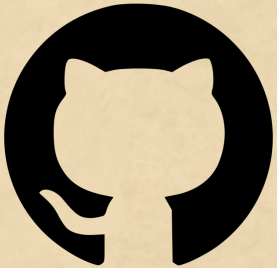
Using elrond in DFIR

acquired artefacts to TTPs, all before elevenses

Ben Smith – Lead Threat Hunter

whoami



Masquerading: Masquerade File Type

Other sub-techniques of Masquerading (8)

Adversaries may masquerade malicious payloads as legitimate files through changes to the payload's formatting, including the file's signature, extension, and contents. Various file types have a typical standard format, including how they are encoded and organized. For example, a file's signature (also known as header or magic bytes) is the beginning bytes of a file and is often used to identify the file's type. For example, the header of a JPEG file, is `0xFF 0xD8` and the file extension is either `.JPE`, `.JPEG` or `.JPG`.

ID: T1036.008

Sub-technique of: T1036

ⓘTactic: Defense Evasion

ⓘPlatforms: Linux, Windows, macOS

Contributors: Ben Smith; CrowdStrike Falcon OverWatch

Agenda

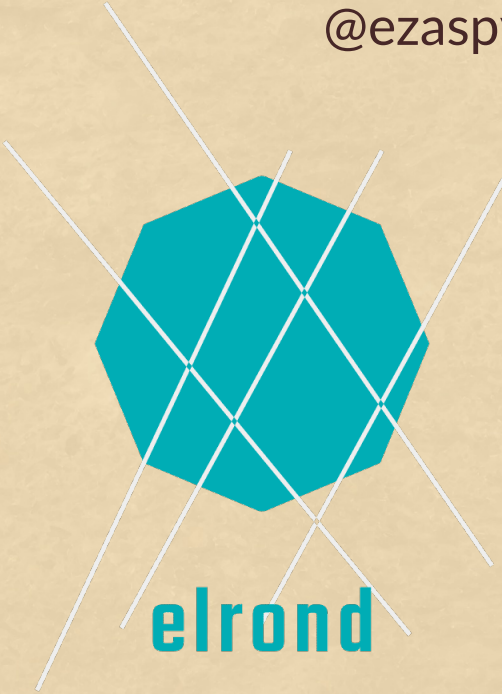
gandalf

elrond

elrond

@ezaspy

- Mount
  - E01, VMDK, dd, raw, img
  - Windows, Linux, macOS, memory
- Collect & Process
  - Raw format -> existing tool -> JSON/CSV
- Ingest (post)
  - Splunk, Elastic/Kibana
  - ATT&CK navigator
- Analyse
  - Hashing, file recovery, keyword searching, IoC extraction, AV scanning, Timelining...
- Audited



Inspiration

Acquire

- Images
- Artefacts

Parse

- Different artefact…
- Different tool…

Ingest

- Many images*
- Previous cases

Analyse

- Different output…
- Different tool…

*VSS
*Multiple partitions

Inspiration

Acquire

- Images
- Artefacts

Parse

- Different artefact…
- Different tool…

Ingest

- Many images*
- Previous cases

Analyse

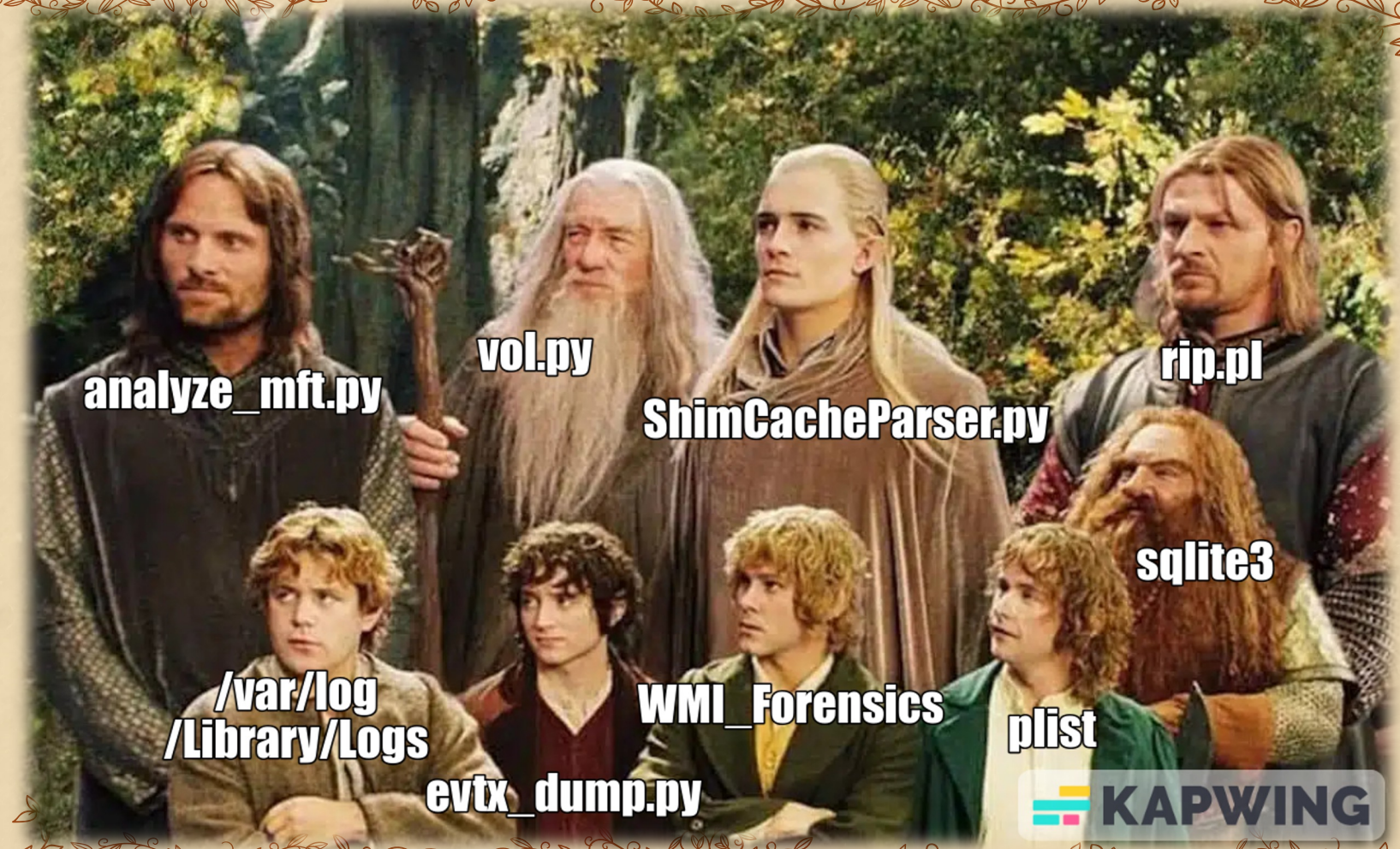
- Different output…
- Different tool…

- Existing tools
- Same output

- Repeatable
- Consistent

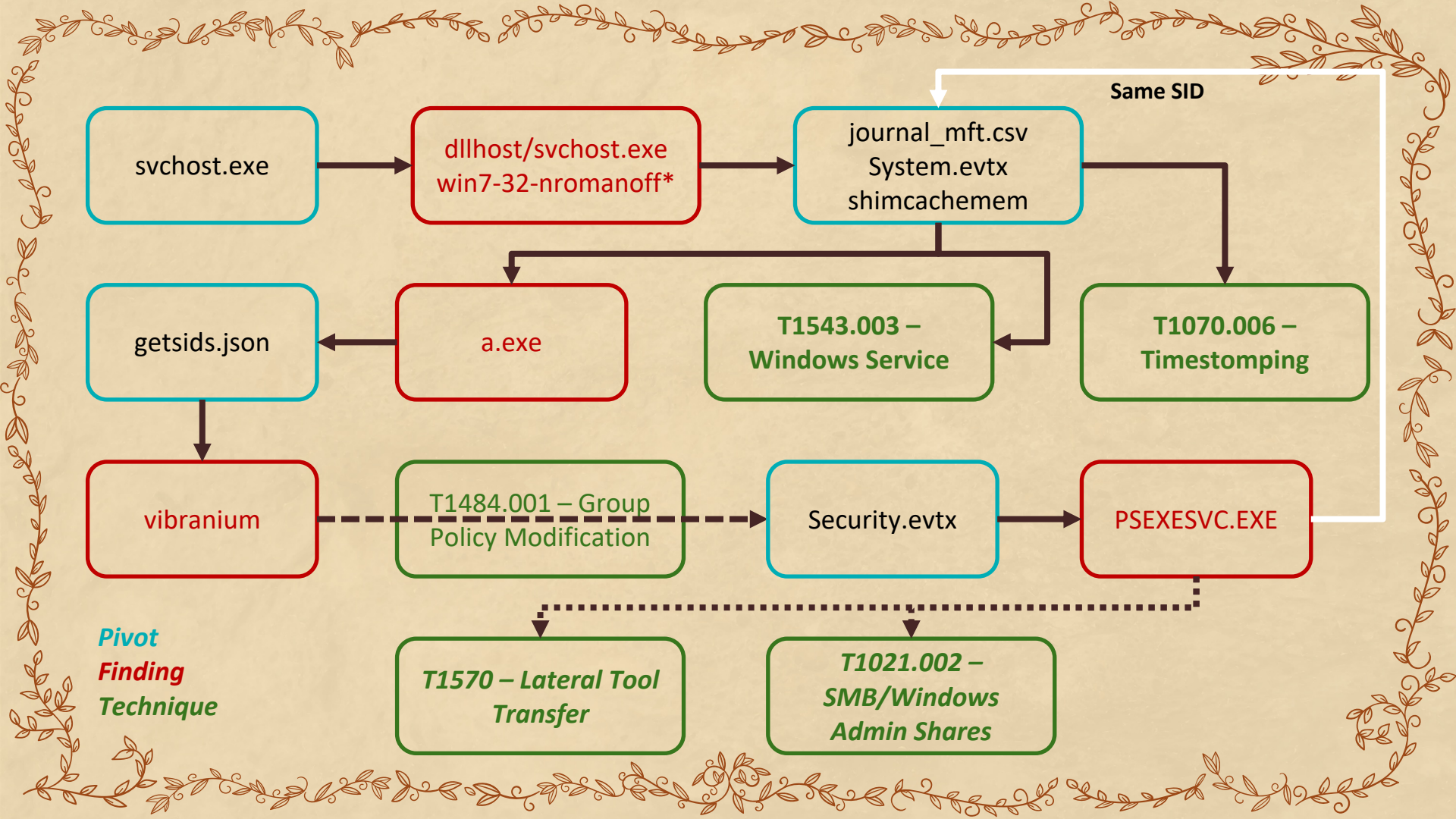
- Fast
- Easy to pivot

*VSS
*Multiple partitions


analyze_mft.py
vol.py
ShimCacheParser.py
rip.pl
sqlite3
/var/log
/Library/Logs
WMI_Forensics
plist
evtx_dump.py
KAPWING

elrond

Demo


Same SID
svchost.exe
dllhost/svchost.exe
win7-32-nromanoff*
journal_mft.csv
System.evtx
shimcachemem
getsids.json
a.exe
T1543.003 – Windows Service
T1070.006 – Timestomping
vibranium
T1484.001 – Group Policy Modification
Security.evtx
PSEXESVC.EXE
T1570 – Lateral Tool Transfer
T1021.002 – SMB/Windows Admin Shares
Pivot
Finding
Technique

Inspiration

Acquire

- Images
- Artefacts

Parse

- Different artefact…
- Different tool…

- Existing tools
- Same output

Ingest

- Many images*
- Previous cases

- Repeatable
- Consistent

Analyse

- Different output…
- Different tool…

- Fast
- Easy to pivot

*VSS
*Multiple partitions

Inspiration

Acquire

- Images
- Artefacts

- One tool
- Native technology

Parse

- Different artefact…
- Different tool…

- Existing tools
- Same output

Ingest

- Many images*
- Previous cases

- Repeatable
- Consistent

Analyse

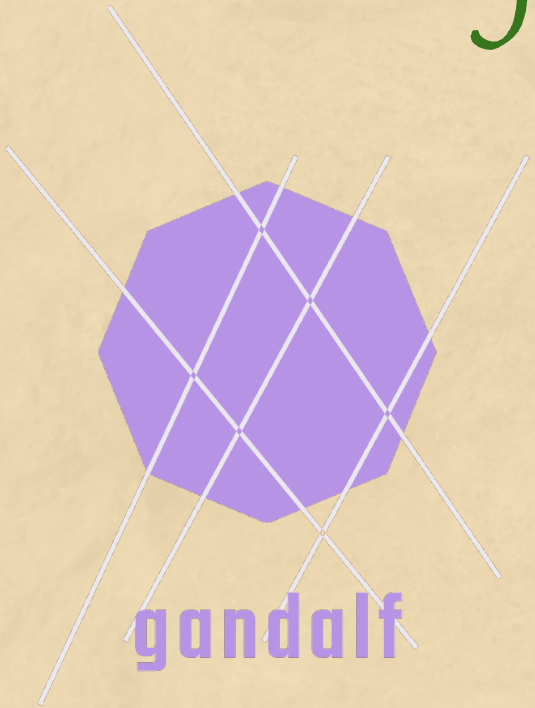
- Different output…
- Different tool…

- Fast
- Easy to pivot

*VSS
*Multiple partitions

gandalf

@ezaspy



- PowerShell, Python, *bash* artefact acquisition scripts
  - Windows, Linux & macOS targets
  - Order of volatility
  - elrond-ready

- Cross-Platform Acquisition (XPA)
  - Python3 on Windows
    - Linux/macOS target
  - pwsh on Linux/macOS
    - Windows target

- Audited

gandalf

Single tool for digital forensics artefact acquisition

- Native technology acquisition scripts
- XPA

elrond

Mount, Collect, Process, Ingest and Analyse digital forensic artefacts

- Automate processing and accelerate analysis
- Leveraging existing tools

/in/itsbensmith

@ezaspy

officialpicturetaker.picfair.com

Q&A