# Observing SSH & DHCP Traffic Using Wireshark & PowerShell in Windows VM

---

## Part 1: Observe ssh Traffic

---

### Step 1: Start VMs and Ensure they are Running

- Open Azure and start VMs
- Open Microsoft Remote Desktop and login to your Windows VM

---

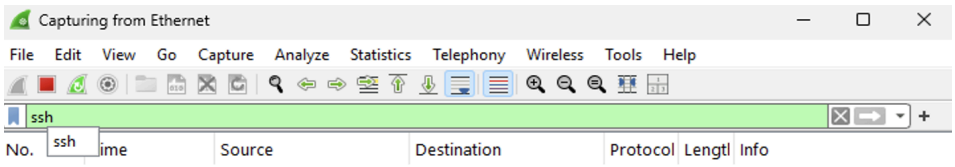
### Step 2: Observe SSH Traffic

- Open Wireshark.
- Begin packet capture on the appropriate Ethernet interface.

---

### Step 3: Apply SSH Filter

- In Wireshark's filter bar, type:
  `ssh`
- Press Enter to apply the filter.



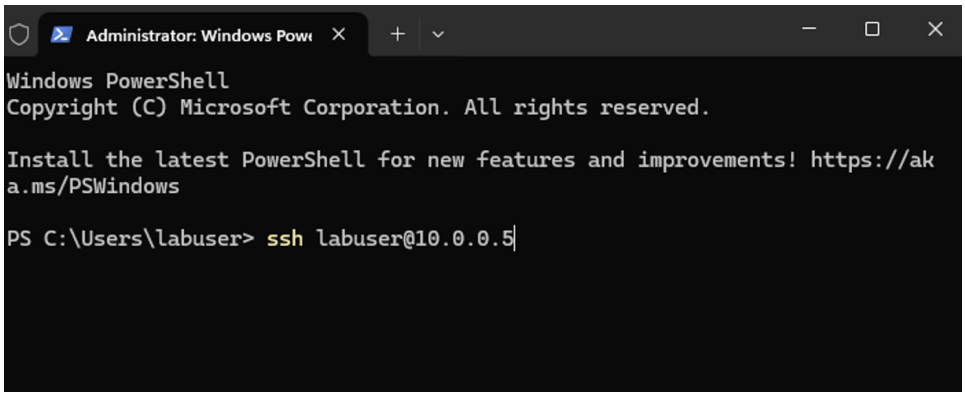

---

## Step 4: SSH into the Ubuntu VM

- Open PowerShell as Administrator on the Windows VM.

Enter the SSH command:
ssh <username>@<Private IP Address>

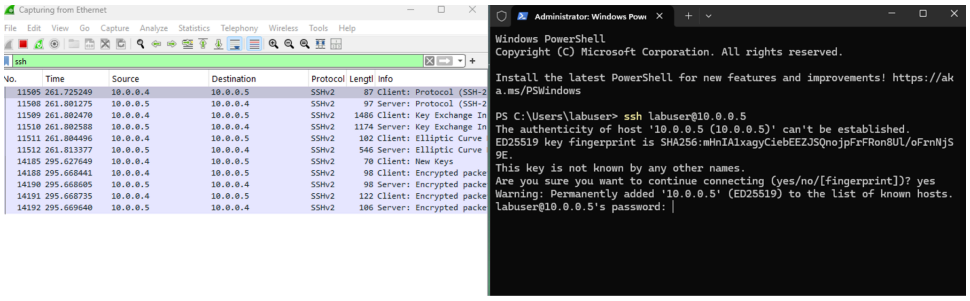
```
ssh labuser@10.0.0.5
```




---

## Step 5: Accept Host Key and Authenticate

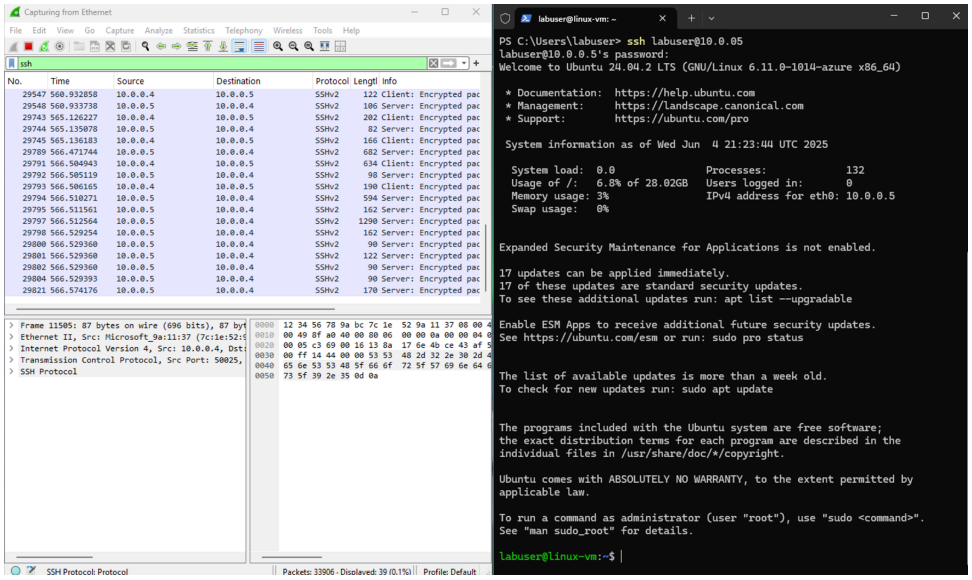
- When prompted, type `yes` to accept the fingerprint.
- Enter the password for `labuser`.
- Notice that with every entry there is ssh traffic.




---

## Step 6: Observe ssh Traffic

- Now that we are in the ubuntu vm we can begin to observe more ssh traffic.




---

## Step 7: Execute Linux Commands

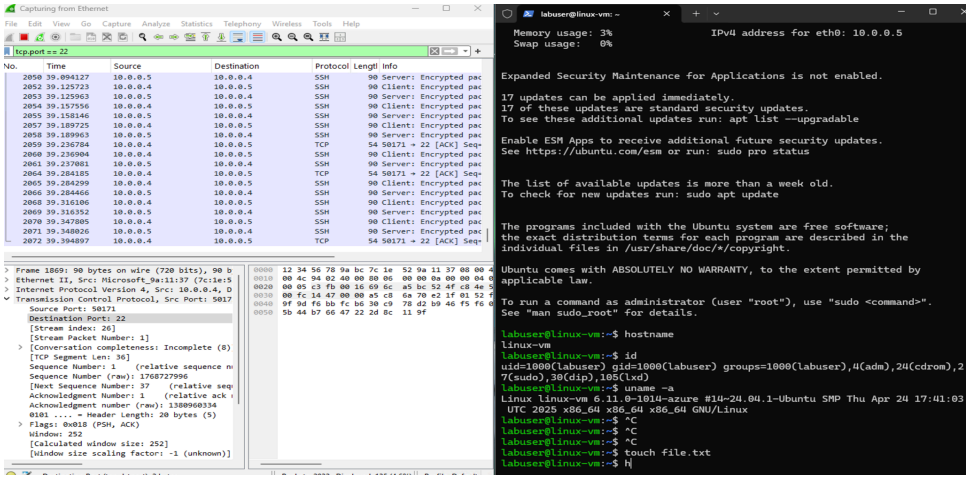
- Once connected to the Ubuntu VM, type the following:
- `hostname`
- `id`
- `uname -a`
- `touch file.txt` this will create a file
- Observe that with every key stroke there is ssh traffic

```
Last login: Wed Jun  4 21:23:45 2025 from 10.0.0.4
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

labuser@linux-vm:~$ hostname
linux-vm
labuser@linux-vm:~$ id
uid=1000(labuser) gid=1000(labuser) groups=1000(labuser),4(adm),24(cdrom),27(sudo),30(dip),105(lxd)
labuser@linux-vm:~$ uname -a
Linux linux-vm 6.11.0-1014-azure #14~24.04.1-Ubuntu SMP Thu Apr 24 17:41:03 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
labuser@linux-vm:~$ touch file.txt
labuser@linux-vm:~$ touchfile.txt
```

---

## Step 8: Observe SSH Packet Activity in Wireshark

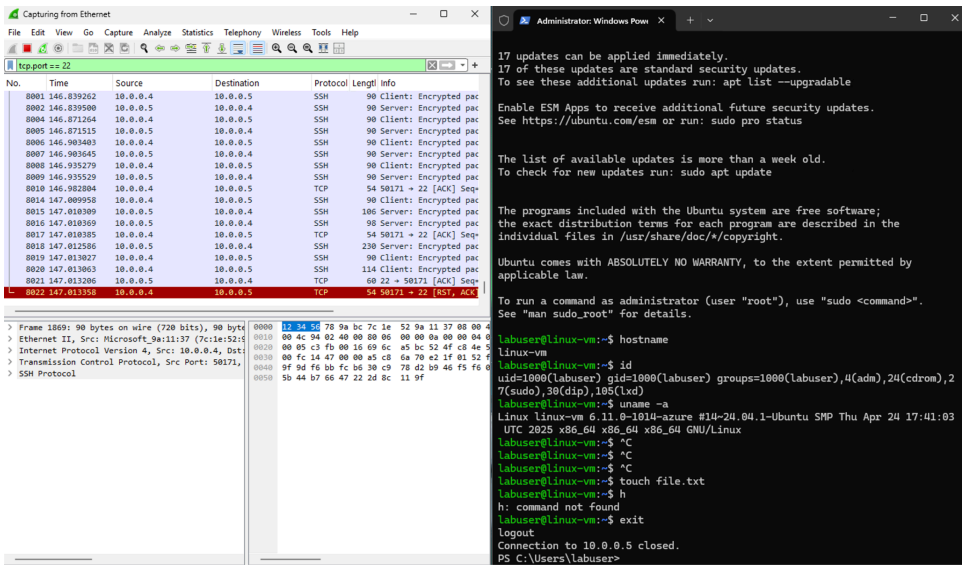
- In the Wireshark filter type:
  `tcp.port == 22`
- ssh uses TCP port 22
- Observe the live stream of encrypted packets during the SSH session.




---

## Step 9: Exit the SSH Session

- In PowerShell type:
  `exit`
- Confirm the session closes and SSH traffic stops.



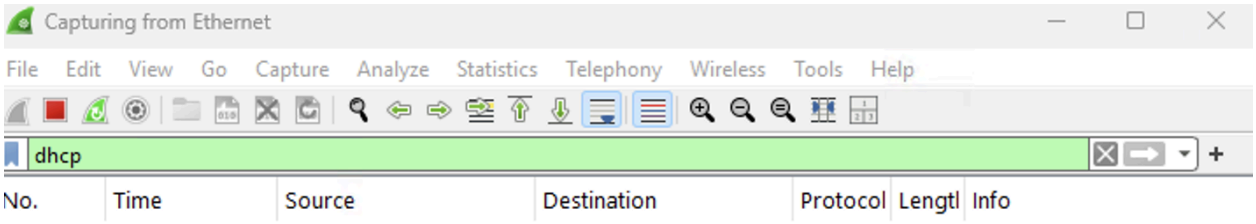

---

# Part 2: Observe DHCP Traffic

---

## Step 1: Filter for DHCP Traffic in Wireshark

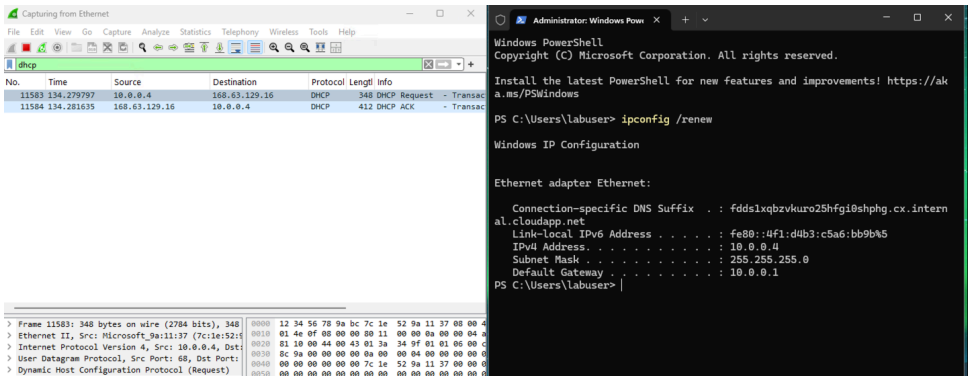
- In Wireshark's filter bar, type:
  `dhcp`
- Press Enter.




---

## Step 2: Release & Renew IP Address via PowerShell

- Open PowerShell as Administrator.
- Run the following in PowerShell:
  `ipconfig /renew`

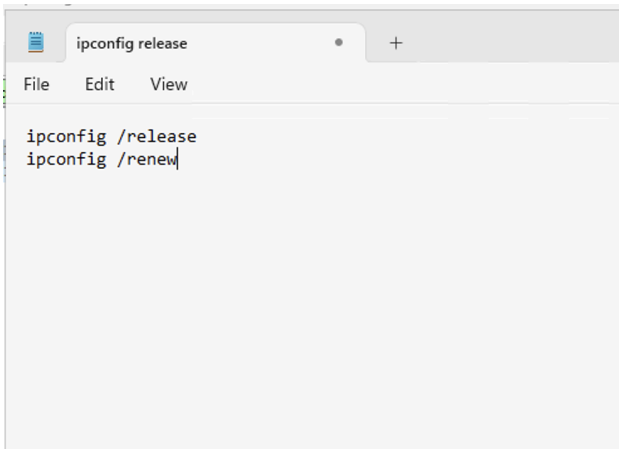


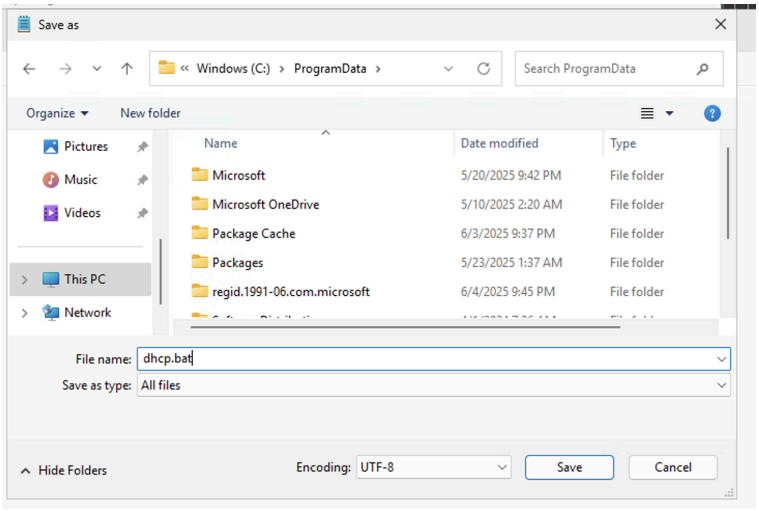

---

## Step 3: Automate IP Renewal with a Batch Script (Optional)

- Open Notepad and type:
  ```
  ipconfig /release
  ipconfig /renew
  ```

- Save the file as: `dhcp.bat`
- Save it in: `C:\ProgramData`




---

## Step 4: Navigate to Batch Script Location

- In PowerShell type:
  `cd C:\ProgramData`
- `ls`

```
PS C:\Users\labuser> cd c:\programdata
PS C:\programdata> ls


    Directory: C:\programdata


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d---s-         5/20/2025   9:42 PM                Microsoft
d-----         5/10/2025   2:20 AM                Microsoft OneDrive
d-----          6/3/2025   9:37 PM                Package Cache
d-----         5/23/2025   1:37 AM                Packages
d-----          6/4/2025   9:45 PM                regid.1991-06.com.micros
                                                  oft
d-----          4/1/2024   7:26 AM                SoftwareDistribution
d-----          4/1/2024   8:08 AM                ssh
d-----         5/10/2025   2:19 AM                USOPrivate
d-----          4/1/2024   7:26 AM                USOShared
-a----          6/4/2025   9:50 PM             34 dhcp.bat


PS C:\programdata>
```

---

## Step 5: Run the Script to Trigger DHCP Events

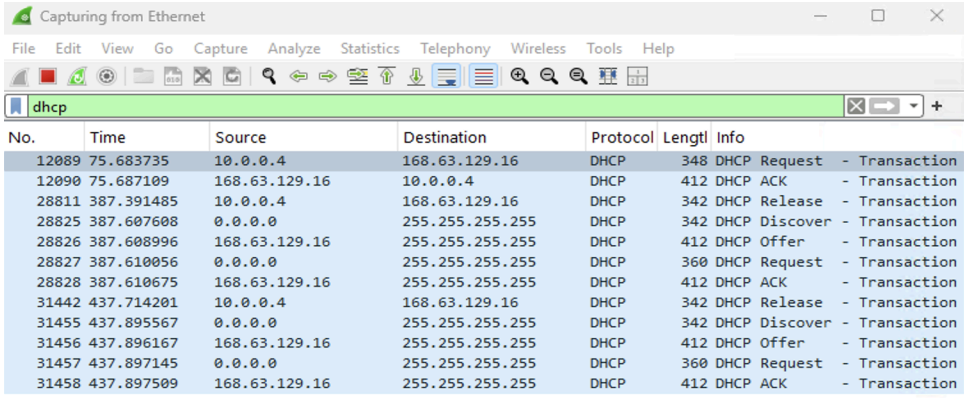
- Execute the script in PowerShell:
  `.\dhcp.bat`

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : fdds1xqbzvkuro25hfgi0shphg.cx.intern
al.cloudapp.net
   Link-local IPv6 Address . . . . . : fe80::4f1:d4b3:c5a6:bb9b%6
   IPv4 Address. . . . . . . . . . . : 10.0.0.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1
PS C:\programdata> .\dhcp.bat

C:\ProgramData>ipconfig /release

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4f1:d4b3:c5a6:bb9b%6
   Default Gateway . . . . . . . . . :

C:\ProgramData>ipconfig /renew

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : fdds1xqbzvkuro25hfgi0shphg.cx.intern
al.cloudapp.net
   Link-local IPv6 Address . . . . . : fe80::4f1:d4b3:c5a6:bb9b%6
   IPv4 Address. . . . . . . . . . . : 10.0.0.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1
PS C:\programdata>
```

---

## Step 6: Observe DHCP Traffic in Wireshark

- In Wireshark, observe the following:
  - **DHCP Discover**
  - **DHCP Offer**
  - **DHCP Request**
  - **DHCP ACK**




| No. | Time | Source | Destination | Protocol | Lengtl | Info |
|---|---|---|---|---|---|---|
| 12089 | 75.683735 | 10.0.0.4 | 168.63.129.16 | DHCP | 348 | DHCP Request - Transaction |
| 12090 | 75.687109 | 168.63.129.16 | 10.0.0.4 | DHCP | 412 | DHCP ACK - Transaction |
| 28811 | 387.391485 | 10.0.0.4 | 168.63.129.16 | DHCP | 342 | DHCP Release - Transaction |
| 28825 | 387.607608 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Transaction |
| 28826 | 387.608996 | 168.63.129.16 | 255.255.255.255 | DHCP | 412 | DHCP Offer - Transaction |
| 28827 | 387.610056 | 0.0.0.0 | 255.255.255.255 | DHCP | 360 | DHCP Request - Transaction |
| 28828 | 387.610675 | 168.63.129.16 | 255.255.255.255 | DHCP | 412 | DHCP ACK - Transaction |
| 31442 | 437.714201 | 10.0.0.4 | 168.63.129.16 | DHCP | 342 | DHCP Release - Transaction |
| 31455 | 437.895567 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Transaction |
| 31456 | 437.896167 | 168.63.129.16 | 255.255.255.255 | DHCP | 412 | DHCP Offer - Transaction |
| 31457 | 437.897145 | 0.0.0.0 | 255.255.255.255 | DHCP | 360 | DHCP Request - Transaction |
| 31458 | 437.897509 | 168.63.129.16 | 255.255.255.255 | DHCP | 412 | DHCP ACK - Transaction |

---

## Step 7: Handle Temporary Disconnection

- If connection drops briefly after IP release, you may see a message like: