

Basic Malware Analysis Practical Labs

Software Security

a.a. 2022/2023

Laurea Magistrale in Ing. Informatica

Roberto Natella

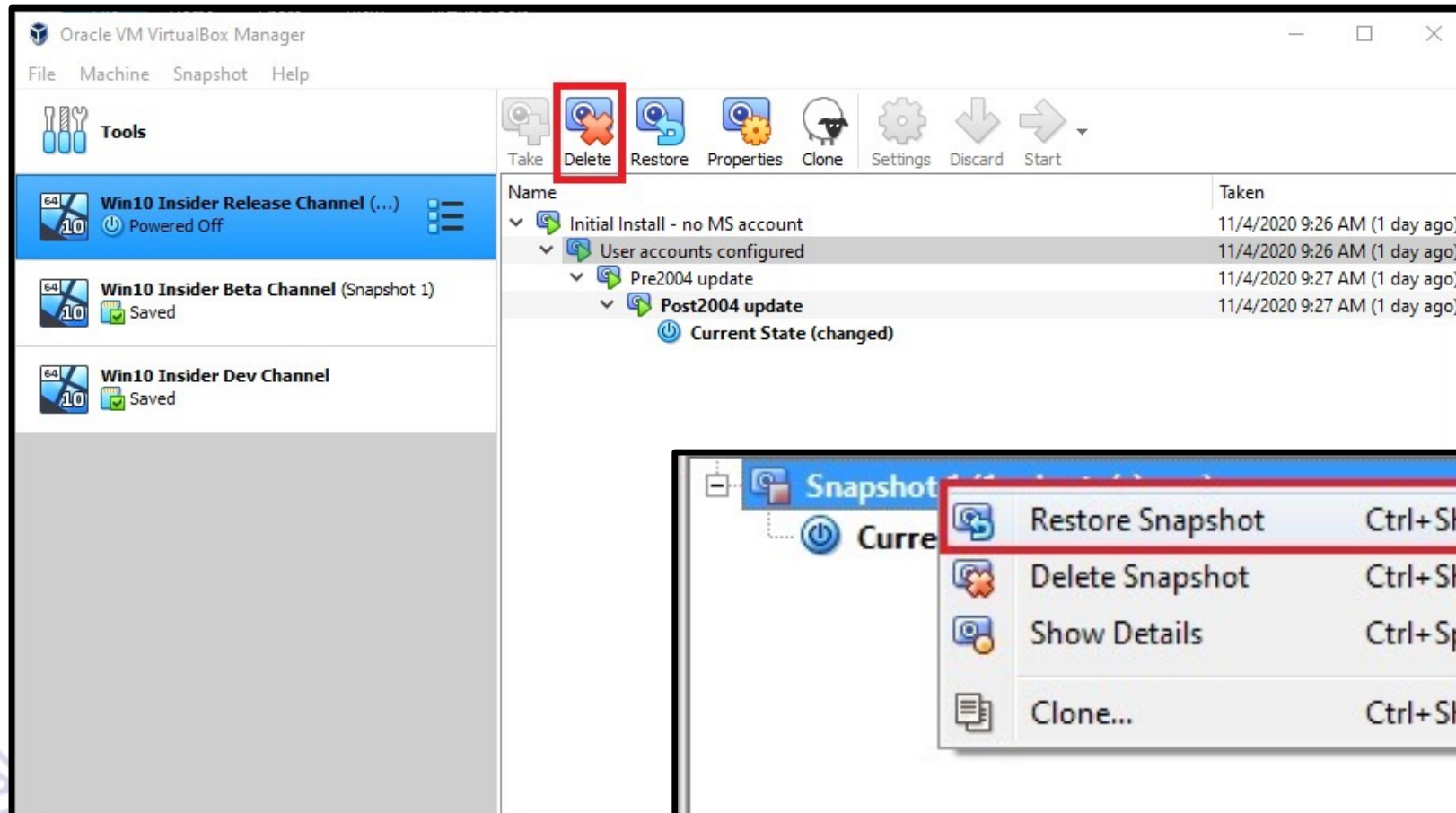


Warning

- Warning: malware executable can damage your computer!
- Before starting, save a snapshot of the virtual machine
- After the lab, save your files outside the VM
- You can then restore the snapshot

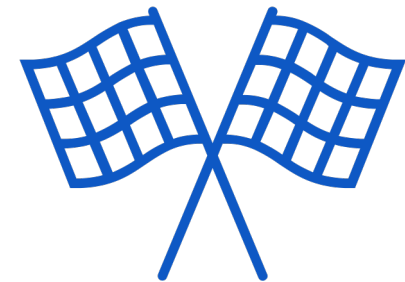


Snapshots



Labs overview

- In order to simulate realistic malware analysis, you will be given **little or no information about the program**
- They contain **meaningless or misleading names** (as typical of malware)
- Follow the steps in the slides
- Find the **secret "flags"** to check your progress!
- Optional flags are marked as "**extra**"



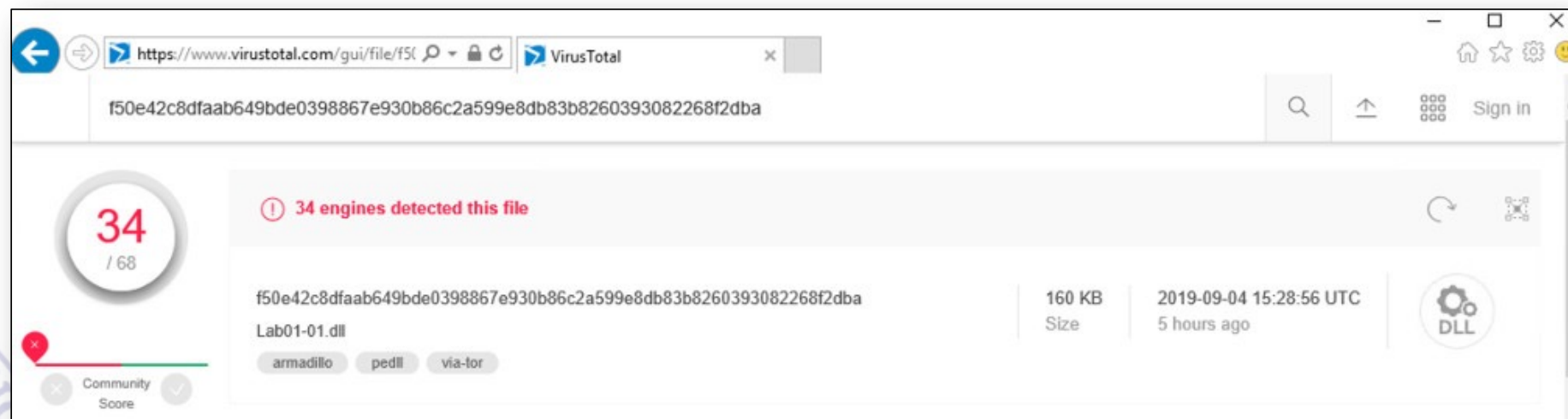
Basic Static Analysis

- This lab uses the files *Lab01-01.exe* and *Lab01-01.dll* (password: "malware")
- Questions:
 1. Upload the files to <http://www.VirusTotal.com> and view the reports. Does either file match any existing antivirus signatures?
 2. When were these files compiled?
 3. Are there any indications that either of these files is packed or obfuscated? If so, what are these indicators?
 4. Do any imports hint at what this malware does? If so, which imports are they?
 5. Are there any other files or host-based indicators that you could look for on infected systems?
 6. What network-based indicators could be used to find this malware on infected machines?
 7. What would you guess is the purpose of these files?



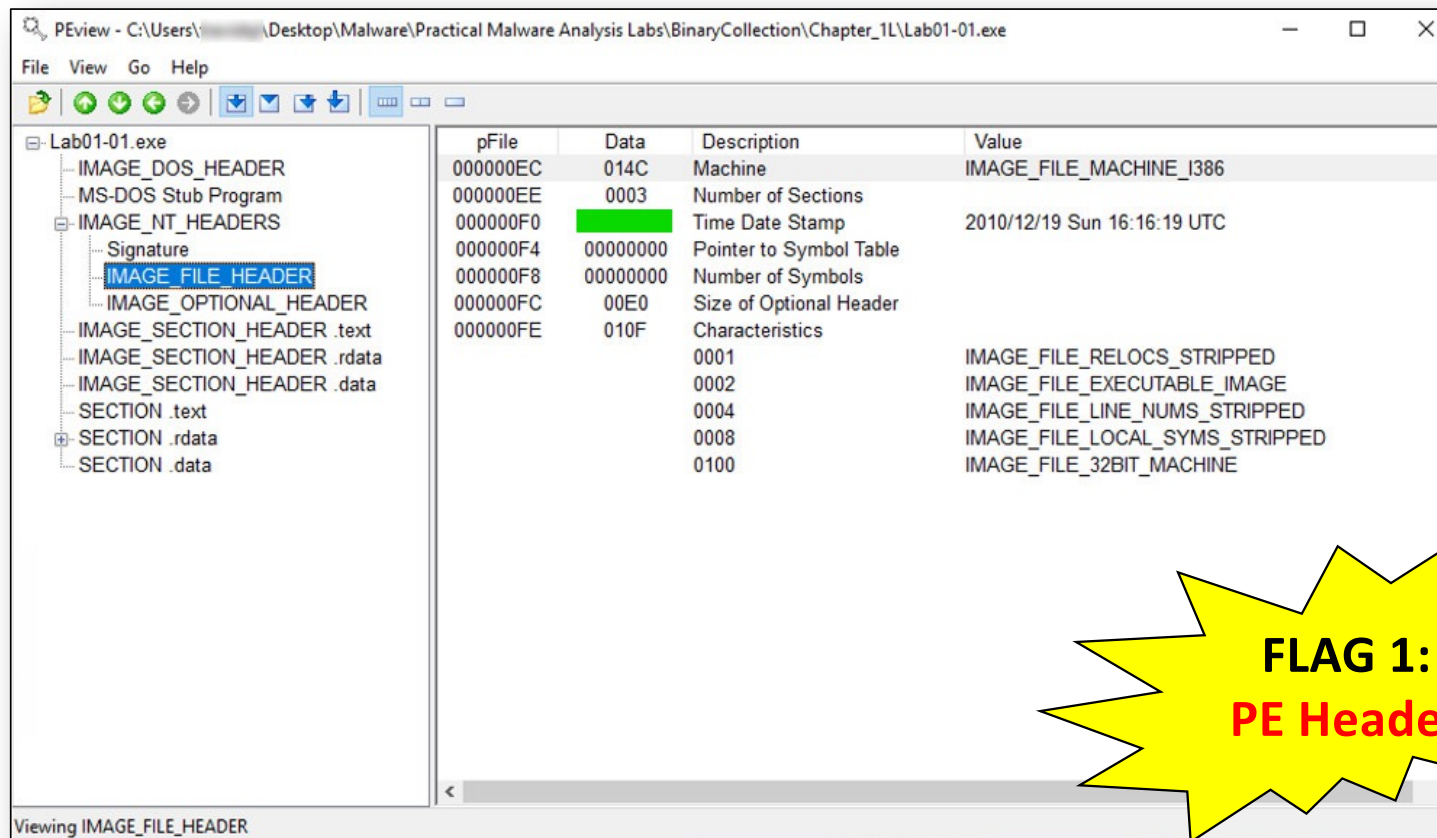
VirusTotal

- VirusTotal compares a file to a **database of antivirus engines**
- You can upload files, but that may **alert attackers** that you have detected an intrusion
- Using it to search for a hash value of a sample is **safer**



PEview

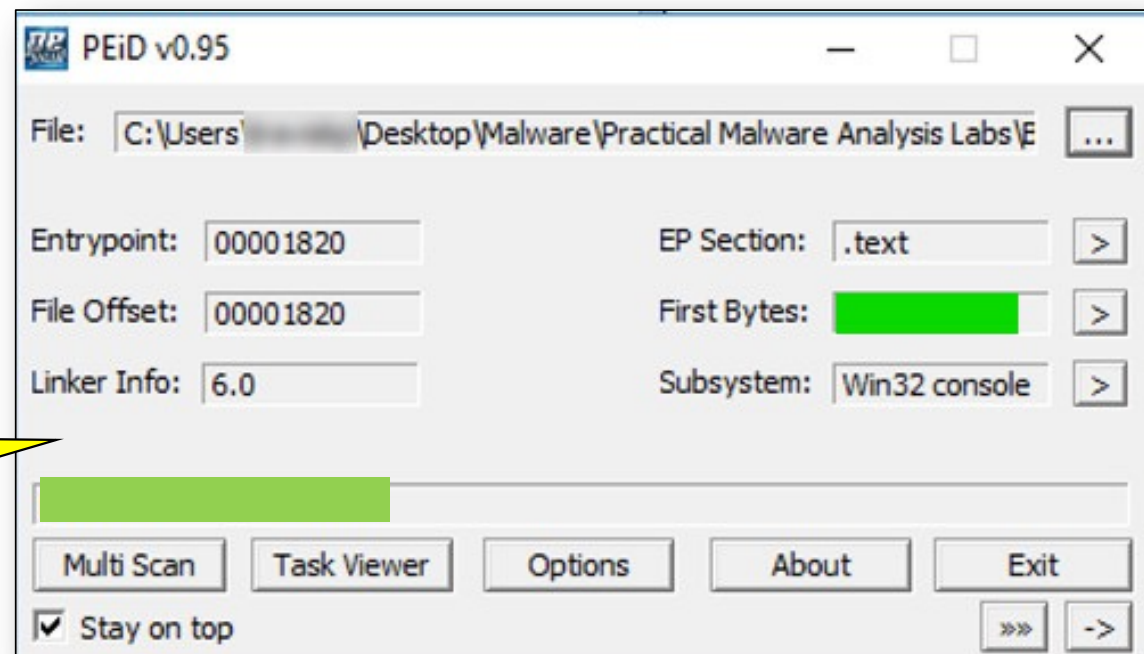
- Find the **Data** that is covered by a green box in the image below.



FLAG 1:
PE Header

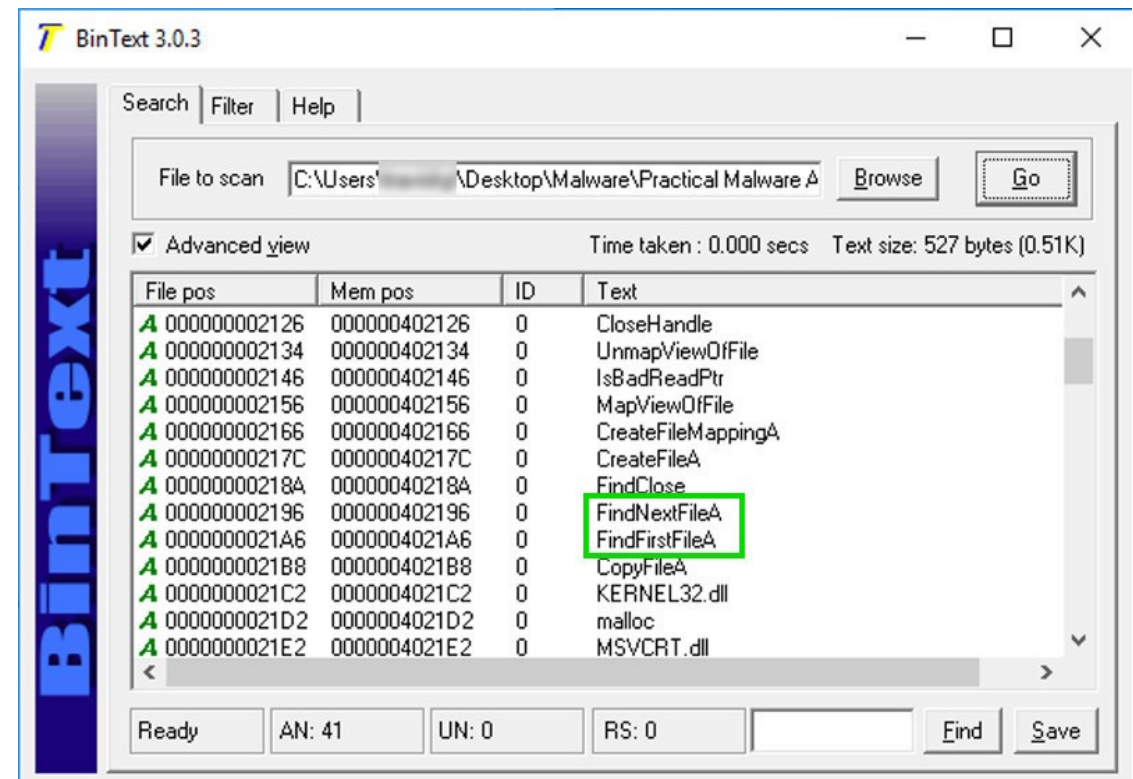
PEiD

- Analyze the EXE with PEiD
- Is it a **packed** executable?
- Note the "**First Bytes**", covered by a green box in the image



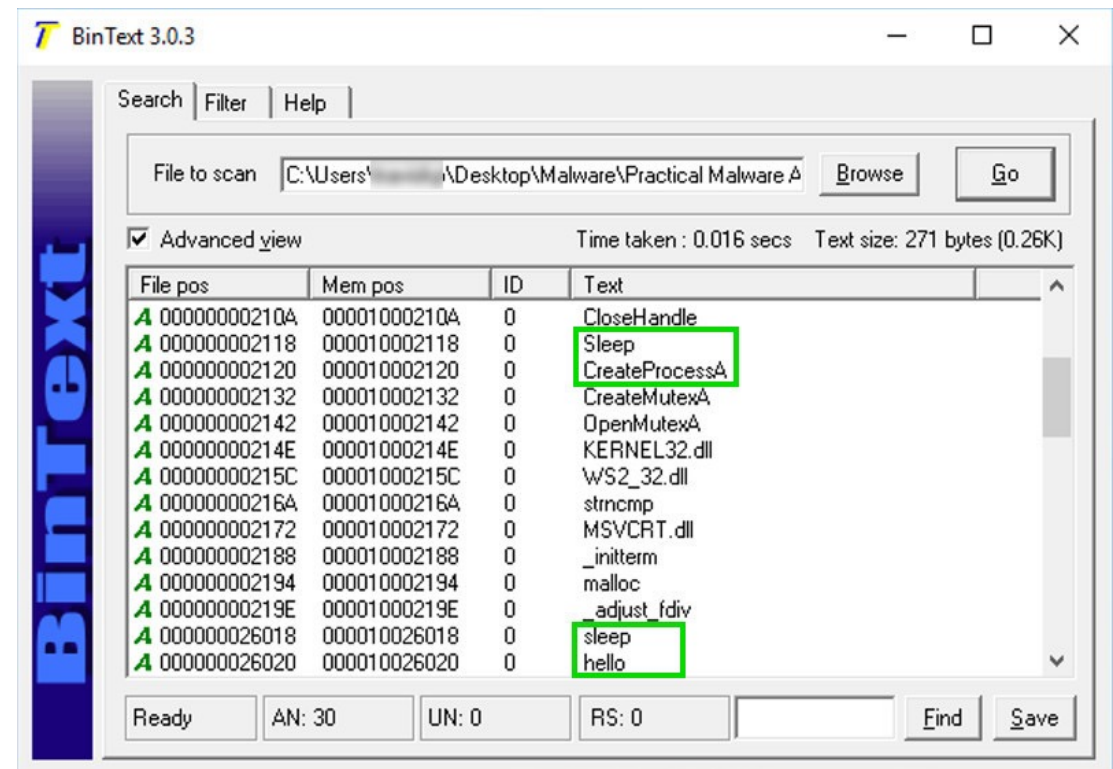
BinText

- Analyze strings in Lab01-01.exe with BinText
- Notice **FindNextFileA**, **FindFirstFileA**, **CopyFileA**. What is their purpose?
- Which other anomalous string can you notice?
- Hint: a "weird" DLL name



BinText

- Analyze Lab01-01.dll with BinText
- Notice the following strings:
 - **Sleep**
 - **CreateProcessA**
 - **sleep**
 - **hello**
- What is their purpose?

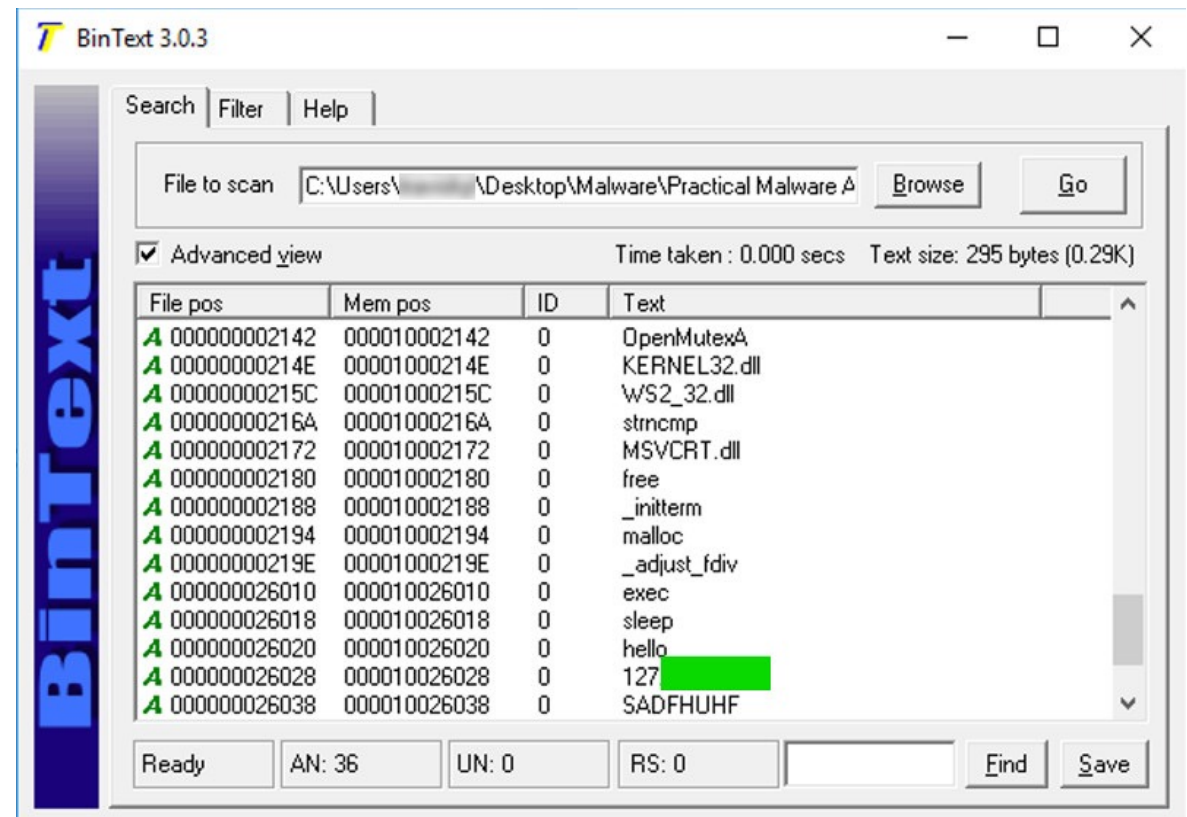


BinText

- In Lab01-01.dll, find the IP address beginning with **127** (covered by a green box in the image)

FLAG 3:

IP Address



Dependency Walker

- Analyze imports in Lab01-01.exe
- Find imports that also appeared among strings (the previous analysis with BinText)

Dependency Walker - [Lab01-01]

File Edit View Options Profile Window Help

LAB01-01.EXE

KERNEL32.DLL

API-MS-WIN-CORE-RTLSUPPORT-L1-2-0

NTDLL.DLL

KERNELBASE.DLL

API-MS-WIN-CORE-PROCESSTHREADS-L

API-MS-WIN-CORE-PROCESSTHREADS-L

API-MS-WIN-CORE-REGISTRY-L1-1-0.DLL

API-MS-WIN-CORE-HEAP-L1-2-0.DLL

API-MS-WIN-CORE-HEAP-L2-1-0.DLL

API-MS-WIN-CORE-MEMORY-L1-1-2.DLL

API-MS-WIN-CORE-ENCLAVE-L1-1-0.DLL

API-MS-WIN-CORE-HANDLE-L1-1-0.DLL

API-MS-WIN-CORE-SYNCH-L1-2-0.DLL

API-MS-WIN-CORE-SYNCH-L1-2-1.DLL

API-MS-WIN-CORE-FILE-L1-2-1.DLL

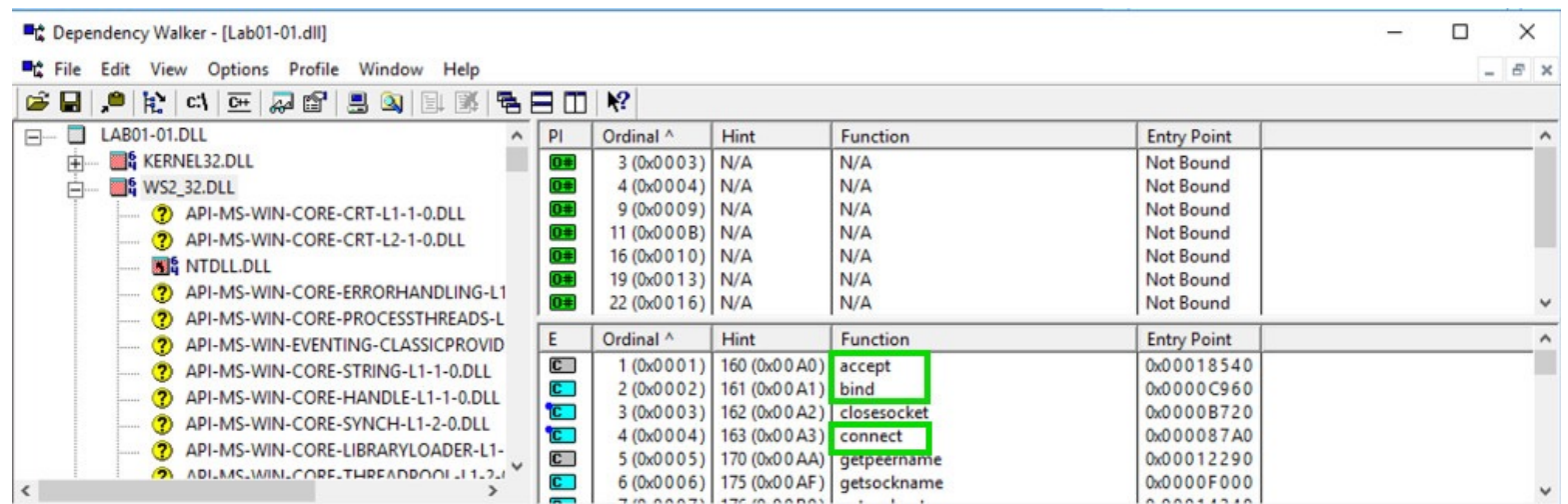
PI	Ordinal ^	Hint	Function	Entry Point
	N/A	27 (0x0018)	CloseHandle	Not Bound
	N/A	40 (0x0028)	CopyFileA	Not Bound
	N/A	52 (0x0034)	CreateFileA	Not Bound
	N/A	53 (0x0035)	CreateFileMappingA	Not Bound
	N/A	144 (0x0090)	FindClose	Not Bound
	N/A	148 (0x0094)	FindFirstFileA	Not Bound
	N/A	157 (0x009D)	FindNextFileA	Not Bound
	N/A	437 (0x1B5)	IsBadReadPtr	Not Bound
	N/A	470 (0x1D6)	MapViewOfFile	Not Bound
	N/A	688 (0x2B0)	UnmapViewOfFile	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
	1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
	2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
	3 (0x0003)	2 (0x0002)	ActivateActCtx	0x0001EFB0
	4 (0x0004)	3 (0x0003)	ActivateActCtxWorker	0x0001A1C0
	5 (0x0005)	4 (0x0004)	AddAtomA	0x000235A0



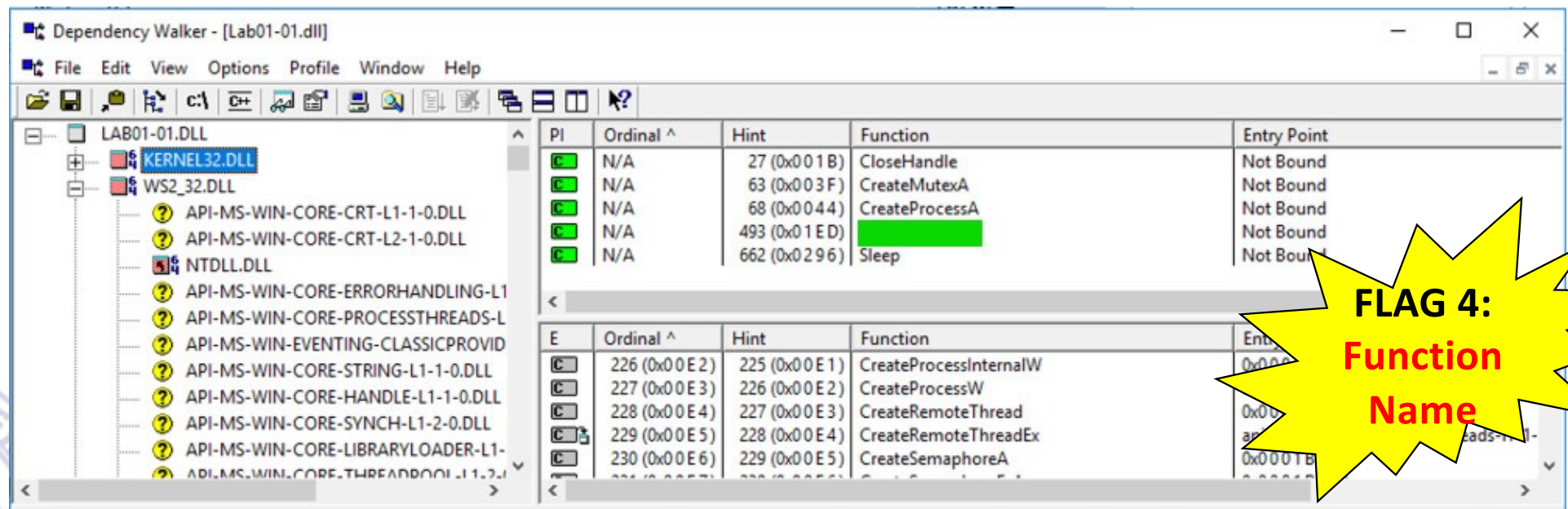
Dependency Walker

- Analyze imports in Lab01-01.dll
- Imported function names do not appear (see [Linking by Ordinal](#))
- What is the purpose of WS2_32.DLL?



Dependency Walker

- Analyze imports in Lab01-01.dll
- Find the function name that is covered by a green box in the image, imported from Kernel32.DLL



Basic Static Analysis

- Analyze the sample **Lab01-04.exe**
- It downloads a file from this domain: **practicalmalwareanalysis.com**. Find that file's name (**Extra Flag 5: Find the downloaded file**)
- It imports a function from **WINTRUST.DLL** with a name ending in "Trust". Find that function's name. (**Extra Flag 6: Find the imported function**)
- Find the date when sample **Lab01-04.exe** was compiled, like this: **2000/01/01**. (**Extra Flag 7: Find the timestamp**)

EXTRA FLAGS:

5, 6, 7



Keylogger

- Get the file **key.exe** (password: "malware")
- Analyze with PEvent, notice suspicious APIs

PEview - C:\Users\...\Desktop\Malware\key.exe

File View Go Help

key.exe

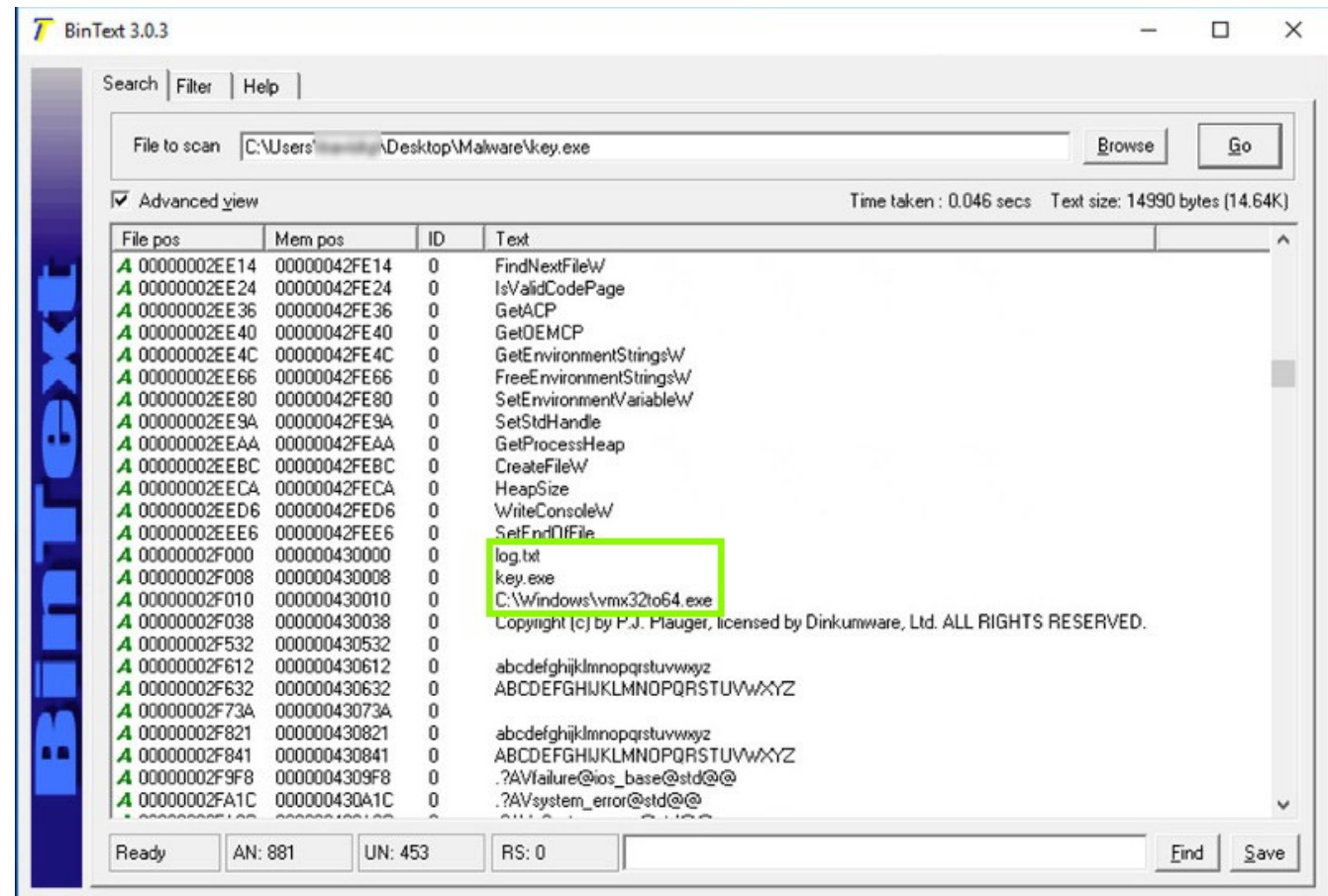
- IMAGE_DOS_HEADER
- MS-DOS Stub Program
- IMAGE_NT_HEADERS
 - IMAGE_SECTION_HEADER .text
 - IMAGE_SECTION_HEADER .rdata
 - IMAGE_SECTION_HEADER .data
 - IMAGE_SECTION_HEADER .reloc
 - SECTION .text
 - SECTION .rdata
 - IMPORT Address Table
 - IMAGE_DEBUG_DIRECTORY
 - IMAGE_LOAD_CONFIG_DIRECTORY
 - IMAGE_DEBUG_TYPE_
 - IMPORT Directory Table
 - IMPORT Name Table
 - IMPORT Hints/Names & DLL Names
 - SECTION .data
 - SECTION .reloc

pFile	Data	Description	Value
00021000	0002F93E	Hint/Name RVA	02A8 RegSetValueExA
00021004	0002F930	Hint/Name RVA	028A RegOpenKeyA
00021008	0002F922	Hint/Name RVA	025B RegCloseKey
0002100C	00000000	End of Imports	ADVAPI32.dll
00021010	0002FEC8	Hint/Name RVA	034E HeapSize
00021014	0002FED4	Hint/Name RVA	0611 WriteConsoleW
00021018	0002FC46	Hint/Name RVA	0462 RaiseException
0002101C	0002F95E	Hint/Name RVA	057D Sleep
00021020	0002F966	Hint/Name RVA	00A8 CopyFileA
00021024	0002F972	Hint/Name RVA	0207 GetConsoleWindow
00021028	0002F986	Hint/Name RVA	0261 GetLastError
0002102C	0002F996	Hint/Name RVA	05FE WideCharToMultiByte
00021030	0002F9AC	Hint/Name RVA	0131 EnterCriticalSection
00021034	0002F9C4	Hint/Name RVA	03BD LeaveCriticalSection
00021038	0002F9DC	Hint/Name RVA	0110 DeleteCriticalSection
0002103C	0002F9F4	Hint/Name RVA	0532 SetLastError
00021040	0002FA04	Hint/Name RVA	035F InitializeCriticalSectionAndSpinCount
00021044	0002FA2C	Hint/Name RVA	0587 SwitchToThread
00021048	0002FA3E	Hint/Name RVA	059E TlsAlloc



Keylogger

- Examine strings in key.exe
- What can you notice?



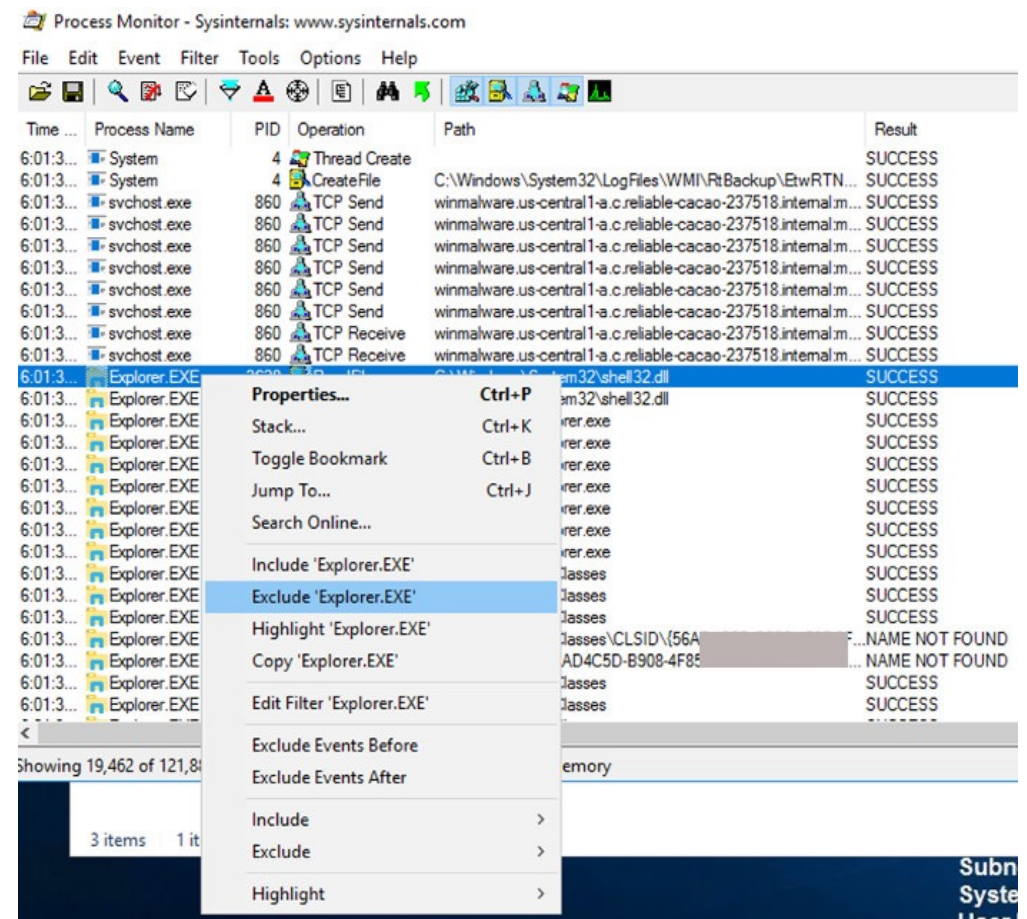
Basic Dynamic Analysis

- Tools for dynamic analysis:
 - Process Monitor
 - Process Explorer



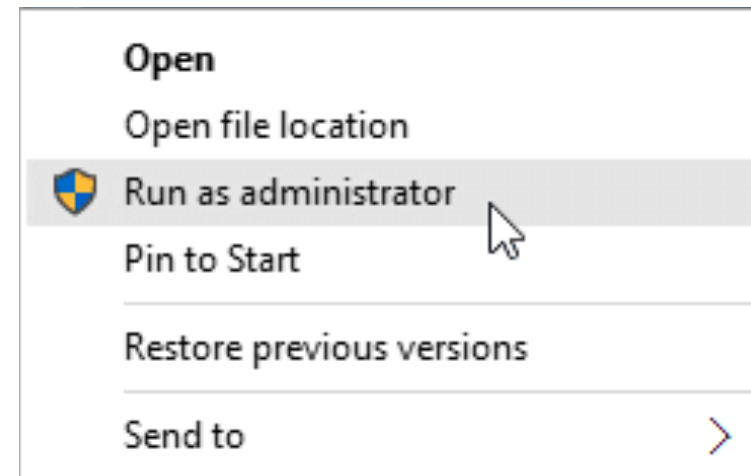
Process Monitor

- **Note:** Process Monitor records events in RAM. **Don't leave it running for too long!**
- In Process Monitor, you can add **filters to exclude system processes** (explorer.exe, lsass.exe)



Run keylogger as administrator

- Run keylogger **as administrator!**
- It is needed to activate **persistence** mechanisms



Viewing the running malware in Process Explorer

- In Process Explorer, in the top pane, find **key.exe** and click it
- Find the name of the exe covered in green in the image below

Process Explorer - Sysinternals: www.sysinternals.com [WINMALWARE]

File Options View Process Find Handle Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
lsass.exe		5,952 K	15,772 K	592	Local Security Authority Proc...	Microsoft Corporation
csrss.exe	< 0.01	1,748 K	4,280 K	460		
winlogon.exe		1,652 K	8,372 K	504		
LogonUI.exe	0.24	13,928 K	52,264 K	848		
dwm.exe		5,492 K	18,472 K	856		
csrss.exe	0.02	2,212 K	8,524 K	2948		
winlogon.exe		2,000 K	7,784 K	1980		
dwm.exe	0.21	19,112 K	59,148 K	2900		
explorer.exe	0.03	31,576 K	95,452 K	3736	Windows Explorer	Microsoft Corporation
procexp64.exe	0.36	17,296 K	38,764 K	4288	Sysinternals Process Explorer	Sysinternals - www.sysinter...
MSASCui.exe		4,604 K	19,392 K	4492	Windows Defender User Inte...	Microsoft Corporation
MSASCuiL.exe		3,016 K	13,264 K	4144	Windows Defender notificati...	Microsoft Corporation
Procmon.exe		2,712 K	15,828 K	2612	Process Monitor	Sysinternals - www.sysinter...
Procmon64.exe	0.15	9,596 K	27,292 K	3236		
key.exe	0.14	1,080 K	4,764 K	4112		
key.exe		5,400 K	12,112 K	5064		

FLAG 8:
Process
Explorer



Viewing the running malware in Process Monitor

- Go to **ProcMon** and scroll until you get to key.exe
- You can view the steps the malware is taking
- You will find that it creates an EXE file in the **C:\Windows** directory

Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path
4:42:2...	consent.exe	5064	CloseFile	C:\Windows\Fonts\segoeui.ttf
4:42:2...	key.exe	1876	Process Start	
4:42:2...	key.exe	1876	Thread Create	
4:42:2...	key.exe	1876	Load Image	C:\Users\...\Desktop\Malware\key.exe
4:42:2...	key.exe	1876	Load Image	C:\Windows\System32\ntdll.dll
4:42:2...	key.exe	1876	Load Image	C:\Windows\SysWOW64\ntdll.dll
4:42:2...	key.exe	1876	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap
4:42:2...	key.exe	1876	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap
4:42:2...	key.exe	1876	CreateFile	C:\Windows
4:42:2...	key.exe	1876	Load Image	C:\Windows\System32\wow64.dll
4:42:2...	key.exe	1876	Load Image	C:\Windows\System32\wow64win.dll
4:42:2...	key.exe	1876	CreateFile	C:\Windows\System32\wow64log.dll
4:42:2...	key.exe	1876	Load Image	C:\Windows\System32\kernel32.dll
4:42:2...	key.exe	1876	Load Image	C:\Windows\SysWOW64\kernel32.dll
4:42:2...	key.exe	1876	Load Image	C:\Windows\System32\kernel32.dll
4:42:2...	key.exe	1876	Load Image	C:\Windows\System32\user32.dll
4:42:2...	key.exe	1876	CreateFile	C:\Windows
4:42:2...	key.exe	1876	QueryNameInformationFile	C:\Windows
4:42:2...	key.exe	1876	CloseFile	C:\Windows
4:42:2...	key.exe	1876	RegOpenKey	HKLM\Software\Microsoft\Wow64\x86
4:42:2...	key.exe	1876	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\x86\key.exe



Viewing the running malware in Process Monitor

- The malware also creates persistence by modifying the run registry key for the current user (HKCU = HKEY_CURRENT_USER)
- Find the path of that key and take note of it
- The flag is the text covered in green

FLAG 9:
Process
Monitor

4:42:2... key.exe
4:42:2... key.exe
4:42:2... key.exe
4:42:3... key.exe
4:42:3... key.exe
4:42:3... key.exe
4:42:3... key.exe
4:42:3... key.exe
4:42:3... key.exe
4:42:3... key.exe
4:42:3... key.exe
4:42:3... key.exe
4:42:5... key.exe
4:42:5... key.exe
4:42:5... key.exe
4:42:5... key.exe
4:43:0... key.exe
4:43:0... key.exe

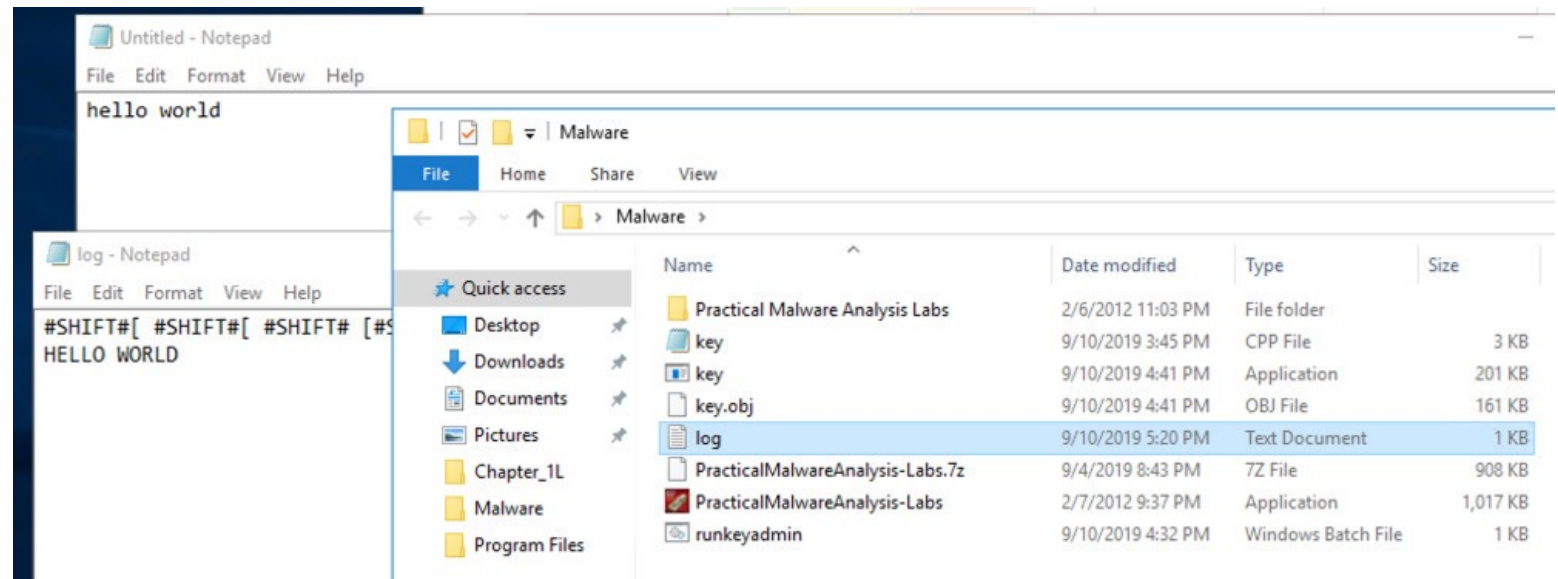
1876 QueryRemoteProtocolInformation
1876 CloseFile
1876 CloseFile
1876 RegOpenKey
1876 RegQueryKey
1876 RegQueryKey
1876 RegOpenKey
1876 RegSetInfoKey
1876 RegQueryKey
1876 **RegQueryKey**
1876 RegCloseKey
1876 Thread Exit
1876 Thread Exit
1876 Thread Exit
1876 CreateFile

C:\Windows\vmx32to64.exe
C:\Windows\vmx32to64.exe
C:\Users\traviskp\Desktop\Malware\key.exe
HKCU
HKCU
HKCU
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\vmx32to64
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
C:\Users\traviskp\Desktop\Malware\log.txt
C:\Users\traviskp\Desktop\Malware\log.txt



Run the keylogger

- Open notepad and type some text
- Go to the folder where key.exe is, find **log.txt** and open it
- You see the captured keystrokes



Persistence

- In Process Explorer, right click **key.exe** and choose **Kill Process**
- **Restart the machine.** Check that the malware is still running
- Inspect **handles** in Process Explorer, find the flag

Process Explorer - Sysinternals: www.sysinternals.com [WINMALWARE\traviskp]

File Options View Process Find Handle Users Help

Process

Process	CPU	Private Bytes	Working Set	Session ID	Company Name
svchost.exe	< 0.01	1,760 K			
msdtc.exe	< 0.01	2,900 K			
Nis.Srv.exe	< 0.01	3,692 K			
svchost.exe	< 0.01	4,120 K			
sppsvc.exe	< 0.01	5,684 K			
lsass.exe	0.13	1,944 K			
csrss.exe	< 0.01	1,636 K			
winlogon.exe	0.24	14,452 K			
LogonUI.exe	0.07	5,728 K	18,860		
dwm.exe	0.07	2,072 K	5,168		
csrss.exe	0.07	2,080 K	7,868	472	
winlogon.exe	0.07	13,532 K	44,680	392	
dwm.exe	0.66	21,220 K	67,516 K	3524	Windows Explorer
explorer.exe	0.14	864 K	3,892 K	4288	Microsoft Corporation
vmx32to64.exe		5,256 K	11,068 K	4296	Console Window Host
conhost.exe	16.63	16,488 K	35,532 K	4800	Sysinternals Process Explorer
procexp64.exe					Sysinternals - www.sysinter...

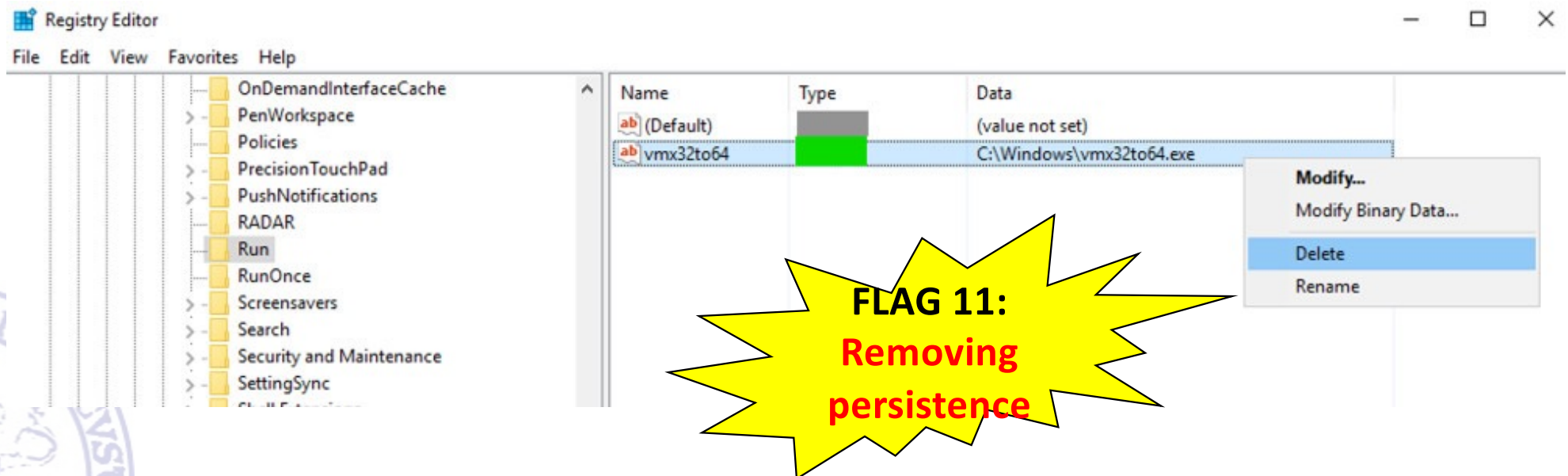
FLAG 10: Persistence

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\KnownDlls32
Directory	\KnownDlls32
File	C:\Windows
File	C:\Windows\SysWOW64
File	\Device\ConDrv
File	\Device\ConDrv
File	\Device\ConDrv
File	\Device\ConDrv
File	\Device\ConDrv
File	\Device\ConDrv
File	\Device\CNG
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Key	HKLM\SYSTEM\Control\Nls\Sorting\Versions
Key	HKCU
WindowStation	\Sessions\2\Windows\WindowStations\WinSta0
WindowStation	\Sessions\2\Windows\WindowStations\WinSta0



Removing persistence

- Run regedit
- Navigate to
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Remove the Run entry, take note of the type (flag)



Run Key

- Download **key12.exe** (from key12.7z, pass "malware")
- Analyze with ProcMon, find the name of the Run entry

**EXTRA
FLAG 12:
Run Key**

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path
7:22:25...	key12.exe	4116	RegQueryKey	HKCU
7:22:25...	key12.exe	4116	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run
7:22:25...	key12.exe	4116	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
7:22:25...	key12.exe	4116	RegQueryKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
7:22:25...	key12.exe	4116	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
7:22:25...	key12.exe	4116	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
7:22:25...	key12.exe	4116	RegQueryKey	HKLM
7:22:25...	key12.exe	4116	RegQueryKey	HKLM
7:22:25...	key12.exe	4116	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters
7:22:25...	key12.exe	4116	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters
7:22:25...	key12.exe	4116	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters
7:22:25...	key12.exe	4116	RegQueryKey	HKLM
7:22:25...	key12.exe	4116	RegQueryKey	HKLM
7:22:25...	key12.exe	4116	RegOpenKey	HKLM\System\CurrentControlSet\Services\DnsCache\Parameters
7:22:25...	key12.exe	4116	RegOpenKey	HKLM\System\CurrentControlSet\Services\DnsCache\Parameters
7:22:25...	key12.exe	4116	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\DnsCache\Parameters
7:22:25...	key12.exe	4116	RegQueryKey	HKLM
7:22:25...	key12.exe	4116	RegQueryKey	HKLM
7:22:25...	key12.exe	4116	RegOpenKey	HKLM\Software\WOW6432Node\Policies\Microsoft\Windows NT\DnsClient

Event Properties

Event	Process	Stack
Date:	9/18/2019 7:22:25.9701750 AM	
Thread:	1112	
Class:	Registry	
Operation:	RegSetValue	
Result:	SUCCESS	
Path:	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\	
Duration:	0.0000211	
Type:	REG_SZ	
Length:	70	
Data:	C:\Windows\niceness.exe	

DNS Traffic

- Examine DNS traffic by **key12.exe**
- Use **Wireshark** and/or fake DNS (**Fakenet-NG**)
- Find the key in the DNS traffic

Protocol	Length	Info
DNS	80	Standard query 0xe33a A [REDACTED].samsclass.info
DNS	128	Standard query response 0xe33a A [REDACTED].samsclass.info CNAME

EXTRA FLAG 13:
DNS traffic



HTTP Traffic

- Examine HTTP traffic by **key12.exe**
- Find the key in the HTTP traffic

Protocol	Length	Info
TCP	66	50463 → 80 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
TCP	60	80 → 50463 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
TCP	54	50463 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
HTTP	143	GET /?flag=[REDACTED] HTTP/1.1
TCP	60	80 → 50463 [ACK] Seq=1 Ack=90 Win=64240 Len=0

EXTRA FLAG 14:
HTTP traffic



- Get the **capa** tool (<https://github.com/fireeye/capa/releases>)
- Use it on **Lab01-01.exe**

```
[Sam-2:Downloads sambowne$ ./capa ./.Practical\ Malware\ Analysis\ Labs\ BinaryCollection\ Chapter_1L\ Lab01-01.exe]
loading : 100%|██████████████████████████████████████████████████████████████████████████████| 341/341 [00:01<00:00, 189.00 rules/s]
matching: 100%|██████████████████████████████████████████████████████████████████████████████| 13/13 [00:00<00:00, 37.13 functions/s]

+-----+-----+
| md5    | bb7425b82141a1c0f7d60e5106676bb1 |
| sha1   | 9dce39ac1bd36d877fdb0025ee88fdaff0627cdb |
| sha256 | 58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47 |
| path   | Practical Malware Analysis Labs/BinaryCollection/Chapter_1L/Lab01-01.exe |
+-----+-----+

+-----+-----+
| ATT&CK Tactic | ATT&CK Technique |
+-----+-----+
| DISCOVERY     | File and Directory Discovery [T1083] |
+-----+-----+

+-----+-----+
| CAPABILITY                                | NAMESPACE |
+-----+-----+
| copy file                                 | host-interaction/file-system/copy |
| enumerate files via kernel32 functions   | host-interaction/file-system/files/list |
| read file via mapping (2 matches)        | host-interaction/file-system/read |
+-----+-----+
```

Capa

- Analyze **Lab01-01.dll** with capa
- This file has networking capabilities
- Find the word covered by a green box

FLAG 15:
capa (dll)

```

Command Prompt

MBC Objective      | MBC Behavior
+-----+-----+
COMMAND AND CONTROL | C2 Communication::Receive Data [B0030.002]
COMMUNICATION       | C2 Communication::Send Data [B0030.001]
                   | Socket Communication::Connect Socket [C0001.004]
                   | Socket Communication::Create TCP Socket [C0001.011]
                   | Socket Communication::Initialize Winsock Library [C0001.009]
                   | Socket Communication::Receive Data [C0001.006]
                   | Socket Communication::Send Data [C0001.007]
                   | Socket Communication::TCP Client [C0001.008]
PROCESS            | Check Mutex [C0043]
                   | Create Mutex [C0042]
                   | Create Process [C0017]
+-----+-----+

CAPABILITY         | NAMESPACE
+-----+-----+
receive data       | communication
send data          | communication
initialize winsock library | communication/socket
act as TCP client  | communication/tcp/client
check [REDACTED]    | host-interaction/mutex
create mutex       | host-interaction/mutex
create process     | host-interaction/process/create
+-----+-----+

C:\Users\IEUser\Downloads\capa-v1.6.0-windows>

```



Capa

- Analyze **Lab01-04.exe** with capa
- This file uses three ATT&CK tactics
- Find the word covered by a green box

FLAG 16:
capa (exe)

```

Command Prompt
C:\Users\IEUser\Downloads\capa-v1.6.0-windows>capa "C:\PMA\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\Lab01-04.exe"
loading : 100%| 469/469 [00:00<00:00, 589.05 rules/s
]
matching: 100%| 13/13 [00:00<00:00, 16.18 functions/s
]
+-----+-----+
| md5    | 625ac05fd47adc3c63700c3b30de79ab |
| sha1   | 9369d80106dd245938996e245340a3c6f17587fe |
| sha256 | 0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126 |
| path   | C:\PMA\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\Lab01-04.exe |
+-----+-----+
+-----+-----+
| ATT&CK Tactic | ATT&CK Technique |
+-----+-----+
| DISCOVERY    | File and Directory Discovery [T1083] |
| EXECUTION    | Shared Modules [T1129] |
| [REDACTED]   | Access Token Manipulation [T1134] |
+-----+-----+

```