Monitoring ICMP Traffic with Wireshark & Security Protocols on Azure

---

Step 1: Access Azure Portal

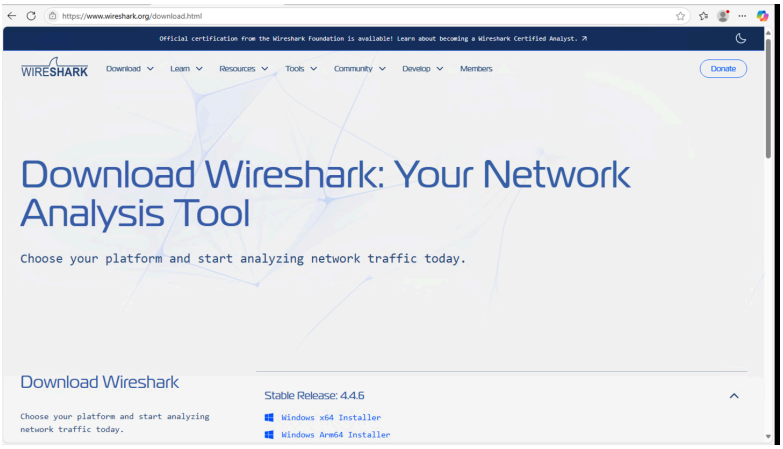
- Go to https://portal.azure.com
- Confirm your Windows and Ubuntu VMs are running

Step 2: Launch Microsoft Remote Desktop (on macOS)

- Install Microsoft Remote Desktop from the App Store if not already installed
- Connect to your Windows 10 VM

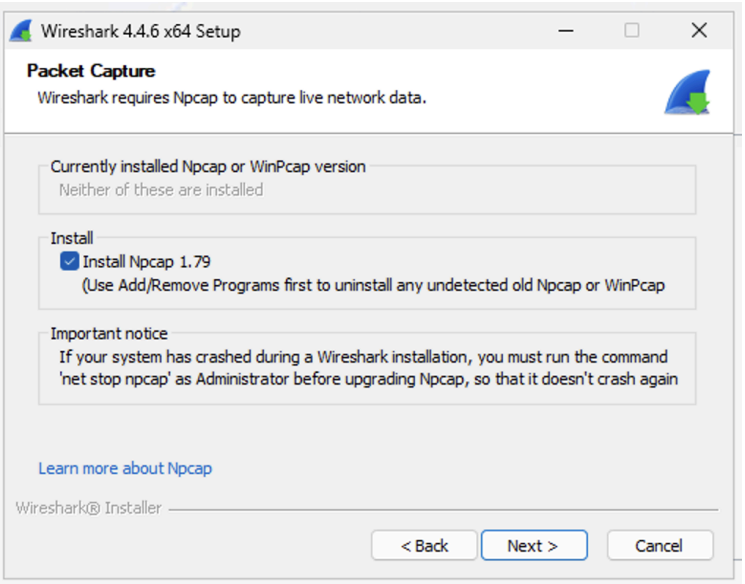
Step 3: Download and Install Wireshark

- Visit https://www.wireshark.org/download.html
- Download the appropriate Windows installer
- → *in this case, we'll use the 64 bit installer.*



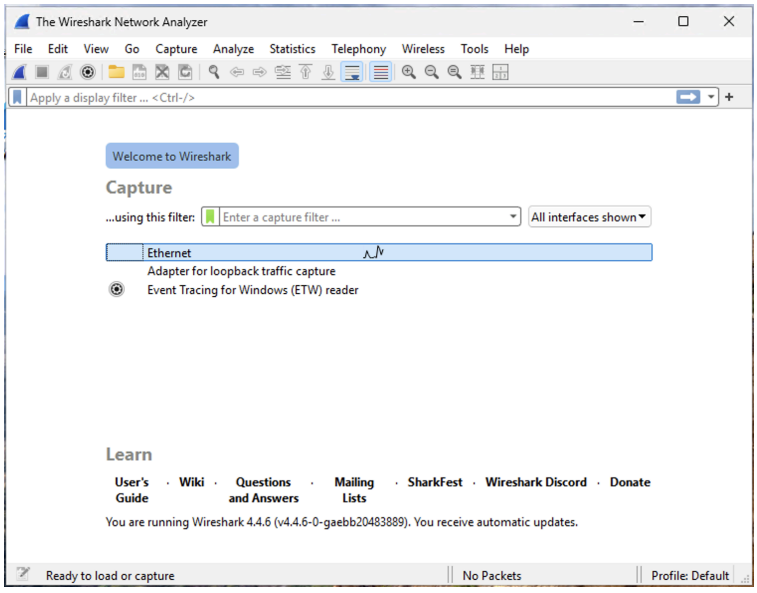
Step 4: Complete Wireshark Setup

- Run the installer and proceed through the setup wizard
- Accept the license and confirm Npcap installation
- Skip the USBcap, we don't need that one
- Accept the license agreement



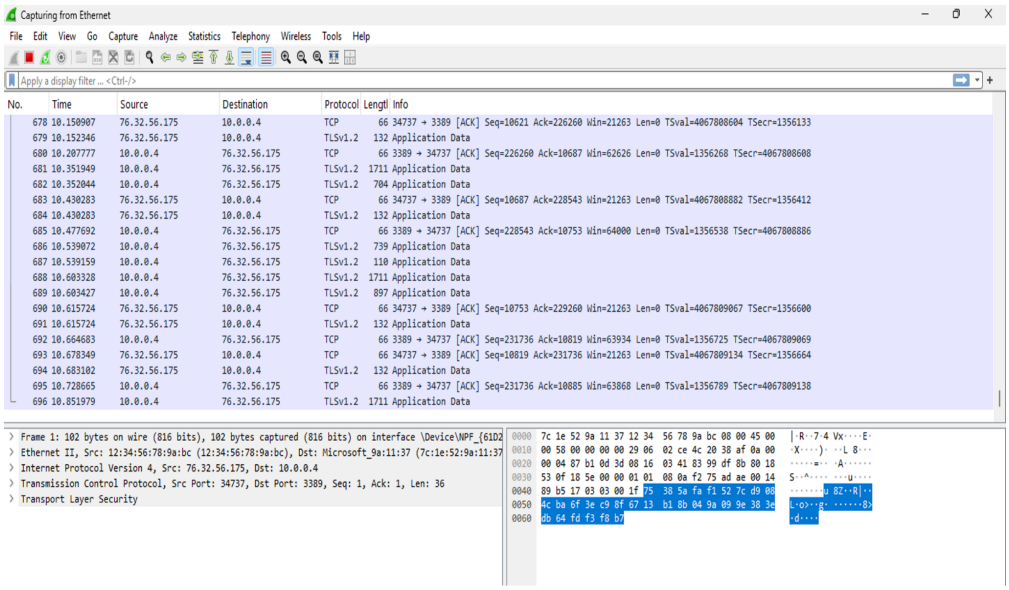
Step 5: Launch Wireshark

- Open Wireshark and select the Ethernet interface
- Begin capturing traffic



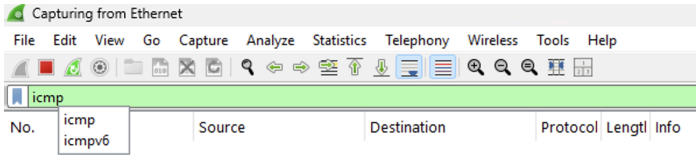
Step 6: Observe Traffic

- Before any filters are input, you'll observe a lot of traffic in Wireshark



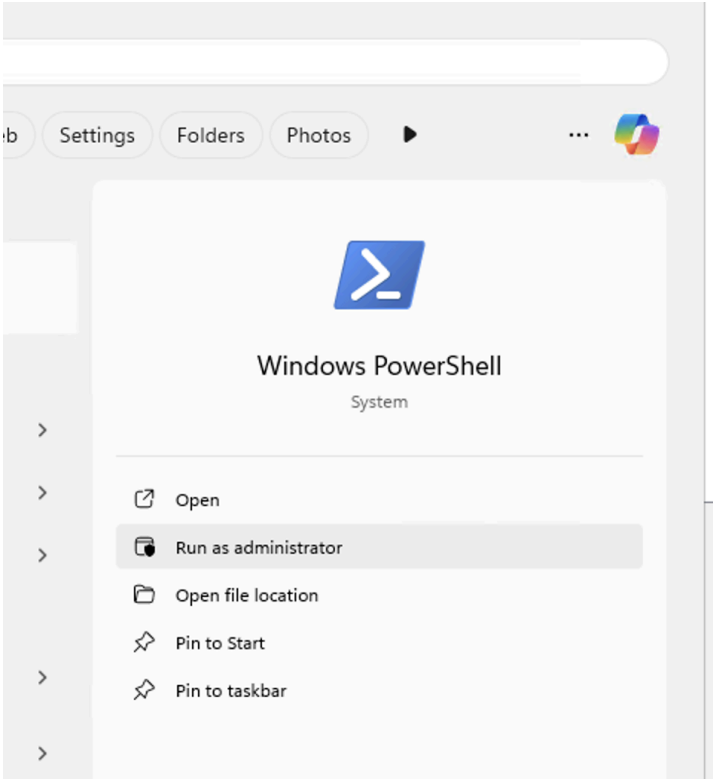
Step 7: Filter for ICMP Traffic

- Type `icmp` into the display filter bar to isolate ping traffic



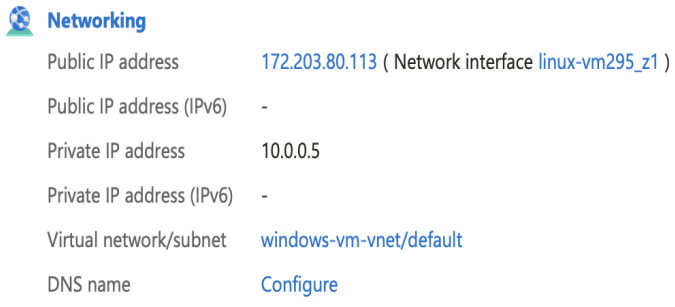
Step 8: Open PowerShell as Admin

- Launch PowerShell using “Open PowerShell”



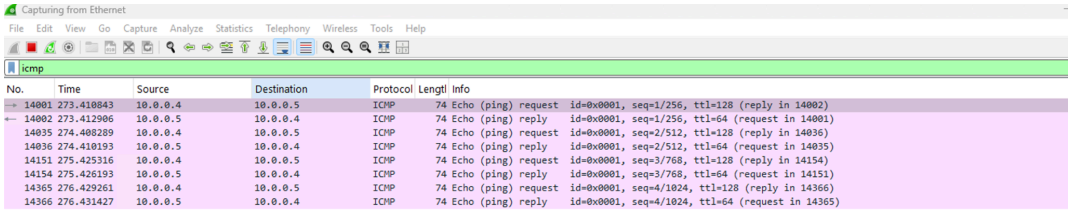
Step 9: Go to Azure and copy the Private IP Address for your Ubunt VM

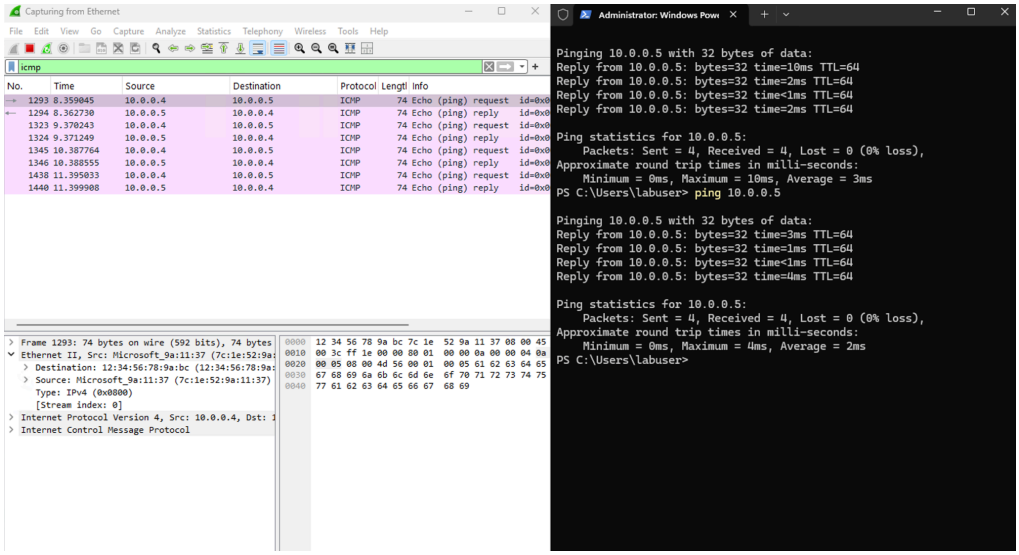
- Copy the Ubunt-vm Private IP Address



Step 10: In PowerShell Start a Ping

- In PowerShell, type “ping” and paste the Ubunt -vm Private IP Address
  `ping 10.0.0.5`
- Go back to Wireshark and observe the filtered ICMP Traffic
- Once you’re done observing the ICMP Traffic, refresh without saving

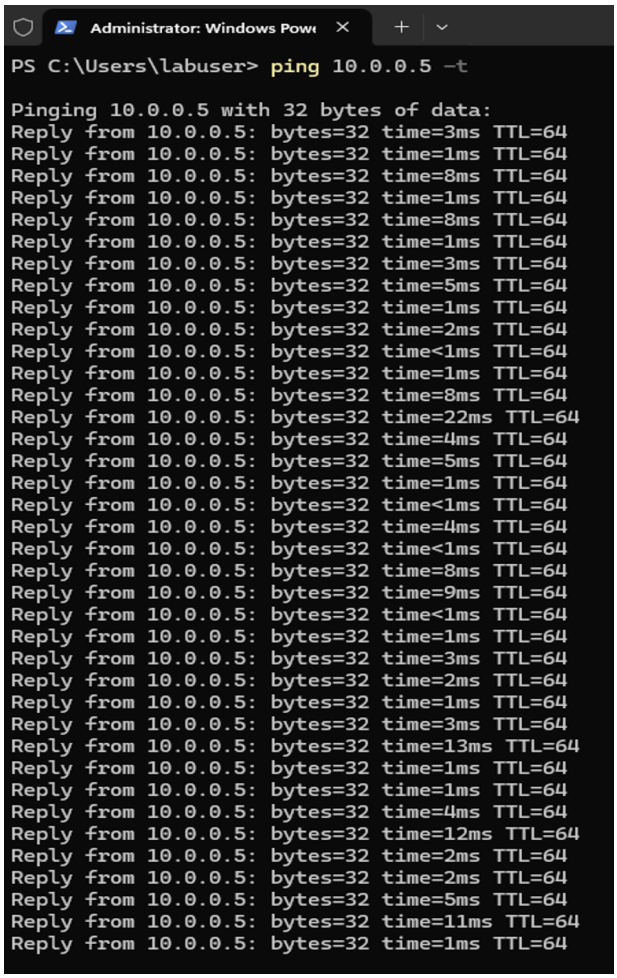




Step 11: Start Continuous Ping

- From Windows VM, run:
- In Powershell, type “ping” the Ubunt-vm “Private IP Address” and then “-t”

```
ping 10.0.0.5 -t
```



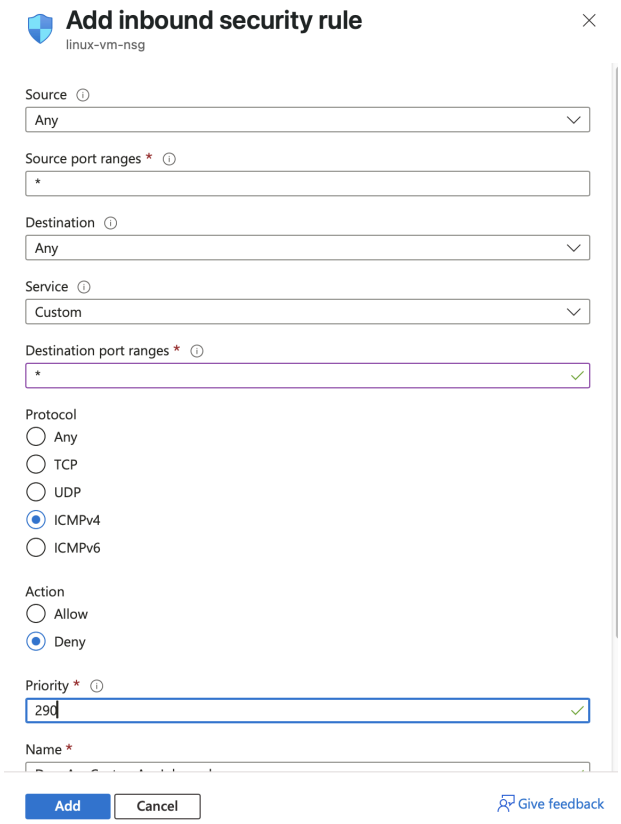
Step 12: Observe ICMP Requests and Replies in Wireshark

- You should see continuous echo requests and replies in Wireshark
- Confirm successful packet round trips
- Leave the continuous Ping running

Setup Network Security Group

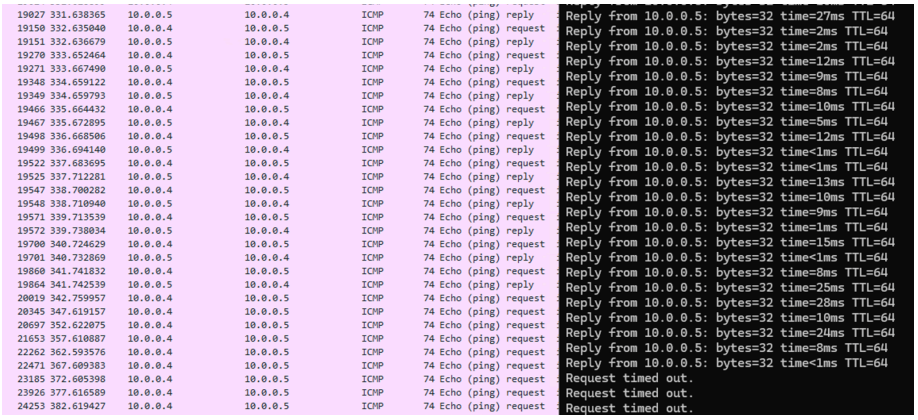
Step 13: Apply an NSG Rule to Block ICMP

- Go to the Ubuntu VM's Network Security Group
- Add a new inbound rule:
    - Protocol: ICMPv4
    - Action: Deny
    - Priority: Lower than existing allow rules



Step 14: Observe Ping Timeouts

- Return to the Windows VM
- The ping command should now display “Request timed out”
- Wireshark shows ICMP requests but no replies



19027	331.638365	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply
19150	332.635040	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
19151	332.636679	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply
19270	333.652464	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
19271	333.667490	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply
19348	334.659122	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
19349	334.659793	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply
19466	335.664432	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
19467	335.672895	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply
19498	336.668506	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
19499	336.694140	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply
19522	337.683695	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
19525	337.712281	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply
19547	338.700282	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
19548	338.710940	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply
19571	339.713539	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
19572	339.738034	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply
19700	340.724629	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
19701	340.732869	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply
19860	341.741832	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
19864	341.742539	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply
20019	342.759957	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
20345	347.619157	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
20697	352.622075	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
21653	357.610887	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
22262	362.593576	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
22471	367.609383	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
23185	372.605398	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
23926	377.616589	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request
24253	382.619427	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request

```
Reply from 10.0.0.5: bytes=32 time=27ms TTL=64
Reply from 10.0.0.5: bytes=32 time=2ms TTL=64
Reply from 10.0.0.5: bytes=32 time=2ms TTL=64
Reply from 10.0.0.5: bytes=32 time=12ms TTL=64
Reply from 10.0.0.5: bytes=32 time=9ms TTL=64
Reply from 10.0.0.5: bytes=32 time=8ms TTL=64
Reply from 10.0.0.5: bytes=32 time=10ms TTL=64
Reply from 10.0.0.5: bytes=32 time=5ms TTL=64
Reply from 10.0.0.5: bytes=32 time=12ms TTL=64
Reply from 10.0.0.5: bytes=32 time<1ms TTL=64
Reply from 10.0.0.5: bytes=32 time<1ms TTL=64
Reply from 10.0.0.5: bytes=32 time=13ms TTL=64
Reply from 10.0.0.5: bytes=32 time=10ms TTL=64
Reply from 10.0.0.5: bytes=32 time=9ms TTL=64
Reply from 10.0.0.5: bytes=32 time=1ms TTL=64
Reply from 10.0.0.5: bytes=32 time=15ms TTL=64
Reply from 10.0.0.5: bytes=32 time<1ms TTL=64
Reply from 10.0.0.5: bytes=32 time=8ms TTL=64
Reply from 10.0.0.5: bytes=32 time=25ms TTL=64
Reply from 10.0.0.5: bytes=32 time=28ms TTL=64
Reply from 10.0.0.5: bytes=32 time=10ms TTL=64
Reply from 10.0.0.5: bytes=32 time=24ms TTL=64
Reply from 10.0.0.5: bytes=32 time=8ms TTL=64
Reply from 10.0.0.5: bytes=32 time<1ms TTL=64
Request timed out.
Request timed out.
Request timed out.
```

Step 15: Remove/Disable the Deny Rule

- Go back to Azure and remove or disable the ICMP deny rule

Step 16: Observe Ping Recovery

- Ping replies should resume
- Wireshark should show echo replies again