UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

Basic Malware Analysis Practical Labs

Software Security

a.a. 2022/2023

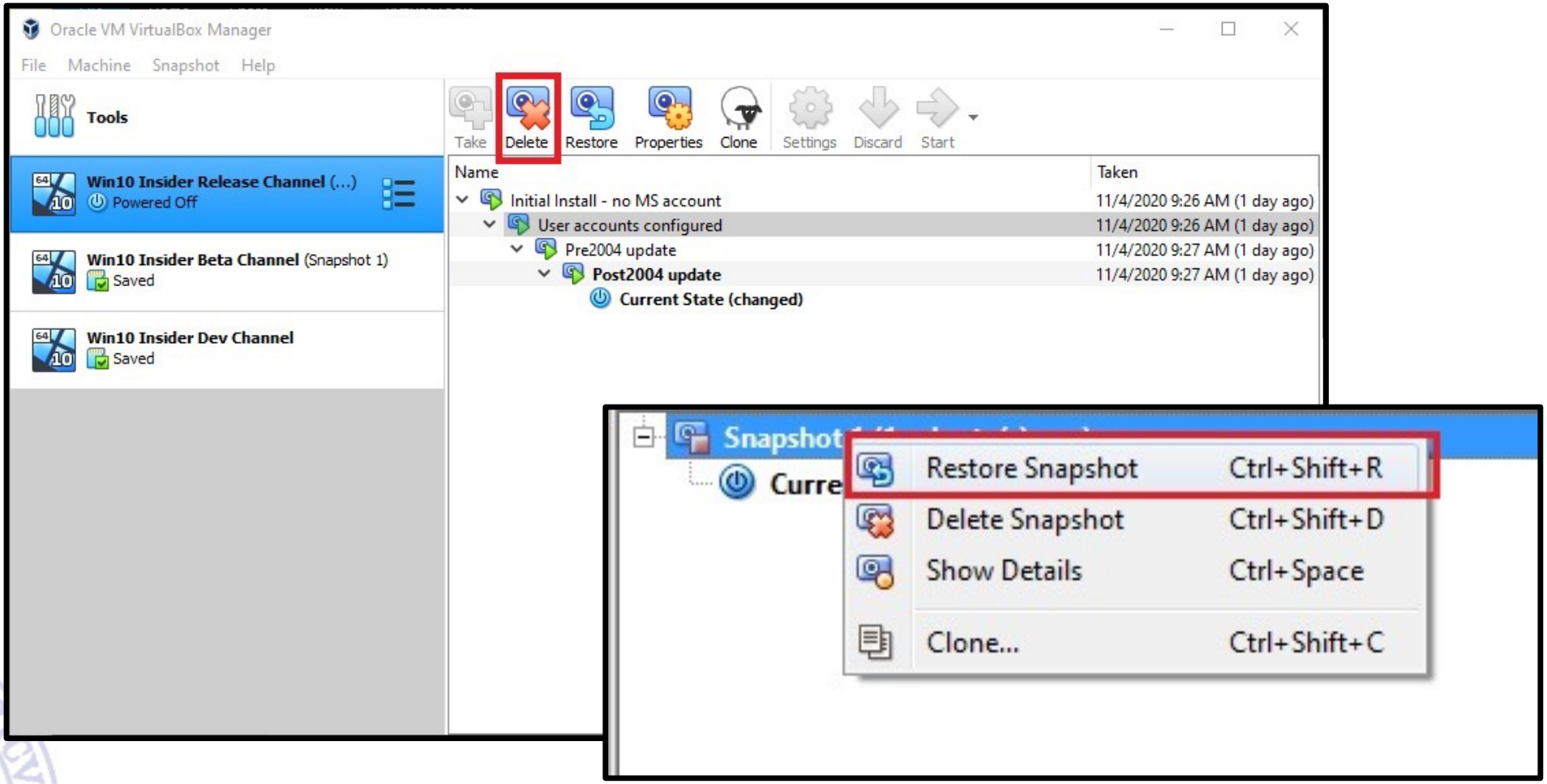
Laurea Magistrale in Ing. Informatica

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

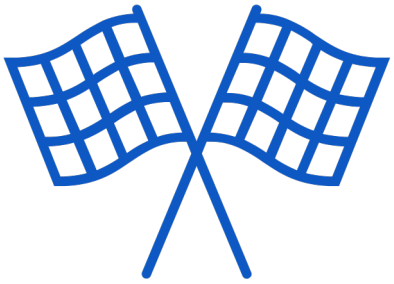
Snapshots


Oracle VM VirtualBox Manager
File Machine Snapshot Help
Tools
Win10 Insider Release Channel (...)
Powered Off
Win10 Insider Beta Channel (Snapshot 1)
Saved
Win10 Insider Dev Channel
Saved
Take Delete Restore Properties Clone Settings Discard Start
Name
Taken
Initial Install - no MS account
11/4/2020 9:26 AM (1 day ago)
User accounts configured
11/4/2020 9:26 AM (1 day ago)
Pre2004 update
11/4/2020 9:27 AM (1 day ago)
Post2004 update
11/4/2020 9:27 AM (1 day ago)
Current State (changed)
Restore Snapshot Ctrl+Shift+R
Delete Snapshot Ctrl+Shift+D
Show Details Ctrl+Space
Clone... Ctrl+Shift+C

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**"



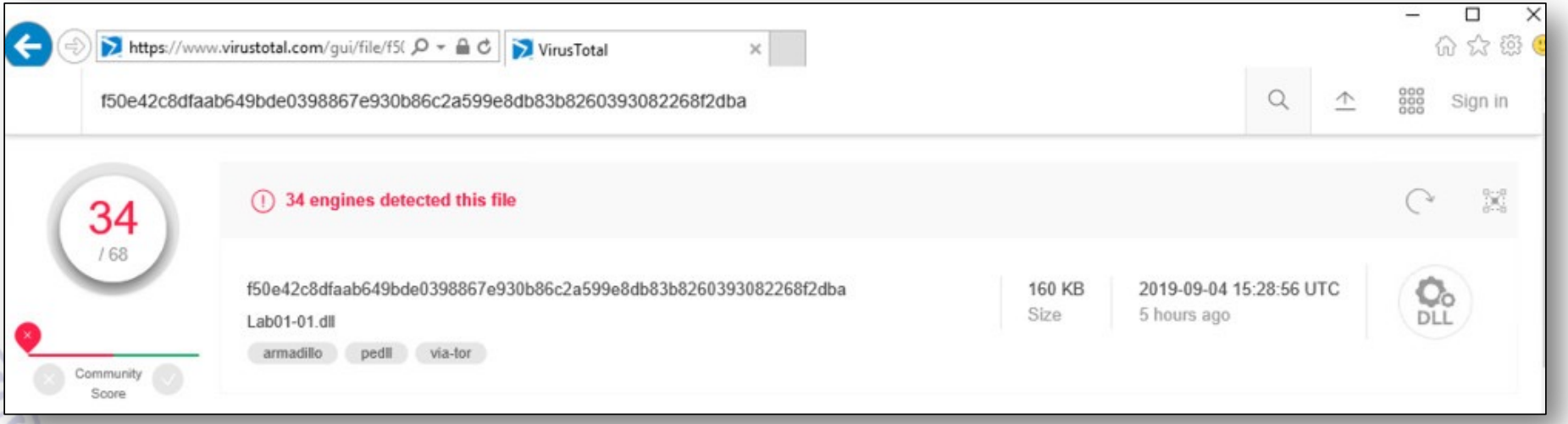
Basic Static Analysis

- 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?

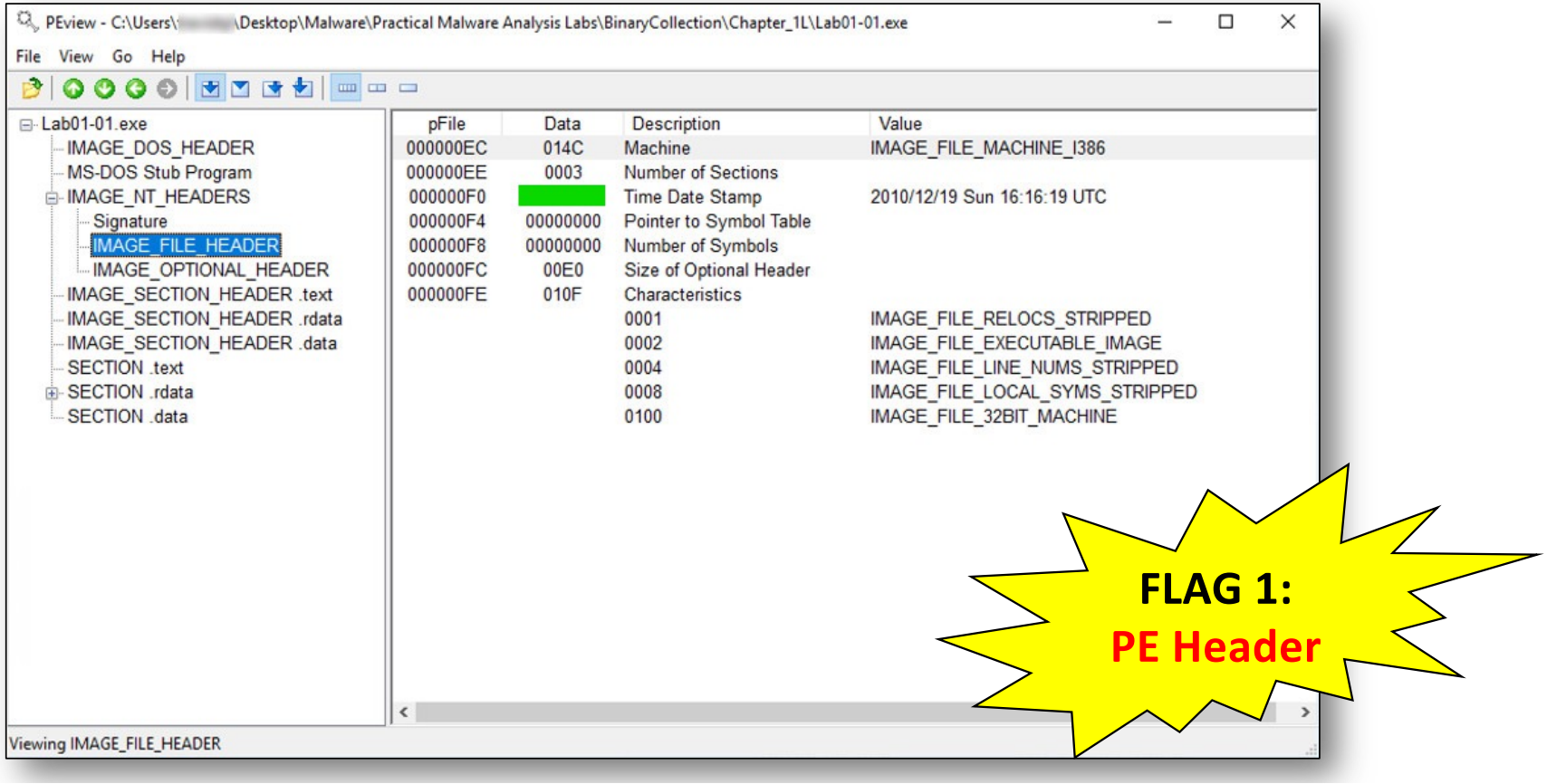
VirusTotal

- 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**



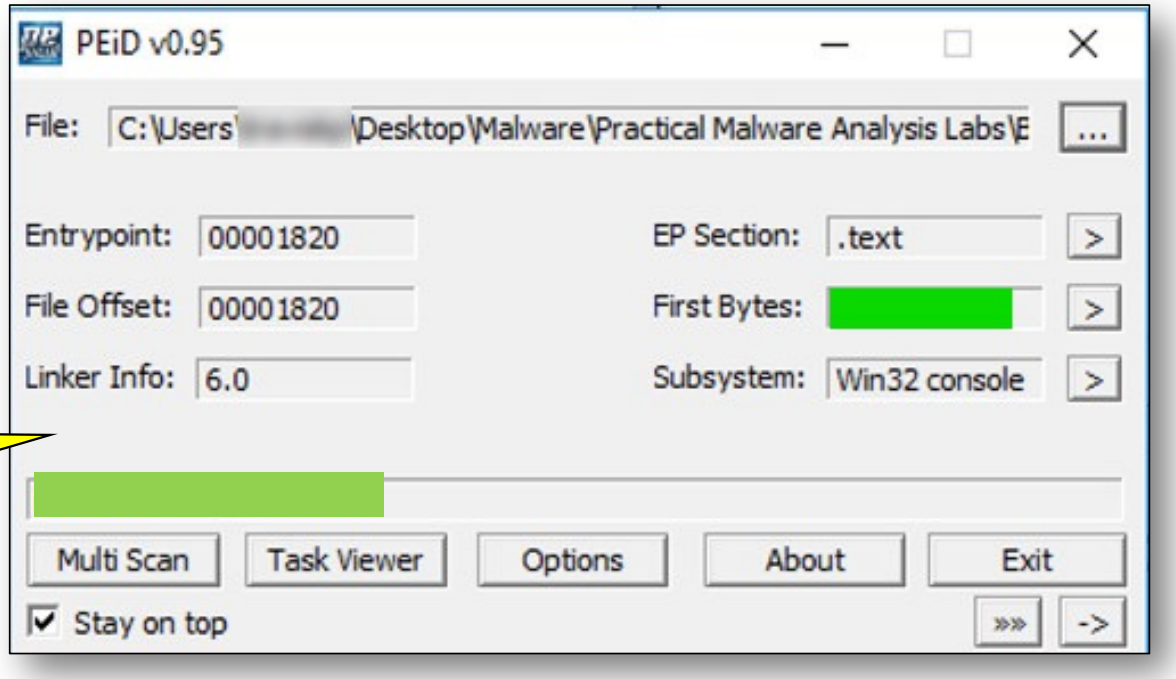
PEview

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



PEiD

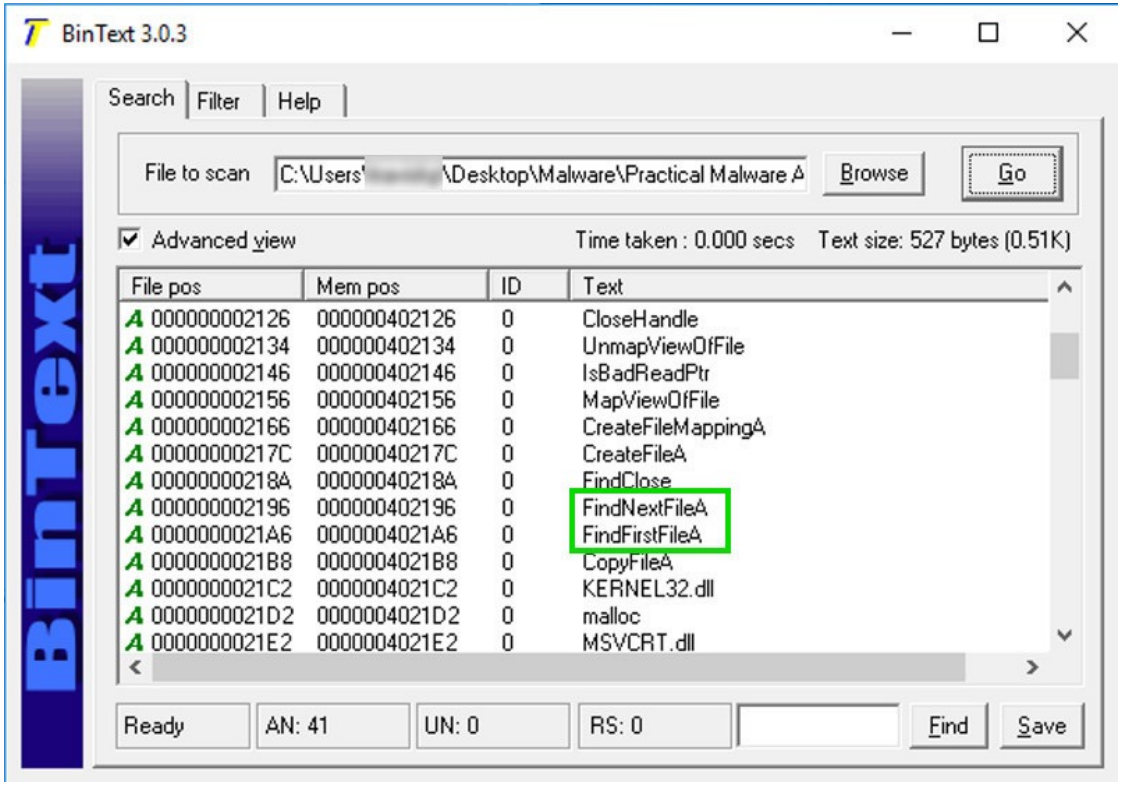
- Analyze the EXE with PEiD
- Is it a **packed** executable?
- Note the "**First Bytes**", covered by a green box in the image



FLAG 2:
First Bytes

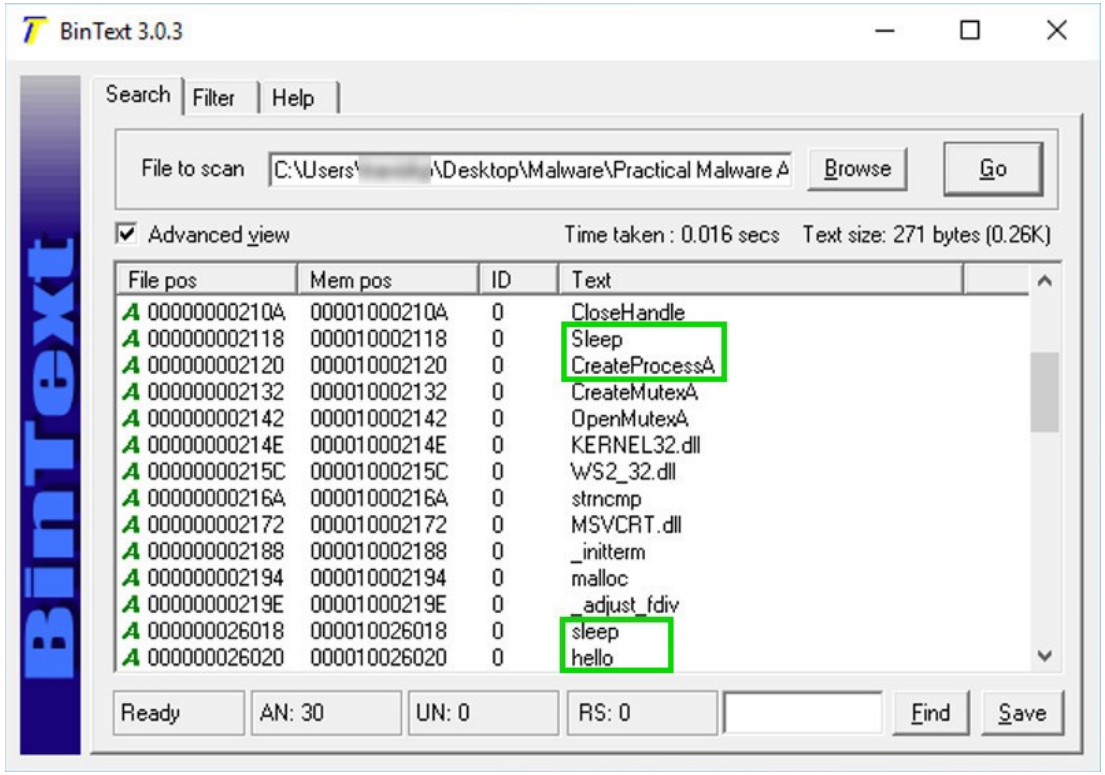
BinText

- 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



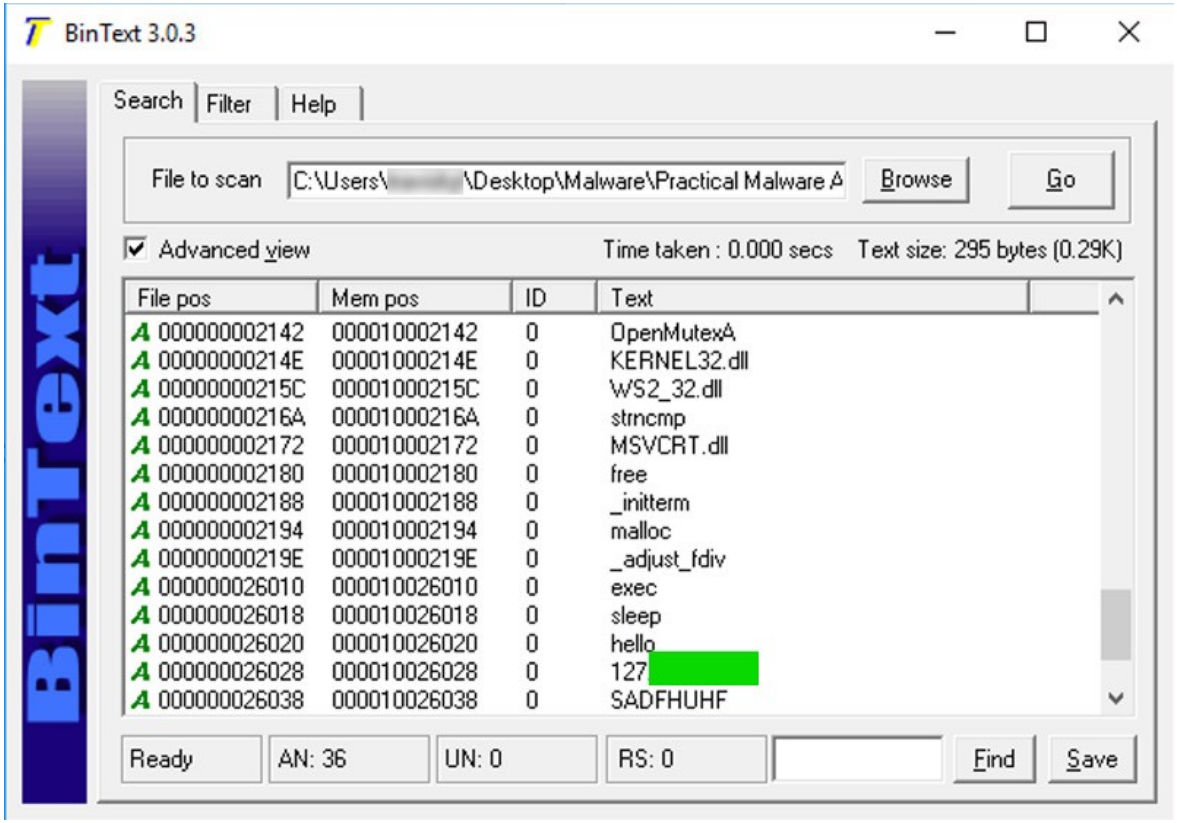
BinText

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



BinText

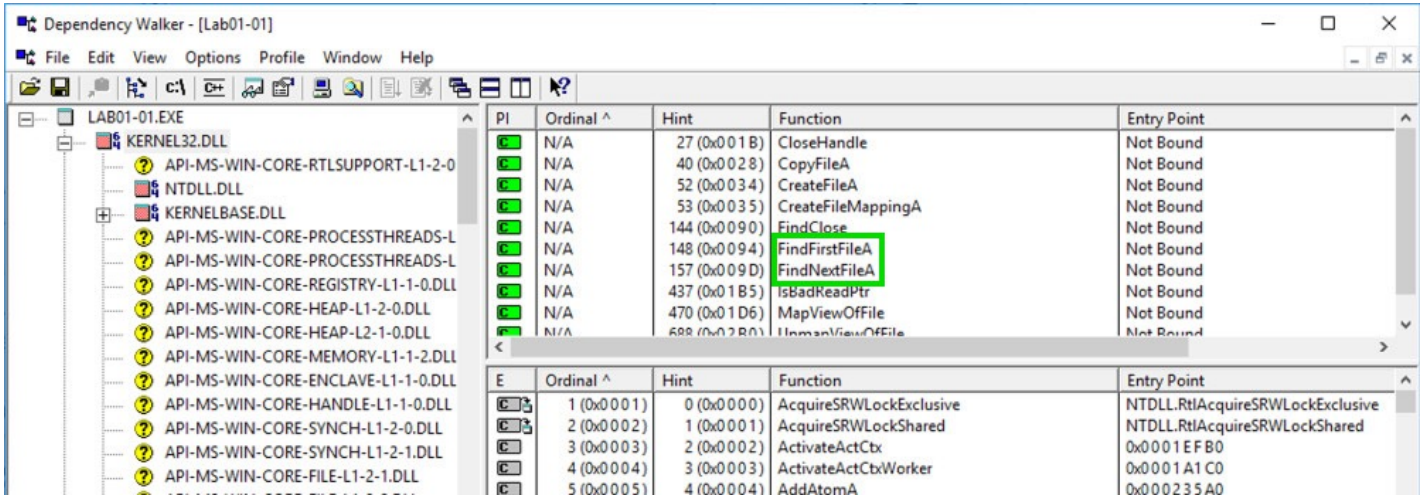
- In Lab01-01.dll, find the IP address beginning with **127** (covered by a green box in the image)



FLAG 3:
IP Address

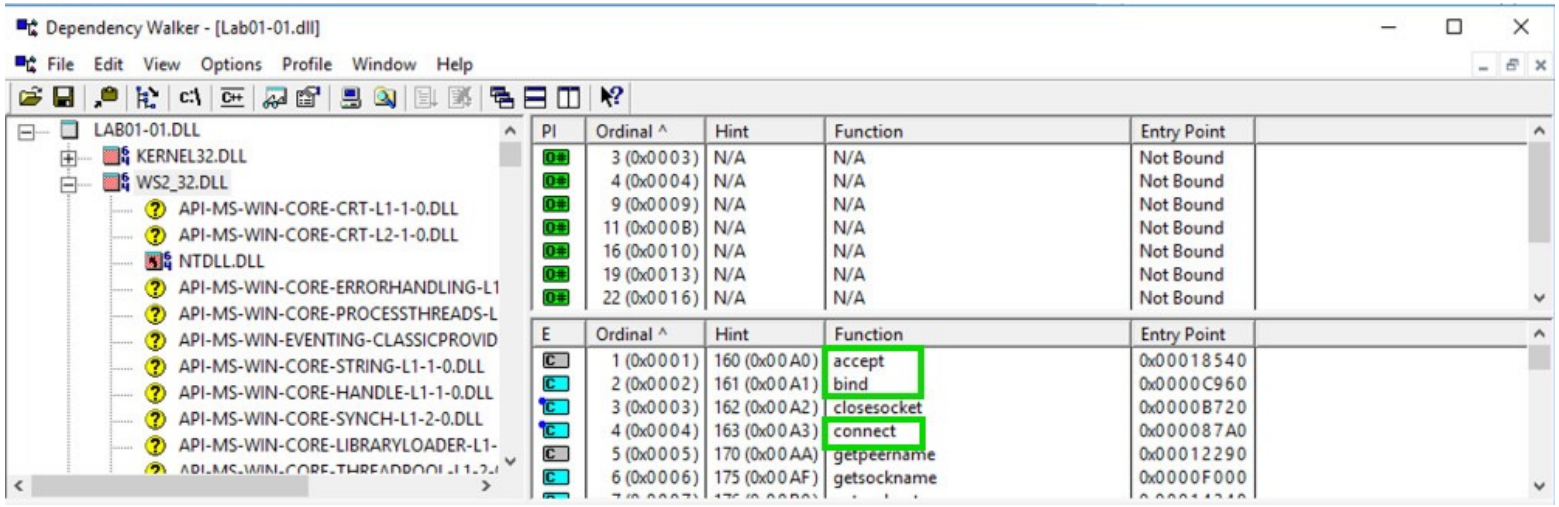
Dependency Walker

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



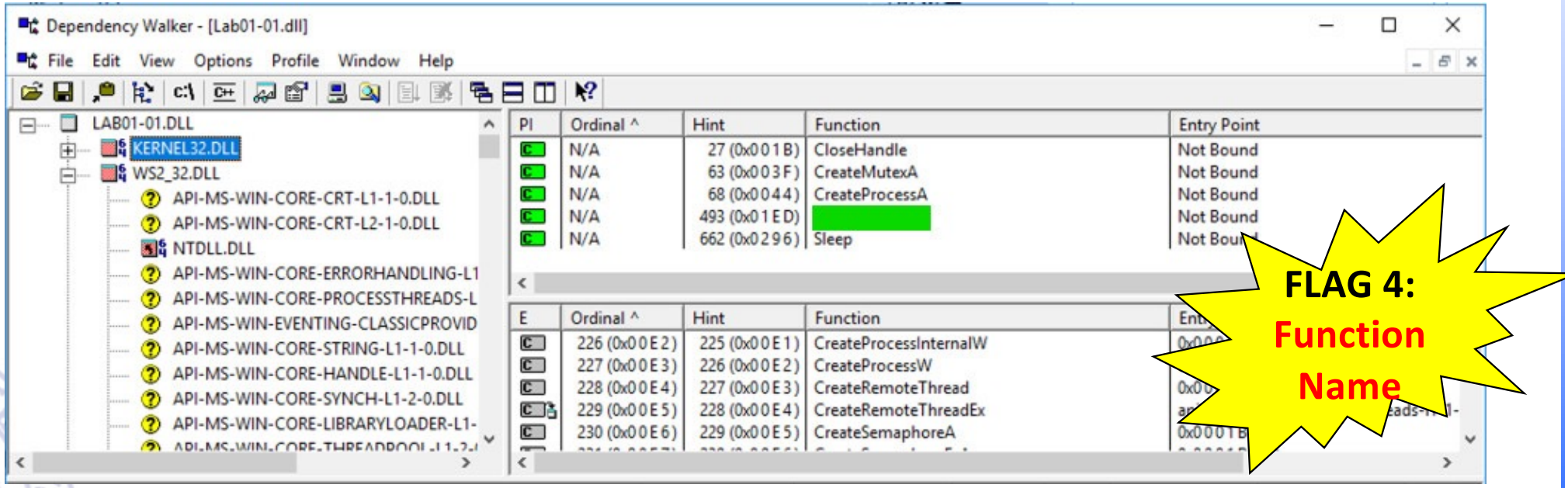
Dependency Walker

- 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

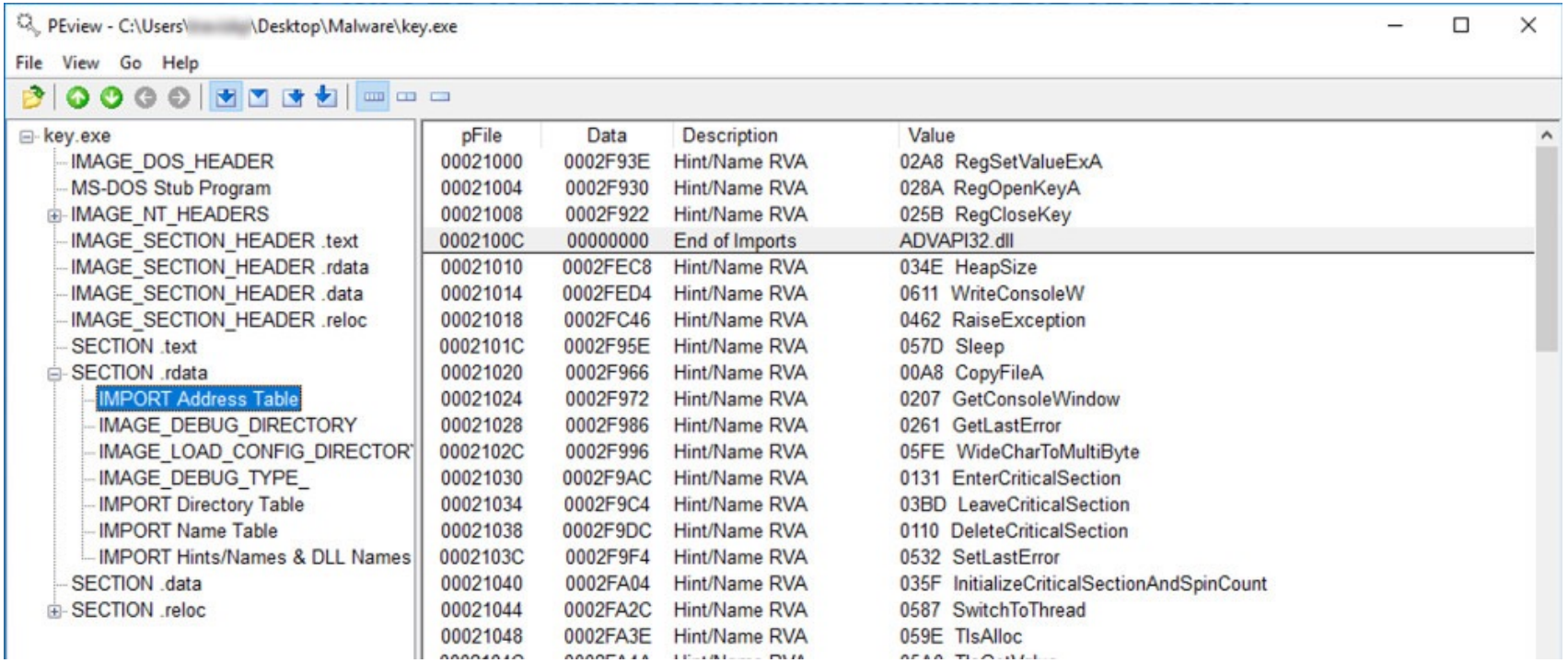


Basic Static Analysis

- 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 datestamp**)

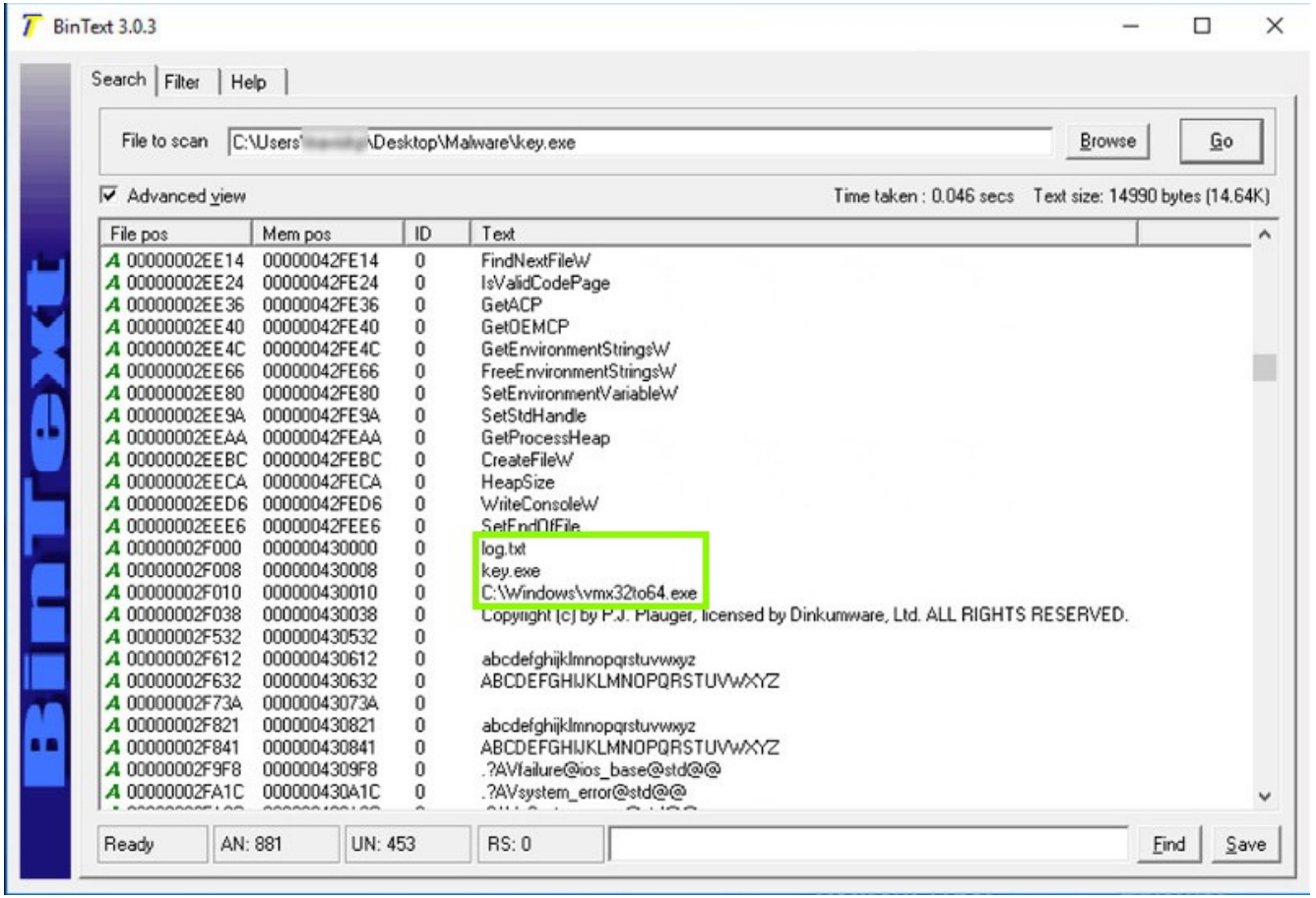
Keylogger

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



Keylogger

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

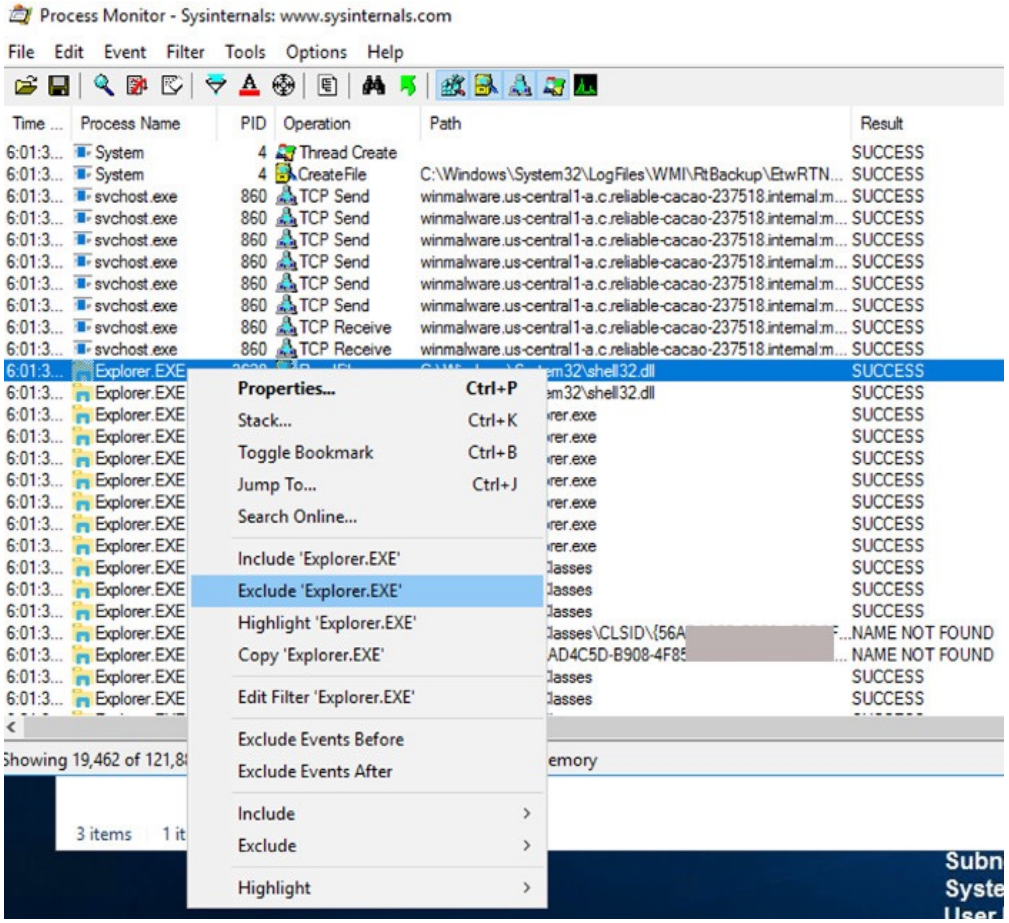


Basic Dynamic Analysis

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

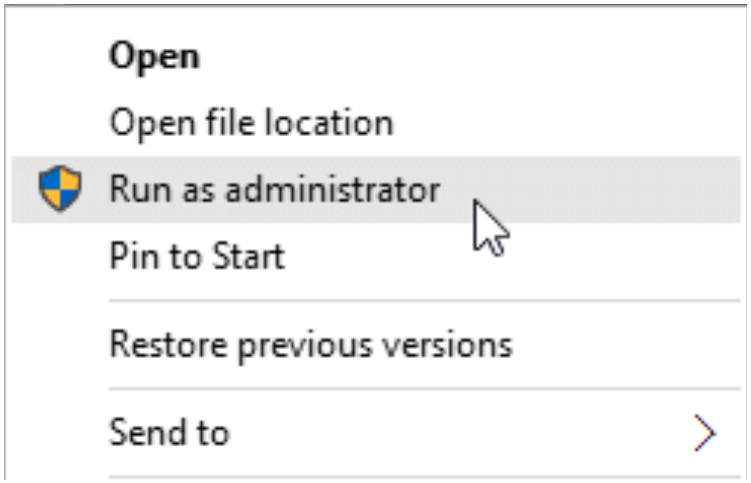
Process Monitor

- **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)



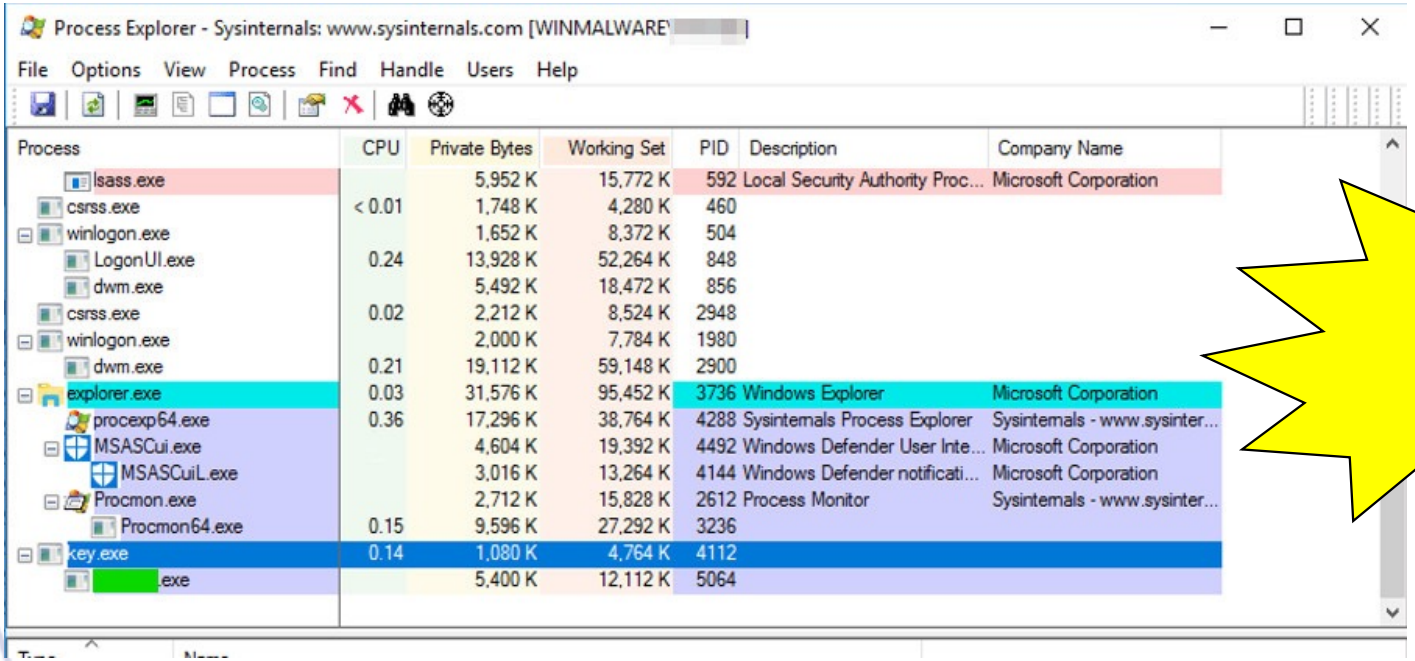
Run keylogger as administrator

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



Viewing the running malware in Process Explorer

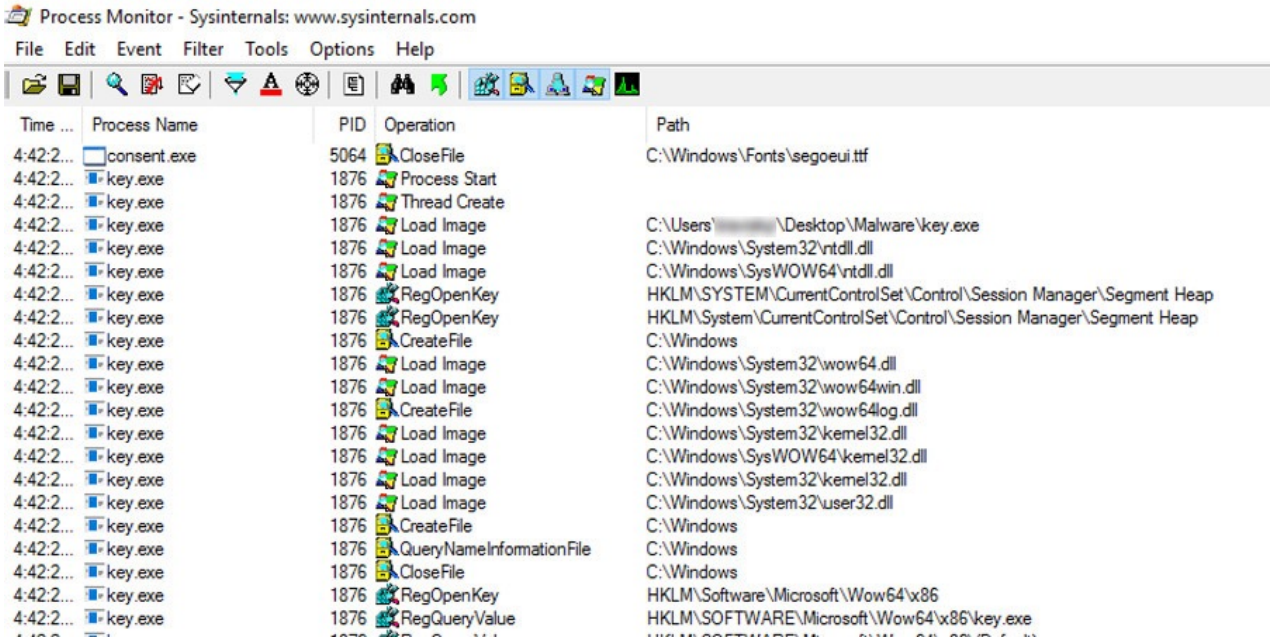
- In Process Explorer, in the top pane, find **key.exe** and click it
- Find the name of the exe covered in green in the image below



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



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\[redacted]\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

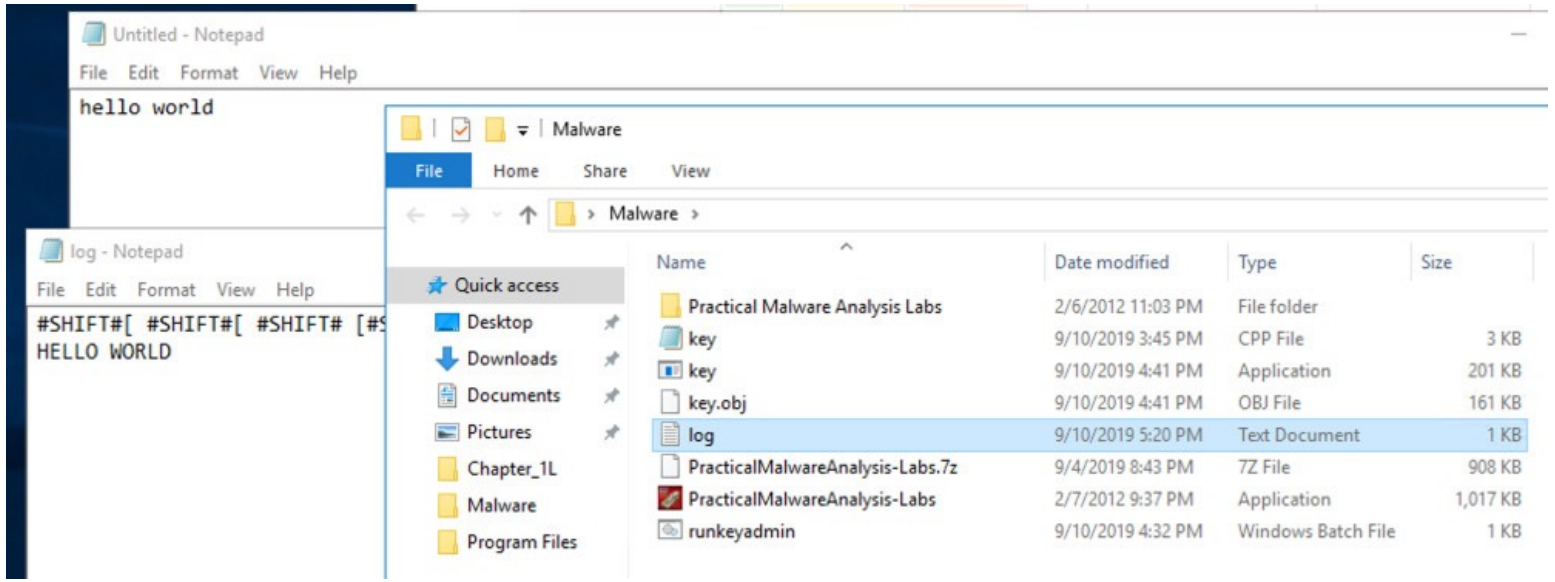
- The malware also creates persistence by modifying the run registry key for the current user (HKCU = HKEY_CURRENT_USER)
- Find the path of that key and take note of it
- The flag is the text covered in green

FLAG 9: Process Monitor

4:42:2...	key.exe	1876	QueryRemoteProtocolInformation	C:\Windows\vmx32to64.exe
4:42:2...	key.exe	1876	CloseFile	C:\Windows\vmx32to64.exe
4:42:3...	key.exe	1876	CloseFile	C:\Users\traviskp\Desktop\Malware\key.exe
4:42:3...	key.exe	1876	RegOpenKey	HKCU
4:42:3...	key.exe	1876	RegQueryKey	HKCU
4:42:3...	key.exe	1876	RegQueryKey	HKCU
4:42:3...	key.exe	1876	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run
4:42:3...	key.exe	1876	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
4:42:3...	key.exe	1876	RegQueryKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
4:42:3...	key.exe	1876	[redacted]	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\vmx32to64
4:42:3...	key.exe	1876	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
4:42:5...	key.exe	1876	Thread Exit	
4:42:5...	key.exe	1876	Thread Exit	
4:42:5...	key.exe	1876	Thread Exit	
4:43:0...	key.exe	1876	CreateFile	C:\Users\traviskp\Desktop\Malware\log.txt

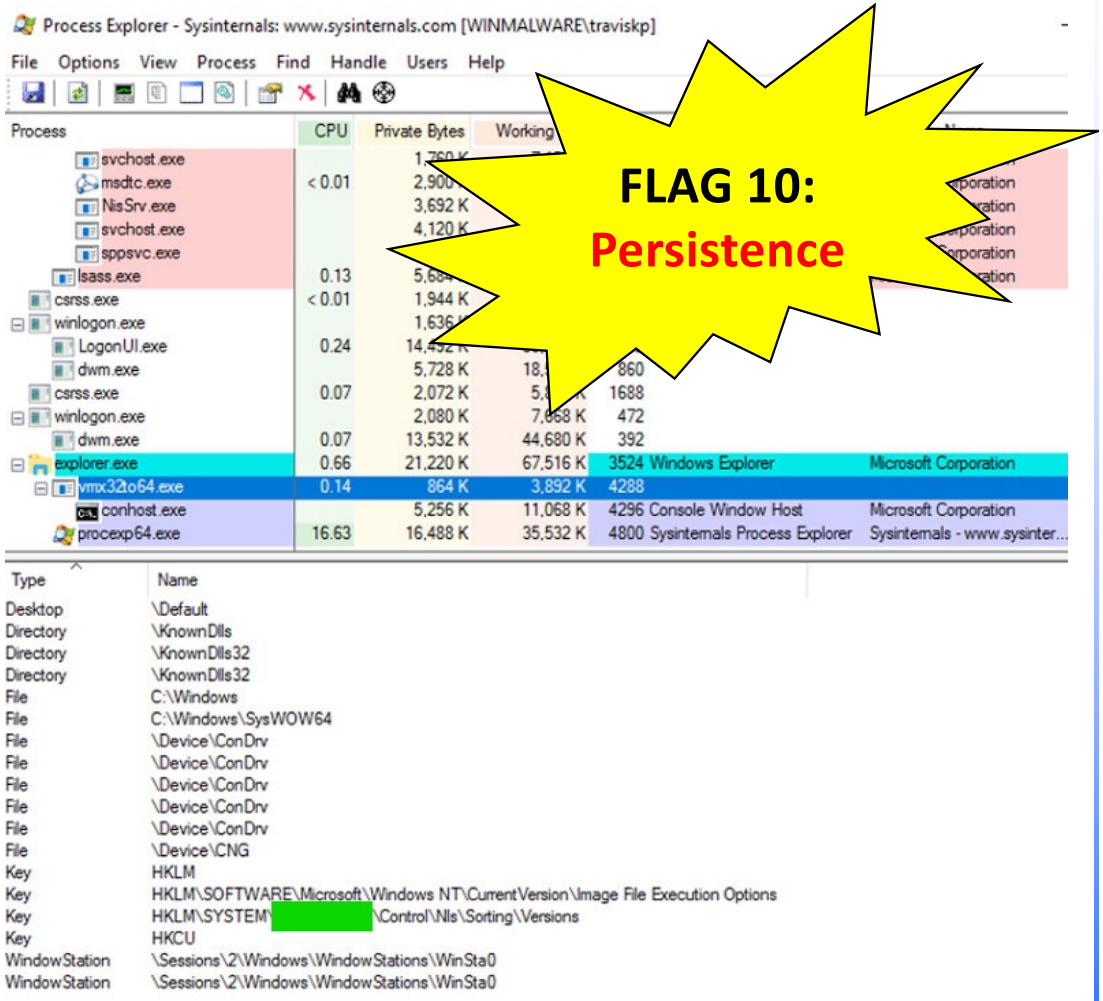
Run the keylogger

- 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



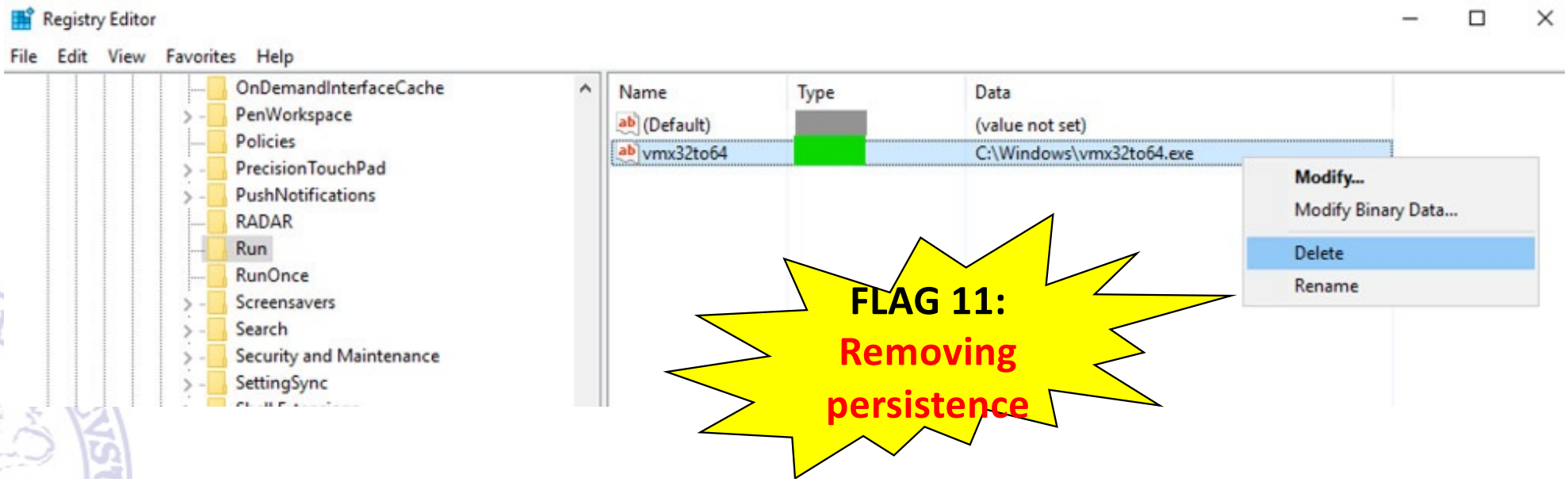
Persistence

- 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



Removing persistence

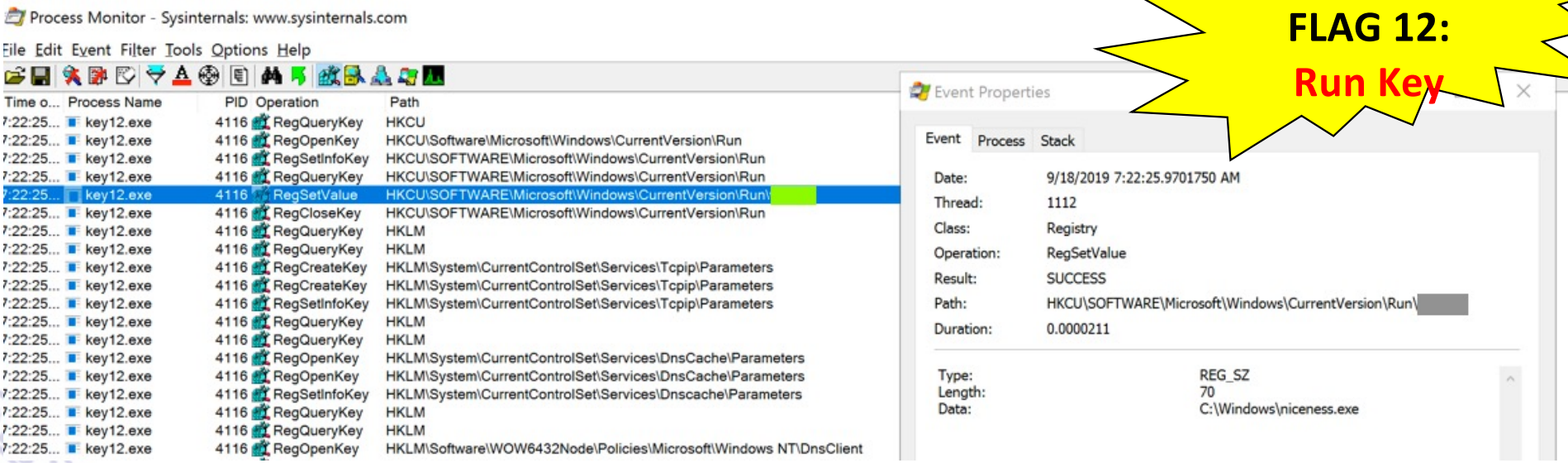
- Run regedit
- Navigate to **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**
- Remove the Run entry, take note of the type (flag)



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



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

Capa

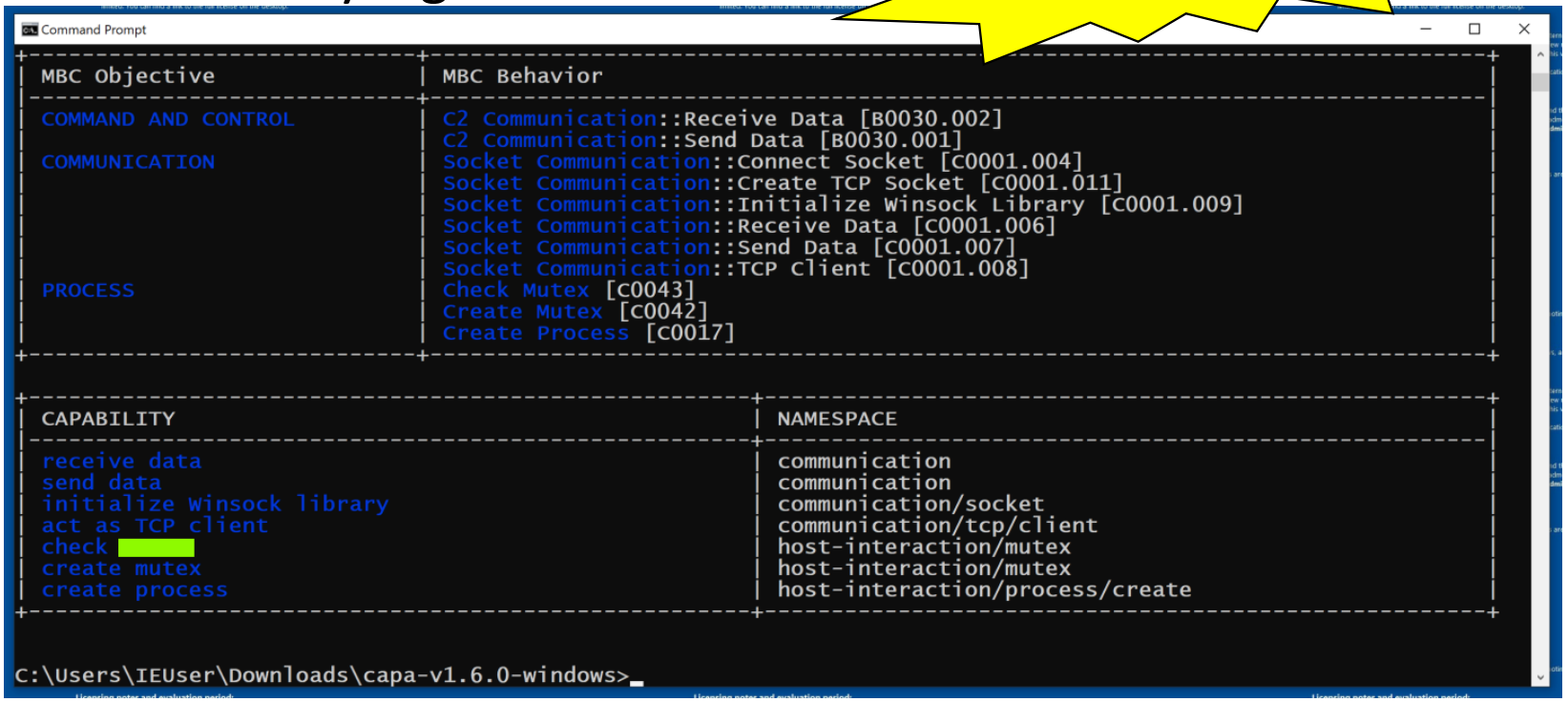
- Get the **capa** tool (https://github.com/fireeye/capa/releases)
- Use it on **Lab01-01.exe**

```
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)



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)