27/9 lab

Nmap XMAS scan and discover by wireshark

By : Hadeer Amr Fawzy

Xmas scan (-sX)

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

An XMAS scan is a type of network reconnaissance technique used to identify open ports on a target system

It gets its name from the way it sets multiple TCP flags, making the packet look like a Christmas tree when viewed in binary.

specific TCP flags:

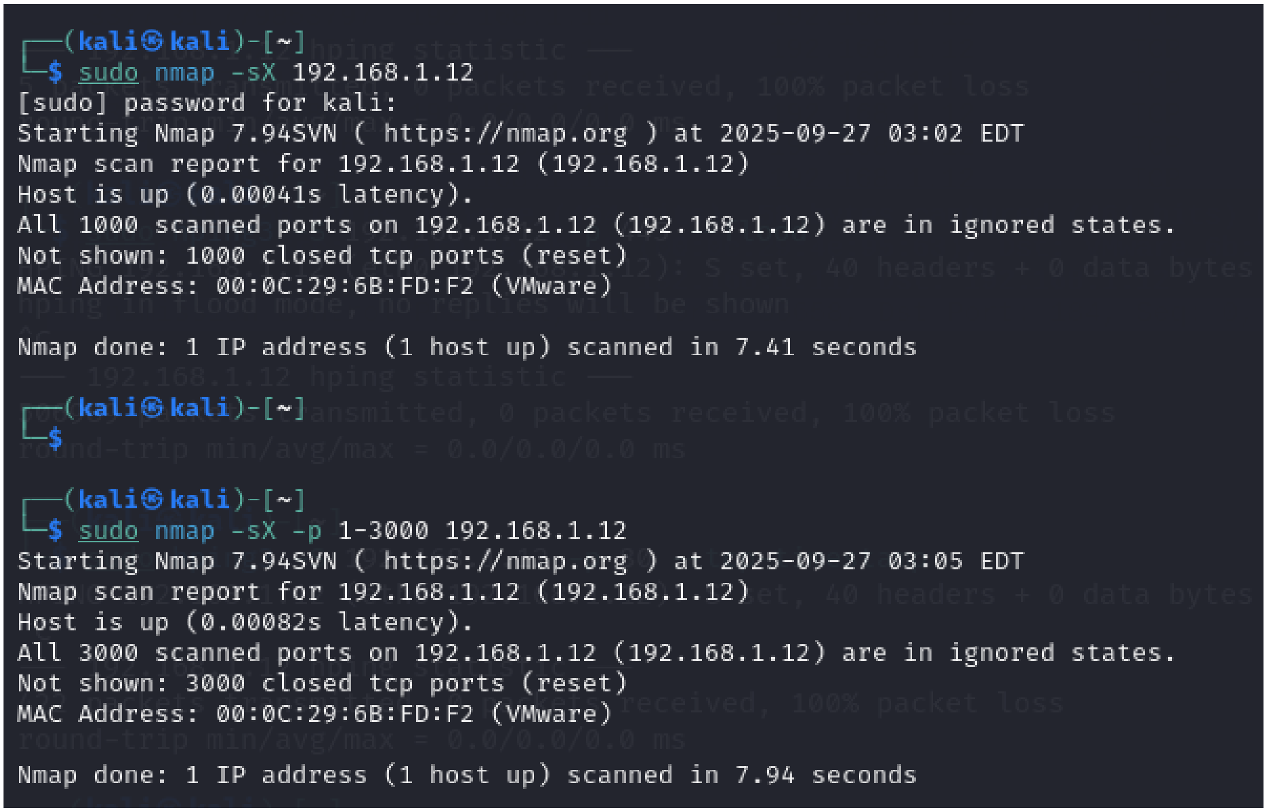
FIN (0x01): Indicates end of data transmission

PSH (0x08): Pushes data to application

URG (0x20): Marks urgent data

Nmap commands I used :

sudo nmap -sX 192.168.1.12
sudo nmap -sX -p 1-3000 192.168.1.12



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sX 192.168.1.12
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-27 03:02 EDT
Nmap scan report for 192.168.1.12 (192.168.1.12)
Host is up (0.00041s latency).
All 1000 scanned ports on 192.168.1.12 (192.168.1.12) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:6B:FD:F2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 7.41 seconds

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sX -p 1-3000 192.168.1.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-27 03:05 EDT
Nmap scan report for 192.168.1.12 (192.168.1.12)
Host is up (0.00082s latency).
All 3000 scanned ports on 192.168.1.12 (192.168.1.12) are in ignored states.
Not shown: 3000 closed tcp ports (reset)
MAC Address: 00:0C:29:6B:FD:F2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 7.94 seconds
```

Wireshark searching queries I used :

tcp.flags == 0x29

This filter uses hexadecimal 0x29 to represent the combination of FIN (0x01), PUSH (0x08), and URGENT (0x20) flags

the value 0x29 is the sum of these individual flag values (0x01 + 0x08 + 0x20 = 0x29).

basic XMAS Scan Detection use when to quickly identify XMAS scan attempts ideal for automated scripts or quick analysis and most efficient for high-volume packet capture

tcp.flags.fin == 1 && tcp.flags.psh == 1 && tcp.flags.urg == 1

This filter explicitly checks each TCP flag individually

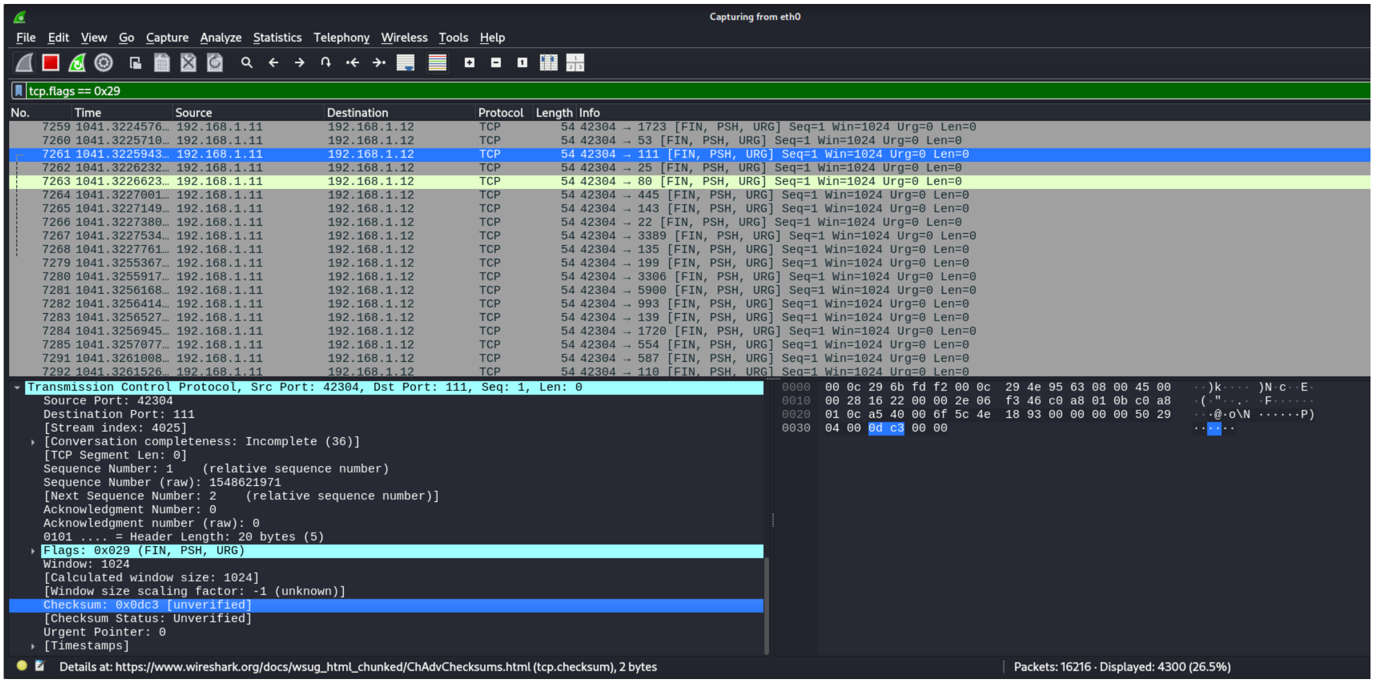
It's more verbose but clearly shows that we're looking for packets where
FIN flag is set (1) and PUSH flag is set (1) and URGENT flag is set (1)

makes it clear what flags are being checked and easier to modify individual conditions

(tcp.flags.fin == 1 && tcp.flags.psh == 1 && tcp.flags.urg == 1) || tcp.flags.reset == 1

This filter combines XMAS scan detection with reset packet detection the parentheses ensure proper logical grouping, and the OR operator (||) allows matching either condition. This is useful for detecting both types of suspicious network activity and helpful for comprehensive security monitoring and good for capturing both XMAS scans and connection resets

https://www.hackingarticles.in/nmap-scans-using-hex-value-flags/


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags == 0x29
```

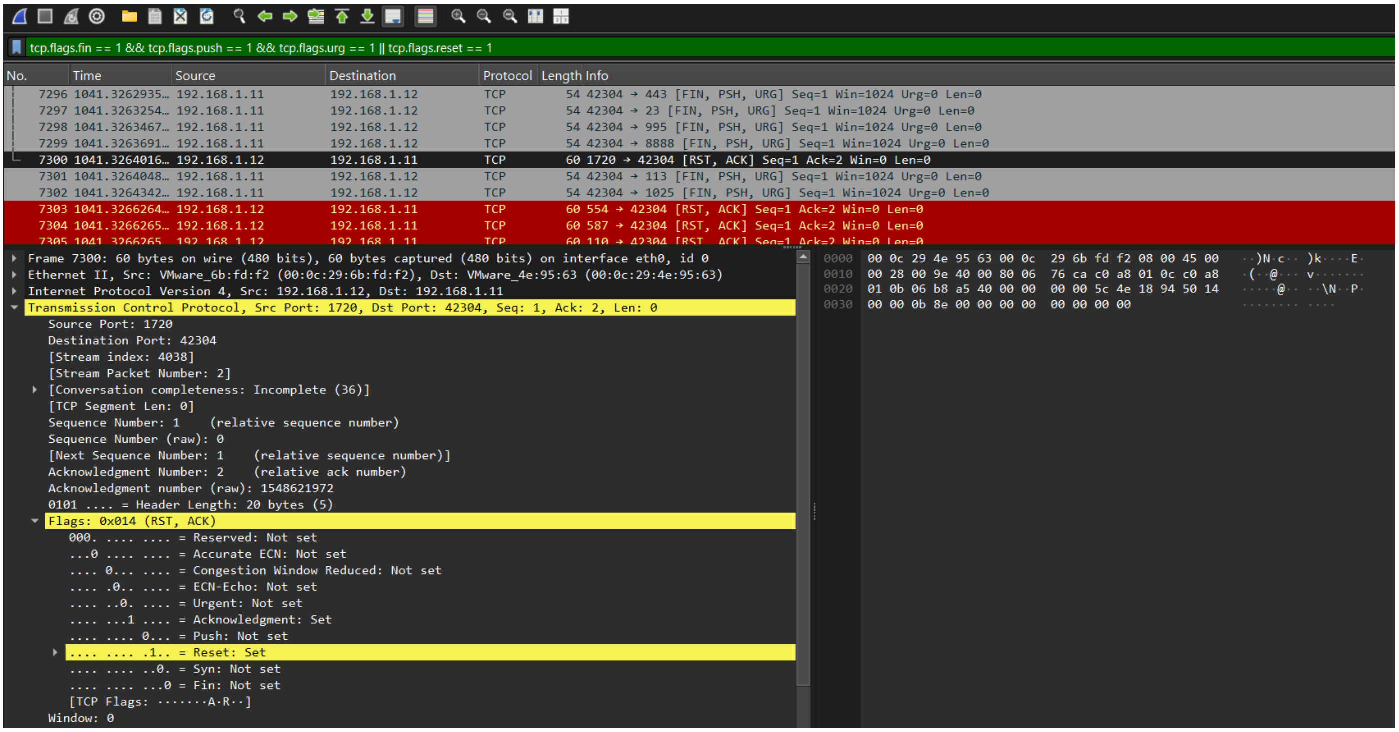
```
No.  Time            Source         Destination    Protocol Length Info
7259 1041.3224576… 192.168.1.11   192.168.1.12   TCP      54 42304 → 1723 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7260 1041.3225710… 192.168.1.11   192.168.1.12   TCP      54 42304 → 53 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7261 1041.3225943… 192.168.1.11   192.168.1.12   TCP      54 42304 → 111 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7262 1041.3226232… 192.168.1.11   192.168.1.12   TCP      54 42304 → 25 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7263 1041.3226623… 192.168.1.11   192.168.1.12   TCP      54 42304 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7264 1041.3227001… 192.168.1.11   192.168.1.12   TCP      54 42304 → 445 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7265 1041.3227149… 192.168.1.11   192.168.1.12   TCP      54 42304 → 143 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7266 1041.3227380… 192.168.1.11   192.168.1.12   TCP      54 42304 → 22 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7267 1041.3227534… 192.168.1.11   192.168.1.12   TCP      54 42304 → 3389 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7268 1041.3227761… 192.168.1.11   192.168.1.12   TCP      54 42304 → 135 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7279 1041.3255367… 192.168.1.11   192.168.1.12   TCP      54 42304 → 199 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7280 1041.3255917… 192.168.1.11   192.168.1.12   TCP      54 42304 → 3306 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7281 1041.3256168… 192.168.1.11   192.168.1.12   TCP      54 42304 → 5900 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7282 1041.3256414… 192.168.1.11   192.168.1.12   TCP      54 42304 → 993 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7283 1041.3256527… 192.168.1.11   192.168.1.12   TCP      54 42304 → 139 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7284 1041.3256945… 192.168.1.11   192.168.1.12   TCP      54 42304 → 1720 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7285 1041.3257077… 192.168.1.11   192.168.1.12   TCP      54 42304 → 554 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7291 1041.3261008… 192.168.1.11   192.168.1.12   TCP      54 42304 → 587 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7292 1041.3261526… 192.168.1.11   192.168.1.12   TCP      54 42304 → 110 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
```

```
▾ Transmission Control Protocol, Src Port: 42304, Dst Port: 111, Seq: 1, Len: 0
    Source Port: 42304
    Destination Port: 111
    [Stream index: 4025]
  ▸ [Conversation completeness: Incomplete (36)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1548621971
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x029 (FIN, PSH, URG)
    Window: 1024
    [Calculated window size: 1024]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x0dc3 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ [Timestamps]
```

```
0000  00 0c 29 6b fd f2 00 0c  29 4e 95 63 08 00 45 00   ··)k····)N·c··E·
0010  00 28 16 22 00 00 2e 06  f3 46 c0 a8 01 0b c0 a8   ·(·"··.··F······
0020  01 0c a5 40 00 6f 5c 4e  18 93 00 00 00 00 50 29   ···@·o\N······P)
0030  04 00 0d c3 00 00                                  ······
```

Details at: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (tcp.checksum), 2 bytes

Packets: 16216 · Displayed: 4300 (26.5%)

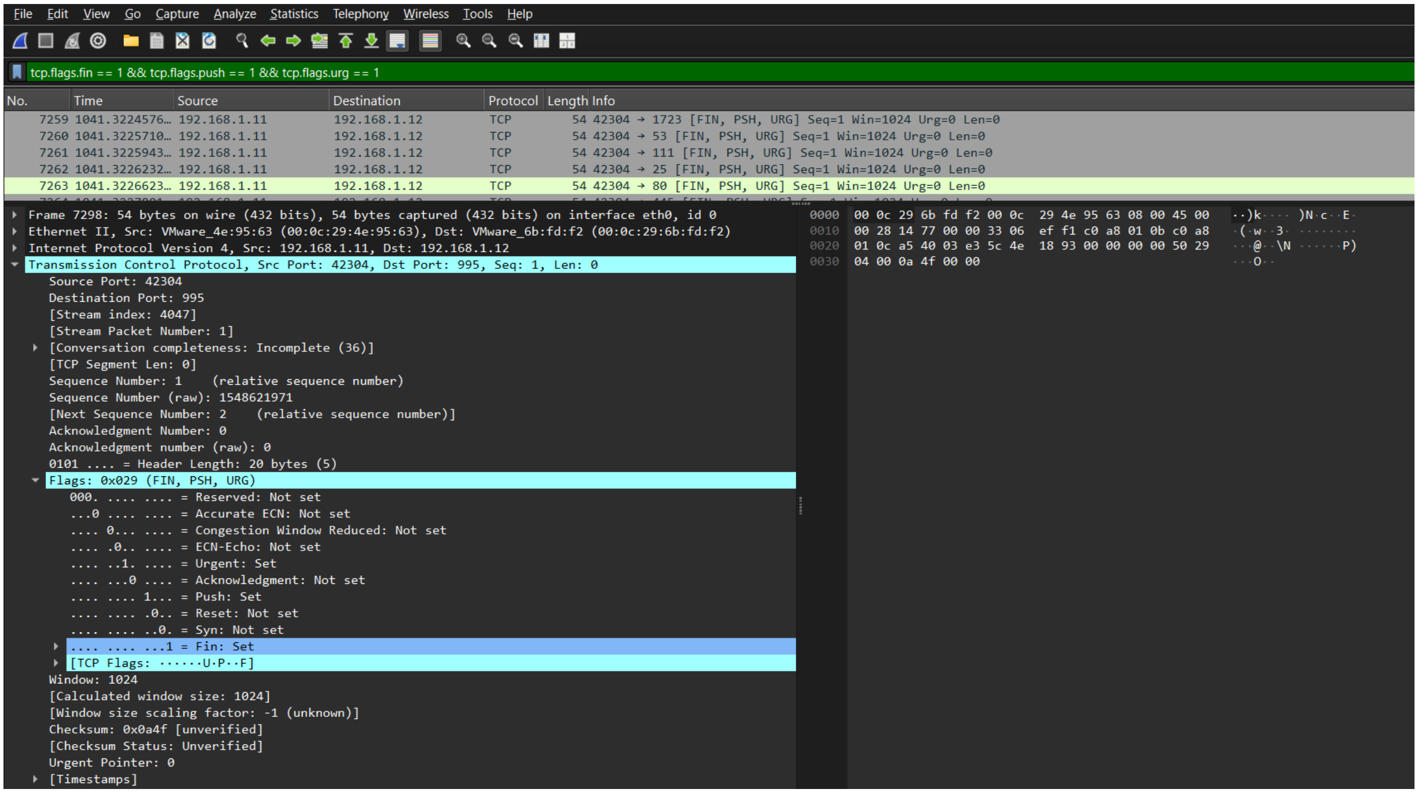


```
tcp.flags.fin == 1 && tcp.flags.push == 1 && tcp.flags.urg == 1 || tcp.flags.reset == 1

No.  Time              Source        Destination   Protocol Length Info
7296 1041.3262935…     192.168.1.11  192.168.1.12  TCP      54 42304 → 443 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7297 1041.3263254…     192.168.1.11  192.168.1.12  TCP      54 42304 → 23 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7298 1041.3263467…     192.168.1.11  192.168.1.12  TCP      54 42304 → 995 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7299 1041.3263691…     192.168.1.11  192.168.1.12  TCP      54 42304 → 8888 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7300 1041.3264016…     192.168.1.12  192.168.1.11  TCP      60 1720 → 42304 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
7301 1041.3264048…     192.168.1.11  192.168.1.12  TCP      54 42304 → 113 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7302 1041.3264342…     192.168.1.11  192.168.1.12  TCP      54 42304 → 1025 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7303 1041.3266264…     192.168.1.12  192.168.1.11  TCP      60 554 → 42304 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
7304 1041.3266265…     192.168.1.12  192.168.1.11  TCP      60 587 → 42304 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
7305 1041.3266265      192.168.1.12  192.168.1.11  TCP      60 110 → 42304 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

Frame 7300: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: VMware_6b:fd:f2 (00:0c:29:6b:fd:f2), Dst: VMware_4e:95:63 (00:0c:29:4e:95:63)
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 192.168.1.11
Transmission Control Protocol, Src Port: 1720, Dst Port: 42304, Seq: 1, Ack: 2, Len: 0
   Source Port: 1720
   Destination Port: 42304
   [Stream index: 4038]
   [Stream Packet Number: 2]
   [Conversation completeness: Incomplete (36)]
   [TCP Segment Len: 0]
   Sequence Number: 1    (relative sequence number)
   Sequence Number (raw): 0
   [Next Sequence Number: 1    (relative sequence number)]
   Acknowledgment Number: 2    (relative ack number)
   Acknowledgment number (raw): 1548621972
   0101 .... = Header Length: 20 bytes (5)
   Flags: 0x014 (RST, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .1.. = Reset: Set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A·R··]
   Window: 0

0000  00 0c 29 4e 95 63 00 0c  29 6b fd f2 08 00 45 00   ··)N·c·· )k····E·
0010  00 28 00 9e 40 00 80 06  76 ca c0 a8 01 0c c0 a8   ·(··@··· v·······
0020  01 0b 06 b8 a5 40 00 00  00 00 5c 4e 18 94 50 14   ·····@·· ··\N··P·
0030  00 00 0b 8e 00 00 00 00  00 00 00 00               ········ ····
```



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags.fin == 1 && tcp.flags.push == 1 && tcp.flags.urg == 1

No.  Time              Source        Destination   Protocol Length Info
7259 1041.3224576…     192.168.1.11  192.168.1.12  TCP      54 42304 → 1723 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7260 1041.3225710…     192.168.1.11  192.168.1.12  TCP      54 42304 → 53 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7261 1041.3225943…     192.168.1.11  192.168.1.12  TCP      54 42304 → 111 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7262 1041.3226232…     192.168.1.11  192.168.1.12  TCP      54 42304 → 25 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7263 1041.3226623…     192.168.1.11  192.168.1.12  TCP      54 42304 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

Frame 7298: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: VMware_4e:95:63 (00:0c:29:4e:95:63), Dst: VMware_6b:fd:f2 (00:0c:29:6b:fd:f2)
Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.12
Transmission Control Protocol, Src Port: 42304, Dst Port: 995, Seq: 1, Len: 0
   Source Port: 42304
   Destination Port: 995
   [Stream index: 4047]
   [Stream Packet Number: 1]
   [Conversation completeness: Incomplete (36)]
   [TCP Segment Len: 0]
   Sequence Number: 1    (relative sequence number)
   Sequence Number (raw): 1548621971
   [Next Sequence Number: 2    (relative sequence number)]
   Acknowledgment Number: 0
   Acknowledgment number (raw): 0
   0101 .... = Header Length: 20 bytes (5)
   Flags: 0x029 (FIN, PSH, URG)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..1. .... = Urgent: Set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 1... = Push: Set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...1 = Fin: Set
      [TCP Flags: ······U·P··F]
   Window: 1024
   [Calculated window size: 1024]
   [Window size scaling factor: -1 (unknown)]
   Checksum: 0x0a4f [unverified]
   [Checksum Status: Unverified]
   Urgent Pointer: 0
   [Timestamps]

0000  00 0c 29 6b fd f2 00 0c  29 4e 95 63 08 00 45 00   ··)k···· )N·c··E·
0010  00 28 14 77 00 00 33 06  ef f1 c0 a8 01 0b c0 a8   ·(·w··3· ········
0020  01 0c a5 40 03 e3 5c 4e  18 93 00 00 00 00 50 29   ···@··\N ······P)
0030  04 00 0a 4f 00 00                                  ···O··
```