NCT Bloodhound Neo4j Instructions v4

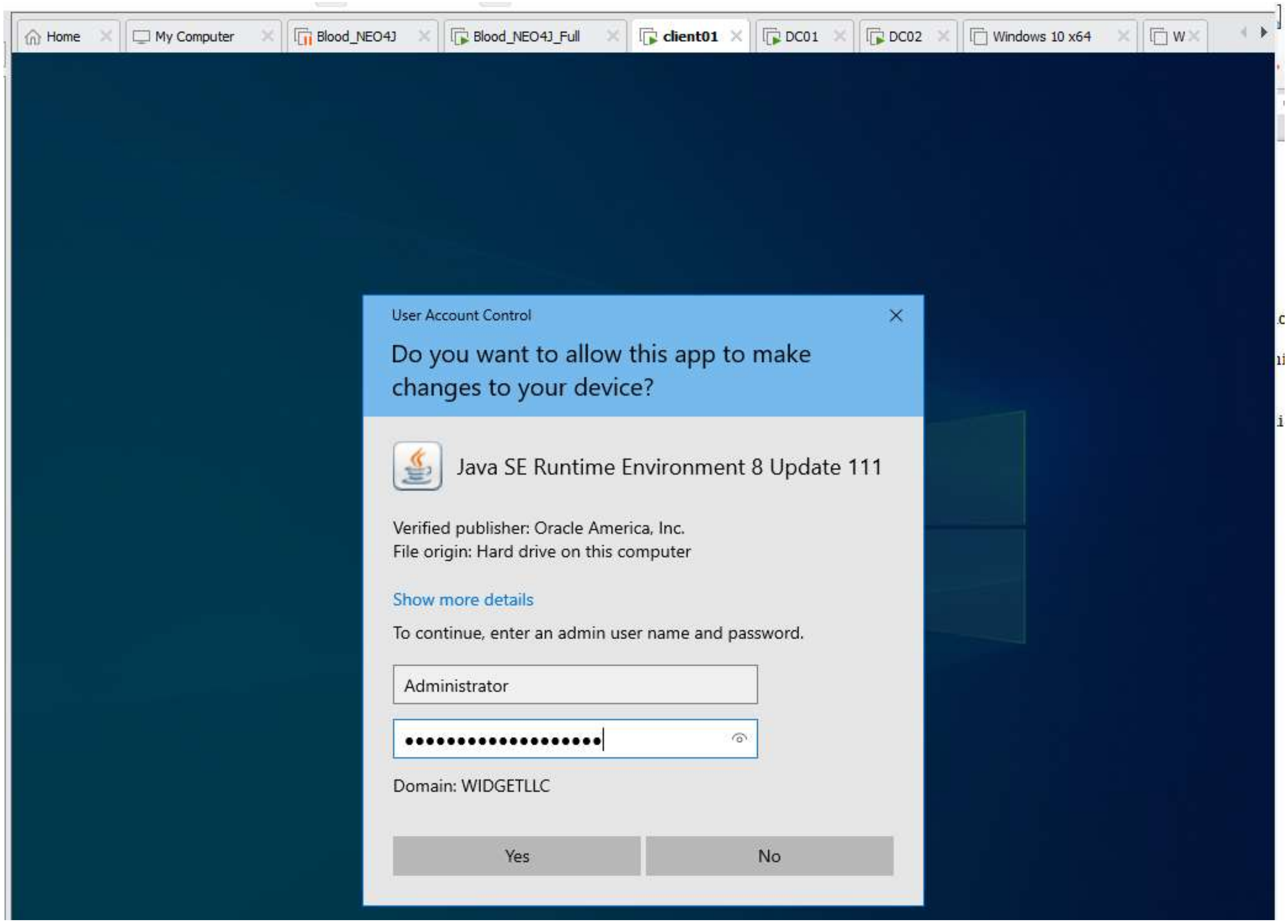
We are following along with the instructions on: NCT Bloodhound Neo4j Instructions v3

But we are installing this all on the VM "client01" which is a Windows 10 machine that is connected to the Domain/AD VM set.

We are following those prior working instructions, this document is just to note any differences that we may see on this Domain-connected machine.

Started with the Java installation.
Installations requires Admin password. On client01, in the WIDGETLLC domain:

Administrator
@5L 22 N



User Account Control

Do you want to allow this app to make changes to your device?

Java SE Runtime Environment 8 Update 111

Verified publisher: Oracle America, Inc.
File origin: Hard drive on this computer

Show more details

To continue, enter an admin user name and password.

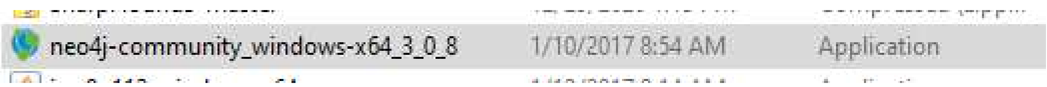
Administrator

••••••••••••••••••••

Domain: WIDGETLLC

Successfully installed, and did the 2 updates for Java.

Next, I tried to install Neo4j from the \Desktop\BloodHound folder.



neo4j-community_windows-x64_3_0_8 1/10/2017 8:54 AM Application

This worked fine when I did it in the base Windows 10 machine, but since we are connected to a domain, it tells me that I don't have permissions for the "\Program Files" directory where neo4j is trying to install itself.

We do a workaround by running PowerShell as an administrator.
Since we had logged into this VM through the domain that we had created we then moved PowerShell into the directory:

```
cd C:\Users\ncterry.WIDGETLLC\Desktop\Bloodhound
```

The we executed the neo file.

```
.\neo4j-community_windows-x64_3_0_8.exe
```

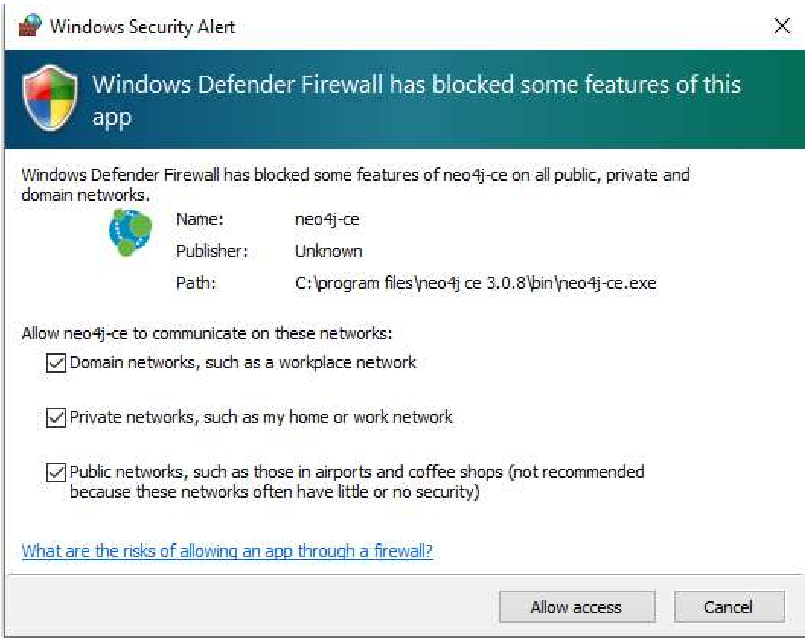
This installed the same as the default Windows 10 machine.
In the default Windows 10 machine, this placed the default directory for the Neo4j in

```
\Users\ncterry\Documents\Neo4j\default.graphdb
```

Since we are in the domain, it defaulted to:

```
\Users\Administrator\Documents\Neo4j\default.graphdb
```

When I tried to start the Neo4j application we got a Windows Defender Notification.
We checked all of the boxes (not sure if we should or not) and clicked "Allow Access"



Windows Security Alert

Windows Defender Firewall has blocked some features of this app

Windows Defender Firewall has blocked some features of neo4j-ce on all public, private and domain networks.

Name: neo4j-ce
Publisher: Unknown
Path: C:\program files\neo4j ce 3.0.8\bin\neo4j-ce.exe

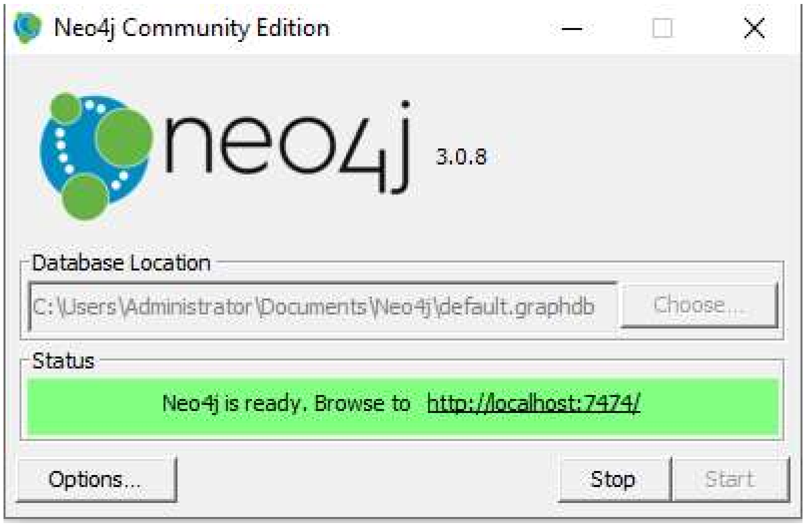
Allow neo4j-ce to communicate on these networks:

☑ Domain networks, such as a workplace network

☑ Private networks, such as my home or work network

☑ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

That gave us:



Database Location: C:\Users\Administrator\Documents\Neo4j\default.graphdb

Status: Neo4j is ready. Browse to http://localhost:7474/

Click the link.
The let us enter the default username and password:

neo4j
neo4j

We kept the username as neo4j
We changed the password to: “BloodHound”

We then opened the BloodHound app as instructed with this new password and it opened fine.
No data yet.

Since we are going for the actual SharpHound analysis, I am not going to import any example data sets.

Now we will try and get the RSAT and stuff setup on this Domain connected machine.

1. We need to have the Remote Server Administration Tool package installed. Which is not currently in Windows10 1919 iso.

2. The RSAT is in the Shared system on Viper:
    1. \\fs.code.net\Public\Software\Microsoft\Remote Server Administration Tools\Remote Server Administration Tools for Windows 10

3. We copied and dragged into the VM from the shared folder:
    1. WindowsTH-RSAT_WS_1709-x64

4. We dragged this onto the VM Desktop. If you open PowerShell and just execute them, it will install. With a few default settings. We installed x64:
    1. .\ WindowsTH-RSAT_WS_1709-x64

5. I kept everything default, clicked yes, and I accept a few times and it was in.
6. We had to restart the VM
7. Logged back in:
    1. \WIDGETLLC\ncterry
    2. @5L 22 Natio

Below in RED – not sure if anything needs to be done.
We are on a machine, in the Domain, with Active directory ……
TBD….moving onto try SharpHound

8. *Now under the windows search:*
    1. *Windows Administrative Tools*
        1. *Active Directory* → There are several options.*

    2. *But we are not connected to a domain with this single VMware Windows 10 1909 machine, so we have to get that set up if we want to add groups and users in AD.*

9. *Note there are things that we can turn on/off such as:*
    1. *Active Directory Lightweight Directory Services*
    2. *I don't know if we need this for this project, but it is good to know where it is:*
    3. *Search:*
        1. *"Turn Windows Features on or off"*
    4. *This brings up a checkbox list of potentials that we may need in the future*

NOW WE ARE RUNNING SHARPHOUND (trying to)

1. \Desktop\BloodHound\BloodHound-master\Collectors
2. PowerShell (Administrator) Run:
    1. .\SharpHound.ps1

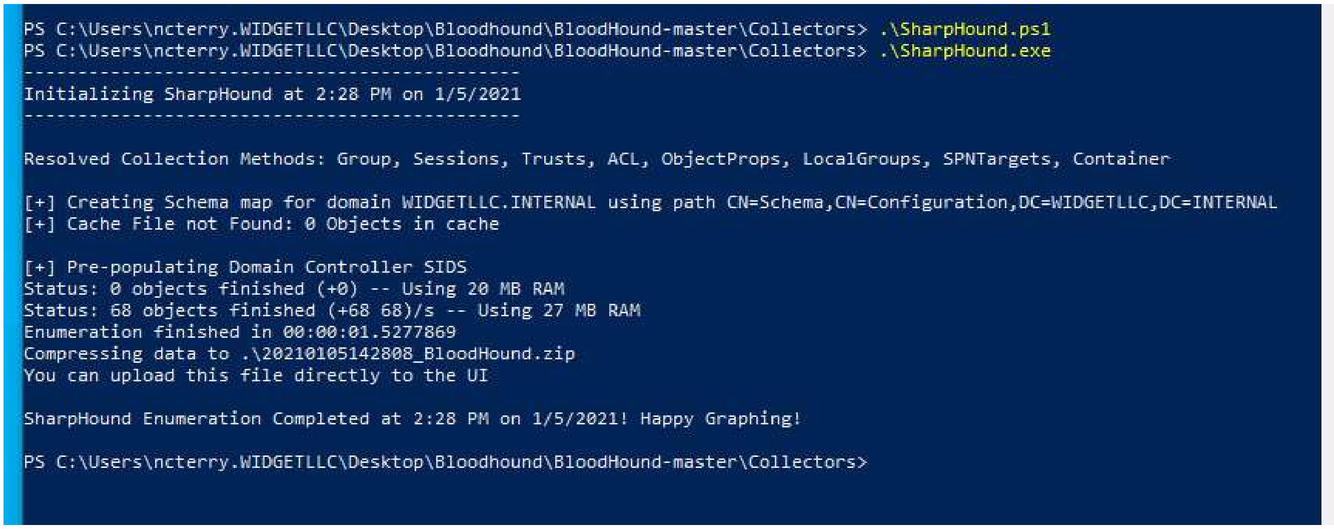
3. Note that since we are on a new install of our VM, we were not initially allowed to run scripts. We will get an error. To bypass this…..

4. In PowerShell, as an Administrator, Run:
    1. > Set-ExecutionPolicy RemoteSigned

5. Now Run:
    1. .\SharpHound.ps1

6. The first run seemed to execute just fine, but nothing happened that was displayed at all.
7. No changes were made to a data set either.
8. I then tried to run:
    1. .\SharpHound.exe

In the original machine Windows 10 not connected to a Domain, that worked, but could not do anything since it was not connected to a Domain or Forest. On this machine “client01” IT WORKED!



```
PS C:\Users\ncterry.WIDGETLLC\Desktop\Bloodhound\BloodHound-master\Collectors> .\SharpHound.ps1
PS C:\Users\ncterry.WIDGETLLC\Desktop\Bloodhound\BloodHound-master\Collectors> .\SharpHound.exe
-----------------------------------------------
Initializing SharpHound at 2:28 PM on 1/5/2021
-----------------------------------------------

Resolved Collection Methods: Group, Sessions, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container

[+] Creating Schema map for domain WIDGETLLC.INTERNAL using path CN=Schema,CN=Configuration,DC=WIDGETLLC,DC=INTERNAL
[+] Cache File not Found: 0 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 20 MB RAM
Status: 68 objects finished (+68 68)/s -- Using 27 MB RAM
Enumeration finished in 00:00:01.5277869
Compressing data to .\20210105142808_BloodHound.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 2:28 PM on 1/5/2021! Happy Graphing!

PS C:\Users\ncterry.WIDGETLLC\Desktop\Bloodhound\BloodHound-master\Collectors>
```

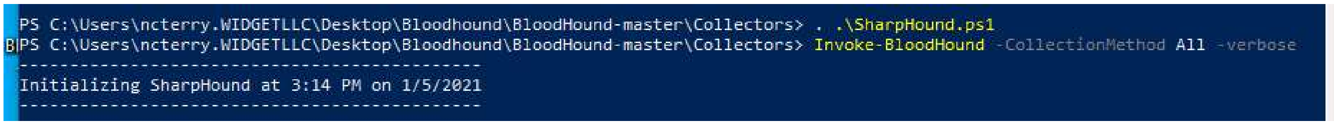
This completed and saved the file to:

\ncterry.WIDGETLLC\Desktop\Bloodhound\BloodHound-master\Collectors

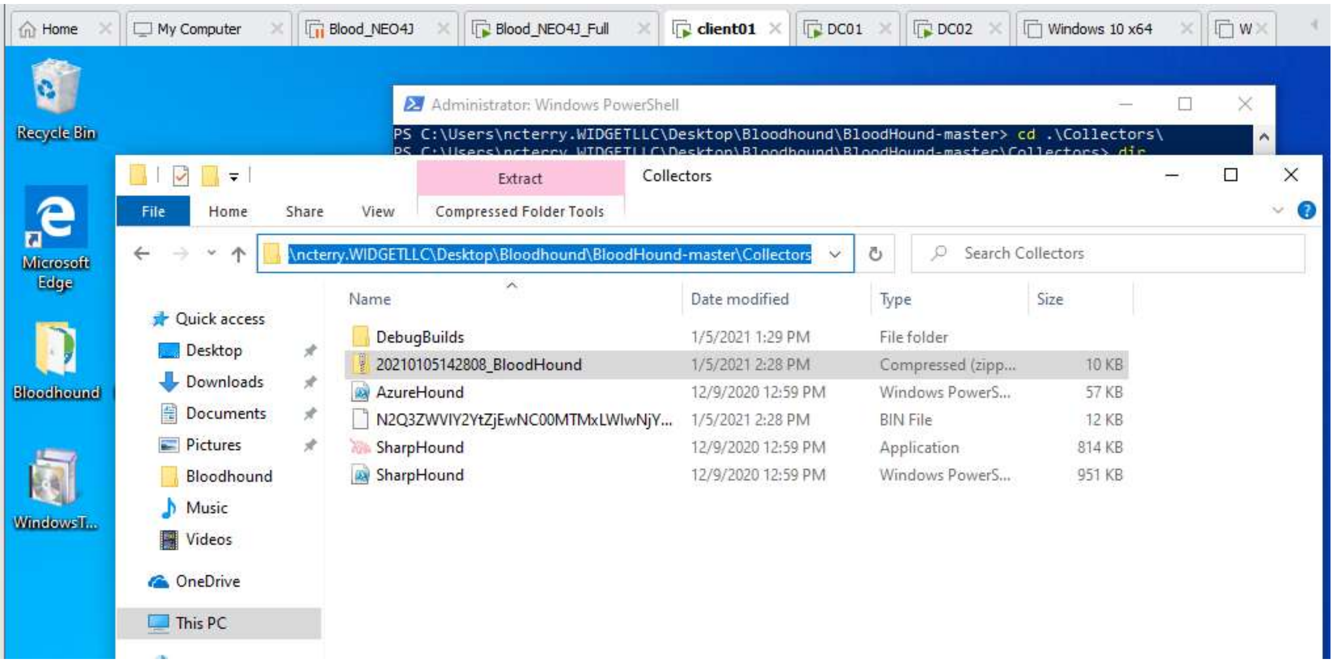
So it saved it right where we executed SharpHound from.

I was also able to run it with this method. Not sure if either are different in results

> . .\SharpHound.ps1
> Invoke-BloodHound -CollectionMethod All -verbose



```
PS C:\Users\ncterry.WIDGETLLC\Desktop\Bloodhound\BloodHound-master\Collectors> . .\SharpHound.ps1
PS C:\Users\ncterry.WIDGETLLC\Desktop\Bloodhound\BloodHound-master\Collectors> Invoke-BloodHound -CollectionMethod All -verbose
-----------------------------------------------
Initializing SharpHound at 3:14 PM on 1/5/2021
-----------------------------------------------
```



```
PS C:\Users\ncterry.WIDGETLLC\Desktop\Bloodhound\BloodHound-master> cd .\Collectors\
PS C:\Users\ncterry.WIDGETLLC\Desktop\Bloodhound\BloodHound-master\Collectors> dir
```

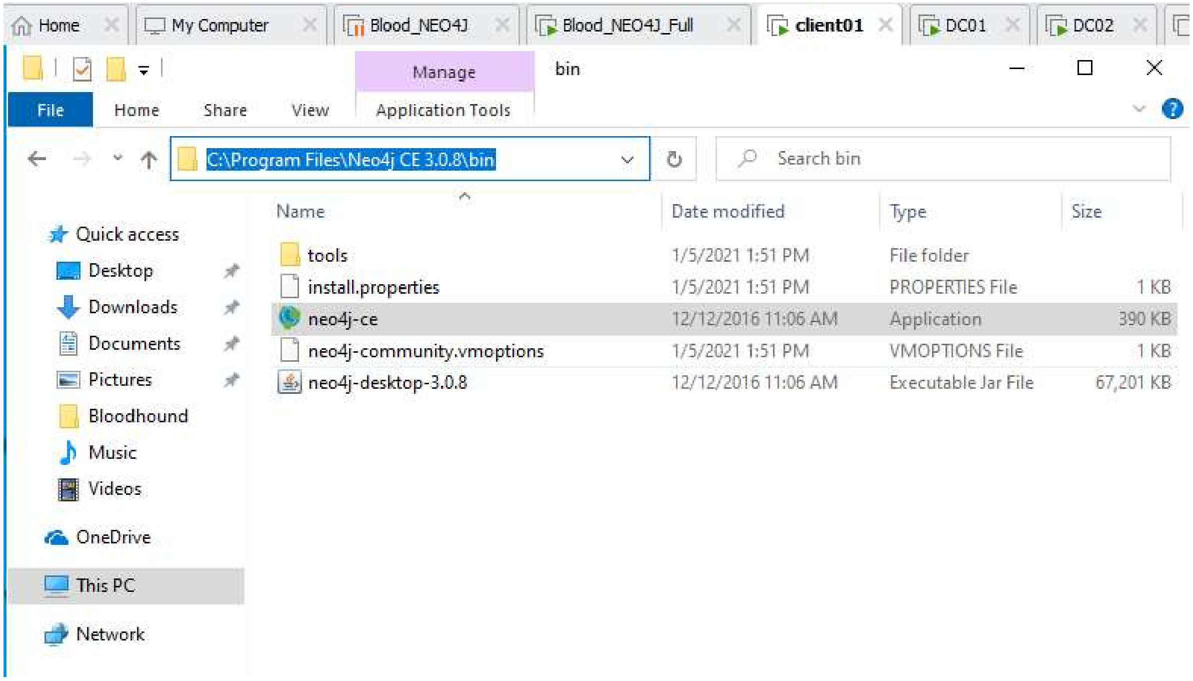
\ncterry.WIDGETLLC\Desktop\Bloodhound\BloodHound-master\Collectors

Name	Date modified	Type	Size
DebugBuilds	1/5/2021 1:29 PM	File folder	
20210105142808_BloodHound	1/5/2021 2:28 PM	Compressed (zipp...	10 KB
AzureHound	12/9/2020 12:59 PM	Windows PowerS...	57 KB
N2Q3ZWVlY2YtZjEwNC00MTMxLWIwNjY...	1/5/2021 2:28 PM	BIN File	12 KB
SharpHound	12/9/2020 12:59 PM	Application	814 KB
SharpHound	12/9/2020 12:59 PM	Windows PowerS...	951 KB

Now that we have the analysis we need to open up Neo4j and BloodHound and import this data. Remember this was installed deep in the Domain, so the Neo4j Application itself is currently in:

C:\Program Files\Neo4jCE 3.0.8\bin.

I double clicked on this app seen below, and it opened up Neo4j as expected.



C:\Program Files\Neo4j CE 3.0.8\bin

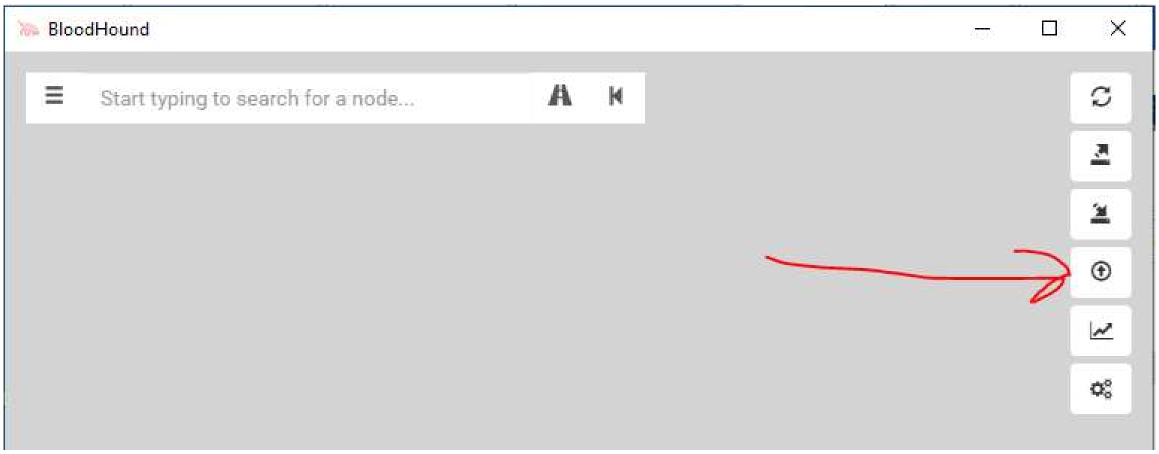
Name	Date modified	Type	Size
tools	1/5/2021 1:51 PM	File folder	
install.properties	1/5/2021 1:51 PM	PROPERTIES File	1 KB
neo4j-ce	12/12/2016 11:06 AM	Application	390 KB
neo4j-community.vmoptions	1/5/2021 1:51 PM	VMOPTIONS File	1 KB
neo4j-desktop-3.0.8	12/12/2016 11:06 AM	Executable Jar File	67,201 KB

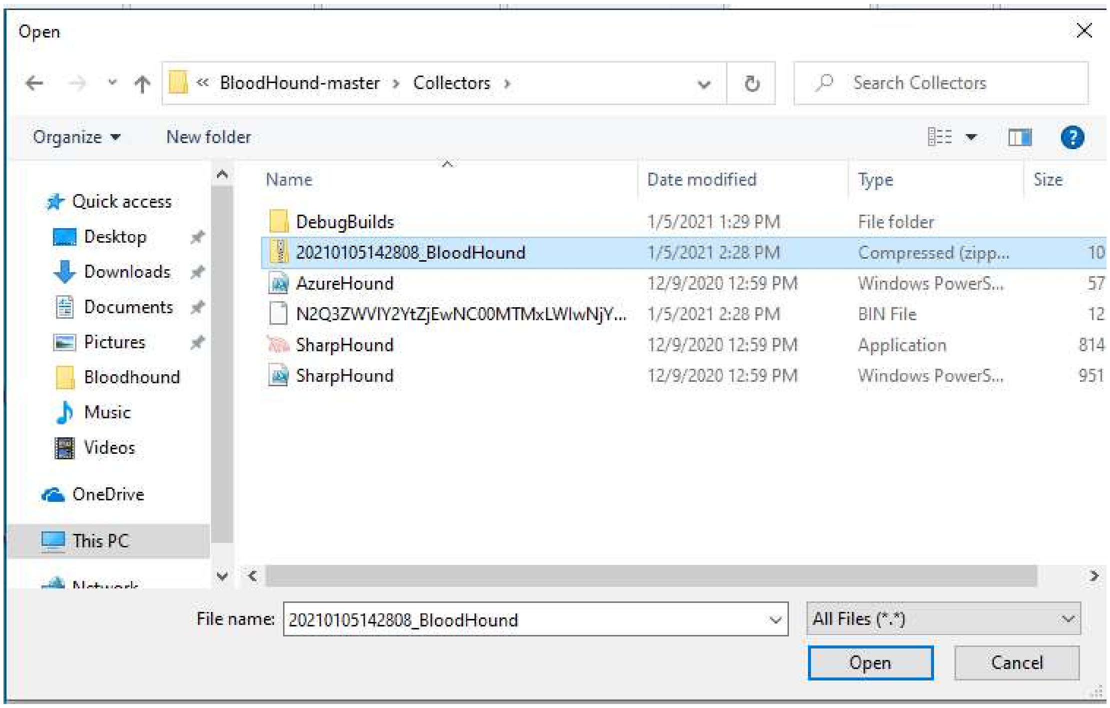
I kept Neo4j on it’s default database location:

C:\Users\Administrator\Documents\Neo4j\default.graphdb

Click start.
It gave me a link but I did not click it. Keep this popup open, and now we need to open BloodHound and import that SharpHound zip data file that we just collected.

Double click on the BloodHound App
It still opens a blank, grey, BloodHound since at the moment we have not imported any data.
Click on the upload data icon shown below.





Name	Date modified	Type	Size
DebugBuilds	1/5/2021 1:29 PM	File folder	
20210105142808_BloodHound	1/5/2021 2:28 PM	Compressed (zipp...	10
AzureHound	12/9/2020 12:59 PM	Windows PowerS...	57
N2Q3ZWVlY2YtZjEwNC00MTMxLWIwNjY...	1/5/2021 2:28 PM	BIN File	12
SharpHound	12/9/2020 12:59 PM	Application	814
SharpHound	12/9/2020 12:59 PM	Windows PowerS...	951

File name: 20210105142808_BloodHound
All Files (*.*)

Import that zipped file that SharpHound just collected and saved.

BUT 1/5/21 on my first try, when I try to import, BloodHound tells me “Unrecognized CSV file”
All of the files in the zipped folder are JSON files. Not sure what is going on……

I watched videos and their actions are the same, and their files inside their zipped collection are all JSON as well. But on their, BloodHound says that is is ‘Processing……’ where mine says Unrecognized.

Remember that with the agency files, we brought in the BloodHound-win32-x64 from the Agency shared folder, ‘BloodHound’. But this primary executate for Bloodhound, while it is was able to install and work on our VM, it is 4 years old. I was not able to download the new GitHub version and bring it into our VM. Mitchel Rukat was able to bring in the recent SharpHound, and it looks like that SharpHound is saving the collected results in a JSON format that is unreadable by the old Bloodhound.

So everything works, but the old Bloodhound, cant process results from a new SharpHound