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

RECON INFOSEC

WHAT DO WE DO?

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

RECON INFOSEC

IR IS HARD TO SCALE

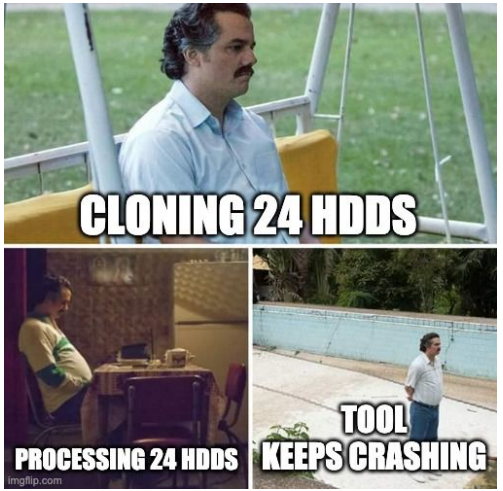
1. **Identify** compromised systems
   a. Without a SIEM? Good luck!
2. **Acquire** forensics images
   a. Many+ hours
3. **Process** forensic images
   a. Many+ hours *per* image
4. **Analyze** forensic data
   a. One!

      system!

      at!

      a!

      time!



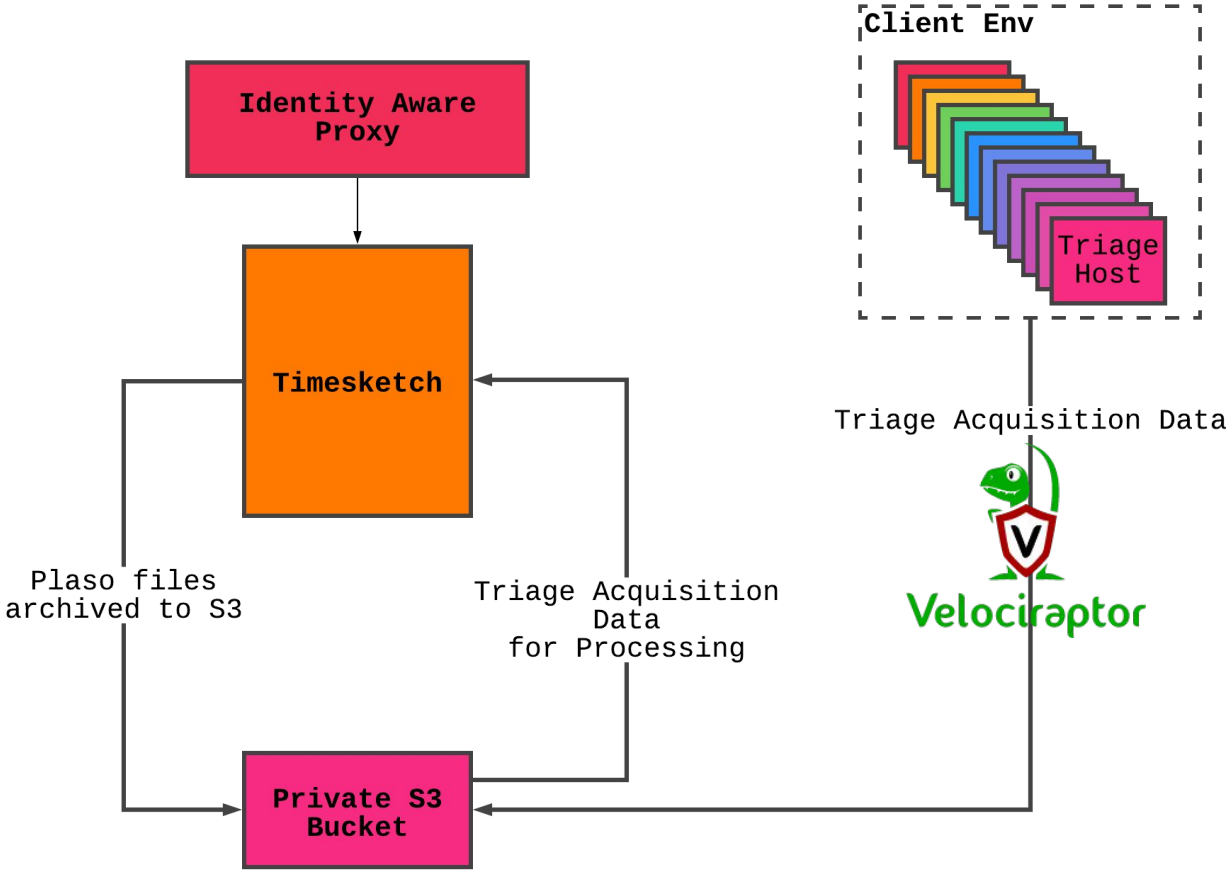
WHAT ARE WE DOING TODAY?

- IR at scale!

+ <magic>

==

WHAT THIS LOOKS LIKE



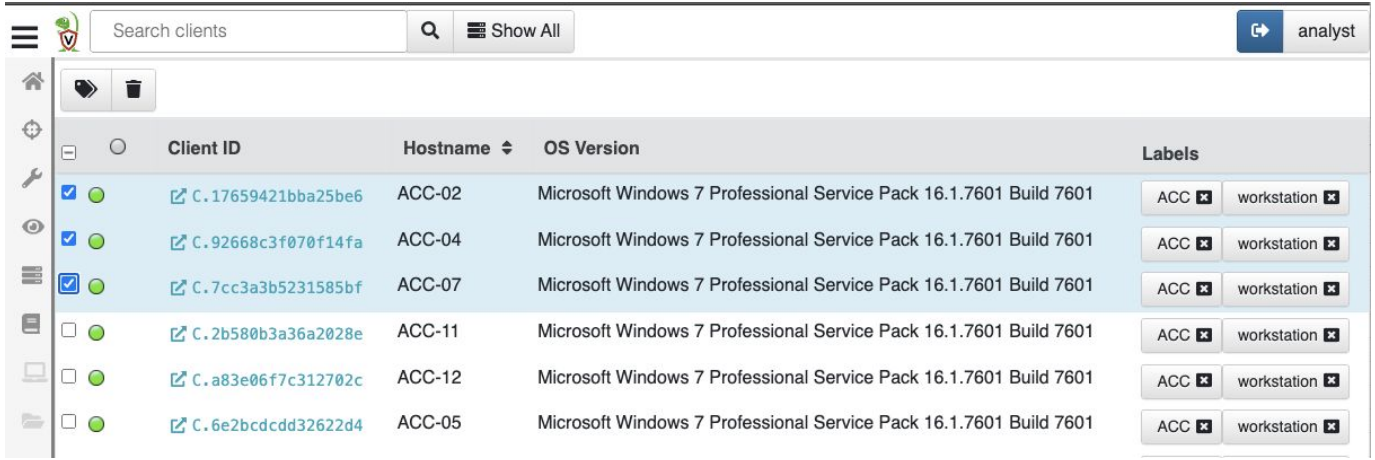
THE DFIR MAGIC

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...

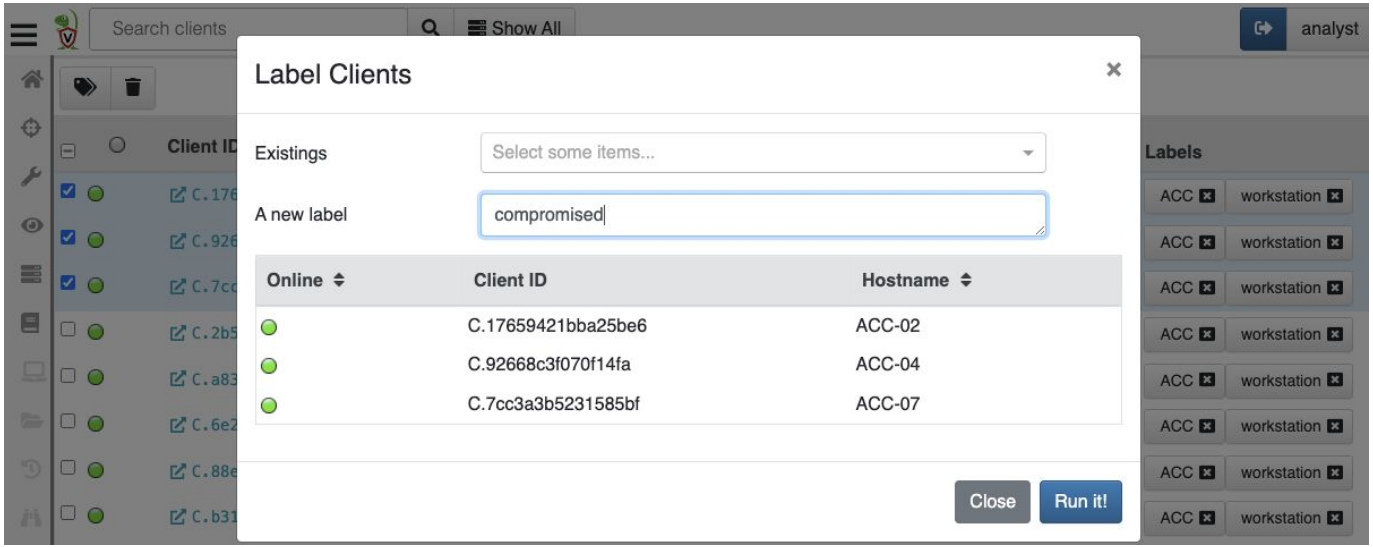
https://www.velocidex.com/

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR



TRIAGE ACQUISITIONS WITH VELOCIRAPTOR

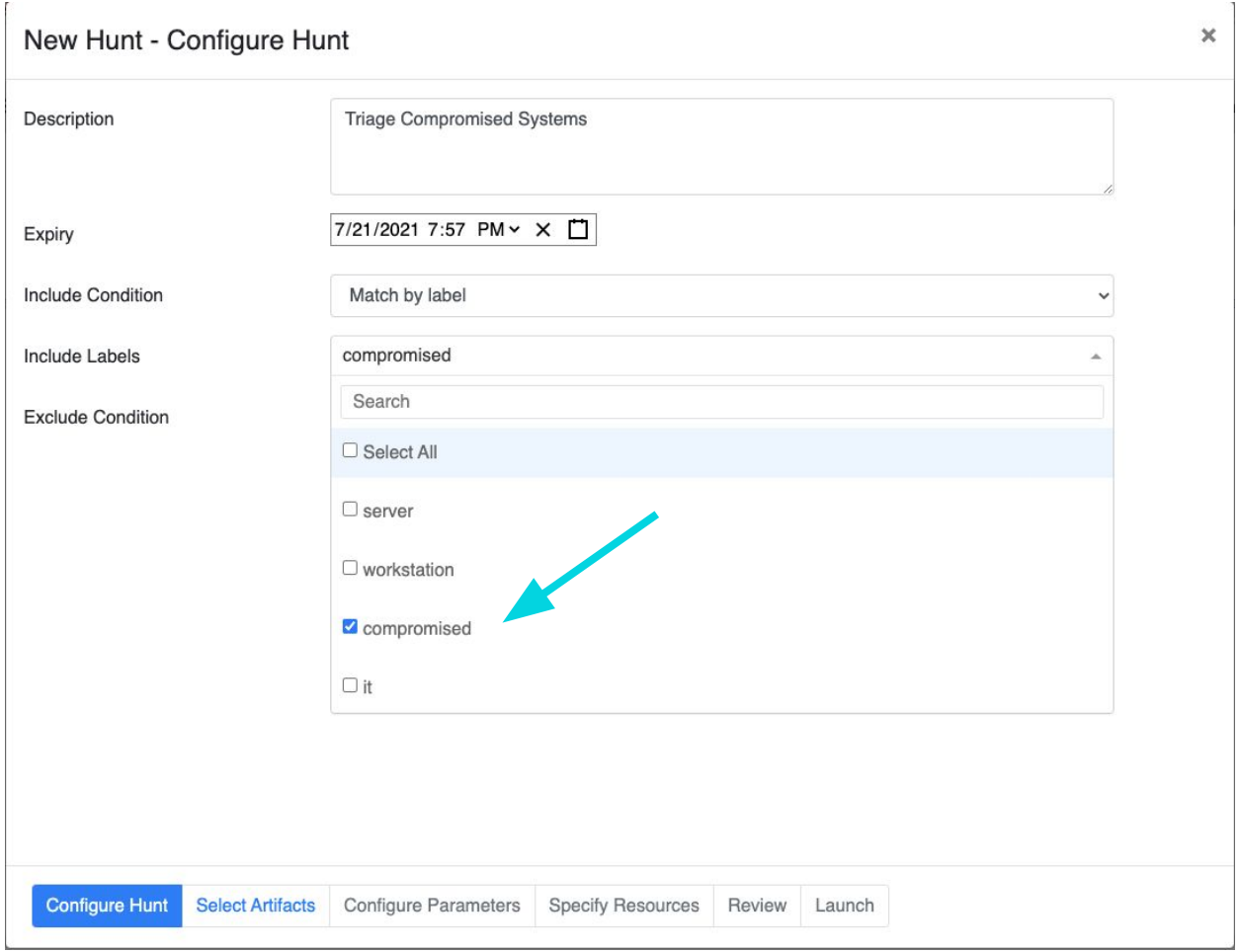
Velociraptor



RECON INFOSEC

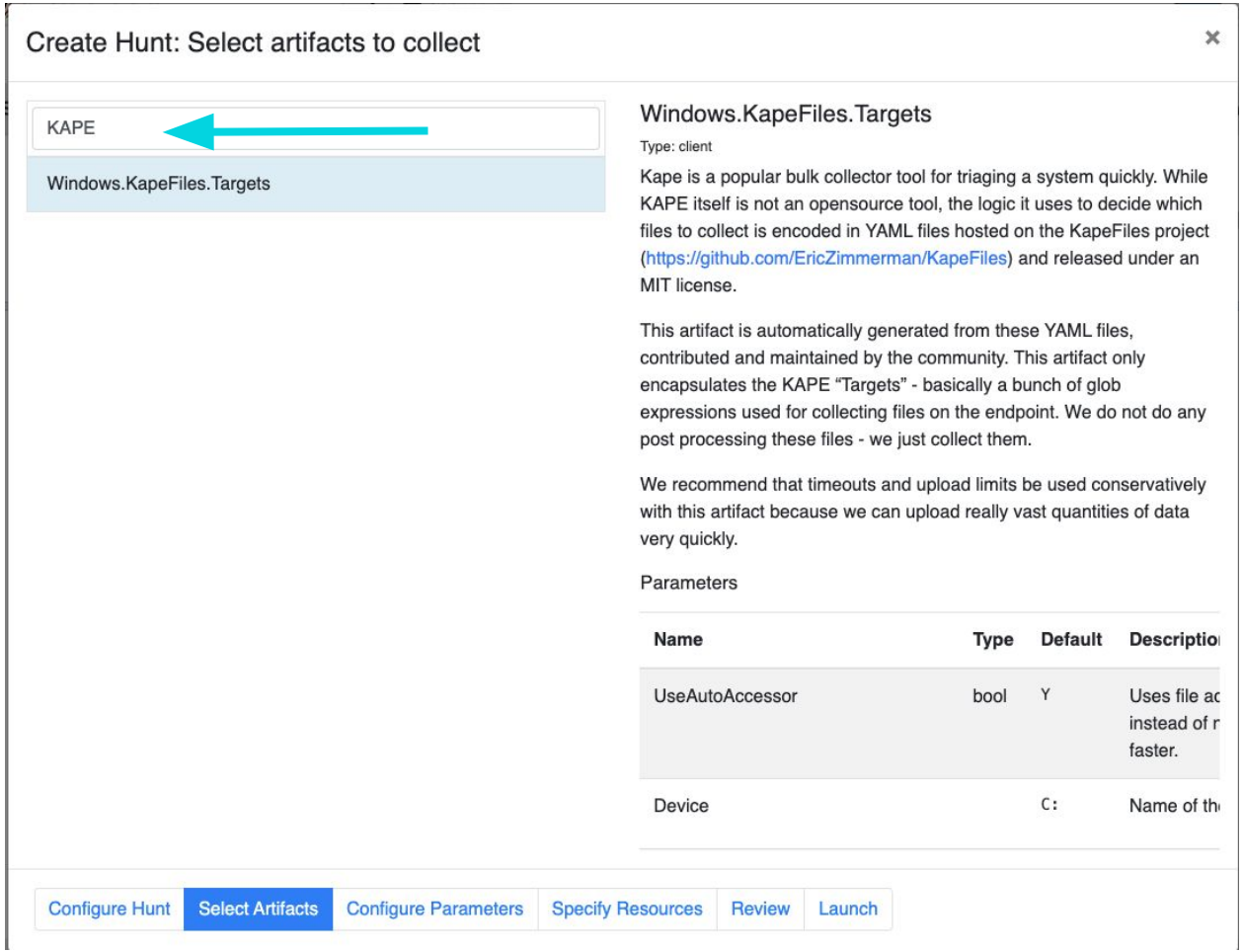
TRIAGE ACQUISITIONS WITH VELOCIRAPTOR

Velociraptor



TRIAGE ACQUISITIONS WITH VELOCIRAPTOR

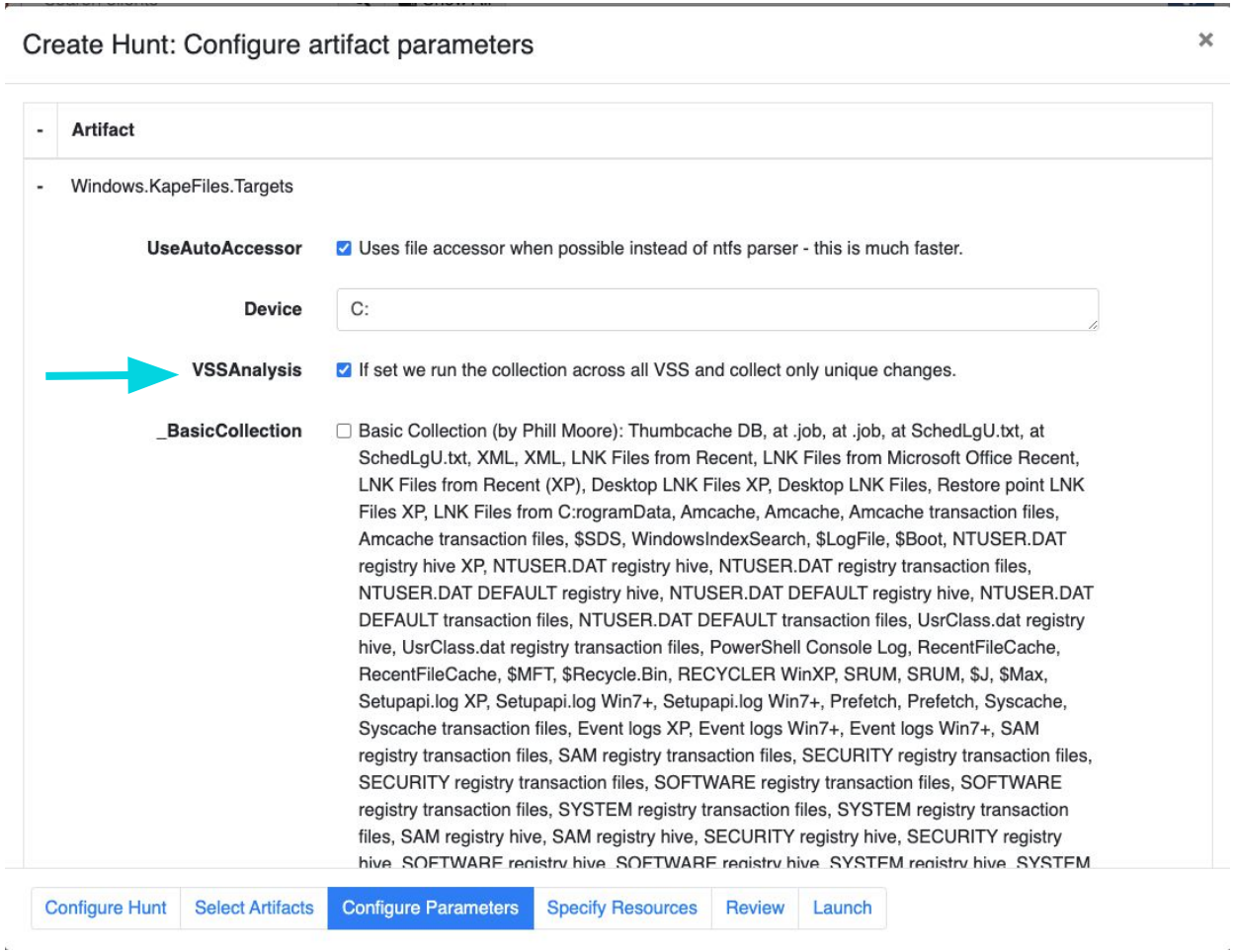
Velociraptor



https://github.com/EricZimmerman/KapeFiles

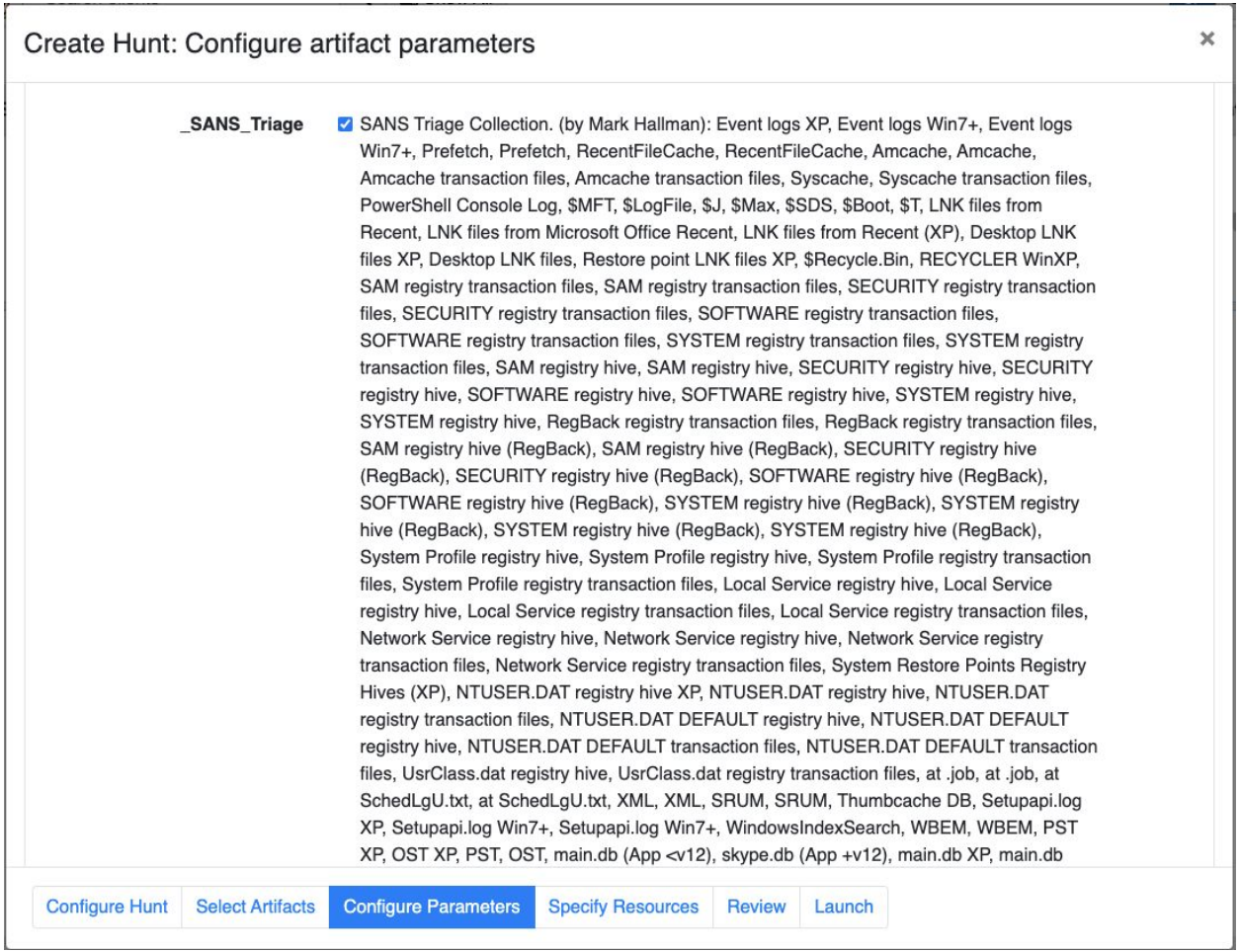
RECON INFOSEC

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR



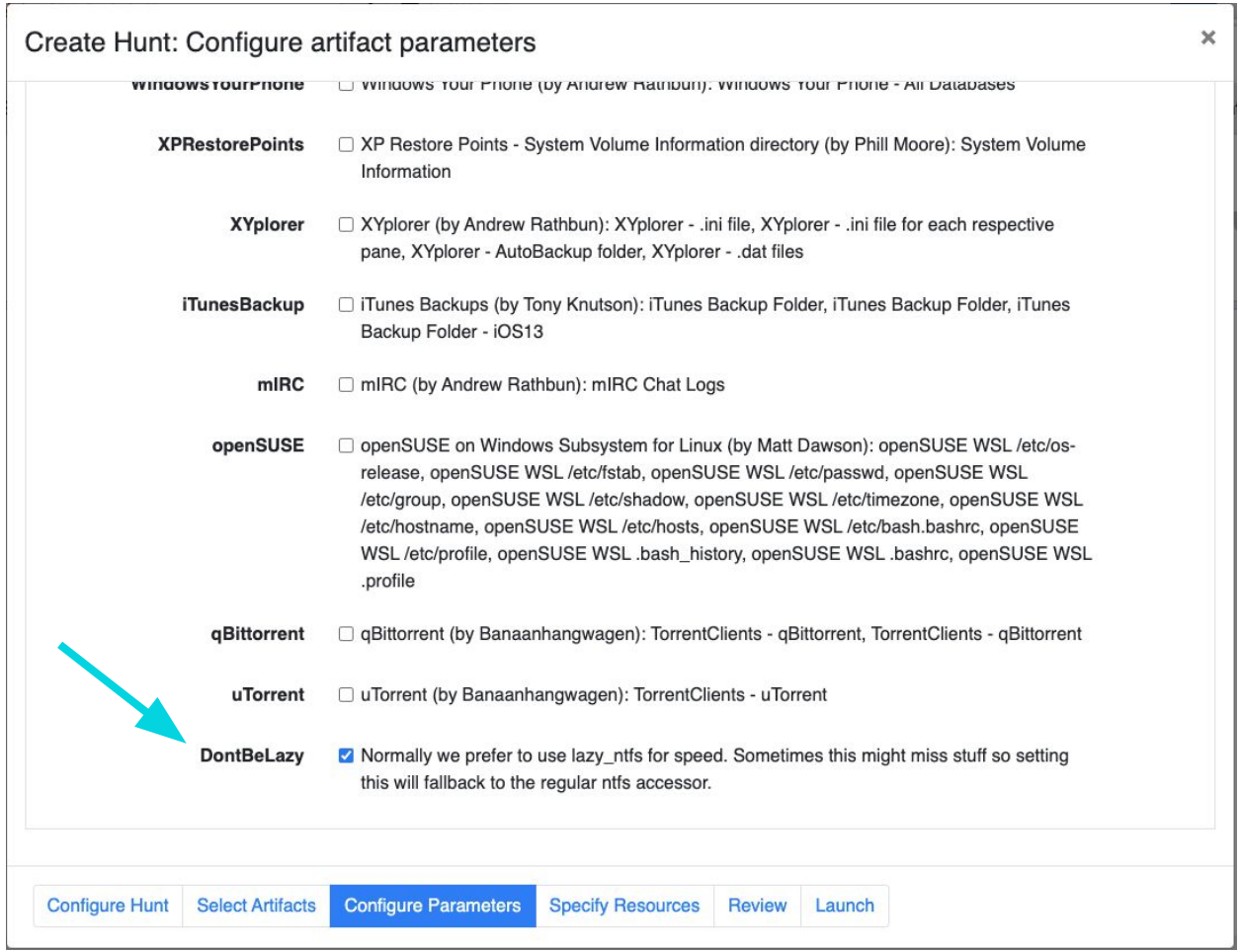
RECON INFOSEC

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR



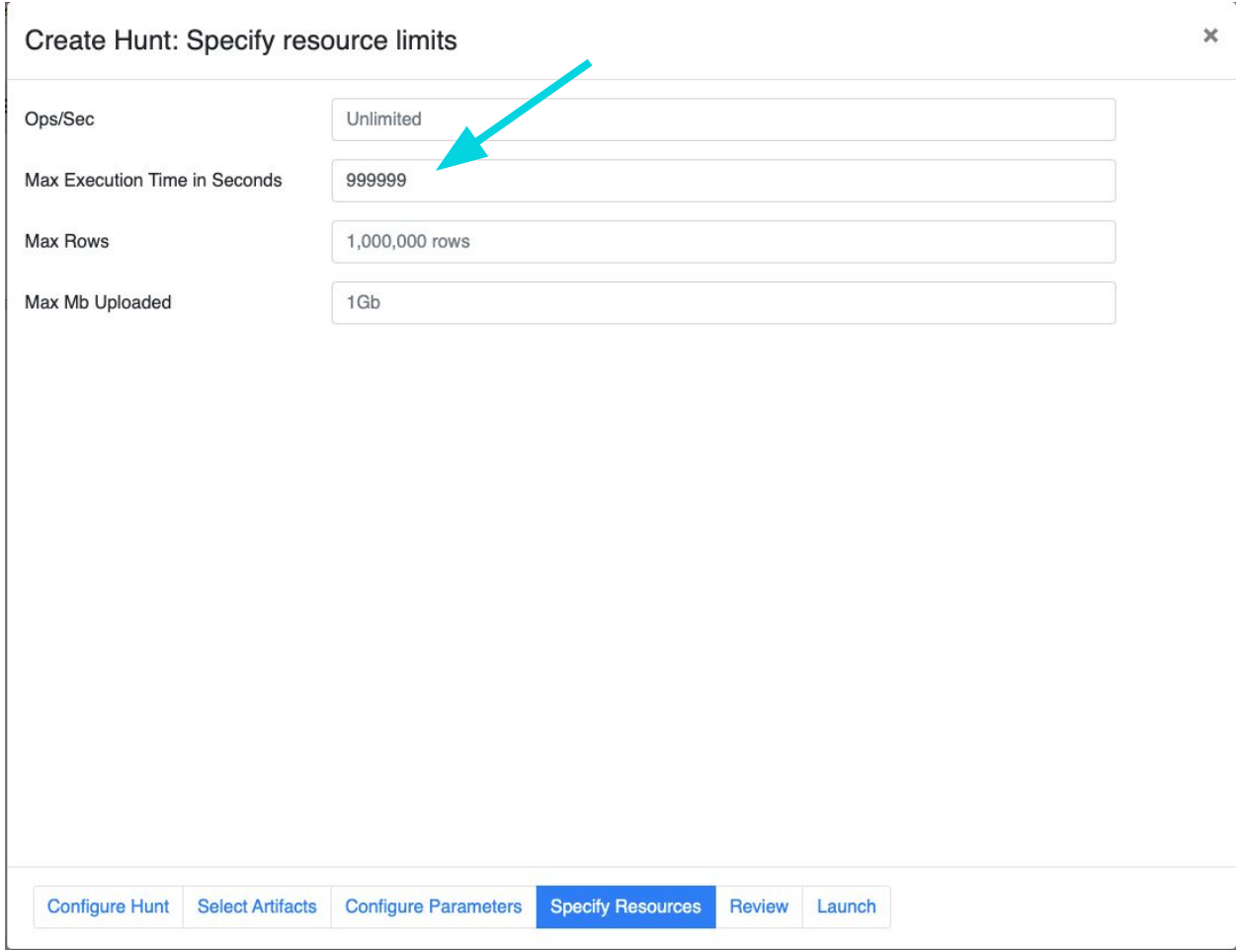
RECON INFOSEC

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR



RECON INFOSEC

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR



RECON INFOSEC

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR

Create Hunt: Review request

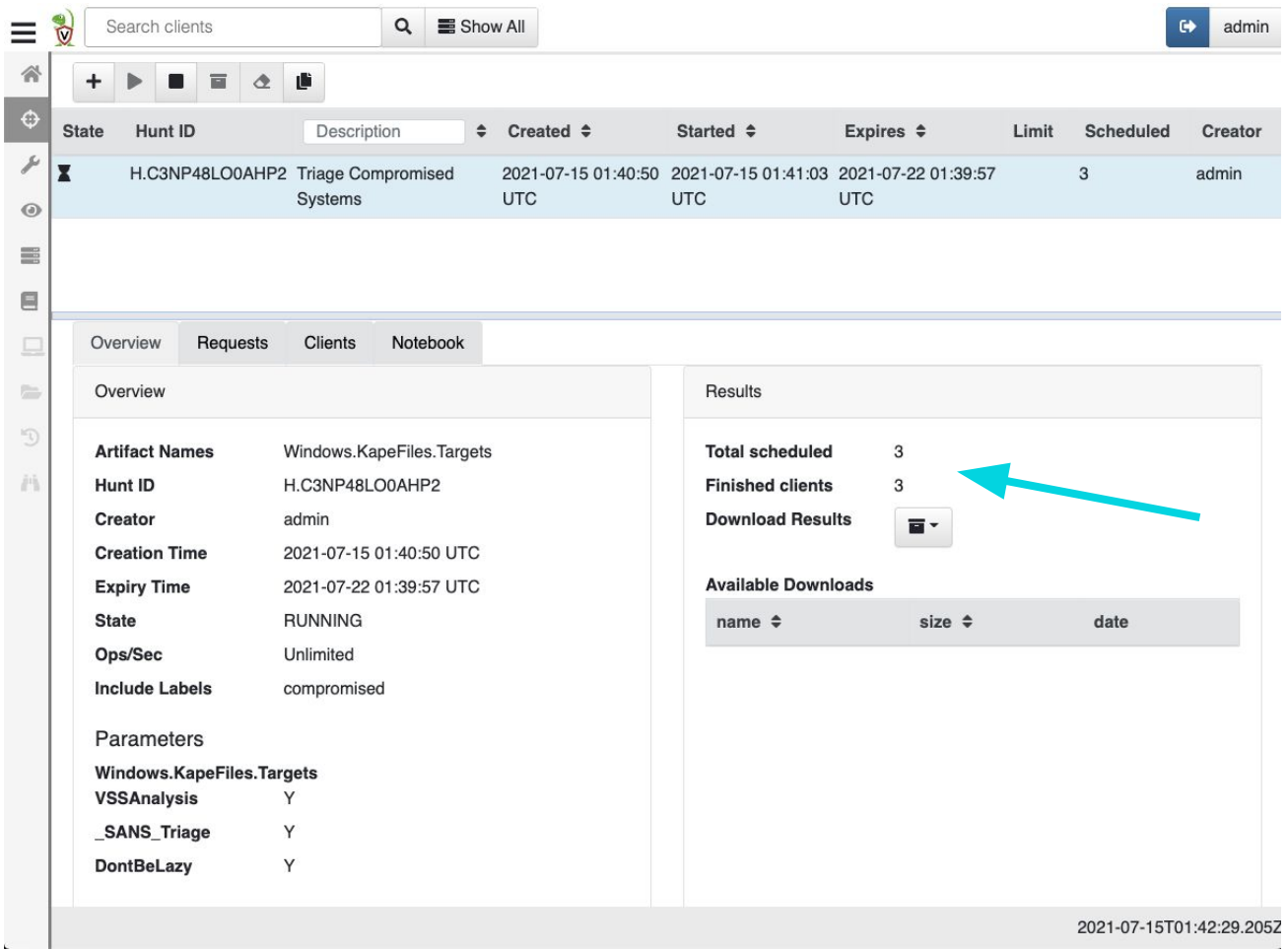
```
{
  "start_request": {
    "artifacts": [
      "Windows.KapeFiles.Targets"
    ],
    "specs": [
      {
        "artifact": "Windows.KapeFiles.Targets",
        "parameters": {
          "env": [
            {
              "key": "_SANS_Triage",
              "value": "Y"
            },
            {
              "key": "DontBeLazy",
              "value": "Y"
            },
            {
              "key": "VSSAnalysis",
              "value": "Y"
            }
          ]
        }
      }
    ],
    "timeout": 999999
  },
  "condition": {
    "labels": {
      "label": [
        "compromised"
      ]
    }
  },
  "expires": 1626915471150000,
  "hunt_description": "Triage Compromised Systems"
}
```

Configure Hunt | Select Artifacts | Configure Parameters | Specify Resources | Review | Launch

RECON INFOSEC

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR

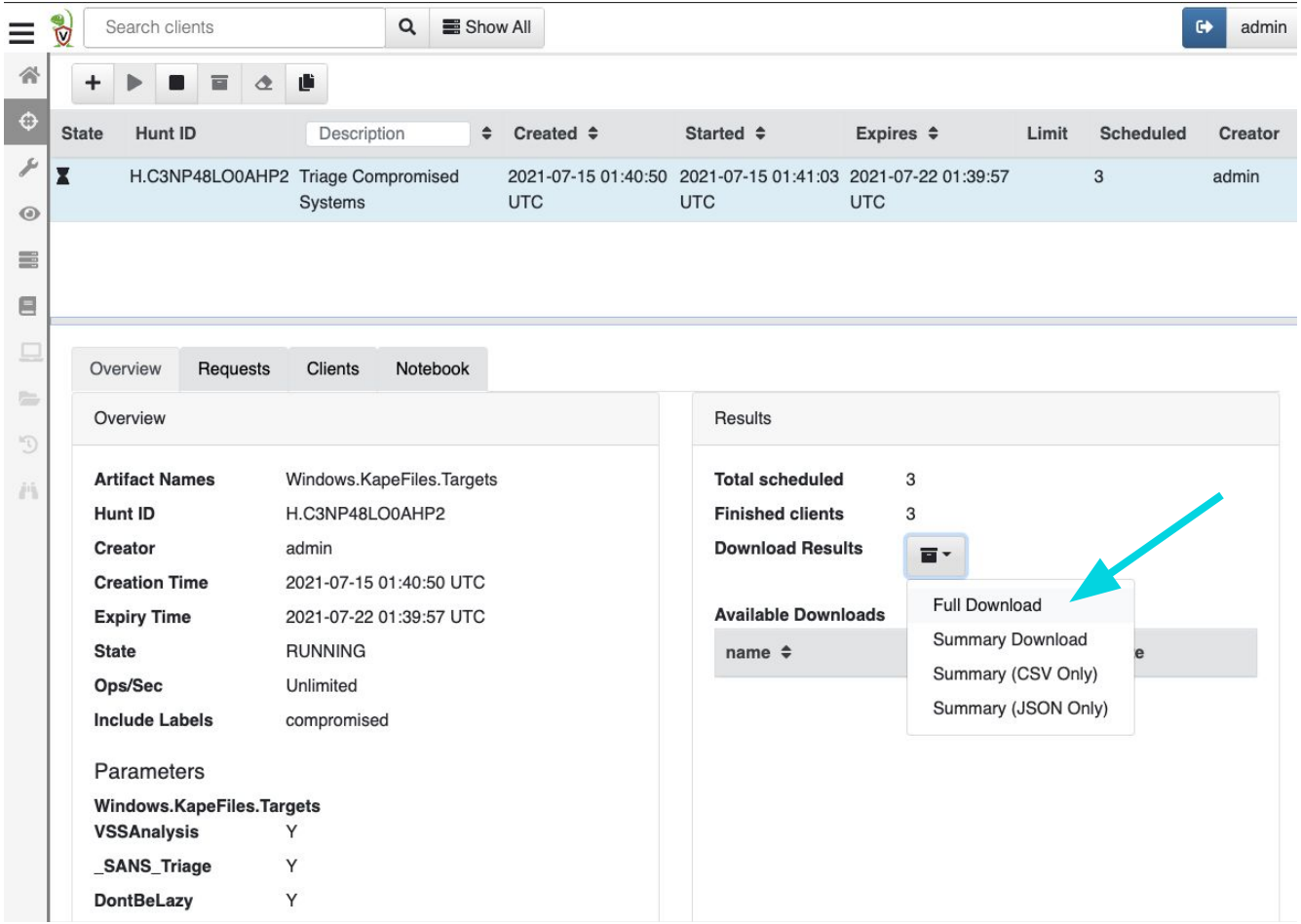
Velociraptor



RECON INFOSEC

TRIAGE ACQUISITIONS WITH VELOCIRAPTOR

Velociraptor



RECON INFOSEC

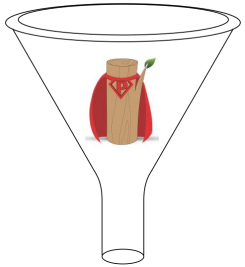
PLASO

- 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	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	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	Prefetch [IEXPLORE.EXE] was executed - run count 29 path hints: \PROGRAM FILES (X86)\INTERNET EXPLORER\IEXPLORE.EXE hash: 0xF6A52C86 volume: 1 [serial number: 0xEA90BF…	SAL-05
2021-06-15T20:48:21	[4688 / 0x1250] Source Name: Microsoft-Windows-Security-Auditing Message string: A new process has been created.\n\nSubject:\n\tSecurity ID:\t\tS-1-5-18\n\tAccount Name:\t\tSAL-05$\n\tAc…	SAL-05
2021-06-15T20:48:21	[4688 / 0x1250] Source Name: Microsoft-Windows-Security-Auditing Message string: A new process has been created.\n\nSubject:\n\tSecurity ID:\t\tS-1-5-18\n\tAccount Name:\t\tSAL-05$\n\tAc…	SAL-05
2021-06-15T20:46:50	[4688 / 0x1250] Source Name: Microsoft-Windows-Security-Auditing Message string: A new process has been created.\n\nSubject:\n\tSecurity ID:\t\tS-1-5-18\n\tAccount Name:\t\tSAL-05$\n\tAc…	SAL-05
2021-06-15T20:46:50	[4688 / 0x1250] Source Name: Microsoft-Windows-Security-Auditing Message string: A new process has been created.\n\nSubject:\n\tSecurity ID:\t\tS-1-5-18\n\tAccount Name:\t\tSAL-05$\n\tAc…	SAL-05
2021-06-15T20:46:46	Prefetch [POWERSHELL.EXE] was executed - run count 6 path hints: \WINDOWS\SYSWOW64\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE hash: 0x3E7086C1 volume: 1 [serial nu…	SAL-05
2021-06-15T20:46:46	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

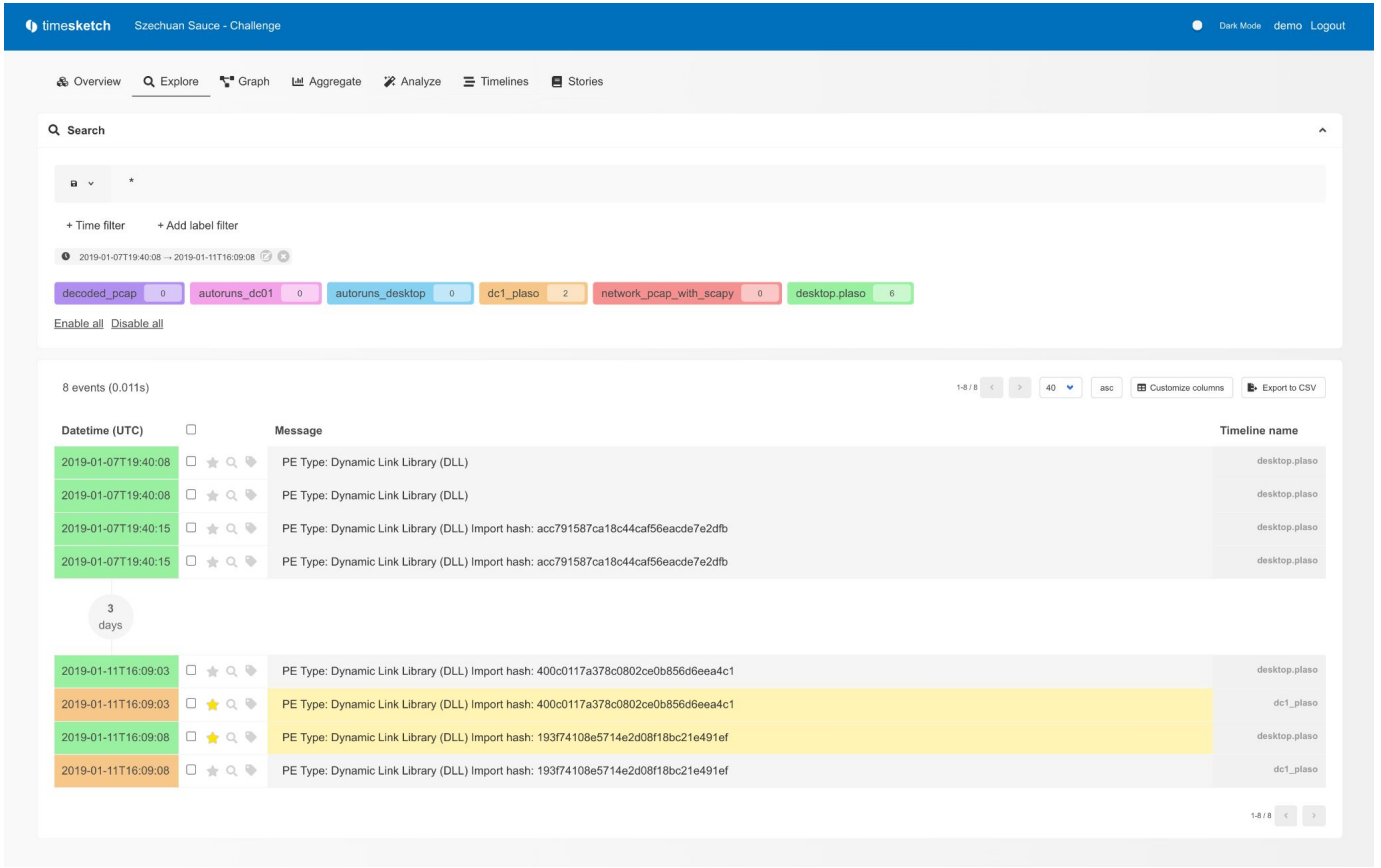
RECON INFOSEC

TIMESKETCH

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

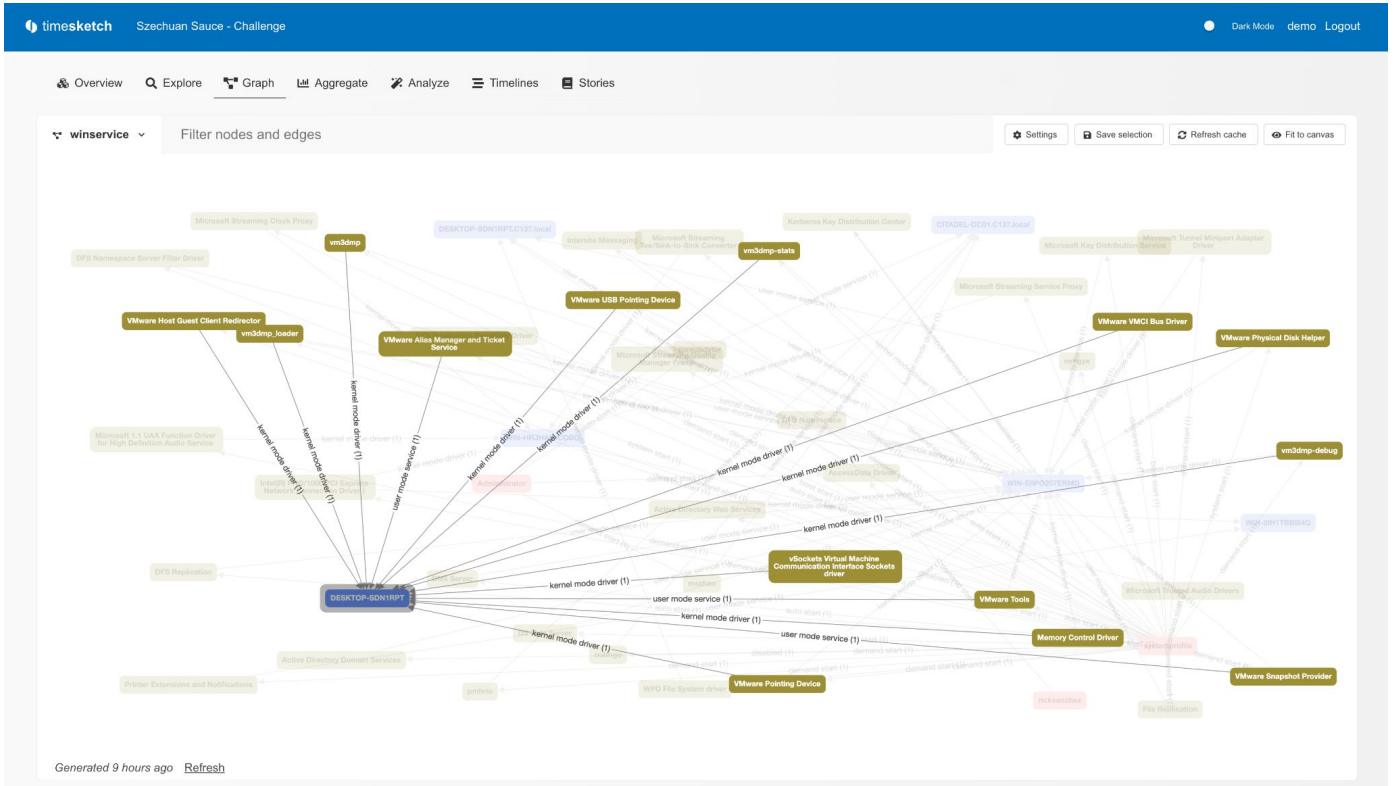
https://github.com/google/timesketch

TIMESKETCH



https://github.com/google/timesketch

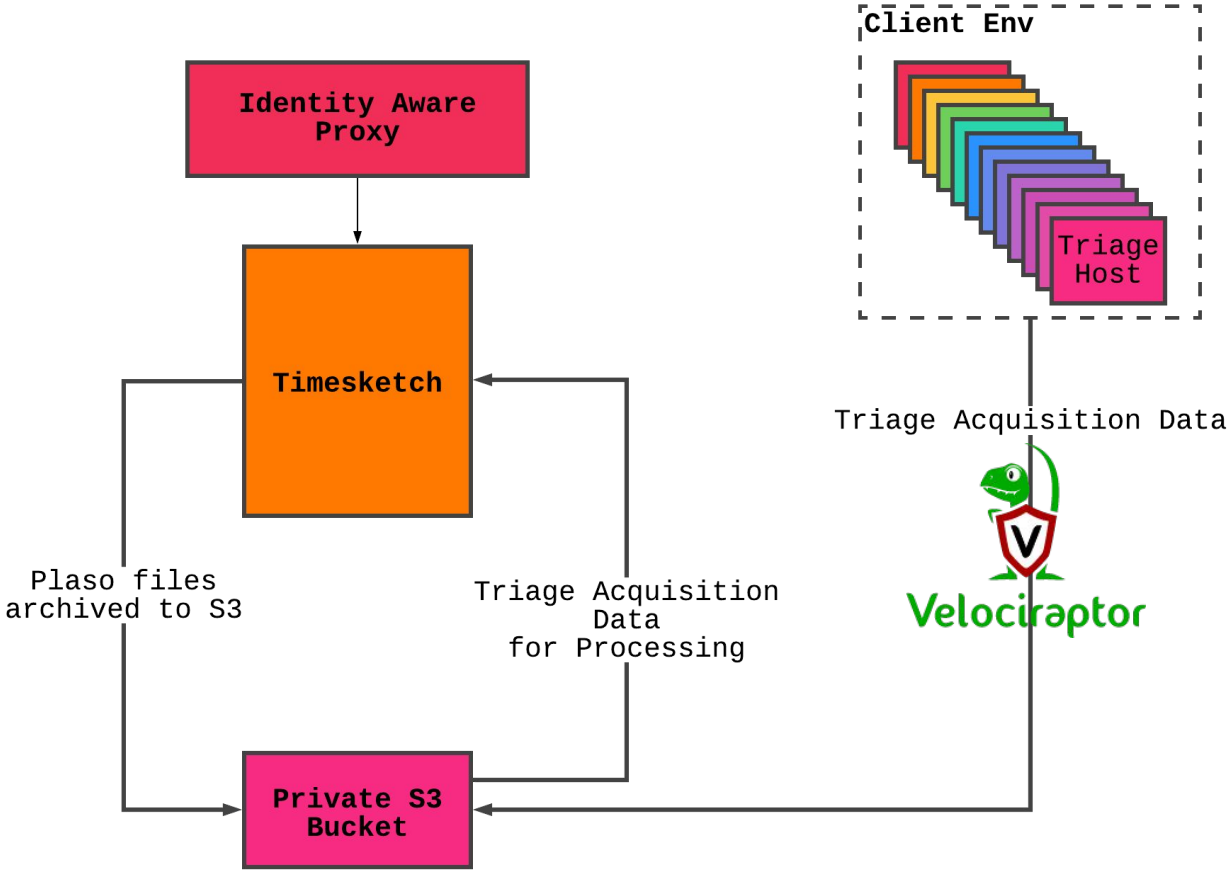
TIMESKETCH



https://github.com/google/timesketch

RECON INFOSEC

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

RECON INFOSEC

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

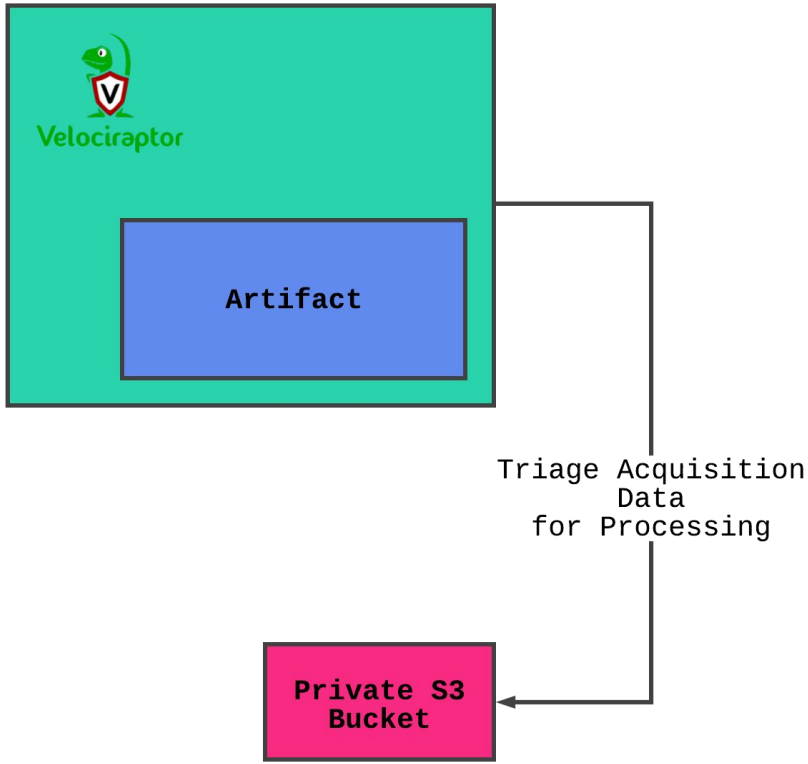
I HOPE YOU MEMORIZED ALL THAT!

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

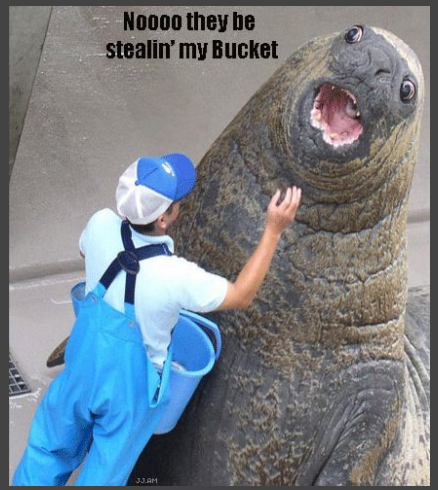
COMPONENT #1

Velociraptor

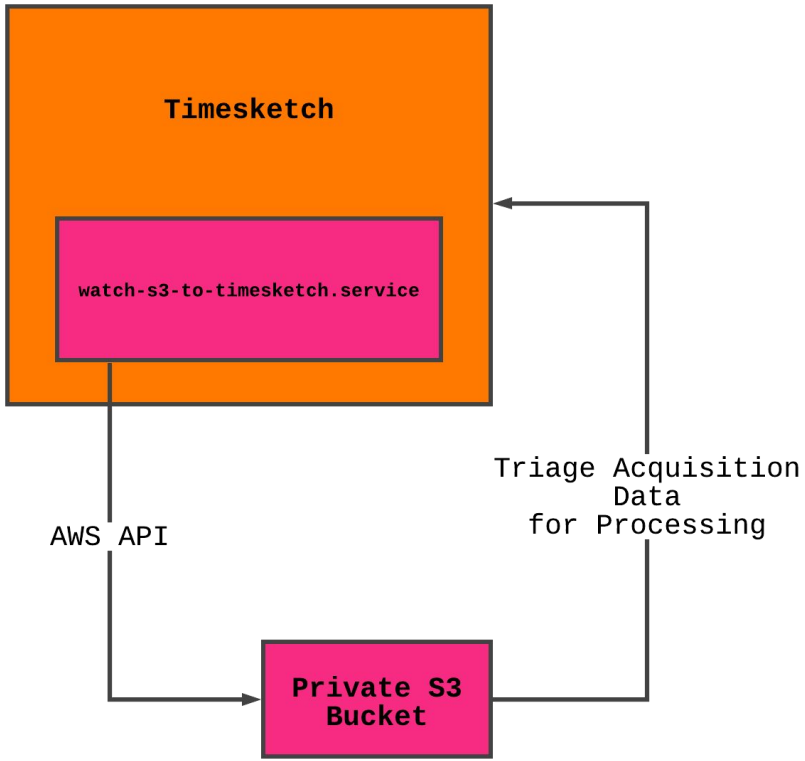
Artifact.Custom.Server.Utils.KAPEtoS3



COMPONENT #2



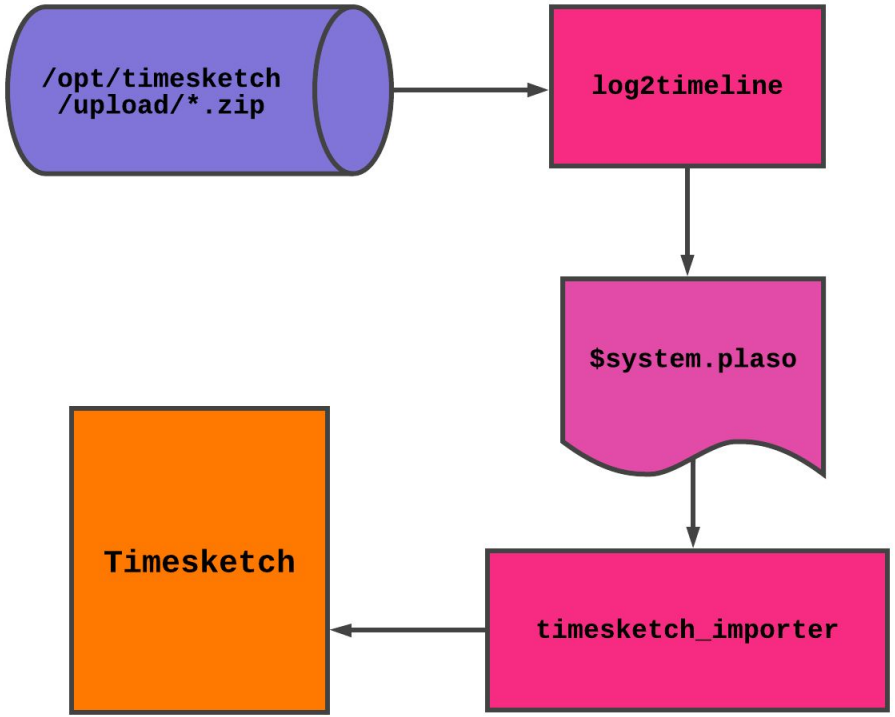
watch-s3-to-timesketch.service



RECON INFOSEC

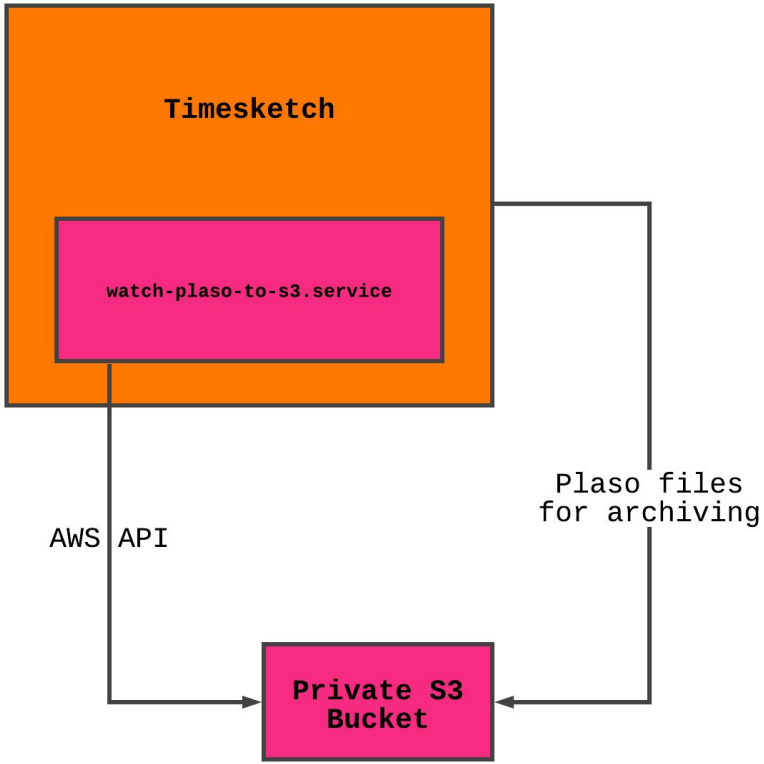
COMPONENT #3

data-to-timesketch.service

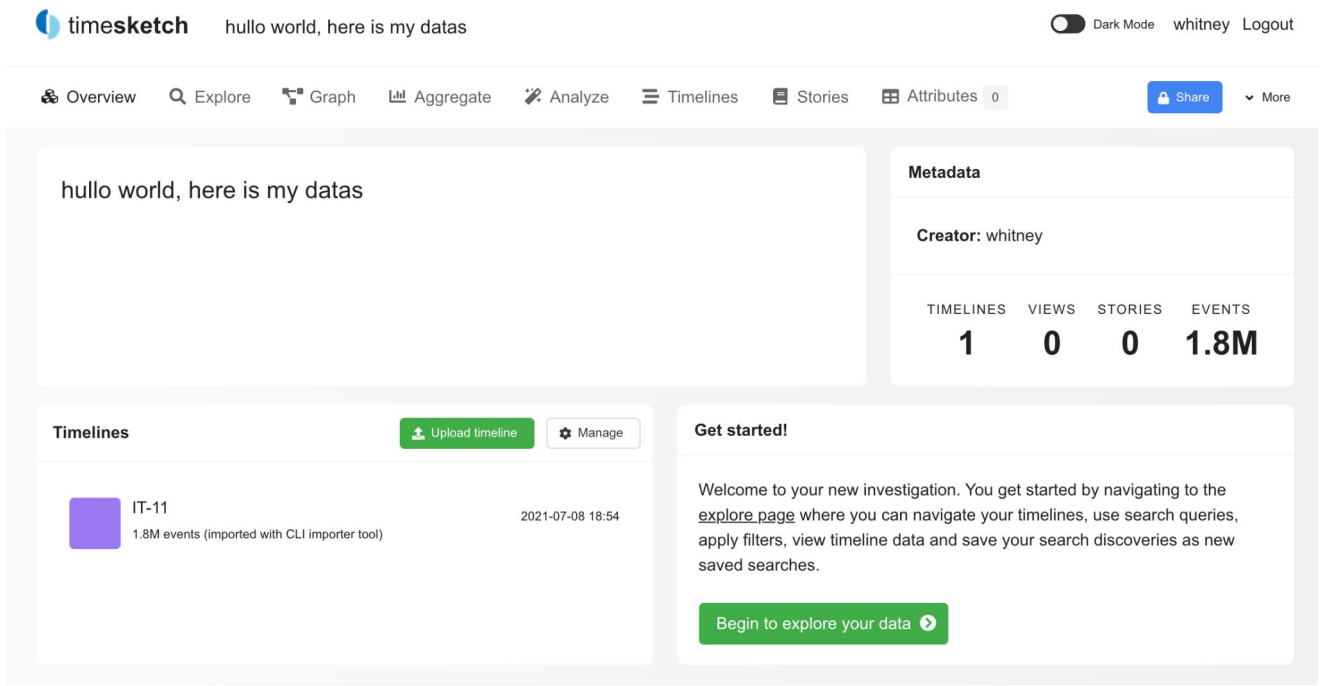


COMPONENT #4

watch-plaso-to-s3.service



WE HAVE DATA!



RECON INFOSEC

AS PROMISED

THE GITHUBS

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

RECON INFOSEC

THANK YOU

RECON
INFOSEC

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

OPEN SOC
NETWORK DEFENSE RANGE

Eric Capuano, @eric_capuano
Whitney Champion, @shortxstack