

Monitoring ICMP Traffic with Wireshark & Security Protocols on Azure

Step 1: Access Azure Portal

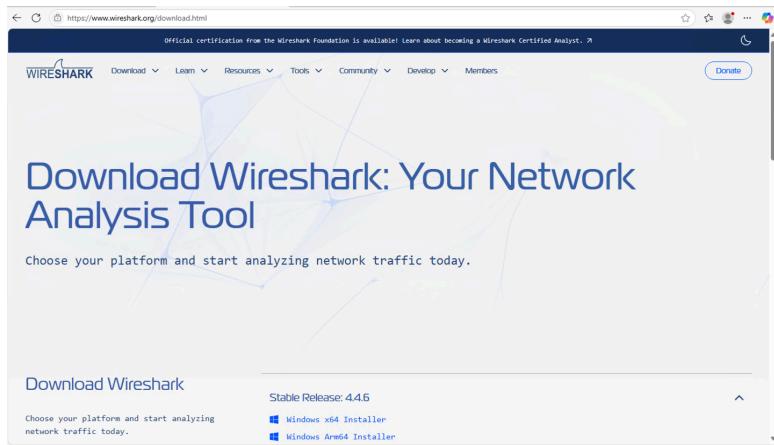
- Go to <https://portal.azure.com>
 - Confirm your Windows and Ubuntu VMs are running
-

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
-

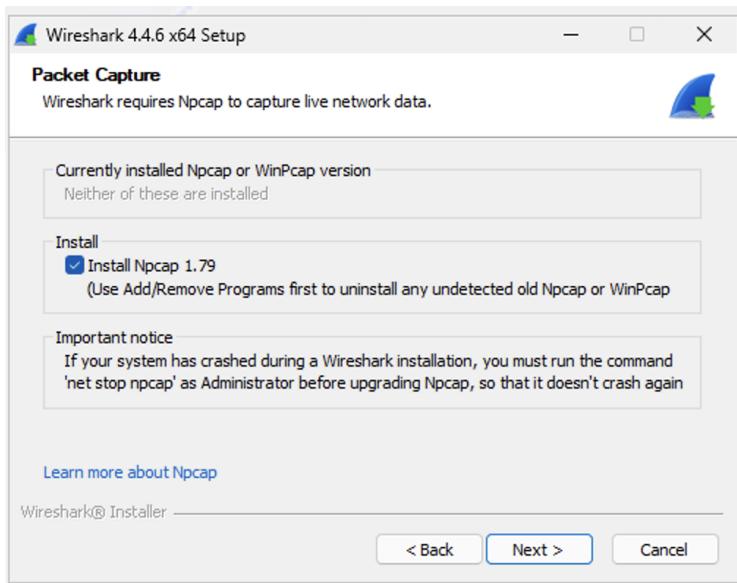
Step 3: Download and Install Wireshark

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



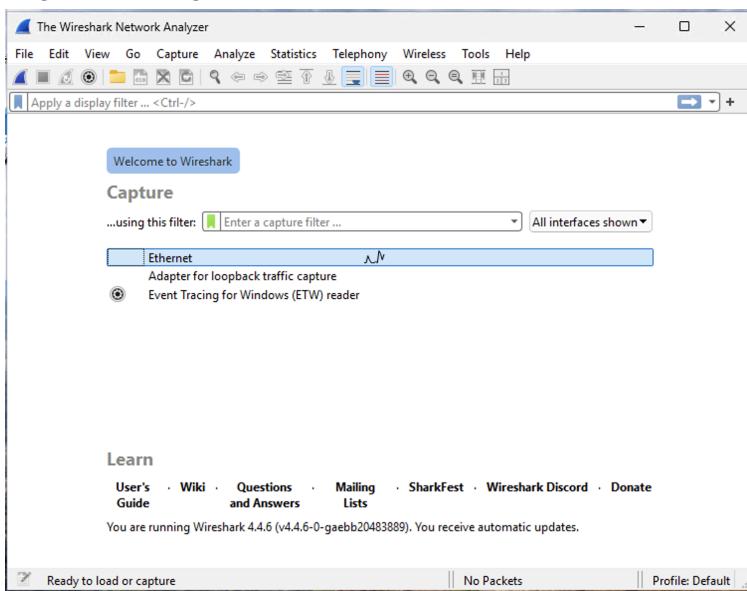
Step 4: Complete Wireshark Setup

- 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



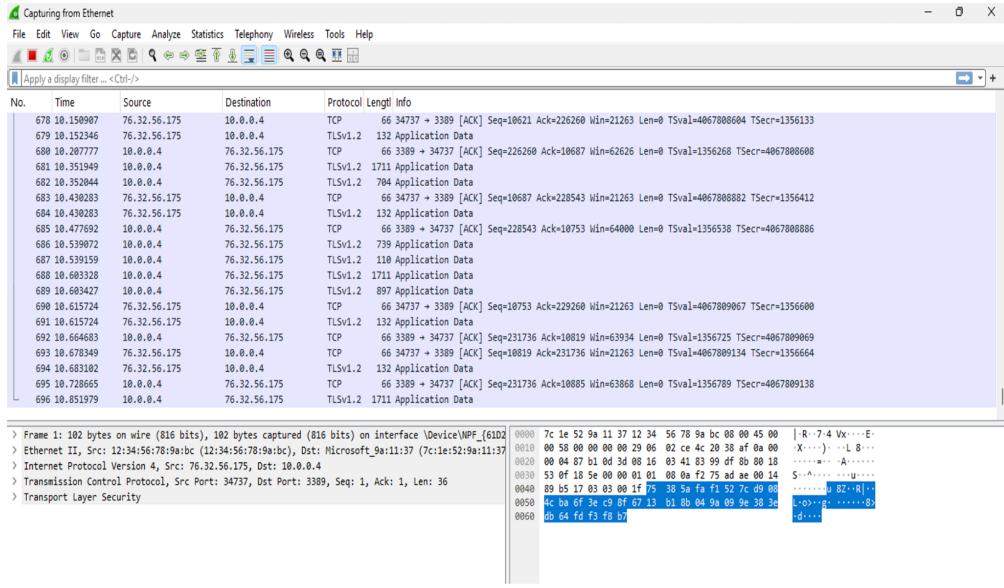
Step 5: Launch Wireshark

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



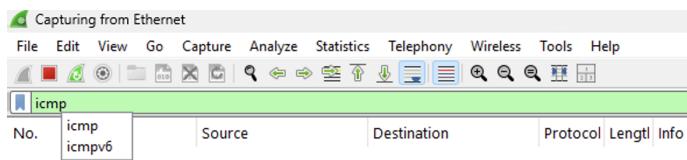
Step 6: Observe Traffic

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



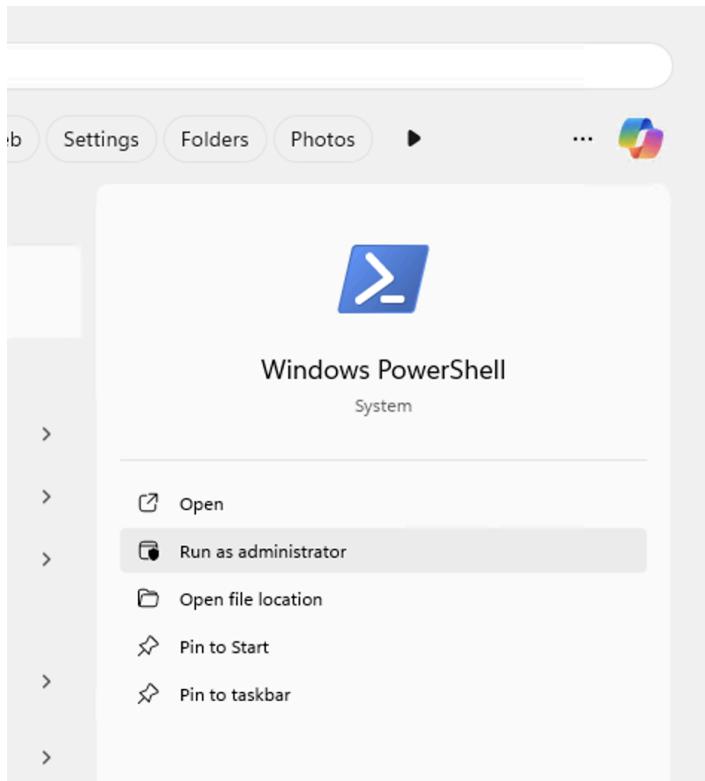
Step 7: Filter for ICMP Traffic

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



Step 8: Open PowerShell as Admin

- Launch PowerShell using “Open PowerShell”



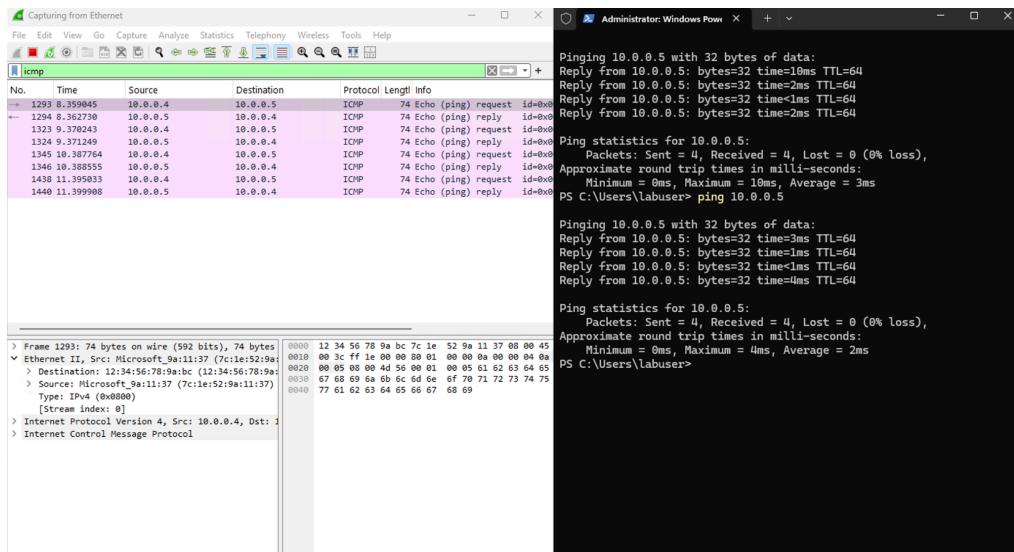
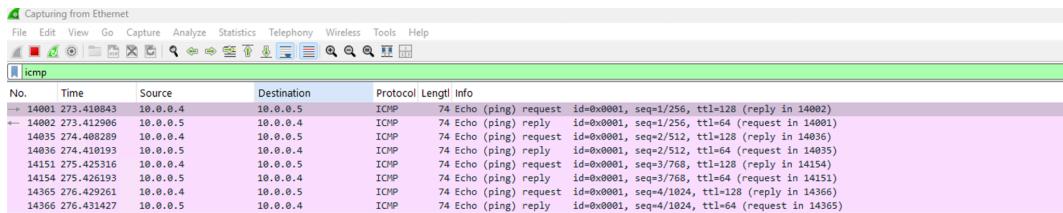
Step 9: Go to Azure and copy the Private IP Address for your Ubuntu VM

- Copy the Ubuntu-vm Private IP Address

Networking	
Public IP address	172.203.80.113 (Network interface linux-vm295_z1)
Public IP address (IPv6)	-
Private IP address	10.0.0.5
Private IP address (IPv6)	-
Virtual network/subnet	windows-vm-vnet/default
DNS name	Configure

Step 10: In PowerShell Start a Ping

- In PowerShell, type “ping” and paste the Ubuntu -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 Ubuntu-vm “Private IP Address” and then “-t”
`ping 10.0.0.5 -t`



A screenshot of a Windows PowerShell window titled "Administrator: Windows Pow". The command entered is "ping 10.0.0.5 -t". The output shows a continuous stream of ping responses from the target IP address, 10.0.0.5. Each response includes the number of bytes (32), the time taken (e.g., 3ms, 1ms, 8ms, etc.), and the TTL value (64). The responses are timestamped and show varying round-trip times.

```
PS C:\Users\labuser> ping 10.0.0.5 -t

Pinging 10.0.0.5 with 32 bytes of data:
Reply from 10.0.0.5: bytes=32 time=3ms 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=1ms 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
Reply from 10.0.0.5: bytes=32 time=3ms TTL=64
Reply from 10.0.0.5: bytes=32 time=5ms TTL=64
Reply from 10.0.0.5: bytes=32 time=1ms TTL=64
Reply from 10.0.0.5: bytes=32 time=2ms 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=8ms TTL=64
Reply from 10.0.0.5: bytes=32 time=22ms TTL=64
Reply from 10.0.0.5: bytes=32 time=4ms TTL=64
Reply from 10.0.0.5: bytes=32 time=5ms 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=4ms 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=9ms 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=3ms TTL=64
Reply from 10.0.0.5: bytes=32 time=2ms TTL=64
Reply from 10.0.0.5: bytes=32 time=1ms TTL=64
Reply from 10.0.0.5: bytes=32 time=3ms TTL=64
Reply from 10.0.0.5: bytes=32 time=13ms 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=4ms TTL=64
Reply from 10.0.0.5: bytes=32 time=12ms 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=5ms TTL=64
Reply from 10.0.0.5: bytes=32 time=11ms TTL=64
Reply from 10.0.0.5: bytes=32 time=1ms TTL=64
```

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

 **Add inbound security rule** ×

linux-vm-nsgrule

Source ①

Source port ranges * ①

Destination ①

Service ①

Destination port ranges * ①

Protocol
 Any
 TCP
 UDP
 ICMPv4
 ICMPv6

Action
 Allow
 Deny

Priority * ①

Name * ①

Give feedback

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

19827	331.638365	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply	Reply from 10.0.0.5: bytes=32 time=27ms TTL=64
19150	332.635940	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Reply from 10.0.0.5: bytes=32 time=2ms TTL=64
19151	332.636679	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply	Reply from 10.0.0.5: bytes=32 time=2ms TTL=64
19270	333.636674	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Reply from 10.0.0.5: bytes=32 time=12ms TTL=64
19271	333.637489	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply	Reply from 10.0.0.5: bytes=32 time=27ms TTL=64
19348	334.635912	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Reply from 10.0.0.5: bytes=32 time=9ms TTL=64
19349	334.635973	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply	Reply from 10.0.0.5: bytes=32 time=8ms TTL=64
19466	335.664432	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Reply from 10.0.0.5: bytes=32 time=10ms TTL=64
19467	335.672895	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply	Reply from 10.0.0.5: bytes=32 time=5ms TTL=64
19498	336.668596	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Reply from 10.0.0.5: bytes=32 time=12ms TTL=64
19499	336.694140	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply	Reply from 10.0.0.5: bytes=32 time<1ms TTL=64
19522	337.683695	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Reply from 10.0.0.5: bytes=32 time=1ms TTL=64
19525	337.712281	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply	Reply from 10.0.0.5: bytes=32 time=1ms TTL=64
19547	338.700282	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Reply from 10.0.0.5: bytes=32 time=1ms TTL=64
19548	338.710940	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply	Reply from 10.0.0.5: bytes=32 time=10ms TTL=64
19571	339.713539	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Reply from 10.0.0.5: bytes=32 time=9ms TTL=64
19572	339.738034	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply	Reply from 10.0.0.5: bytes=32 time=1ms TTL=64
19700	340.724629	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Reply from 10.0.0.5: bytes=32 time=15ms TTL=64
19701	340.732869	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply	Reply from 10.0.0.5: bytes=32 time<1ms TTL=64
19860	341.741832	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Reply from 10.0.0.5: bytes=32 time=8ms TTL=64
19864	341.742539	10.0.0.5	10.0.0.4	ICMP	74 Echo (ping) reply	Reply from 10.0.0.5: bytes=32 time=25ms TTL=64
20019	342.759957	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Reply from 10.0.0.5: bytes=32 time=28ms TTL=64
20345	347.619157	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Reply from 10.0.0.5: bytes=32 time=10ms TTL=64
20697	352.622675	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Reply from 10.0.0.5: bytes=32 time=24ms TTL=64
21653	357.610887	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Reply from 10.0.0.5: bytes=32 time=8ms TTL=64
22262	362.593576	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Reply from 10.0.0.5: bytes=32 time=1ms TTL=64
22471	367.603383	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Reply from 10.0.0.5: bytes=32 time=8ms TTL=64
23153	371.649748	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Request timed out.
23926	377.615589	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	Request timed out.
24253	382.619427	10.0.0.4	10.0.0.5	ICMP	74 Echo (ping) request	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

No.	Time	Source	Destination	Protocol	Length	Info
94972	1768.060321	10.0.0.4	10.0.0.5	ICMP	74	Echo (ping) request id=0
95621	1773.055258	10.0.0.4	10.0.0.5	ICMP	74	Echo (ping) request id=0
95899	1778.055850	10.0.0.4	10.0.0.5	ICMP	74	Echo (ping) request id=0
96270	1783.045415	10.0.0.4	10.0.0.5	ICMP	74	Echo (ping) request id=0
96438	1788.046617	10.0.0.4	10.0.0.5	ICMP	74	Echo (ping) request id=0
96529	1793.046486	10.0.0.4	10.0.0.5	ICMP	74	Echo (ping) request id=0
96676	1798.057656	10.0.0.4	10.0.0.5	ICMP	74	Echo (ping) request id=0
96776	1803.057738	10.0.0.4	10.0.0.5	ICMP	74	Echo (ping) request id=0
96871	1808.057790	10.0.0.4	10.0.0.5	ICMP	74	Echo (ping) request id=0
97018	1813.059061	10.0.0.4	10.0.0.5	ICMP	74	Echo (ping) request id=0
97122	1818.051601	10.0.0.4	10.0.0.5	ICMP	74	Echo (ping) request id=0
97210	1823.057520	10.0.0.4	10.0.0.5	ICMP	74	Echo (ping) request id=0
97371	1828.054591	10.0.0.4	10.0.0.5	ICMP	74	Echo (ping) request id=0
97372	1828.055284	10.0.0.5	10.0.0.4	ICMP	74	Echo (ping) reply id=0
97399	1829.057772	10.0.0.4	10.0.0.5	ICMP	74	Echo (ping) request id=0
97400	1829.058436	10.0.0.5	10.0.0.4	ICMP	74	Echo (ping) reply id=0
97429	1830.062560	10.0.0.4	10.0.0.5	ICMP	74	Echo (ping) request id=0
97430	1830.063317	10.0.0.5	10.0.0.4	ICMP	74	Echo (ping) reply id=0