**Invisible Wireshark Install Directions & File Recovery – MUST BE ADMIN!**  
Install Wireshark 64 bit from the internet: <https://2.na.dl.wireshark.org/win64/Wireshark-win64-3.2.3.exe> Save to Downloads and install as Administrator from there. (Remember to delete the file after you complete all the following steps!)

Copy this wireshark.bat below to the *C:\Program Files\Wireshark* directory

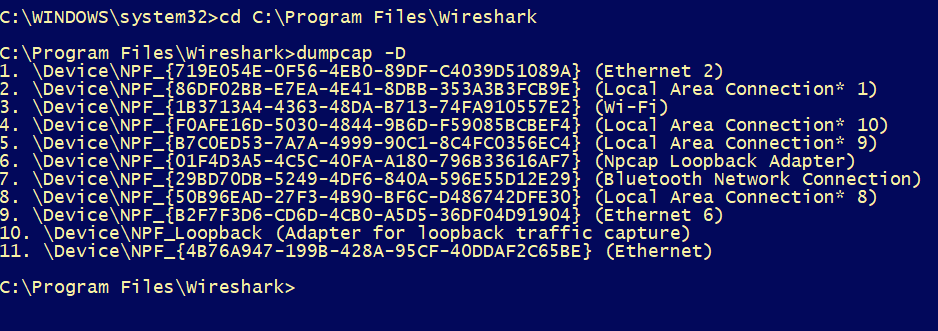


Go to the remote PC’s CMD and run as Administrator.

Then type: cd *c:\Program Files\Wireshark*

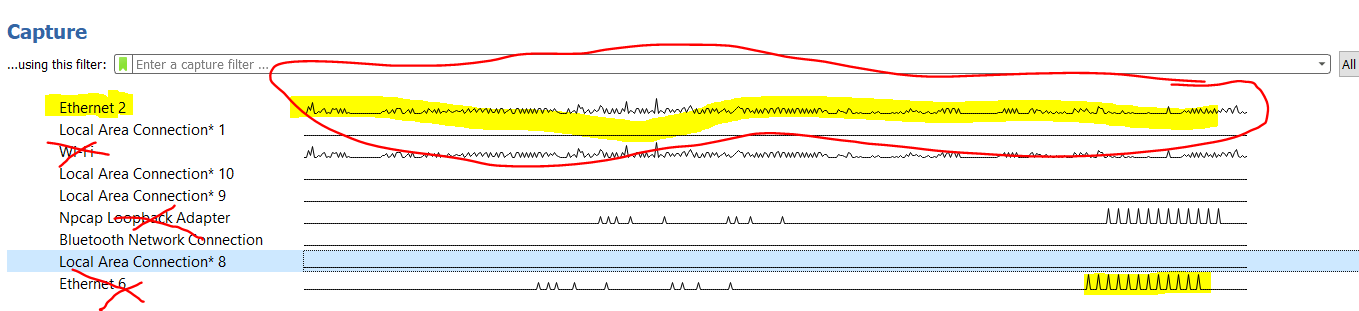
When in the directory, Type: *dumpcap -D*

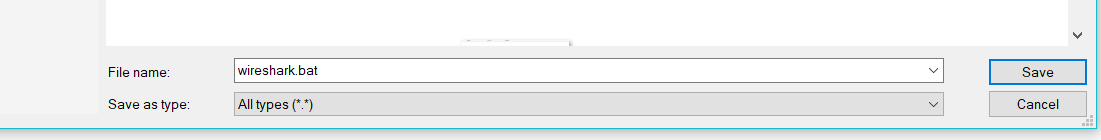
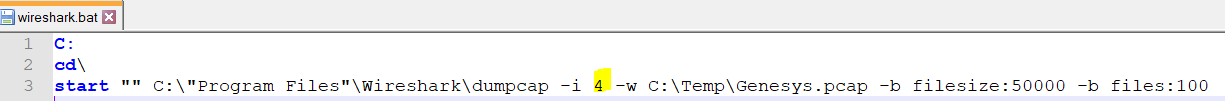
The output will look like this:



Look for the Ethernet interface. In this case it is 11

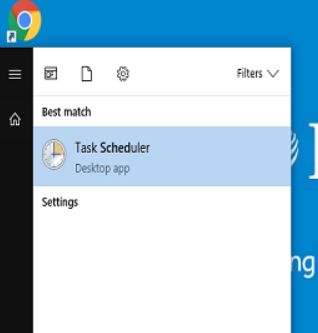
**STOP!** If the PC is not in an office, and is using VPN, the interface may not be Ethernet. These Work From Home (WFH) set ups can fool you into capturing the wrong interface.

If not sure, start the Wireshark GUI program and look for activity. I am disconnected from an Ethernet cable and using WiFi (I am breaking all Genesys rules tonight..) so here is my output:  
  
In my case, we want to track Ethernet 2 which shows Banner traffic that we want to see. WiFi is not interesting. Ignore all Loopback interfaces and ignore all additional Ethernet interfaces that have minimal traffic. And in this case, Ethernet 2 is Interface 1 if you look in the CMD window up above.

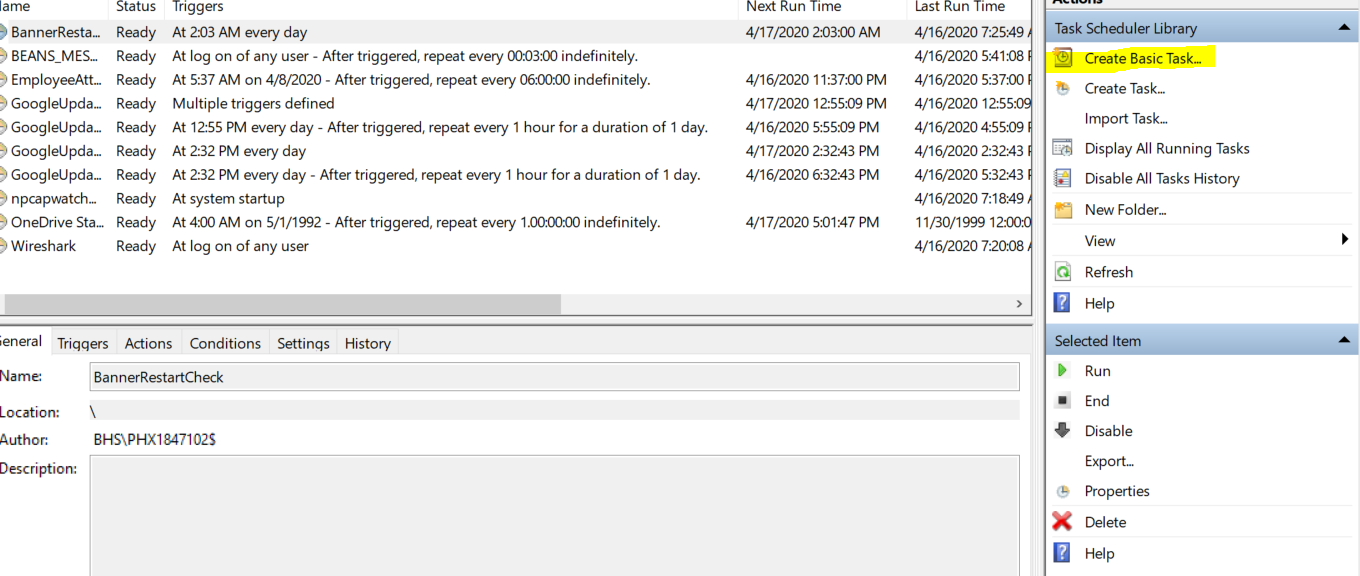
Open the wireshark.bat in Notepad and change the interface number. 4 is the default. In this case, I would change it to 1, then save the file as wireshark.bat (make sure you don’t let notepad save it as a .txt file by changing it to All Types: 

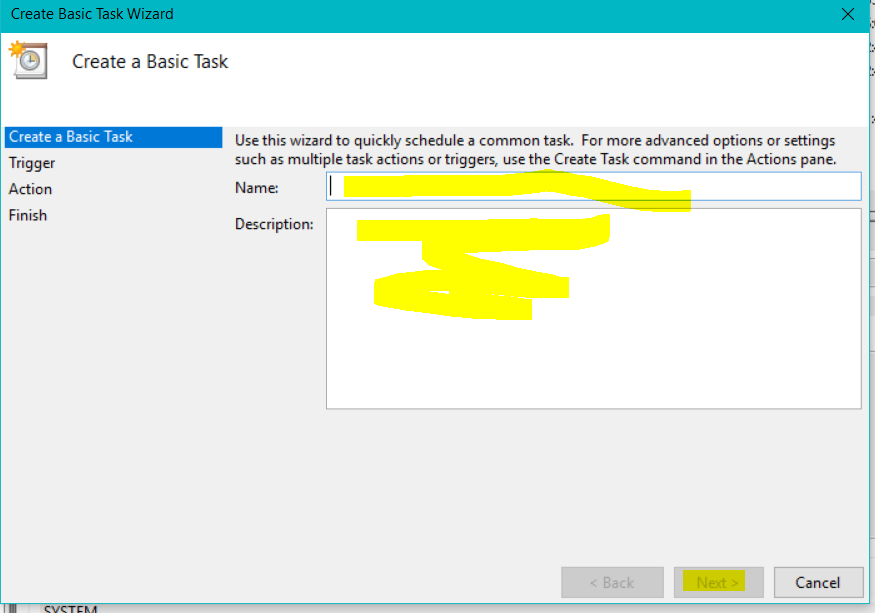
Now that the .bat file is configured for the PC, we need to make sure it starts every time someone logs into the PC.

Go to Task Scheduler from Start menu



Click Create Basic Task (at the right)

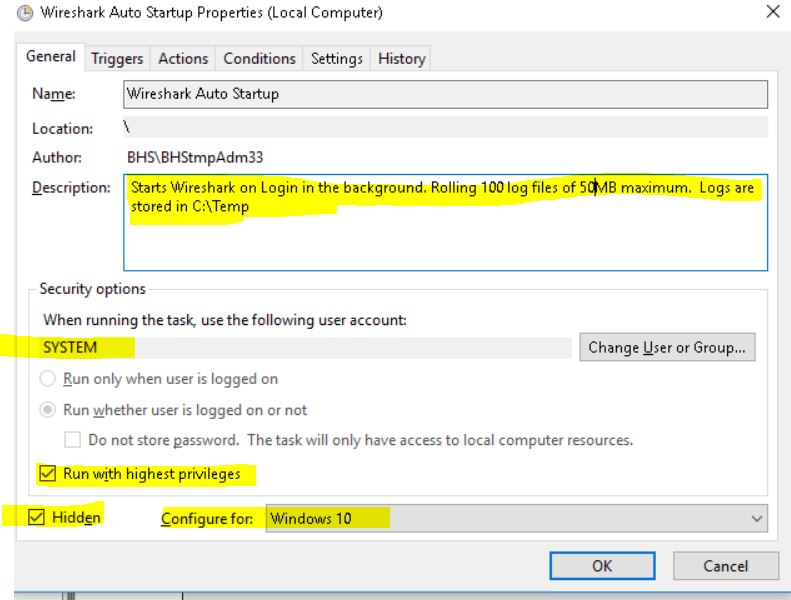


Fill in the Name and Description with the following:  


*Wireshark Auto Start Up*

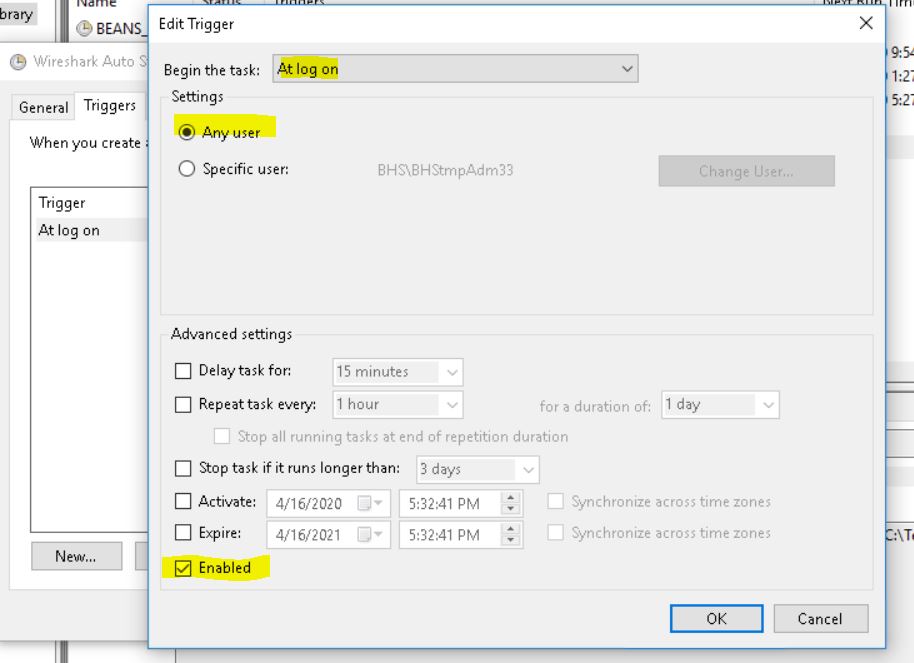
*Starts Wireshark on Login in the background. Rolling 100 log files of 50MB maximum. Logs are stored in C:\Temp*

Click on User or Group, type in SYSTEM and then Check Name, then OK  
Check Run with Highest Privileges  
Check Hidden and change Configure for: to Windows 10



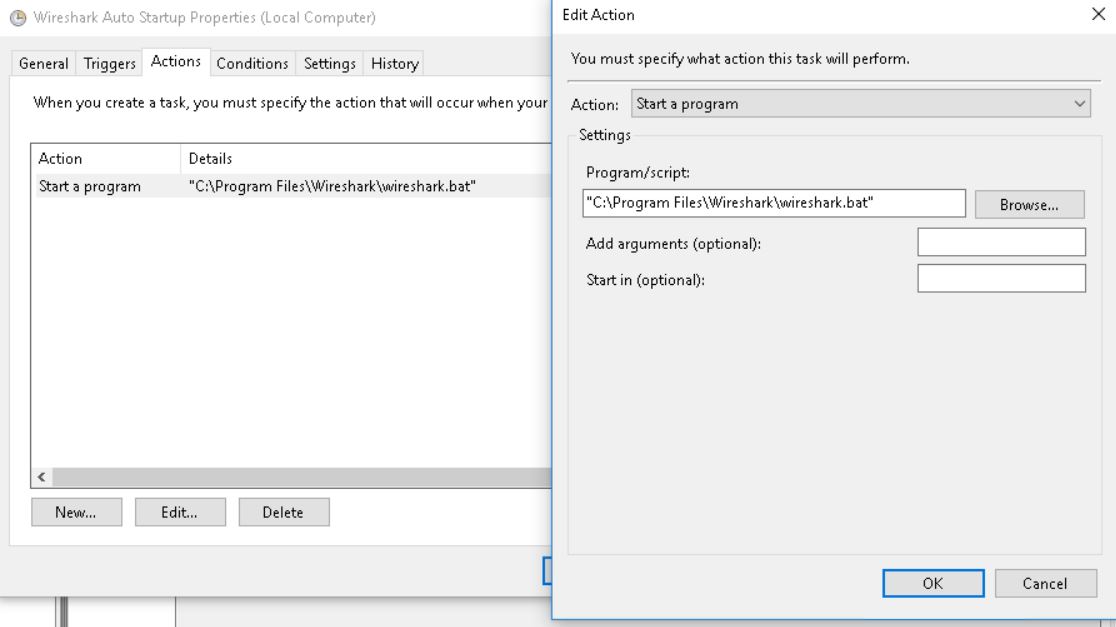
When you click Next at the bottom, you will go to Triggers  
At log on

Any User  
Check Enabled at the bottom

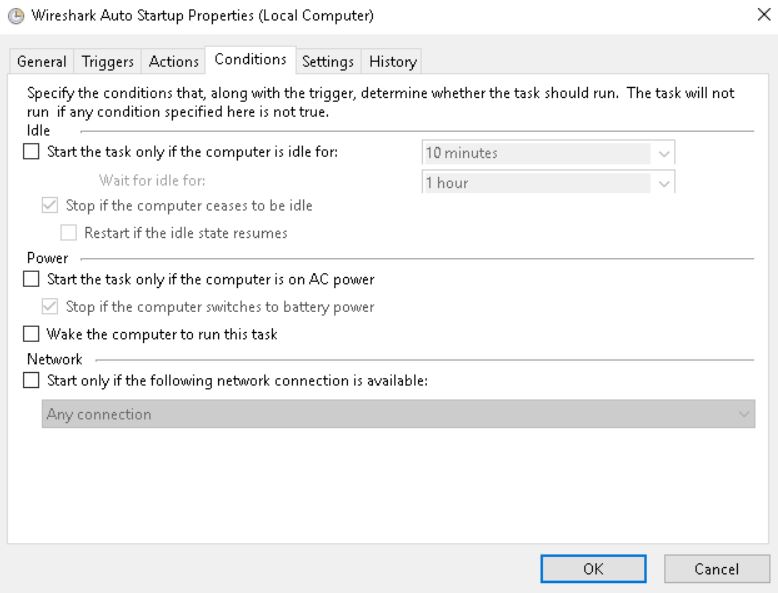


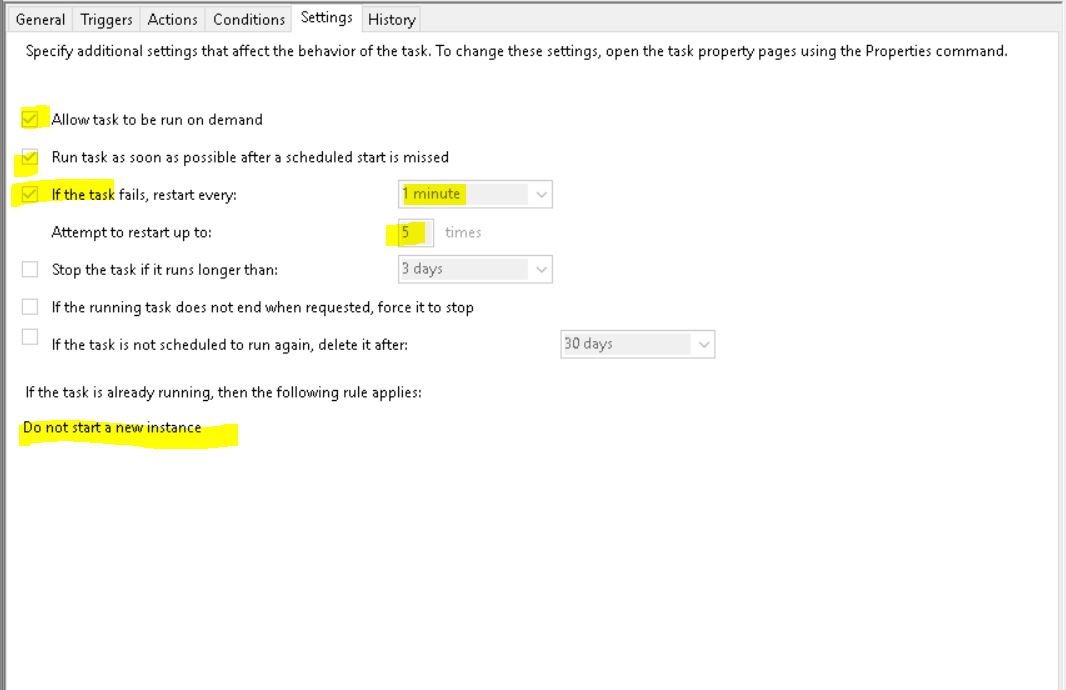
At Actions, New.  
Then Start a Program

Browse to the C:\Program Files\Wireshark directory and select wireshark.bat



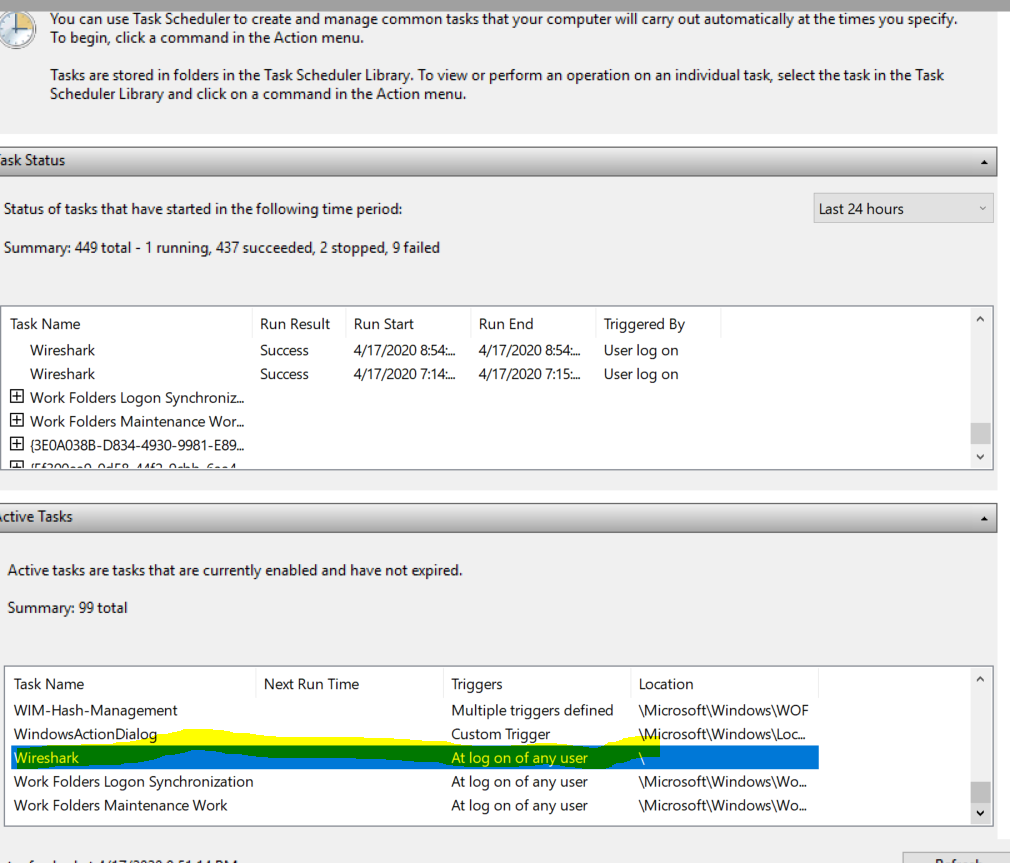
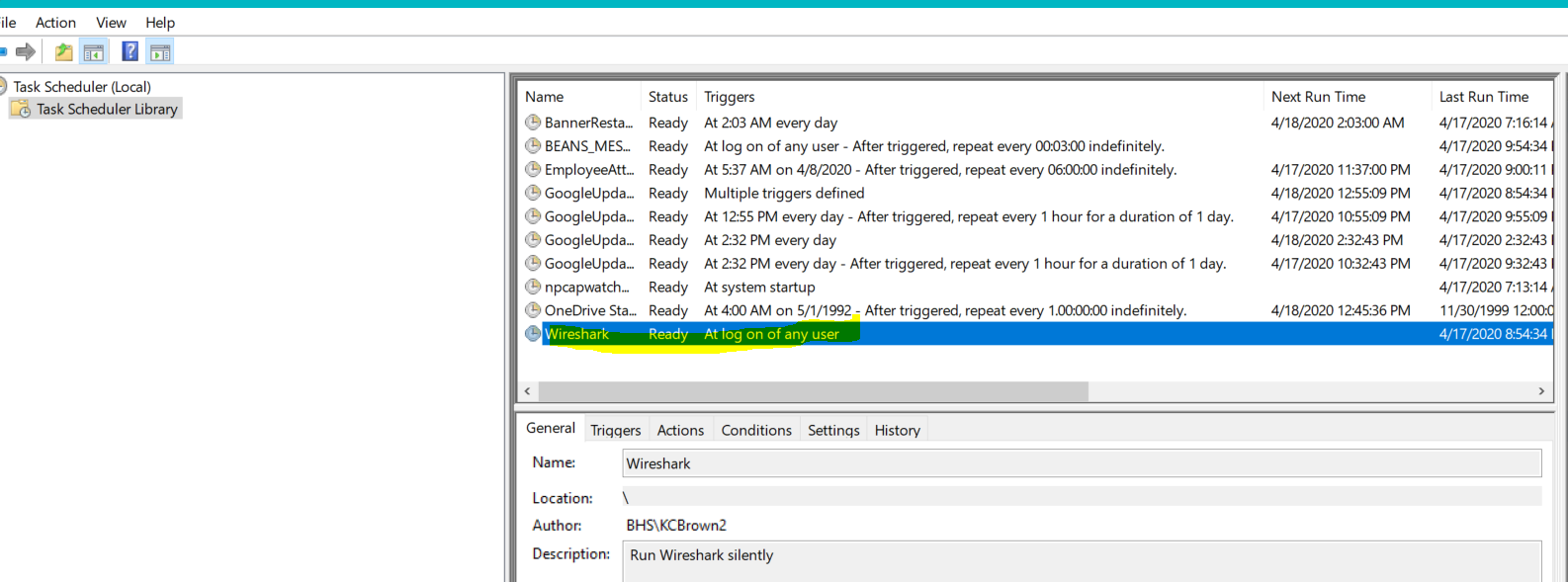
For conditions, keep all clear as below

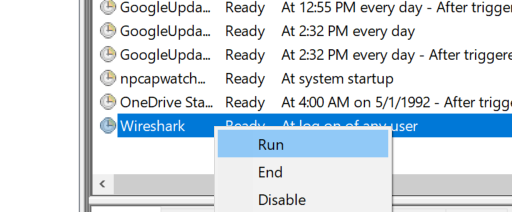


Settings, fill as below:  


Then Finish.

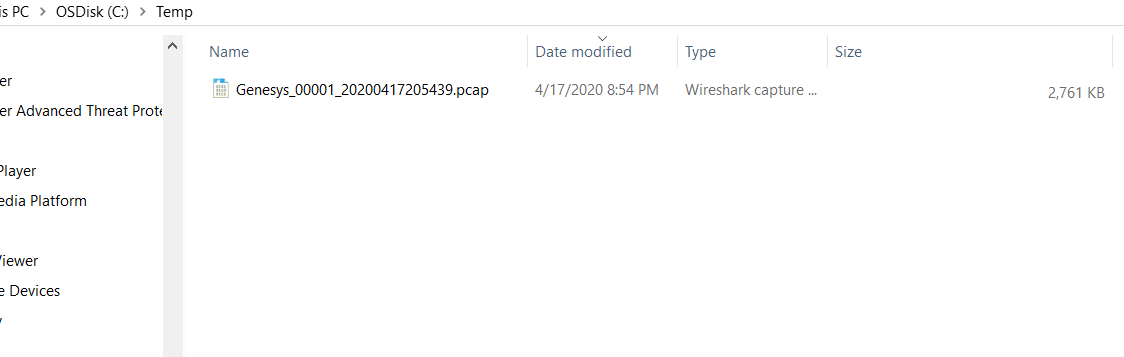
To check it is working properly, go back to Task Scheduler and double click on Wireshark:

Then right click on Wireshark, and then click on Run  


Wait two minutes and then check C:\Temp for content

You should see something above 200Kb

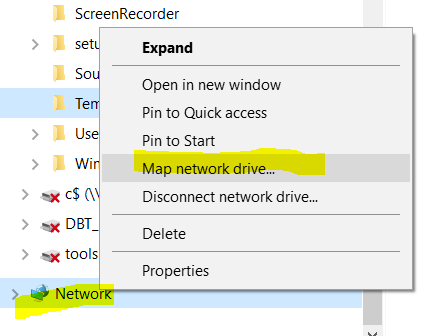


You are finished with install. If you are not getting a log file of any size, return back to checking the interfaces and the corresponding interface number in the wireshark.bat file

**Recovering Wireshark Log Files**

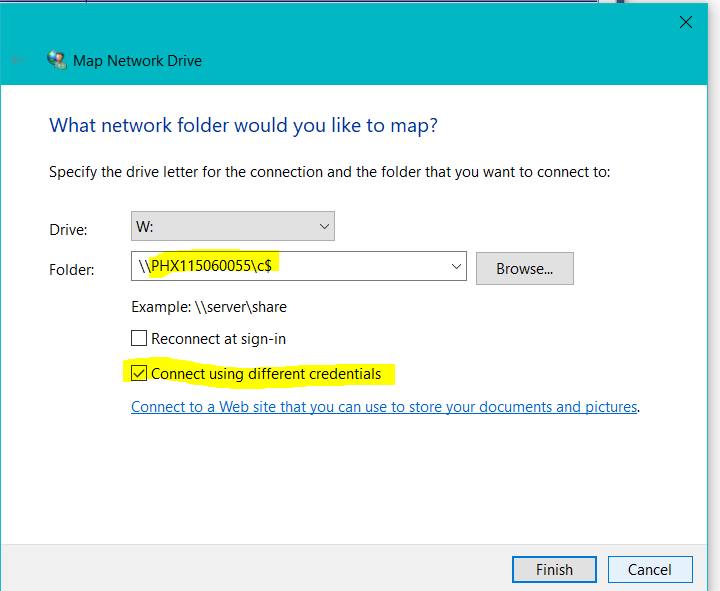
You will need Admin privileges again

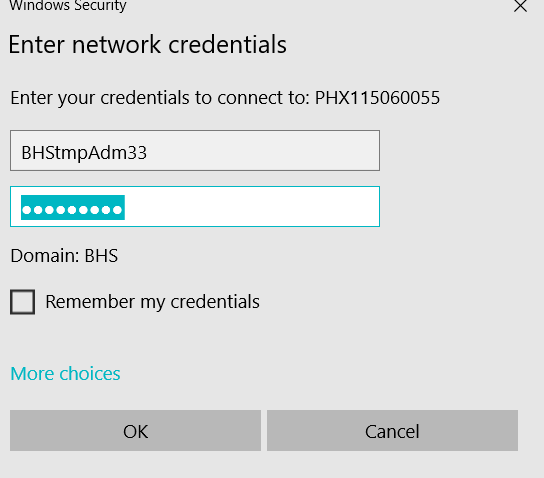
Go to File Manager, right click on Network, click on Map network drive…

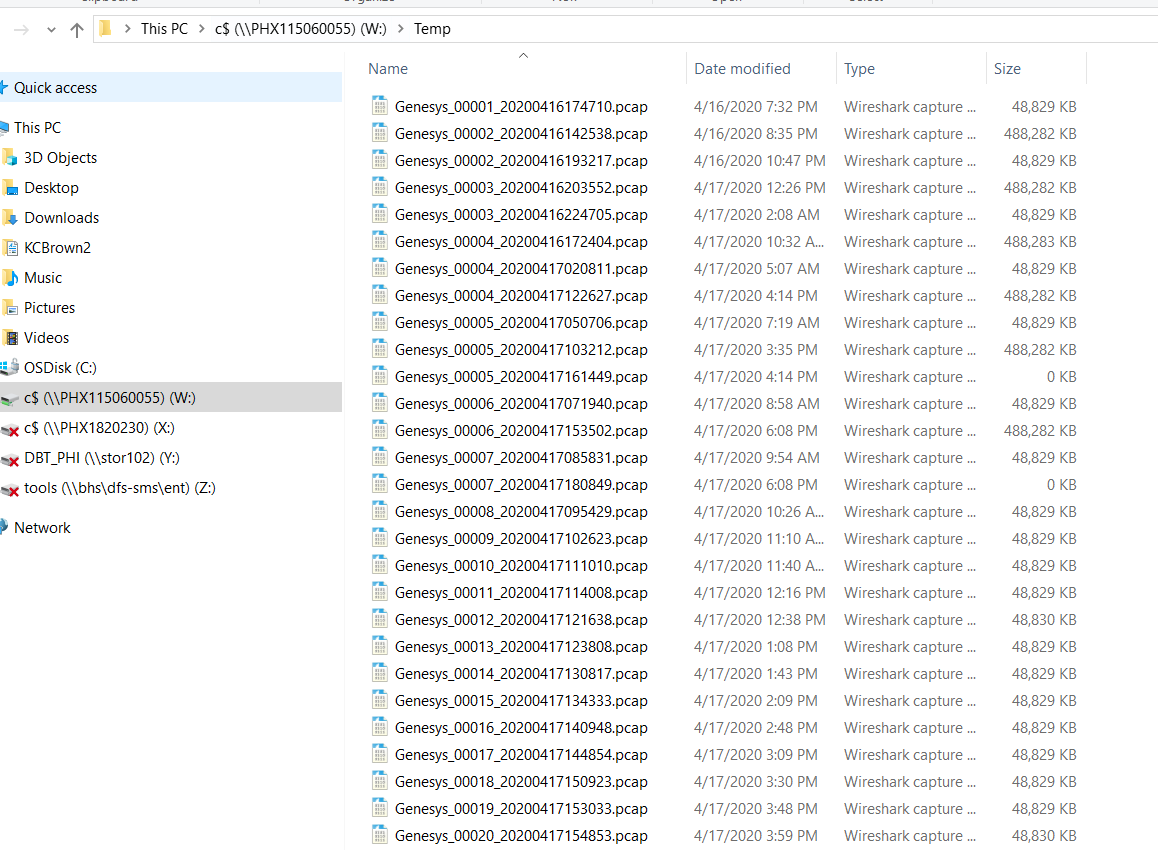


When prompted to map a drive, choose any drive letter that is open on your PC (W in my case)

Then enter [\\PCNAME\c$](file:///\\PCNAME\c$) then clear the Reconnect at login, check the Connect using different credentials tick box.



You will be presented with the login with Admin credentials  


Once you have been authorized, you will see the remote PC’s files:  


Always **copy** the log file, anything else will fail due to the Wireshark process in place managing these log files.

**HINT:** If you are looking for a specific timeframe, say 04/17/2020 3:38 when an incident has been noted in a log, copy the log before and after. In this case copy both 15:30 and 15:38 logs.