

## Lab-0000: VM startup... Time circuits on...flux capacitor, fluxing

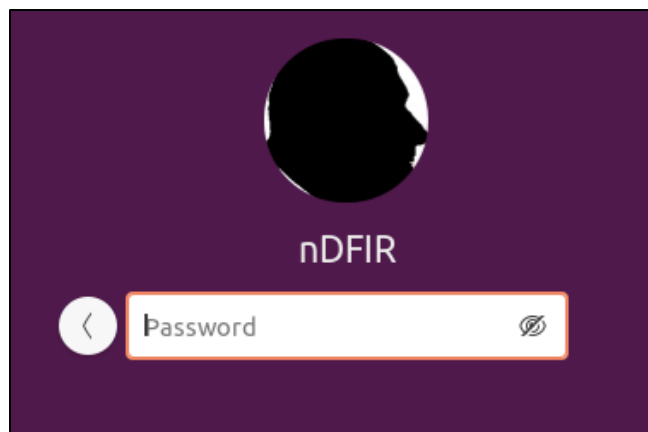
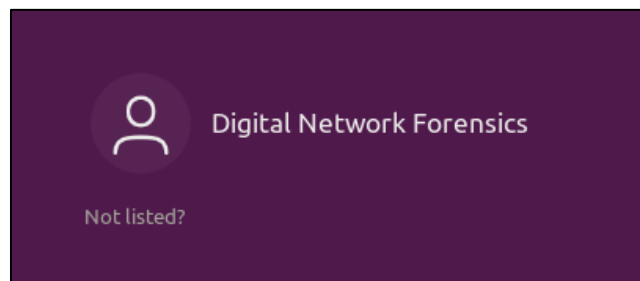
---

*Evidence: NDFIR-2021-11-29.ovf*

*Takeaways: Students will be introduced to the Network DFIR Workstation and included tools.*

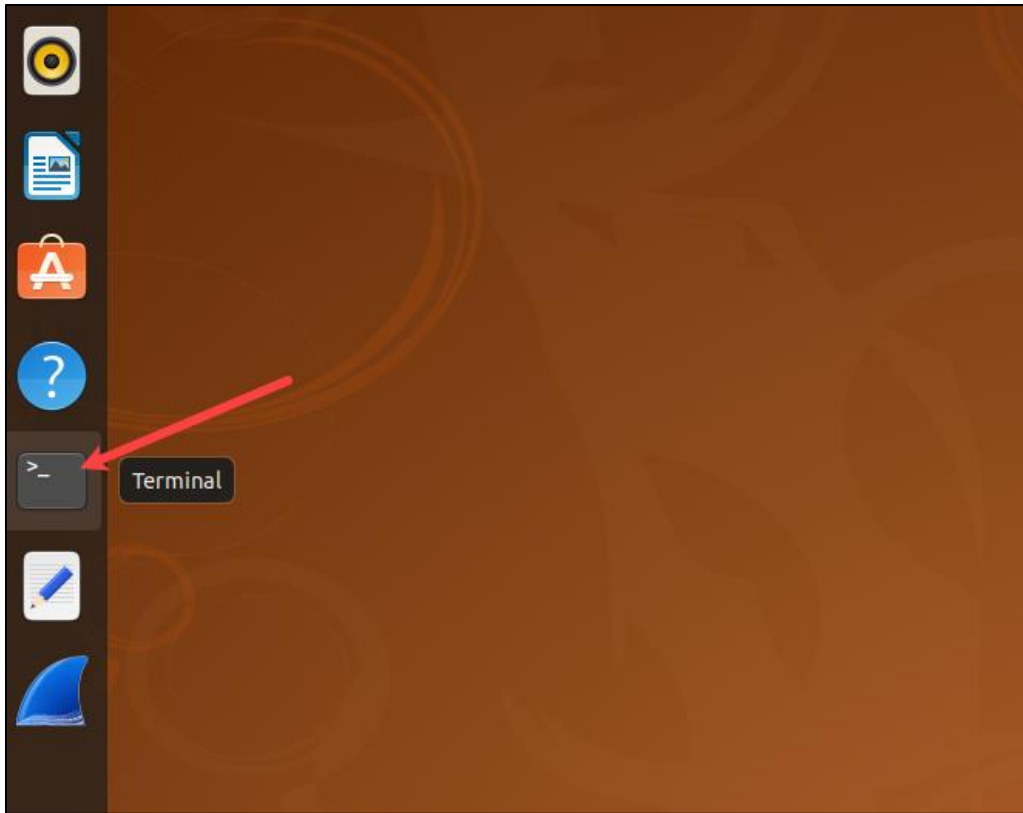
---

1. Download the virtual machine here: [https://ndfir.s3.amazonaws.com/OVF\\_2021-11-29.zip](https://ndfir.s3.amazonaws.com/OVF_2021-11-29.zip) (URL subject to change)
  - a. Unzip and open (pw: lheartpcaps\_2021-11-29)
  - b. Proceed to install
2. Login:
  - a. User: **ndfir**
  - b. Pass: **ndfir**



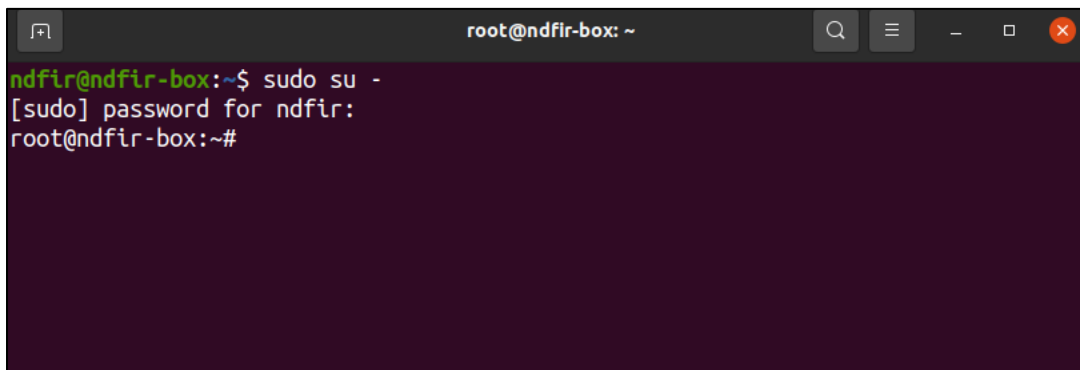
**NDFIR VM Login**

3. Start a terminal session and ensure you can elevate to root:



Issue the following command and type 'ndfir' for the password.

```
sudo su -
```



4. Internet check

```
ping 8.8.8.8
```

```
root@ndfir-box: ~  
root@ndfir-box:~#  
root@ndfir-box:~# ping -c 5 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=24.6 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=28.9 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=13.3 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=18.9 ms  
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=14.5 ms  
  
--- 8.8.8.8 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4008ms  
rtt min/avg/max/mdev = 13.286/20.029/28.861/5.938 ms  
root@ndfir-box:~#
```

5. Navigate to /home/ndfir/labs/

```
cd /home/ndfir/labs/
```

```
root@ndfir-box:/home/ndfir/labs# ls  
0001 0010 0011 0100 0101 0110 0111 1000 1001 1010  
root@ndfir-box:/home/ndfir/labs#  
root@ndfir-box:/home/ndfir/labs#
```

6. Each folder will be used, respectively, to complete each lab.
  - a. NOTE: some folders have been left empty (0101 and 1010) – this is intentional.