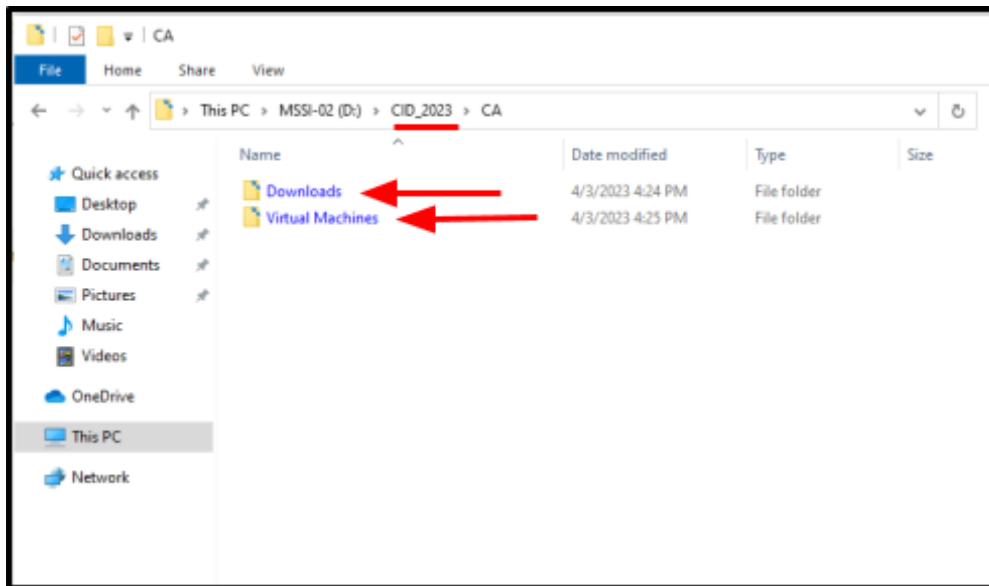


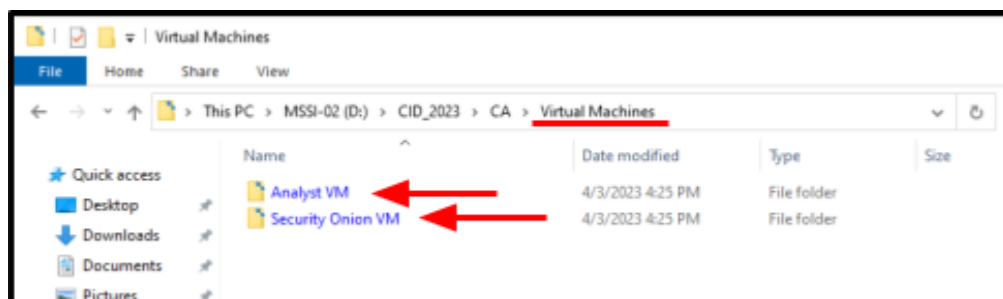
Task 1: Importing the Analyst VM

1. Create specific folders.

- 1.1. Create one folder called **[Downloads]**, and another folder called **[Virtual Machines]** in your team based shared folder inside **[D:\CID_2023\TeamX]** where X stands for your team number.



- 1.2. Open the **Virtual Machines** folder, and create one folder called **[Analyst VM]** and another folder called **[Security Onion VM]**



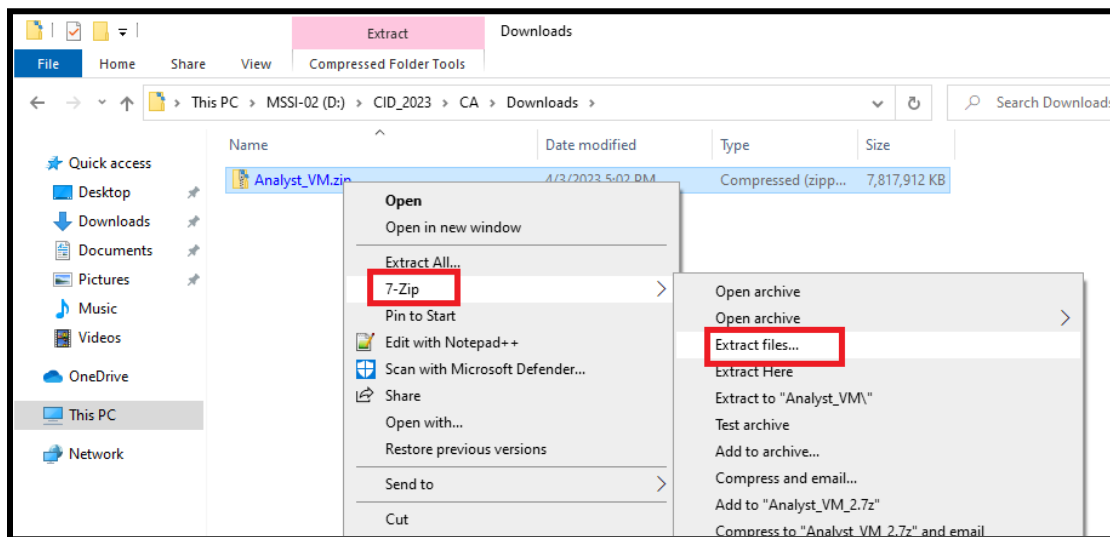
2. Download Ubuntu image file

- 2.1. Download Ubuntu 22.04 image file from: [Analyst_VM.zip](#), and save it in **D:\CID_2023\TeamX\Downloads** folder.

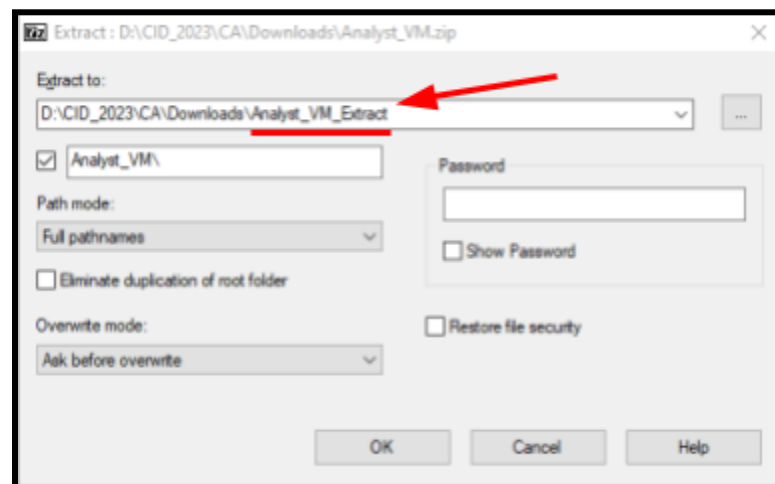
Note: Modify the setting of the downloads on your browser, before you start to download the **[Analyst_VM.zip]**. You could do that by following the next steps:

- Chrome -> Settings -> Downloads -> Enable (Ask where to save each file before downloading)

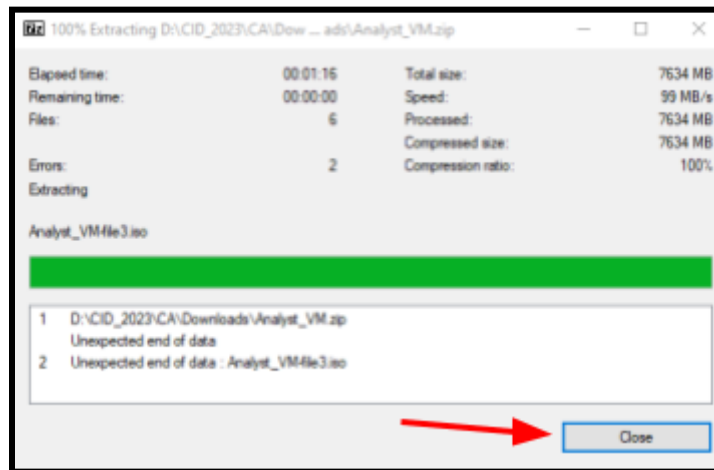
- 2.2. Extract the **[Analyst_VM.zip]** using the **[7-Zip]**:



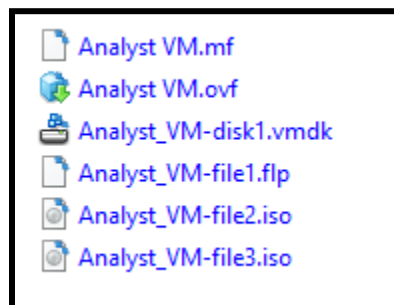
- 2.3. Extract the file in the new folder called **[Analyst_VM_Extract]** inside the **[Downloads]** folder. Then click **[OK]** to start extracting files:



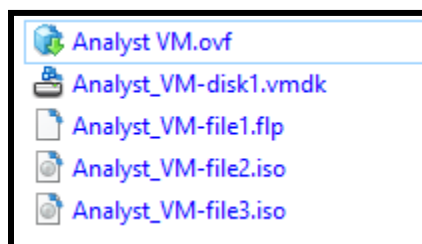
2.4. After we finish the extract of the Zip file, click **[Close]**



2.5. Then, you should be able to see those files in
D:\CID_2023\TeamX\Downloads\Analyst_VM_Extract\Analyst_VM

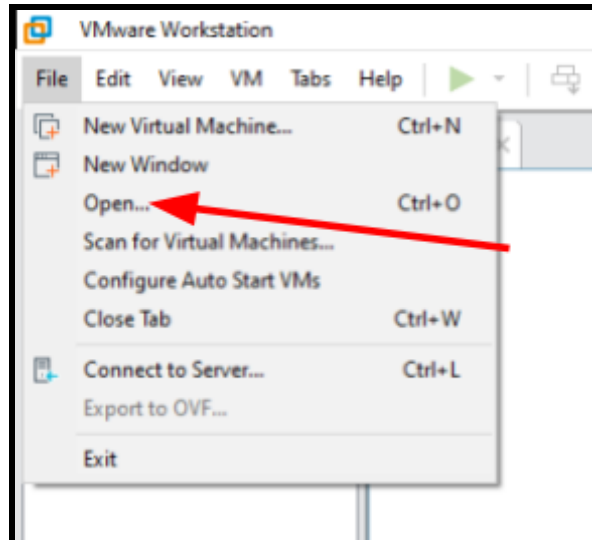


2.6. Delete the **Analyst VM.mf** file, and you should only have 5 files left in this folder.

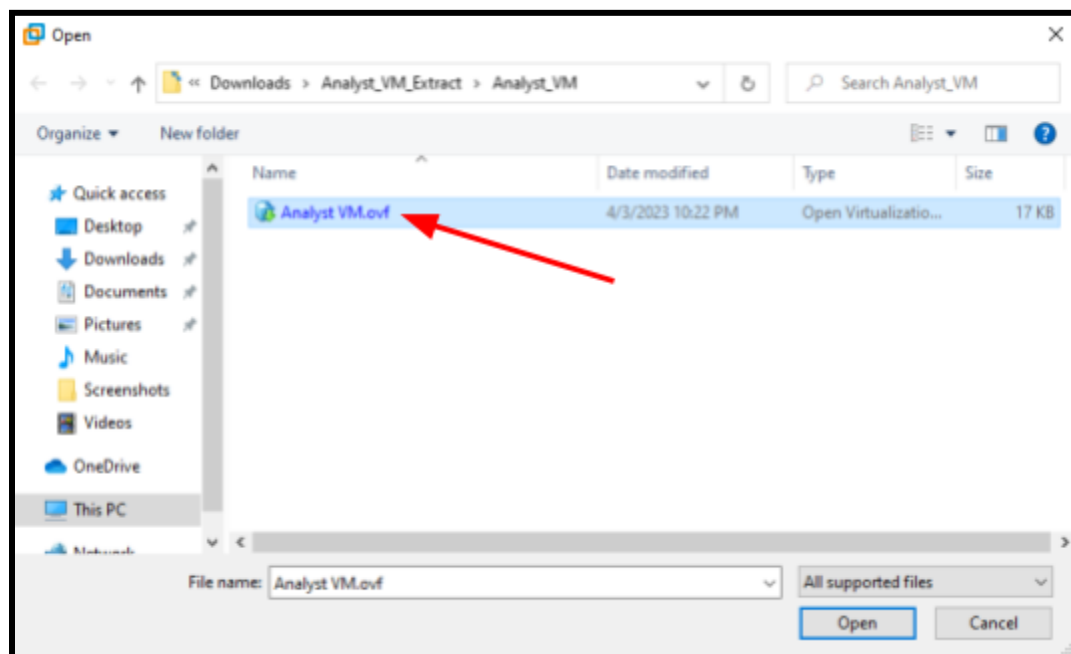


3. Import the Analyst Virtual Machine in VMware:

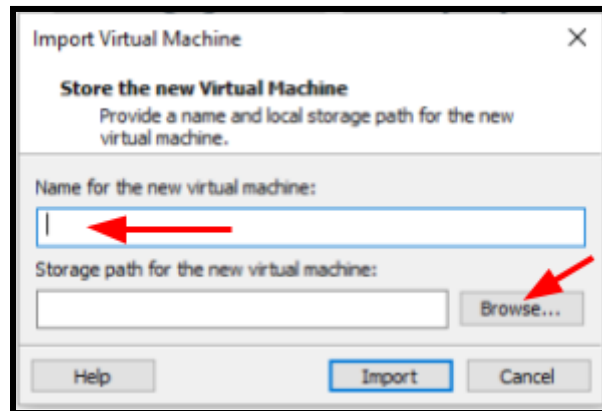
- 3.1. Open the VMware and select [File] from the menu bar, then choose [Open a Virtual Machine].



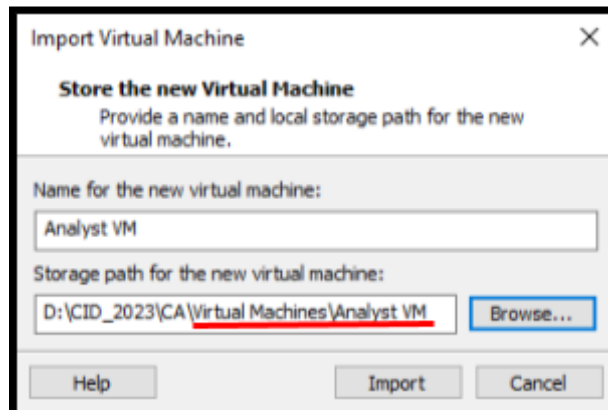
- 3.2. Navigate to the folder that you download your analyst VM in and select the [Analyst VM.ovf] file. Then click [Open]



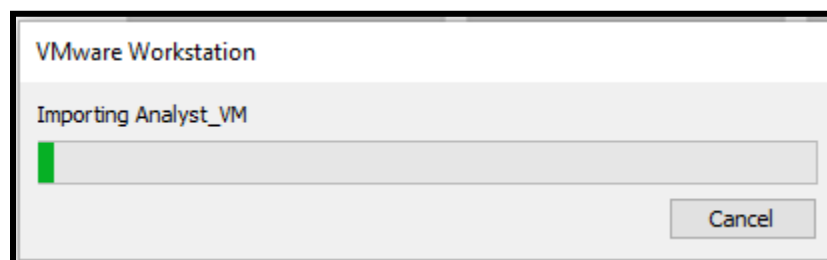
- 3.3. Type in the name for the new virtual machine [**Analyst_VM**], and Storage path for the new virtual machine in the group shared folder.



- 3.4. Make sure that your storage path for the new virtual machine is [**D:\CID_2023\TeamX\Virtual Machines\Analyst VM**] not the **Downloads** folder.



- 3.5. Click on [**Import**] to start to import the Analyst VM.

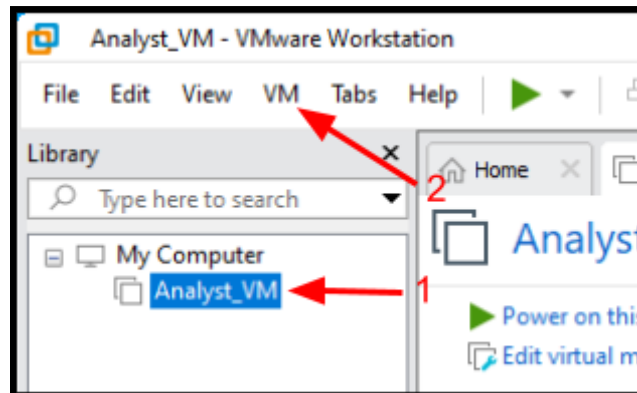


After importing the Analyst VM, you should be able to see it on the left-hand side of your VMware.

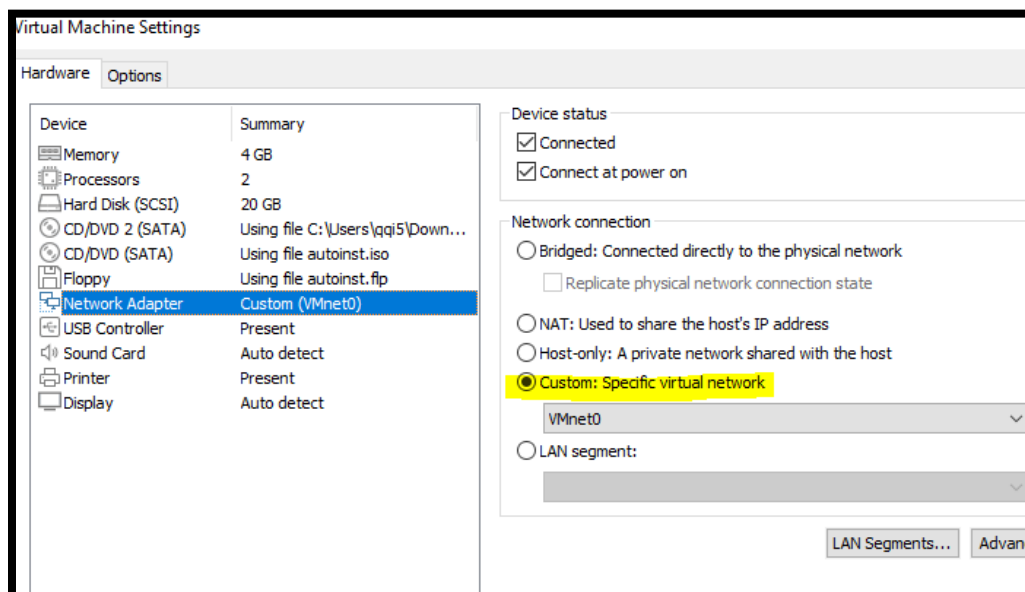
4. Configuring the Analyst VM:

Once the VM is running again we must configure this machine and connect it to the management Network [VMnet0]

- 4.1. Check the left side of VMware Workstation window, click on [Analyst VM] then click on [VM] menu and choose [Setting]



- 4.2. Click on [Network Adapter] and change the network connection to [Custom] and choose [VMnet0].



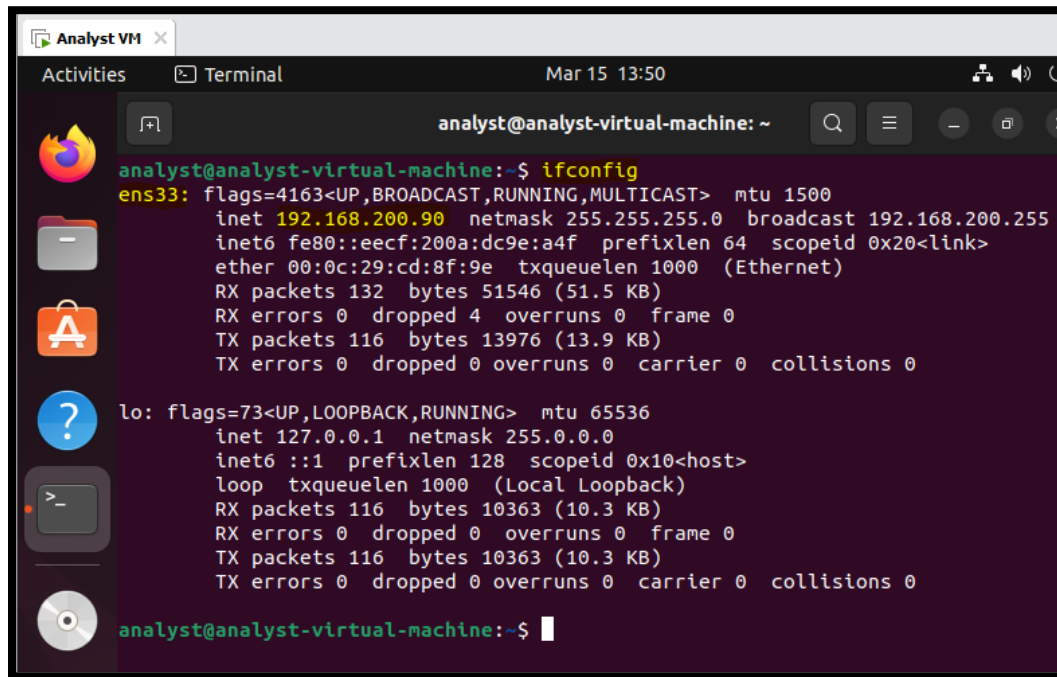
Note: VMnet0 is a bridged mode network. In this lab environment, this network will be used for management operations only. Hence only the Analyst VM will be connected to this machine along with the Security Onion VM.

- 4.3. Reboot your machine and run the command **[ifconfig]** to get the IP Address of the Analyst VM.

Note: The account information for the **[Analyst VM]** is

Username: user

Password: user



```
analyst@analyst-virtual-machine: ~  
analyst@analyst-virtual-machine:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.200.90 netmask 255.255.255.0 broadcast 192.168.200.255  
    inet6 fe80::eecf:200a:dc9e:a4f prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:cd:8f:9e txqueuelen 1000 (Ethernet)  
    RX packets 132 bytes 51546 (51.5 KB)  
    RX errors 0 dropped 4 overruns 0 frame 0  
    TX packets 116 bytes 13976 (13.9 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 116 bytes 10363 (10.3 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 116 bytes 10363 (10.3 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
analyst@analyst-virtual-machine:~$
```

Now we know that the IP Address for the Analyst machine is: **193.168.200.90**. Additionally, the interface used for the Management Network is **[ens33]**. These are important information and will be used when we configure the Security Onion VM.

Note: in your machine the interface may be different based on what you get when you **[ifconfig]** the Analyst VM.

Tasks

Task 1.1: Provide a screenshot of the analyst VM that shows the IP Address and the interface name

Task 1.2: Provide a table that summarizes all information related to both the Management Network and the Monitor Network. Make sure that you include: Network Type, Network Name, Interface Name, CIDR IP Address and any related information.