Did I do that?

Understanding action and artifacts in real-time

Matthew Seyer @forensic_matt
David Cowen @HECFBlog

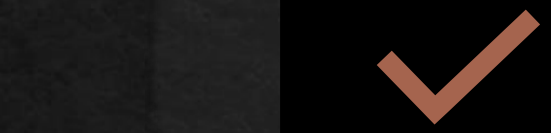
KPMG

Did I do that?

- Understanding the connections between action and artifact
- Not always what we think
- Hypothesis and Validation

KPMG

Common Methodologies



Before and After Collection/Parsing

Collect

Parse

Differential

Live Monitoring

Watch File System Events

- Process Monitor, etc.

Hybrid Approach

- Combine the two methodologies
- Near real time results
- Use of other tools/libs we are familiar with
  - Optional use of native API vs libraries
    - Can account for data not committed to disk
- Differencing on time
- Leave collection behind

Reasons to Listen

Monitor for Understanding

- Not artifact specific
- High level overview

Monitor for Triggering

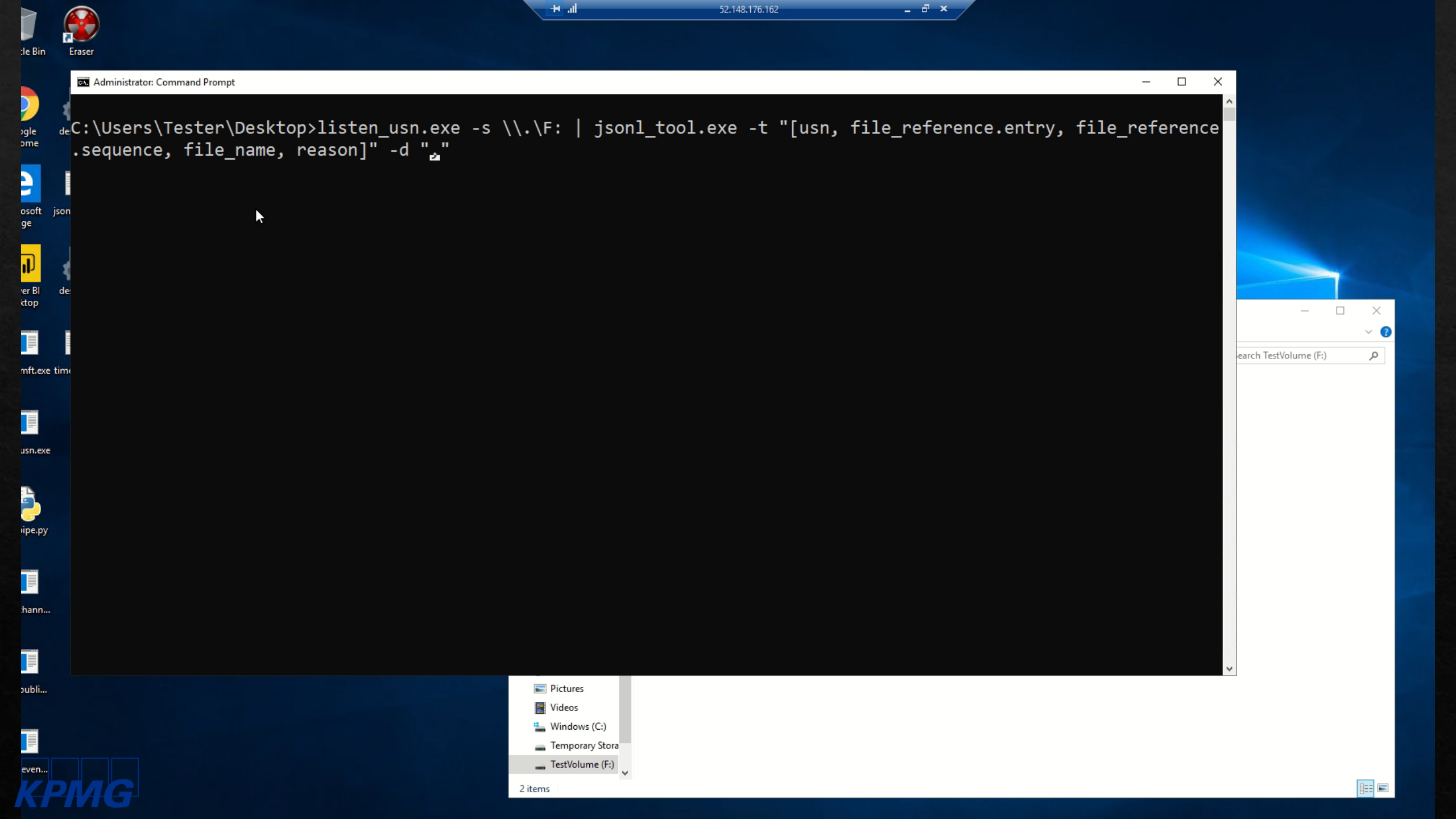
- Perform action on a high level event
- Artifact specific

USN Listening

- Windows API: DeviceIoControl
- Control Code: FSCTL_QUERY_USN_JOURNAL
- Reference: https://docs.microsoft.com/en-us/windows/win32/api/winioctl/ni-winioctl-fsctl_query_usn_journal
- Retrieves USN record buffer from the live volume
  - Contains multiple records in the buffer
- Control ranges fetched with the Update Sequence Number
  - Pro Tip: USN numbers represent offset into the data stream (hence the sparse nature)

What do you get? (Examples)

Value	Meaning
USN_REASON_DATA_EXTEND 0x00000002	The file or directory is extended (added to).
USN_REASON_DATA_OVERWRITE 0x00000001	The data in the file or directory is overwritten.
USN_REASON_DATA_TRUNCATION 0x00000004	The file or directory is truncated.
USN_REASON_FILE_CREATE 0x00000100	The file or directory is created for the first time.
USN_REASON_FILE_DELETE 0x00000200	The file or directory is deleted.
USN_REASON_RENAME_NEW_NAME 0x00002000	A file or directory is renamed, and the file name in the USN_RECORD_V2 structure is the new name.
USN_REASON_RENAME_OLD_NAME 0x00001000	The file or directory is renamed, and the file name in the USN_RECORD_V2 structure is the previous name.


52.148.176.162
Administrator: Command Prompt
C:\Users\Tester\Desktop>listen_usn.exe -s \\.\F: | jsonl_tool.exe -t "[usn, file_reference.entry, file_reference.sequence, file_name, reason]" -d ","
Pictures
Videos
Windows (C:)
Temporary Stora
TestVolume (F:)
2 items
Search TestVolume (F:)
Eraser
KPMG

Slide Throw Back

ArangoDB Result

Query | 138 elements | 7.504 s | JSON | Table

timestamp	original_file	last_wiped_name
2018-04-26 18:41:11.954	commit-msg.sample	+xd'zYuYDR}A7yWb_
2018-04-26 18:41:15.626	45695673349e3947e8e5ae42332d0ac3164cd7	cnKR3JdlGHcwxlI`gZYM'aVE`h!IcRbeRx_ygT
2018-04-26 18:41:14.345	7b8b1e5c9d0984ef36e991b5b02de6e53600ed	Lp_4NI~7(CyoVgB60]3u_5g63~P5ctV_)Kc]A)
2018-04-26 18:41:16.220	aaf43278567996a93d40e0de1bd96762e7911f	s7),_udch0yVq3iWZ5v7qd)Q(c2+HMQl0B656w
2018-04-26 18:41:09.392	d1a0740484a17cfd6bd7ba5912f54601d407c7	5dZ-0L{tl8o50}ukYa_'!J)HW4,I4jgx9j]V,B
2018-04-26 18:41:10.595	index	_oj+I
2018-04-26 18:41:16.548	description	pLApzc7Ffuu

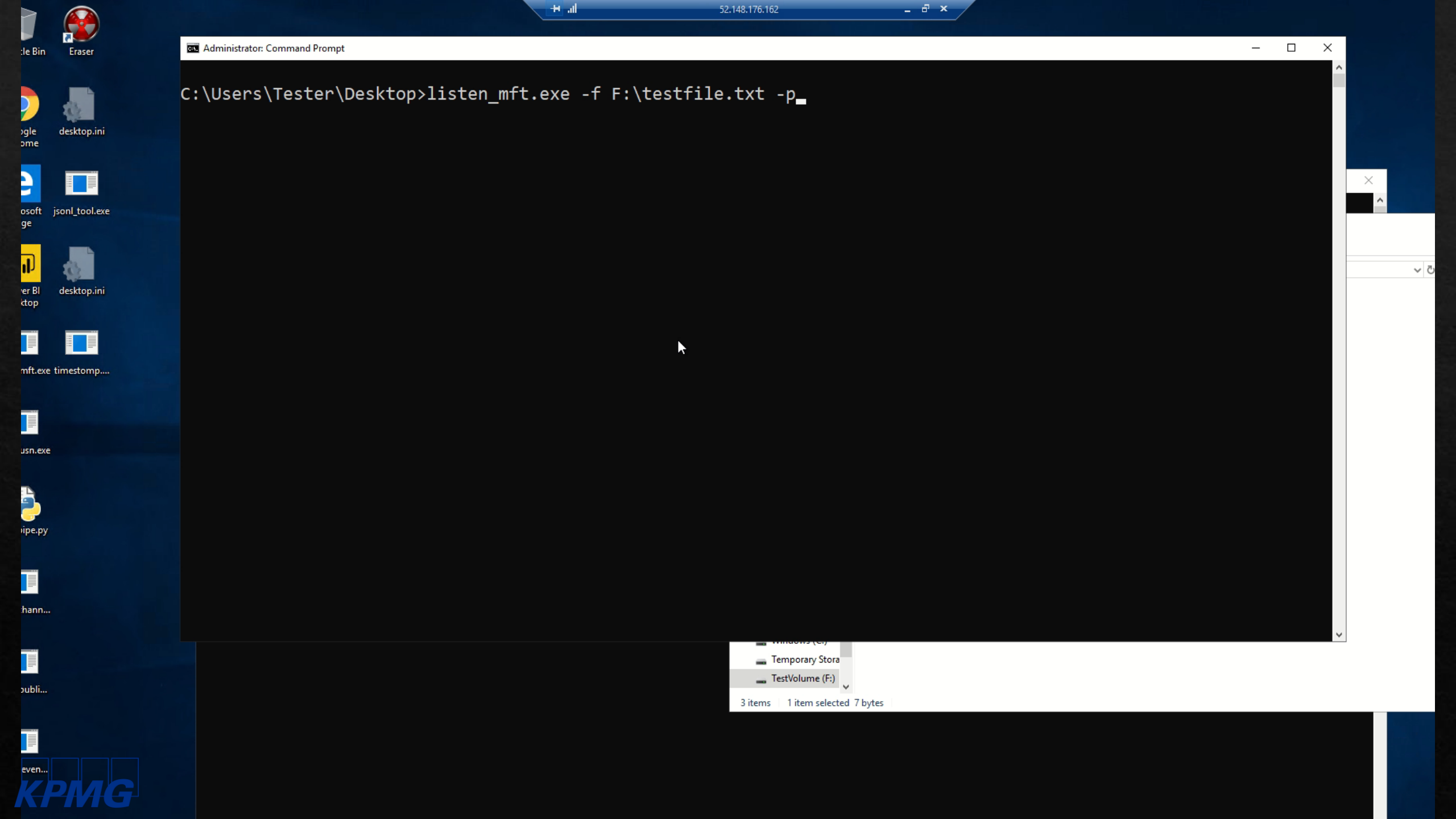
KPMG

MFT Listening

- Windows API: DeviceIoControl
- Control Code: FSCTL_GET_NTFS_FILE_RECORD
- Reference: https://docs.microsoft.com/en-us/windows/win32/api/winioctl/ni-winioctl-fsctl_get_ntfs_file_record
- Retrieves the first file record that is in use and is of a lesser than or equal ordinal value to the requested file reference number
  - Not able to fetch unallocated records

MFT Listening

- Combines Triggering, Parsing, and Differencing
- No monitor specific APIs


52.148.176.162
Administrator: Command Prompt
C:\Users\Tester\Desktop>listen_mft.exe -f F:\testfile.txt -p
Eraser
desktop.ini
jsonl_tool.exe
desktop.ini
timestomp....
Temporary Stora
TestVolume (F:)
3 items
1 item selected 7 bytes

Event Log Listening

- Windows API: EvtSubscribe (One of many)
- Reference: https://docs.microsoft.com/en-us/windows/win32/api/winevt/nf-winevt-evtsubscribe
- Creates a subscription that will receive current and future events from a channel or log file that match the specified query criteria
- First enumerate available channels to know what you can subscribe too
- Difficult subsystem that contains dozens of Evt* functions that pair together

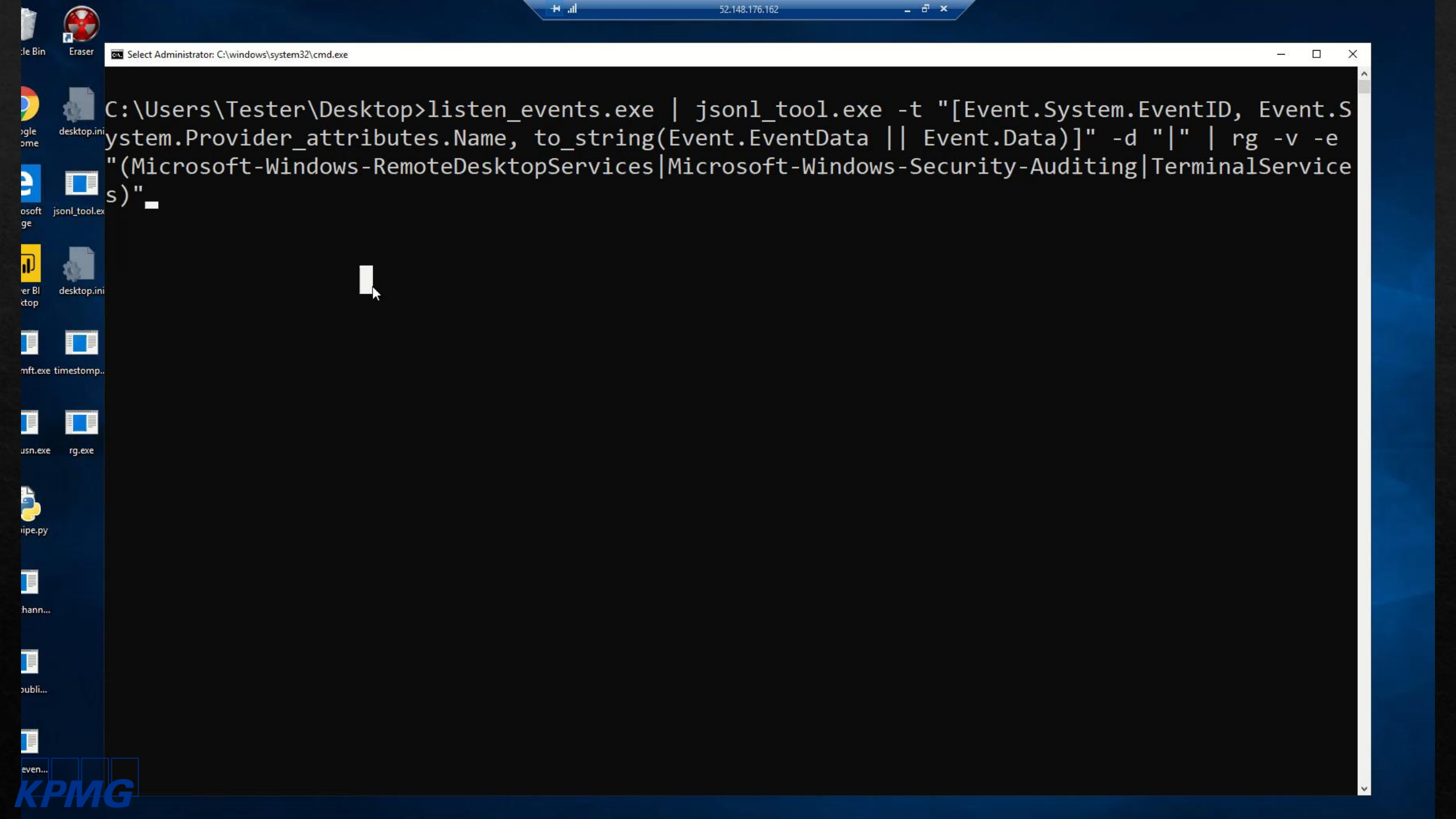
Windows Event Log API

Uses a callback system

Unlike USN listening method

Allows you to use queries for Event filtering (XPath 1.0 query or structured XML query)

KPMG

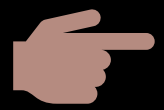

52.148.176.162
Select Administrator: C:\windows\system32\cmd.exe
C:\Users\Tester\Desktop>listen_events.exe | jsonl_tool.exe -t "[Event.System.EventID, Event.System.Provider_attributes.Name, to_string(Event.EventData || Event.Data)]" -d "|" | rg -v -e "(Microsoft-Windows-RemoteDesktopServices|Microsoft-Windows-Security-Auditing|TerminalServices)"
Eraser
desktop.ini
jsonl_tool.ex
desktop.ini
timestomp..
rg.exe
KPMG

Event Trace Listening (ETW)

- Windows API: ProcessTrace (One of many)
- Reference: https://docs.microsoft.com/en-us/windows/win32/api/evntrace/nf-evntrace-processtrace
- The **ProcessTrace** function delivers events from one or more event tracing sessions to the consumer
- Difficult subsystem that contains dozens of functions that pair together
- Enumerate Providers, use Controllers, implement Consumers

ETW API

Uses a callback system like Windows Events API



Allows you to select which Providers and filters to use

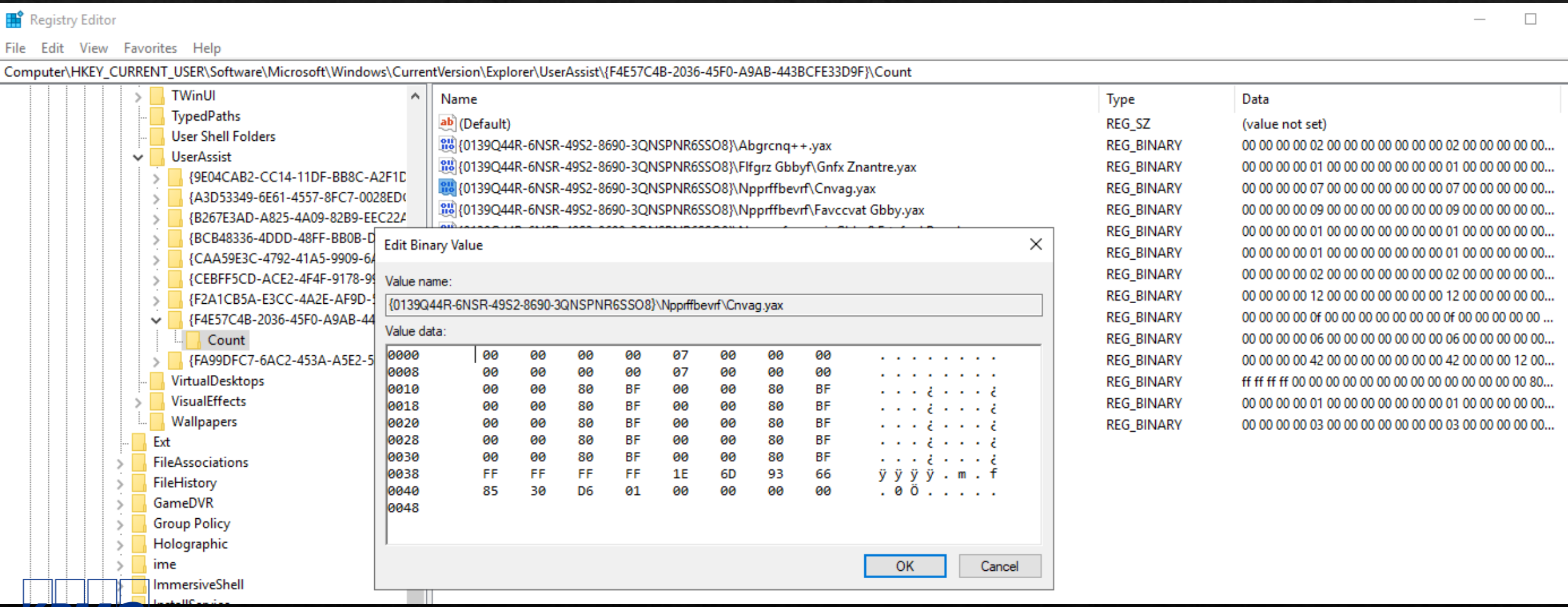
Complicated system

KPMG

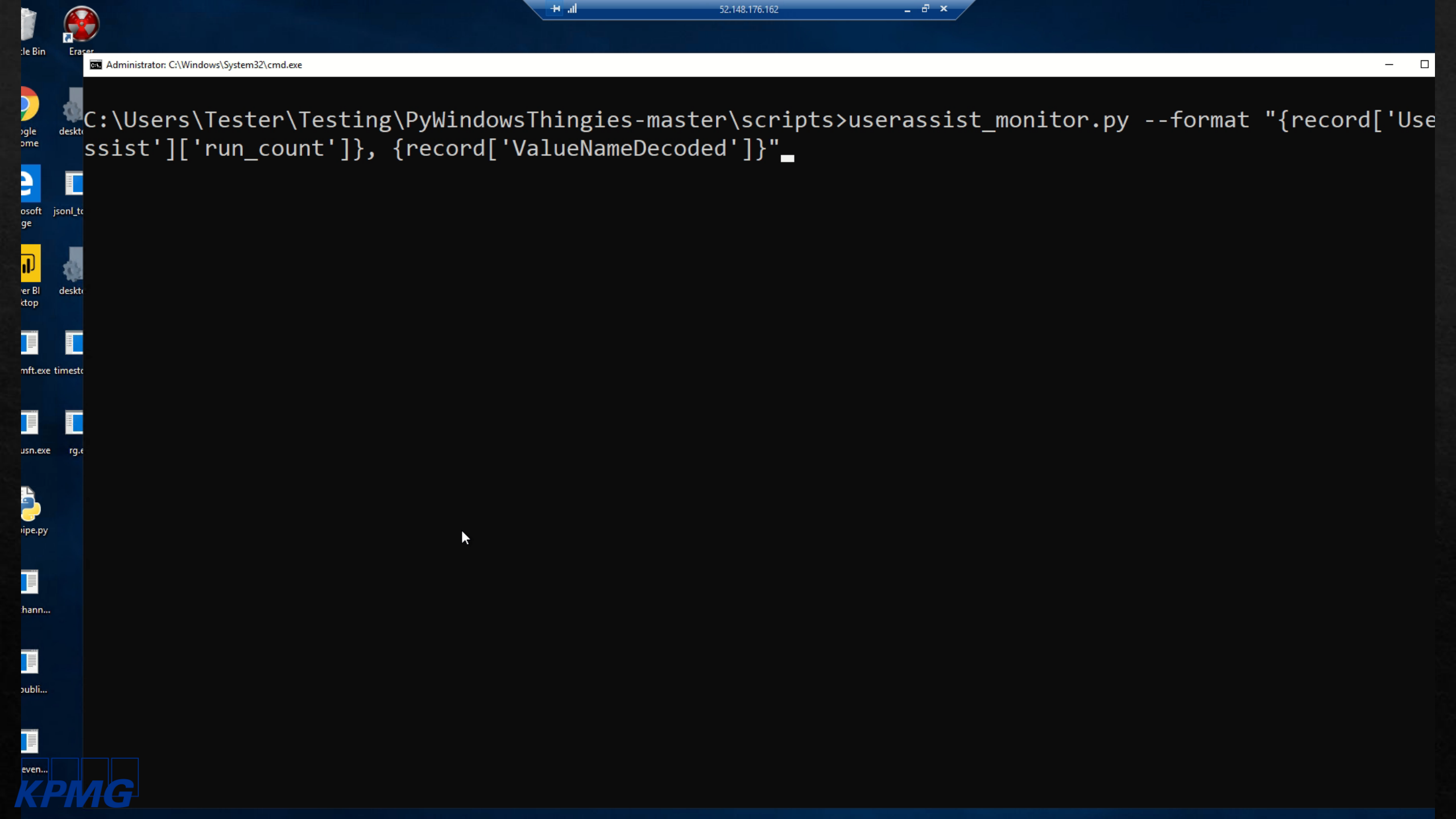
Example Tool: UserAssist Monitor

- Custom Artifact Monitor
- Windows API for triggers
- Custom parsing for mapping logic and artifact parsing
- Steps
  - Map UserAssist Keys in Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
  - Listen to ETW for Registry Changes to UserAssist keys
  - Parse UserAssist data structures

Why is this difficult?



KPMG


52.148.176.162
Administrator: C:\Windows\System32\cmd.exe
C:\Users\Tester\Testing\PyWindowsThingies-master\scripts>userassist_monitor.py --format "{record['Use
ssist']['run_count']}, {record['ValueNameDecoded']}"
KPMG

Windows API Overview/Cheetsheet

Artifact	Windows API	Control Code or Filters	Description
USN	DeviceIoControl	FSCTL_READ_USN_JOURNAL	Retrieves the set of update sequence number (USN) change journal records between two specified USN values
MFT	DeviceIoControl	FSCTL_GET_NTFS_FILE_RECORD	Retrieves the first file record that is in use and is of a lesser than or equal ordinal value to the requested file reference number
Registry	RegNotifyChangeKeyValue	REG_NOTIFY_CHANGE_NAME | REG_NOTIFY_CHANGE_ATTRIBUTES | REG_NOTIFY_CHANGE_LAST_SET | REG_NOTIFY_CHANGE_SECURITY	Notifies the caller about changes to the attributes or contents of a specified registry key
Windows Events	EvtSubscribe …	Query (XPath 1.0 queryor structured XML query)	Creates a subscription that will receive current and future events from a channel or log file that match the specified query criteria
Event Tracing	OpenTrace ProcessTrace …		The ProcessTrace function delivers events from one or more event tracing sessions to the consumer

Components by OS (More than just Windows)

Windows APIs

ETW
USN
Registry

Mac APIs

fsevents

Linux APIs

inotify

KPMG

Can we be friends?

- System APIs are not practitioner friendly and hardly dev friendly
- Good news!
  - Tools and libs that already exist
  - Not limited to Windows

Python

- Its something we all use… (Except Brain Moran, keeping Perl alive)
- File System Events
  - Watchdog (Python API and shell utilities to monitor file system events)
    - https://pypi.org/project/watchdog/
- Pywintrace
  - Python-based ctypes wrapper around the Win32 APIs necessary for controlling ETW sessions and processing message data
    - https://github.com/fireeye/pywintrace

Questions

- Hit us up – Matthew Seyer @forensic_matt, David Cowen @HECFBlog
- Rust and Windows API PoCs (https://github.com/forensicmatt/RsWindowsThingies)
- Python and Windows API PoCs (https://github.com/forensicmatt/PyWindowsThingies)

KPMG