MAXIMUM YOUR DFIR VALUE WITH *MINIMUM* COST

whoAmI

Pham Tai Tue @tuedenn

- Now: Cyber Security Engineer *at* Giaohangtietkiem
- Former: Cyber Incident Responder *at* Viettel Cyber Security

Doing stuff

- Digital Forensic
- Threat Hunting
- Incident Response
- or something related

/TueDenn   /tuedenn

Intro: The typical DFIR problems

@TueDenn

- Recruitment talented people is a very difficult challenge
- High cost for educate current workforce
- High cost for buy MSSP service & commercial tools (DFIR/EDR)
- IR is hard, but will be harder without IR tools
- etc

→ *MAXIMUM* YOUR DFIR VALUE WITH *MINIMUM* COST

Agenda

1. DFIR(*) Values
   - What is DFIR values?
   - SANS Process
     - (*some*) Vietnam's Enterprise companies
2. Maximum your DFIR values
   - Key Principles for Successful DFIR
   - DFIR Tools
     - Minimum cost option
3. Demo
4. Summary

(*) Digital Forensic & Incident Response

DFIR Values

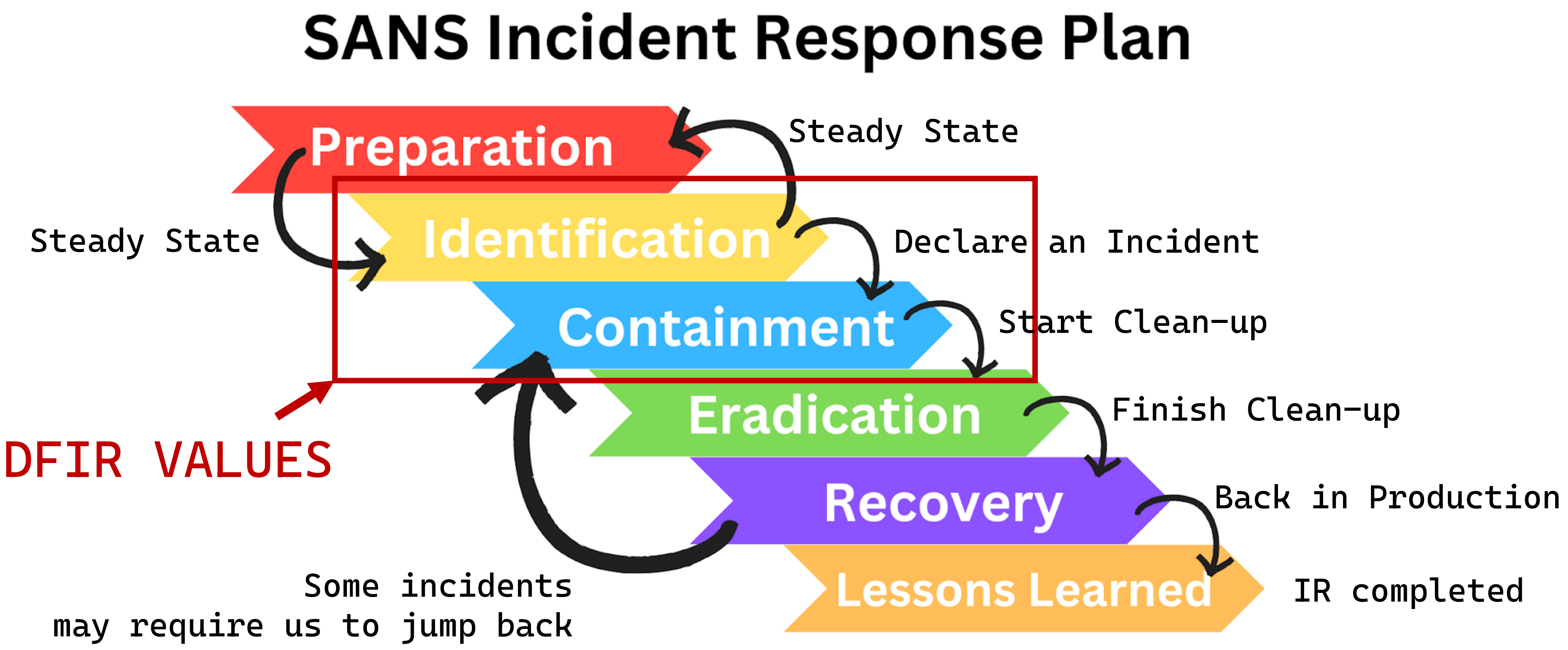
DFIR Values

- Blueteam Mission:
  - Reduce effects of compromise to the minimum *possible*
- The question is:
  - How fast and appropriate you react, if you be breached?
    (If you think you will never be breached, you're wrong!)

→You have to move fast and efficiently to overtake the attacker

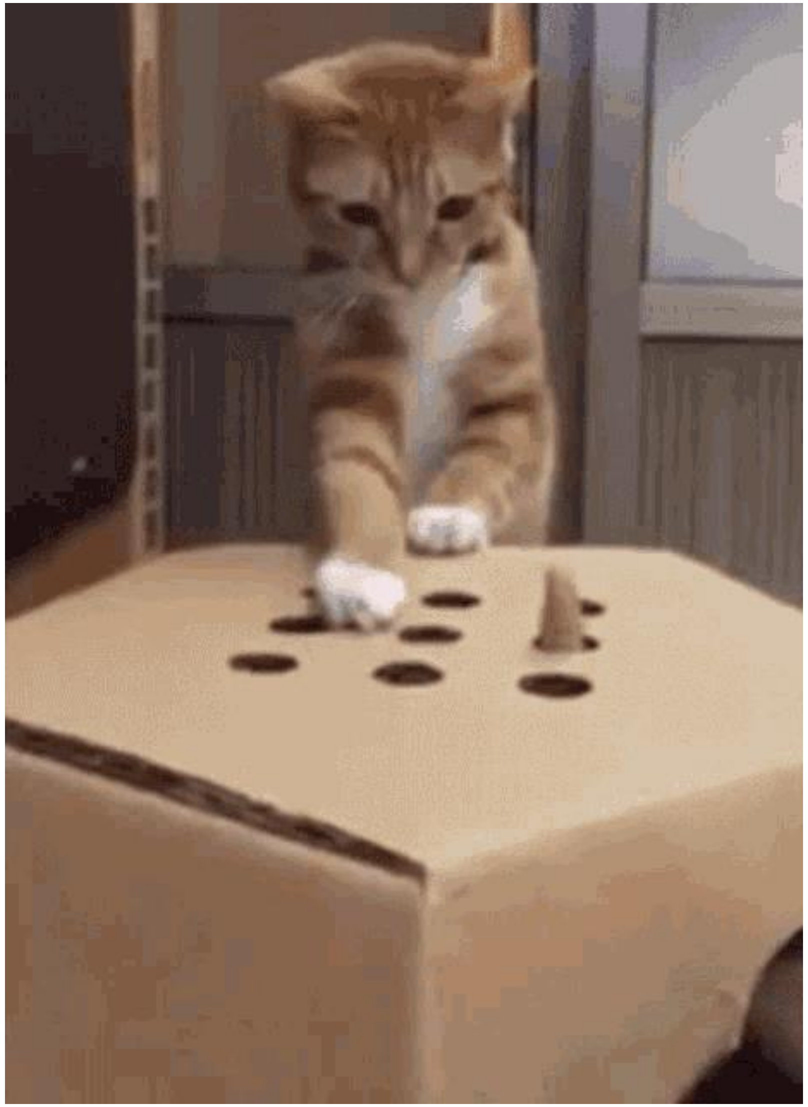
DFIR Values: SANS Process

@TueDenn



DFIR Values: Without DFIR

- Imagine you have no idea with DFIR
  - Or minimum values of DFIR
- Can you answer
  - How many system has been compromised?
  - What did attacker do after initial access?
  - What is the root cause of this breached?
  - etc.
- Without DFIR
  - The game be like “*What a mole*”
  - Sadly, most organizations in Vietnam are like that



https://media.tenor.com/zlGIDr_LfjgAAAAd/whack-a-mole-cute.gif

DFIR Values

DFIR VALUES

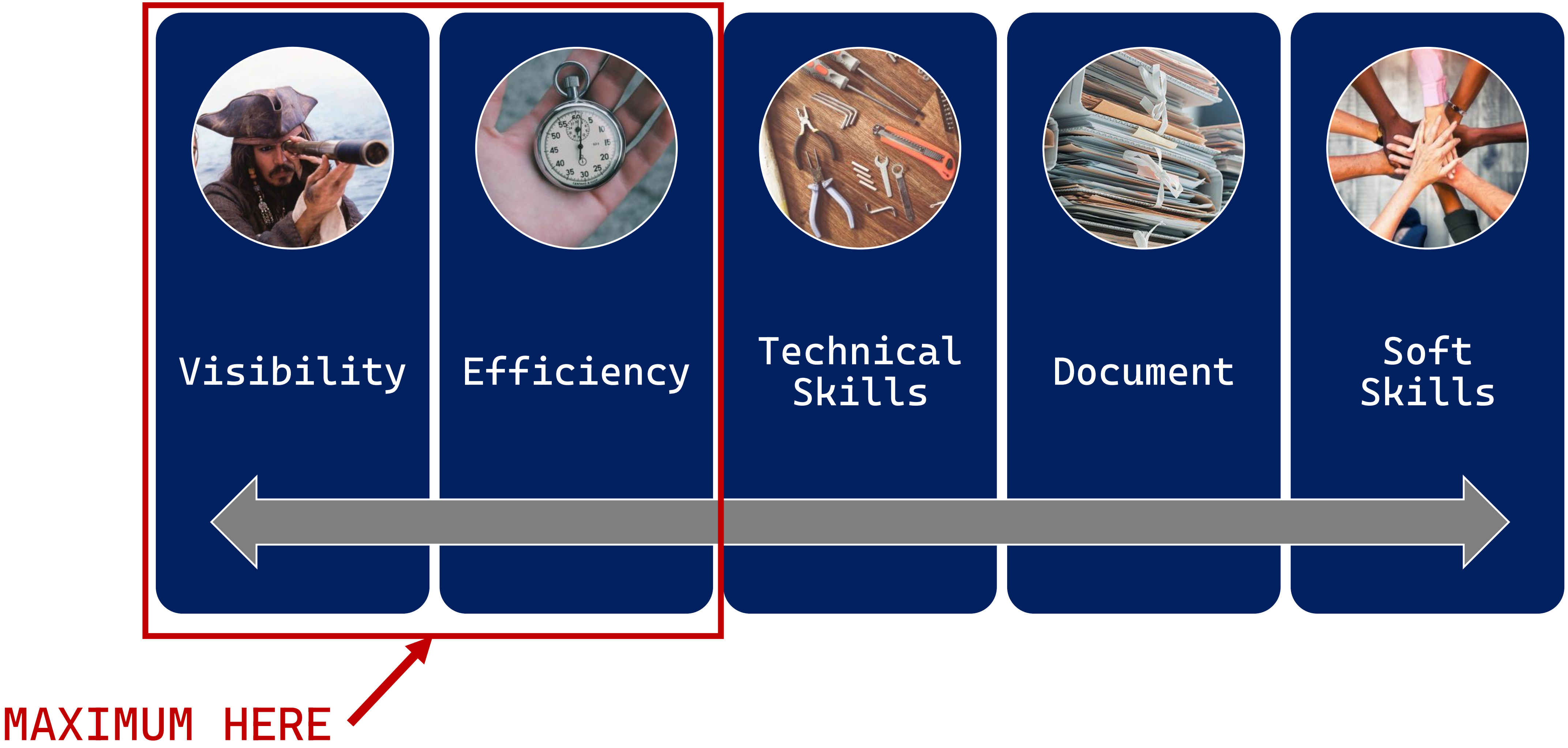
- “If you know the enemy and know yourself, you need not fear the result of a hundred battles.
- If you *know yourself* but *not the enemy*, for every victory gained you will also suffer a defeat.
- If you *know neither the enemy nor yourself*, you will succumb in every battle.”

– Sun Tzu, *The Art of War*

Maximum your DFIR values

With minimum cost

Maximum DFIR Values: Key Principles



Visibility

Efficiency

Technical Skills

Document

Soft Skills

MAXIMUM HERE

Maximum DFIR Values: Visibility

- You have total 10k endpoints (*many sites*), so, try to answer:
  1. How much computer has been compromised? More detail?
  2. Search a file (name, extension or hash) among them?
  3. Collect artifacts remain in compromised systems?
  4. Run a tool/script in an/multiple endpoints?
  5. Isolate an/multiple endpoints?

     Etc.

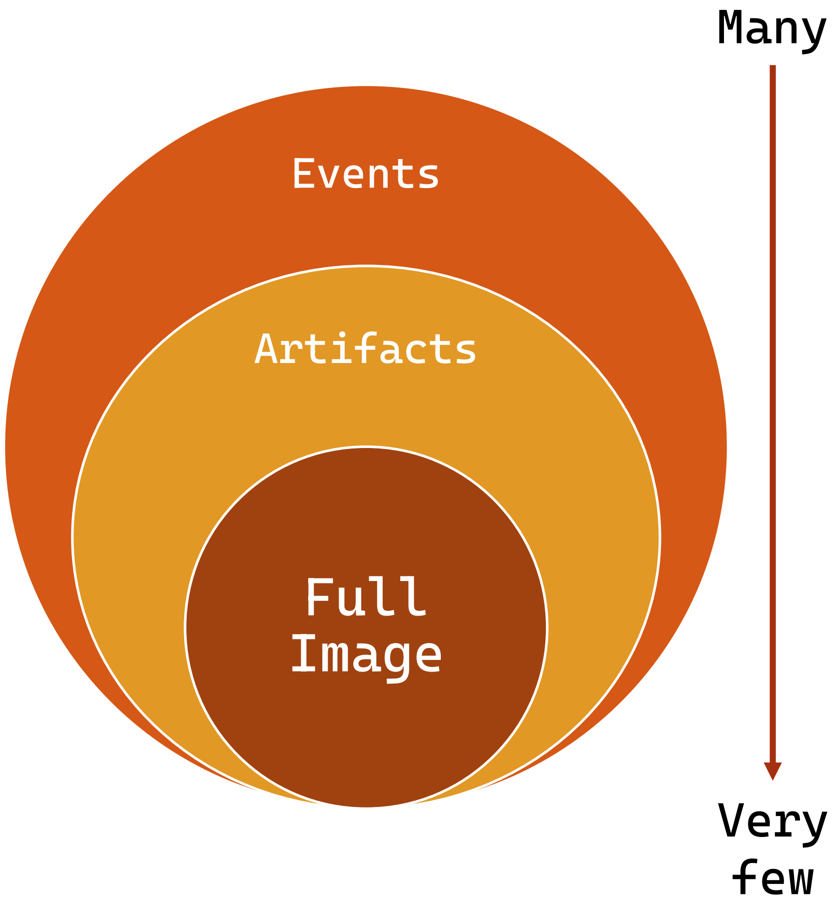
→ To maximum your DFIR values, you’ll need to have wide visibility into the environment

Maximum DFIR Values: Efficiency

- Efficiency is a difficult topic in DFIR
- Ex: Full disk image collection is good
  - But takes many cost to done
    - Collect
    - Storage
    - Parsing
    - Analyst

  → not efficiency

Events are not Pokémon,
We should strive to be tactical,
not hoarding



Maximum DFIR Values: Tool

- So, we need a tool which can help
  - Increase visibility capabilities
  - Collect, and analyst efficiency

- What is your choice?
  - Commercial
  - Opensource

DFIR Tool: Commercial

@TueDenn

👍 Advantages

- A strong and stable features set
- Technical support
  - 24/7 available
- Professional training

👎 Disadvantages

- More features = more money
  - Hard or Impossible your desired
- More money for tool = Less money for people
  - And other priorities

DFIR Tool: Opensource

👍 Advantages

- Almost ZERO COST
  - Cheaper money
  - Smart money for people & hardware
- Fully customizable
  - Add improvements
  - Add your desired feature

👎 Disadvantages

- Almost no support
  - Paid support options
- Other issues
  - CVE, bug, discontinue

  → riskier proposition

Maximum DFIR Values: Minimum cost

Selection criteria:

- Open source
- Paid support options
- Active community
- Fast, simple
- Multi-OS support
- Frequent updates/development
- Efficiency hunting/Forensic at Scale

osquery

GRR
RAPID RESPONSE

Velociraptor

Maximum DFIR Values: Minimum cost

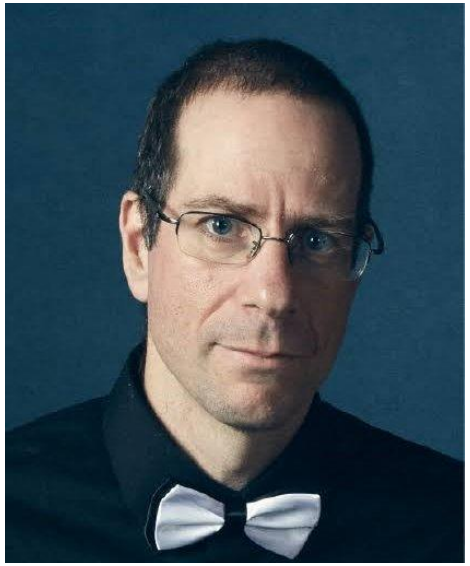
My recommendation: Velociraptor

- Open source ✓ Of course
- Paid support options ✓ Yes
- Active community ✓ Very Active in Discord
- Fast, simple ✓ Written in Go, better perform
- Multi-OS support ✓ As Golang support
- Frequent updates/development ✓ Yes, check github
- Efficiency hunting/Forensic at Scale ✓

By DFIR, for DFIR

Minimum cost with Velociraptor: What is Velo?

- Unique, Free and Open Source DFIR tool
- Created by Michael Cohen
  - Former software engineer at Google
  - Lead development of GRR & Rekall
- Released in August 2018
  - Velocidex company
  - based on an idea to create a new, more effective version of GRR
  - Affero GPL – a friendly open-source license
- Acquired by Rapid7 in April 2021
  - Metasploit for Red, Velociraptor for Blue
- By DFIR, for DFIR

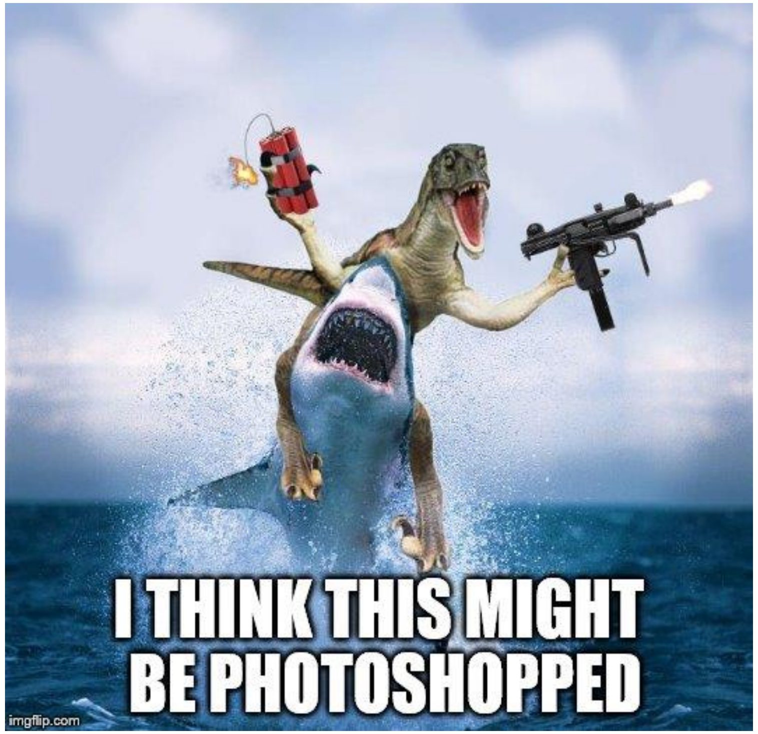


Minimum cost with Velociraptor: Feature

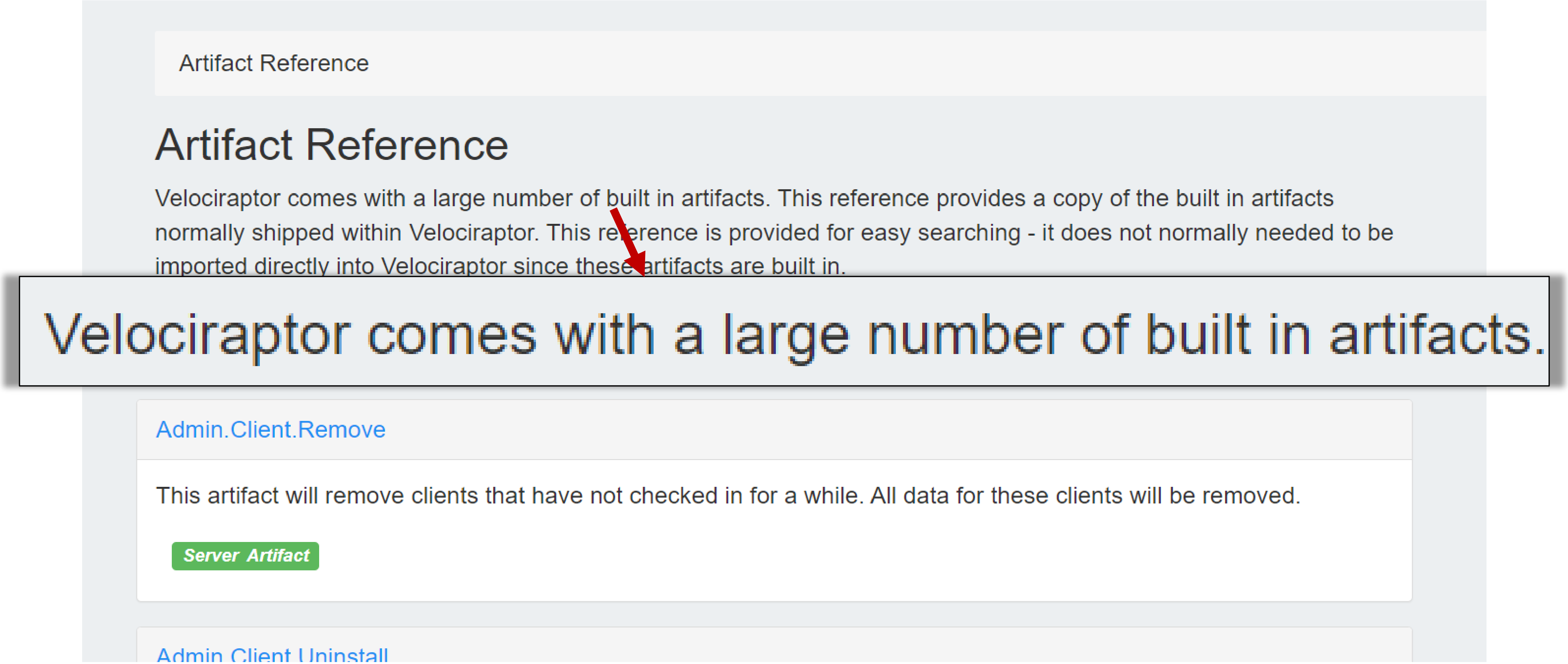
- Interactive shell & VFS viewer
- Automated response capabilities
- Continuous client monitoring
- Hunt for artifacts at scale
  - Over thousands of end points within minutes!
- Velociraptor uses expert knowledge to find the evidence
  - Reuse/reshare artifacts – via VQL (flexible)
  - Goal to automate DFIR task *as much as possible*

...

- More at *https://docs.velociraptor.app/* or my blog *https://tuedenn.github.io/blog/tags/velociraptor/*



Reuse Expert Knowledge – via Artifacts



Artifact Reference

Artifact Reference

Velociraptor comes with a large number of built in artifacts. This reference provides a copy of the built in artifacts normally shipped within Velociraptor. This reference is provided for easy searching - it does not normally needed to be imported directly into Velociraptor since these artifacts are built in.

Velociraptor comes with a large number of built in artifacts.

Admin.Client.Remove

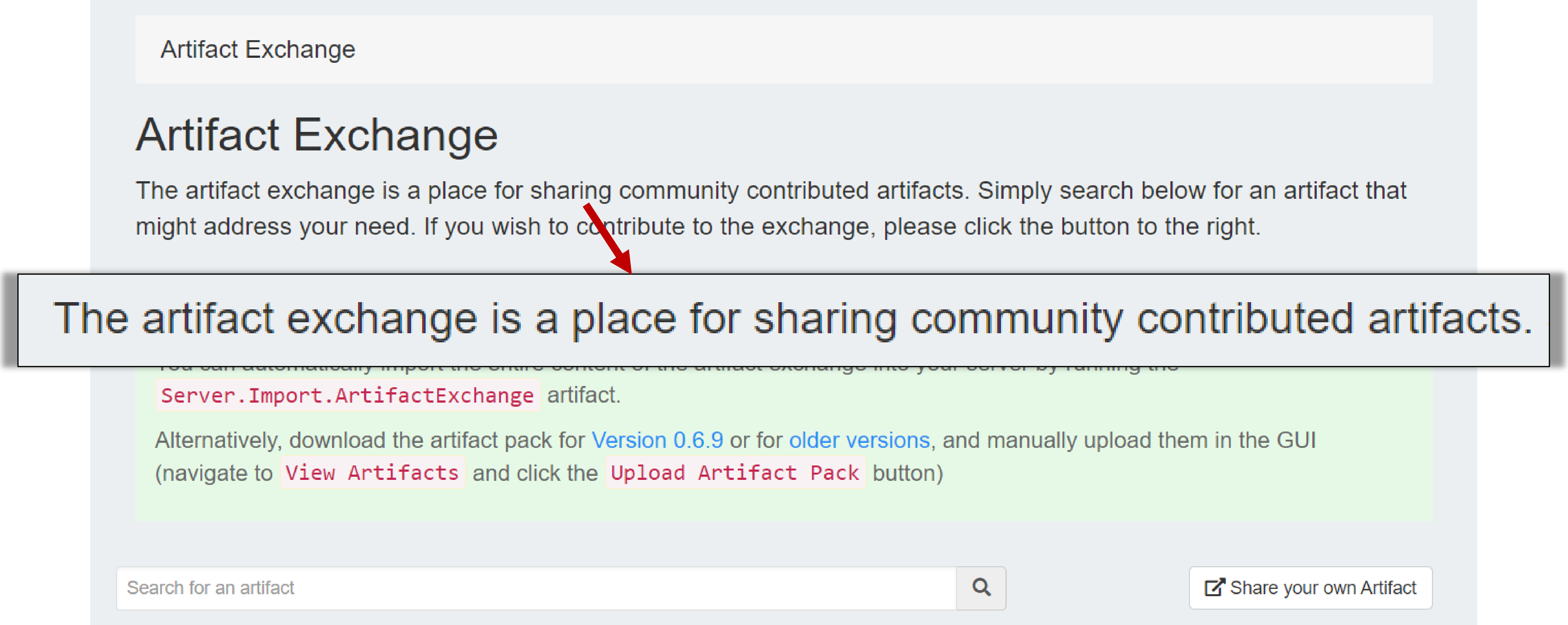
This artifact will remove clients that have not checked in for a while. All data for these clients will be removed.

Admin.Client.Uninstall

https://docs.velociraptor.app/artifact_references/

Reshare Community Knowledge – via Artifacts

@TueDenn



Artifact Exchange

Artifact Exchange

The artifact exchange is a place for sharing community contributed artifacts. Simply search below for an artifact that might address your need. If you wish to contribute to the exchange, please click the button to the right.

The artifact exchange is a place for sharing community contributed artifacts.

You can automatically import the entire content of the artifact exchange into your server by running the `Server.Import.ArtifactExchange` artifact.

Alternatively, download the artifact pack for Version 0.6.9 or for older versions, and manually upload them in the GUI (navigate to `View Artifacts` and click the `Upload Artifact Pack` button)

https://docs.velociraptor.app/exchange/

Minimum cost with Velociraptor: New DFIR Approach

@TueDenn

Traditional DFIR Approach

1. Acquisition
   - fetch raw data from end point (MFT, EVTX)
2. Transport
   - Move the data off the endpoint
   - e.g. Cloud upload, VHDX
3. Analysis
   - Parse data centrally on server
   - Use standalone tools, timelines etc

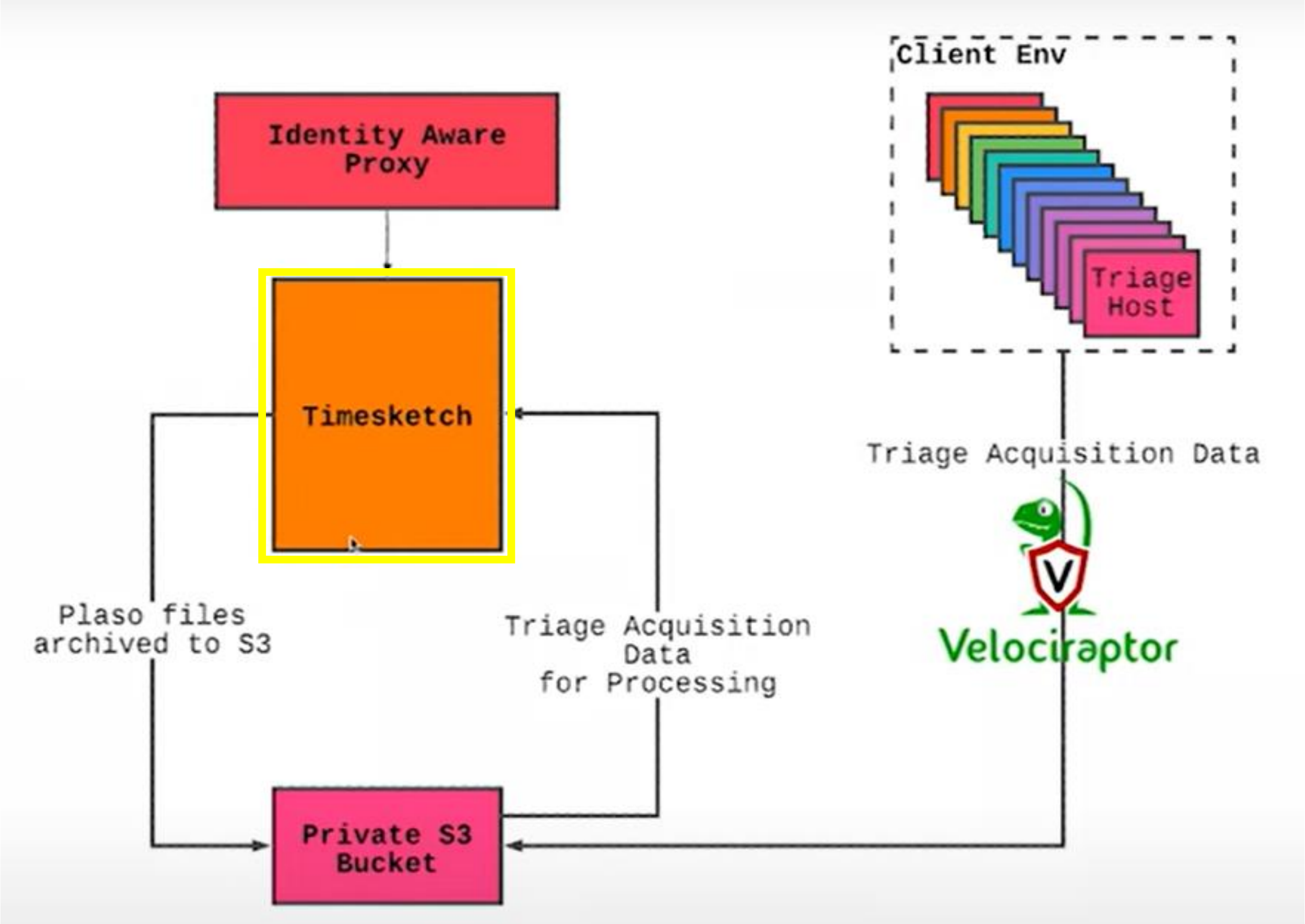
Velociraptor DFIR Approach

1. Parse and analyze on the endpoint
2. Targeted collections
3. Pivot with further collections as needed.
4. Scale up collection
5. Flexible query language allows quickly creating new analysis

Minimum cost with Velociraptor: Architecture

@TueDenn

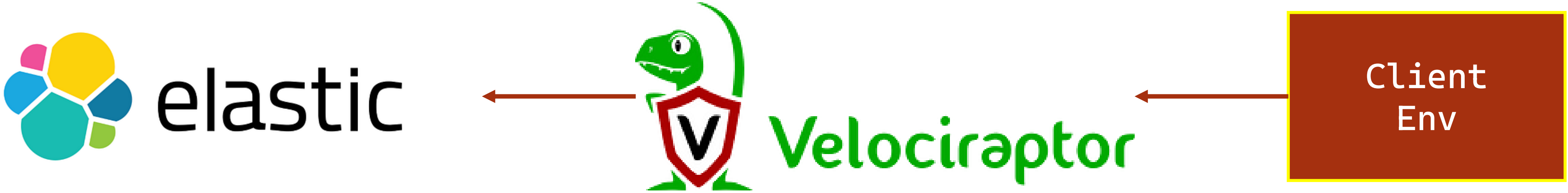
- Large:
  - Scaling Forensics across *many* systems



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

Minimum cost with Velociraptor: Architecture

- Medium (>25K endpoints)
  - Using Elastic or Splunk is better for large engagements
- Velociraptor has artifact for exporting to Elastic and Splunk
  - Send event artifacts continuously (*Elastic.Events.Clients*)
  - Send hunt results as they complete (*Elastic.Flows.Upload*)

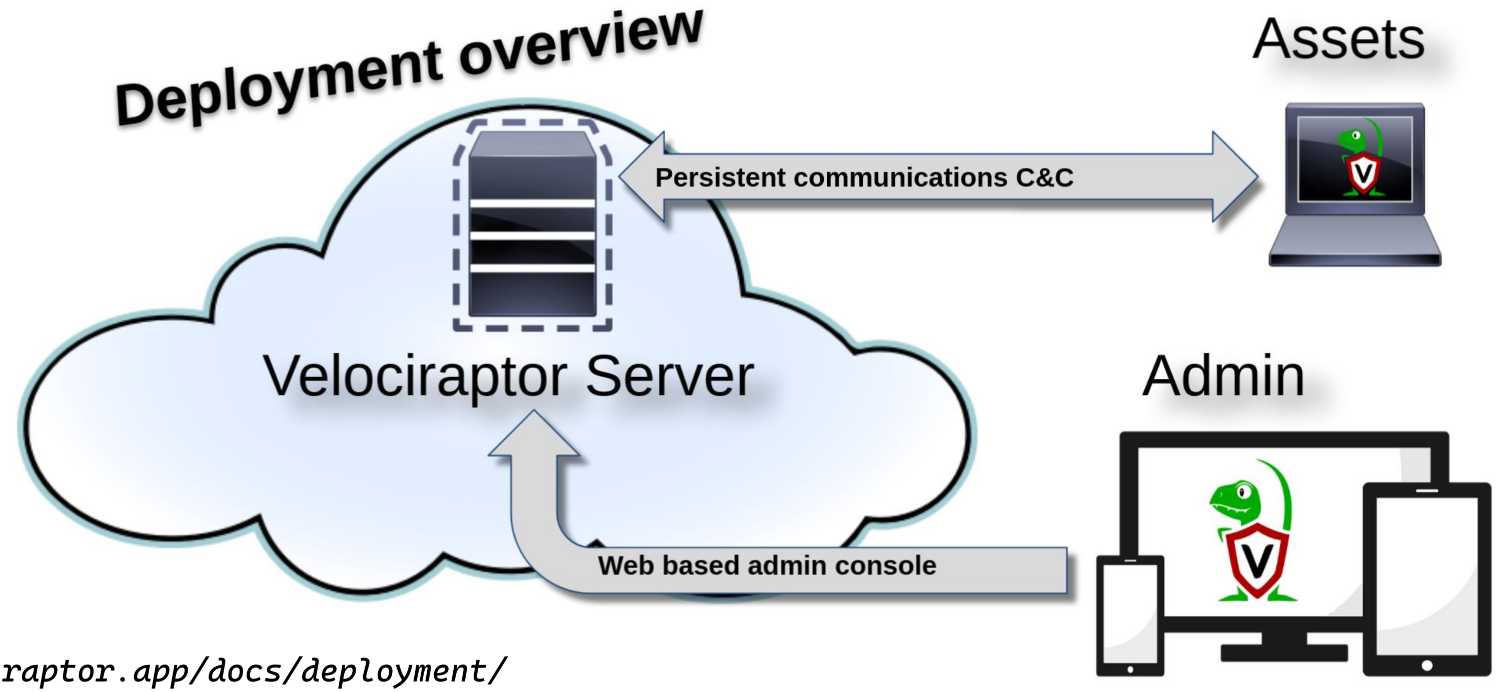


https://docs.velociraptor.app/blog/2019/2019-12-08-velociraptor-to-elasticsearch-3a9fc02c6568/

Minimum cost with Velociraptor: Architecture

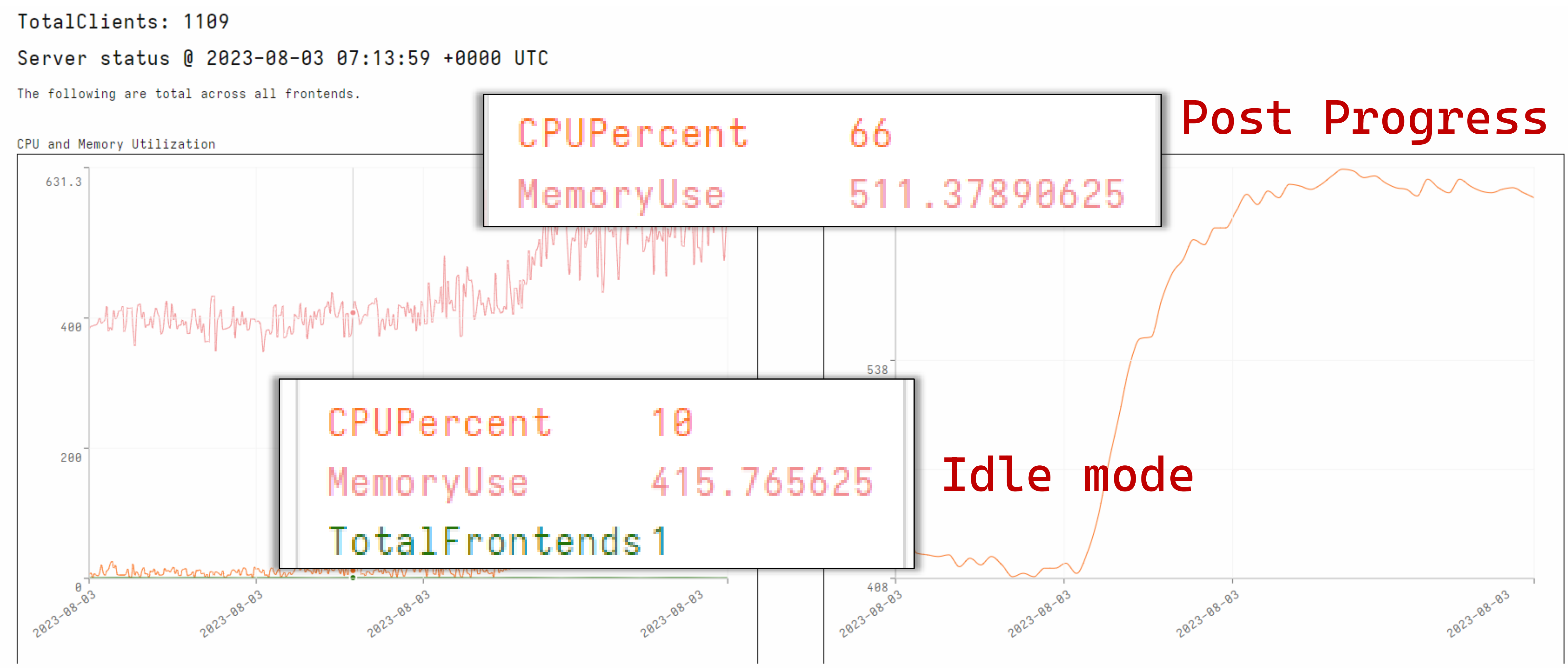
MINIMUM COST

- Small (<15k)
  - *A typical Velociraptor deployment*
  - Great for analyzing *small-to-medium* sized data sets
  - 8GB, 2 Core server for 10-15k Endpoints (*~t2.large at AWS*)



https://docs.velociraptor.app/docs/deployment/

Typical Deployment Performance



TotalClients: 1109

Server status @ 2023-08-03 07:13:59 +0000 UTC

The following are total across all frontends.

CPU and Memory Utilization

```
CPUPercent      66
MemoryUse       511.37890625
```

Post Progress

```
CPUPercent      10
MemoryUse       415.765625
TotalFrontends  1
```

Idle mode

https://docs.velociraptor.app/docs/deployment/resources/

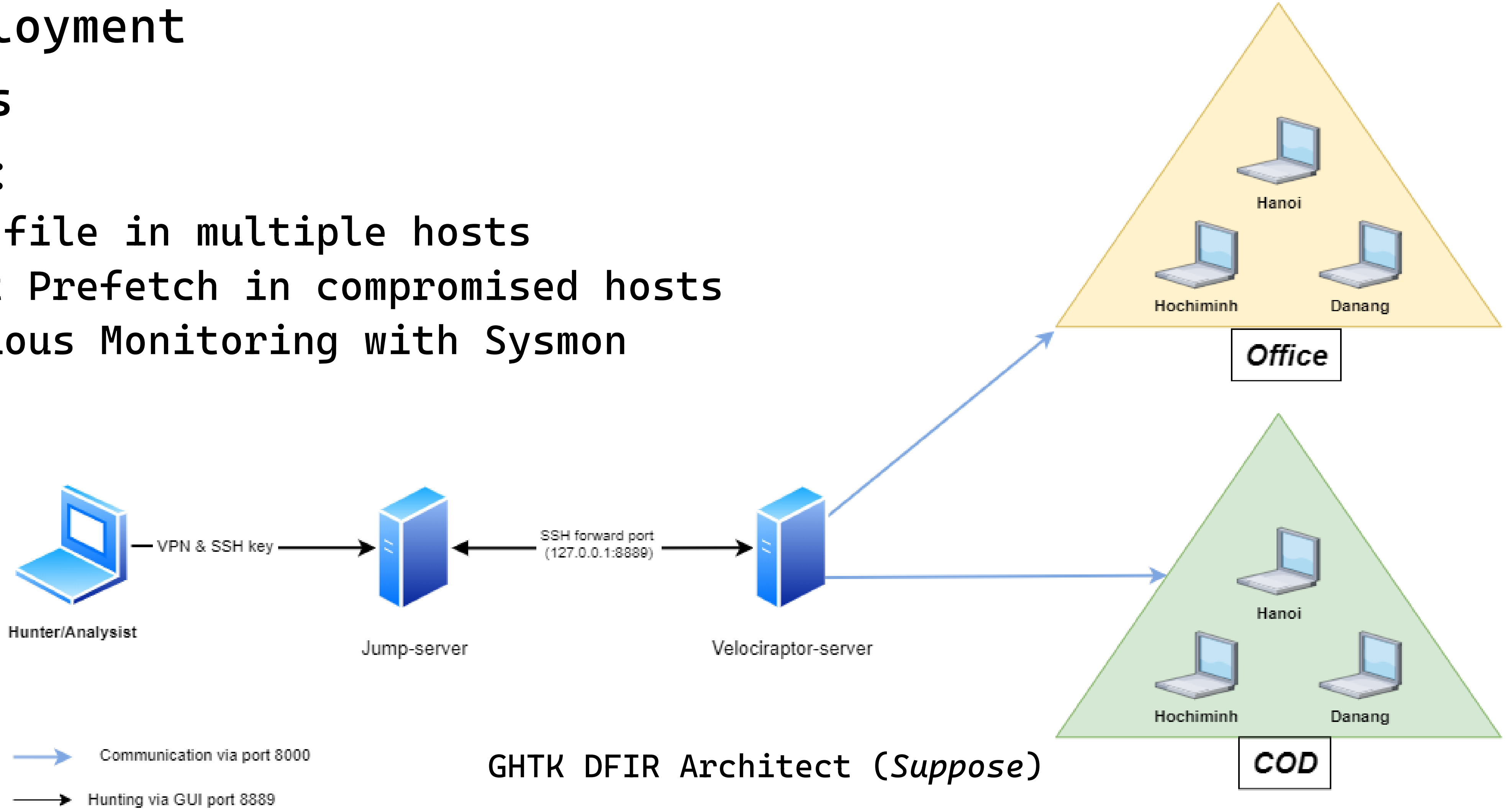
Idle performance statistics

DEMO

With Velo

Demo: Use-cases

- Small deployment
- 1k Clients
- Use-cases:
    1. Search file in multiple hosts
    2. Collect Prefetch in compromised hosts
    3. Continuous Monitoring with Sysmon



GHTK DFIR Architect (*Suppose*)

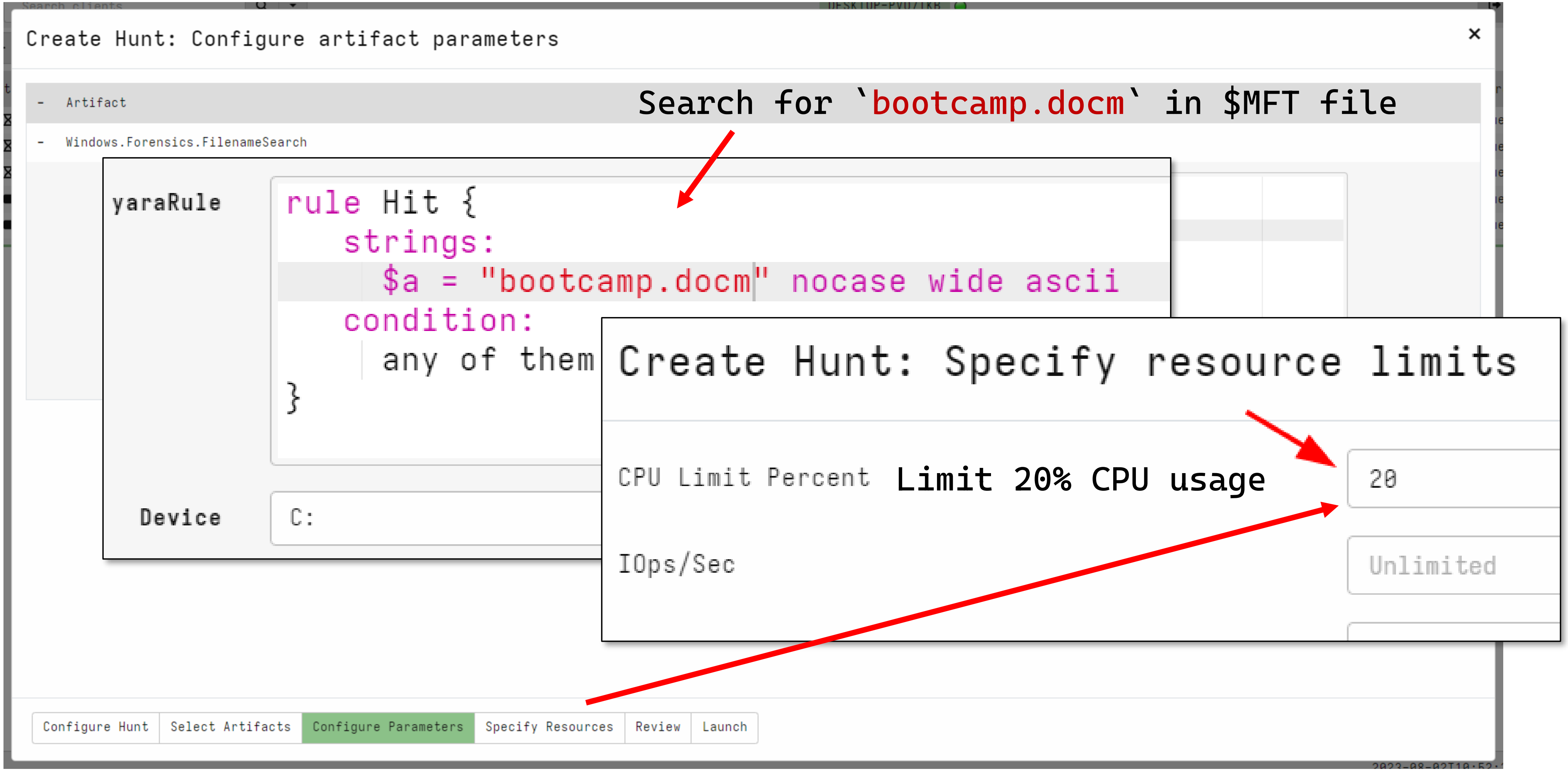
Use-case 0x1: Search file in multiple hosts

- Scenario:
  - An phishing email was sent for 1k users, link to file bootcamp.docm
  - How many user has been download bootcamp.docm?
- Hypothesis:
  - User click download, and save in Downloads folder
- Todo List:
  - List all file in C:\Users\*\Downloads
  - Search file which named bootcamp.docm
- Velociraptor
  - Use Windows.Forensics.FilenameSearch or Windows.Search.FileFinder
  - With parameter regex C:\Users\*\Downloads\bootcamp.docm

“DFIR is often about finding files on the endpoint”

Use-case 0x1: Search file in multiple hosts

@TueDenn



Create Hunt: Configure artifact parameters

- Artifact
- Windows.Forensics.FilenameSearch

Search for `bootcamp.docm` in $MFT file

yaraRule

```
rule Hit {
   strings:
     $a = "bootcamp.docm" nocase wide ascii
   condition:
     any of them
}
```

Device: C:

Create Hunt: Specify resource limits

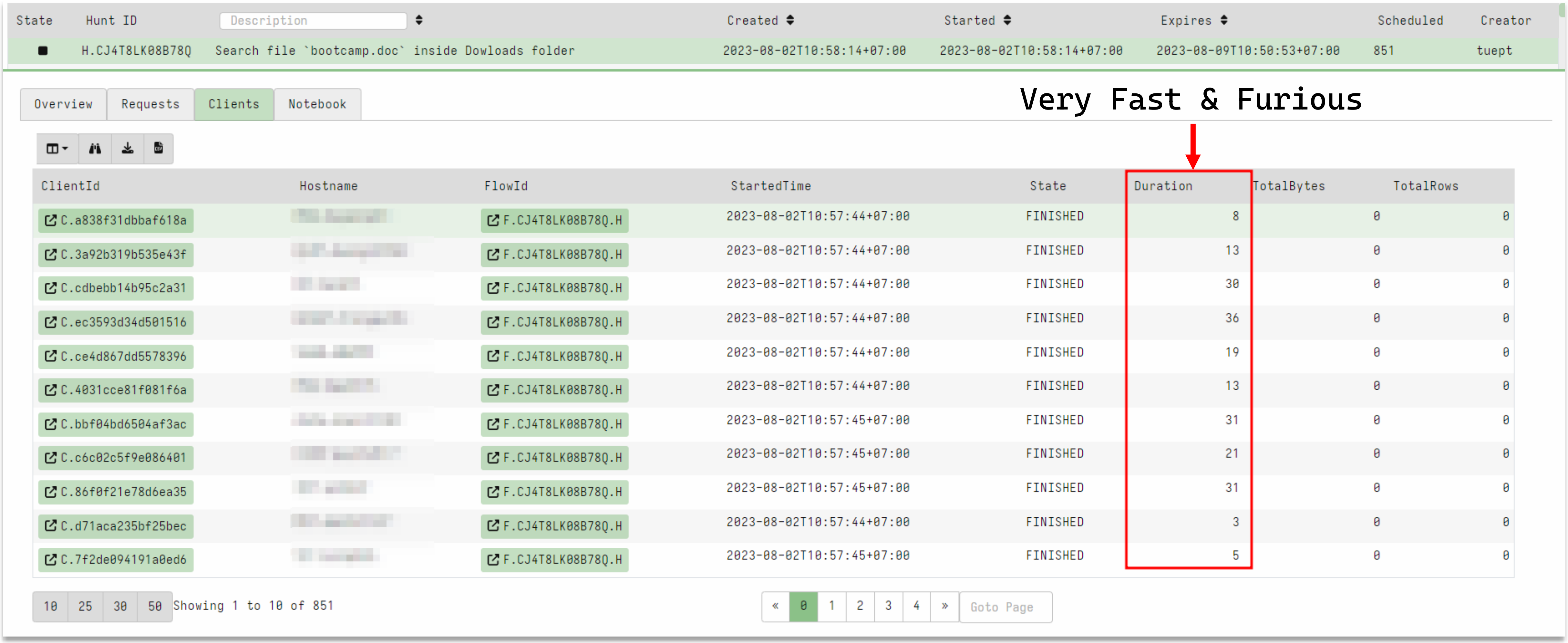
CPU Limit Percent: 20

Limit 20% CPU usage

IOps/Sec: Unlimited

Use-case 0x1: Search file in multiple hosts

@TueDenn



State	Hunt ID	Description	Created	Started	Expires	Scheduled	Creator
■	H.CJ4T8LK08B78Q	Search file `bootcamp.doc` inside Dowloads folder	2023-08-02T10:58:14+07:00	2023-08-02T10:58:14+07:00	2023-08-09T10:50:53+07:00	851	tuept

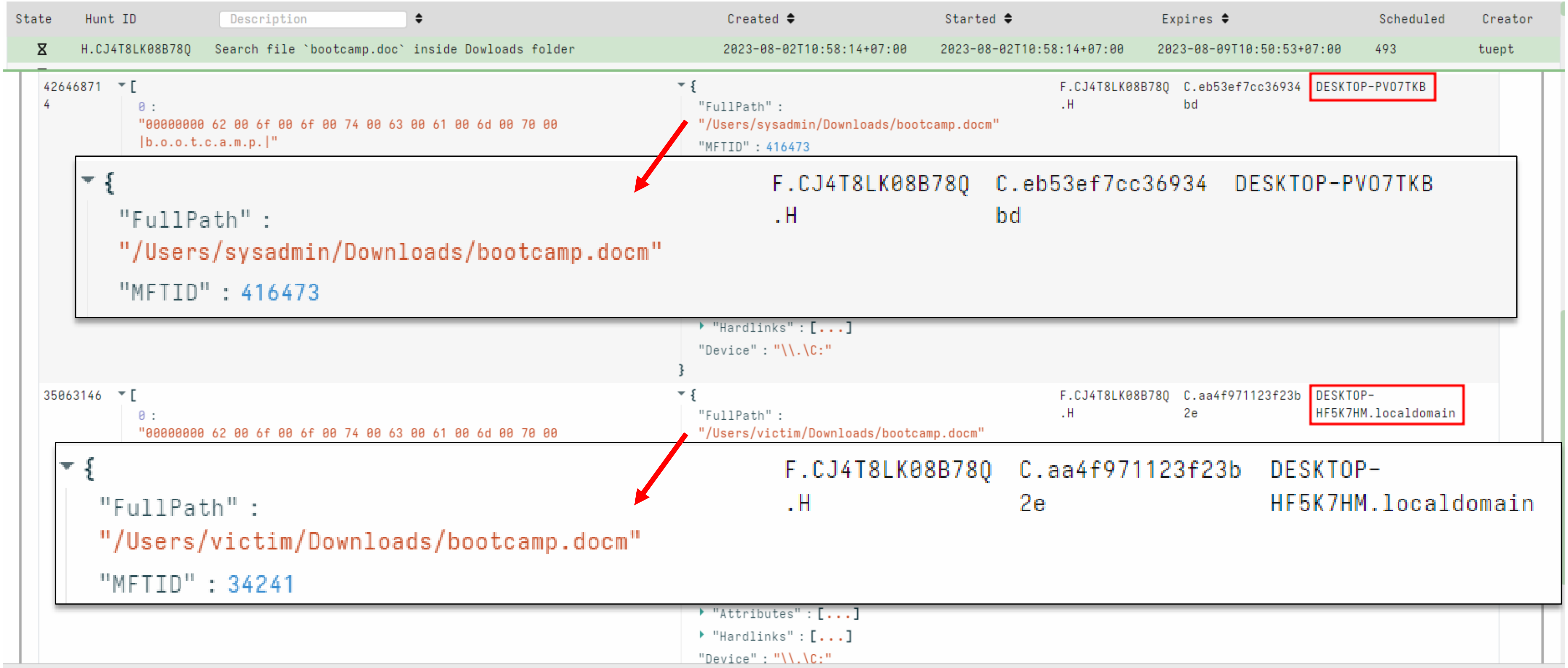
Very Fast & Furious

ClientId	Hostname	FlowId	StartedTime	State	Duration	TotalBytes	TotalRows
C.a838f31dbbaf618a	[redacted]	F.CJ4T8LK08B78Q.H	2023-08-02T10:57:44+07:00	FINISHED	8	0	0
C.3a92b319b535e43f	[redacted]	F.CJ4T8LK08B78Q.H	2023-08-02T10:57:44+07:00	FINISHED	13	0	0
C.cdbebb14b95c2a31	[redacted]	F.CJ4T8LK08B78Q.H	2023-08-02T10:57:44+07:00	FINISHED	30	0	0
C.ec3593d34d501516	[redacted]	F.CJ4T8LK08B78Q.H	2023-08-02T10:57:44+07:00	FINISHED	36	0	0
C.ce4d867dd5578396	[redacted]	F.CJ4T8LK08B78Q.H	2023-08-02T10:57:44+07:00	FINISHED	19	0	0
C.4031cce81f081f6a	[redacted]	F.CJ4T8LK08B78Q.H	2023-08-02T10:57:44+07:00	FINISHED	13	0	0
C.bbf04bd6504af3ac	[redacted]	F.CJ4T8LK08B78Q.H	2023-08-02T10:57:45+07:00	FINISHED	31	0	0
C.c6c02c5f9e086401	[redacted]	F.CJ4T8LK08B78Q.H	2023-08-02T10:57:45+07:00	FINISHED	21	0	0
C.86f0f21e78d6ea35	[redacted]	F.CJ4T8LK08B78Q.H	2023-08-02T10:57:45+07:00	FINISHED	31	0	0
C.d71aca235bf25bec	[redacted]	F.CJ4T8LK08B78Q.H	2023-08-02T10:57:44+07:00	FINISHED	3	0	0
C.7f2de094191a0ed6	[redacted]	F.CJ4T8LK08B78Q.H	2023-08-02T10:57:45+07:00	FINISHED	5	0	0

Showing 1 to 10 of 851

Use-case 0x1: Search file in multiple hosts

@TueDenn



State	Hunt ID	Description	Created	Started	Expires	Scheduled	Creator
⧗	H.CJ4T8LK08B78Q	Search file `bootcamp.doc` inside Dowloads folder	2023-08-02T10:58:14+07:00	2023-08-02T10:58:14+07:00	2023-08-09T10:50:53+07:00	493	tuept

```
426468714  [
             0 :
             "00000000 62 00 6f 00 6f 00 74 00 63 00 61 00 6d 00 70 00
             |b.o.o.t.c.a.m.p.|"
                                   {
                                     "FullPath" :
                                     "/Users/sysadmin/Downloads/bootcamp.docm"
                                     "MFTID" : 416473
                                     "Hardlinks" : [...]
                                     "Device" : "\\.\C:"
                                   }
                                                     F.CJ4T8LK08B78Q.H  C.eb53ef7cc36934bd  DESKTOP-PVO7TKB
```

```
{
  "FullPath" :
  "/Users/sysadmin/Downloads/bootcamp.docm"
  "MFTID" : 416473
                 F.CJ4T8LK08B78Q.H   C.eb53ef7cc36934bd   DESKTOP-PVO7TKB
```

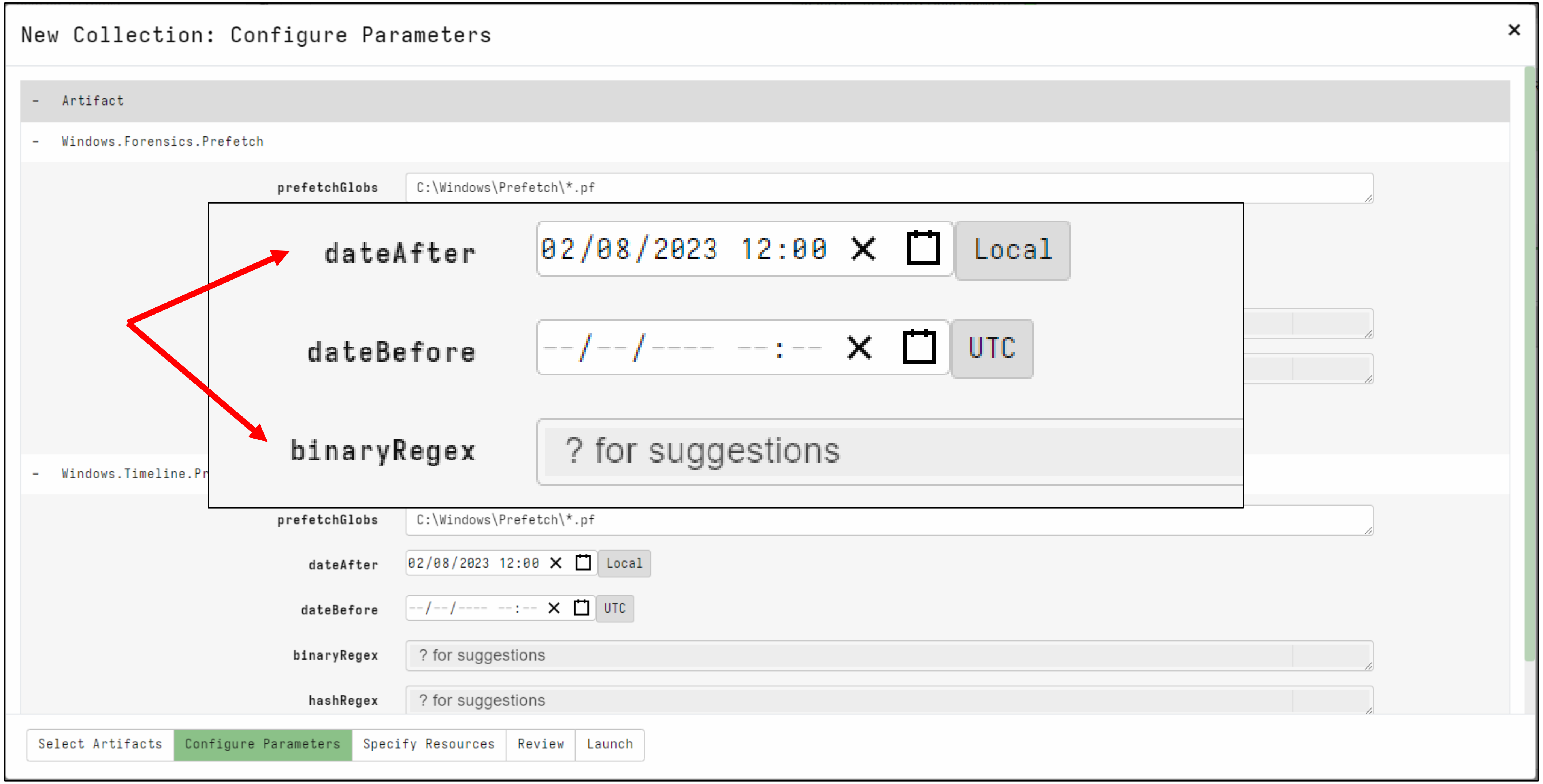
```
35063146  [
            0 :
            "00000000 62 00 6f 00 6f 00 74 00 63 00 61 00 6d 00 70 00
                                   {
                                     "FullPath" :
                                     "/Users/victim/Downloads/bootcamp.docm"
                                     "Attributes" : [...]
                                     "Hardlinks" : [...]
                                     "Device" : "\\.\C:"
                                                     F.CJ4T8LK08B78Q.H  C.aa4f971123f23b2e  DESKTOP-HF5K7HM.localdomain
```

```
{
  "FullPath" :
  "/Users/victim/Downloads/bootcamp.docm"
  "MFTID" : 34241
                 F.CJ4T8LK08B78Q.H   C.aa4f971123f23b2e   DESKTOP-HF5K7HM.localdomain
```

Use-case 0x2: Collect Prefetch

- Scenario:
  - User clicked to run bootcamp.docm
  - Word spawns a new process and may have done some bad things
  - What process has been run?
- Hypothesis:
  - There is no monitoring service running on this computer
- Todo List:
  - Collect all prefetch file in C:\Windows\Prefetch\*
  - Parser and analysis
- Velociraptor
  - Use Windows.Forensics.Prefetch or Windows.Timeline.Prefetch
  - Filter by date with parameter: dateAfter and dateBefore

Use-case 0x2: Collect Prefetch



New Collection: Configure Parameters

- Artifact
- Windows.Forensics.Prefetch

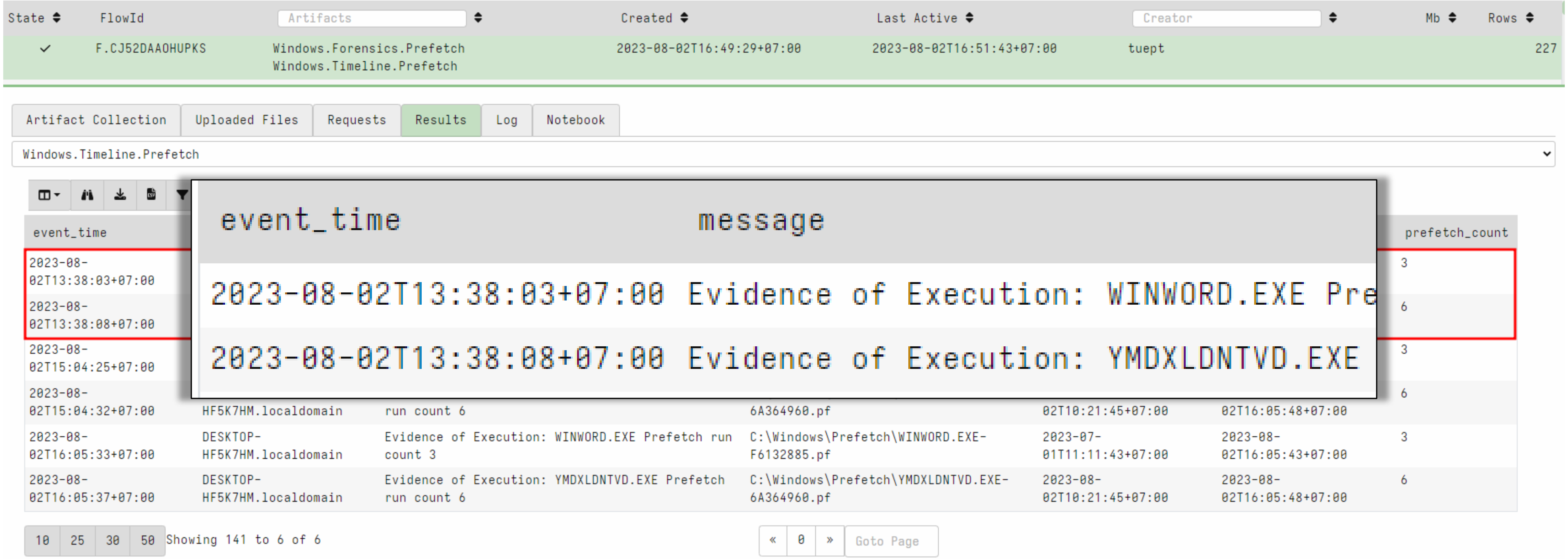
prefetchGlobs	C:\Windows\Prefetch\*.pf
dateAfter	02/08/2023 12:00 Local
dateBefore	--/--/---- --:-- UTC
binaryRegex	? for suggestions

- Windows.Timeline.Pr

prefetchGlobs	C:\Windows\Prefetch\*.pf
dateAfter	02/08/2023 12:00 Local
dateBefore	--/--/---- --:-- UTC
binaryRegex	? for suggestions
hashRegex	? for suggestions

Use-case 0x2: Collect Prefetch

@TueDenn



State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.CJ52DAAOHUPKS	Windows.Forensics.Prefetch Windows.Timeline.Prefetch	2023-08-02T16:49:29+07:00	2023-08-02T16:51:43+07:00	tuept		227

Windows.Timeline.Prefetch

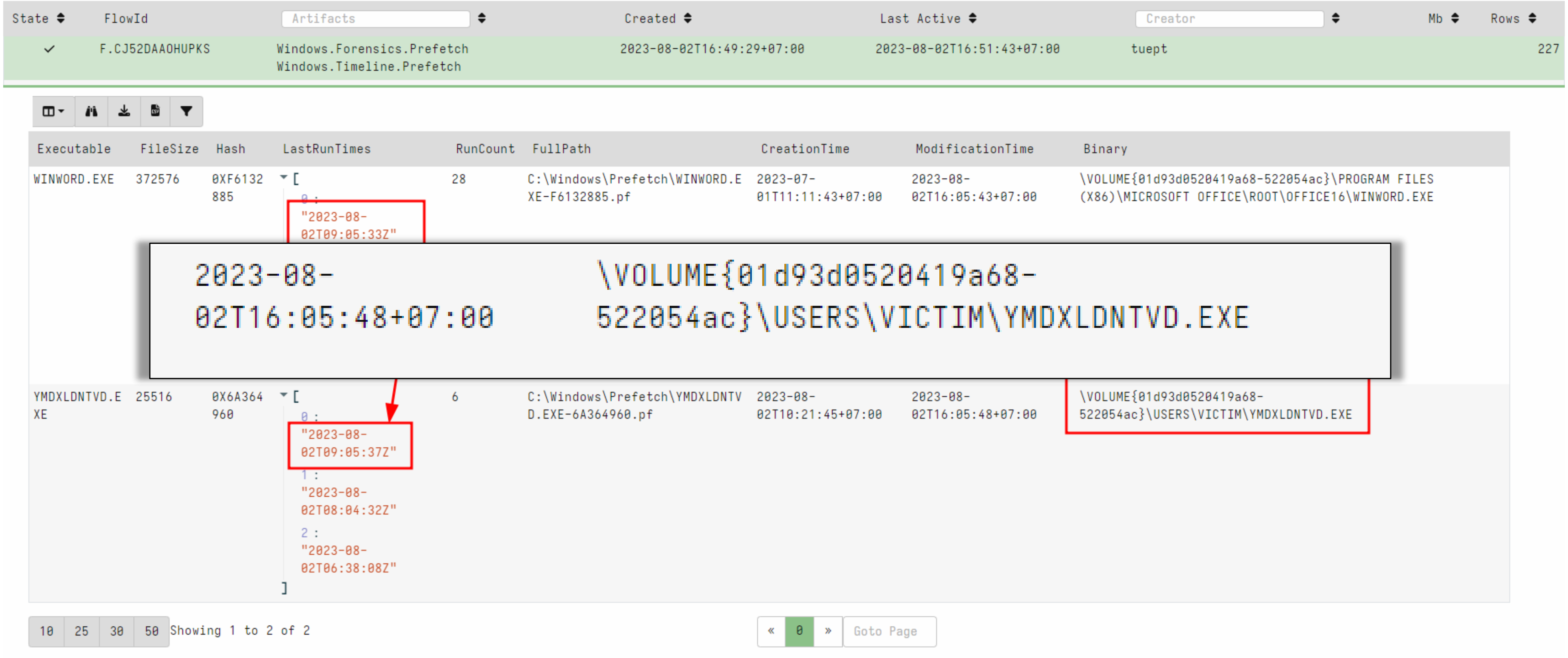
event_time	message
2023-08-02T13:38:03+07:00	Evidence of Execution: WINWORD.EXE Pre
2023-08-02T13:38:08+07:00	Evidence of Execution: YMDXLDNTVD.EXE

event_time						prefetch_count
2023-08-02T13:38:03+07:00						3
2023-08-02T13:38:08+07:00						6
2023-08-02T15:04:25+07:00						3
2023-08-02T15:04:32+07:00	HF5K7HM.localdomain	run count 6	6A364960.pf	02T10:21:45+07:00	02T16:05:48+07:00	6
2023-08-02T16:05:33+07:00	DESKTOP-HF5K7HM.localdomain	Evidence of Execution: WINWORD.EXE Prefetch run count 3	C:\Windows\Prefetch\WINWORD.EXE-F6132885.pf	2023-07-01T11:11:43+07:00	2023-08-02T16:05:43+07:00	3
2023-08-02T16:05:37+07:00	DESKTOP-HF5K7HM.localdomain	Evidence of Execution: YMDXLDNTVD.EXE Prefetch run count 6	C:\Windows\Prefetch\YMDXLDNTVD.EXE-6A364960.pf	2023-08-02T10:21:45+07:00	2023-08-02T16:05:48+07:00	6

Showing 141 to 6 of 6

Use-case 0x2: Collect Prefetch

@TueDenn



State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.CJ52DAAOHUPKS	Windows.Forensics.Prefetch Windows.Timeline.Prefetch	2023-08-02T16:49:29+07:00	2023-08-02T16:51:43+07:00	tuept		227

Executable	FileSize	Hash	LastRunTimes	RunCount	FullPath	CreationTime	ModificationTime	Binary
WINWORD.EXE	372576	0XF6132885	[0 : "2023-08-02T09:05:33Z"	28	C:\Windows\Prefetch\WINWORD.EXE-F6132885.pf	2023-07-01T11:11:43+07:00	2023-08-02T16:05:43+07:00	\VOLUME{01d93d0520419a68-522054ac}\PROGRAM FILES (X86)\MICROSOFT OFFICE\ROOT\OFFICE16\WINWORD.EXE
YMDXLDNTVD.EXE	25516	0X6A364960	[0 : "2023-08-02T09:05:37Z" 1 : "2023-08-02T08:04:32Z" 2 : "2023-08-02T06:38:08Z"]	6	C:\Windows\Prefetch\YMDXLDNTVD.EXE-6A364960.pf	2023-08-02T10:21:45+07:00	2023-08-02T16:05:48+07:00	\VOLUME{01d93d0520419a68-522054ac}\USERS\VICTIM\YMDXLDNTVD.EXE

2023-08-02T16:05:48+07:00 \VOLUME{01d93d0520419a68-522054ac}\USERS\VICTIM\YMDXLDNTVD.EXE

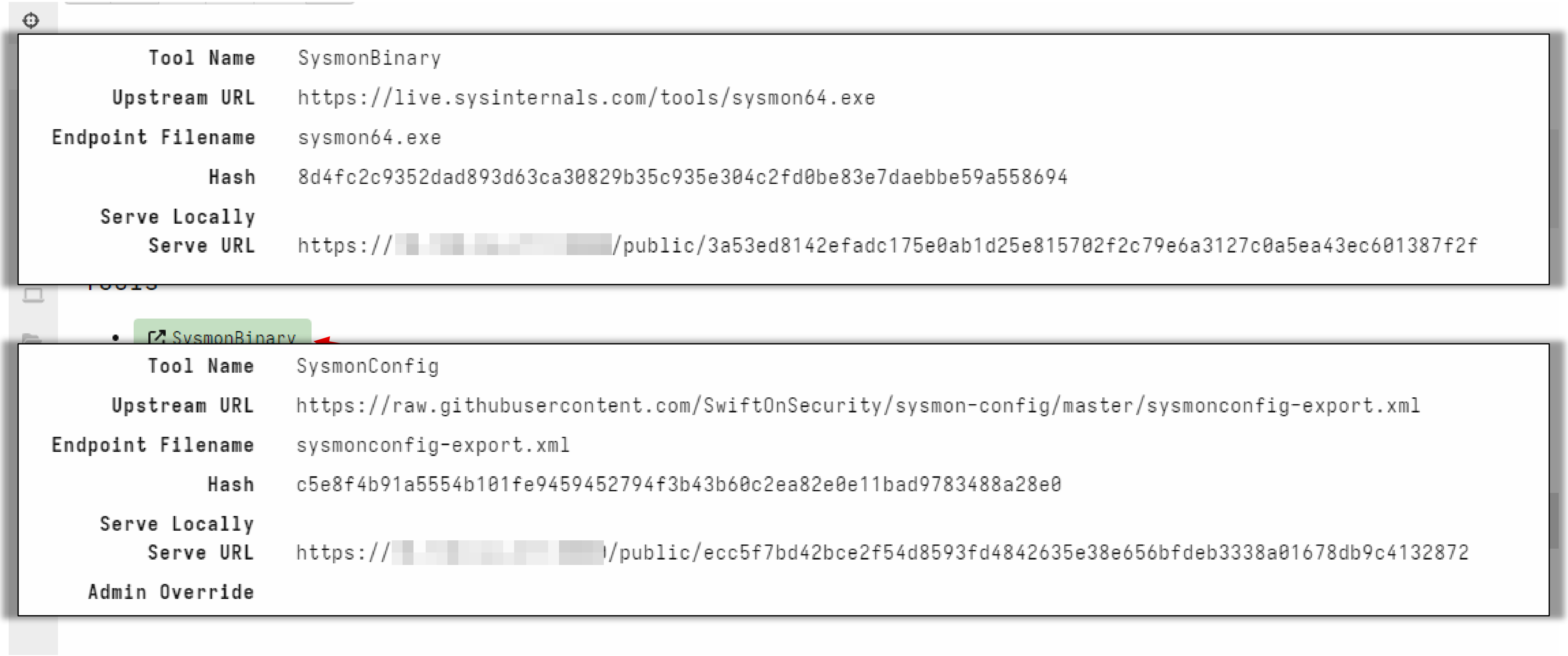
10 25 30 50 Showing 1 to 2 of 2

Use-case 0x3: Continuous monitoring with Sysmon

- Scenario:
  - There is no monitoring service running on this computer
  - Install Sysmon for increase event logging (*visibility*)
- Todo List:
  - Prepare Sysmon config file
  - In each endpoint, download and install Sysmon
- Velociraptor
  - Use Windows.Sysinternals.SysmonLogForward
  - or Windows.Sysinternals.SysmonInstall
  - Use Elastic.Events.Clients to forward to Elastic (*if needed*)

Use-case 0x3: Continuous monitoring with Sysmon

@TueDenn

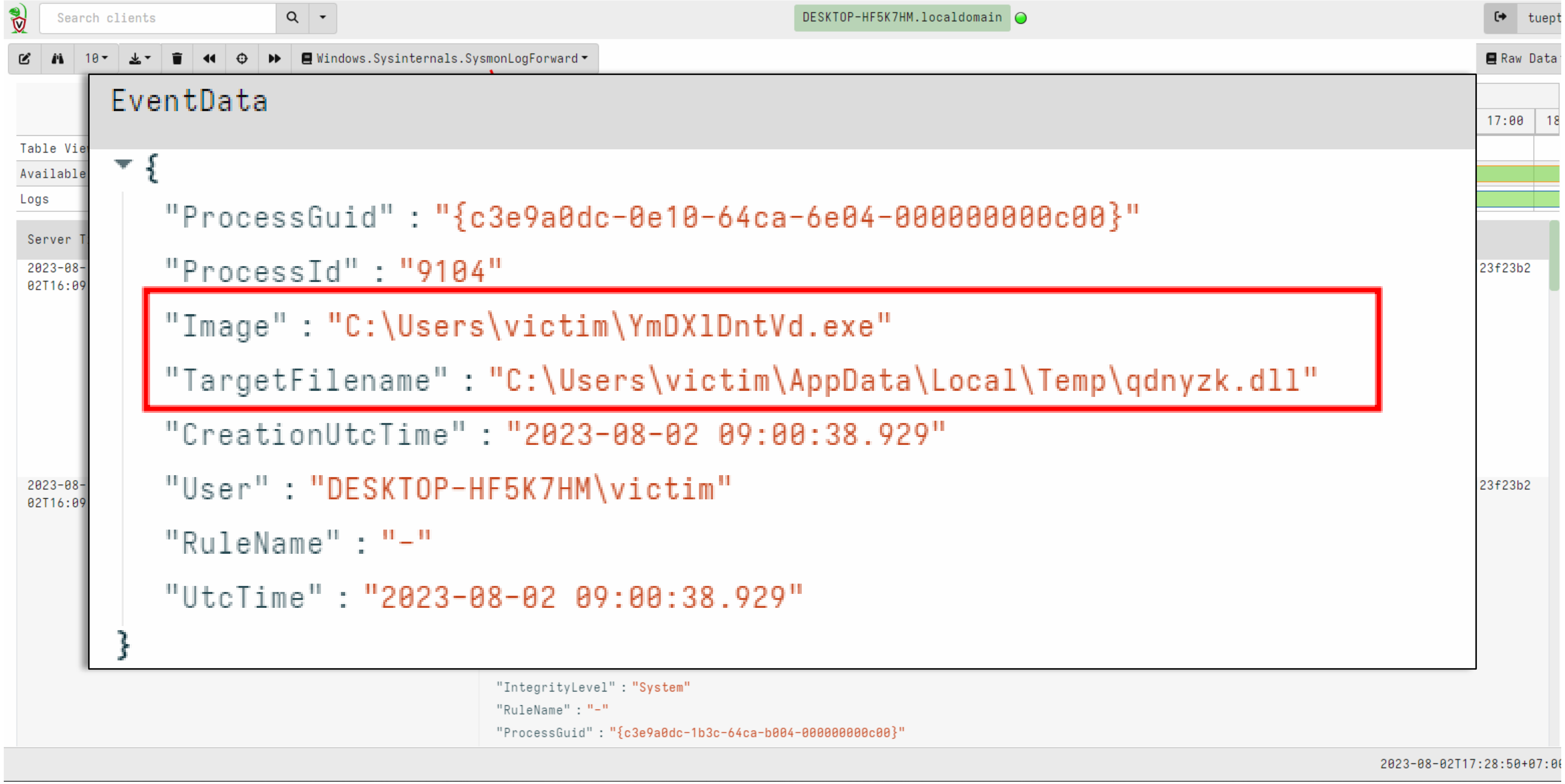


Tool Name	SysmonBinary
Upstream URL	https://live.sysinternals.com/tools/sysmon64.exe
Endpoint Filename	sysmon64.exe
Hash	8d4fc2c9352dad893d63ca30829b35c935e304c2fd0be83e7daebbe59a558694
Serve Locally	
Serve URL	https://[redacted]/public/3a53ed8142efadc175e0ab1d25e815702f2c79e6a3127c0a5ea43ec601387f2f

Tool Name	SysmonConfig
Upstream URL	https://raw.githubusercontent.com/SwiftOnSecurity/sysmon-config/master/sysmonconfig-export.xml
Endpoint Filename	sysmonconfig-export.xml
Hash	c5e8f4b91a5554b101fe9459452794f3b43b60c2ea82e0e11bad9783488a28e0
Serve Locally	
Serve URL	https://[redacted]/public/ecc5f7bd42bce2f54d8593fd4842635e38e656bfdeb3338a01678db9c4132872
Admin Override	

Use-case 0x3: Continuous monitoring with Sysmon

@TueDenn



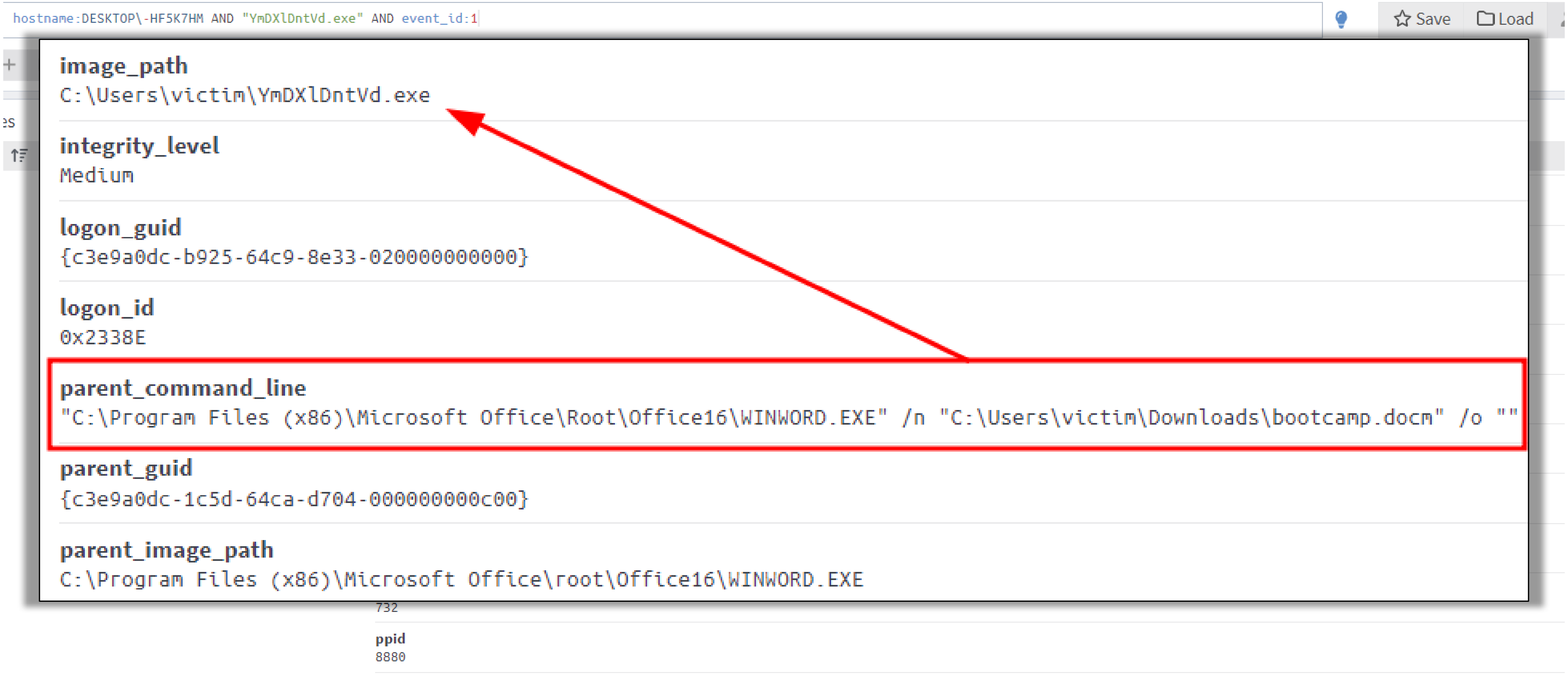
EventData

```
{
  "ProcessGuid" : "{c3e9a0dc-0e10-64ca-6e04-000000000c00}"
  "ProcessId" : "9104"
  "Image" : "C:\Users\victim\YmDX1DntVd.exe"
  "TargetFilename" : "C:\Users\victim\AppData\Local\Temp\qdnyzk.dll"
  "CreationUtcTime" : "2023-08-02 09:00:38.929"
  "User" : "DESKTOP-HF5K7HM\victim"
  "RuleName" : "-"
  "UtcTime" : "2023-08-02 09:00:38.929"
}
```

```
2023-08-
02T16:09
23f23b2
2023-08-
02T16:09
23f23b2
"IntegrityLevel" : "System"
"RuleName" : "-"
"ProcessGuid" : "{c3e9a0dc-1b3c-64ca-b004-000000000c00}"
2023-08-02T17:28:50+07:0
```

Use-case 0x3: Continuous monitoring with Sysmon

@TueDenn



```
hostname:DESKTOP\-HF5K7HM AND "YmDXlDntVd.exe" AND event_id:1
```

image_path
C:\Users\victim\YmDXlDntVd.exe

integrity_level
Medium

logon_guid
{c3e9a0dc-b925-64c9-8e33-020000000000}

logon_id
0x2338E

parent_command_line
"C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\victim\Downloads\bootcamp.docm" /o ""

parent_guid
{c3e9a0dc-1c5d-64ca-d704-000000000c00}

parent_image_path
C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE

732

ppid
8880

One thing to remember!

@TueDenn

Velociraptor has a lot more than we were able to cover here

1. Many more sources of data: Event logs, ETW, WMI event
2. Multi-Platform: Linux, MacOS, Windows, FreeBSD
3. Endpoint monitoring in real time
4. Automatic remediation: Apply active remediation
5. Server automation and monitoring in real time: Python API
6. Etc.

One thing to remember!

SUMMARY – Key Takeaways

- DFIR is a valued part of a successful defense strategy
  - Help fully understand the situation (know the enemy and know yourself)
  - Without DFIR, the game will be like “*What a mole*”
- Opensource tool can help maximum DFIR values, eg Velociraptor
  - Low cost
  - Hunting, Monitoring, Forensic, Response capabilities
  - By DFIR, for DFIR → Reuse/share expert knowledge
  - Goal to automate DFIR tasks as much as possible
  - Fast, Powerful, Flexible via Query Language (VQL)
  - New approach for efficiency DFIR
- The bottom line is people, you need someone
  - Have a skill set about DFIR
  - Have responsibility for tame the Velociraptor

SUMMARY

THANKS

FOR YOUR ATTENDANCE!