Threat Hunting: Velociraptor for Endpoint Monitoring

September 1, 2020 By Raj Chandel

A velociraptor is a tool for collecting host-based state information using Velocidex Query Language (VQL) queries.

To learn more about Velociraptor, read the documentation on **https://www.velocidex.com/docs**

Table of Content

Introduction to Velociraptor

Velociraptor is a free and open-source software project developed by the Velocidex Company. Velociraptor is generally based on GRR, OSQuery, and Google's Rekall tools. Velociraptor allows users to collect Forensics Evidence, Threat Hunting, Monitoring artifacts, Executing remote triage process. As an open-source platform, Velociraptor continues to improve and evolve through inputs and feedback of digital forensics investigation and cybersecurity practitioner

Velociraptor natively works on Linux, Windows, and macOS. You can create or deploy a server within few minutes using SCCM or Group policy.

Architecture

Main components- all in one binary

Frontend

- Receive connections from clients
- Queue message to clients
- Process Responses from clients (Flows)

GUI

- Allow Scheduling Flows/Hunts
- Inspect results from Flows/Hunts

- View the client's virtual file system

What is VQL

Velociraptor Query Language (VQL) is an expressive query language designed to adapt your requirements easily without doing any modifications in codes, Query, or artifacts nor deploying any additional software.

VQL encapsulates digital forensics expertise into human-readable files called 'artifacts' which can be shared and exchanged freely within the community.

Let's begin

As shown in the above image there are a few agents like windows or Linux or cloud distros… these agents will point to TCP port 8000 while Digital forensics or cybersecurity experts will consult the web interface to TCP port 8889. The best part of this Architecture is if one of the computers leaves the office or another environment and operates from home or by any other place, it will be able to continue reporting to the server.

Prerequisites

To configure Velociraptor in your Windows Platform, there are some prerequisites required for installation.

- Windows 10 with minimum 4gb Ram and 4 CPU cores
- Admin privileges
- CMD with admin Privilege

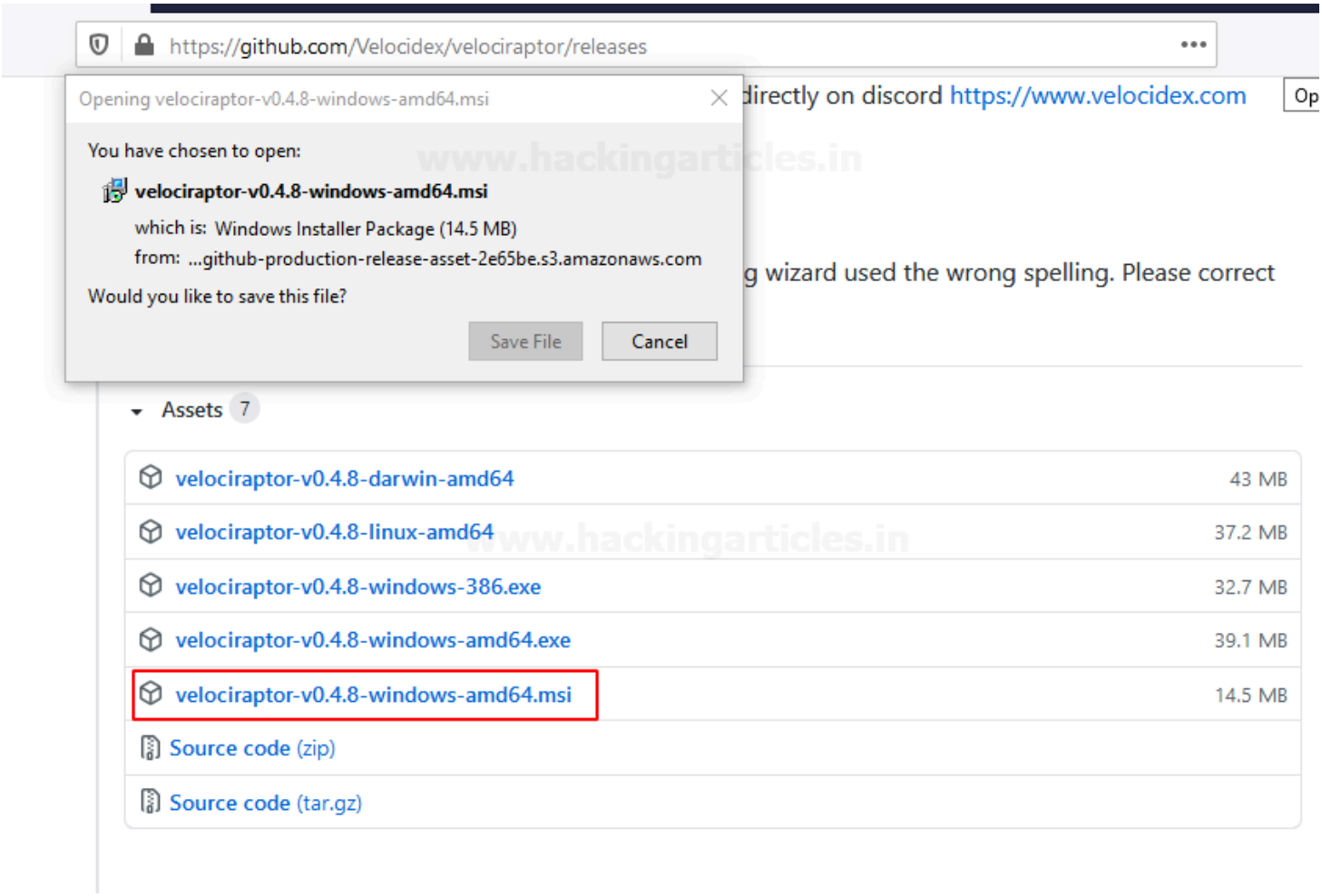
Velociraptor Environment

In this blog we will target to install Velociraptor on windows 10, to make it as real as possible, the installation can be carried out to a server in the cloud as shown in the image above. In this blog, I'm going to use windows 10 as a server. You can Download Velociraptor by following the below Link.

https://github.com/Velocidex/velociraptor/releases

Windows Version

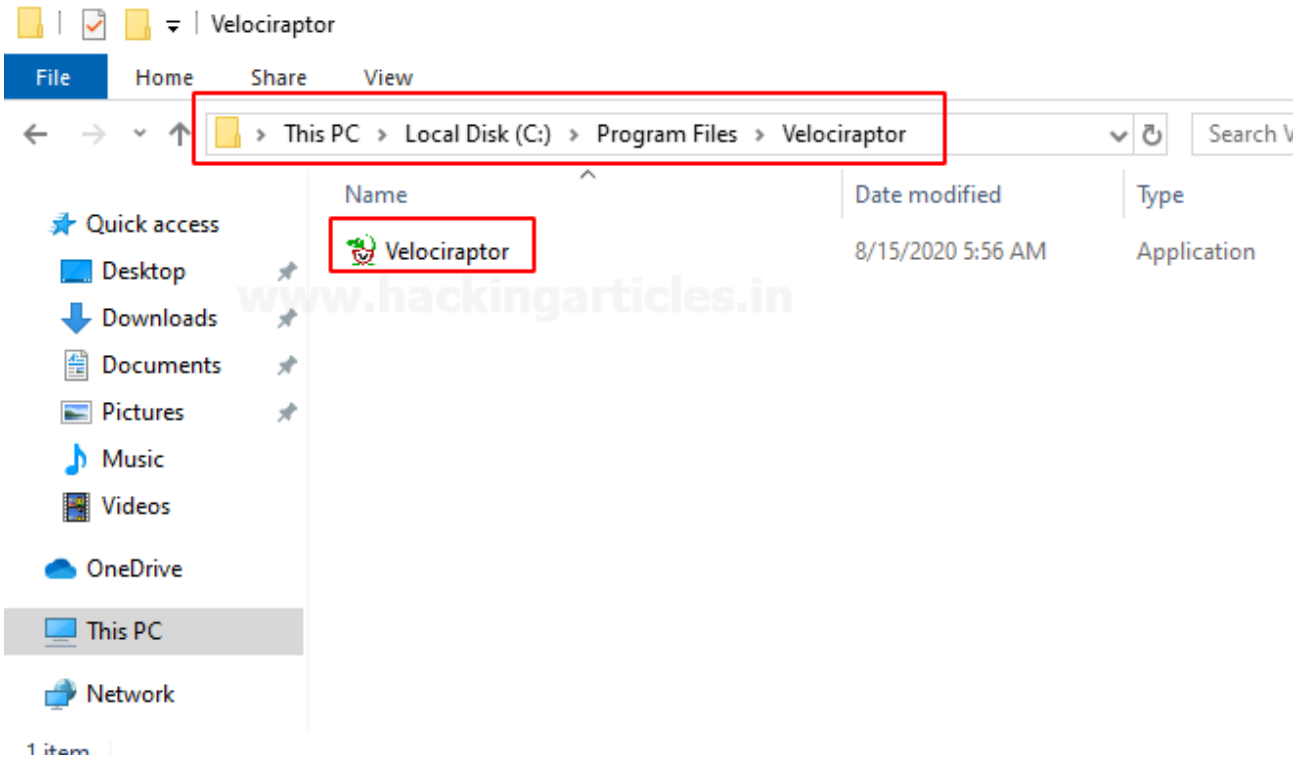
To download the latest version of Velociraptor in a windows server, go to the official GitHub page by following the above link then locate and select the option **velociraptor-v0.4.8-windows-amd64.msi** or you can directly download by accessing the above .msi extension hyperlink.



Velociraptor installation

Let's start deploying master server in windows And after the download complete what we can do now is to go to the download folder and just simply install it.

Here, windows will try to prevent this happening but once the installer is complete what we saw here is that under the program files have the Velociraptor folder.

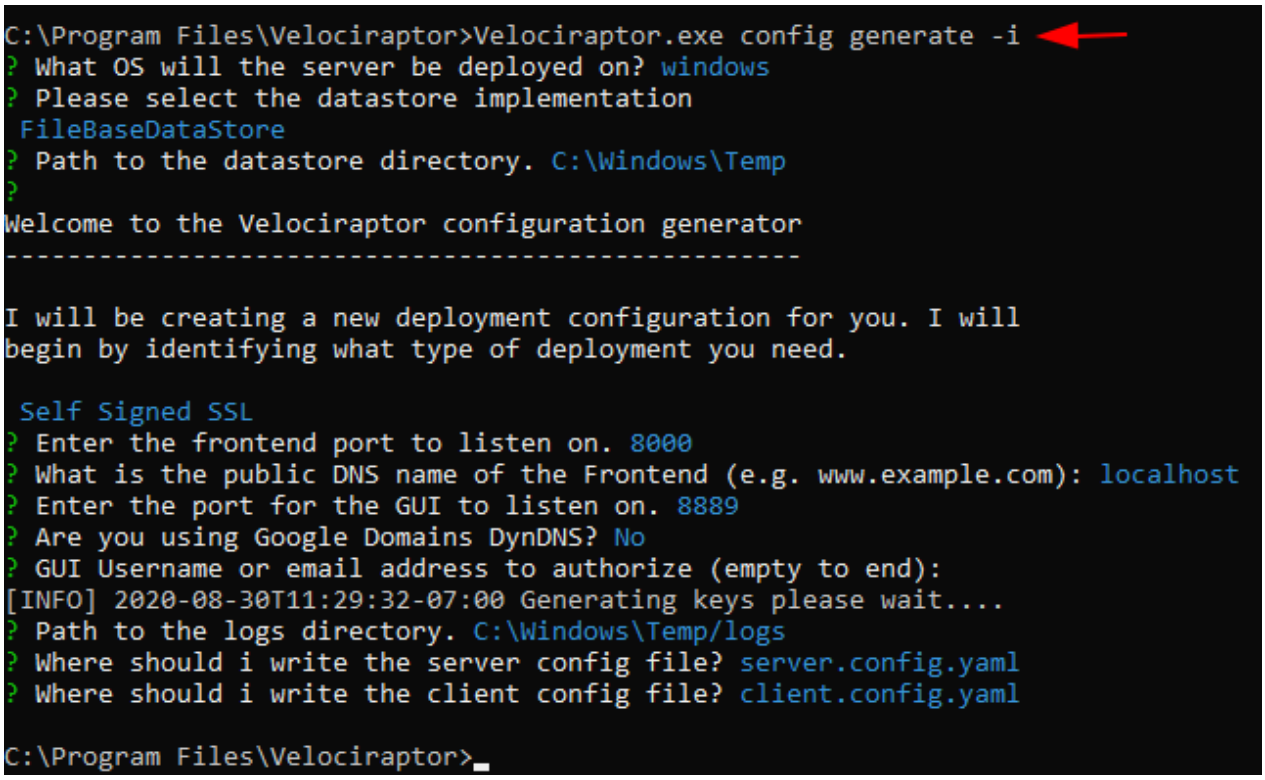


now let's open the command prompt with administrator privilege and navigate to

```
cd C:\Program Files\Velociraptor
```

so now what we need to do is to generate the configuration to do this enter the below arguments into the CMD prompt

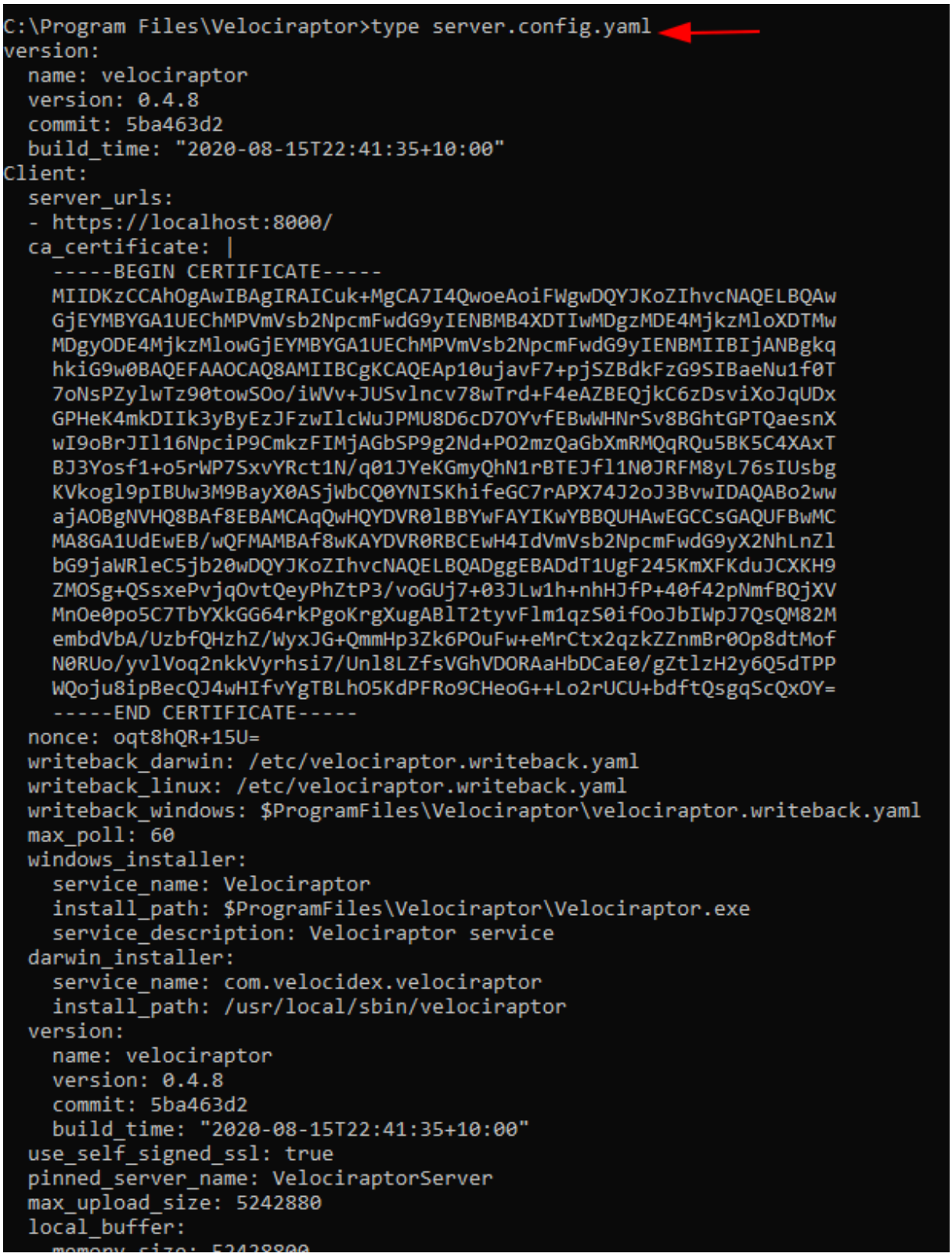
```
velociraptor.exe config generate -i
```



And we would like to generate the configuration for the Windows machine so select windows and then hit enter then next select FilebaseDatastore you can also go with the MySQL option but the MySQL option is suitable for the production environment and then next select the path of Velociraptor configuration is c:\window\Temp and then use Self-signed SSL we would like to leave everything on default but if you have different requirements you can make changes as per your own and at last we are not using any google domains so on that place type N and hit enter and enter till last to set options as default as shown In the image below.

Now you can check the configuration of your server by entering below argument

```
type server.config.yaml
```



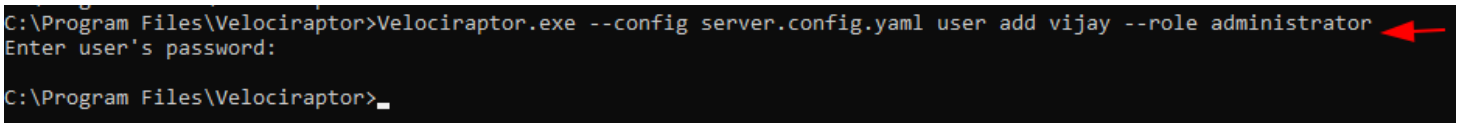
```
C:\Program Files\Velociraptor>type server.config.yaml
version:
  name: velociraptor
  version: 0.4.8
  commit: 5ba463d2
  build_time: "2020-08-15T22:41:35+10:00"
Client:
  server_urls:
  - https://localhost:8000/
  ca_certificate: |
    -----BEGIN CERTIFICATE-----
    MIIDKzCCAhOgAwIBAgIRAICuk+MgCA7I4QwoeAoiFWgwDQYJKoZIhvcNAQELBQAw
    GjEYMBYGA1UEChMPVmVsb2NpcmFwdG9yIENBMB4XDTIwMDgzMDE4MjkzMloXDTMw
    MDgyODE4MjkzMlowGjEYMBYGA1UEChMPVmVsb2NpcmFwdG9yIENBMIIBIjANBgkq
    hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAp10ujavF7+pjSZBdkFzG9SIBaeNu1f0T
    7oNsPZylwTz90towSOo/iWVv+JUSvlncv78wTrd+F4eAZBEQjkC6zDsviXoJqUDx
    GPHeK4mkDIIk3yByEzJFzwIlcWuJPMU8D6cD7OYvfEBwWHNrSv8BGhtGPTQaesnX
    wI9oBrJIl16NpciP9CmkzFIMjAGbSP9g2Nd+PO2mzQaGbXmRMQqRQu5BK5C4XAxT
    BJ3Yosf1+o5rWP7SxvYRct1N/q01JYeKGmyQhN1rBTEJfl1N0JRFM8yL76sIUsbg
    KVkogl9pIBUw3M9BayX0ASjWbCQ0YNISKhifeGC7rAPX74J2oJ3BvwIDAQABo2ww
    ajAOBgNVHQ8BAf8EBAMCAqQwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMC
    MA8GA1UdEwEB/wQFMAMBAf8wKAYDVR0RBCEwH4IdVmVsb2NpcmFwdG9yX2NhLnZl
    bG9jaWRleC5jb20wDQYJKoZIhvcNAQELBQADggEBADdT1UgF245KmXFKduJCXKH9
    ZMOSg+QSsxePvjqOvtQeyPhZtP3/voGUj7+03JLw1h+nhHJfP+40f42pNmfBQjXV
    MnOe0po5C7TbYXkGG64rkPgoKrgXugABlT2tyvFlm1qzS0ifOoJbIWpJ7QsQM82M
    embdVbA/UzbfQHzhZ/WyxJG+QmmHp3Zk6POuFw+eMrCtx2qzkZZnmBr0Op8dtMof
    N0RUo/yvlVoq2nkkVyrhsi7/Unl8LZfsVGhVDORAaHbDCaE0/gZtlzH2y6Q5dTPP
    WQoju8ipBecQJ4wHIfvYgTBLhO5KdPFRo9CHeoG++Lo2rUCU+bdftQsgqScQxOY=
    -----END CERTIFICATE-----
  nonce: oqt8hQR+15U=
  writeback_darwin: /etc/velociraptor.writeback.yaml
  writeback_linux: /etc/velociraptor.writeback.yaml
  writeback_windows: $ProgramFiles\Velociraptor\velociraptor.writeback.yaml
  max_poll: 60
  windows_installer:
    service_name: Velociraptor
    install_path: $ProgramFiles\Velociraptor\Velociraptor.exe
    service_description: Velociraptor service
  darwin_installer:
    service_name: com.velocidex.velociraptor
    install_path: /usr/local/sbin/velociraptor
  version:
    name: velociraptor
    version: 0.4.8
    commit: 5ba463d2
    build_time: "2020-08-15T22:41:35+10:00"
  use_self_signed_ssl: true
  pinned_server_name: VelociraptorServer
  max_upload_size: 5242880
  local_buffer:
    memory_size: 52428800
```

And as we can see what the configuration for our server is and it sets our frontend is listening to **localhost** port **8000** and the certificate directory and so on… basically it's just a description what the configuration for our server.

Now, since we have this part done what we need to is to add user and we can do it with entering the below command

```
velociraptor.exe --config server.config.yaml user add vijay --role administrator
```

And we need to create the password to access the GUI interface

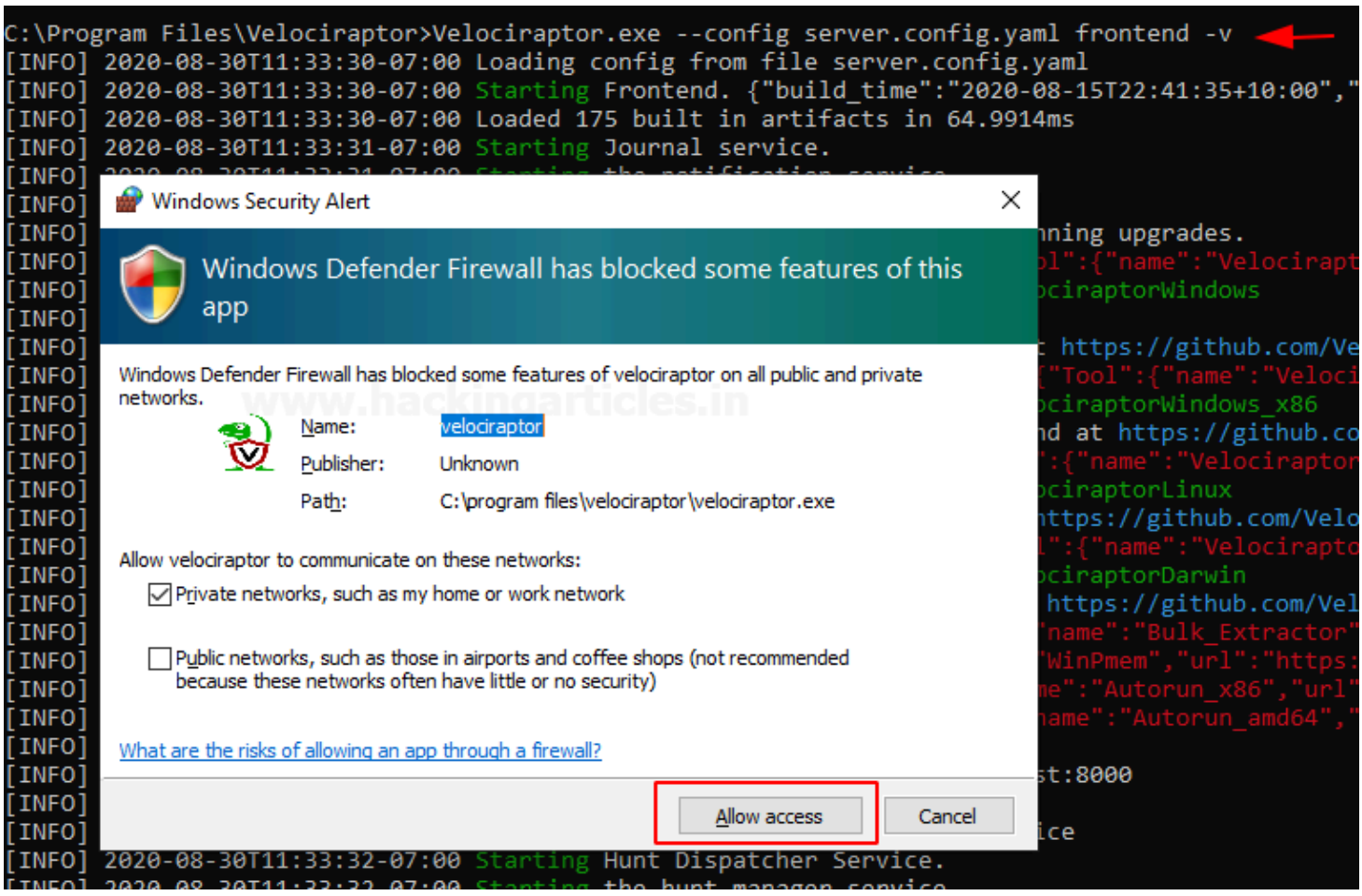


and what we can do now is to run our server so how we can run it…. To do this issue the following command

```
velociraptor.exe --config server.config.yaml frontend -v
```

Here -v stands for verbose

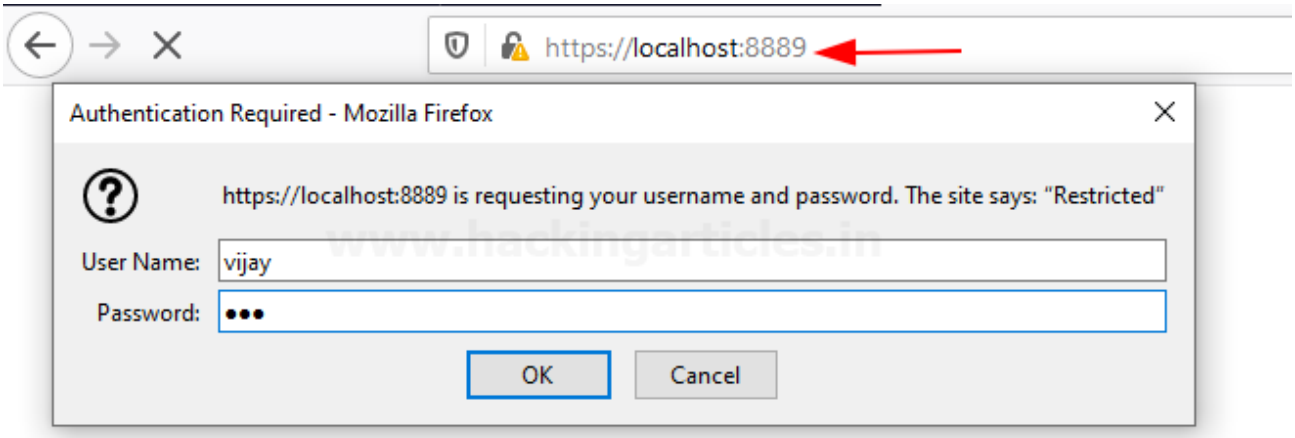
By running the above argument a prompt screen opens on your screen that needs admin access to setting up the environment and then the setup continues.



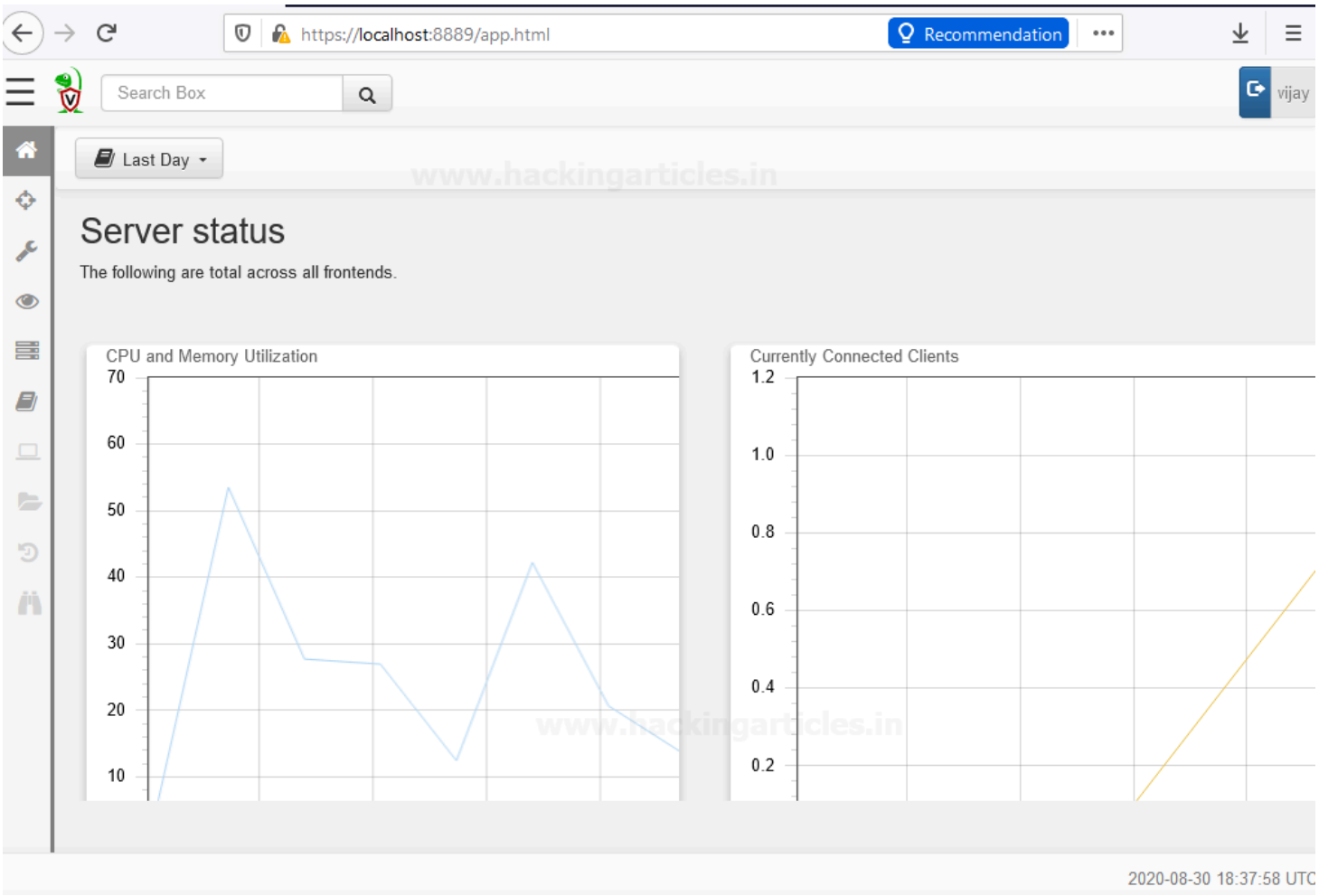
Congratulations! Finally, you have setup Velociraptor in your windows machine. You can now access the Velociraptor GUI interface at your favourite browser by ping following URL

https://localhost:8889

And use your credentials to log in that you created at the time of installation.



After login into the interface, you'll have your Velociraptor GUI dashboard



Here we can see the home page, which is about basically the load of the server, connected client's users, and so on….and this is not all we can end to do….

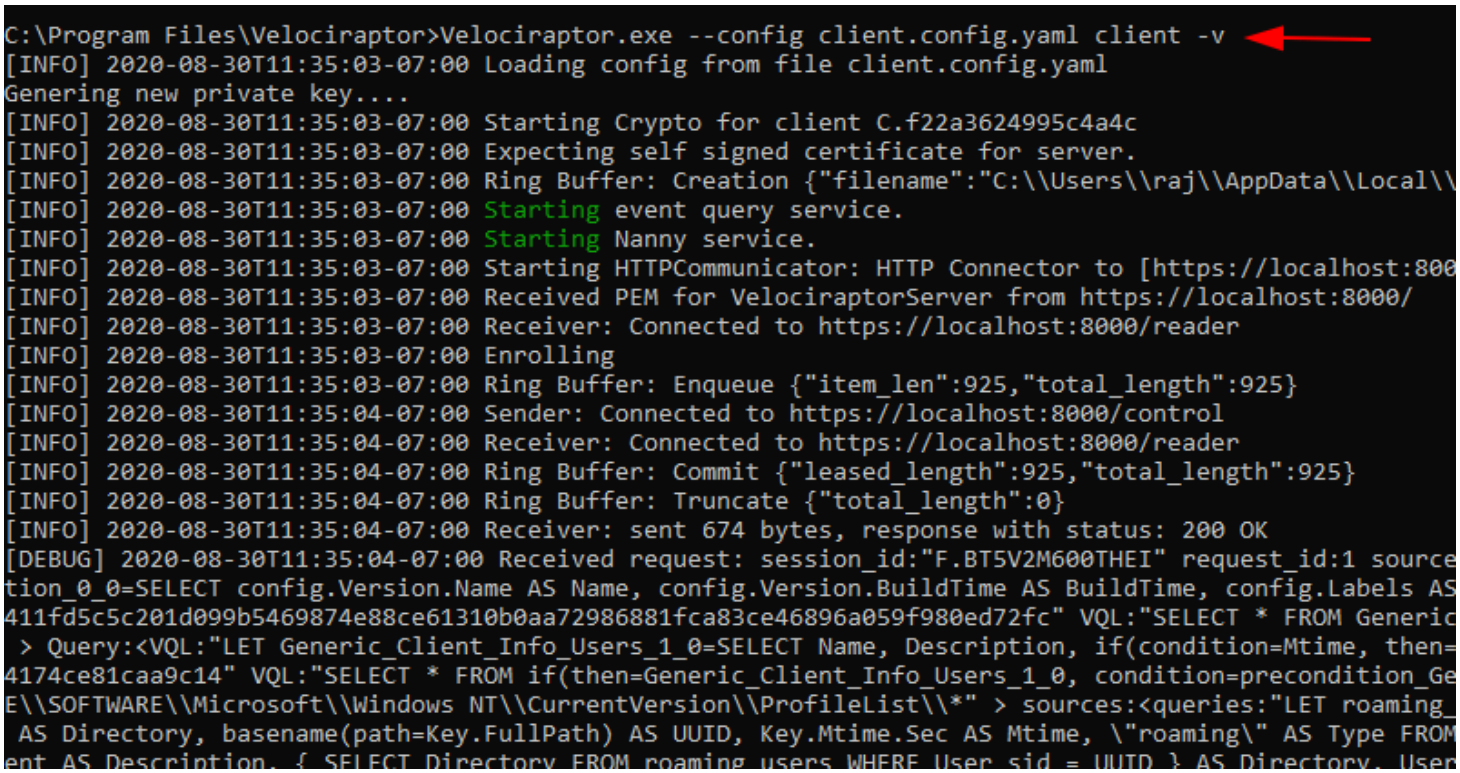
Addition of Host

Currently, we have no clients connected to the server so let's rectify that by opening a new terminal with admin privilege

And then follow the below arguments

```
cd C:\Program Files\Velociraptor
velociraptor.exe --config client.config.yaml client -v
```

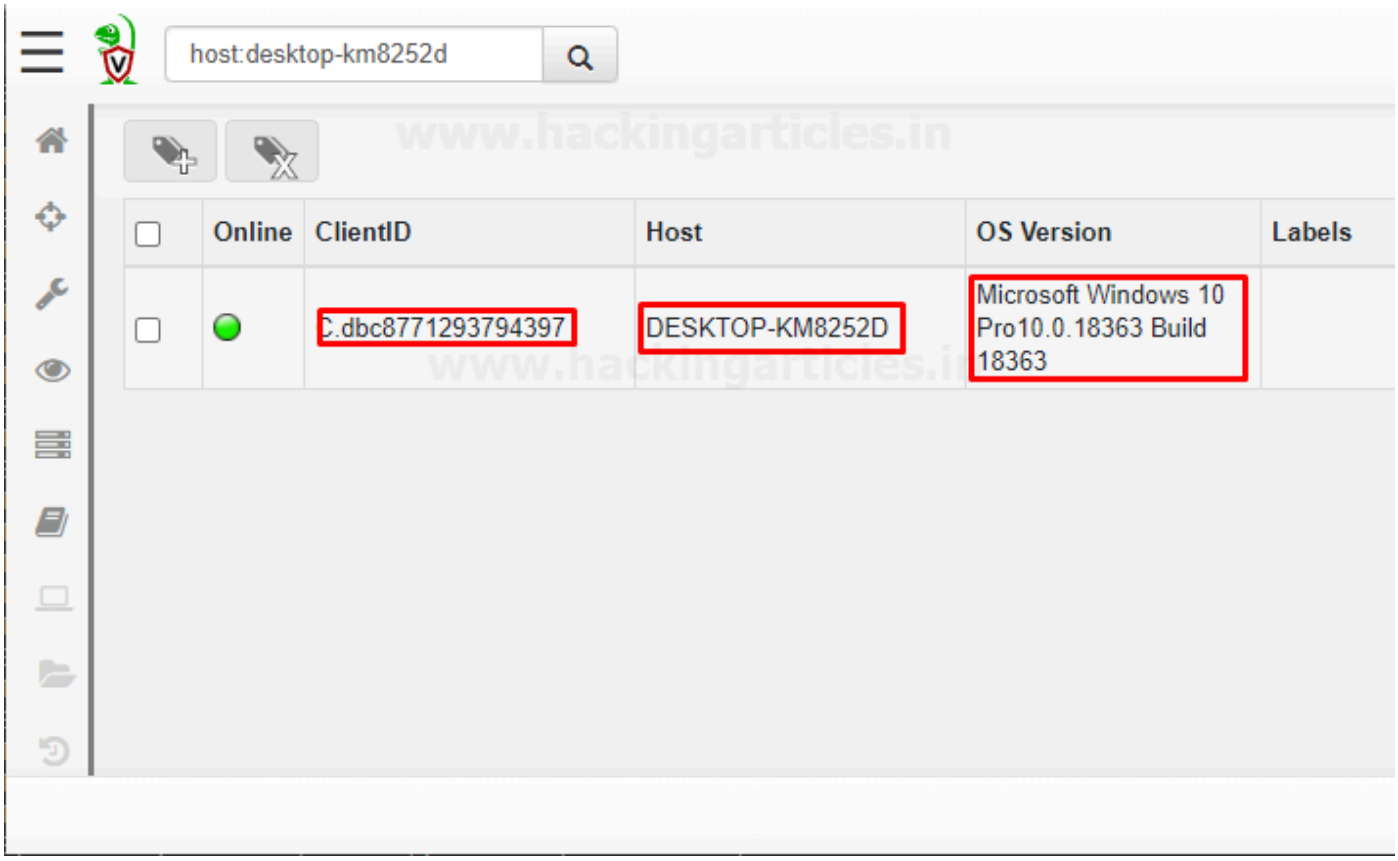
And the client Is connected and is going to enrol in the specific server based on the client config file so you could use the client config file with very little modifications to enrol your client to your existing master server if needed in the future.



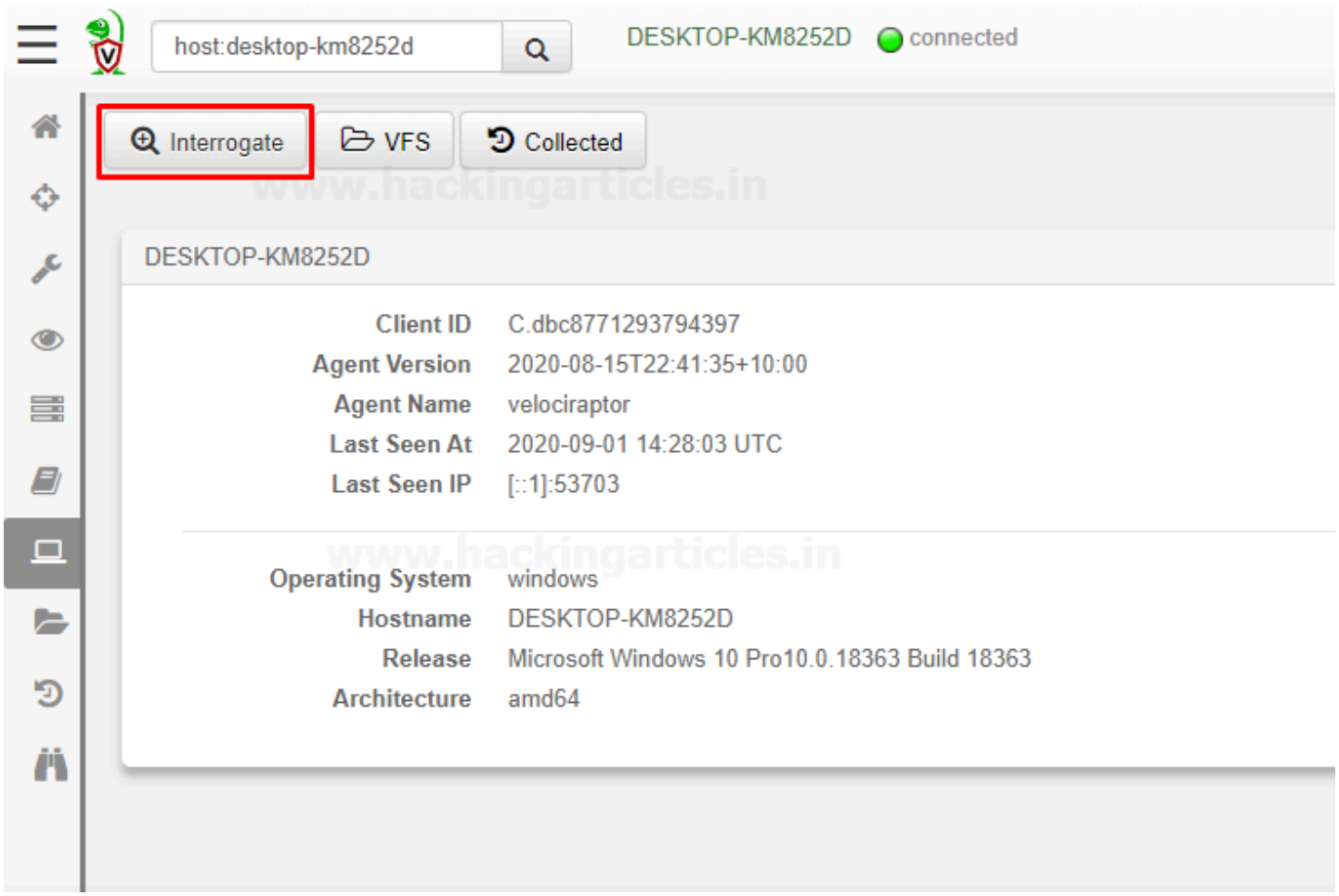
And now what you see is that your client has successfully connected to the localhost and we have one client added into the master server.

Forensics Investigation / Threat Hunting

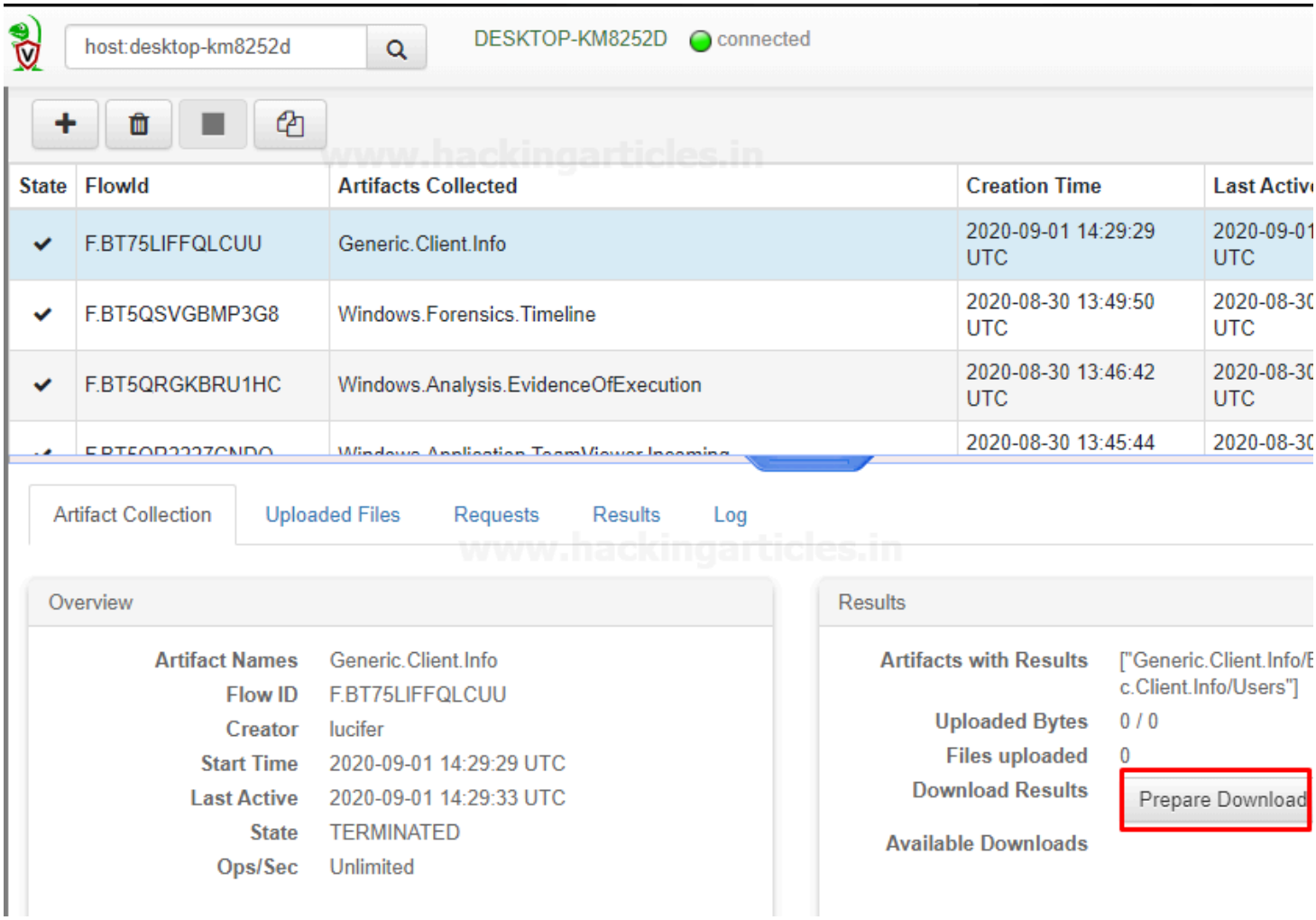
Now if you go back to the homepage you could be able to see your host by searching in the filter box.



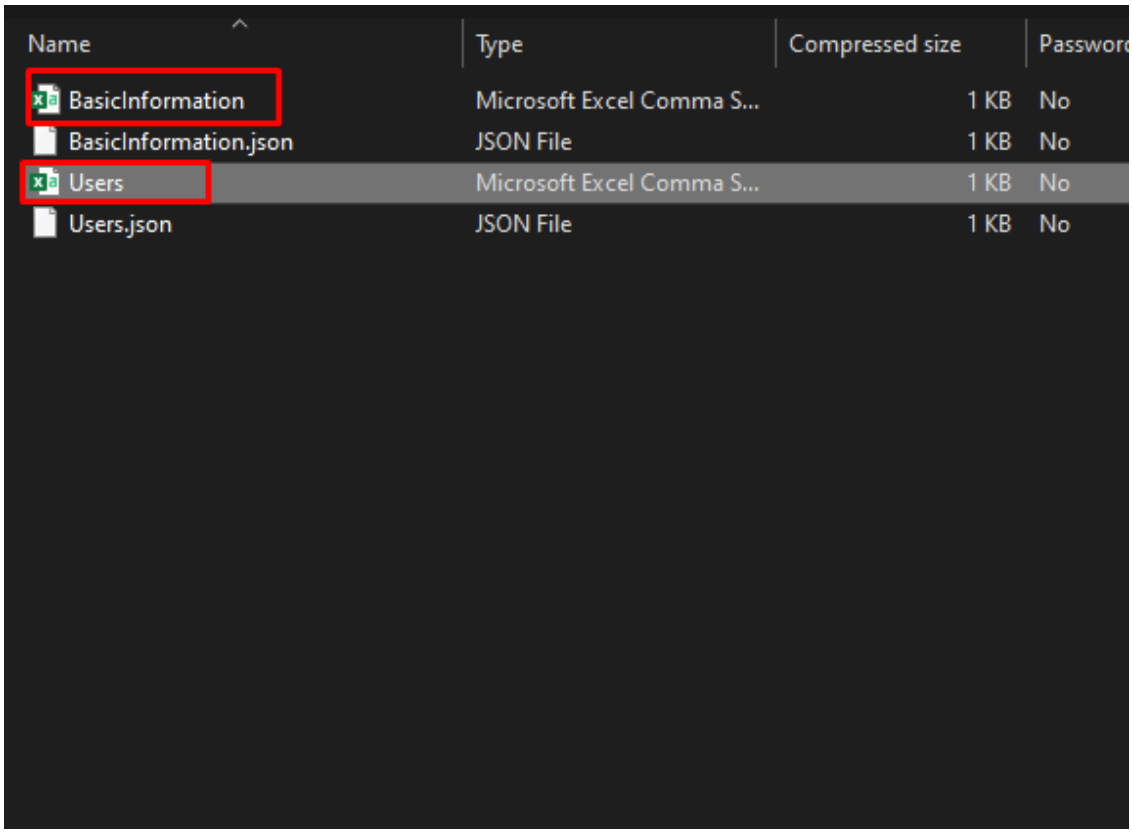
And then you can see the host have a client id, hostname OS version, and so on….



And we could interrogate the host and we could check collected information and by default, some basic information is collected about clients.

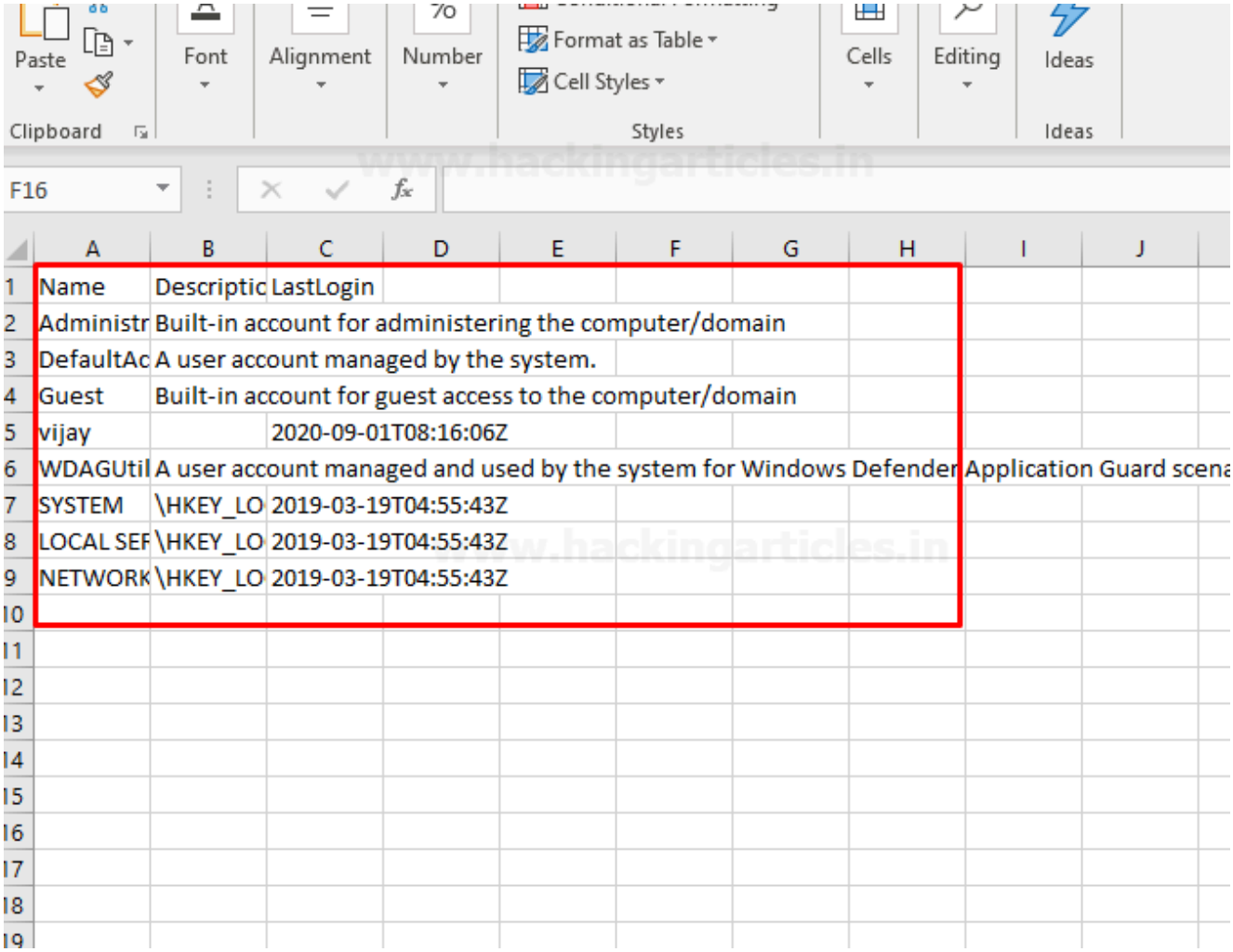


So now what we can and should do is to try to figure out what's inside this information by downloading it. As we can see a zip folder downloaded inside downloads after opening it you can see these files there that contain the host details.



Let’s check what’s inside these folders open it one by one and this part is gonna a little bit special but it’s not enough

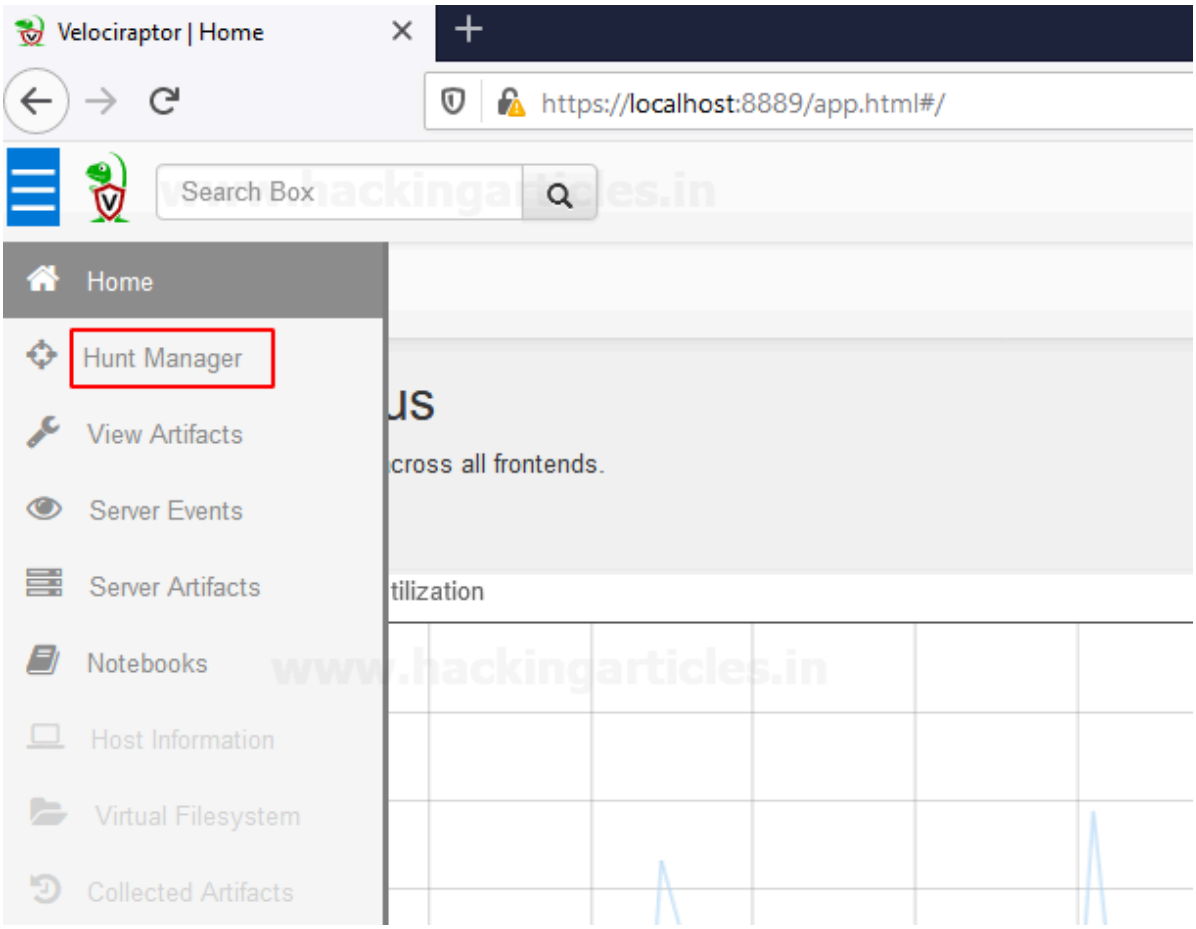
Hold tight! ?



Wow! It contains quite useful information

Let's dig it deeper

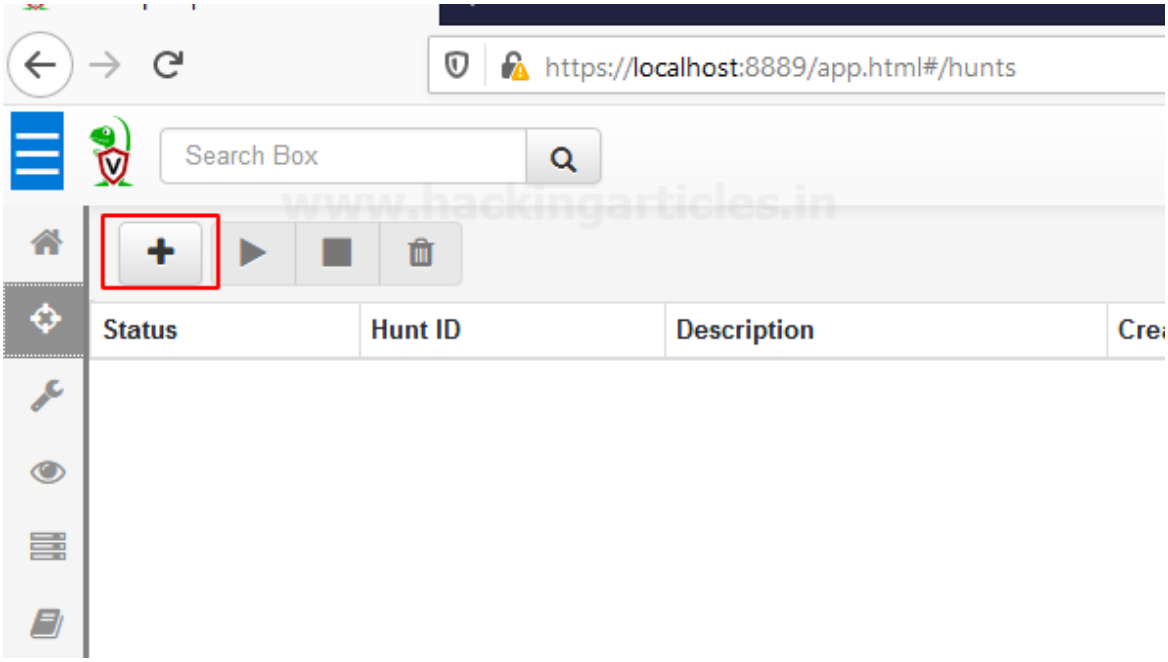
So now we have the **Hunt manager** you can easily find it on your Dashboard



Hunt manager allows you to hunt for the specific events that happened to your client and also you can view specific artifacts and you could see the server events as well and you could check server artifacts on the dashboard console of Velociraptor

Let's begin the **Hunt**

we need to create a hunt with specific artifacts To do this move your cursor to the **"+"** button and select it as shown below.

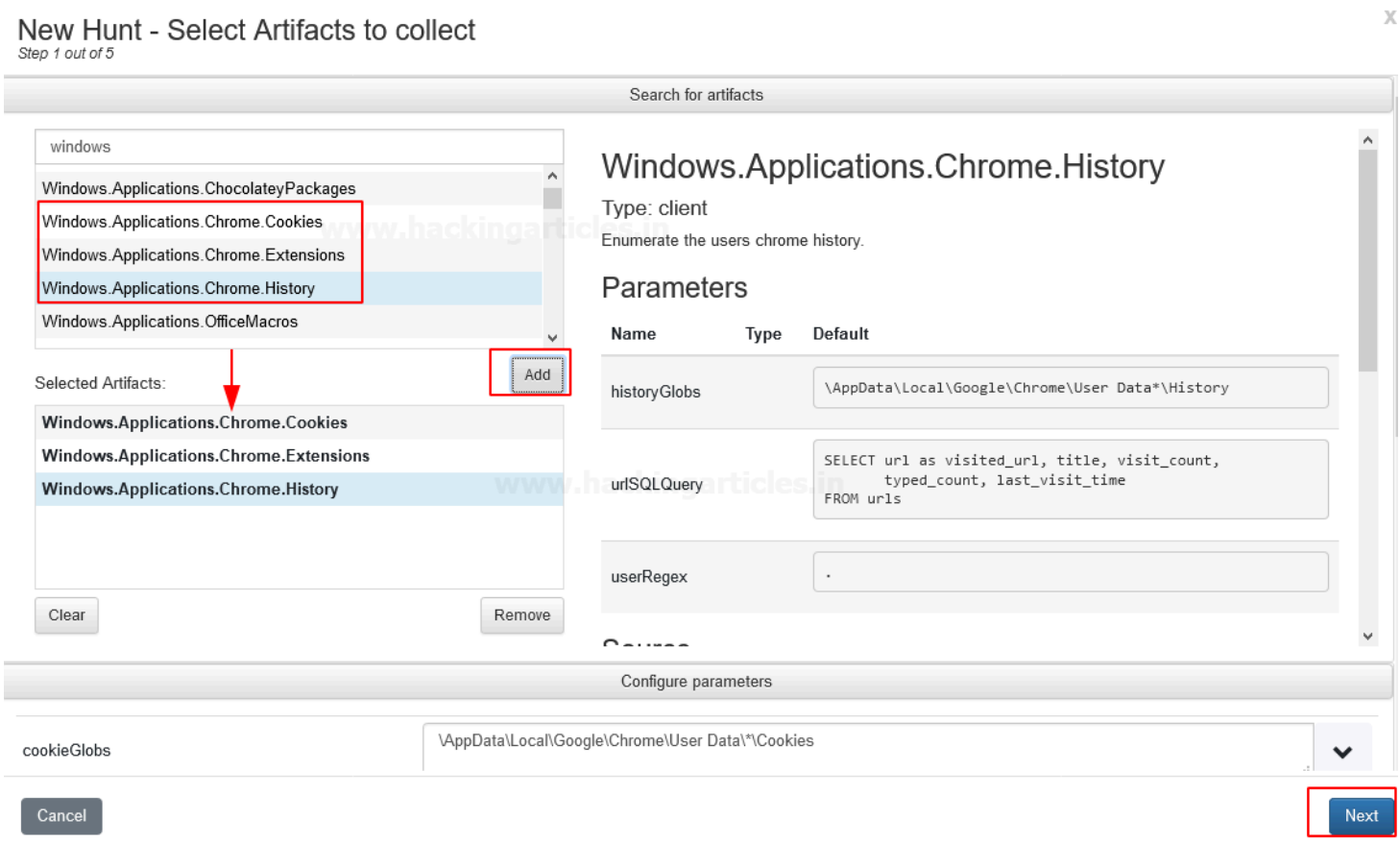


Chrome Hunting

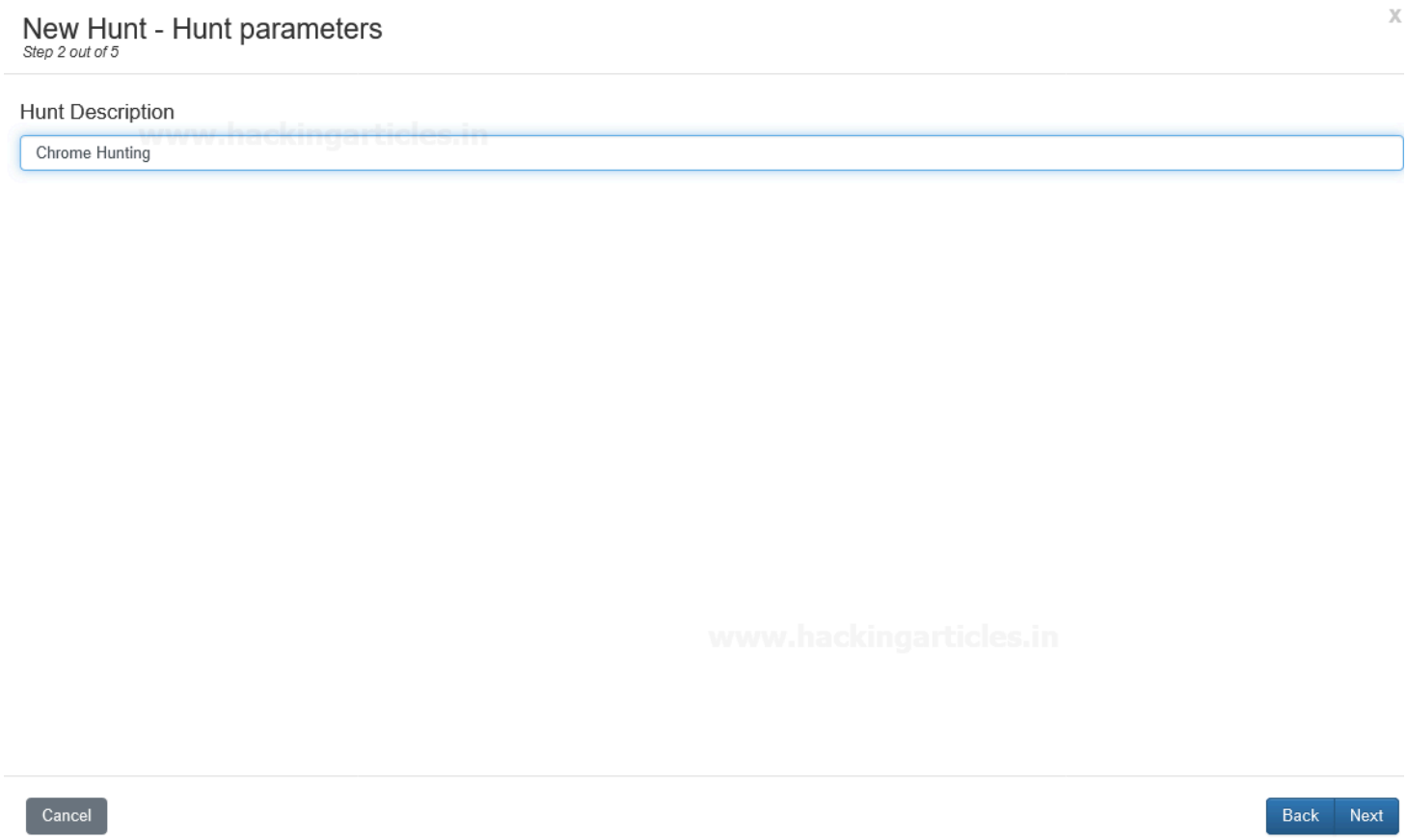
Now the time has come for us to like spy on our user HaHaHa ? with the help of our clients if they are using chrome so we are going to check on which website or page they have visited recently unless they are not using incognito mode

To create new hunt in the search window start typing windows then select the artifacts that you want to hunt and add then select **"Next"**,

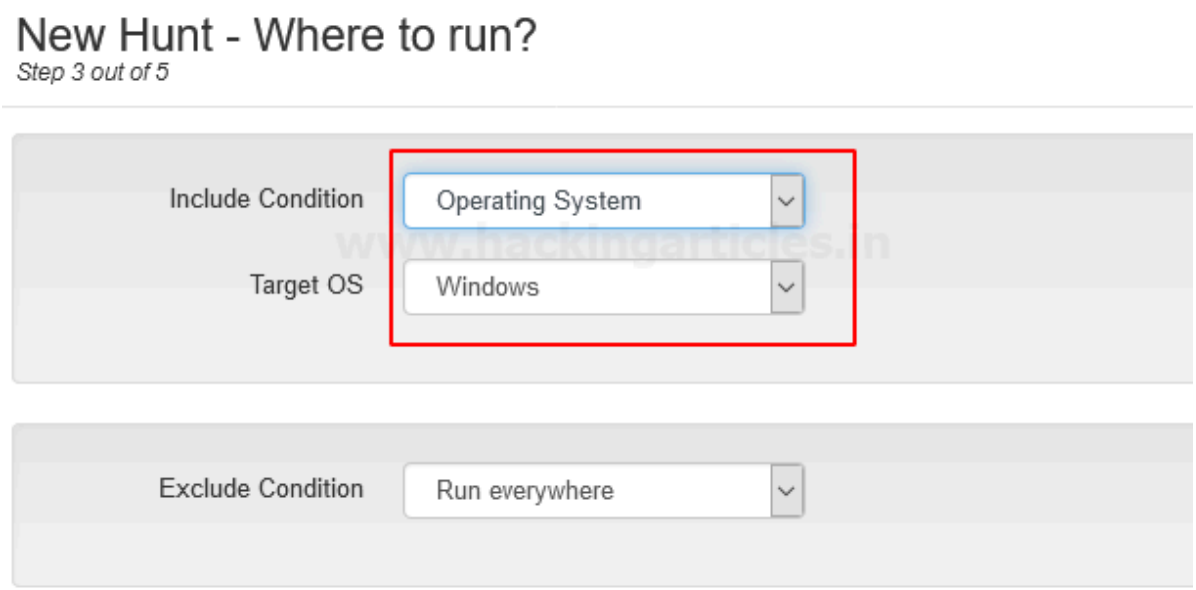
In my case, I'm selecting Chrome Cookies, Chrome Extensions, Chrome History you can select as much you want.



After selecting next it redirects you to next prompt when you need to Hunt Description and then select **"Next"**



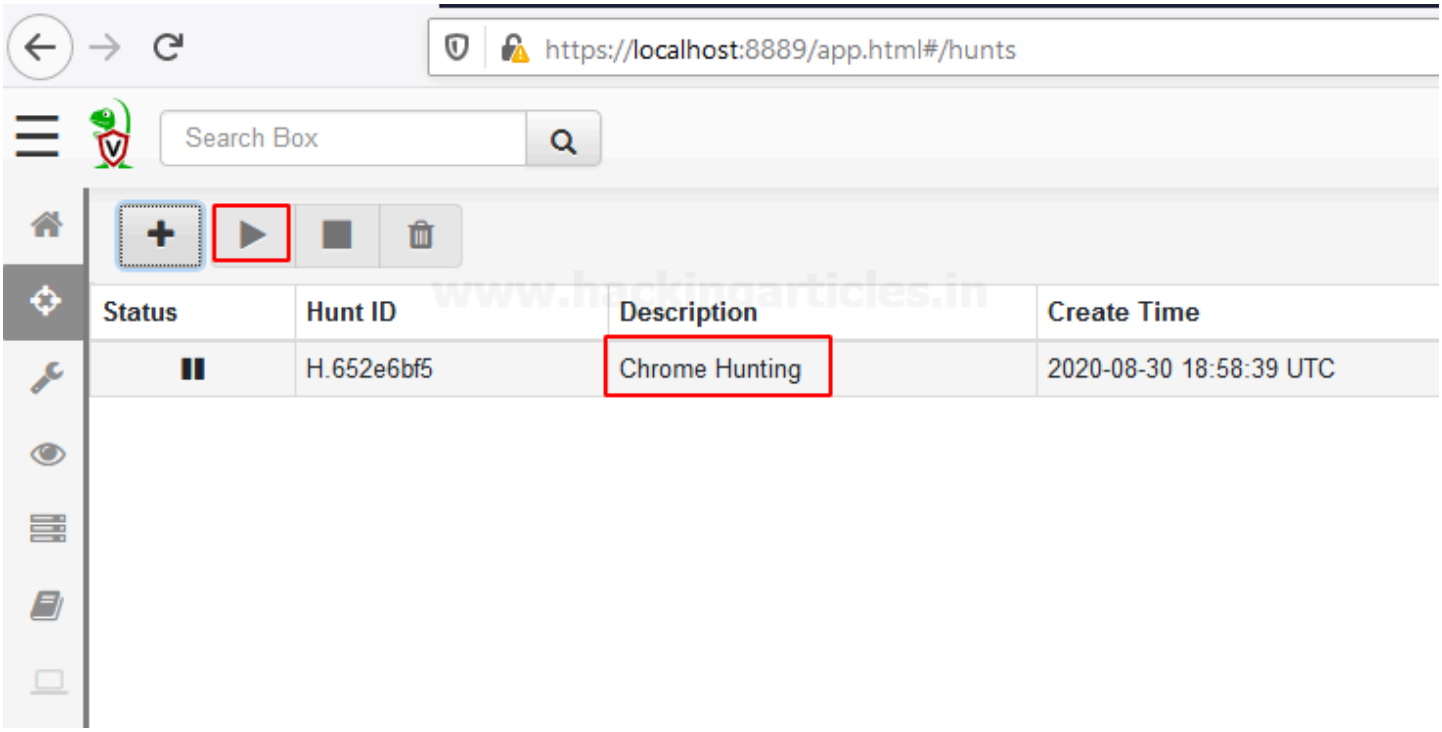
Hunt conditions should be in "**operating system"** select it in the drop-down menu of Include Condition then select Target OS **"Windows"** and then hit **"Next"**



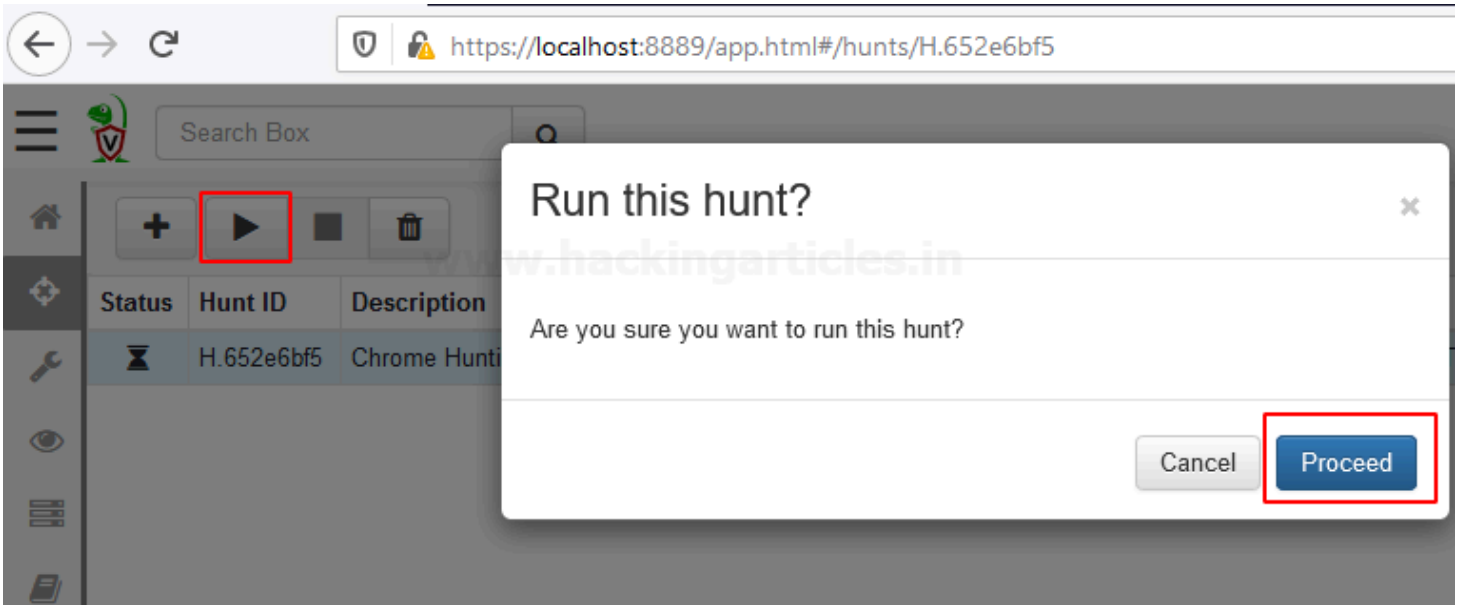
At next screen, you have your hunt Description or Artefact review if you do some modifications with the artifacts if needed otherwise leave it as default and then select option **"Create Hunt"**

Now we have created a new Hunt Named Chrome Hunting it reflects to your Hunts panel

And We would like to run this hunt by pressing the play button to see what's next in the result…

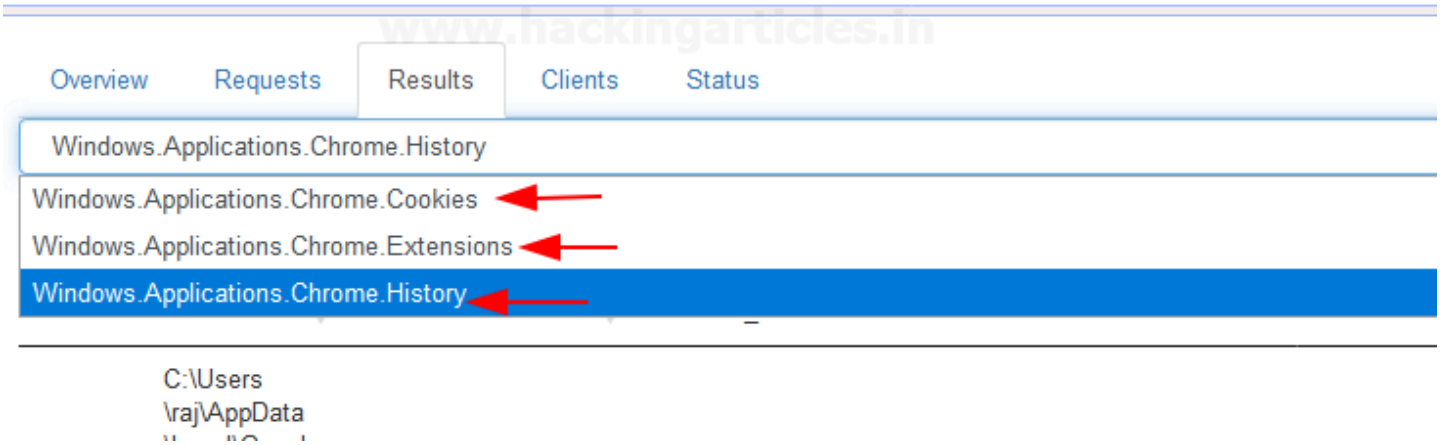


And then a pop flash on your screen that wants your permission to proceed…

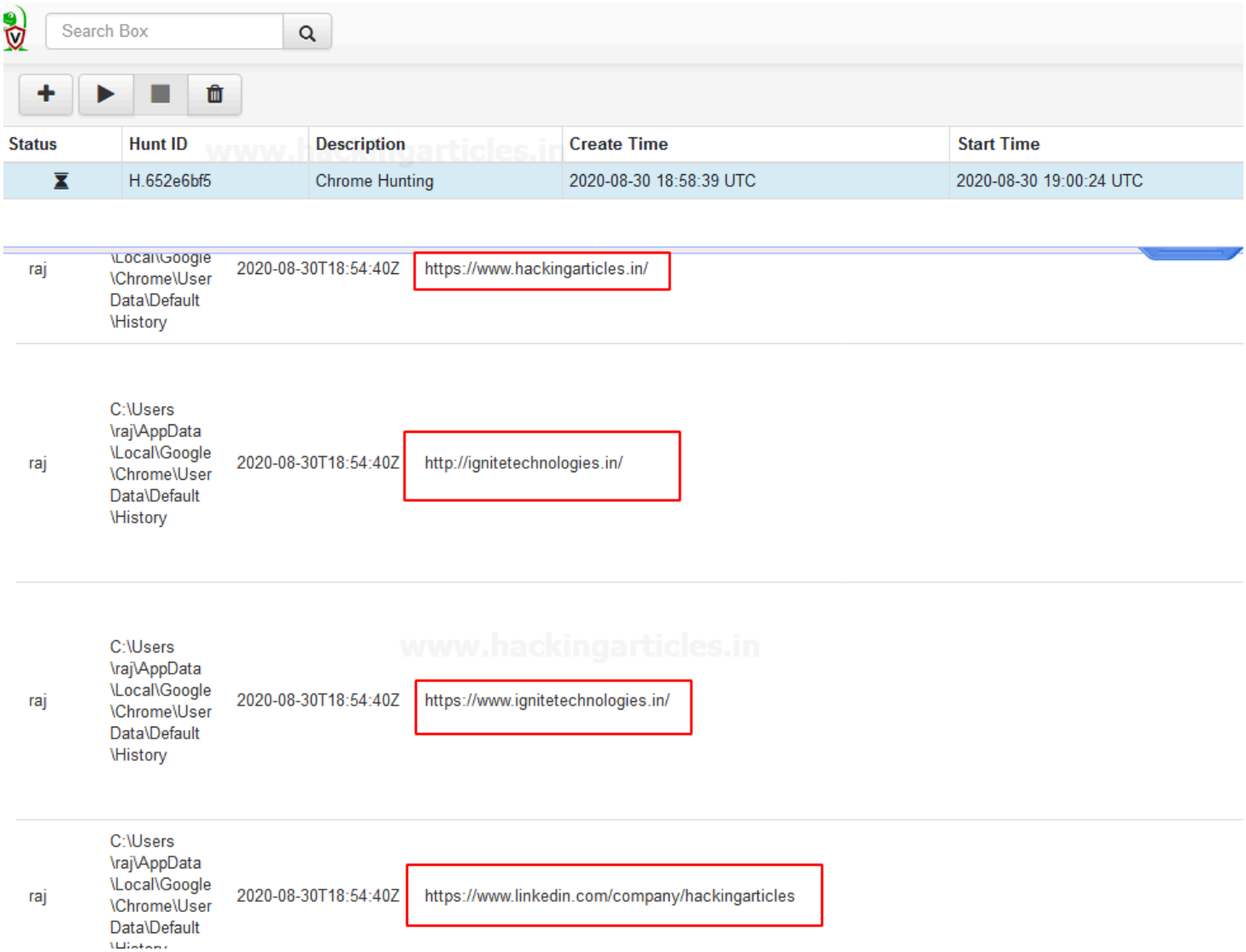


After proceeding it will take you to next screen where you have your hunt results you can select which results you want to see by drop down the Results tab

Status	Hunt ID	Description	Create Time
⧗	H.652e6bf5	Chrome Hunting	2020-08-30 18:58:39 UTC



As we can see we have a history of chrome that the client used to visit on the chrome



Also, we can see chrome cookies by select It form Results dropdown

Status	Hunt ID	Description	Create Time	Start Tim
⧗	H.652e6bf5	Chrome Hunting	2020-08-30 18:58:39 UTC	2020-08-3

Overview Requests Results Clients Status

Windows.Applications.Chrome.Cookies

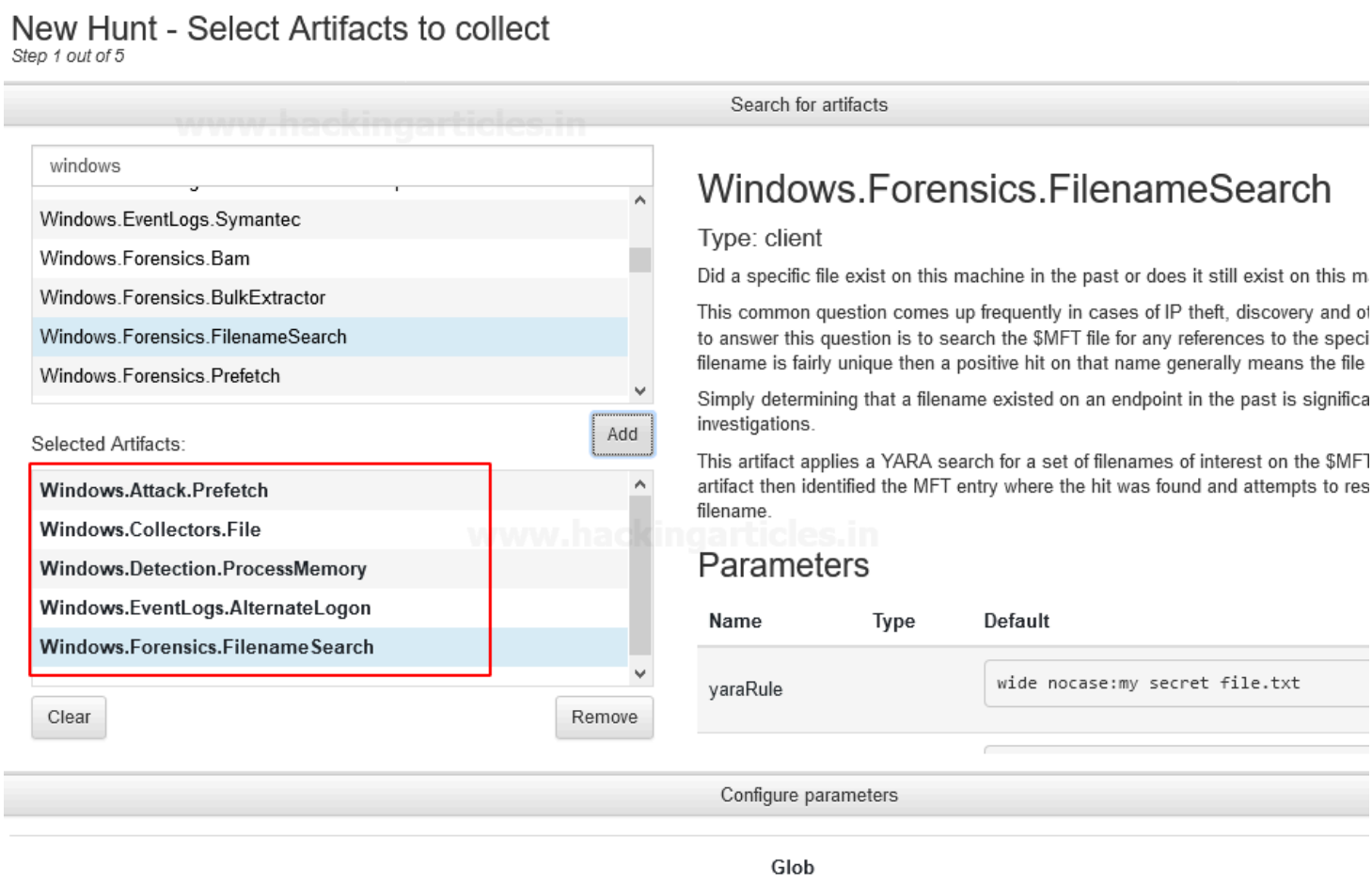
Show 10 entries

Created	LastAccess	Expires	host_key	name	path	value
2020-08-30T18:43:10Z	2020-08-30T18:43:10Z	2020-09-29T18:43:09Z	.hackingarticles.in	__cfduid	/	
2020-08-30T18:43:27Z	2020-08-30T18:43:27Z	2020-08-31T18:43:27Z	.twitter.com	tfw_exp	/	
2020-08-30T18:43:32Z	2020-08-30T18:43:32Z	2022-08-31T06:21:04Z	.linkedin.com	bcookie	/	
2020-08-30T18:43:32Z	2020-08-30T18:43:32Z	2022-08-31T06:21:04Z	.www.linkedin.com	bscookie	/	
2020-08-30T18:43:32Z	2020-08-30T18:43:32Z	2020-08-31T18:43:32Z	.linkedin.com	lidc	/	
2020-08-30T18:43:32Z	2020-08-30T18:43:32Z	2021-08-30T18:43:32Z	.linkedin.com	lissc	/	
2020-08-30T18:43:33Z	2020-08-30T18:43:33Z	2022-08-30T18:43:33Z	.linkedin.com	_ga	/	
2020-08-30T18:43:33Z	2020-08-30T18:43:33Z	2020-08-31T18:43:33Z	.linkedin.com	_gid	/	
2020-08-30T18:43:34Z	2020-08-30T18:43:34Z	2022-08-20T18:43:34Z	.scorecardresearch.com	UID	/	

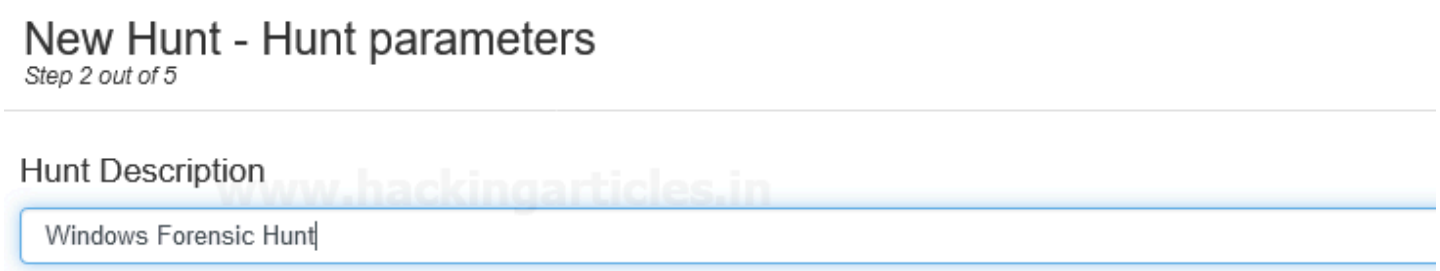
Let's Begin some Forensics investigation

Will do it by adding some predefined windows artifacts here, I'm using

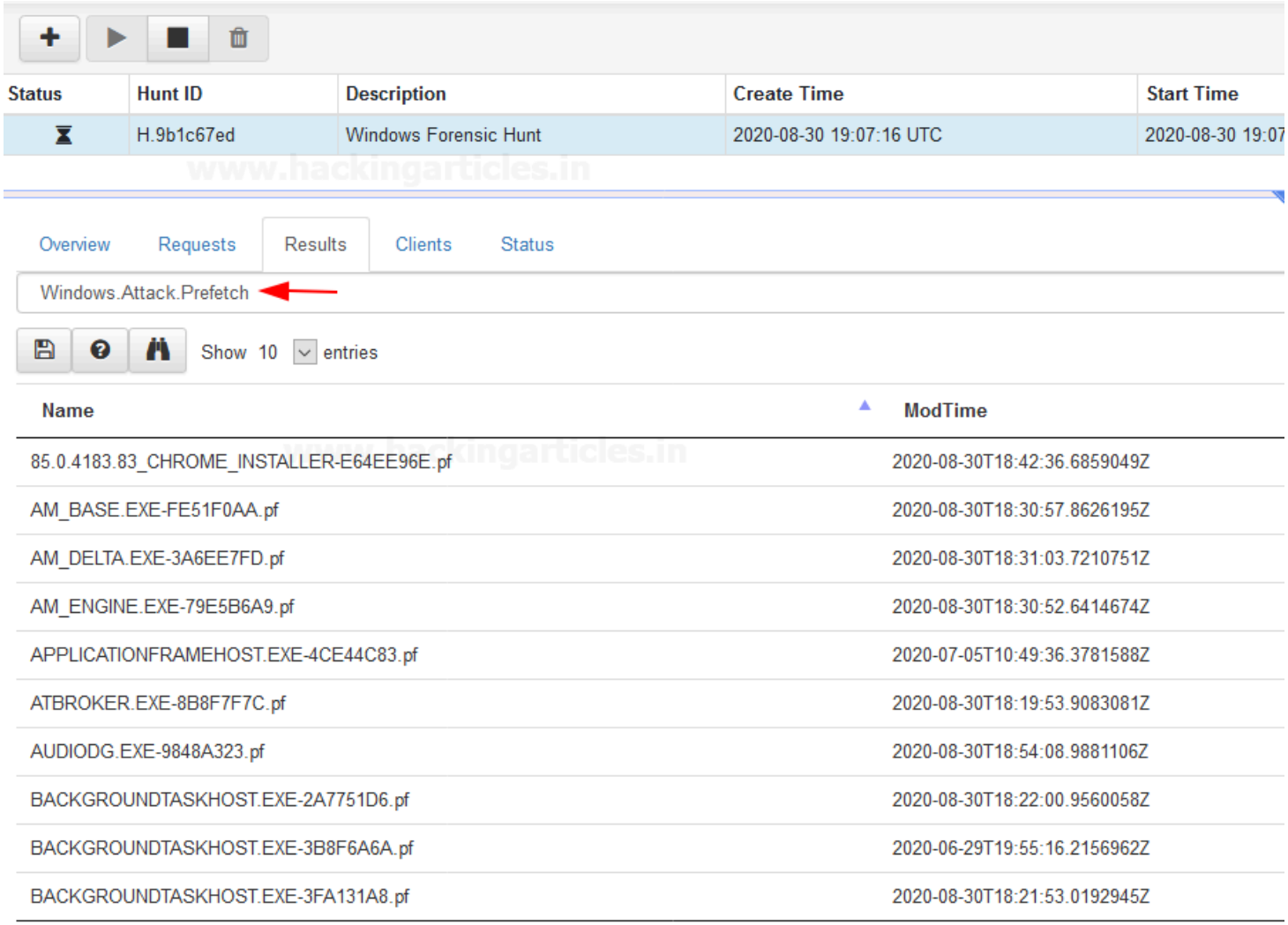
- Attack.Prefetch
- Collectors.File
- Detection.ProcessMemory
- EventLogs.AlternateLogon
- Forensics.FilenameSearch



Enter the Hunt Parameters or Hunt Description



And at the next screen, we have our Hunt results…. For example, if you want to see **"Windows.Attack.Prefetch"** select It form Results dropdown



Status	Hunt ID	Description	Create Time	Start Time
⧗	H.9b1c67ed	Windows Forensic Hunt	2020-08-30 19:07:16 UTC	2020-08-30 19:07

Overview | Requests | Results | Clients | Status

Windows.Attack.Prefetch

Show 10 entries

Name	ModTime
85.0.4183.83_CHROME_INSTALLER-E64EE96E.pf	2020-08-30T18:42:36.6859049Z
AM_BASE.EXE-FE51F0AA.pf	2020-08-30T18:30:57.8626195Z
AM_DELTA.EXE-3A6EE7FD.pf	2020-08-30T18:31:03.7210751Z
AM_ENGINE.EXE-79E5B6A9.pf	2020-08-30T18:30:52.6414674Z
APPLICATIONFRAMEHOST.EXE-4CE44C83.pf	2020-07-05T10:49:36.3781588Z
ATBROKER.EXE-8B8F7F7C.pf	2020-08-30T18:19:53.9083081Z
AUDIODG.EXE-9848A323.pf	2020-08-30T18:54:08.9881106Z
BACKGROUNDTASKHOST.EXE-2A7751D6.pf	2020-08-30T18:22:00.9560058Z
BACKGROUNDTASKHOST.EXE-3B8F6A6A.pf	2020-06-29T19:55:16.2156962Z
BACKGROUNDTASKHOST.EXE-3FA131A8.pf	2020-08-30T18:21:53.0192945Z

Same if you want to see **"Windows.EvemtLogs.AlternateLogon"** select it from result dropdown and hit enter….

Status	Hunt ID	Description	Create Time	Start Time
⧗	H.9b1c67ed	Windows Forensic Hunt	2020-08-30 19:07:16 UTC	2020-08-30 19:07:39 UTC

Overview Requests Results Clients Status

Windows.EventLogs.AlternateLogon

Show 10 entries

IpAddress	Port	ProcessName	SubjectUserSid	SubjectUserName
127.0.0.1	0	C:\Windows\System32\svchost.exe	S-1-5-18	WIN-QS6CDL0PEHM$
127.0.0.1	0	C:\Windows\System32\svchost.exe	S-1-5-18	WIN-QS6CDL0PEHM$
127.0.0.1	0	C:\Windows\System32\svchost.exe	S-1-5-18	DESKTOP-TT14AQK$
192.168.0.147	0	C:\Windows\System32\svchost.exe	S-1-5-18	DESKTOP-TT14AQK$
NaN	NaN	C:\Windows\System32\wininit.exe	S-1-5-18	MINWINPC$
NaN	NaN	C:\Windows\System32\winlogon.exe	S-1-5-18	MINWINPC$
NaN	NaN	C:\Windows\System32\winlogon.exe	S-1-5-18	MINWINPC$
NaN	NaN	C:\Windows\System32\wininit.exe	S-1-5-18	WIN-QS6CDL0PEHM$
NaN	NaN	C:\Windows\System32\winlogon.exe	S-1-5-18	WIN-QS6CDL0PEHM$
NaN	NaN	C:\Windows\System32\winlogon.exe	S-1-5-18	WIN-QS6CDL0PEHM$

Similarly, you can Dig it much Deeper by adding as many artifacts as you need

Hang tight this is not enough!

More will be discussed in part **2nd**.