Lab 4 — Network Monitoring & Threat Detection

Student: Clayton Holden
Course: CYBR-2102
Tool Used: Wireshark (Windows)

---

1. Overview

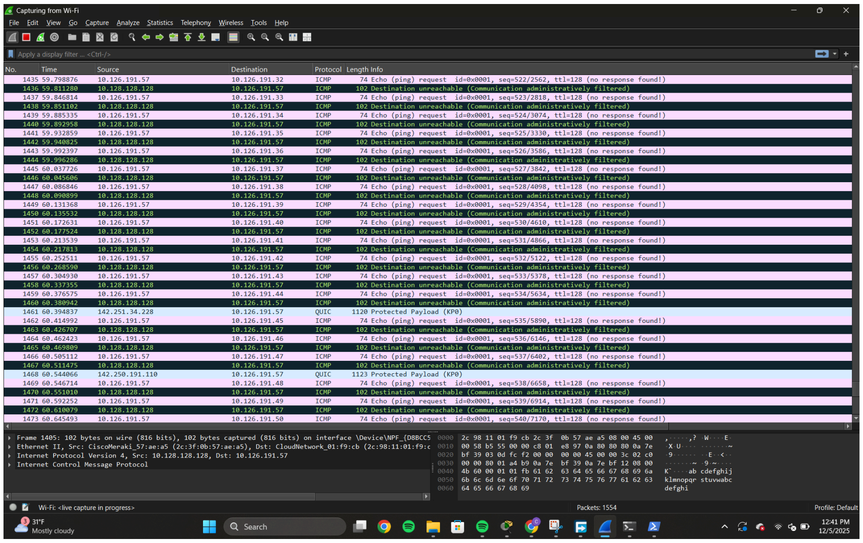
The purpose of this lab was to use Wireshark to capture real network traffic, identify suspicious or malicious activity, and document alerts that reflect common attack patterns such as ping sweeps, port scans, and DoS-like behavior.

Normal traffic was generated using continuous pings and web activity.
Attack-like traffic was simulated using Windows commands to create ICMP sweeps, TCP SYN port scans, and high-rate ICMP packets.

---

2. Evidence Screenshots

Screenshot 1: ICMP Ping Sweep


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Search
31°F
Mostly cloudy

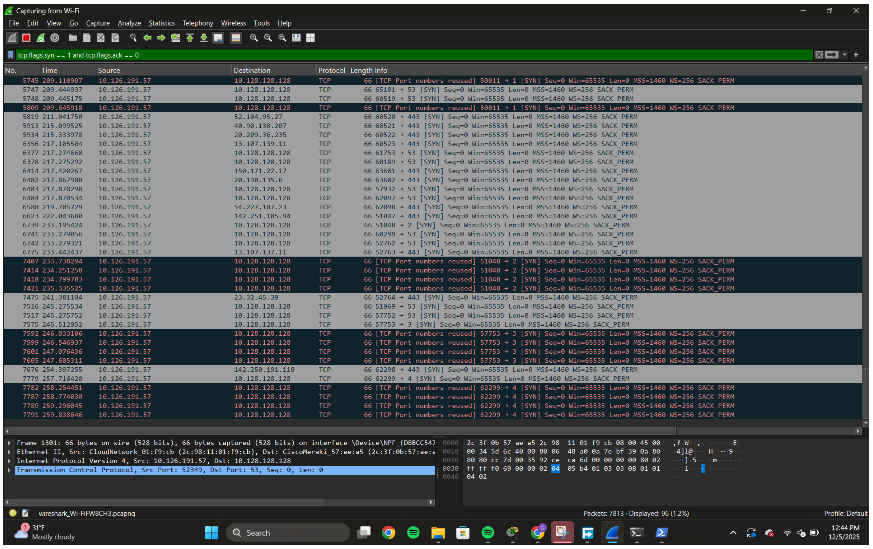
```
No.   Time      Source           Destination     Protocol Length Info
 1435 59.798876 10.126.191.57    10.126.191.32   ICMP      74 Echo (ping) request  id=0x0001, seq=522/2562, ttl=128 (no response found!)
 1436 59.811280 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1437 59.846814 10.126.191.57    10.126.191.33   ICMP      74 Echo (ping) request  id=0x0001, seq=523/2818, ttl=128 (no response found!)
 1438 59.851102 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1439 59.885335 10.126.191.57    10.126.191.34   ICMP      74 Echo (ping) request  id=0x0001, seq=524/3074, ttl=128 (no response found!)
 1440 59.892958 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1441 59.932859 10.126.191.57    10.126.191.35   ICMP      74 Echo (ping) request  id=0x0001, seq=525/3330, ttl=128 (no response found!)
 1442 59.940825 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1443 59.992397 10.126.191.57    10.126.191.36   ICMP      74 Echo (ping) request  id=0x0001, seq=526/3586, ttl=128 (no response found!)
 1444 59.996286 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1445 60.037726 10.126.191.57    10.126.191.37   ICMP      74 Echo (ping) request  id=0x0001, seq=527/3842, ttl=128 (no response found!)
 1446 60.045606 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1447 60.086846 10.126.191.57    10.126.191.38   ICMP      74 Echo (ping) request  id=0x0001, seq=528/4098, ttl=128 (no response found!)
 1448 60.090899 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1449 60.131368 10.126.191.57    10.126.191.39   ICMP      74 Echo (ping) request  id=0x0001, seq=529/4354, ttl=128 (no response found!)
 1450 60.135532 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1451 60.172631 10.126.191.57    10.126.191.40   ICMP      74 Echo (ping) request  id=0x0001, seq=530/4610, ttl=128 (no response found!)
 1452 60.177524 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1453 60.213539 10.126.191.57    10.126.191.41   ICMP      74 Echo (ping) request  id=0x0001, seq=531/4866, ttl=128 (no response found!)
 1454 60.217813 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1455 60.252511 10.126.191.57    10.126.191.42   ICMP      74 Echo (ping) request  id=0x0001, seq=532/5122, ttl=128 (no response found!)
 1456 60.268590 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1457 60.304930 10.126.191.57    10.126.191.43   ICMP      74 Echo (ping) request  id=0x0001, seq=533/5378, ttl=128 (no response found!)
 1458 60.337355 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1459 60.376575 10.126.191.57    10.126.191.44   ICMP      74 Echo (ping) request  id=0x0001, seq=534/5634, ttl=128 (no response found!)
 1460 60.380942 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1461 60.394837 142.251.34.228   10.126.191.57   QUIC    1120 Protected Payload (KP0)
 1462 60.414992 10.126.191.57    10.126.191.45   ICMP      74 Echo (ping) request  id=0x0001, seq=535/5890, ttl=128 (no response found!)
 1463 60.426707 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1464 60.462423 10.126.191.57    10.126.191.46   ICMP      74 Echo (ping) request  id=0x0001, seq=536/6146, ttl=128 (no response found!)
 1465 60.469809 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1466 60.505112 10.126.191.57    10.126.191.47   ICMP      74 Echo (ping) request  id=0x0001, seq=537/6402, ttl=128 (no response found!)
 1467 60.511475 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1468 60.544066 142.250.191.110  10.126.191.57   QUIC    1123 Protected Payload (KP0)
 1469 60.546714 10.126.191.57    10.126.191.48   ICMP      74 Echo (ping) request  id=0x0001, seq=538/6658, ttl=128 (no response found!)
 1470 60.551010 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1471 60.592252 10.126.191.57    10.126.191.49   ICMP      74 Echo (ping) request  id=0x0001, seq=539/6914, ttl=128 (no response found!)
 1472 60.610079 10.128.128.128   10.126.191.57   ICMP     102 Destination unreachable (Communication administratively filtered)
 1473 60.645493 10.126.191.57    10.126.191.50   ICMP      74 Echo (ping) request  id=0x0001, seq=540/7170, ttl=128 (no response found!)
```

```
> Frame 1405: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{D8BCC5
> Ethernet II, Src: CiscoMeraki_57:ae:a5 (2c:3f:0b:57:ae:a5), Dst: CloudNetwork_01:f9:cb (2c:98:11:01:f9:c
> Internet Protocol Version 4, Src: 10.128.128.128, Dst: 10.126.191.57
> Internet Control Message Protocol

0000  2c 98 11 01 f9 cb 2c 3f  0b 57 ae a5 08 00 45 00   ,·····,? ·W····E·
0010  00 58 b5 55 00 00 c8 01  e8 97 0a 80 80 80 0a 7e   ·X·U···· ·······~
0020  bf 39 03 0d fc f2 00 00  00 00 45 00 00 3c 02 c0   ·9······ ··E··<··
0030  00 00 80 01 a4 b9 0a 7e  bf 39 0a 7e bf 12 08 00   ·······~ ·9·~····
0040  4b 60 00 01 01 fb 61 62  63 64 65 66 67 68 69 6a   K`····ab cdefghij
0050  6b 6c 6d 6e 6f 70 71 72  73 74 75 76 77 61 62 63   klmnopqr stuvwabc
0060  64 65 66 67 68 69                                  defghi

Wi-Fi: <live capture in progress>          Packets: 1554          Profile: Default
```

12:41 PM
12/5/2025

Sequential ICMP Echo Requests to multiple IP addresses (10.126.191.x), consistent with network scanning.

Screenshot 2: TCP SYN Scan


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Search
31°F
Mostly cloudy

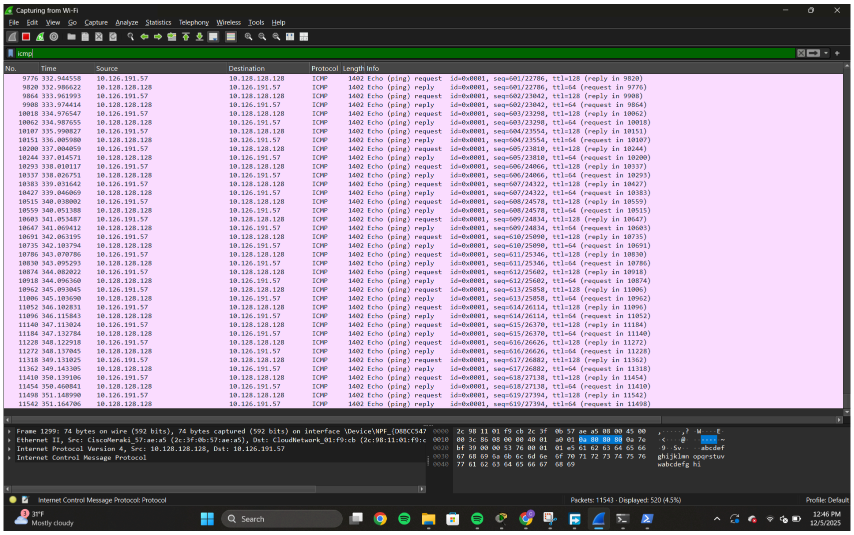
```
tcp.flags.syn == 1 and tcp.flags.ack == 0

No.   Time       Source          Destination      Protocol Length Info
 5745 209.110907 10.126.191.57   10.128.128.128   TCP      66 [TCP Port numbers reused] 50011 → 1 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 5747 209.444937 10.126.191.57   10.128.128.128   TCP      66 65101 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 5748 209.445175 10.126.191.57   10.128.128.128   TCP      66 60519 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 5809 209.645918 10.126.191.57   10.128.128.128   TCP      66 [TCP Port numbers reused] 50011 → 1 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 5819 211.041750 10.126.191.57   52.104.95.27     TCP      66 60520 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 5913 215.099525 10.126.191.57   40.90.130.207    TCP      66 60521 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 5934 215.333978 10.126.191.57   20.209.36.235    TCP      66 60522 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 6356 217.105504 10.126.191.57   13.107.139.11    TCP      66 60523 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 6377 217.274668 10.126.191.57   10.128.128.128   TCP      66 61753 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 6378 217.275292 10.126.191.57   10.128.128.128   TCP      66 60189 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 6414 217.420267 10.126.191.57   150.171.22.17    TCP      66 63681 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 6482 217.867980 10.126.191.57   20.190.135.6     TCP      66 63682 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 6483 217.878298 10.126.191.57   10.128.128.128   TCP      66 57932 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 6484 217.878534 10.126.191.57   10.128.128.128   TCP      66 62097 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 6588 219.705729 10.126.191.57   54.227.187.23    TCP      66 62098 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 6623 222.043680 10.126.191.57   142.251.185.94   TCP      66 51047 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 6739 233.195424 10.126.191.57   10.128.128.128   TCP      66 51048 → 2 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 6741 233.279056 10.126.191.57   10.128.128.128   TCP      66 60299 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 6742 233.279321 10.126.191.57   10.128.128.128   TCP      66 52762 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 6775 233.442437 10.126.191.57   13.107.137.11    TCP      66 52763 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7407 233.738294 10.126.191.57   10.128.128.128   TCP      66 [TCP Port numbers reused] 51048 → 2 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7414 234.251258 10.126.191.57   10.128.128.128   TCP      66 [TCP Port numbers reused] 51048 → 2 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7418 234.799783 10.126.191.57   10.128.128.128   TCP      66 [TCP Port numbers reused] 51048 → 2 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7421 235.335525 10.126.191.57   10.128.128.128   TCP      66 [TCP Port numbers reused] 51048 → 2 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7475 241.381104 10.126.191.57   23.32.45.39      TCP      66 52764 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7516 245.275534 10.126.191.57   10.128.128.128   TCP      66 51969 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7517 245.275752 10.126.191.57   10.128.128.128   TCP      66 57752 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7575 245.512952 10.126.191.57   10.128.128.128   TCP      66 57753 → 3 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7592 246.033106 10.126.191.57   10.128.128.128   TCP      66 [TCP Port numbers reused] 57753 → 3 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7599 246.546937 10.126.191.57   10.128.128.128   TCP      66 [TCP Port numbers reused] 57753 → 3 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7601 247.076436 10.126.191.57   10.128.128.128   TCP      66 [TCP Port numbers reused] 57753 → 3 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7605 247.605311 10.126.191.57   10.128.128.128   TCP      66 [TCP Port numbers reused] 57753 → 3 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7676 254.397255 10.126.191.57   142.250.191.110  TCP      66 62298 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7779 257.716420 10.126.191.57   10.128.128.128   TCP      66 62299 → 4 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7782 258.254451 10.126.191.57   10.128.128.128   TCP      66 [TCP Port numbers reused] 62299 → 4 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7787 258.774030 10.126.191.57   10.128.128.128   TCP      66 [TCP Port numbers reused] 62299 → 4 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7789 259.296045 10.126.191.57   10.128.128.128   TCP      66 [TCP Port numbers reused] 62299 → 4 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 7791 259.838646 10.126.191.57   10.128.128.128   TCP      66 [TCP Port numbers reused] 62299 → 4 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
```

```
> Frame 1301: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{D8BCC547
> Ethernet II, Src: CloudNetwork_01:f9:cb (2c:98:11:01:f9:cb), Dst: CiscoMeraki_57:ae:a5 (2c:3f:0b:57:ae:a
> Internet Protocol Version 4, Src: 10.126.191.57, Dst: 10.128.128.128
> Transmission Control Protocol, Src Port: 52349, Dst Port: 53, Seq: 0, Len: 0

0000  2c 3f 0b 57 ae a5 2c 98  11 01 f9 cb 08 00 45 00   ,?·W··,· ······E·
0010  00 34 5d 6c 40 00 80 06  48 a0 0a 7e bf 39 0a 80   ·4]l@··· H··~·9··
0020  80 80 cc 7d 00 35 92 ce  ca 6d 00 00 00 00 80 02   ···}·5·· ·m······
0030  ff ff f0 69 00 00 02 04  05 b4 01 03 03 08 01 01   ···i···· ········
0040  04 02                                              ··

wireshark_Wi-FiFW8CH3.pcapng          Packets: 7813 · Displayed: 96 (1.2%)          Profile: Default
```

12:44 PM
12/5/2025

Multiple SYN packets targeting different ports on the gateway, consistent with a port scan (used PowerShell Test-NetConnection loop).

Screenshot 3: DoS-like High-Rate ICMP



Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
icmp
No.   Time        Source           Destination      Protocol Length Info
 9776 332.944558  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=601/22786, ttl=128 (reply in 9820)
 9820 332.986622  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=601/22786, ttl=64 (request in 9776)
 9864 333.961993  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=602/23042, ttl=128 (reply in 9908)
 9908 333.974414  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=602/23042, ttl=64 (request in 9864)
10018 334.976547  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=603/23298, ttl=128 (reply in 10062)
10062 334.987655  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=603/23298, ttl=64 (request in 10018)
10107 335.990827  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=604/23554, ttl=128 (reply in 10151)
10151 336.005980  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=604/23554, ttl=64 (request in 10107)
10200 337.004059  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=605/23810, ttl=128 (reply in 10244)
10244 337.014571  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=605/23810, ttl=64 (request in 10200)
10293 338.010117  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=606/24066, ttl=128 (reply in 10337)
10337 338.026751  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=606/24066, ttl=64 (request in 10293)
10383 339.031642  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=607/24322, ttl=128 (reply in 10427)
10427 339.046069  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=607/24322, ttl=64 (request in 10383)
10515 340.038002  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=608/24578, ttl=128 (reply in 10559)
10559 340.051388  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=608/24578, ttl=64 (request in 10515)
10603 341.053487  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=609/24834, ttl=128 (reply in 10647)
10647 341.069412  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=609/24834, ttl=64 (request in 10603)
10691 342.063195  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=610/25090, ttl=128 (reply in 10735)
10735 342.103794  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=610/25090, ttl=64 (request in 10691)
10786 343.070786  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=611/25346, ttl=128 (reply in 10830)
10830 343.095293  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=611/25346, ttl=64 (request in 10786)
10874 344.082022  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=612/25602, ttl=128 (reply in 10918)
10918 344.096360  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=612/25602, ttl=64 (request in 10874)
10962 345.093045  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=613/25858, ttl=128 (reply in 11006)
11006 345.103690  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=613/25858, ttl=64 (request in 10962)
11052 346.102831  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=614/26114, ttl=128 (reply in 11096)
11096 346.115843  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=614/26114, ttl=64 (request in 11052)
11140 347.113024  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=615/26370, ttl=128 (reply in 11184)
11184 347.132784  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=615/26370, ttl=64 (request in 11140)
11228 348.122918  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=616/26626, ttl=128 (reply in 11272)
11272 348.137045  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=616/26626, ttl=64 (request in 11228)
11318 349.131025  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=617/26882, ttl=128 (reply in 11362)
11362 349.143305  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=617/26882, ttl=64 (request in 11318)
11410 350.139106  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=618/27138, ttl=128 (reply in 11454)
11454 350.460841  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=618/27138, ttl=64 (request in 11410)
11498 351.148990  10.126.191.57    10.128.128.128   ICMP     1402 Echo (ping) request  id=0x0001, seq=619/27394, ttl=128 (reply in 11542)
11542 351.164706  10.128.128.128   10.126.191.57    ICMP     1402 Echo (ping) reply    id=0x0001, seq=619/27394, ttl=64 (request in 11498)
```

```
Frame 1299: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D8BCC547
Ethernet II, Src: CiscoMeraki_57:ae:a5 (2c:3f:0b:57:ae:a5), Dst: CloudNetwork_01:f9:cb (2c:98:11:01:f9:c
Internet Protocol Version 4, Src: 10.128.128.128, Dst: 10.126.191.57
Internet Control Message Protocol
```

```
0000  2c 98 11 01 f9 cb 2c 3f  0b 57 ae a5 08 00 45 00   ,·····,? ·W····E·
0010  00 3c 86 08 00 00 40 01  a0 01 0a 80 80 80 0a 7e   ·<····@· ·······~
0020  bf 39 00 00 53 76 00 01  01 e5 61 62 63 64 65 66   ·9··Sv·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Internet Control Message Protocol: Protocol
Packets: 11543 · Displayed: 520 (4.5%)
Profile: Default
31°F
Mostly cloudy
Search
12:46 PM
12/5/2025

Large, repeated ICMP packets (`ping -t -l 65000`) representing high-volume ICMP flood behavior.

3. Alert Summary Table

Alert ID	Protocol	Source	Destination	Description	Severity	Status
1	ICMP	10.126.191.57	10.126.191.x	ICMP ping sweep detected (multiple sequential echo requests)	Low	True Positive
2	TCP	10.126.191.57	10.128.128.128	SYN packets targeting multiple ports → port scan	Medium	True Positive
3	ICMP	10.126.191.57	10.128.128.128	High-size, high-frequency ICMP packets (DoS-like pattern)	Medium	True Positive

Status = True Positive because all traffic was intentionally generated.

4. Technical Summary

During this lab, Wireshark was used to capture and analyze both normal and suspicious traffic on a Windows host. Normal traffic such as continuous ICMP pings was first captured to establish a baseline. Attack-like traffic was then simulated, including an ICMP ping sweep across a range of IPs, a TCP SYN scan across multiple ports, and a high-rate ICMP flood using large payloads. These activities were clearly visible in Wireshark using display filters such as `icmp` and `tcp.flags.syn == 1 and tcp.flags.ack == 0`. Each alert was identified as a true positive since the traffic was intentionally generated. The results demonstrate how network monitoring tools detect reconnaissance and potential DoS patterns in real time.