Velociraptor for Incident Response

ISACA®

San Francisco Chapter

2021 SF ISACA Fall Conference

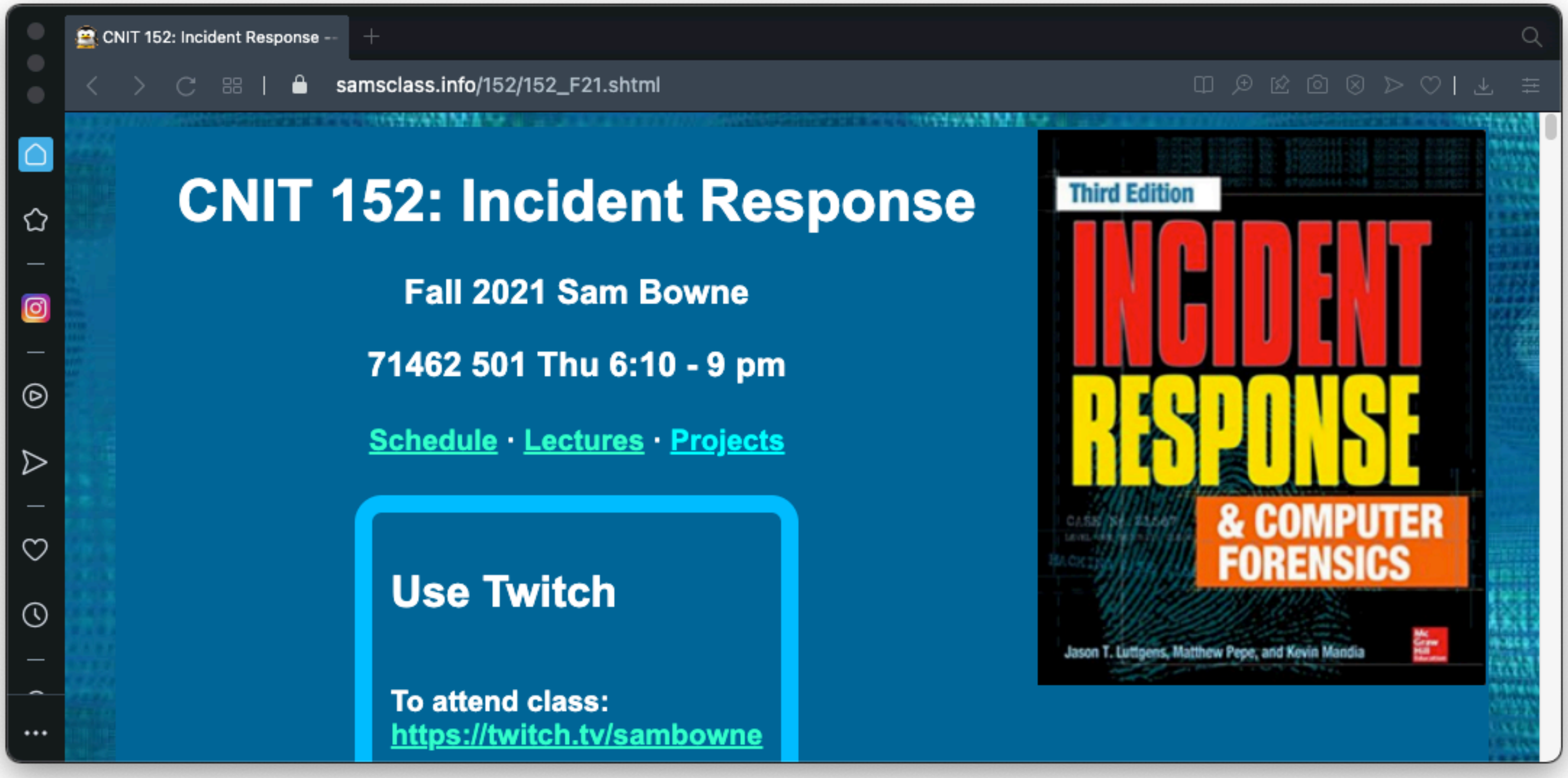
Sam Bowne, Oct 26, 2021

Bio

- Instructor at City College San Francisco
- Founder of Infosec Decoded, Inc.
  - Custom security training for corporations
- Presented at DEF CON, Black Hat, HOPE, etc.

Materials

- This talk and all the materials for these projects are freely available at **samsclass.info**



CNIT 152: Incident Response --
samsclass.info/152/152_F21.shtml
Third Edition
INCIDENT RESPONSE
& COMPUTER FORENSICS
Jason T. Luttgens, Matthew Pepe, and Kevin Mandia

CNIT 152: Incident Response

Fall 2021 Sam Bowne

71462 501 Thu 6:10 - 9 pm

Schedule · Lectures · Projects

Use Twitch

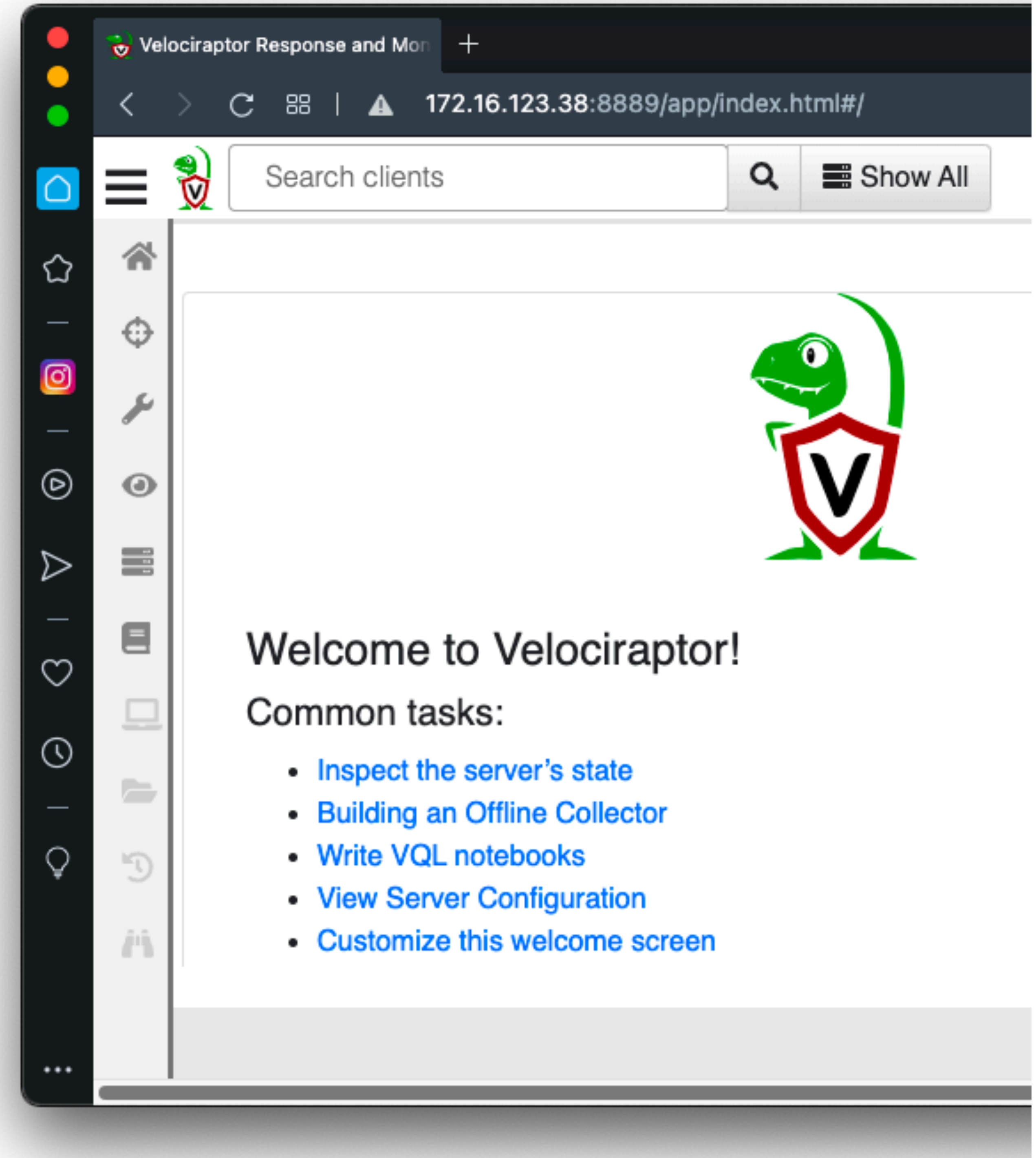
To attend class:
https://twitch.tv/sambowne

Incident Response

- Large network of computers
- An incident is reported
  - Such as a malware infection
- Scope: how big is the problem?

Velociraptor

- A central server to perform IR tasks
- Collecting data from endpoints
- Hunting for Indicators of Compromise

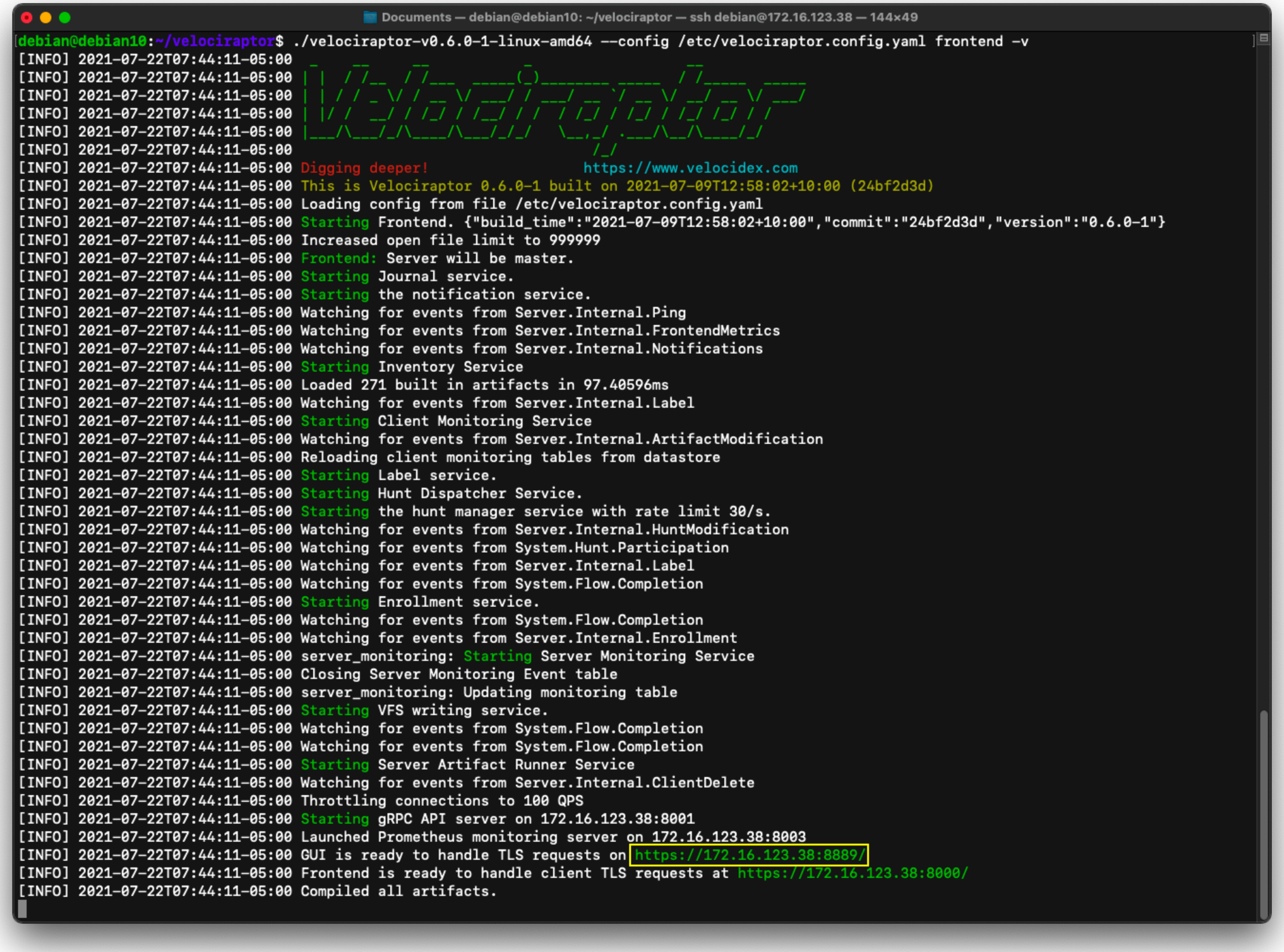

Velociraptor Response and Mon
172.16.123.38:8889/app/index.html#/
Search clients
Show All

Welcome to Velociraptor!

Common tasks:

- Inspect the server's state
- Building an Offline Collector
- Write VQL notebooks
- View Server Configuration
- Customize this welcome screen

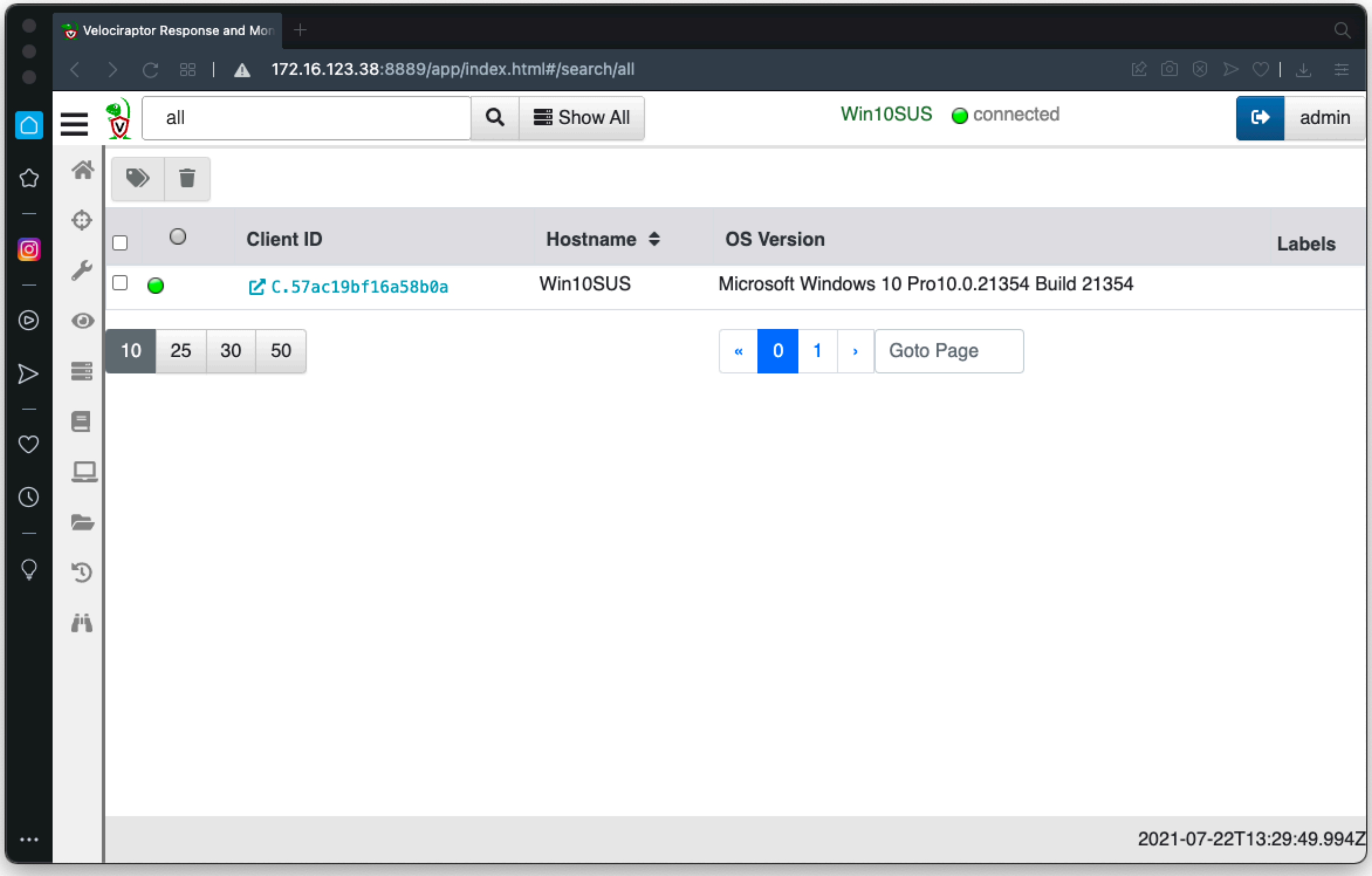
Simple Server



Documents — debian@debian10: ~/velociraptor — ssh debian@172.16.123.38 — 144×49

```
debian@debian10:~/velociraptor$ ./velociraptor-v0.6.0-1-linux-amd64 --config /etc/velociraptor.config.yaml frontend -v
[INFO] 2021-07-22T07:44:11-05:00  _    __     __           _                __
[INFO] 2021-07-22T07:44:11-05:00 | |  / /__  / /___  _____(_)________ _____  / /_____  _____
[INFO] 2021-07-22T07:44:11-05:00 | | / / _ \/ / __ \/ ___/ / ___/ __ `/ __ \/ __/ __ \/ ___/
[INFO] 2021-07-22T07:44:11-05:00 | |/ /  __/ / /_/ / /__/ / /  / /_/ / /_/ / /_/ /_/ / /
[INFO] 2021-07-22T07:44:11-05:00 |___/\___/_/\____/\___/_/_/   \__,_/ .___/\__/\____/_/
[INFO] 2021-07-22T07:44:11-05:00                                   /_/
[INFO] 2021-07-22T07:44:11-05:00 Digging deeper!                  https://www.velocidex.com
[INFO] 2021-07-22T07:44:11-05:00 This is Velociraptor 0.6.0-1 built on 2021-07-09T12:58:02+10:00 (24bf2d3d)
[INFO] 2021-07-22T07:44:11-05:00 Loading config from file /etc/velociraptor.config.yaml
[INFO] 2021-07-22T07:44:11-05:00 Starting Frontend. {"build_time":"2021-07-09T12:58:02+10:00","commit":"24bf2d3d","version":"0.6.0-1"}
[INFO] 2021-07-22T07:44:11-05:00 Increased open file limit to 999999
[INFO] 2021-07-22T07:44:11-05:00 Frontend: Server will be master.
[INFO] 2021-07-22T07:44:11-05:00 Starting Journal service.
[INFO] 2021-07-22T07:44:11-05:00 Starting the notification service.
[INFO] 2021-07-22T07:44:11-05:00 Watching for events from Server.Internal.Ping
[INFO] 2021-07-22T07:44:11-05:00 Watching for events from Server.Internal.FrontendMetrics
[INFO] 2021-07-22T07:44:11-05:00 Watching for events from Server.Internal.Notifications
[INFO] 2021-07-22T07:44:11-05:00 Starting Inventory Service
[INFO] 2021-07-22T07:44:11-05:00 Loaded 271 built in artifacts in 97.40596ms
[INFO] 2021-07-22T07:44:11-05:00 Watching for events from Server.Internal.Label
[INFO] 2021-07-22T07:44:11-05:00 Starting Client Monitoring Service
[INFO] 2021-07-22T07:44:11-05:00 Watching for events from Server.Internal.ArtifactModification
[INFO] 2021-07-22T07:44:11-05:00 Reloading client monitoring tables from datastore
[INFO] 2021-07-22T07:44:11-05:00 Starting Label service.
[INFO] 2021-07-22T07:44:11-05:00 Starting Hunt Dispatcher Service.
[INFO] 2021-07-22T07:44:11-05:00 Starting the hunt manager service with rate limit 30/s.
[INFO] 2021-07-22T07:44:11-05:00 Watching for events from Server.Internal.HuntModification
[INFO] 2021-07-22T07:44:11-05:00 Watching for events from System.Hunt.Participation
[INFO] 2021-07-22T07:44:11-05:00 Watching for events from Server.Internal.Label
[INFO] 2021-07-22T07:44:11-05:00 Watching for events from System.Flow.Completion
[INFO] 2021-07-22T07:44:11-05:00 Starting Enrollment service.
[INFO] 2021-07-22T07:44:11-05:00 Watching for events from System.Flow.Completion
[INFO] 2021-07-22T07:44:11-05:00 Watching for events from Server.Internal.Enrollment
[INFO] 2021-07-22T07:44:11-05:00 server_monitoring: Starting Server Monitoring Service
[INFO] 2021-07-22T07:44:11-05:00 Closing Server Monitoring Event table
[INFO] 2021-07-22T07:44:11-05:00 server_monitoring: Updating monitoring table
[INFO] 2021-07-22T07:44:11-05:00 Starting VFS writing service.
[INFO] 2021-07-22T07:44:11-05:00 Watching for events from System.Flow.Completion
[INFO] 2021-07-22T07:44:11-05:00 Watching for events from System.Flow.Completion
[INFO] 2021-07-22T07:44:11-05:00 Starting Server Artifact Runner Service
[INFO] 2021-07-22T07:44:11-05:00 Watching for events from Server.Internal.ClientDelete
[INFO] 2021-07-22T07:44:11-05:00 Throttling connections to 100 QPS
[INFO] 2021-07-22T07:44:11-05:00 Starting gRPC API server on 172.16.123.38:8001
[INFO] 2021-07-22T07:44:11-05:00 Launched Prometheus monitoring server on 172.16.123.38:8003
[INFO] 2021-07-22T07:44:11-05:00 GUI is ready to handle TLS requests on https://172.16.123.38:8889/
[INFO] 2021-07-22T07:44:11-05:00 Frontend is ready to handle client TLS requests at https://172.16.123.38:8000/
[INFO] 2021-07-22T07:44:11-05:00 Compiled all artifacts.
```

Windows Client

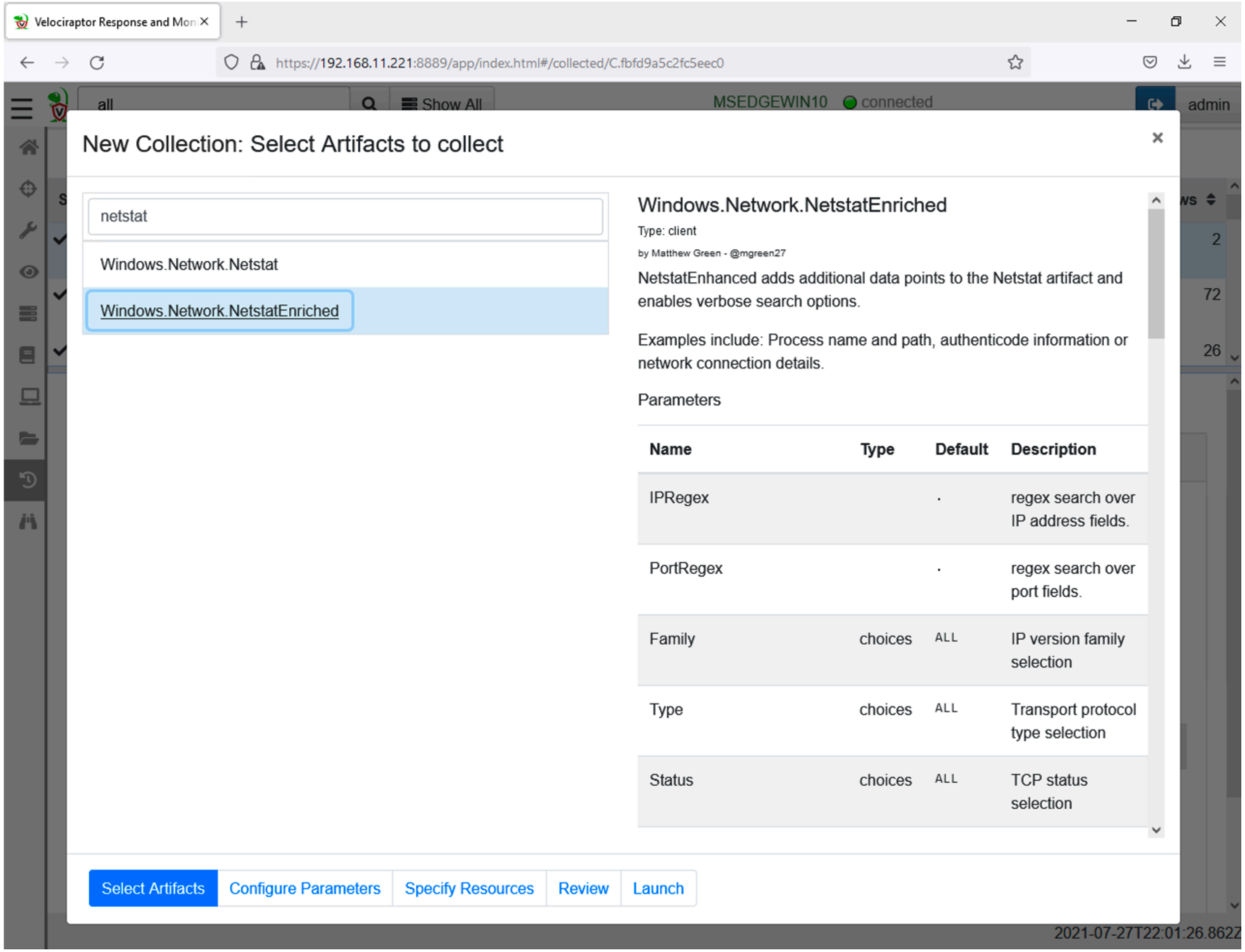


Velociraptor Response and Mon
172.16.123.38:8889/app/index.html#/search/all
all
Show All
Win10SUS
connected
admin
10
25
30
50
«
0
1
›
Goto Page

□	○	Client ID	Hostname	OS Version	Labels
□	●	C.57ac19bf16a58b0a	Win10SUS	Microsoft Windows 10 Pro10.0.21354 Build 21354	

2021-07-22T13:29:49.994Z

Demo: Artifacts


Velociraptor Response and Mon
https://192.168.11.221:8889/app/index.html#/collected/C.fbfd9a5c2fc5eec0
all
Show All
MSEDGEWIN10
connected
admin

New Collection: Select Artifacts to collect

netstat

Windows.Network.Netstat

Windows.Network.NetstatEnriched

Windows.Network.NetstatEnriched

Type: client

by Matthew Green - @mgreen27

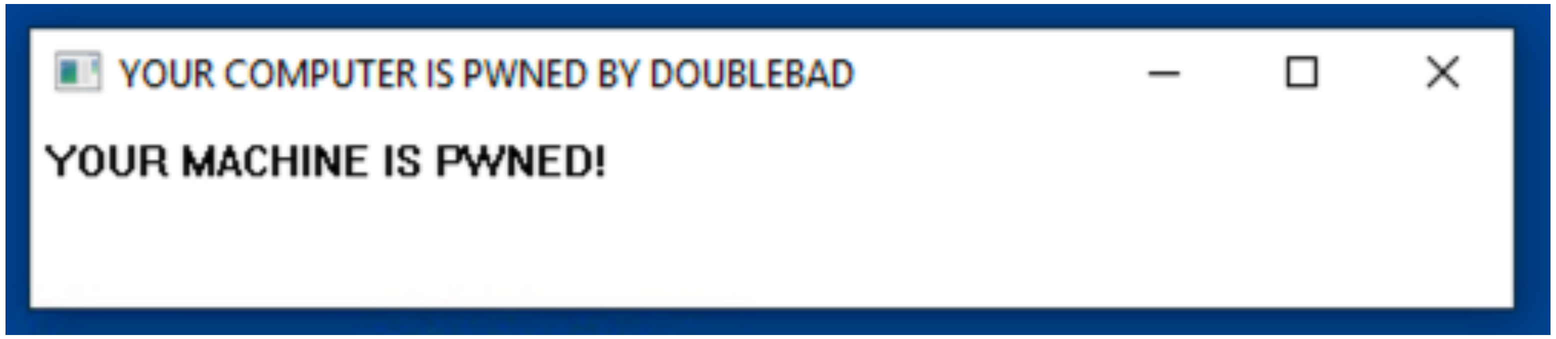
NetstatEnhanced adds additional data points to the Netstat artifact and enables verbose search options.

Examples include: Process name and path, authenticode information or network connection details.

Parameters

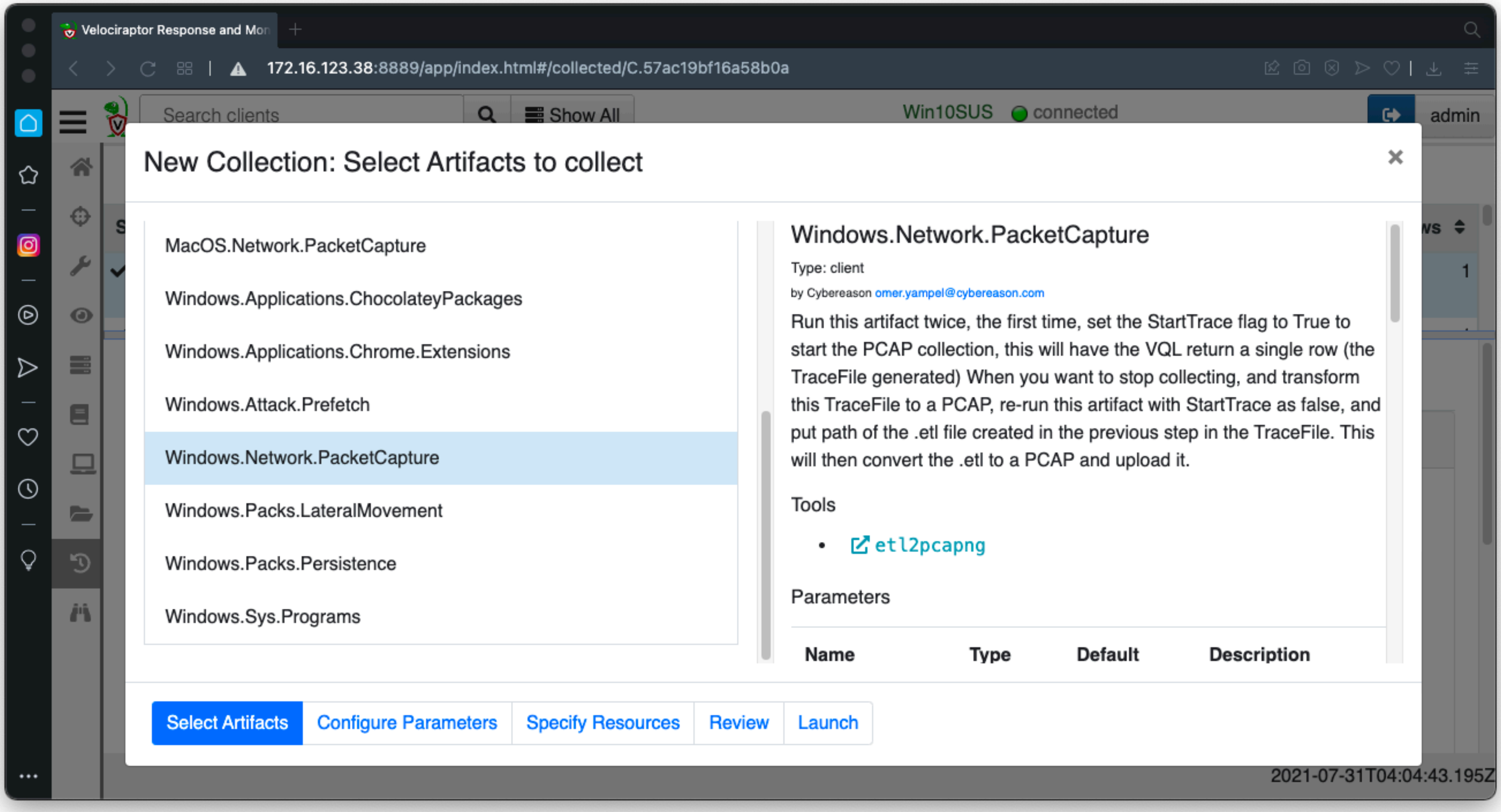
Name	Type	Default	Description
IPRegex		.	regex search over IP address fields.
PortRegex		.	regex search over port fields.
Family	choices	ALL	IP version family selection
Type	choices	ALL	Transport protocol type selection
Status	choices	ALL	TCP status selection

Demo: PUP



YOUR MACHINE IS PWNED!

Demo: Bot



Velociraptor Response and Mon
172.16.123.38:8889/app/index.html#/collected/C.57ac19bf16a58b0a
Search clients
Show All
Win10SUS
connected
admin

New Collection: Select Artifacts to collect

- MacOS.Network.PacketCapture
- Windows.Applications.ChocolateyPackages
- Windows.Applications.Chrome.Extensions
- Windows.Attack.Prefetch
- Windows.Network.PacketCapture
- Windows.Packs.LateralMovement
- Windows.Packs.Persistence
- Windows.Sys.Programs

Windows.Network.PacketCapture

Type: client

by Cybereason omer.yampel@cybereason.com

Run this artifact twice, the first time, set the StartTrace flag to True to start the PCAP collection, this will have the VQL return a single row (the TraceFile generated) When you want to stop collecting, and transform this TraceFile to a PCAP, re-run this artifact with StartTrace as false, and put path of the .etl file created in the previous step in the TraceFile. This will then convert the .etl to a PCAP and upload it.

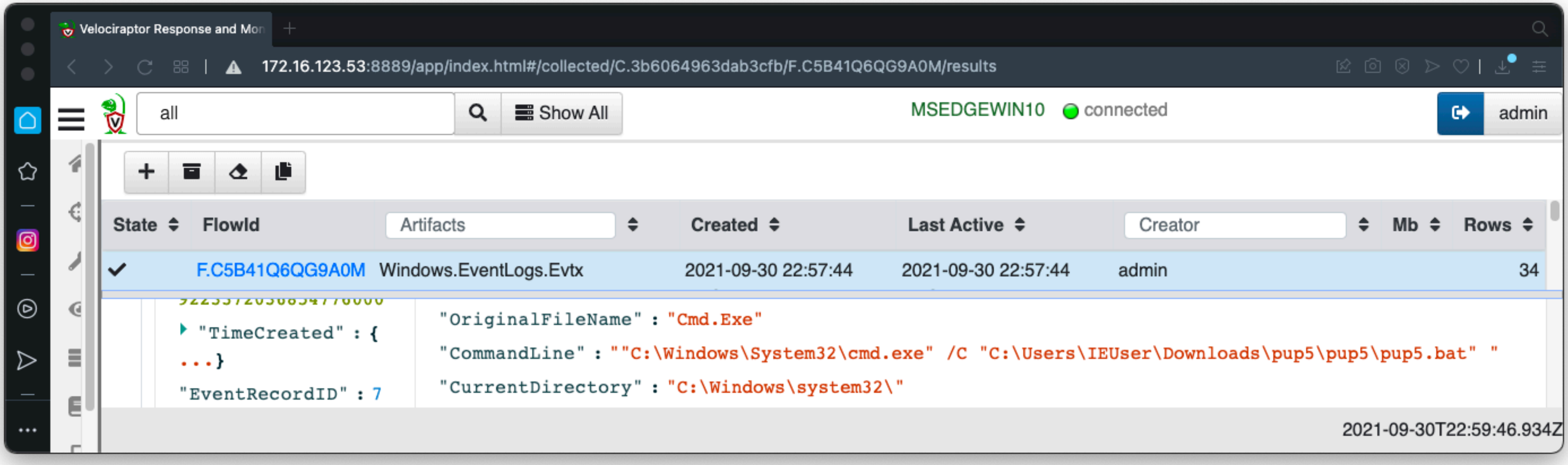
Tools

- etl2pcapng

Parameters

Name	Type	Default	Description

Demo: RAT


Velociraptor Response and Mon
172.16.123.53:8889/app/index.html#/collected/C.3b6064963dab3cfb/F.C5B41Q6QG9A0M/results
all
Show All
MSEDGEWIN10
connected
admin

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.C5B41Q6QG9A0M	Windows.EventLogs.Evtx	2021-09-30 22:57:44	2021-09-30 22:57:44	admin		34

```
9223372036854776000
"TimeCreated" : {
...}
"EventRecordID" : 7
```

```
"OriginalFileName" : "Cmd.Exe"
"CommandLine" : ""C:\Windows\System32\cmd.exe" /C "C:\Users\IEUser\Downloads\pup5\pup5\pup5.bat" "
"CurrentDirectory" : "C:\Windows\system32\"
```

2021-09-30T22:59:46.934Z

Questions