

# Threat Hunting: Velociraptor for Endpoint Monitoring

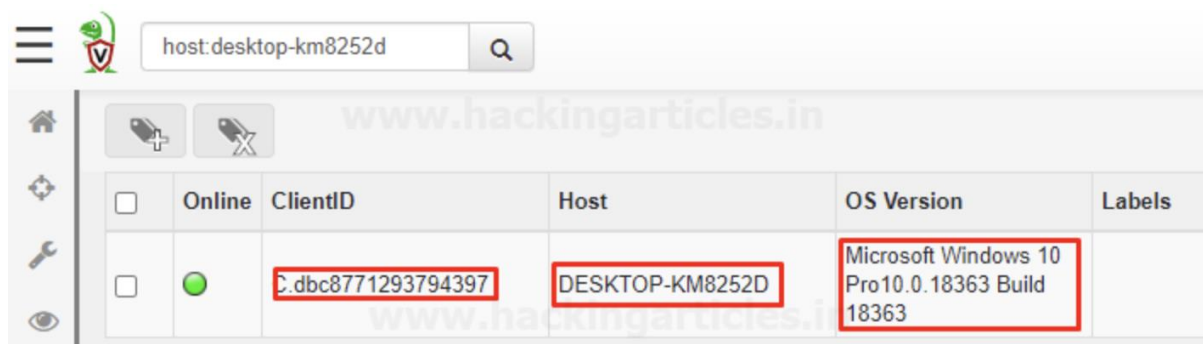
## 1. Introduction to Velociraptor

Velociraptor is a free and open-source software project developed by the Velocidex Company. Velociraptor is generally based on GRR, OSQuery, and Google's Rekal 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

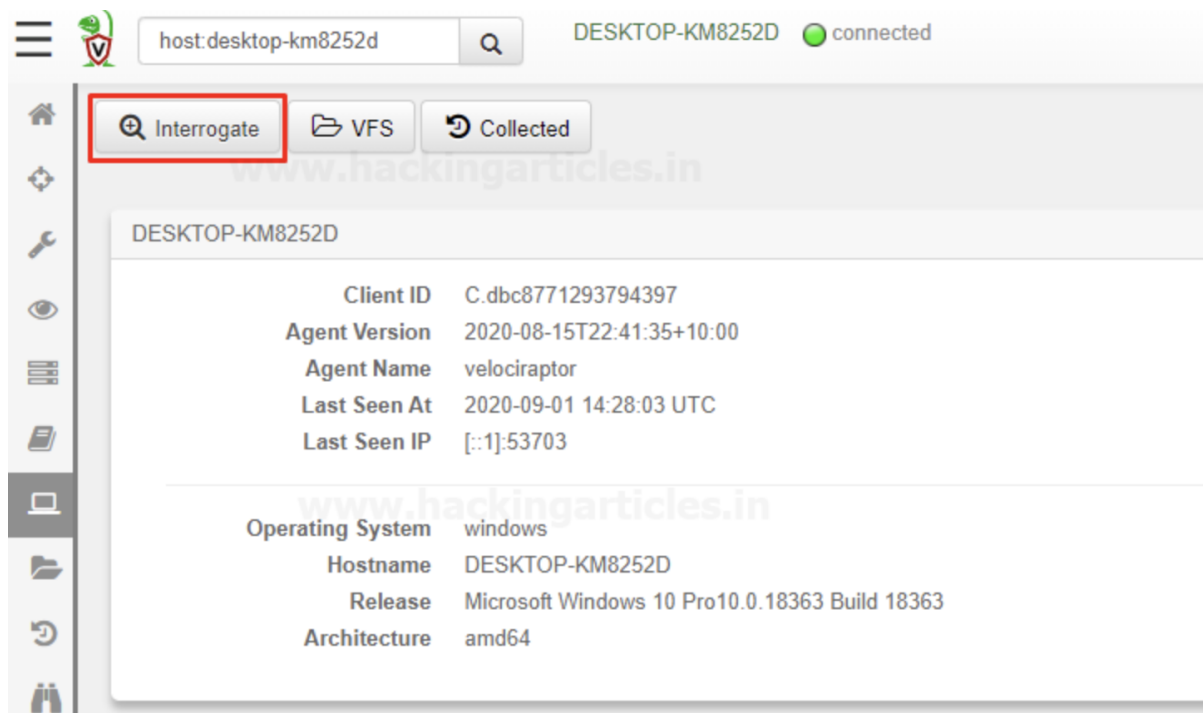
Velociraptor natively works on Linux, Windows, and macOS. You can create or deploy a server within few minutes using SCCM or Group policy.

## 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.

host:desktop-km8252d DESKTOP-KM8252D connected

State	FlowId	Artifacts Collected	Creation Time	Last Active
✓	F.BT75LIFFQLCUU	Generic.Client.Info	2020-09-01 14:29:29 UTC	2020-09-01 14:29:33 UTC
✓	F.BT5QSVGBMP3G8	Windows.Forensics.Timeline	2020-08-30 13:49:50 UTC	2020-08-30 13:49:50 UTC
✓	F.BT5QRGKBRU1HC	Windows.Analysis.EvidenceOfExecution	2020-08-30 13:46:42 UTC	2020-08-30 13:46:42 UTC
✓	F.BT5QD2327CNDQ	Windows.Application.TeamViewerAccessing	2020-08-30 13:45:44 UTC	2020-08-30 13:45:44 UTC

Artifact Collection Uploaded Files Requests Results Log

Overview

Artifact Names Generic.Client.Info

Flow ID F.BT75LIFFQLCUU

Creator lucifer

Start Time 2020-09-01 14:29:29 UTC

Last Active 2020-09-01 14:29:33 UTC

State TERMINATED

Ops/Sec Unlimited

Results

Artifacts with Results ["Generic.Client.Info/EvidenceOfExecution/"]

Uploaded Bytes 0 / 0

Files uploaded 0

Download Results **Prepare Download**

Available Downloads

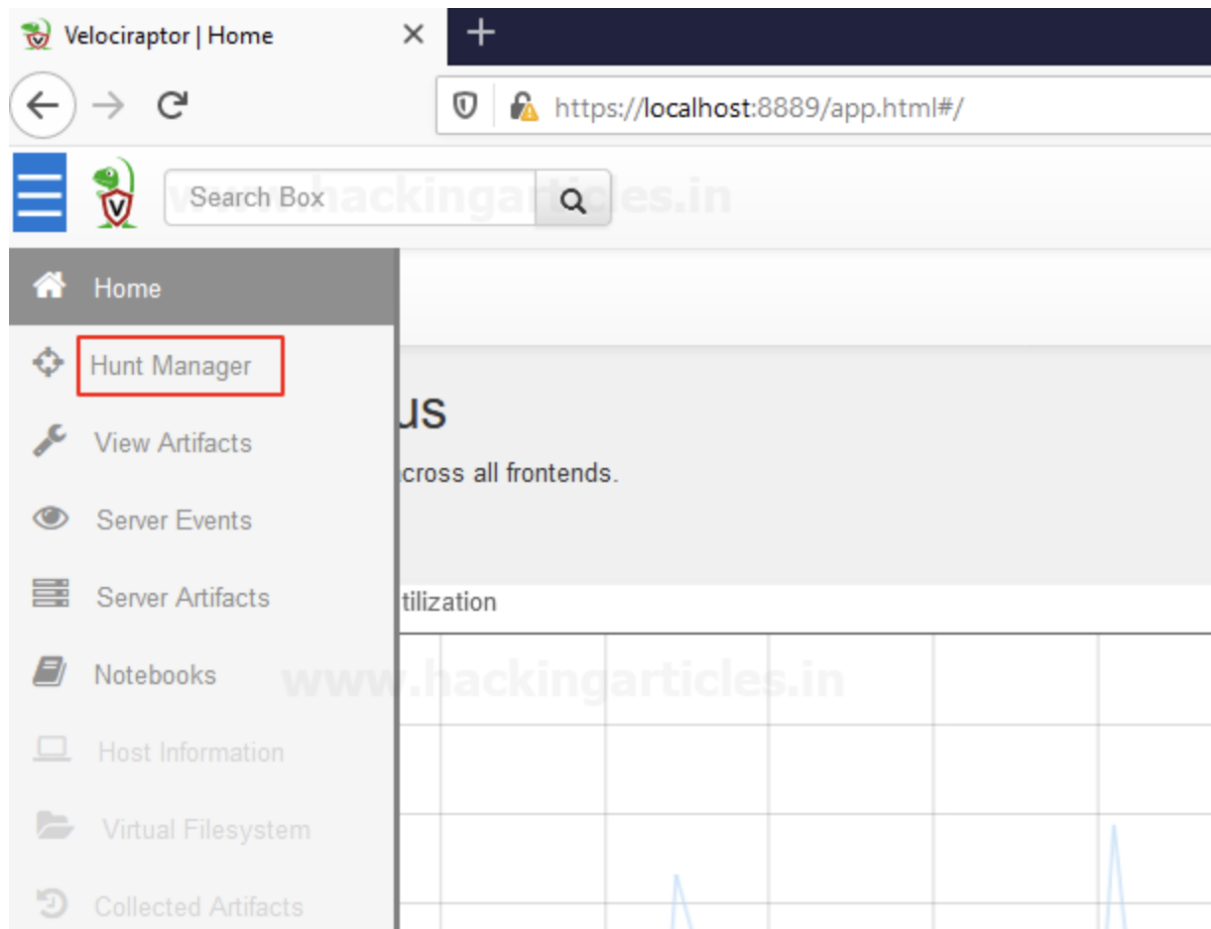
So now what we can and should do is to try to figure out what's inside this information by downloading it. As we can see a zip folder downloaded inside downloads after opening it you can see these files there that contain the host details.

Name	Type	Compressed size	Password
<b>BasicInformation</b>	Microsoft Excel Comma S...	1 KB	No
BasicInformation.json	JSON File	1 KB	No
<b>Users</b>	Microsoft Excel Comma S...	1 KB	No
Users.json	JSON File	1 KB	No

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.

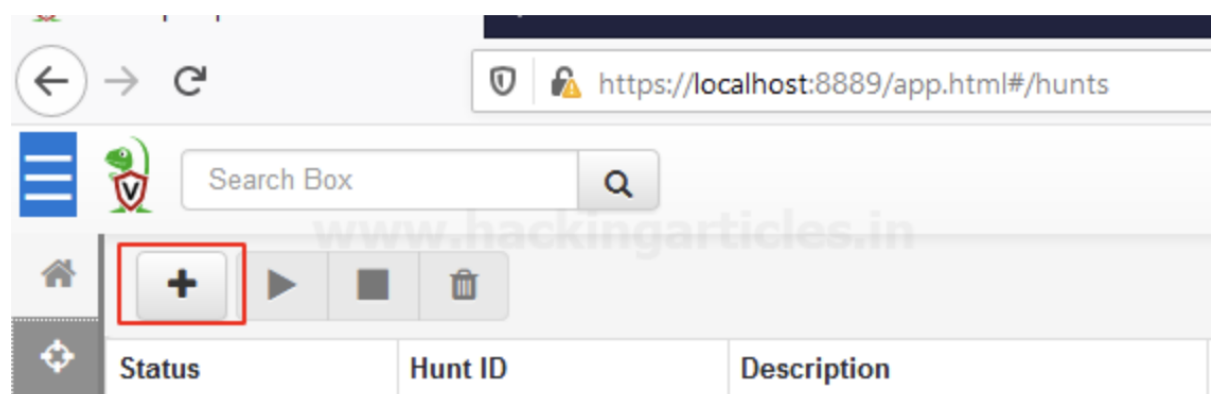
Name	Descriptic	LastLogin
Administr	Built-in account for administering the computer/domain	
DefaultAc	A user account managed by the system.	
Guest	Built-in account for guest access to the computer/domain	
vijay		2020-09-01T08:16:06Z
WDAGUtil	A user account managed and used by the system for Windows Defender Application Guard scena	
SYSTEM	\HKEY_LO	2019-03-19T04:55:43Z
LOCAL SEF	\HKEY_LO	2019-03-19T04:55:43Z
NETWORK	\HKEY_LO	2019-03-19T04:55:43Z

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.

New Hunt - Select Artifacts to collect  
Step 1 out of 5

Search for artifacts

windows

- Windows.Applications.ChocolateyPackages
- Windows.Applications.Chrome.Cookies
- Windows.Applications.Chrome.Extensions
- Windows.Applications.Chrome.History
- Windows.Applications.OfficeMacros

Selected Artifacts:

- Windows.Applications.Chrome.Cookies
- Windows.Applications.Chrome.Extensions
- Windows.Applications.Chrome.History

Clear Remove

Windows.Applications.Chrome.History

Type: client

Enumerate the users chrome history.

Parameters

Name	Type	Default
historyGlobs		\\AppData\\Local\\Google\\Chrome\\User Data*\\History
urlSQLQuery		SELECT url as visited_url, title, visit_count, typed_count, last_visit_time FROM urls
userRegex		*

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

New Hunt - Hunt parameters  
Step 2 out of 5

Hunt Description

Chrome Hunting

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”**

## New Hunt - Where to run?

Step 3 out of 5

Include Condition

Operating System

Target OS

Windows

Exclude Condition

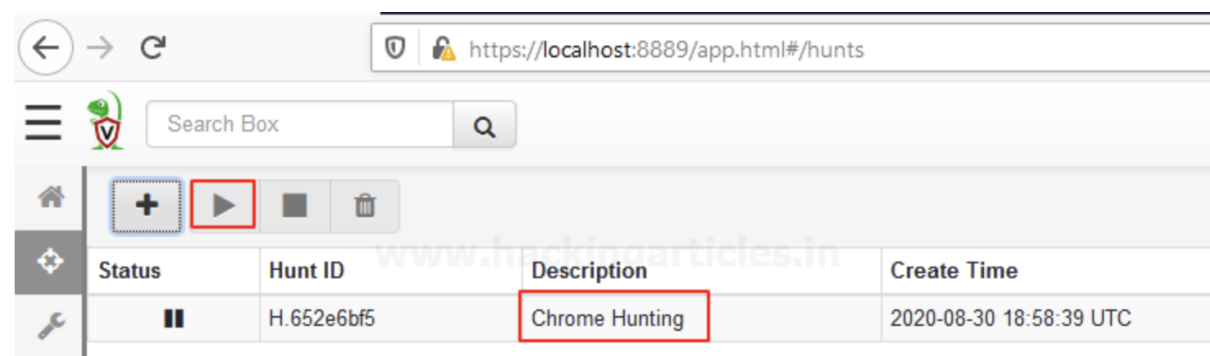
Run everywhere

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”**

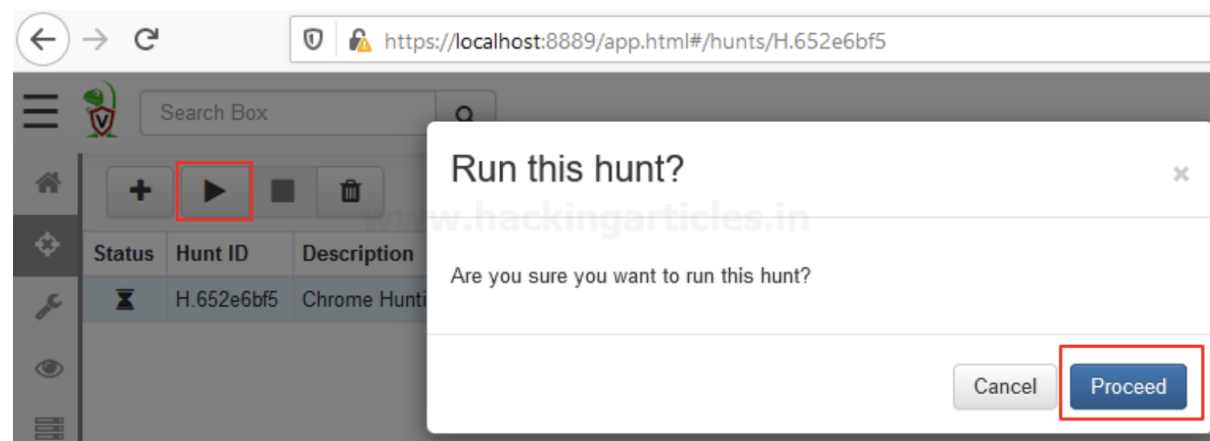
New Hunt - Review  
Step 4 out of 5



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

<div><div>+</div><div>▶</div><div>■</div><div>🗑</div></div>			
Status	Hunt ID	Description	Create Time
⌚	H.652e6bf5	Chrome Hunting	2020-08-30 18:58:39 UTC

Overview	Requests	Results	Clients	Status
Windows.Applications.Chrome.History				
Windows.Applications.Chrome.Cookies				
Windows.Applications.Chrome.Extensions				
Windows.Applications.Chrome.History				

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

<div> <input type="text" value="Search Box"/> </div>				
<div> </div>				
Status	Hunt ID	Description	Create Time	Start Time
	H.652e6bf5	Chrome Hunting	2020-08-30 18:58:39 UTC	2020-08-30 19:00:24 UTC
raj	\\Local\\Google\\Chrome\\User Data\\Default\\History	2020-08-30T18:54:40Z	<a href="https://www.hackingarticles.in/">https://www.hackingarticles.in/</a>	
raj	C:\\Users\\raj\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\History	2020-08-30T18:54:40Z	<a href="http://ignitetechnologies.in/">http://ignitetechnologies.in/</a>	
raj	C:\\Users\\raj\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\History	2020-08-30T18:54:40Z	<a href="https://www.ignitetechnologies.in/">https://www.ignitetechnologies.in/</a>	
raj	C:\\Users\\raj\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\History	2020-08-30T18:54:40Z	<a href="https://www.linkedin.com/company/hackingarticles">https://www.linkedin.com/company/hackingarticles</a>	

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

<div> </div>						
Status	Hunt ID	Description	Create Time	Start Time		
	H.652e6bf5	Chrome Hunting	2020-08-30 18:58:39 UTC	2020-08-30		
<div> <a href="#">Overview</a> <a href="#">Requests</a> <a href="#">Results</a> <a href="#">Clients</a> <a href="#">Status</a> </div>						
<div> Windows Applications Chrome Cookies </div>						
<div>    Show 10 entries </div>						
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	/	

## 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

### New Hunt - Select Artifacts to collect

Step 1 out of 5

Search for artifacts

windows

- Windows.EventLogs.Symantec
- Windows.Forensics.Bam
- Windows.Forensics.BulkExtractor
- Windows.Forensics.FilenameSearch
- Windows.Forensics.Prefetch

Selected Artifacts:

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

Add

Clear

Remove

### Windows.Forensics.FilenameSearch

Type: client

Did a specific file exist on this machine in the past or does it still exist on this machine? This common question comes up frequently in cases of IP theft, discovery and to answer this question is to search the \$MFT file for any references to the specific filename. A fairly unique hit on that name generally means the file existed. Simply determining that a filename existed on an endpoint in the past is significant for investigations. This artifact applies a YARA search for a set of filenames of interest on the \$MFT artifact then identified the MFT entry where the hit was found and attempts to retrieve the filename.

### Parameters

Name	Type	Default
yaraRule		wide nocase:my secret file.txt

Configure parameters

Glob

Enter the Hunt Parameters or Hunt Description

### New Hunt - Hunt parameters

Step 2 out of 5

#### Hunt Description

Windows Forensic Hunt

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 19:07:16 UTC

[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-8B8F77FC.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.EventLogs.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-QS6CDL0PEHMS
127.0.0.1	0	C:\Windows\System32\svchost.exe	S-1-5-18	WIN-QS6CDL0PEHMS
127.0.0.1	0	C:\Windows\System32\svchost.exe	S-1-5-18	DESKTOP-TT14AQKS
192.168.0.147	0	C:\Windows\System32\svchost.exe	S-1-5-18	DESKTOP-TT14AQKS
NaN	NaN	C:\Windows\System32\wininit.exe	S-1-5-18	MINWINPCS
NaN	NaN	C:\Windows\System32\winlogon.exe	S-1-5-18	MINWINPCS
NaN	NaN	C:\Windows\System32\winlogon.exe	S-1-5-18	MINWINPCS
NaN	NaN	C:\Windows\System32\wininit.exe	S-1-5-18	WIN-QS6CDL0PEHMS
NaN	NaN	C:\Windows\System32\winlogon.exe	S-1-5-18	WIN-QS6CDL0PEHMS
NaN	NaN	C:\Windows\System32\winlogon.exe	S-1-5-18	WIN-QS6CDL0PEHMS