information includes 'Selected hive: syscache.hve', 'Last write: 2018-03-30 15:35:07', '7 of 7 values shown (100.00%)', 'Load complete', and 'Hidden keys: 0'.

Key name	# values	# subkeys	Last write
C:\Users\taro\Desktop\{4062c4ef-0264-11e8-9...	=	=	
DefaultObjectStore	0	1	
IndexTable	1	3	
FileIdIndex-{406...	0	1,800	
LruList	1	1,808	
ObjectTable	0	1,800	
1	7	1	
10	7	1	
100	7	1	
101	7	1	
102	7	1	
103	7	1	
104	7	1	
105	7	1	
106	7	1	
107	7	1	
108	7	1	
109	7	1	
10A	7	1	
10B	7	1	

Drag a column header here to group by that column

...	...	Data	...	...	Data Record
...	...	258	...	...	
...	...	89672	...	...	
...	...	281474976760440	...	...	
...	...	29335936	...	...	
...	...	131614226934193228	...	...	
...	...	30-00-30-00-30-00-30-00-65-00-38-00-6...	...	...	
...	...	30-00-30-00-30-00-30-00-64-00-63-00-6...	...	...	

Type viewer Slack viewer

00	01	02	03	04	05	06	07	
00000000	30	00	30	00	30	00	0.0.0.0.	
00000008	64	00	63	00	65	00	33	00
00000010	37	00	66	00	37	00	38	00
00000018	36	00	30	00	66	00	64	00
00000020	61	00	64	00	38	00	38	00
00000028	32	00	63	00	31	00	66	00
00000030	39	00	62	00	39	00	31	00
00000038	64	00	36	00	39	00	36	00
00000040	35	m	65	00	62	00	29	m

Current offset: 0 (0x0) Bytes selected: 0 (0x0)

Value: AeProgramID Collapse all keys

Selected hive: syscache.hve Last write: 2018-03-30 15:35:07 7 of 7 values shown (100.00%) Load complete Hidden keys: 0 1

# CITDatabase

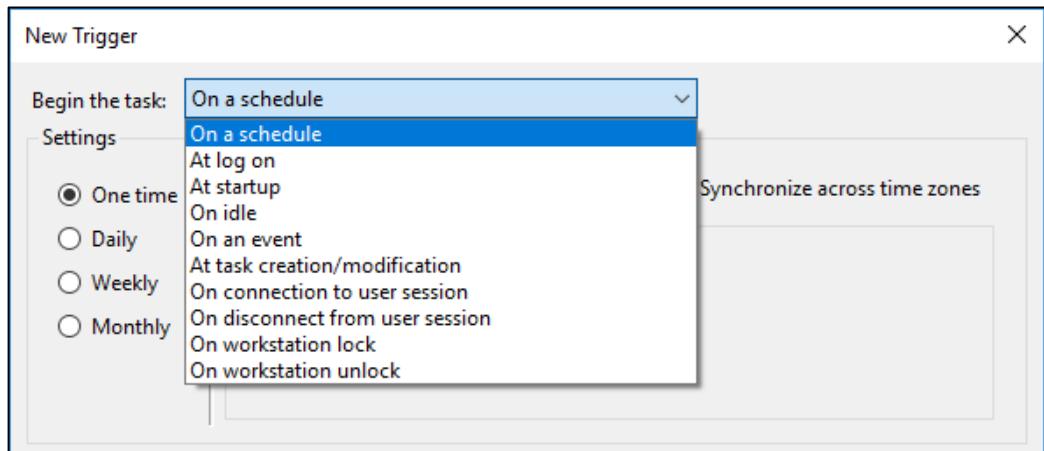
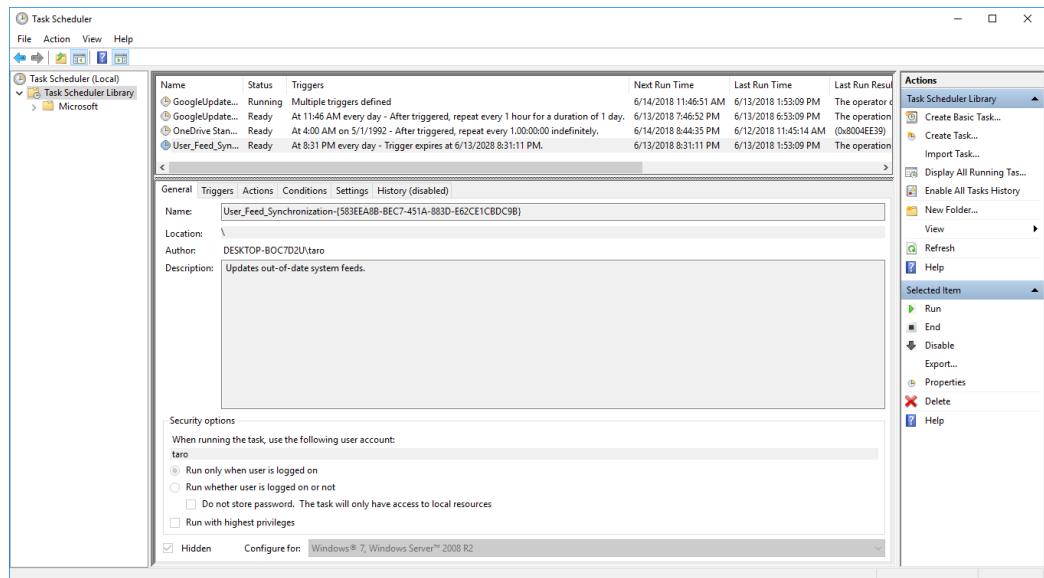
# CITDatabase

- CITDatabase is a program execution artifact on Windows 7 and Windows 8.\* only.
  - [https://twitter.com/errno\\_fail/status/1130150447157796864](https://twitter.com/errno_fail/status/1130150447157796864)
  - [https://twitter.com/errno\\_fail/status/1068654591389118470](https://twitter.com/errno_fail/status/1068654591389118470)
- You can get paths of executable files.
- CITDatabase path
  - HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\CIT\System
- Tool
  - <https://gist.github.com/msuhanov/356b724f9a44030596671427adb6fcf6>

# Task Scheduler

# Task Scheduler

- Task Scheduler is used to execute a program/command at a specified time.
  - Specified “time” does not have to be a chronological time.
    - There are options to execute the task “at log on”, “at startup”, and so on.
    - Some malware use the “at log on” to make them executed when the Windows starts up.



# Task Scheduler Commands

- **at.exe**
  - Used on Windows 7 and older.
  - Command still exists on Windows 8 and later, but it will just show a message saying that the at command is deprecated.
- **schtasks.exe**
  - Currently used command for managing task scheduler.
  - Can be used to show and modify the scheduled tasks.

```
c:\>at
The AT command has been deprecated. Please use schtasks.exe instead.

The request is not supported.

c:\>
```

```
c:\>schtasks

Folder: \
TaskName          Next Run Time      Status
=====
OneDrive Standalone Update Task-S-1-5-21 6/14/2018 5:19:28 PM Ready
User_Feed_Synchronization-{583EEA8B-BEC7} 6/13/2018 8:31:11 PM Ready

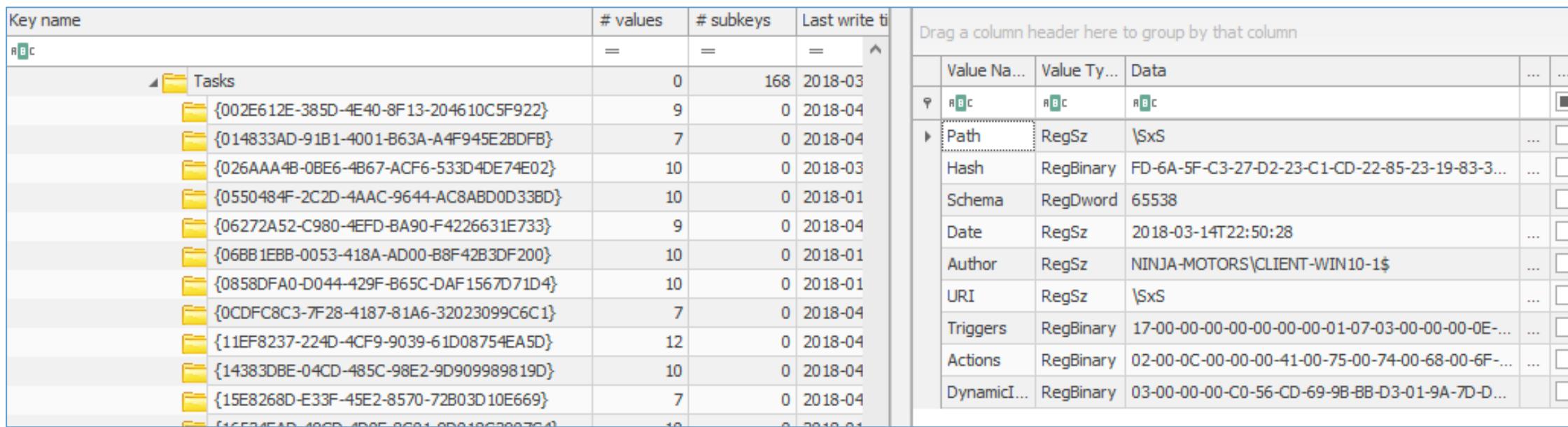
Folder: \Microsoft
TaskName          Next Run Time      Status
=====
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows
TaskName          Next Run Time      Status
=====
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows\.NET Framework
TaskName          Next Run Time      Status
=====
.NET Framework NGEN v4.0.30319        N/A       Ready
.NET Framework NGEN v4.0.30319 64      N/A       Ready
```

# Task Scheduler Artifacts

- When tasks are created, one of the following data is created to store the tasks.
  - Windows Task Scheduler or “schtasks” command:  
**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks**



The image shows two side-by-side screenshots of the Windows Registry Editor. The left screenshot displays the 'Tasks' key under 'HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache'. This key contains 168 subkeys, each represented by a yellow folder icon and a unique GUID name. The right screenshot shows a detailed view of one of these subkeys, specifically the value 'Path', which has a data type of 'RegSz' and a value of '\\$xS'. Other visible values include 'Hash' (RegBinary), 'Schema' (RegDword), 'Date' (RegSz), 'Author' (RegSz), 'URI' (RegSz), 'Triggers' (RegBinary), 'Actions' (RegBinary), and 'DynamicI...' (RegBinary). A tooltip at the top of the right pane says 'Drag a column header here to group by that column'.

Key name	# values	# subkeys	Last write ti
Tasks	=	=	=
{002E612E-385D-4E40-8F13-204610C5F922}	0	168	2018-03
{014833AD-91B1-4001-B63A-A4F945E2BDFB}	9	0	2018-04
{026AAA4B-0BE6-4B67-ACF6-533D4DE74E02}	10	0	2018-03
{0550484F-2C2D-4AAC-9644-AC8ABD0D33BD}	10	0	2018-01
{06272A52-C980-4EFD-BA90-F4226631E733}	9	0	2018-04
{06BB1EBB-0053-418A-AD00-B8F42B3DF200}	10	0	2018-01
{0858DFA0-D044-429F-B65C-DAF1567D71D4}	10	0	2018-01
{0CDFC8C3-7F28-4187-81A6-32023099C6C1}	7	0	2018-04
{11EF8237-224D-4CF9-9039-61D08754EA5D}	12	0	2018-04
{14383DBE-04CD-485C-98E2-9D909989819D}	10	0	2018-04
{15E8268D-E33F-45E2-8570-72B03D10E669}	7	0	2018-04
{4CE7A4EAD-40CD-4B0E-8C01-0D0A10C2007C41}	10	0	2018-01

Value Na...	Value Ty...	Data	...	...
RBC	RBC	RBC		
Path	RegSz	\\$xS		
Hash	RegBinary	FD-6A-5F-C3-27-D2-23-C1-CD-22-85-23-19-83-3...		
Schema	RegDword	65538		
Date	RegSz	2018-03-14T22:50:28		
Author	RegSz	NINJA-MOTORS\CLIENT-WIN10-1\$		
URI	RegSz	\\$xS		
Triggers	RegBinary	17-00-00-00-00-00-00-01-07-03-00-00-00-0E-...		
Actions	RegBinary	02-00-0C-00-00-00-41-00-75-00-74-00-68-00-6F-...		
DynamicI...	RegBinary	03-00-00-00-C0-56-CD-69-9B-BB-D3-01-9A-7D-D...		

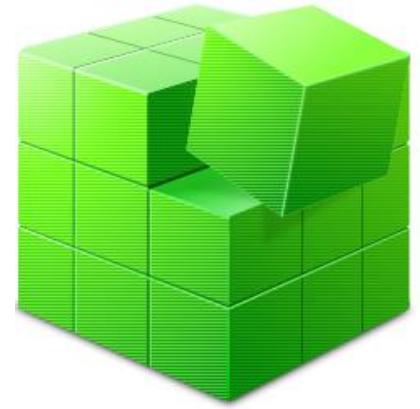
# Practice Exercise: Looking into Task Schedules

# Looking into Task Schedules

- Objectives of the exercise is to look into registry entry of task schedules.

# Looking into Registry

- In this exercise, we will use Registry Explorer by Eric Zimmerman.
  - Open RegistryExplorer.exe in the tools folder.
- We will continue using **Client-Win10-2\_honda.E01** image.
  - Please mount it if you have unmounted it.
- When Registry Explorer is opened, select “**Load offline hive**” under “File” menu.
- Open **G:\Windows\System32\config\SOFTWARE** hive.
  - If the disk image is not mounted as “G”, modify the drive letter.
  - When you open “config” folder, you will be asked to obtain permission.



# Navigating to Tasks Registry Key

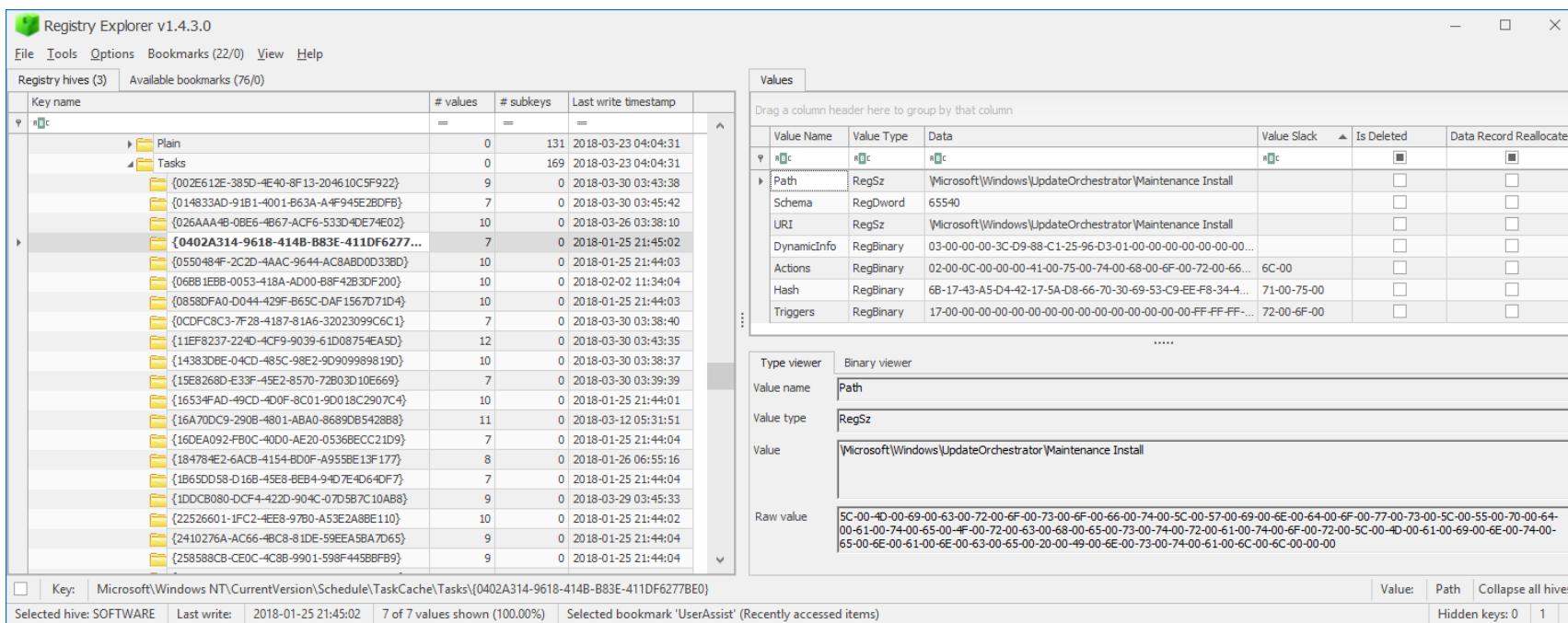
- Tasks registry key is not in the bookmark.
- To see the Tasks registry key, navigate:

**Microsoft\Windows NT\CurrentVersion\Schedule**  
**\TaskCache\Tasks**

- There are “Windows” and “Windows NT” subkeys under Microsoft. Be sure to open the right one.

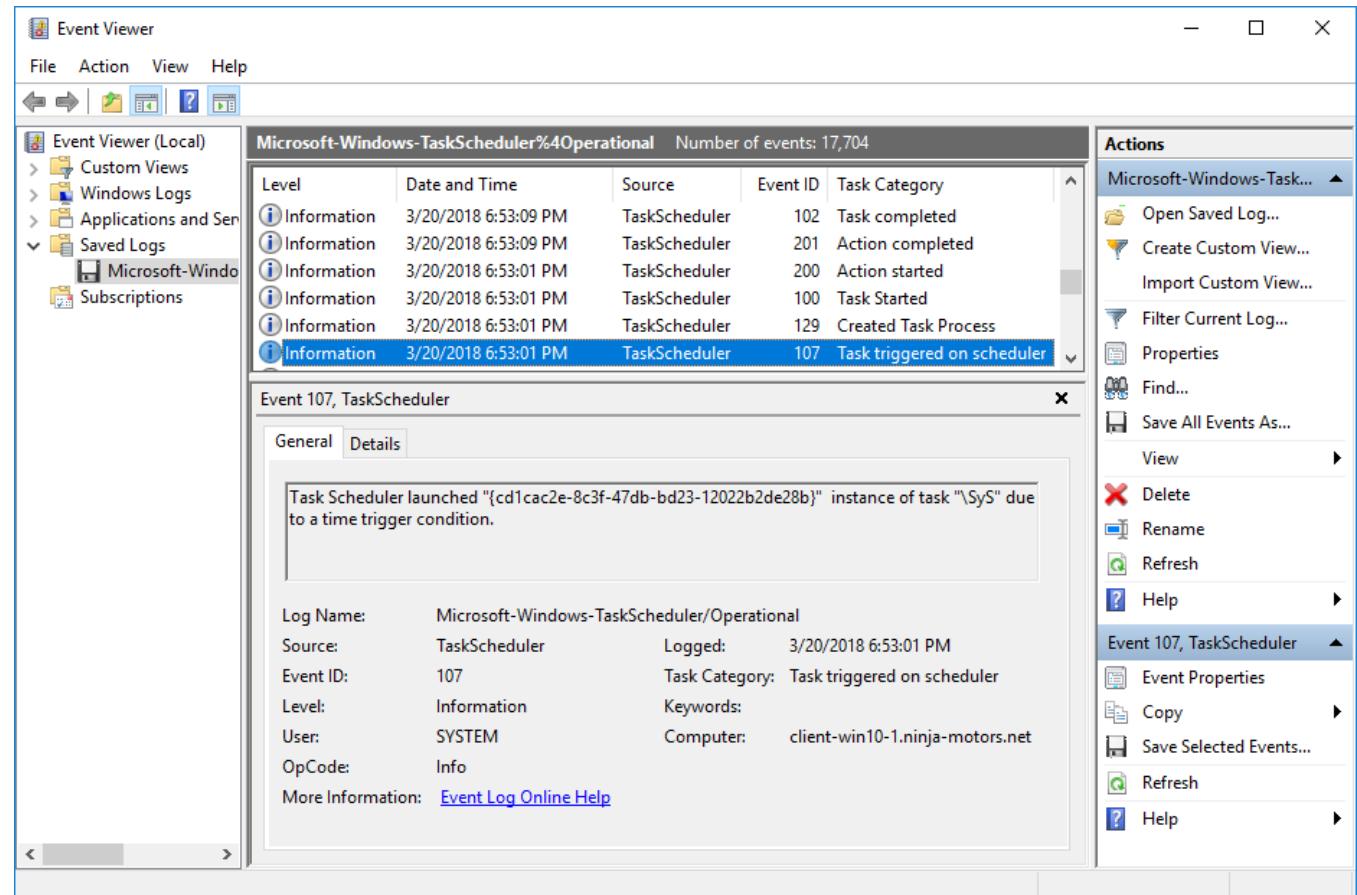
# Inspecting Tasks Registry Values

- You should be able to see the registered tasks.
  - Some values are not human-readable, but you should be able to see the task names and paths.



# Tasks Execution Histories

- When a task was executed:
  - Record remains in the Event Log.
  - Registry value of “DynamicInfo” will be updated.



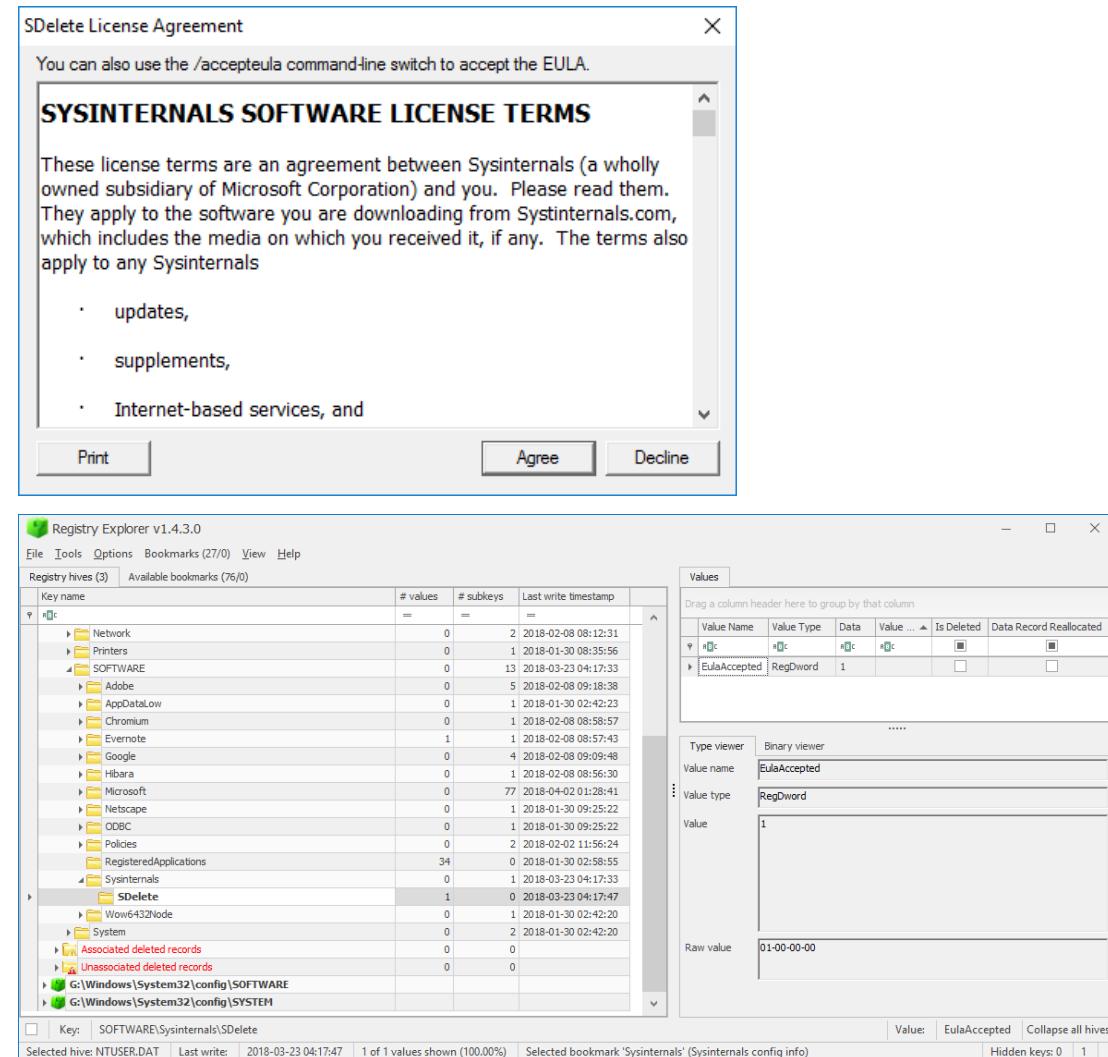
# Sysinternals Tools

# Sysinternals Tools

- Sysinternals Tools are legitimate tools hosted on Microsoft website.
  - <https://docs.microsoft.com/en-us/sysinternals/>
- Example tools include:
  - **Autoruns**: shows startup applications.
  - **Process Explorer**: shows information about running processes.
  - **Process Monitor**: monitors process activities.
  - **PsExec**: execute specified commands on a remote host.
  - **SDelete**: securely erase file by overwriting its contents for multiple times.
  - **Sysmon**: provides additional monitors to the Windows system activities.
- They are legitimate, but sometimes used by attackers in their campaigns.

# Sysinternals End-User License Agreement (EULA)

- When one of the Sysinternals tools is executed, if the user has never agreed to the license agreement, the EULA dialog will be displayed.
- Agreeing to the agreement will create a value in the per-user registry as **“SOFTWARE\Sysinternals\<tool name>\EulaAccepted”**
  - If this value exists, this means that the Sysinternals tool was executed by the user.



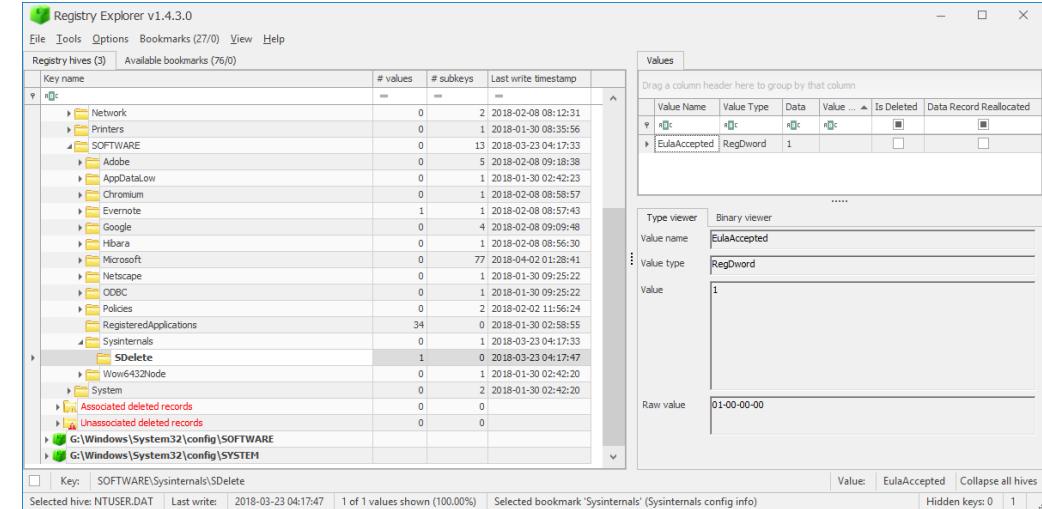
# Scenario 1 Labs:

## Lab 7: Looking into Sysinternals

### Registry Keys for Client-Win10-2

# Lab 7: Locating Sysinternals EULA (1/3)

- Using Registry Explorer, open per-user hive from G:\Users\honda\NTUSER.DAT
- Navigate to the Sysinternals registry key.
  - SOFTWARE\Sysinternals\<app name>
- Were Sysinternals suite executed on the machine? If so, which tool?
- When was the first time the tool was executed?



# Lab 7: Locating Sysinternals EULA (2/3)

The screenshot shows the Registry Explorer interface. The left pane displays a tree view of registry keys under 'Registry hives (3)'. A red box highlights the 'SDelete' key under 'Sysinternals'. The right pane shows the details for this key, including a table of values. One value, 'EulaAccepted', is selected and shown in the details panel. The timestamp for this value is 2018-03-23 04:17:47. A red callout box points to this timestamp with the text: 'From the timestamp, the first execution date/time may be found.'

Key name	# values	# subkeys	Last write timestamp
Network	0	2	2018-02-08 08:12:31
Printers	0	1	2018-01-30 08:35:56
SOFTWARE	0	13	2018-03-23 04:17:33
Adobe	0	5	2018-02-08 09:18:38
AppDataLow	0	1	2018-01-30 02:42:23
Chromium	0	1	2018-02-08 08:58:57
Evernote	1	1	2018-02-08 08:57:43
Google	0	4	2018-02-08 09:09:48
Hibara	0	1	2018-02-08 08:56:30
Microsoft	0	77	2018-04-02 01:28:41
Netscape	0	1	2018-01-30 09:25:22
ODBC			
Policies			
RegisteredApplications			
Sysinternals	0	1	2018-03-23 04:17:33
SDelete	1	0	2018-03-23 04:17:47
Wow6432Node	0	1	2018-01-30 02:42:20
System	0	2	2018-01-30 02:42:20
Associated deleted records	0	0	
Unassociated deleted records	0	0	
G:\Windows\System32\config\SOFTWARE			
G:\Windows\System32\config\SYSTEM			

Values

Value Name	Value Type	Data	Value ...	Is Deleted	Data Record Reallocated
EulaAccepted	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Binary viewer

Value name: EulaAccepted

Value type: RegDword

Raw value: 01-00-00-00

Selected hive: NTUSER.DAT   Last write: 2018-03-23 04:17:47   1 of 1 values shown (100.00%)   Selected bookmark 'Sysinternals' (Sysinternals config info)   Hidden keys: 0   1

# Lab 7: Locating Sysinternals EULA (3/3)

- From the registry keys, the following facts are observed:
  - SDelete was executed on March 23 at 1:17:47 PM (JST).
    - Can we find sdelete from the HDD?
    - The registry keys will remain the same even when attackers modified its filenames.

PF WinPrefetchView

Execution time of l.exe is very close. Is l.exe sdelete?

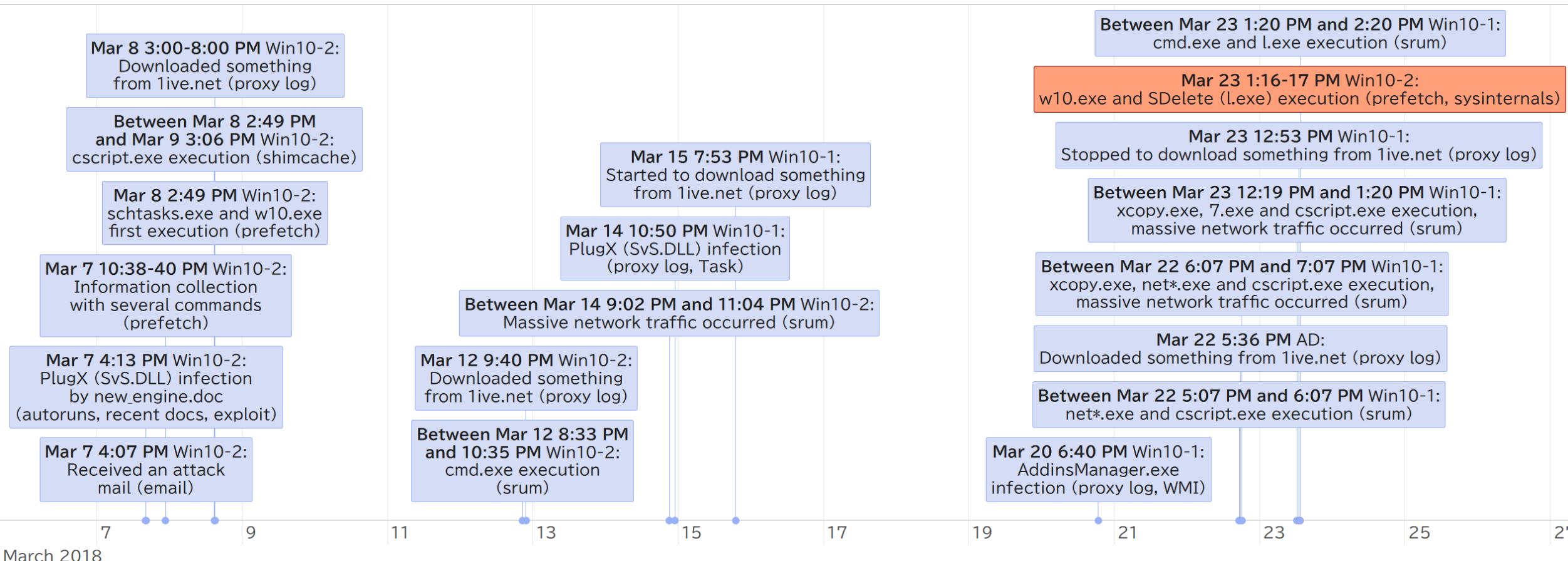
File	Edit	View	Options	Help			
Filename	Created Time	Modified Time	File Size	P..	Process Path	Run Counter	Last Run
SETUP.EXE-58C5970D.pf	2/8/2018 5:56:21 PM	2/8/2018 5:56:21 PM	7,076	S...	G:\PROGRAMDATA\Adobe\Setup\{AC76BA86-...	1	2/8
L.EXE-38698459.pf	3/23/2018 1:17:33 PM	3/23/2018 1:18:13 PM	6,216	L...	G:\PROGRAMDATA\L.EXE	3	3/2
MPENGINE.EXE-F1D867B7.pf	1/29/2018 9:13:19 PM	1/29/2018 9:13:19 PM	1,964	M...	G:\PROGRAMDATA\MICROSOFT\WINDOWS D...	1	1/2
DO.EXE-DB61C8B1.pf	3/14/2018 10:19:24 ...	3/14/2018 10:20:26 P...	7,612	D...	G:\PROGRAMDATA\S\DO.EXE	2	3/1

# Sysinternals EULA and Timestamps

- SDelete is one of the Sysinternals tools that are used in attacks.
  - Overwrites the file with random data for multiple times to avoid files being carved with the forensics procedures.
- If the user has never used the Sysinternals tool and the registry value exists, it is likely that the tool was used during the attack.
  - The EULA is managed for each tool in the Sysinternals. Even if the user has used other Sysinternals tools, if the user has never used SDelete before, then the EulaAccepted value for the SDelete will not exist.
- Registry keys have timestamps. Timestamps of registry keys for the application might be a suggestion for program execution time.

# Scenario 1 Incident Timeline

## After Sysinternals Registry Analysis



# Summary

# Summary (1)

- When programs are executed on Windows, several “records” of execution remains on the computer.
- By examining the “records”, it may be possible to track the programs that were executed during the intrusion.
- The artifacts that remains depend on “how” the programs were executed.

## Summary (2)

- Prefetch, Shimcache and SRUM are powerful for finding attackers' activities and SRUM can be also used to find malware infection.
- UserAssist can be used to know user's activities.
- You can use many other kinds of program execution artifacts finding deleted executable files on the current file system.

# Notes About Timestamps

- When looking the program execution artifacts, knowing about “when” the artifacts get refreshed is important.
- Some artifacts, such as Prefetch and SRUM, is not updated frequently.
  - File system metadata of a prefetch file is created or modified at the earlier one of: the program being closed, or 10 seconds elapse since the program was executed.
  - SRUM is updated once an hour or at the system shutdown.

# The Scenario 1 Incident Timeline So Far

