Threat Hunting: Velociraptor for Endpoint Monitoring

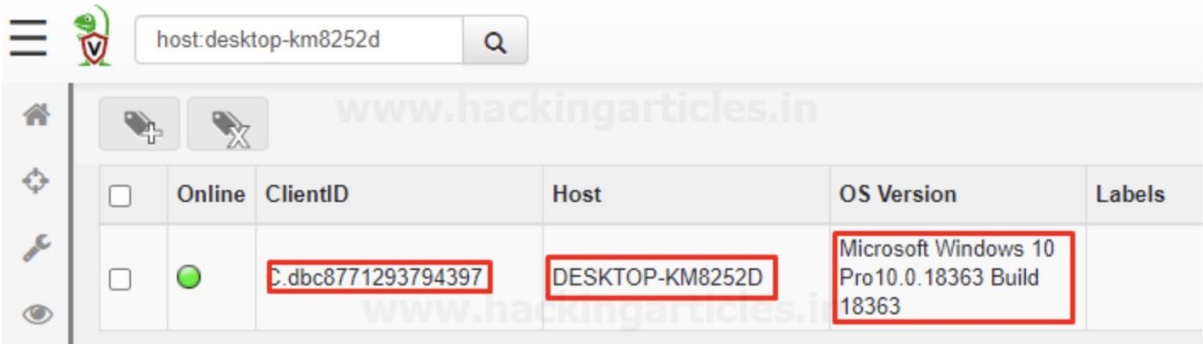
1. Introduction to Velociraptor

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

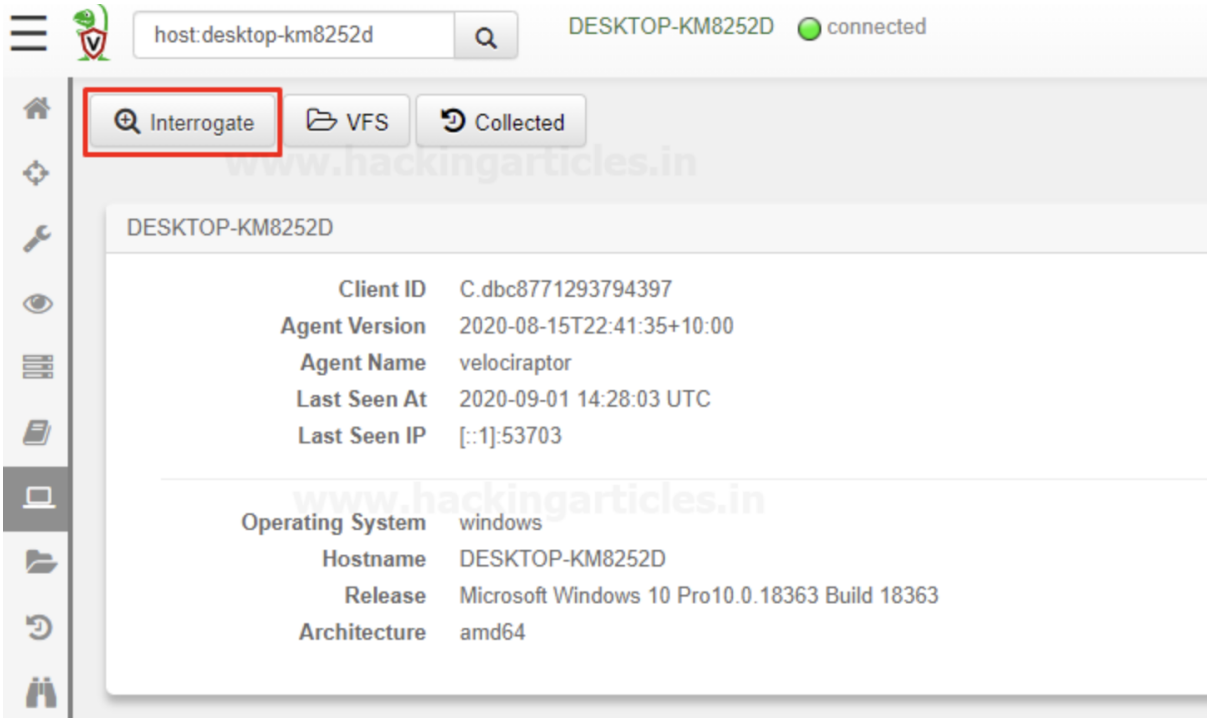
Velociraptor natively works on Linux, Windows, and macOS. You can create or deploy a server within few minutes using SCCM or Group policy.

2. Threat Hunting

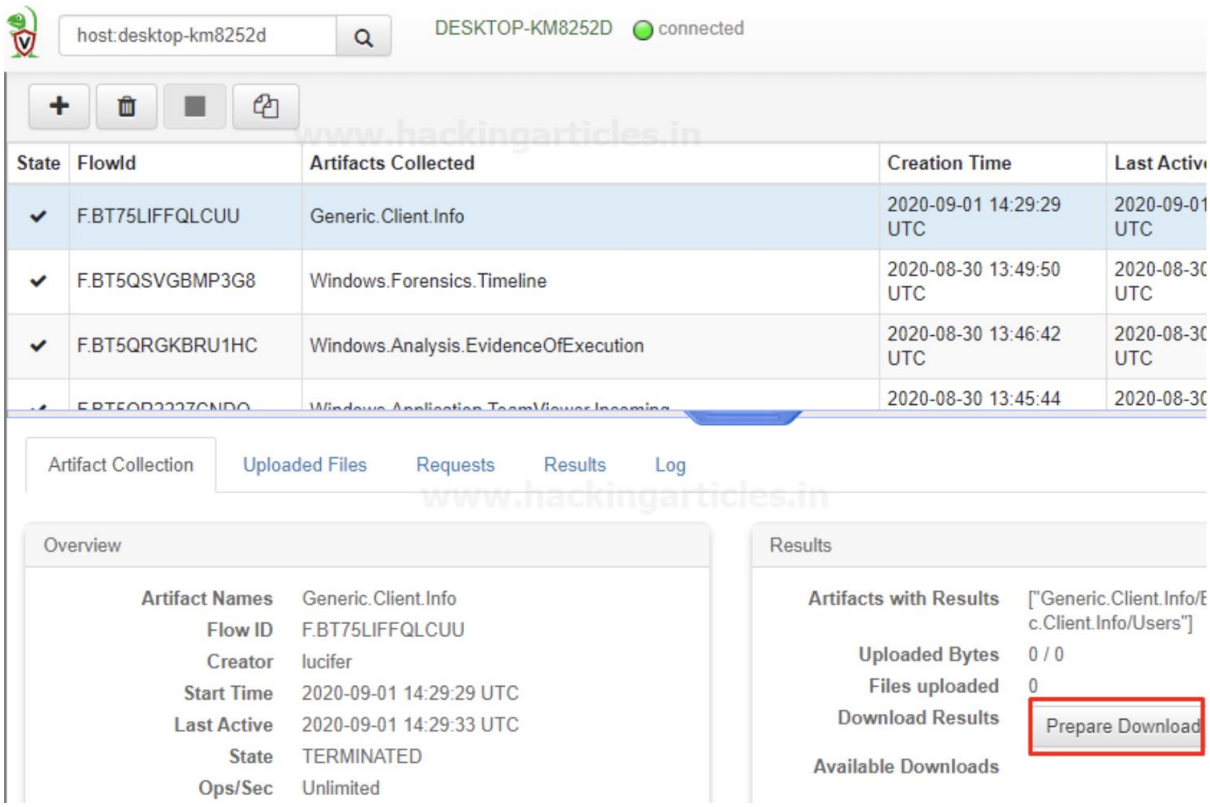
you could be able to see your host by searching in the filter box.



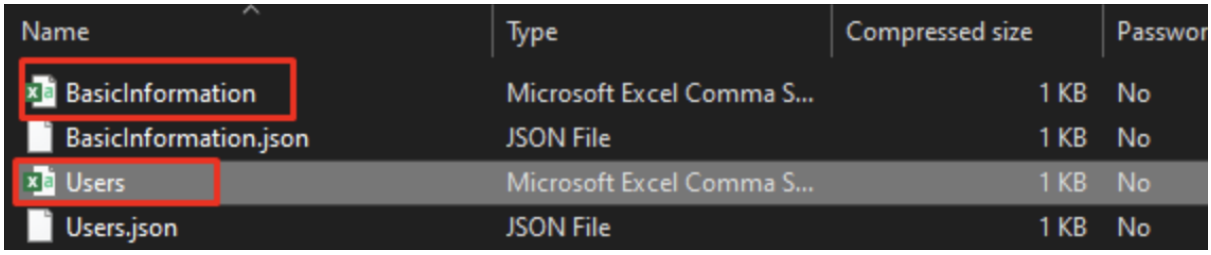
And then you can see the host have a client id, hostname OS version, and so on….



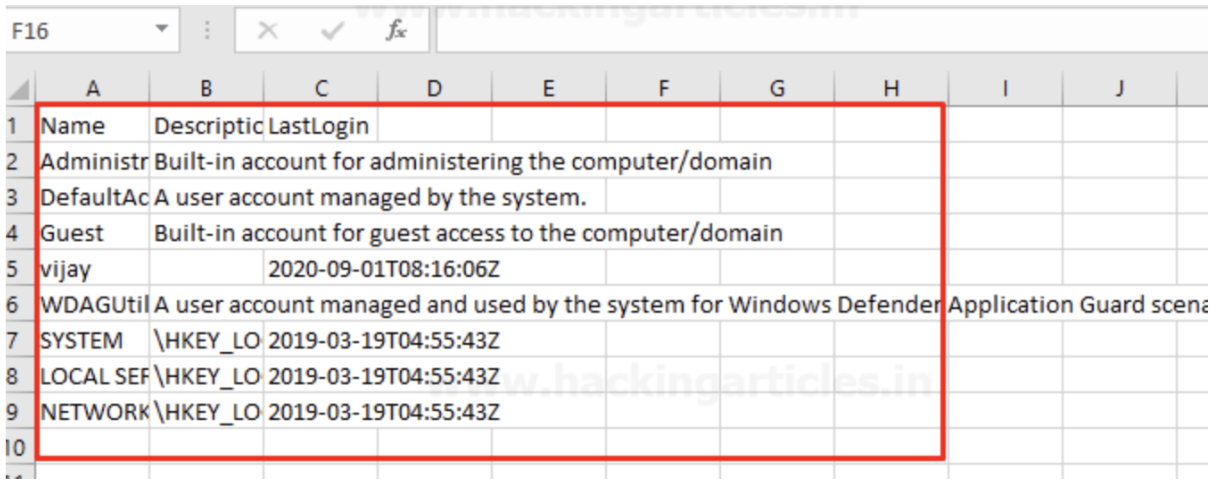
And we could interrogate the host and we could check collected information and by default, some basic information is collected about clients.



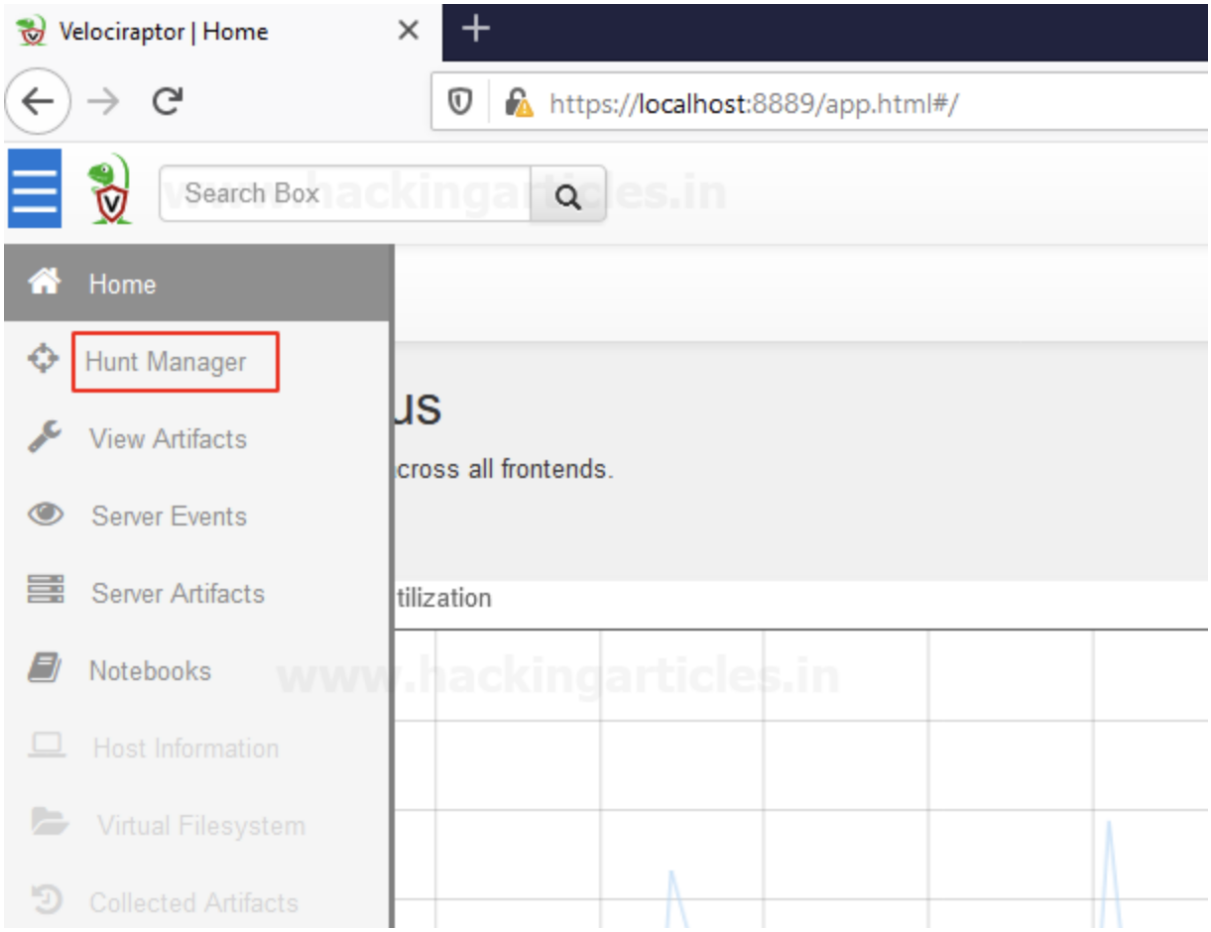
So now what we can and should do is to try to figure out what's inside this information by downloading it. As we can see a zip folder downloaded inside downloads after opening it you can see these files there that contain the host details.



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.

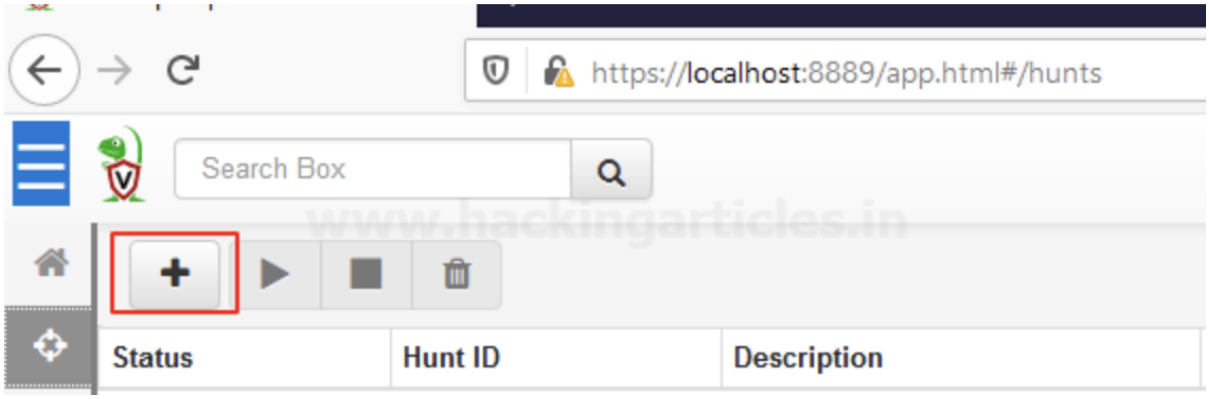


I believe that it contains quite useful information, and **let's dig it deeper**. So now we have the **Hunt manager** you can easily find it on your Dashboard.



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.

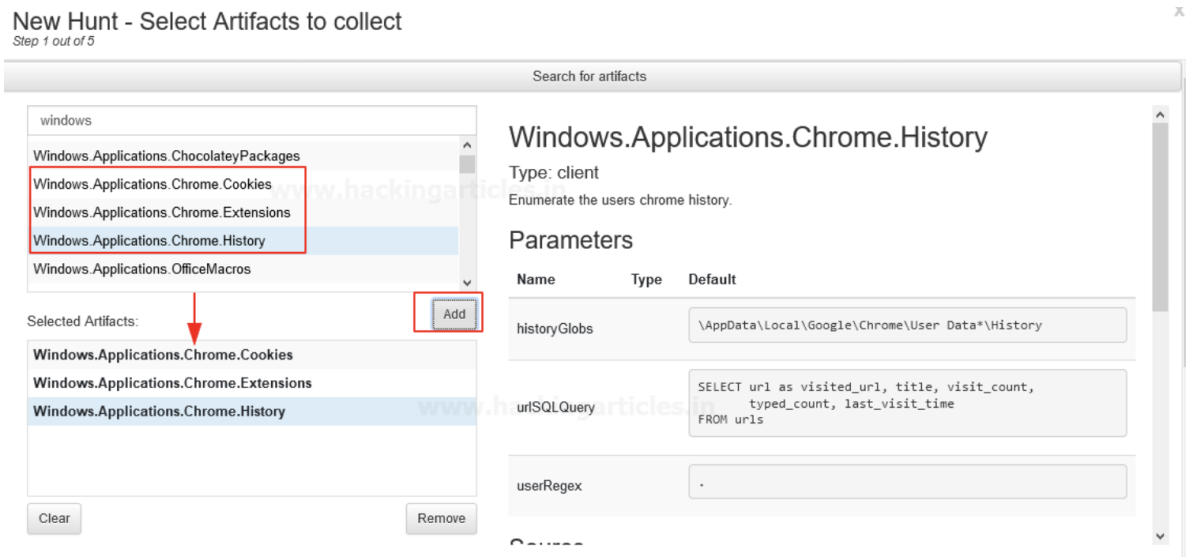


3. Chrome Hunting

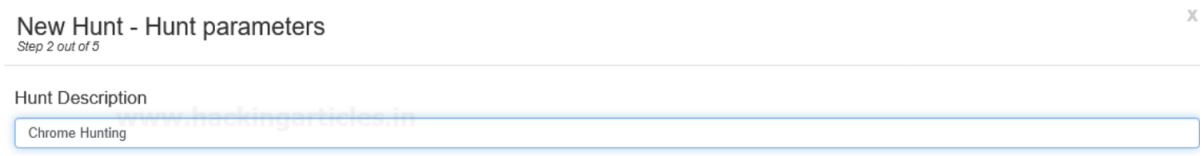
If they are using chrome so we are going to check on which website or page they have visited recently unless they are not using incognito mode.

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”**,

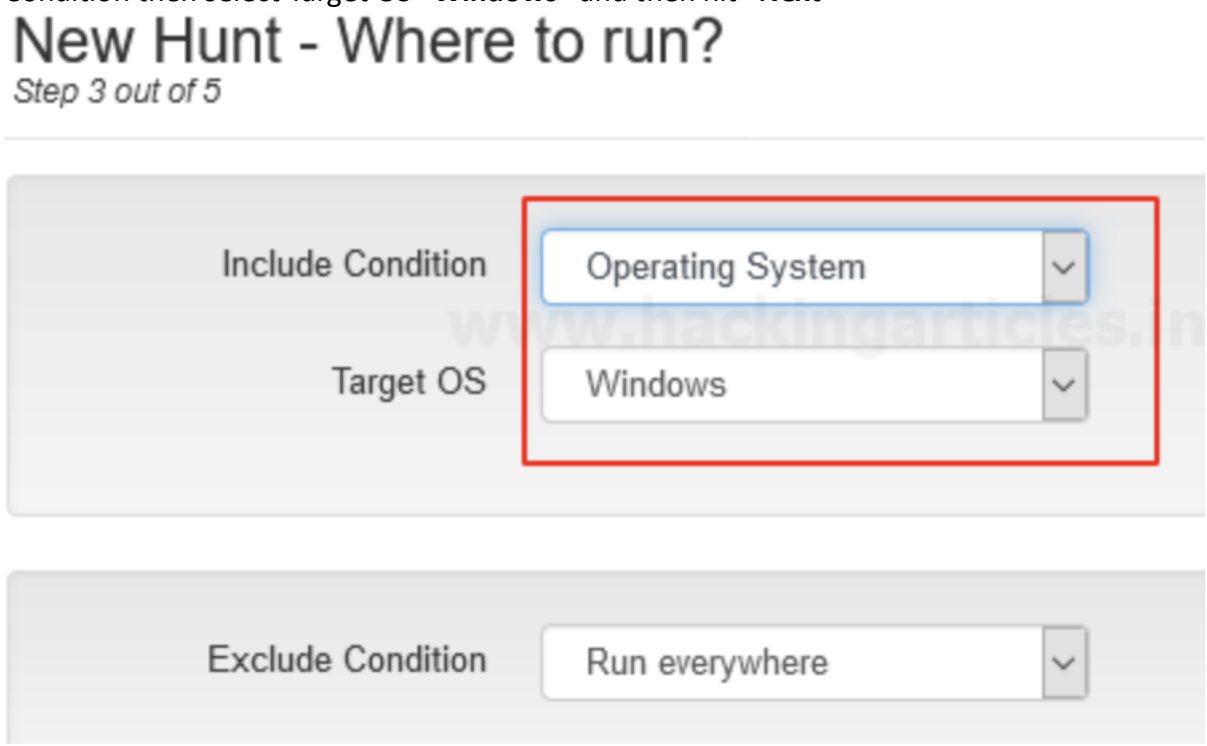
In my case, I’m selecting Chrome Cookies, Chrome Extensions, Chrome History you can select as much you want.



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

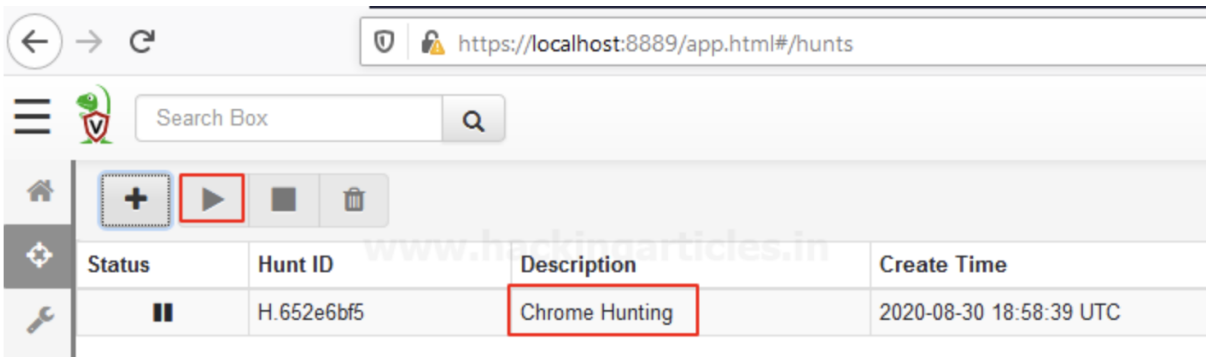


Hunt conditions should be in “**operating system”** select it in the drop-down menu of Include Condition then select Target OS **“Windows”** and then hit **“Next”**

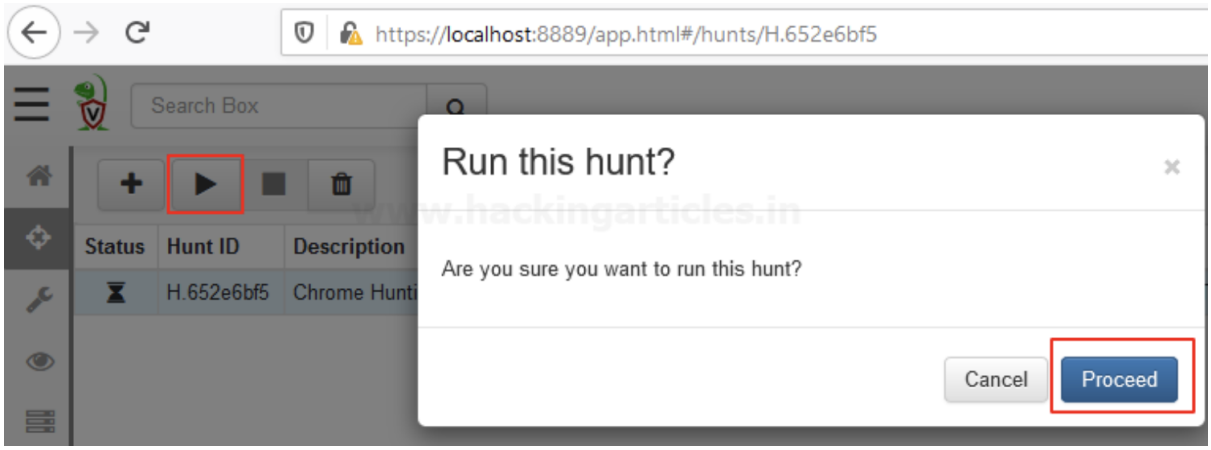


At next screen, you have your hunt Description or Artefact review if you do some modifications with the artifacts if needed otherwise leave it as default and then select option **“Create Hunt”**

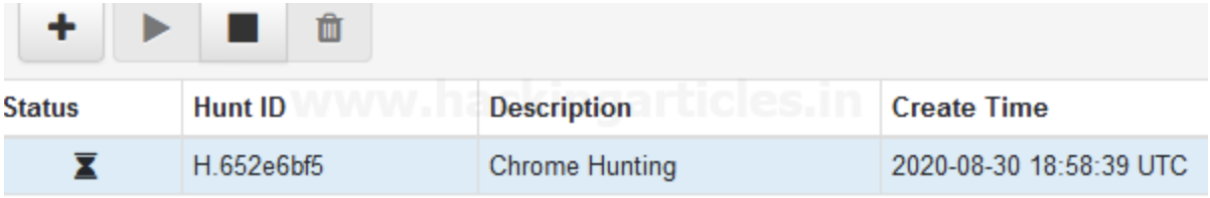
Now we have created a new Hunt Named Chrome Hunting it reflects to your Hunts panel. And we would like to run this hunt by pressing the play button to see what’s next in the result…



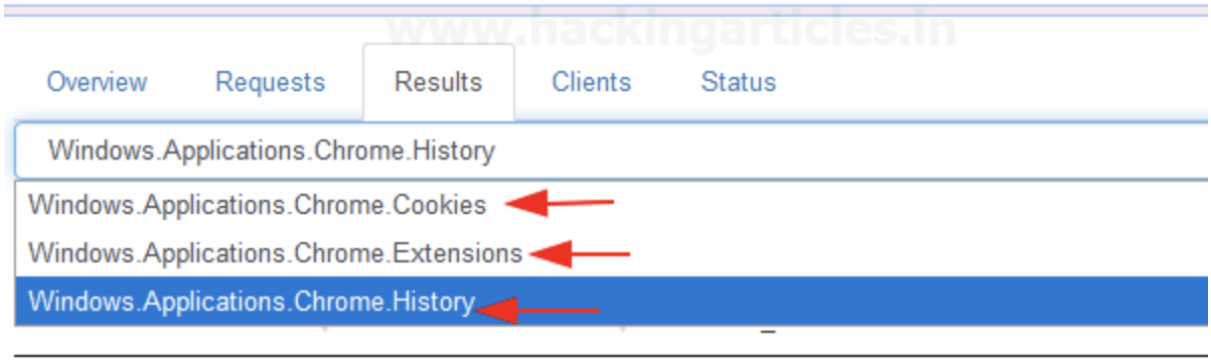
And then a pop flash on your screen that wants your permission to proceed…



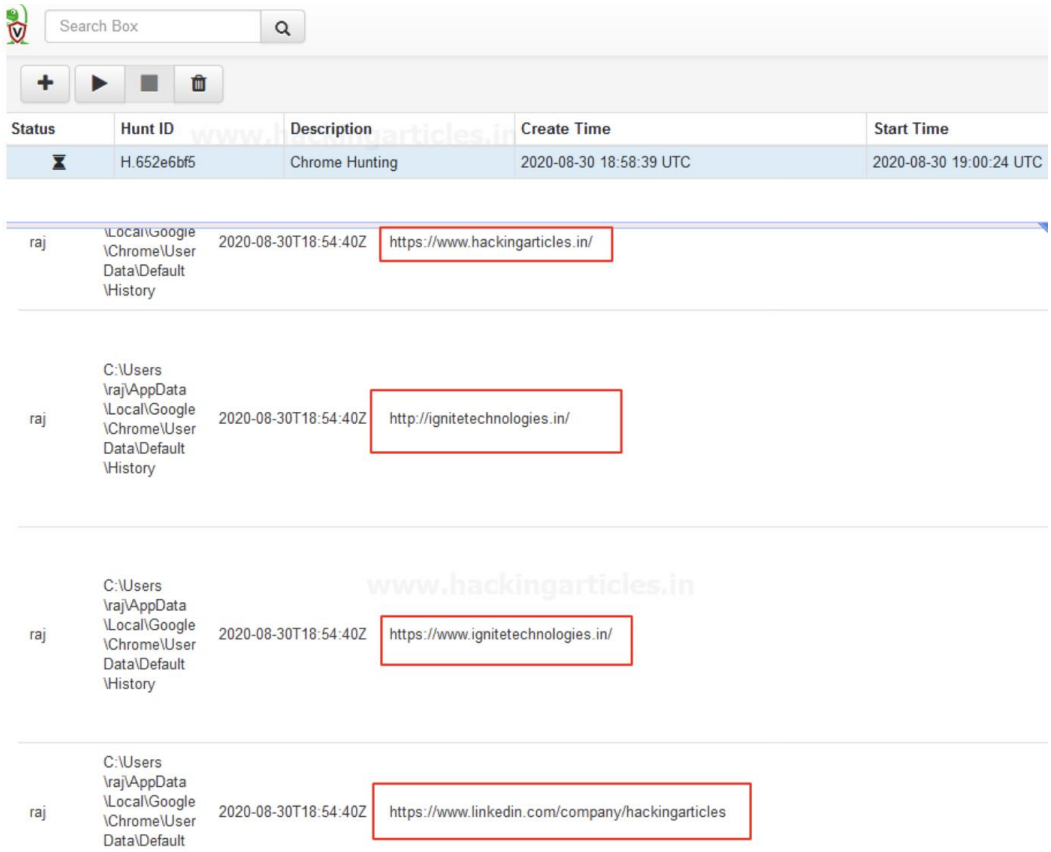
After proceeding it will take you to next screen where you have your hunt results you can select which results you want to see by drop down the Results tab



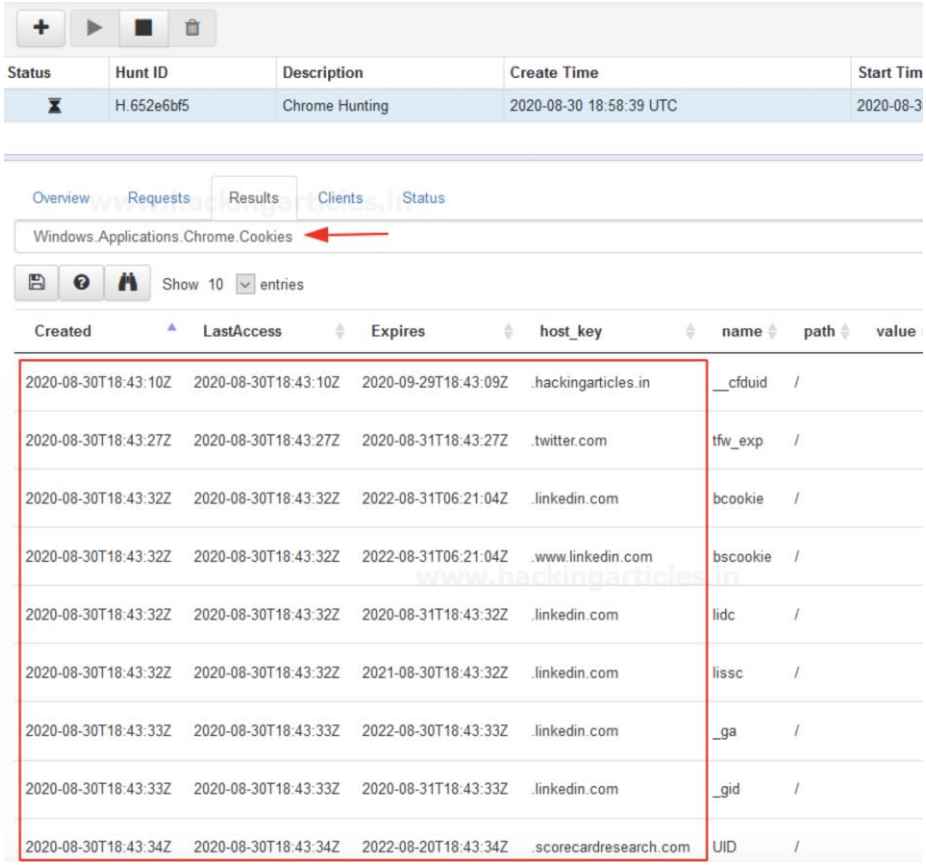
Status	Hunt ID	Description	Create Time
⧗	H.652e6bf5	Chrome Hunting	2020-08-30 18:58:39 UTC



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



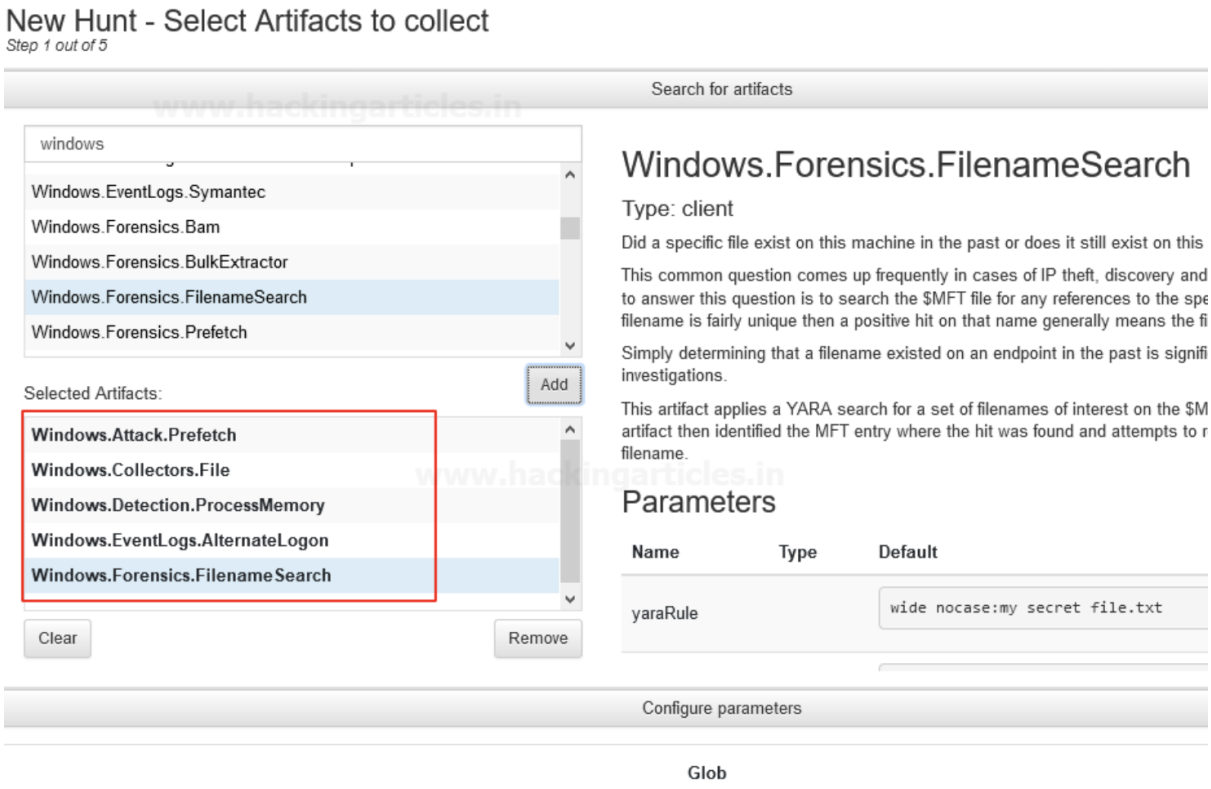
Also, we can see chrome cookies by select It form Results dropdown



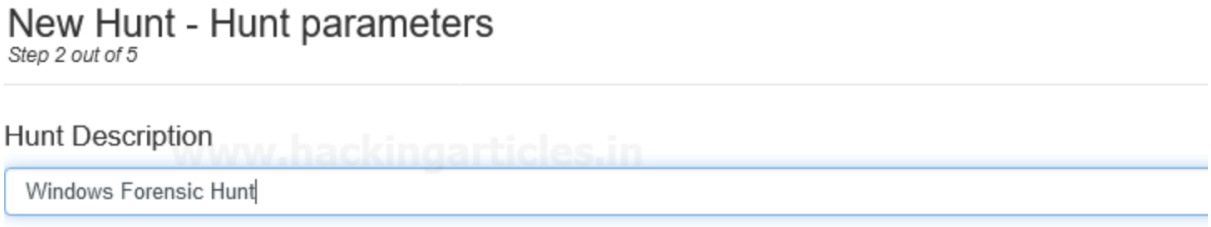
4. Forensics investigation

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

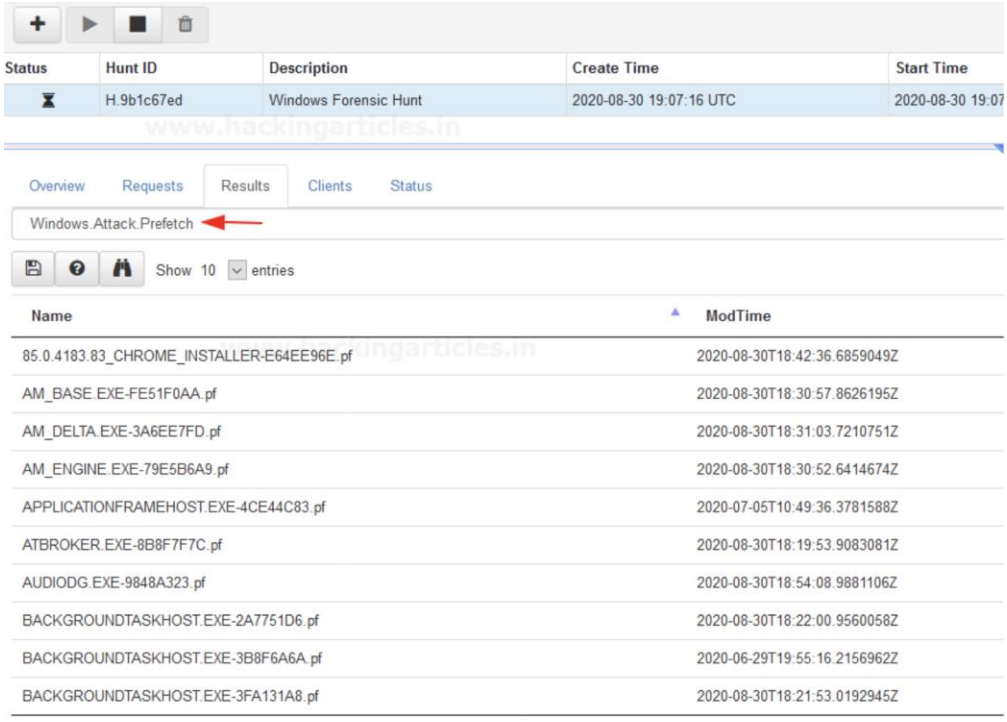
- Attack.Prefetch
- Collectors.File
- Detection.ProcessMemory
- EventLogs.AlternateLogon
- Forensics.FilenameSearch



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

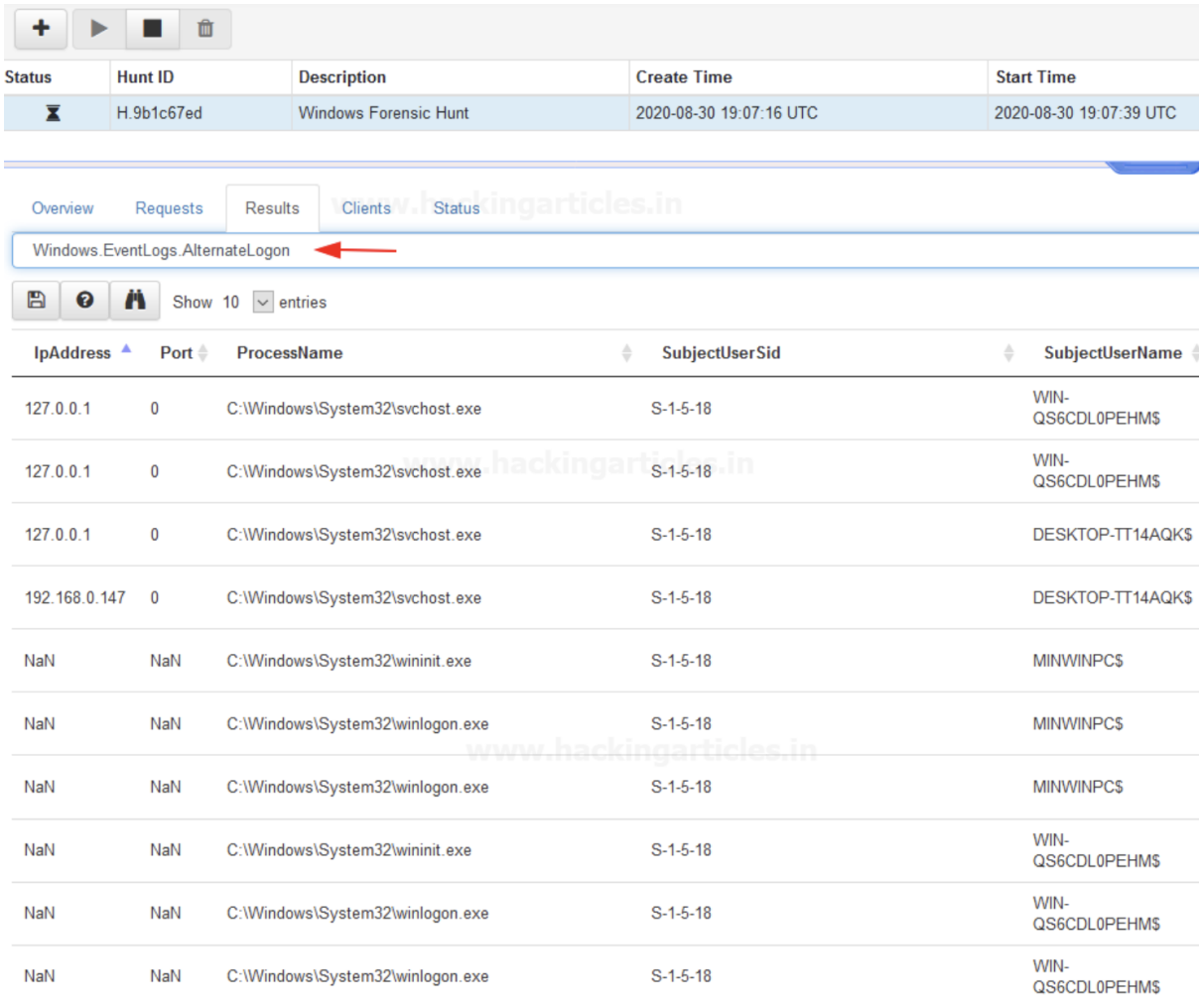
Overview | Requests | Results | Clients | Status

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$