Dynamic Analysis Workflow

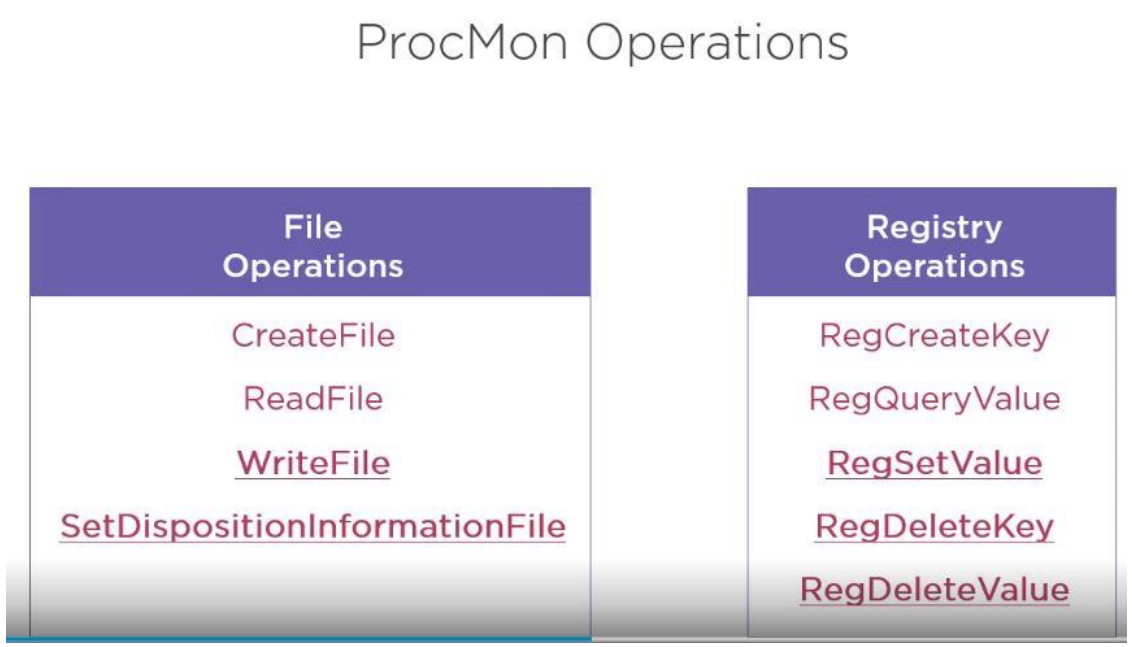
Follow sequence exactly

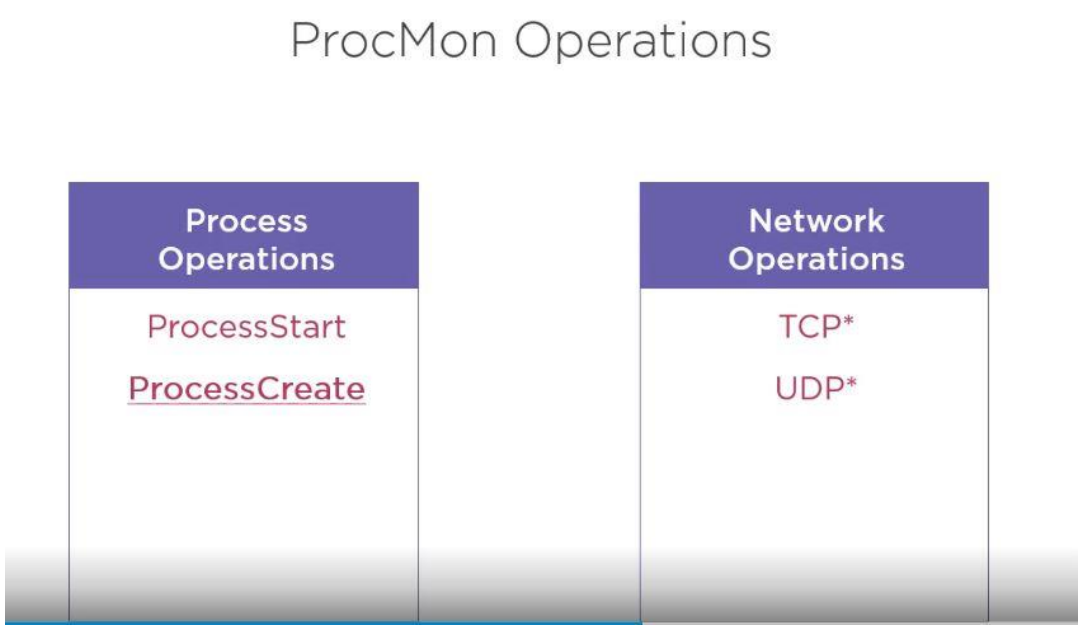
1. Start procmon, then pause and clear
2. Start Fakenet
3. Start Regshot, then take 1st shot
4. Once 1st shot completes, Resume procmon
5. Run Malware for about 1 – 3 mins and study fakenet output
6. After about 3 mins pause procmon
7. Use Regshot, to take 2nd shot
8. Once 2nd shot completes, click Compare->Compare and show output
9. Study Regshot output

Work flow sequence continued

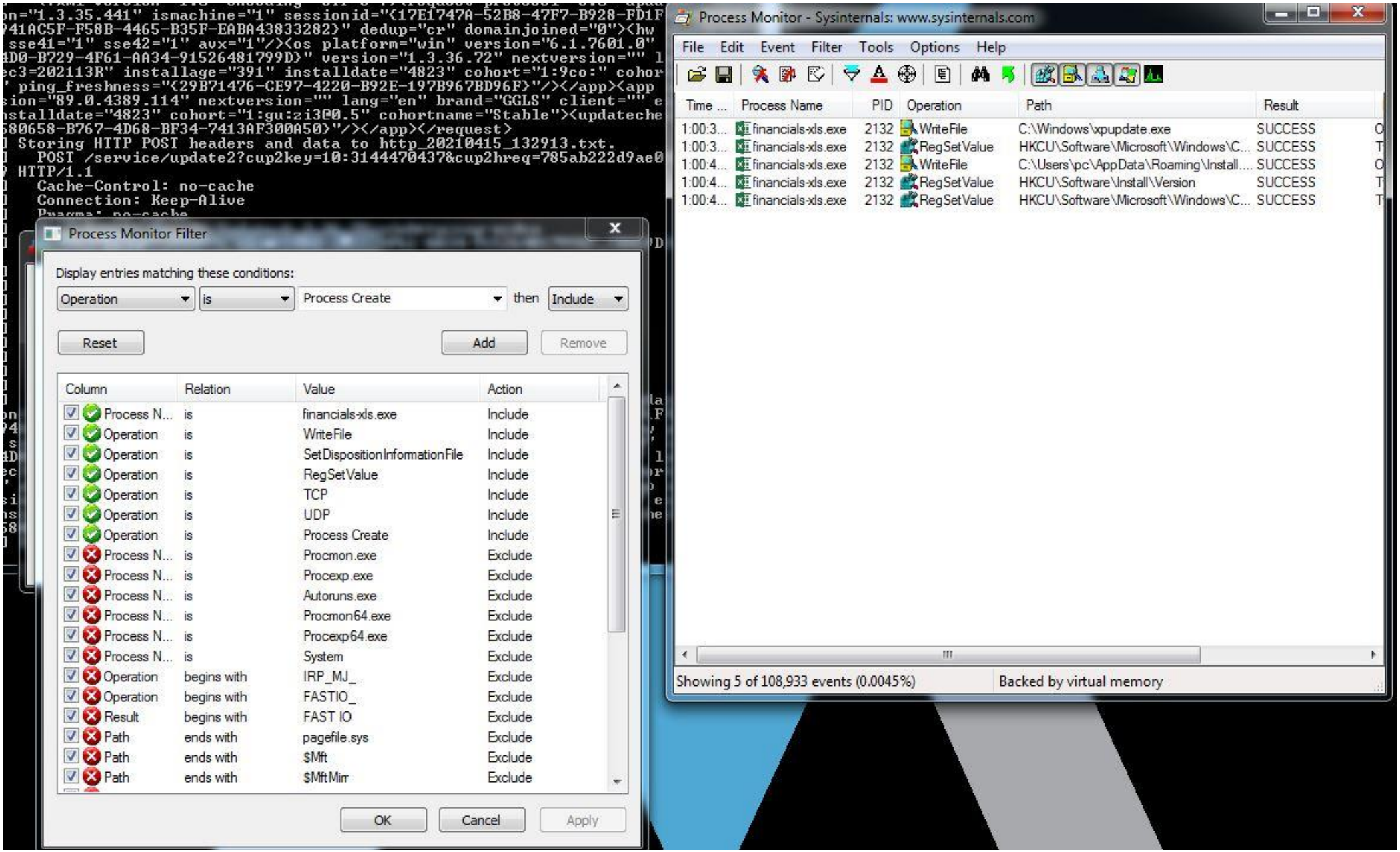
- In procmon apply these filters:
- ProcessName is: malware-name
- Operation is:
  - WriteFile
  - SetDispositionInformationFile
  - RegSetValue
  - ProcessCreate
  - TCP
  - UDP

Procmon filters





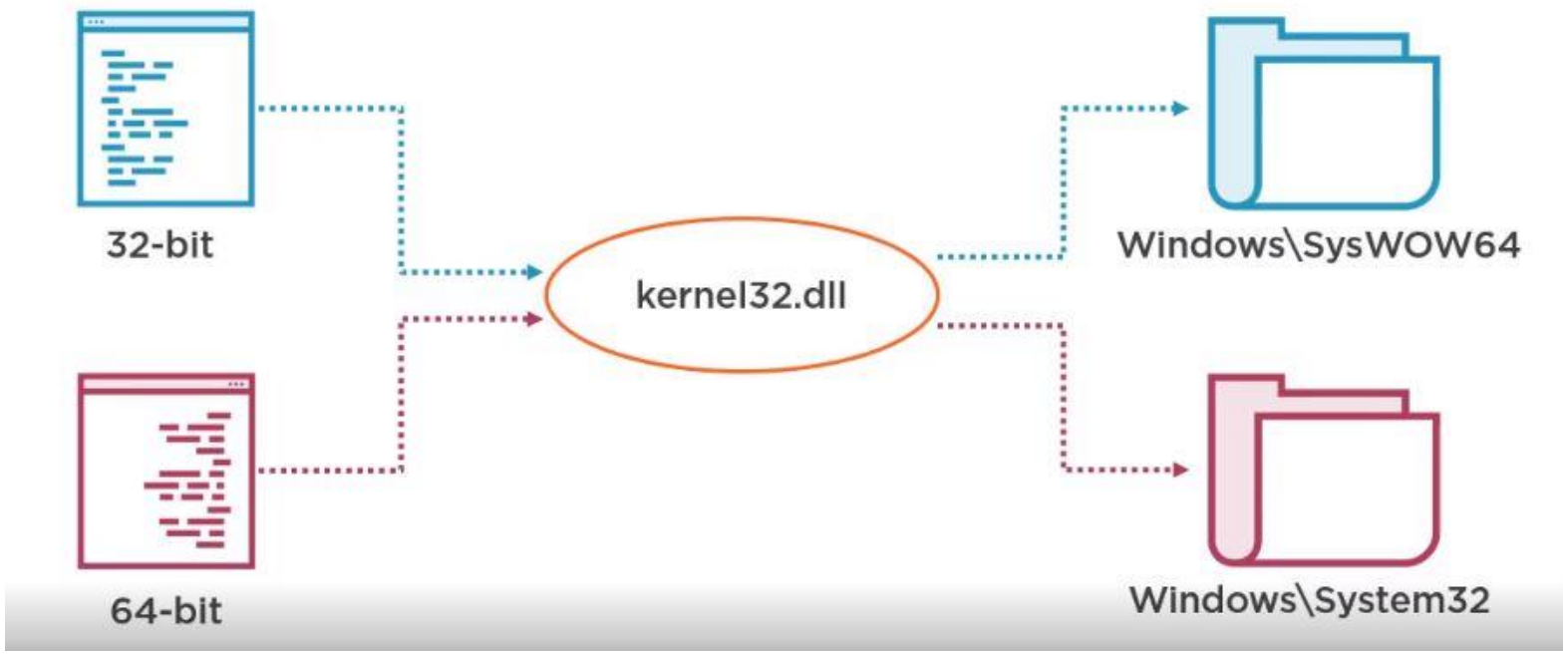
Procmon filters continued

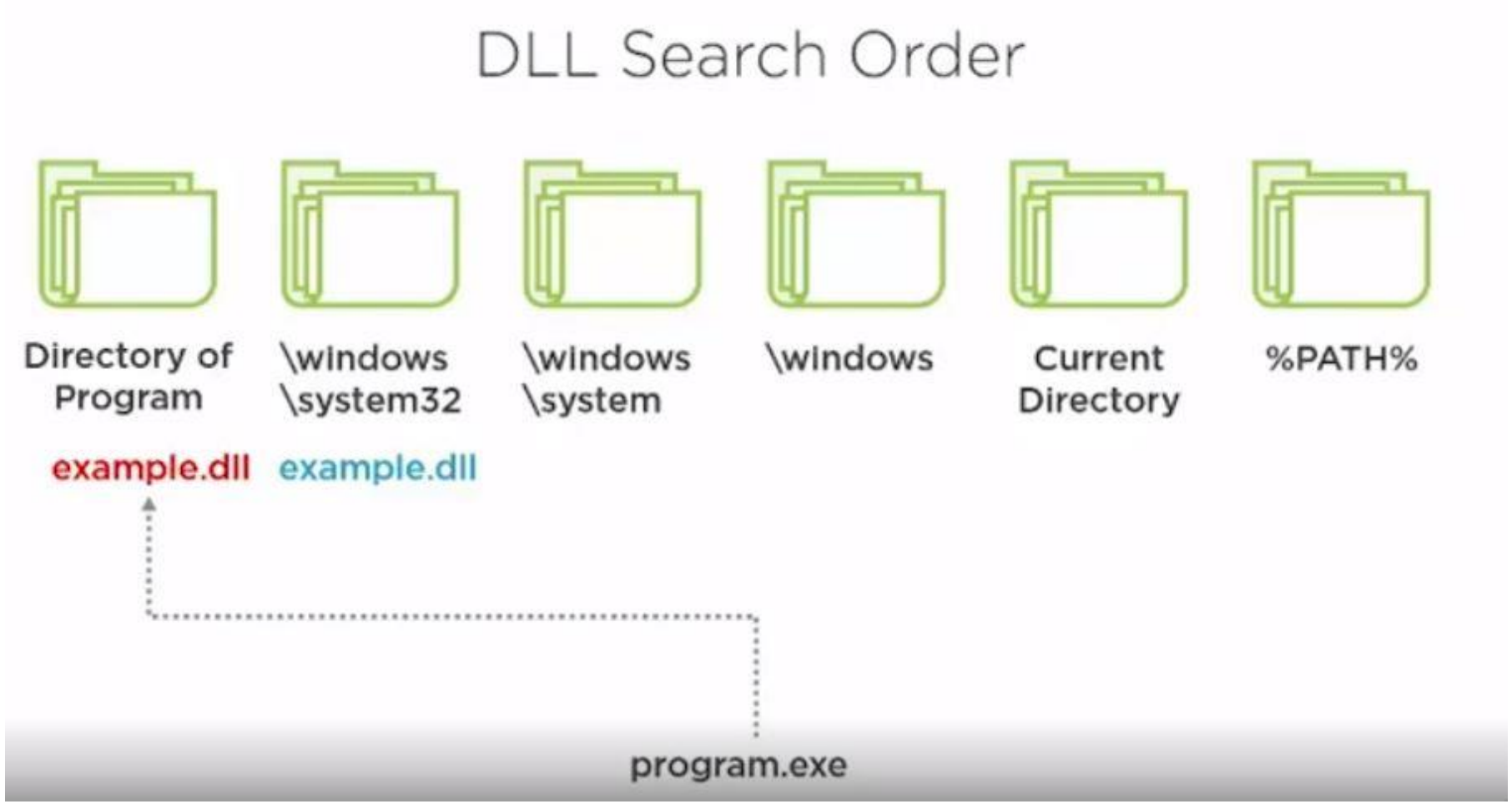


Registry Persistence

HKLM HKU HKCU	\Software\Microsoft\Windows\CurrentVersion\Run
	\Software\Microsoft\Windows\CurrentVersion\RunOnce
	\Software\Microsoft\Windows\CurrentVersion\RunServices
	\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
	\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
	\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs

32-bit Programs on 64-bit Windows




DLL Search Order
Directory of Program
\windows \system32
\windows \system
\windows
Current Directory
%PATH%
example.dll
example.dll
program.exe

Network Analysis

- Fakenet will save a pcap file in the logs folder
- Use wireshark to open it
- Filter out http
- Trace the TCP stream

Thank you