Project Obsidian

Creating a Velociraptor Collector

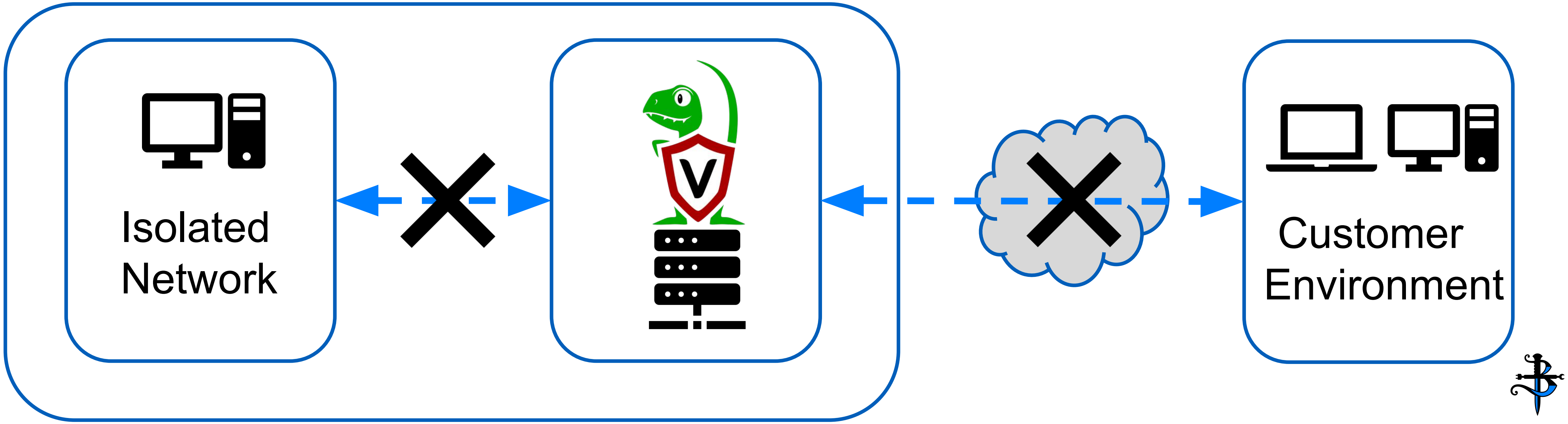
Wes Lambert
@therealwlambert

Overview

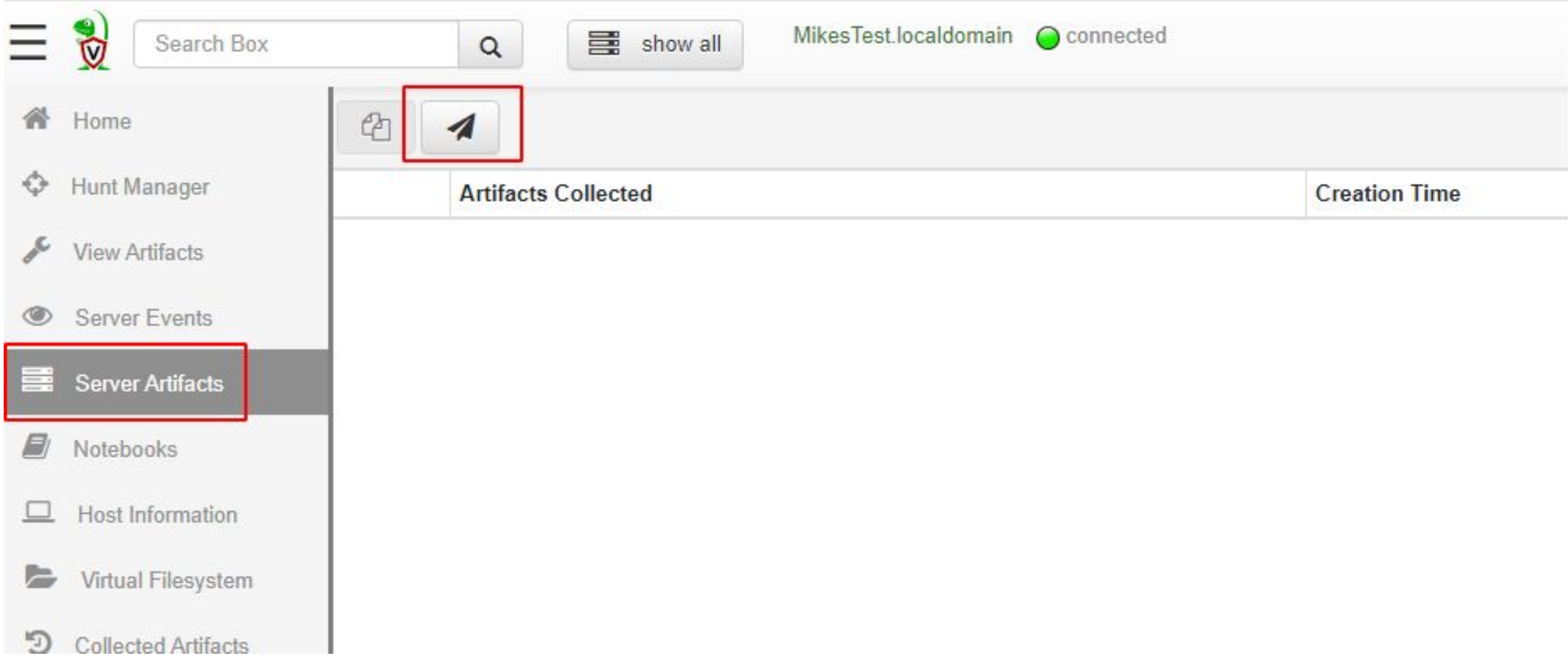
- Why?
- Create offline collector
- Place collector on host
- Run collector
- Obtain collection
- Import collection into the server

Why?

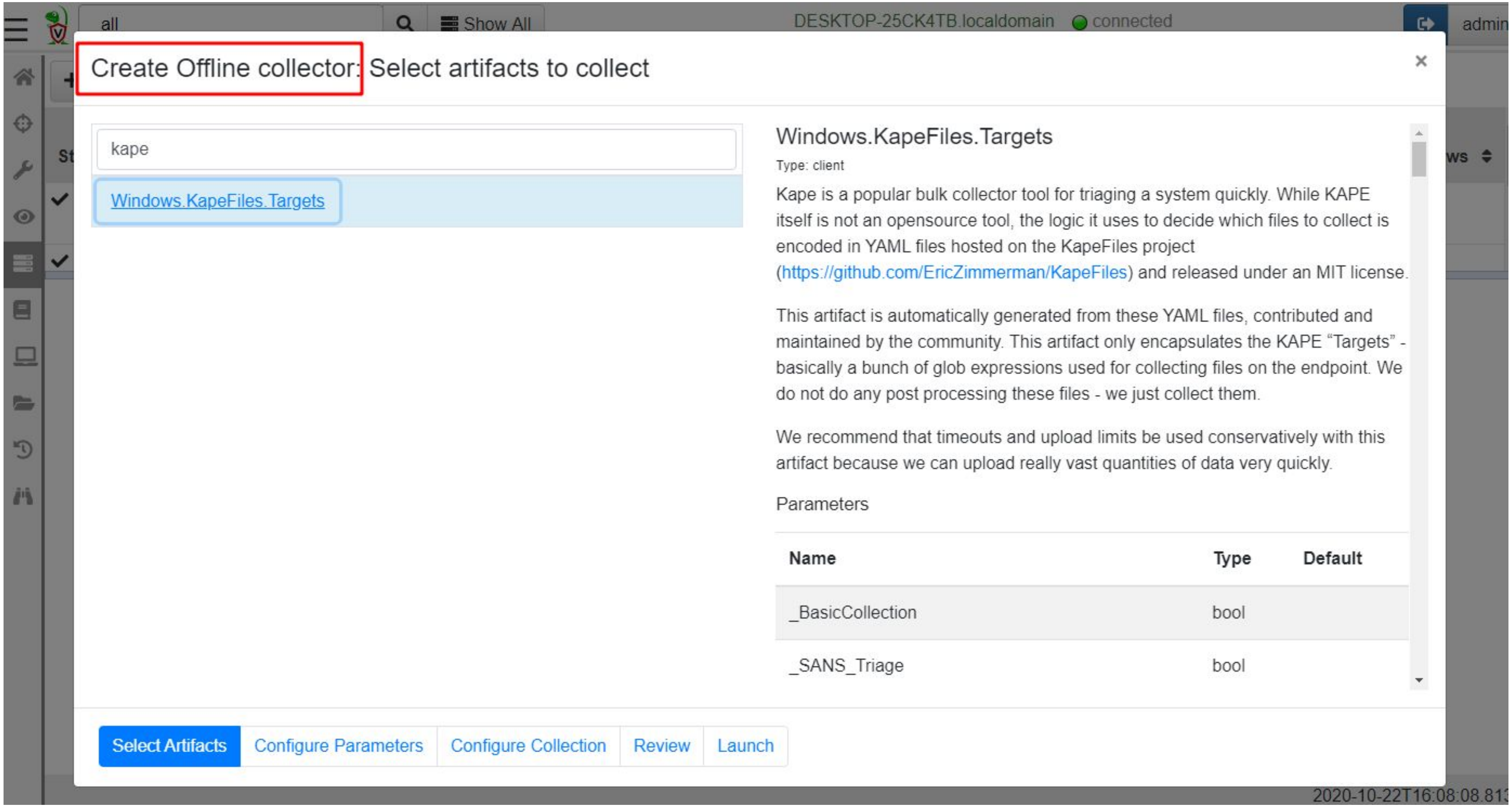
- Hosts in isolated networks
- Customer environments
- Inability or reluctance to install a local service



Create offline collector



https://docs.velociraptor.app/docs/offline_triage/#offline-collections



Create Offline collector: Select artifacts to collect

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.

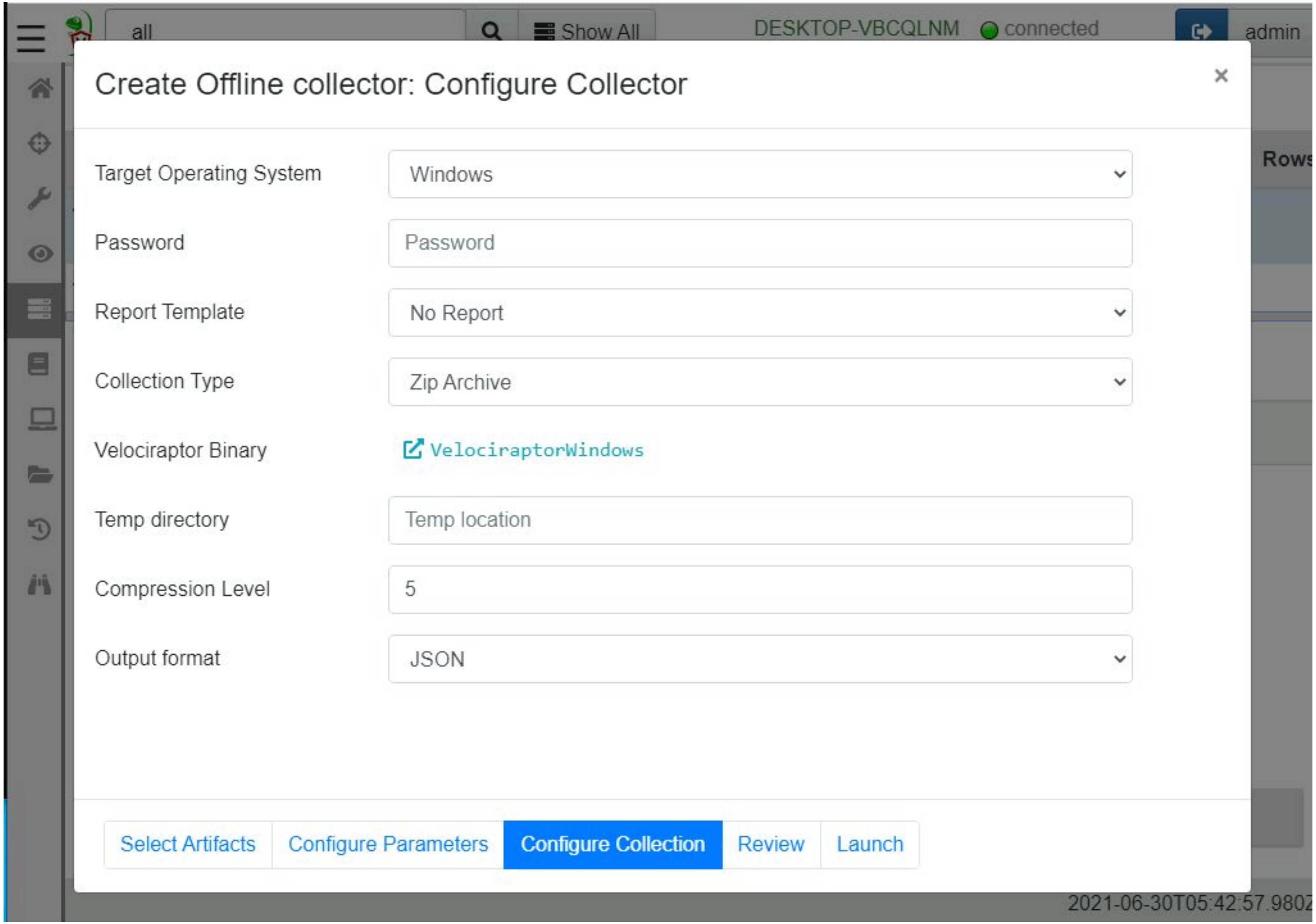
This artifact is automatically generated from these YAML files, contributed and maintained by the community. This artifact only encapsulates the KAPE “Targets” - basically a bunch of glob expressions used for collecting files on the endpoint. We do not do any post processing these files - we just collect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

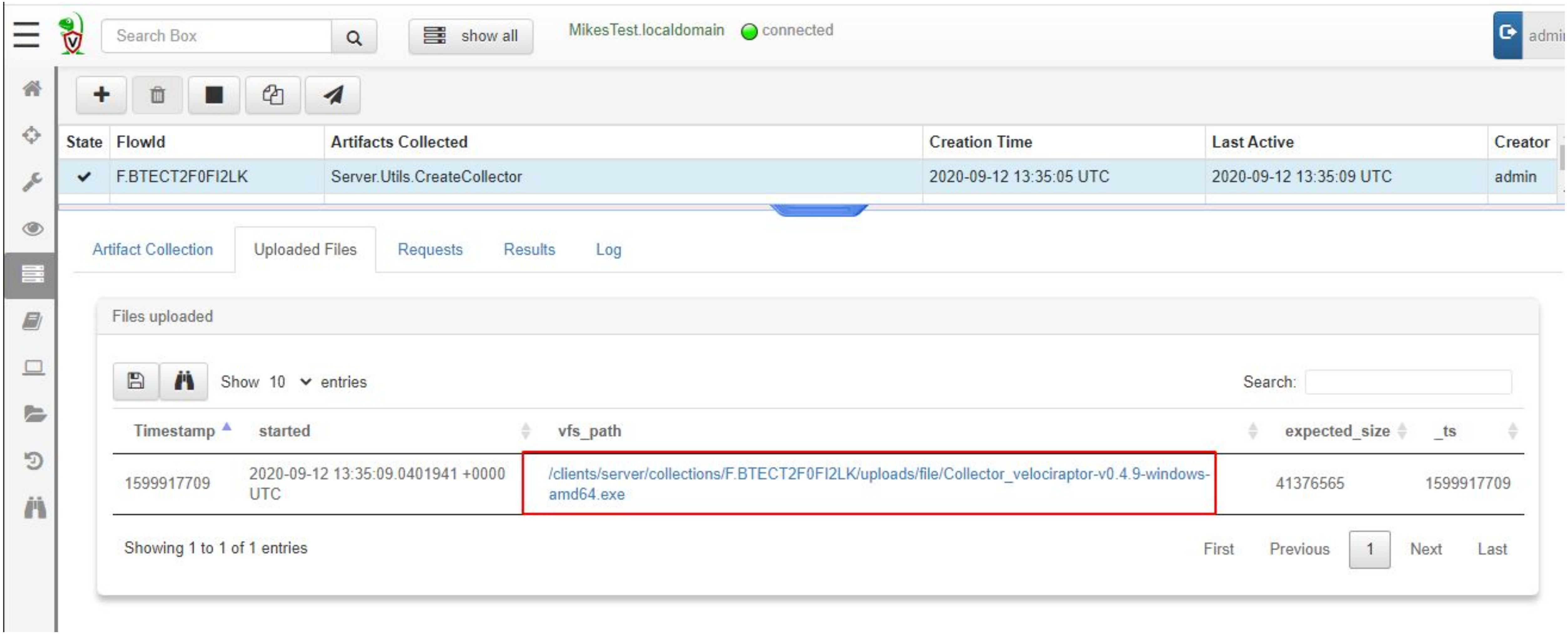
https://docs.velociraptor.app/docs/offline_triage/#offline-collections



Create Offline collector: Configure Collector

Target Operating System	Windows
Password	Password
Report Template	No Report
Collection Type	Zip Archive
Velociraptor Binary	VelociraptorWindows
Temp directory	Temp location
Compression Level	5
Output format	JSON

https://docs.velociraptor.app/docs/offline_triage/#offline-collections

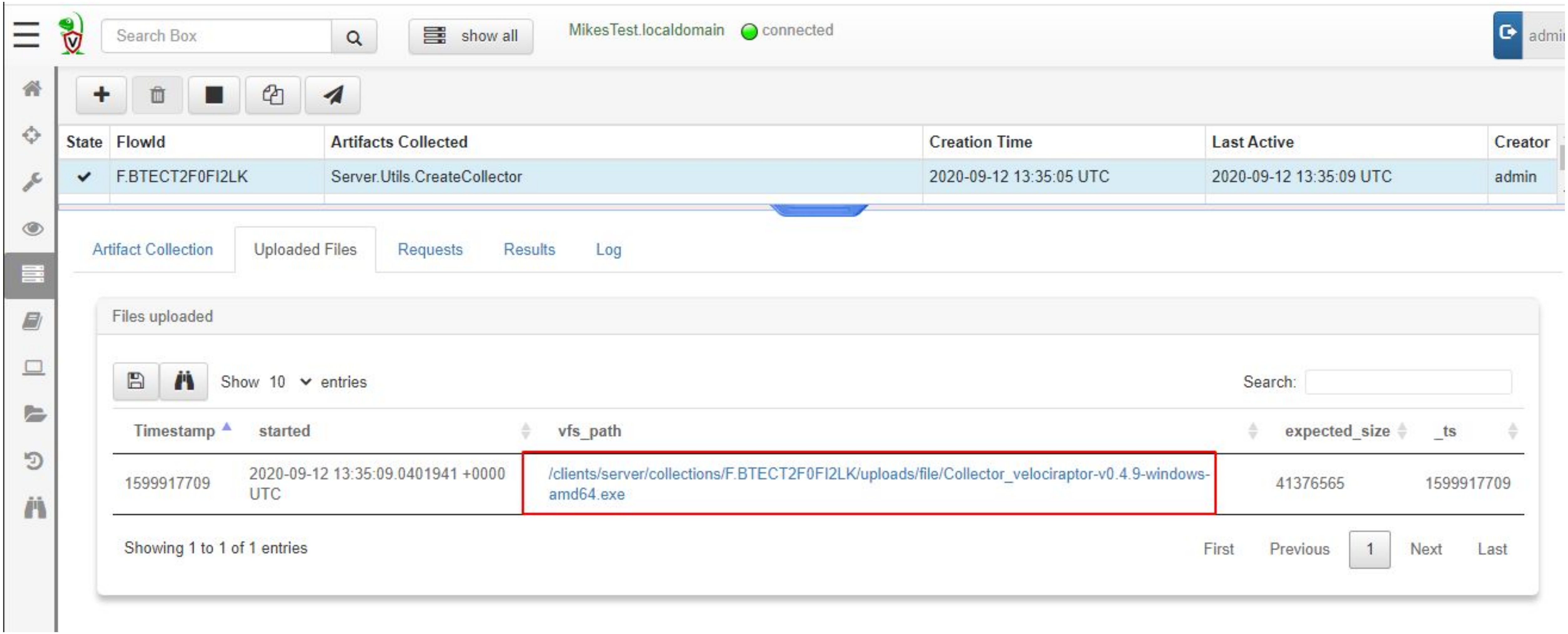


State	FlowId	Artifacts Collected	Creation Time	Last Active	Creator
✓	F.BTECT2F0FI2LK	Server.Utils.CreateCollector	2020-09-12 13:35:05 UTC	2020-09-12 13:35:09 UTC	admin

Timestamp	started	vfs_path	expected_size	_ts
1599917709	2020-09-12 13:35:09.0401941 +0000 UTC	/clients/server/collections/F.BTECT2F0FI2LK/uploads/file/Collector_velociraptor-v0.4.9-windows-amd64.exe	41376565	1599917709

Showing 1 to 1 of 1 entries

https://docs.velociraptor.app/docs/offline_triage/#offline-collections



State	FlowId	Artifacts Collected	Creation Time	Last Active	Creator
✓	F.BTECT2F0FI2LK	Server.Utils.CreateCollector	2020-09-12 13:35:05 UTC	2020-09-12 13:35:09 UTC	admin

Files uploaded

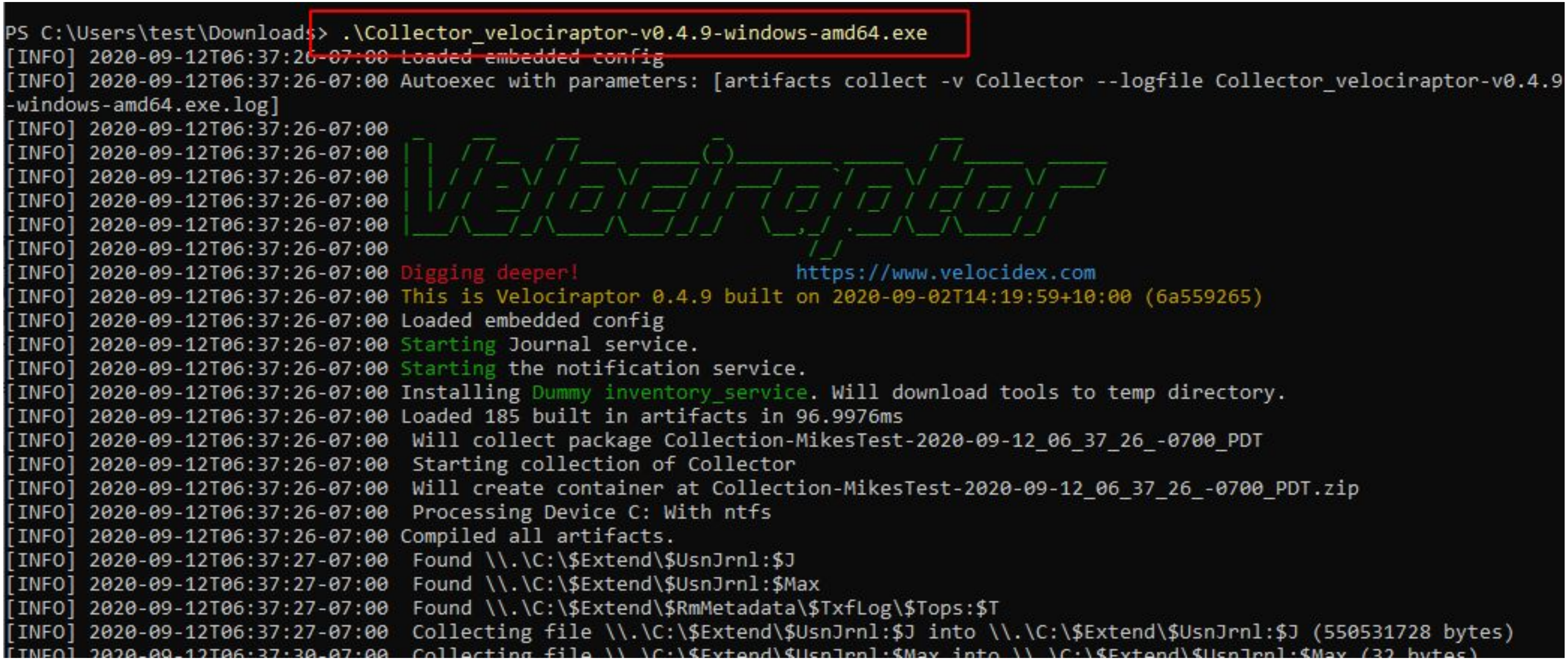
Timestamp	started	vfs_path	expected_size	_ts
1599917709	2020-09-12 13:35:09.0401941 +0000 UTC	/clients/server/collections/F.BTECT2F0FI2LK/uploads/file/Collector_velociraptor-v0.4.9-windows-amd64.exe	41376565	1599917709

Showing 1 to 1 of 1 entries

https://docs.velociraptor.app/docs/offline_triage/#offline-collections

Place collector on host

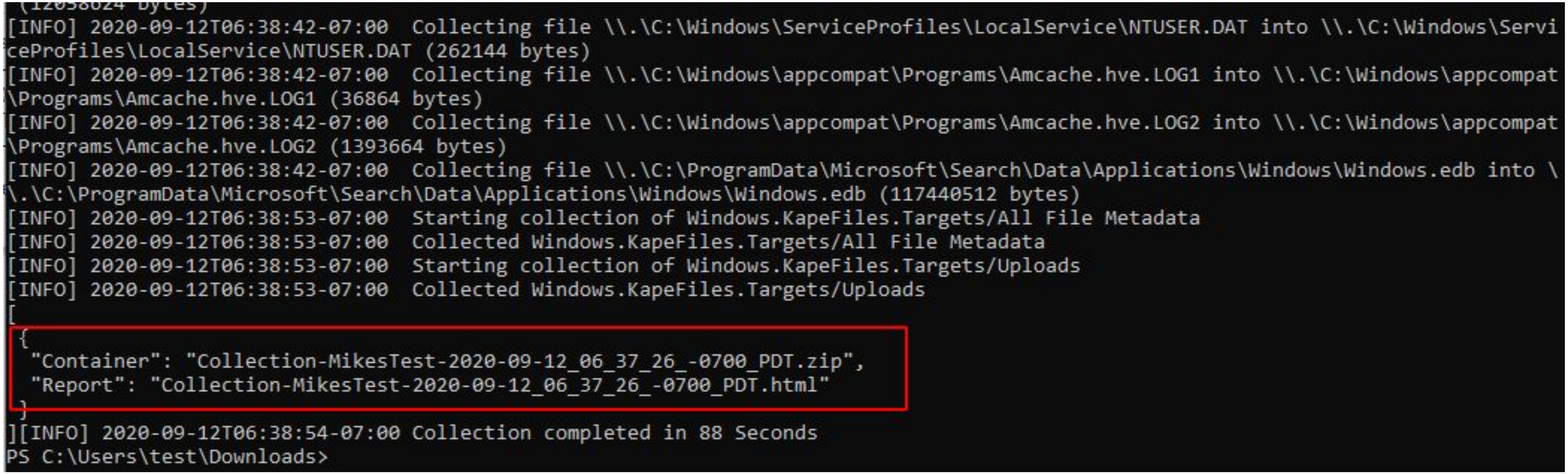
Run collector



```
PS C:\Users\test\Downloads> .\Collector_velociraptor-v0.4.9-windows-amd64.exe
[INFO] 2020-09-12T06:37:26-07:00 Loaded embedded config
[INFO] 2020-09-12T06:37:26-07:00 Autoexec with parameters: [artifacts collect -v Collector --logfile Collector_velociraptor-v0.4.9
-windows-amd64.exe.log]
[INFO] 2020-09-12T06:37:26-07:00  _    __     __           _                  __
[INFO] 2020-09-12T06:37:26-07:00 | |  / /__  / /___  _____(_)________ _____  / /_____  _____
[INFO] 2020-09-12T06:37:26-07:00 | | / / _ \/ / __ \/ ___/ / ___/ __ `/ __ \/ __/ __ \/ ___/
[INFO] 2020-09-12T06:37:26-07:00 | |/ /  __/ / /_/ / /__/ / /  / /_/ / /_/ / /_/ /_/ / /
[INFO] 2020-09-12T06:37:26-07:00 |___/\___/_/\____/\___/_/_/   \__,_/ .___/\__/\____/_/
[INFO] 2020-09-12T06:37:26-07:00                                   /_/
[INFO] 2020-09-12T06:37:26-07:00 Digging deeper!                  https://www.velocidex.com
[INFO] 2020-09-12T06:37:26-07:00 This is Velociraptor 0.4.9 built on 2020-09-02T14:19:59+10:00 (6a559265)
[INFO] 2020-09-12T06:37:26-07:00 Loaded embedded config
[INFO] 2020-09-12T06:37:26-07:00 Starting Journal service.
[INFO] 2020-09-12T06:37:26-07:00 Starting the notification service.
[INFO] 2020-09-12T06:37:26-07:00 Installing Dummy inventory_service. Will download tools to temp directory.
[INFO] 2020-09-12T06:37:26-07:00 Loaded 185 built in artifacts in 96.9976ms
[INFO] 2020-09-12T06:37:26-07:00  Will collect package Collection-MikesTest-2020-09-12_06_37_26_-0700_PDT
[INFO] 2020-09-12T06:37:26-07:00  Starting collection of Collector
[INFO] 2020-09-12T06:37:26-07:00  Will create container at Collection-MikesTest-2020-09-12_06_37_26_-0700_PDT.zip
[INFO] 2020-09-12T06:37:26-07:00  Processing Device C: With ntfs
[INFO] 2020-09-12T06:37:26-07:00 Compiled all artifacts.
[INFO] 2020-09-12T06:37:27-07:00  Found \\.\C:\$Extend\$UsnJrnl:$J
[INFO] 2020-09-12T06:37:27-07:00  Found \\.\C:\$Extend\$UsnJrnl:$Max
[INFO] 2020-09-12T06:37:27-07:00  Found \\.\C:\$Extend\$RmMetadata\$TxfLog\$Tops:$T
[INFO] 2020-09-12T06:37:27-07:00  Collecting file \\.\C:\$Extend\$UsnJrnl:$J into \\.\C:\$Extend\$UsnJrnl:$J (550531728 bytes)
[INFO] 2020-09-12T06:37:30-07:00  Collecting file \\.\C:\$Extend\$UsnJrnl:$Max into \\.\C:\$Extend\$UsnJrnl:$Max (32 bytes)
```

https://docs.velociraptor.app/docs/offline_triage/#offline-collections

Obtain collection

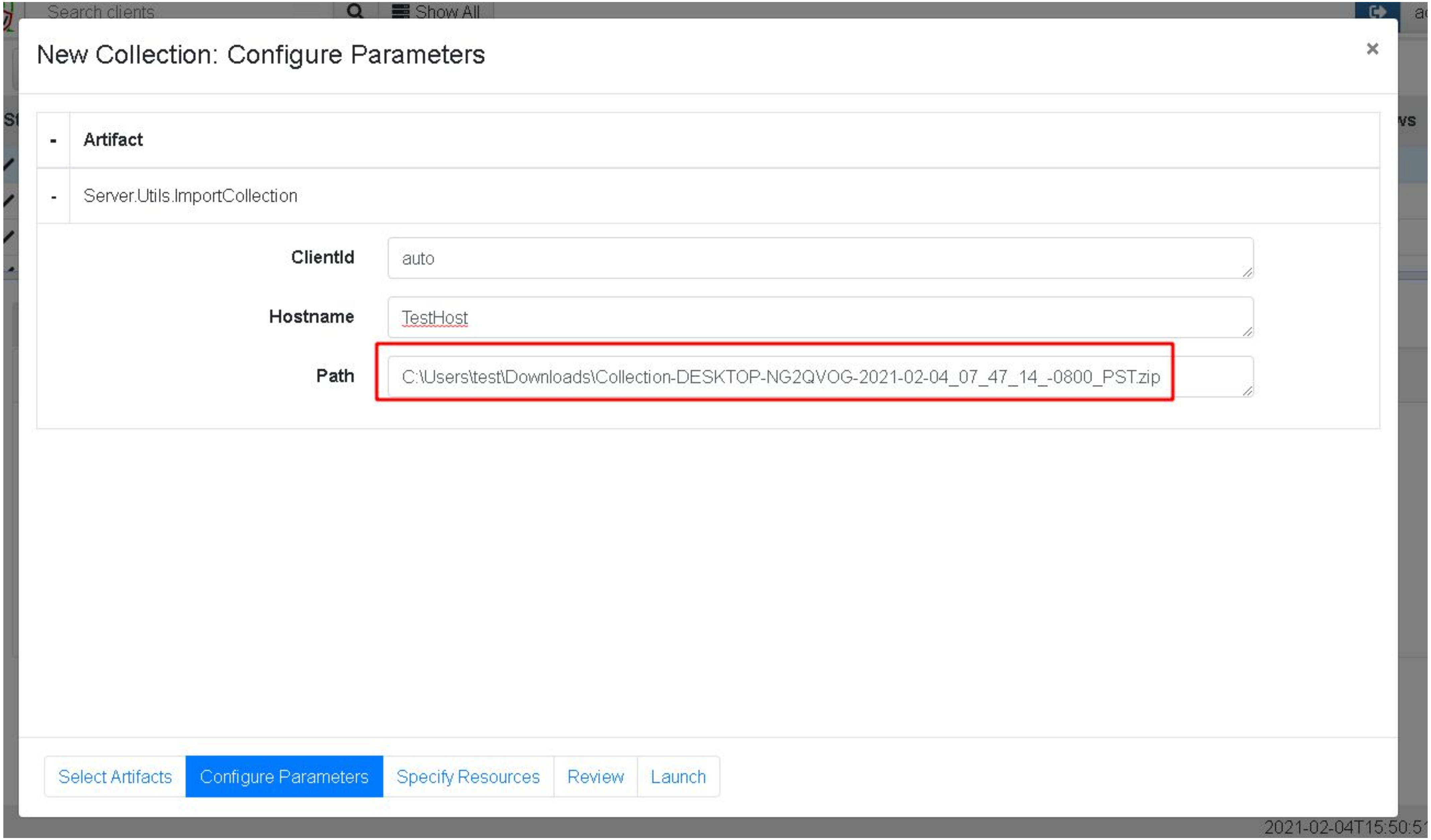


```
 (12058624 bytes)
[INFO] 2020-09-12T06:38:42-07:00  Collecting file \\.\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT into \\.\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT (262144 bytes)
[INFO] 2020-09-12T06:38:42-07:00  Collecting file \\.\C:\Windows\appcompat\Programs\Amcache.hve.LOG1 into \\.\C:\Windows\appcompat\Programs\Amcache.hve.LOG1 (36864 bytes)
[INFO] 2020-09-12T06:38:42-07:00  Collecting file \\.\C:\Windows\appcompat\Programs\Amcache.hve.LOG2 into \\.\C:\Windows\appcompat\Programs\Amcache.hve.LOG2 (1393664 bytes)
[INFO] 2020-09-12T06:38:42-07:00  Collecting file \\.\C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb into \\.\C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb (117440512 bytes)
[INFO] 2020-09-12T06:38:53-07:00  Starting collection of Windows.KapeFiles.Targets/All File Metadata
[INFO] 2020-09-12T06:38:53-07:00  Collected Windows.KapeFiles.Targets/All File Metadata
[INFO] 2020-09-12T06:38:53-07:00  Starting collection of Windows.KapeFiles.Targets/Uploads
[INFO] 2020-09-12T06:38:53-07:00  Collected Windows.KapeFiles.Targets/Uploads
[
 {
  "Container": "Collection-MikesTest-2020-09-12_06_37_26_-0700_PDT.zip",
  "Report": "Collection-MikesTest-2020-09-12_06_37_26_-0700_PDT.html"
 }
][INFO] 2020-09-12T06:38:54-07:00 Collection completed in 88 Seconds
PS C:\Users\test\Downloads>
```

https://docs.velociraptor.app/docs/offline_triage/#offline-collections

Import collection

(optional)



New Collection: Configure Parameters

-	Artifact
-	Server.Utils.ImportCollection

ClientId: auto

Hostname: TestHost

Path: C:\Users\test\Downloads\Collection-DESKTOP-NG2QVOG-2021-02-04_07_47_14_-0800_PST.zip

https://docs.velociraptor.app/docs/offline_triage/#importing-collections-into-the-gui

Questions/Feedback

Contact

@velocidex

@therealwlambert

@BlueTeamVillage

Documentation

https://docs.velociraptor.app/docs/offline_triage/#offline-collections