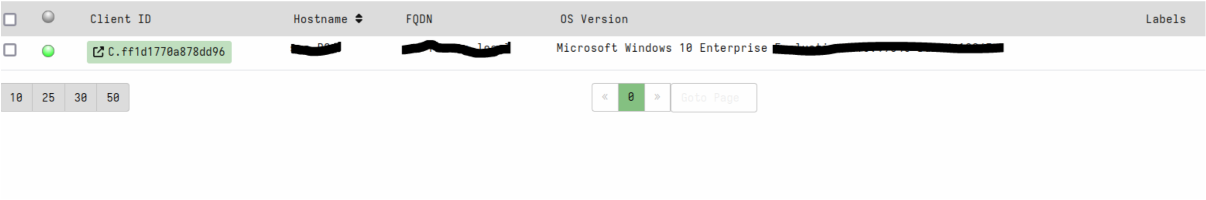
WORKING OF VELOCIRAPTOR

Velociraptor is an open source end point tools used for threat hunting, incident response and Digital Forensics purpose.

After installation we need to open GUI. So open browser and type your ip and port number [i.e. https://IP:8889]. Enter user name and password you mentioned.

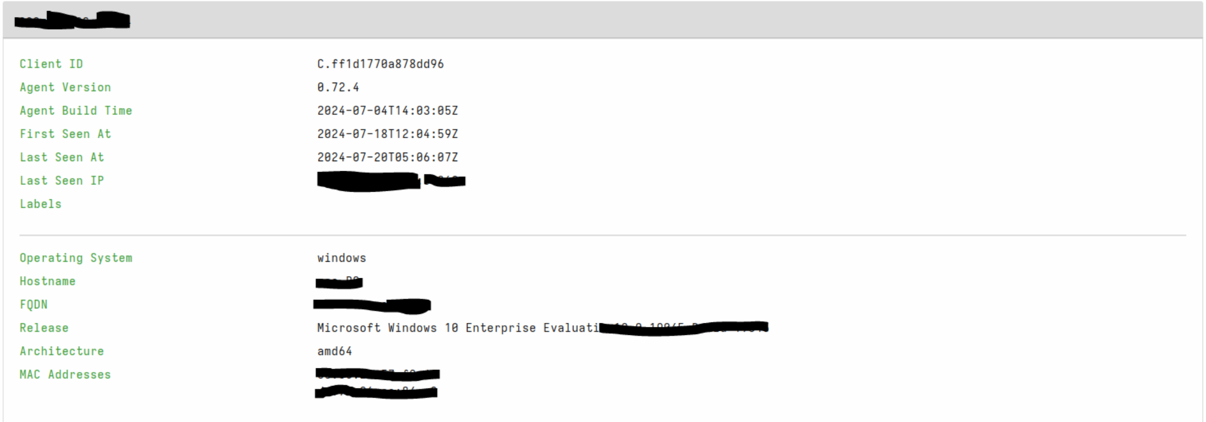
We fill find a device as client in it. We can find an interface as below mentioned if we clicked on search icon.



□	○	Client ID	Hostname	FQDN	OS Version	Labels
□	●	C.ff1d1770a878dd96	[redacted]	[redacted]	Microsoft Windows 10 Enterprise [redacted]	

You can find multiple clients if you installed in more devices. Since we installed in only single device, a single client is present. Now click on the client ID.

We will information about client.

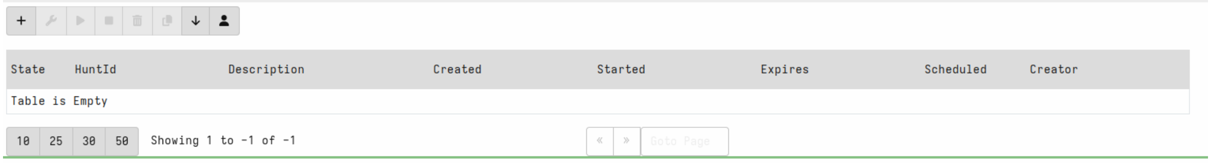


[redacted]

Client ID	C.ff1d1770a878dd96
Agent Version	0.72.4
Agent Build Time	2024-07-04T14:03:05Z
First Seen At	2024-07-18T12:04:59Z
Last Seen At	2024-07-20T05:06:07Z
Last Seen IP	[redacted]
Labels	
Operating System	windows
Hostname	[redacted]
FQDN	[redacted]
Release	Microsoft Windows 10 Enterprise Evaluati[redacted]
Architecture	amd64
MAC Addresses	[redacted]

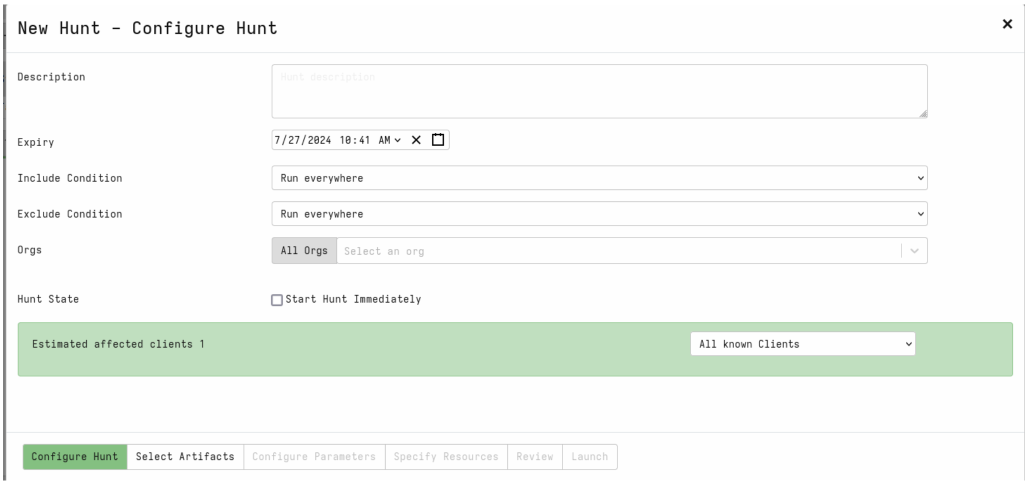
Now we will create a hunt that will fetch all the process of windows.

In order to create a hunt we can navigate to the hunt manager present at the left side of the screen.



State	HuntId	Description	Created	Started	Expires	Scheduled	Creator
Table is Empty							

The table is empty. To create a new hunt click on the plus icon.



New Hunt - Configure Hunt

Description: Hunt description

Expiry: 7/27/2024 10:41 AM

Include Condition: Run everywhere

Exclude Condition: Run everywhere

Orgs: All Orgs — Select an org

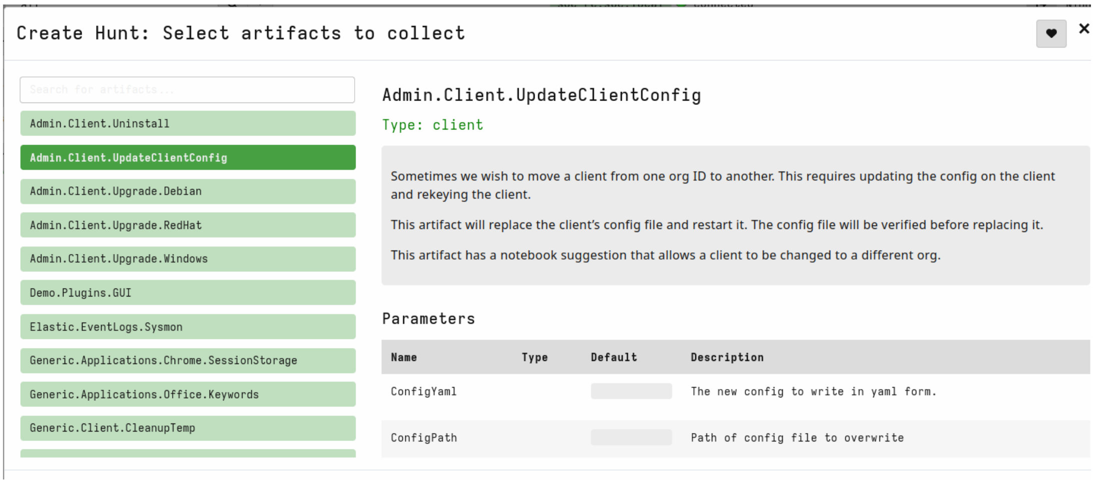
Hunt State: □ Start Hunt Immediately

Estimated affected clients 1 — All known Clients

Fill out the details and select options as per your requirements. After filling out the data, click on the select artifacts option.

Artifacts are the reason what kind of information you request, they will fetch it from client. There will be lot of artifacts presenet, we need to select appropriate artifact.

If we click on the artifact it will give a detailed overview what activity that the artifact will perform.



Create Hunt: Select artifacts to collect

Search for artifacts...

- Admin.Client.Uninstall
- Admin.Client.UpdateClientConfig
- Admin.Client.Upgrade.Debian
- Admin.Client.Upgrade.RedHat
- Admin.Client.Upgrade.Windows
- Demo.Plugins.GUI
- Elastic.EventLogs.Sysmon
- Generic.Applications.Chrome.SessionStorage
- Generic.Applications.Office.Keywords
- Generic.Client.CleanupTemp

Admin.Client.UpdateClientConfig

Type: client

Sometimes we wish to move a client from one org ID to another. This requires updating the config on the client and rekeying the client.

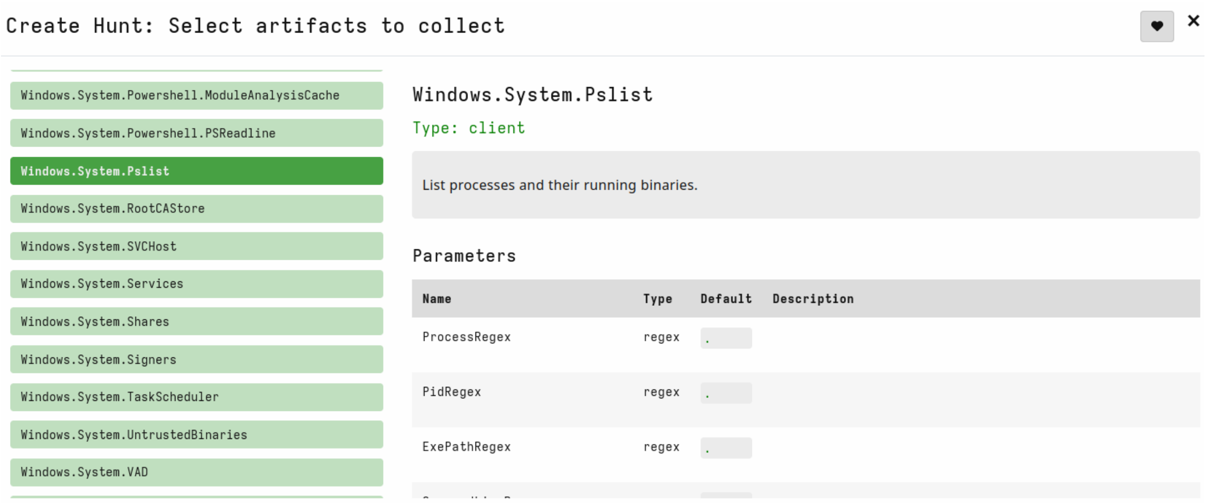
This artifact will replace the client's config file and restart it. The config file will be verified before replacing it.

This artifact has a notebook suggestion that allows a client to be changed to a different org.

Parameters

Name	Type	Default	Description
ConfigYaml			The new config to write in yaml form.
ConfigPath			Path of config file to overwrite

Since I want to list out all the process that are present in the client. I am going to use ps list.



Create Hunt: Select artifacts to collect

- Windows.System.Powershell.ModuleAnalysisCache
- Windows.System.Powershell.PSReadline
- Windows.System.Pslist
- Windows.System.RootCAStore
- Windows.System.SVCHost
- Windows.System.Services
- Windows.System.Shares
- Windows.System.Signers
- Windows.System.TaskScheduler
- Windows.System.UntrustedBinaries
- Windows.System.VAD

Windows.System.Pslist

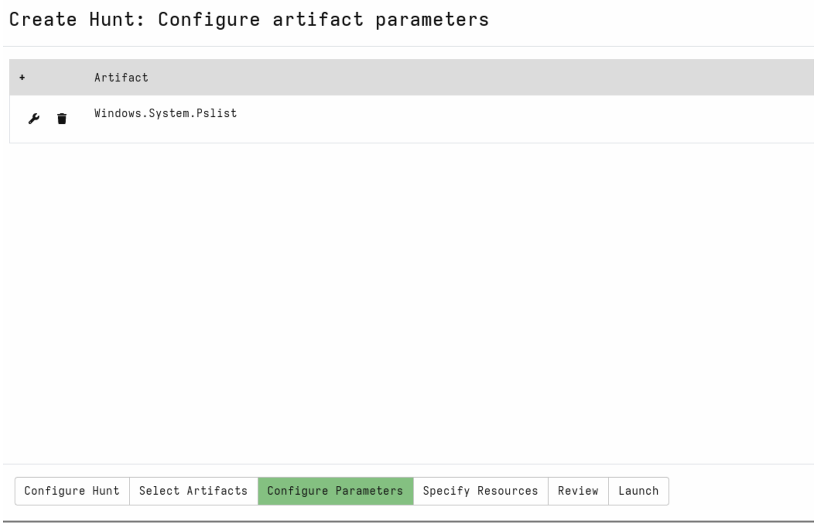
Type: client

List processes and their running binaries.

Parameters

Name	Type	Default	Description
ProcessRegex	regex	.	
PidRegex	regex	.	
ExePathRegex	regex	.	

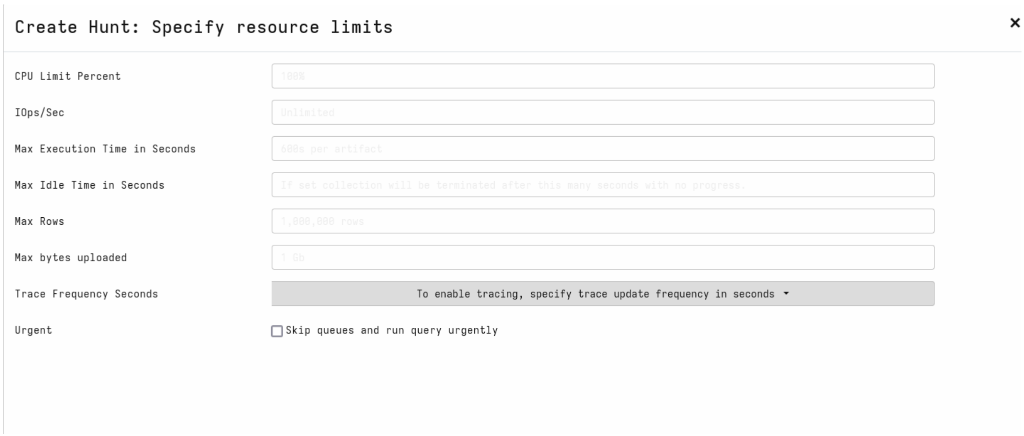
Click on the artifact and click configure parameters. You can find out the artifacts that you have selected in configure parameters



Create Hunt: Configure artifact parameters

+	Artifact
	Windows.System.Pslist

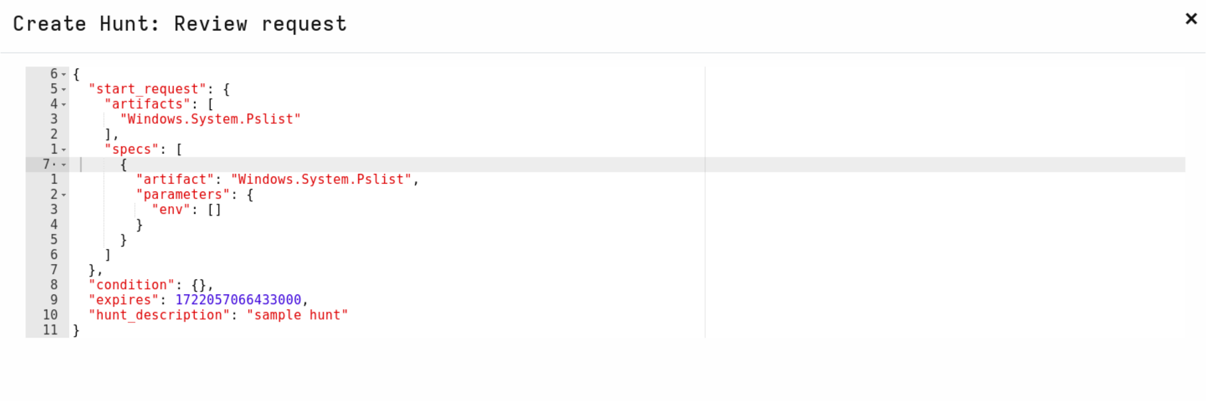
For the specify resources option specify as per system configurations. Otherwise leave it as default. No need to enter any data.



Create Hunt: Specify resource limits

CPU Limit Percent	100%
IOps/Sec	Unlimited
Max Execution Time in Seconds	600s per artifact
Max Idle Time in Seconds	If set collection will be terminated after this many seconds with no progress.
Max Rows	1,000,000 rows
Max bytes uploaded	1 Gb
Trace Frequency Seconds	To enable tracing, specify trace update frequency in seconds
Urgent	□ Skip queues and run query urgently

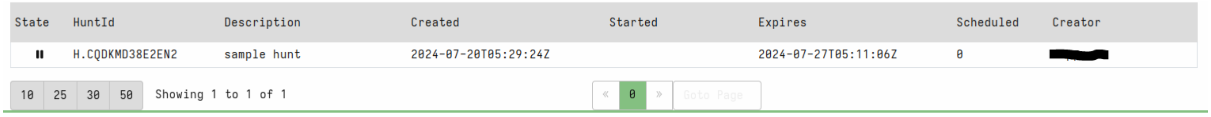
In review you can check out VQL code of the artifact that you have selected.



Create Hunt: Review request

```
{
  "start_request": {
    "artifacts": [
      "Windows.System.Pslist"
    ],
    "specs": [
      {
        "artifact": "Windows.System.Pslist",
        "parameters": {
          "env": []
        }
      }
    ]
  },
  "condition": {},
  "expires": 1722057066433000,
  "hunt_description": "sample hunt"
}
```

Launch the hunt and run it. It will take some time based on system configurations.



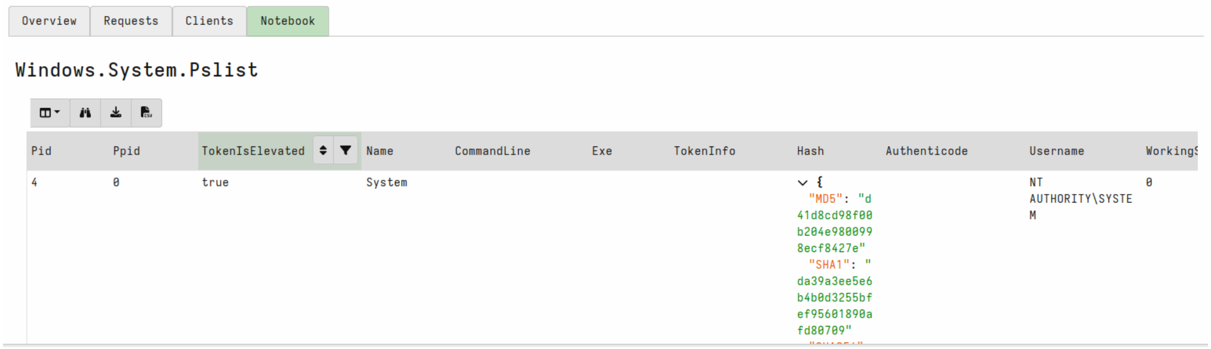
State	HuntId	Description	Created	Started	Expires	Scheduled	Creator
⏸	H.CQDKMD38E2EN2	sample hunt	2024-07-20T05:29:24Z		2024-07-27T05:11:06Z	0	[redacted]

10 25 30 50 Showing 1 to 1 of 1

« 0 » Goto Page

If you click on the notebook you will find out the list of process present in it.

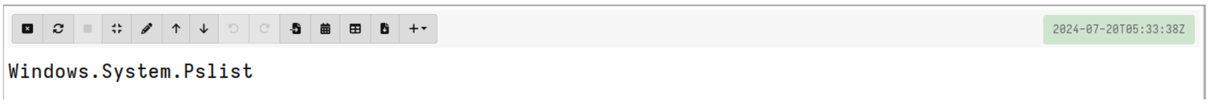
You can edit what ever the process you want to find out.



Windows.System.Pslist

Pid	Ppid	TokenIsElevated	Name	CommandLine	Exe	TokenInfo	Hash	Authenticode	Username	Working$
4	0	true	System				{ "MD5": "d41d8cd98f00b204e9800998ecf8427e" "SHA1": "da39a3ee5e6b4b0d3255bfef95601890afd80709"		NT AUTHORITY\SYSTEM	0

Click on the artifact on the screen. You will find some new options.

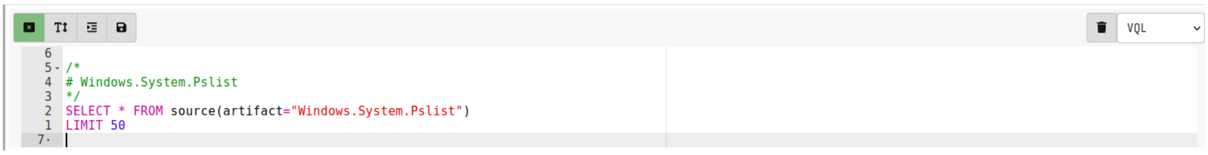


2024-07-20T05:33:38Z

Windows.System.Pslist

Click on edit cell option. You will find out the VQL code available.

You can edit the VQL code as per your requirements to filter out results. We can also export the

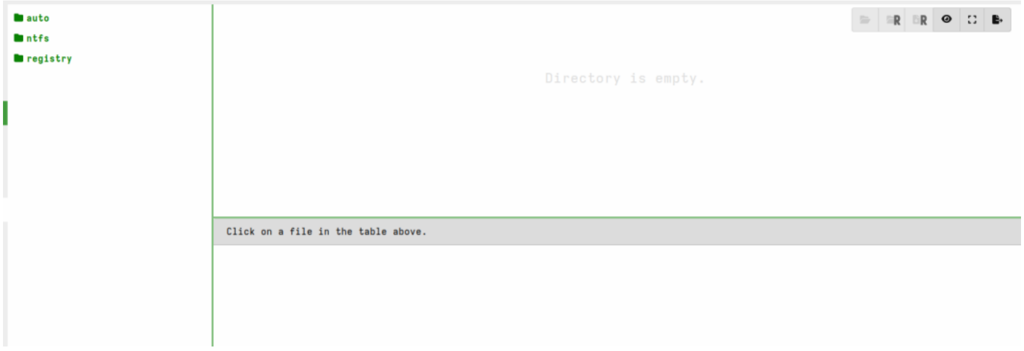


```
/*
# Windows.System.Pslist
*/
SELECT * FROM source(artifact="Windows.System.Pslist")
LIMIT 50
```

NOT: VQL is case sensitive.

We can also download the process as csv or json file format and add them to your siem tools.

There is one powerful option in velociraptor called virtual file systems.

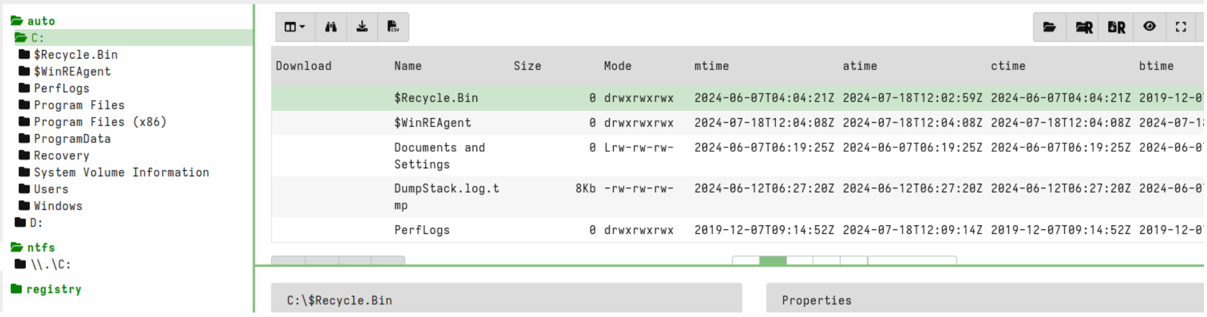


- auto
- ntfs
- registry

Directory is empty.

Click on a file in the table above.

Click on the data that you want to view and click refresh present on right side. I am proceeding with auto. For every refresh you can find out the directories present are being visible.



- auto
  - C:
    - $Recycle.Bin
    - $WinREAgent
    - PerfLogs
    - Program Files
    - Program Files (x86)
    - ProgramData
    - Recovery
    - System Volume Information
    - Users
    - Windows
  - D:
- ntfs
  - \\.\C:
- registry

Download	Name	Size	Mode	mtime	atime	ctime	btime
	$Recycle.Bin	0	drwxrwxrwx	2024-06-07T04:04:21Z	2024-07-18T12:02:59Z	2024-06-07T04:04:21Z	2019-12-0
	$WinREAgent	0	drwxrwxrwx	2024-07-18T12:04:08Z	2024-07-18T12:04:08Z	2024-07-18T12:04:08Z	2024-07-1
	Documents and Settings	0	Lrw-rw-rw-	2024-06-07T06:19:25Z	2024-06-07T06:19:25Z	2024-06-07T06:19:25Z	2024-06-0
	DumpStack.log.tmp	8Kb	-rw-rw-rw-	2024-06-12T06:27:20Z	2024-06-12T06:27:20Z	2024-06-12T06:27:20Z	2024-06-0
	PerfLogs	0	drwxrwxrwx	2019-12-07T09:14:52Z	2024-07-18T12:09:14Z	2019-12-07T09:14:52Z	2019-12-0

C:\$Recycle.Bin

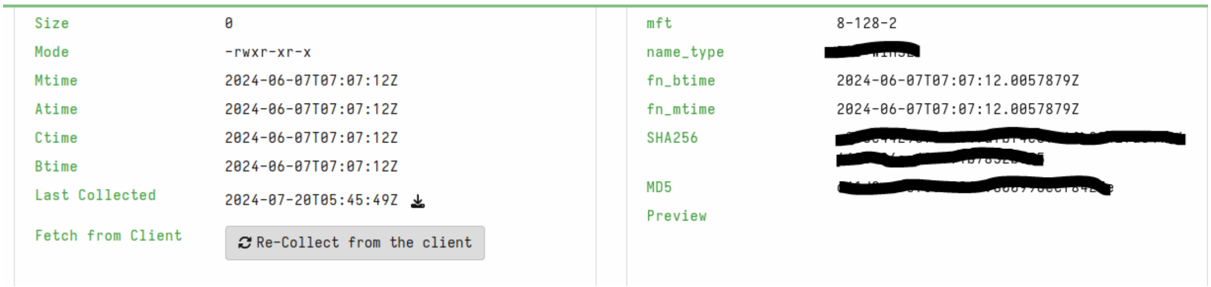
Properties

From this you can also find out if there is any malicious file running the client system. We need to search for it to find whether it is malicious or false positive.

There will option called collect from client

Click on the option. After that you find out the following information.

We can download the file by clicking on the download icon and perform forensic analysis on the file

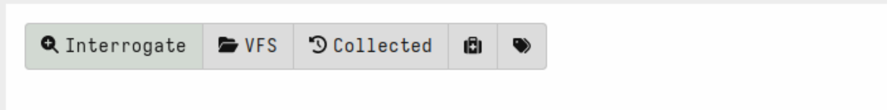


Size	0
Mode	-rwxr-xr-x
Mtime	2024-06-07T07:07:12Z
Atime	2024-06-07T07:07:12Z
Ctime	2024-06-07T07:07:12Z
Btime	2024-06-07T07:07:12Z
Last Collected	2024-07-20T05:45:49Z
Fetch from Client	Re-Collect from the client

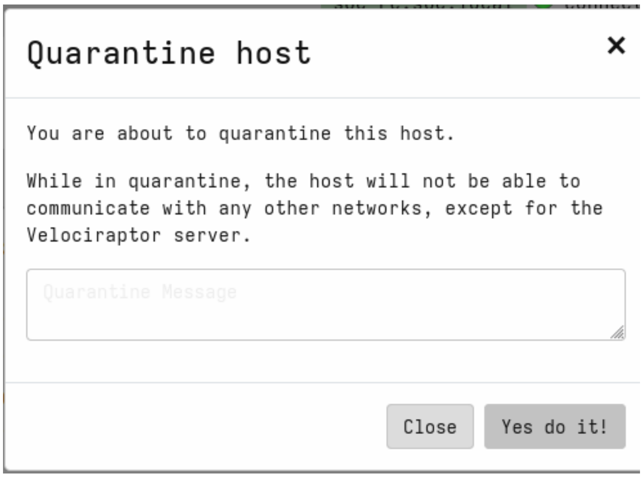
mft	8-128-2
name_type	[redacted]
fn_btime	2024-06-07T07:07:12.0057879Z
fn_mtime	2024-06-07T07:07:12.0057879Z
SHA256	[redacted]
MD5	[redacted]
Preview	

If you found any malicious process, you can quarntine the host.

By clicking on the quarntine option present at the beginning.



Click on quarntine option, a prompt will be opened as shown below. The networking operations on the client machine will be stopped if we click on yes option.



Quarantine host

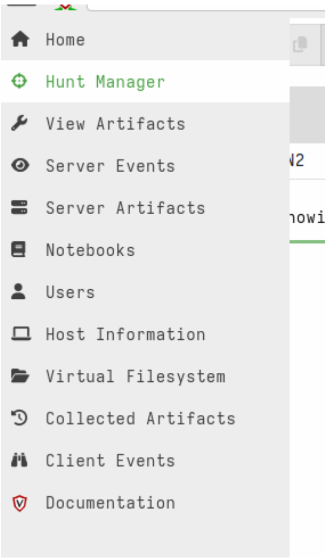
You are about to quarantine this host.

While in quarantine, the host will not be able to communicate with any other networks, except for the Velociraptor server.

You can also unquarntine the host later.

You can also perform multiple activities by selecting multiple artifacts.

There are also different options you can explore in velociraptor and also you can create note book where you list down what operations you are performing in velociraptor.



Try to explore more options present in velociraptor for more information.

In short, Velociraptor allows us to perform various operations to gather client information, modify VQL, create new VQL queries, and streamline our activities efficiently.