

BREACHES BE CRAZY

SCALING FORENSICS ACROSS MANY SYSTEMS



Eric Capuano
Whitney Champion



WHO ARE WE?

ERIC

- ◉ Co-founder/CTO @ Recon InfoSec
- ◉ SANS DFIR Instructor
- ◉ Former USAF, TXANG, TX Dept. Public Safety
- ◉ @eric_capuano

WHITNEY

- ◉ Co-founder/Lead Architect @ Recon InfoSec
- ◉ Formerly Booz Allen, Red Hat, SPAWAR
- ◉ #HackerTracker
- ◉ unicorns.lol
- ◉ @shortxstack

WHAT DO WE DO?

- ◉ Managed Detection & Response
- ◉ Incident Response
- ◉ Network Defense Range Training
- ◉ OpenSOC Blue Team CTF @ DEF CON
- ◉ ~~Retire to the nerderly with our~~
~~calculators~~ Par-tay

IR IS HARD TO SCALE

1. **Identify** compromised systems
 - a. Without a SIEM? Good luck!
2. **Acquire** forensics images
 - a. Many+ hours
3. **Process** forensic images
 - a. Many+ hours *per* image
4. **Analyze** forensic data
 - a. One!
system!
at!
a!
time!



WHAT ARE WE DOING TODAY?

- ◉ IR at scale!



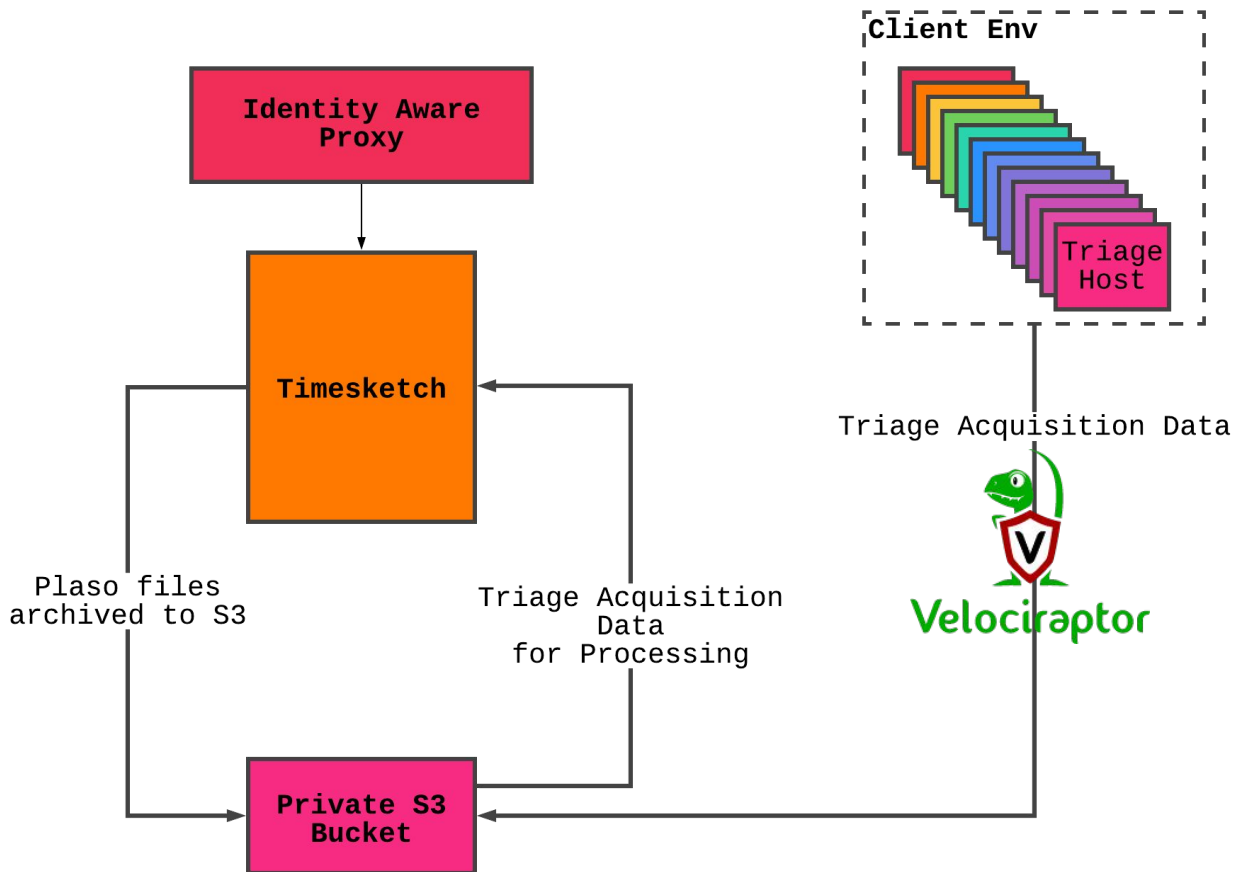
+

<magic>

= =



WHAT THIS LOOKS LIKE



THE DFIR MAGIC

VELOCIRAPTOR



- ⦿ Epic Endpoint Agent
 - Open Source
 - Scalable
 - Cross-platform (Win, Mac, Linux)
 - Extensible via VQL
- ⦿ Multi-purpose
 - Collect forensic artifacts
 - Monitor endpoints
 - Hunt w/ Yara scans
 - Quarantine endpoints
 - So much more...

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR



</

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR



Search clients Show All analyst

Label Clients

Existings

A new label

Online	Client ID	Hostname
<input checked="" type="checkbox"/>	C.17659421bba25be6	ACC-02
<input checked="" type="checkbox"/>	C.92668c3f070f14fa	ACC-04
<input checked="" type="checkbox"/>	C.7cc3a3b5231585bf	ACC-07

Labels

ACC	workstation
ACC	workstation
ACC	workstation
ACC	workstation
ACC	workstation
ACC	workstation
ACC	workstation
ACC	workstation
ACC	workstation

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR



New Hunt - Configure Hunt

Description

Triage Compromised Systems

Expiry

7/21/2021 7:57 PM X [calendar icon]

Include Condition

Match by label

Include Labels

compromised

Exclude Condition

Search

☐ Select All

☐ server

☐ workstation

☒ compromised

☐ it

Configure Hunt

Select Artifacts

Configure Parameters

Specify Resources

Review

Launch

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR



Create Hunt: Select artifacts to collect

KAPE

Windows.KapeFiles.Targets

Windows.KapeFiles.Targets

Type: client

Kape is a popular bulk collector tool for triaging a system quickly. While KAPE itself is not an opensource tool, the logic it uses to decide which files to collect is encoded in YAML files hosted on the KapeFiles project (<https://github.com/EricZimmerman/KapeFiles>) and released under an MIT license.

This artifact is automatically generated from these YAML files, contributed and maintained by the community. This artifact only encapsulates the KAPE "Targets" - basically a bunch of glob expressions used for collecting files on the endpoint. We do not do any post processing these files - we just collect them.

We recommend that timeouts and upload limits be used conservatively with this artifact because we can upload really vast quantities of data very quickly.

Parameters

Name	Type	Default	Description
UseAutoAccessor	bool	Y	Uses file ac instead of r faster.
Device		C:	Name of the

Configure Hunt

Select Artifacts

Configure Parameters

Specify Resources

Review

Launch

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR



Create Hunt: Configure artifact parameters



-	Artifact
-	Windows.KapeFiles.Targets
	UseAutoAccessor <input checked="" type="checkbox"/> Uses file accessor when possible instead of ntfs parser - this is much faster.
	Device <input type="text" value="C:"/>
→	VSSAnalysis <input checked="" type="checkbox"/> If set we run the collection across all VSS and collect only unique changes.
	_BasicCollection <input type="checkbox"/> Basic Collection (by Phill Moore): Thumbcache DB, at .job, at .job, at SchedLgU.txt, at SchedLgU.txt, XML, XML, LNK Files from Recent, LNK Files from Microsoft Office Recent, LNK Files from Recent (XP), Desktop LNK Files XP, Desktop LNK Files, Restore point LNK Files XP, LNK Files from C:\ProgramData, Amcache, Amcache, Amcache transaction files, Amcache transaction files, \$SDS, WindowsIndexSearch, \$LogFile, \$Boot, NTUSER.DAT registry hive XP, NTUSER.DAT registry hive, NTUSER.DAT registry transaction files, NTUSER.DAT DEFAULT registry hive, NTUSER.DAT DEFAULT registry hive, NTUSER.DAT DEFAULT transaction files, NTUSER.DAT DEFAULT transaction files, UsrClass.dat registry hive, UsrClass.dat registry transaction files, PowerShell Console Log, RecentFileCache, RecentFileCache, \$MFT, \$Recycle.Bin, RECYCLER WinXP, SRUM, SRUM, \$J, \$Max, Setupapi.log XP, Setupapi.log Win7+, Setupapi.log Win7+, Prefetch, Prefetch, Syscache, Syscache transaction files, Event logs XP, Event logs Win7+, Event logs Win7+, SAM registry transaction files, SAM registry transaction files, SECURITY registry transaction files, SECURITY registry transaction files, SOFTWARE registry transaction files, SOFTWARE registry transaction files, SYSTEM registry transaction files, SYSTEM registry transaction files, SAM registry hive, SAM registry hive, SECURITY registry hive, SECURITY registry hive, SOFTWARE registry hive, SOFTWARE registry hive, SYSTEM registry hive, SYSTEM registry hive.
Configure Hunt Select Artifacts Configure Parameters Specify Resources Review Launch	

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR



Create Hunt: Configure artifact parameters

_SANS_Triage

☒ SANS Triage Collection. (by Mark Hallman): Event logs XP, Event logs Win7+, Event logs Win7+, Prefetch, Prefetch, RecentFileCache, RecentFileCache, Amcache, Amcache, Amcache transaction files, Amcache transaction files, Syscache, Syscache transaction files, PowerShell Console Log, \$MFT, \$LogFile, \$J, \$Max, \$SDS, \$Boot, \$T, LNK files from Recent, LNK files from Microsoft Office Recent, LNK files from Recent (XP), Desktop LNK files XP, Desktop LNK files, Restore point LNK files XP, \$Recycle.Bin, RECYCLER WinXP, SAM registry transaction files, SAM registry transaction files, SECURITY registry transaction files, SECURITY registry transaction files, SOFTWARE registry transaction files, SOFTWARE registry transaction files, SYSTEM registry transaction files, SYSTEM registry transaction files, SAM registry hive, SAM registry hive, SECURITY registry hive, SECURITY registry hive, SOFTWARE registry hive, SOFTWARE registry hive, SYSTEM registry hive, SYSTEM registry hive, RegBack registry transaction files, RegBack registry transaction files, SAM registry hive (RegBack), SAM registry hive (RegBack), SECURITY registry hive (RegBack), SECURITY registry hive (RegBack), SOFTWARE registry hive (RegBack), SOFTWARE registry hive (RegBack), SYSTEM registry hive (RegBack), SYSTEM registry hive (RegBack), SYSTEM registry hive (RegBack), SYSTEM registry hive (RegBack), System Profile registry hive, System Profile registry hive, System Profile registry transaction files, System Profile registry transaction files, Local Service registry hive, Local Service registry hive, Local Service registry transaction files, Local Service registry transaction files, Network Service registry hive, Network Service registry hive, Network Service registry transaction files, Network Service registry transaction files, System Restore Points Registry Hives (XP), NTUSER.DAT registry hive XP, NTUSER.DAT registry hive, NTUSER.DAT registry transaction files, NTUSER.DAT DEFAULT registry hive, NTUSER.DAT DEFAULT registry hive, NTUSER.DAT DEFAULT transaction files, NTUSER.DAT DEFAULT transaction files, UsrClass.dat registry hive, UsrClass.dat registry transaction files, at .job, at .job, at SchedLgU.txt, at SchedLgU.txt, XML, XML, SRUM, SRUM, Thumbcache DB, Setupapi.log XP, Setupapi.log Win7+, Setupapi.log Win7+, WindowsIndexSearch, WBEM, WBEM, PST XP, OST XP, PST, OST, main.db (App <v12), skype.db (App +v12), main.db XP, main.db

[Configure Hunt](#)[Select Artifacts](#)[Configure Parameters](#)[Specify Resources](#)[Review](#)[Launch](#)

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR



Create Hunt: Configure artifact parameters

- windowsYourPhone** ☐ windows Your Phone (by Andrew Rathbun): windows Your Phone - All Databases
- XPRestorePoints** ☐ XP Restore Points - System Volume Information directory (by Phill Moore): System Volume Information
- XYplorer** ☐ XYplorer (by Andrew Rathbun): XYplorer - .ini file, XYplorer - .ini file for each respective pane, XYplorer - AutoBackup folder, XYplorer - .dat files
- iTunesBackup** ☐ iTunes Backups (by Tony Knutson): iTunes Backup Folder, iTunes Backup Folder, iTunes Backup Folder - iOS13
- mIRC** ☐ mIRC (by Andrew Rathbun): mIRC Chat Logs
- openSUSE** ☐ openSUSE on Windows Subsystem for Linux (by Matt Dawson): openSUSE WSL /etc/os-release, openSUSE WSL /etc/fstab, openSUSE WSL /etc/passwd, openSUSE WSL /etc/group, openSUSE WSL /etc/shadow, openSUSE WSL /etc/timezone, openSUSE WSL /etc/hostname, openSUSE WSL /etc/hosts, openSUSE WSL /etc/bash.bashrc, openSUSE WSL /etc/profile, openSUSE WSL .bash_history, openSUSE WSL .bashrc, openSUSE WSL .profile
- qBittorrent** ☐ qBittorrent (by Banaanhangwagen): TorrentClients - qBittorrent, TorrentClients - qBittorrent
- uTorrent** ☐ uTorrent (by Banaanhangwagen): TorrentClients - uTorrent
- DontBeLazy** ☒ Normally we prefer to use lazy_ntfs for speed. Sometimes this might miss stuff so setting this will fallback to the regular ntfs accessor.

Configure Hunt

Select Artifacts

Configure Parameters

Specify Resources

Review

Launch

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR



Create Hunt: Specify resource limits

Ops/Sec

Unlimited

Max Execution Time in Seconds

999999

Max Rows

1,000,000 rows

Max Mb Uploaded

1Gb

Configure Hunt

Select Artifacts

Configure Parameters

Specify Resources

Review

Launch

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR



Create Hunt: Review request

```
1 {
2   "start_request": {
3     "artifacts": [
4       "Windows.KapeFiles.Targets"
5     ],
6     "specs": [
7       {
8         "artifact": "Windows.KapeFiles.Targets",
9         "parameters": {
10           "env": [
11             {
12               "key": "_SANS_Triage",
13               "value": "Y"
14             },
15             {
16               "key": "DontBelazy",
17               "value": "Y"
18             },
19             {
20               "key": "VSSAnalysis",
21               "value": "Y"
22             }
23           ]
24         }
25       }
26     ],
27     "timeout": 999999
28   },
29   "condition": {
30     "labels": {
31       "label": [
32         "compromised"
33       ]
34     }
35   },
36   "expires": 1626915471150000,
37   "hunt_description": "Triage Compromised Systems"
38 }
```

[Configure Hunt](#)[Select Artifacts](#)[Configure Parameters](#)[Specify Resources](#)[Review](#)[Launch](#)

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR



Search clients

admin

State	Hunt ID	Description	Created	Started	Expires	Limit	Scheduled	Creator
🔍	H.C3NP48LO0AHP2	Triage Compromised Systems	2021-07-15 01:40:50 UTC	2021-07-15 01:41:03 UTC	2021-07-22 01:39:57 UTC	3		admin

Overview Requests Clients Notebook

Overview

Artifact Names Windows.KapeFiles.Targets
Hunt ID H.C3NP48LO0AHP2
Creator admin
Creation Time 2021-07-15 01:40:50 UTC
Expiry Time 2021-07-22 01:39:57 UTC
State RUNNING
Ops/Sec Unlimited
Include Labels compromised

Parameters
Windows.KapeFiles.Targets
VSSAnalysis Y
_SANS_Triage Y
DontBeLazy Y

Results

Total scheduled 3
Finished clients 3
Download Results

Available Downloads

name	size	date
------	------	------

2021-07-15T01:42:29.205Z

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR



Search clients admin

State Hunt ID Description Created Started Expires Limit Scheduled Creator

H.C3NP48LO0AHP2	Triage Compromised Systems	2021-07-15 01:40:50 UTC	2021-07-15 01:41:03 UTC	2021-07-22 01:39:57 UTC	3		admin
-----------------	----------------------------	-------------------------	-------------------------	-------------------------	---	--	-------

Overview Requests Clients Notebook

Overview

Artifact Names Windows.KapeFiles.Targets

Hunt ID H.C3NP48LO0AHP2

Creator admin

Creation Time 2021-07-15 01:40:50 UTC

Expiry Time 2021-07-22 01:39:57 UTC

State RUNNING

Ops/Sec Unlimited

Include Labels compromised

Parameters

Windows.KapeFiles.Targets

VSSAnalysis Y

_SANS_Triage Y

DontBeLazy Y

Results

Total scheduled 3

Finished clients 3

Download Results

Available Downloads

name

- Full Download
- Summary Download
- Summary (CSV Only)
- Summary (JSON Only)

PLASO

- ⦿ Forensic processing powerhouse

- “Super timeline all the things”
- Processes various raw forensic artifacts into universal format timelines



<https://github.com/log2timeline/plaso>

PLASO

- ★ Memory image artifacts
- ★ Evidence of Execution
- ★ File System Metadata
- ★ Registry Hives
 - ★ Event Logs
 - ★ & more...



2021-06-15T21:00:13	<input type="checkbox"/> ★ 🔍 📁	Location: :2021061520210616: Joella.Cerda@file:///C:/Users/Joella.Cerda/AppData/Local/Temp/%7B36BEC576-071D-475A-82C5-5BA512B900DB%7D.html Number of hits: 1 Cached file size:...	SAL-05
2021-06-15T21:00:13	<input type="checkbox"/> ★ 🔍 📁	Location: Visited: Joella.Cerda@file:///C:/Users/Joella.Cerda/AppData/Local/Temp/%7B36BEC576-071D-475A-82C5-5BA512B900DB%7D.html Number of hits: 1 Cached file size: 0 HTTP head...	SAL-05
2021-06-15T21:00:07	<input type="checkbox"/> ★ 🔍 📁	Prefetch [EXPLORE.EXE] was executed - run count 29 path hints: \PROGRAM FILES (X86)\INTERNET EXPLORER\EXPLORE.EXE hash: 0xF6A52C86 volume: 1 [serial number: 0xEA90BF...	SAL-05
2021-06-15T20:48:21	<input type="checkbox"/> ★ 🔍 📁	[4688 / 0x1250] Source Name: Microsoft-Windows-Security-Auditing Message string: A new process has been created.\n\nSubject:\n\nSecurity ID:\t\tS-1-5-18\n\nAccount Name:\t\tSAL-05\n\nAc...	SAL-05
2021-06-15T20:48:21	<input type="checkbox"/> ★ 🔍 📁	[4688 / 0x1250] Source Name: Microsoft-Windows-Security-Auditing Message string: A new process has been created.\n\nSubject:\n\nSecurity ID:\t\tS-1-5-18\n\nAccount Name:\t\tSAL-05\n\nAc...	SAL-05
2021-06-15T20:46:50	<input type="checkbox"/> ★ 🔍 📁	[4688 / 0x1250] Source Name: Microsoft-Windows-Security-Auditing Message string: A new process has been created.\n\nSubject:\n\nSecurity ID:\t\tS-1-5-18\n\nAccount Name:\t\tSAL-05\n\nAc...	SAL-05
2021-06-15T20:46:50	<input type="checkbox"/> ★ 🔍 📁	[4688 / 0x1250] Source Name: Microsoft-Windows-Security-Auditing Message string: A new process has been created.\n\nSubject:\n\nSecurity ID:\t\tS-1-5-18\n\nAccount Name:\t\tSAL-05\n\nAc...	SAL-05
2021-06-15T20:46:46	<input type="checkbox"/> ★ 🔍 📁	Prefetch [POWERSHELL.EXE] was executed - run count 6 path hints: \WINDOWS\SYSWOW64\WINDOWSPOWERSHELL\1.0\POWERSHELL.EXE hash: 0x3E7086C1 volume: 1 [serial nu...	SAL-05
2021-06-15T20:46:46	<input type="checkbox"/> ★ 🔍 📁	Prefetch [CMD.EXE] was executed - run count 6 path hints: \WINDOWS\SYSWOW64\CMD.EXE hash: 0xEABFE48B volume: 1 [serial number: 0xEA90BFAF, device path: \DEVICE\HARDDIS...	SAL-05

TIMESKETCH

- ⦿ Collaborative Timeline Analysis
 - Elasticsearch based
 - View many timelines simultaneously
 - Collaborate & annotate
 - Generate node diagrams

TIMESKETCH

timesketch Szechuan Sauce - Challenge

Dark Mode demo Logout

Overview Explore Graph Aggregate Analyze Timelines Stories

Search

+ Time filter + Add label filter

2019-01-07T19:40:08 -- 2019-01-11T16:09:08

decoded_pcap 0 autoruns_dc01 0 autoruns_desktop 0 dc1_plaso 2 network_pcap_with_scapy 0 desktop_plaso 6

Enable all Disable all

8 events (0.011s)

1-8 / 8 40 asc Customize columns Export to CSV

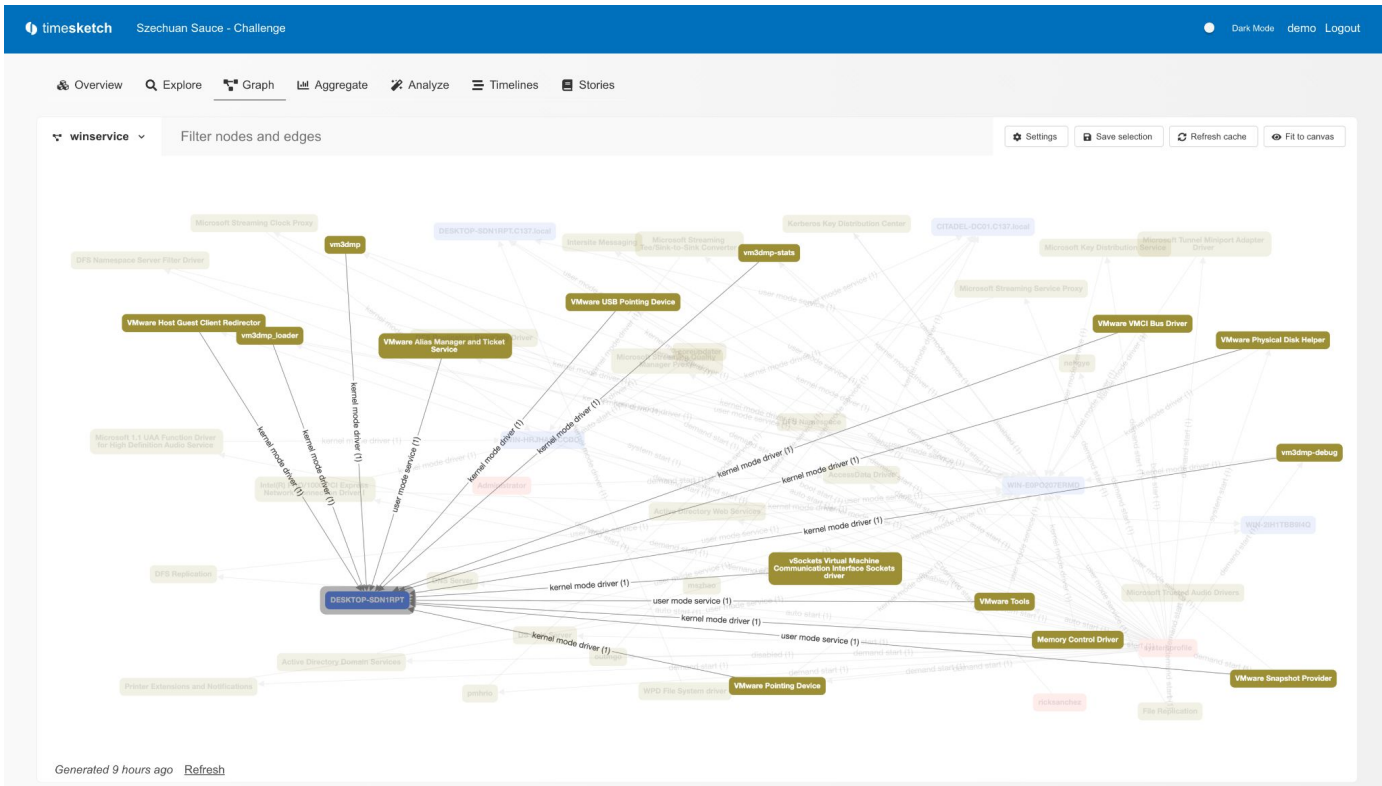
Datetime (UTC)		Message	Timeline name
2019-01-07T19:40:08	<input type="checkbox"/> <input type="star"/> <input type="search"/>	PE Type: Dynamic Link Library (DLL)	desktop_plaso
2019-01-07T19:40:08	<input type="checkbox"/> <input type="star"/> <input type="search"/>	PE Type: Dynamic Link Library (DLL)	desktop_plaso
2019-01-07T19:40:15	<input type="checkbox"/> <input type="star"/> <input type="search"/>	PE Type: Dynamic Link Library (DLL) Import hash: acc791587ca18c44caf56eacde7e2dfb	desktop_plaso
2019-01-07T19:40:15	<input type="checkbox"/> <input type="star"/> <input type="search"/>	PE Type: Dynamic Link Library (DLL) Import hash: acc791587ca18c44caf56eacde7e2dfb	desktop_plaso
3 days			
2019-01-11T16:09:03	<input type="checkbox"/> <input type="star"/> <input type="search"/>	PE Type: Dynamic Link Library (DLL) Import hash: 400c0117a378c0802ce0b856d6eea4c1	desktop_plaso
2019-01-11T16:09:03	<input type="checkbox"/> <input checked="" type="star"/> <input type="search"/>	PE Type: Dynamic Link Library (DLL) Import hash: 400c0117a378c0802ce0b856d6eea4c1	dc1_plaso
2019-01-11T16:09:08	<input type="checkbox"/> <input checked="" type="star"/> <input type="search"/>	PE Type: Dynamic Link Library (DLL) Import hash: 193f74108e5714e2d08f18bc21e491ef	desktop_plaso
2019-01-11T16:09:08	<input type="checkbox"/> <input type="star"/> <input type="search"/>	PE Type: Dynamic Link Library (DLL) Import hash: 193f74108e5714e2d08f18bc21e491ef	dc1_plaso

1-8 / 8 14

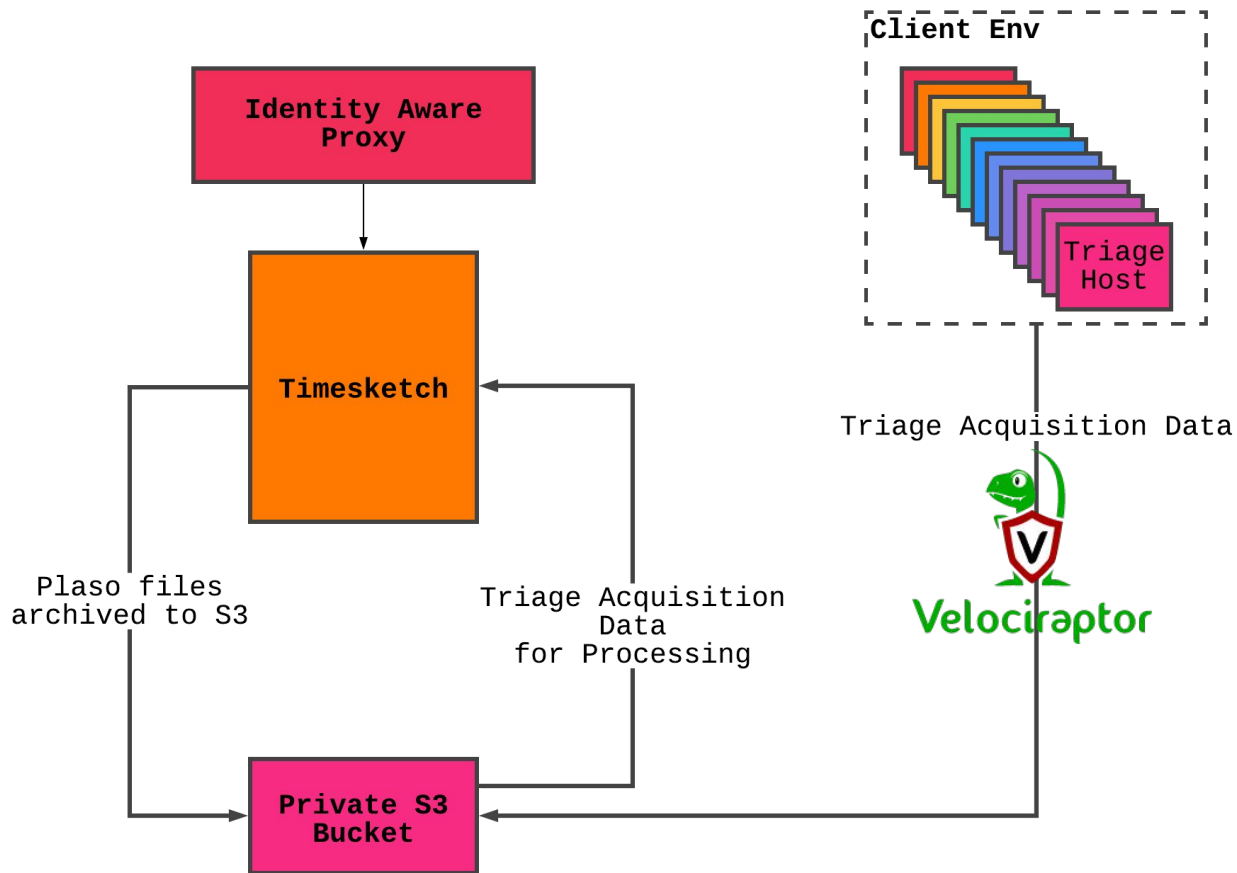
<https://github.com/google/timesketch>

SANS DFIRSummit - 2021

TIMESKETCH



BRINGING IT ALL TOGETHER



THE OPS MAGIC

FOUR COMPONENTS

- ⦿ Velociraptor artifact
- ⦿ watch-s3-to-timesketch.service
- ⦿ data-to-timesketch.service
- ⦿ watch-plaso-to-s3.service

COMPONENT #1



```
LET upload_to_s3(ClientId, FlowId, Fqdn) = SELECT ClientId,
    upload_s3(bucket=bucket,
        credentialskey=credentialskey,
        credentialssecret=credentialssecret,
        region=region,
        file=output_file,
        name=format(format="Host %v %v %v.zip",
            args=[Fqdn, FlowId, timestamp(epoch=now())])) AS S3
FROM collect(artifacts="UploadFlow", artifact_definitions=UploadFlowDefinition,
    args=dict(`UploadFlow`=dict(
        ClientId=ClientId, FlowId=FlowId)),
    output=output_file)

LET completions = SELECT *, client_info(client_id=ClientId).os_info.fqdn AS Fqdn
FROM watch_monitoring(artifact="System.Flow.Completion")
WHERE Flow.artifacts_with_results =~ ArtifactNameRegex

SELECT * FROM foreach(row=completions, query={
    SELECT * FROM upload_to_s3(ClientId=ClientId, FlowId=FlowId, Fqdn=Fqdn)
})
```

COMPONENT #1



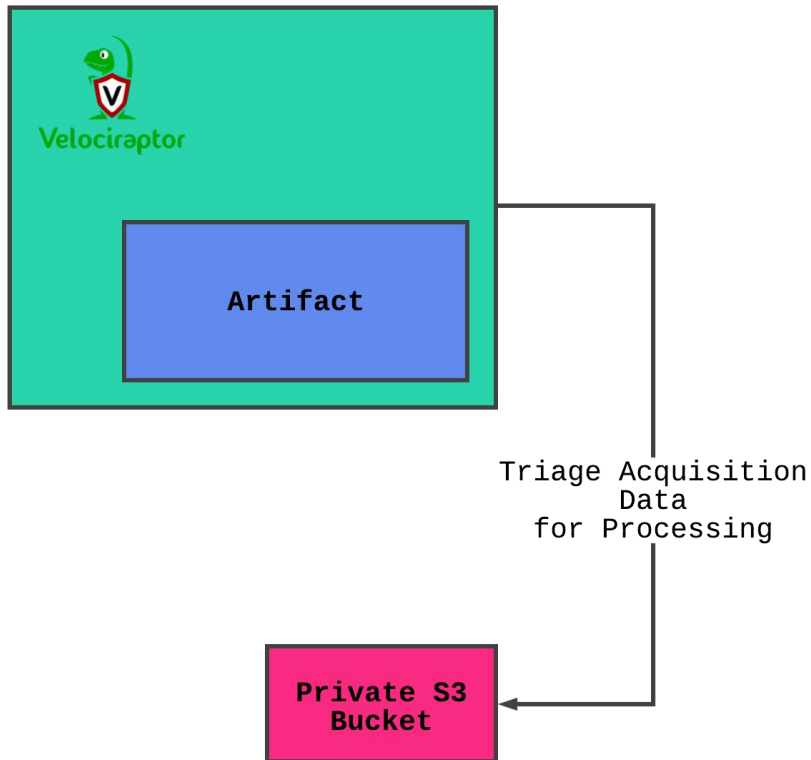
I HOPE YOU MEMORIZED ALL THAT!

- ⊙ J/K LOL
- ⊙ This will all be on GitHub for \$Free.99 <3

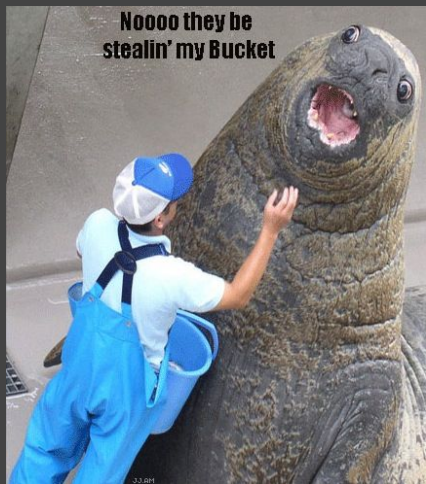
COMPONENT #1



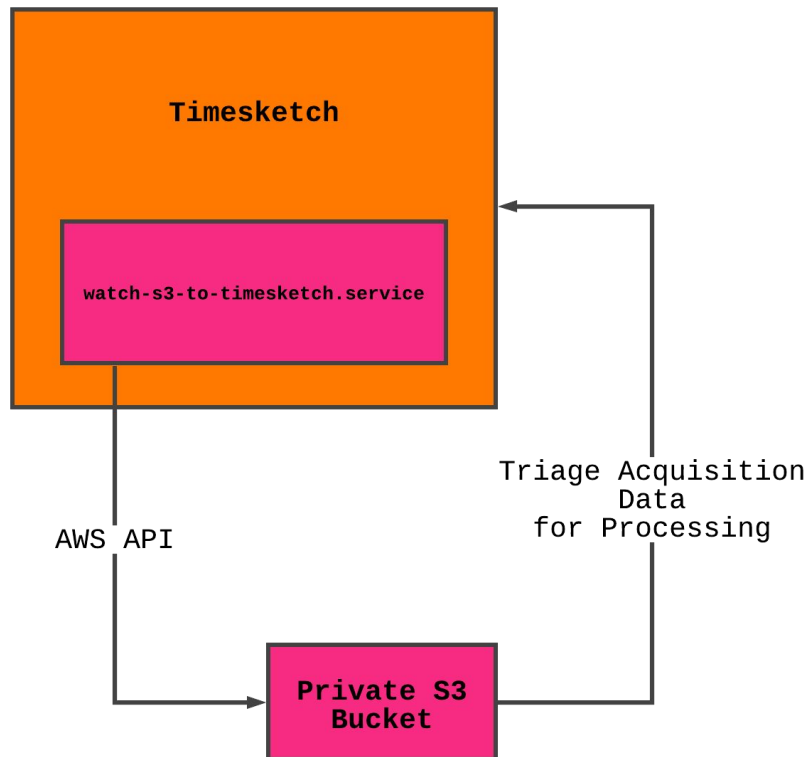
Artifact.Custom.Server.Utils.KAPEtoS3



COMPONENT #2

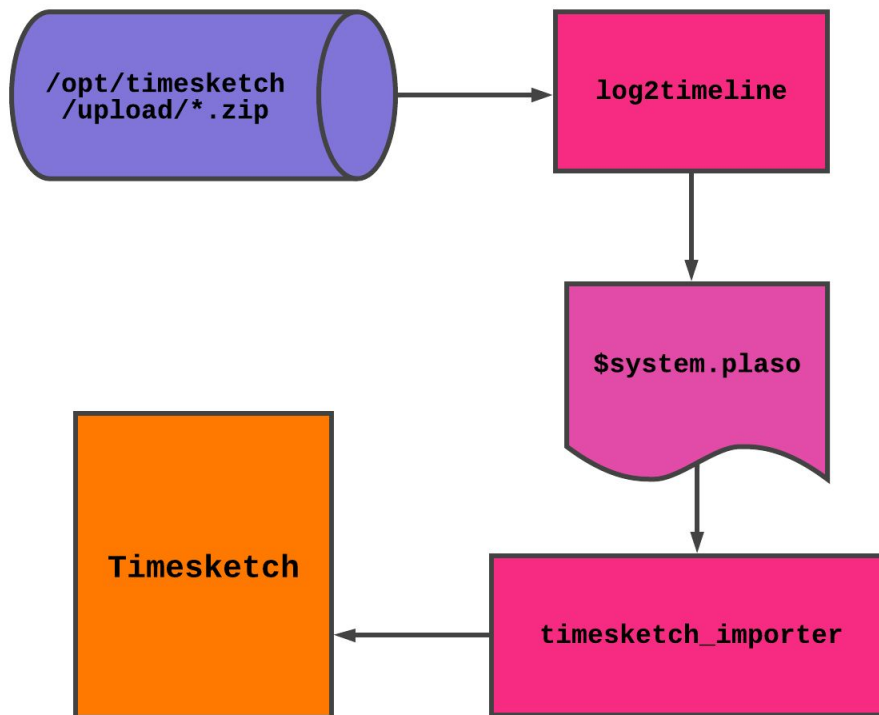


watch-s3-to-timesketch.service



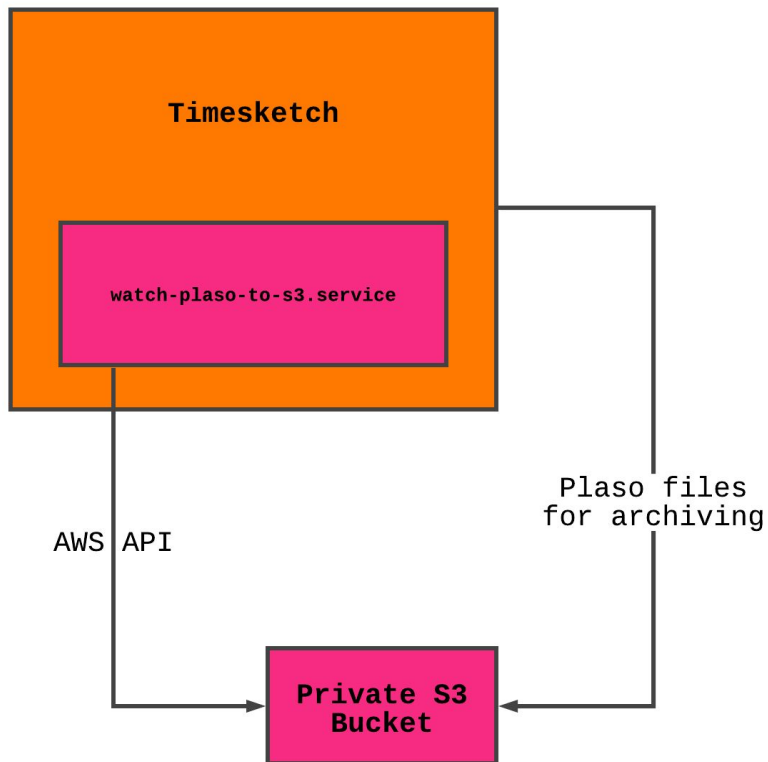
COMPONENT #3

data-to-timesketch.service



COMPONENT #4

watch-plaso-to-s3.service



WE
HAVE
DATA!

The screenshot displays the timesketch web interface. At the top, the header includes the 'timesketch' logo, the title 'hullo world, here is my datas', a 'Dark Mode' toggle, and user options for 'whitney' and 'Logout'. Below the header is a navigation bar with icons and labels for 'Overview', 'Explore', 'Graph', 'Aggregate', 'Analyze', 'Timelines', 'Stories', and 'Attributes' (showing 0). A 'Share' button and a 'More' dropdown are also present.

The main content area is divided into three sections:

- Timeline View:** A large white box containing the text 'hullo world, here is my datas'.
- Metadata:** A sidebar on the right showing 'Creator: whitney' and a summary table:

TIMELINES	VIEWS	STORIES	EVENTS
1	0	0	1.8M
- Timelines:** A section below the main view showing a single timeline entry: 'IT-11' with '1.8M events (imported with CLI importer tool)' and a timestamp of '2021-07-08 18:54'. It includes 'Upload timeline' and 'Manage' buttons.
- Get started!:** A sidebar on the right with a welcome message and a 'Begin to explore your data' button.

AS
PROMISED

THE GITHUBS

<https://github.com/ReconInfoSec/velociraptor-to-timesketch>

THANK YOU

- * reconinfosec.com
- * blog.reconinfosec.com
- * opensoc.io

Eric Capuano, @eric_capuano
Whitney Champion, @shortxstack

