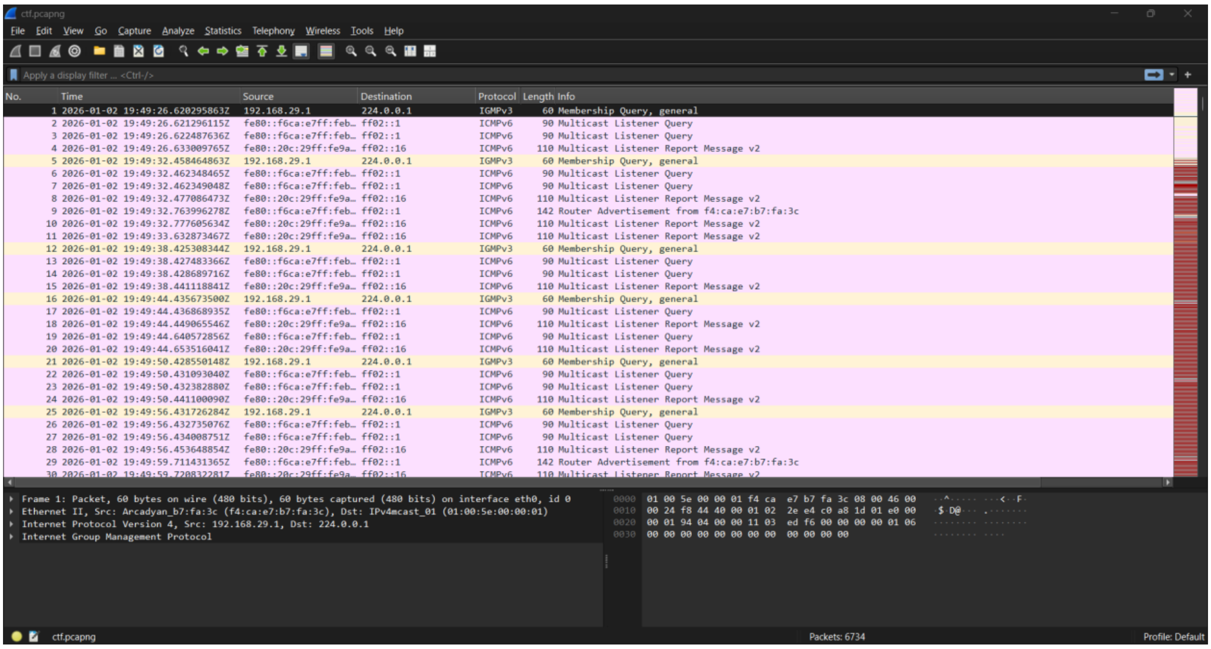
Minor 2 Project

Project 2: Network Traffic Analysis & Incident Investigation Using PCAP (SOC

Analyst Simulation)

You are working as a Junior SOC Analyst in a security operations team. One of the internal systems in your organisation is suspected to be compromised. The SOC team has captured network traffic (PCAP file) during the incident window and handed it over to you for investigation. Your task is to analyse the PCAP file using Wireshark, just like a real SOC analyst, and determine: Who is the attacker Which system is the victim What suspicious activity occurred How sensitive data (a ZIP file) was transferred Extract the ZIP file and retrieve the flag

1.Open the PCAP file in Wireshark



ctf.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

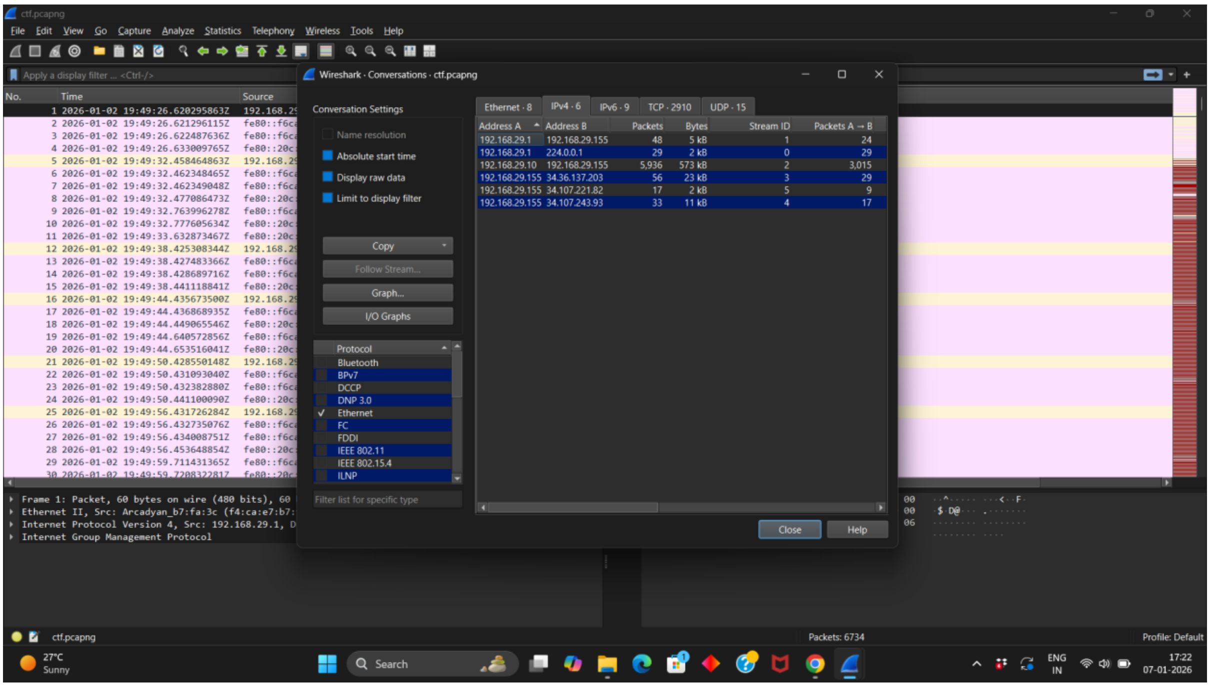
```
No.  Time                            Source                 Destination  Protocol Length Info
   1 2026-01-02 19:49:26.620295863Z  192.168.29.1           224.0.0.1    IGMPv3    60 Membership Query, general
   2 2026-01-02 19:49:26.621296115Z  fe80::f6ca:e7ff:feb…   ff02::1      ICMPv6    90 Multicast Listener Query
   3 2026-01-02 19:49:26.622487636Z  fe80::f6ca:e7ff:feb…   ff02::1      ICMPv6    90 Multicast Listener Query
   4 2026-01-02 19:49:26.633009765Z  fe80::20c:29ff:fe9a…   ff02::16     ICMPv6   110 Multicast Listener Report Message v2
   5 2026-01-02 19:49:32.458464863Z  192.168.29.1           224.0.0.1    IGMPv3    60 Membership Query, general
   6 2026-01-02 19:49:32.462348465Z  fe80::f6ca:e7ff:feb…   ff02::1      ICMPv6    90 Multicast Listener Query
   7 2026-01-02 19:49:32.462349048Z  fe80::f6ca:e7ff:feb…   ff02::1      ICMPv6    90 Multicast Listener Query
   8 2026-01-02 19:49:32.477086473Z  fe80::20c:29ff:fe9a…   ff02::16     ICMPv6   110 Multicast Listener Report Message v2
   9 2026-01-02 19:49:32.763996278Z  fe80::f6ca:e7ff:feb…   ff02::1      ICMPv6   142 Router Advertisement from f4:ca:e7:b7:fa:3c
  10 2026-01-02 19:49:32.777605634Z  fe80::20c:29ff:fe9a…   ff02::16     ICMPv6   110 Multicast Listener Report Message v2
  11 2026-01-02 19:49:33.632873467Z  fe80::20c:29ff:fe9a…   ff02::16     ICMPv6   110 Multicast Listener Report Message v2
  12 2026-01-02 19:49:38.425308344Z  192.168.29.1           224.0.0.1    IGMPv3    60 Membership Query, general
  13 2026-01-02 19:49:38.427483366Z  fe80::f6ca:e7ff:feb…   ff02::1      ICMPv6    90 Multicast Listener Query
  14 2026-01-02 19:49:38.428689716Z  fe80::f6ca:e7ff:feb…   ff02::1      ICMPv6    90 Multicast Listener Query
  15 2026-01-02 19:49:38.441118841Z  fe80::20c:29ff:fe9a…   ff02::16     ICMPv6   110 Multicast Listener Report Message v2
  16 2026-01-02 19:49:44.435673500Z  192.168.29.1           224.0.0.1    IGMPv3    60 Membership Query, general
  17 2026-01-02 19:49:44.436868935Z  fe80::f6ca:e7ff:feb…   ff02::1      ICMPv6    90 Multicast Listener Query
  18 2026-01-02 19:49:44.449065546Z  fe80::20c:29ff:fe9a…   ff02::16     ICMPv6   110 Multicast Listener Report Message v2
  19 2026-01-02 19:49:44.640572856Z  fe80::f6ca:e7ff:feb…   ff02::1      ICMPv6    90 Multicast Listener Query
  20 2026-01-02 19:49:44.653516041Z  fe80::20c:29ff:fe9a…   ff02::16     ICMPv6   110 Multicast Listener Report Message v2
  21 2026-01-02 19:49:50.428550148Z  192.168.29.1           224.0.0.1    IGMPv3    60 Membership Query, general
  22 2026-01-02 19:49:50.431093040Z  fe80::f6ca:e7ff:feb…   ff02::1      ICMPv6    90 Multicast Listener Query
  23 2026-01-02 19:49:50.432382880Z  fe80::f6ca:e7ff:feb…   ff02::1      ICMPv6    90 Multicast Listener Query
  24 2026-01-02 19:49:50.441100090Z  fe80::20c:29ff:fe9a…   ff02::16     ICMPv6   110 Multicast Listener Report Message v2
  25 2026-01-02 19:49:56.431726284Z  192.168.29.1           224.0.0.1    IGMPv3    60 Membership Query, general
  26 2026-01-02 19:49:56.432735076Z  fe80::f6ca:e7ff:feb…   ff02::1      ICMPv6    90 Multicast Listener Query
  27 2026-01-02 19:49:56.434008751Z  fe80::f6ca:e7ff:feb…   ff02::1      ICMPv6    90 Multicast Listener Query
  28 2026-01-02 19:49:56.453648854Z  fe80::20c:29ff:fe9a…   ff02::16     ICMPv6   110 Multicast Listener Report Message v2
  29 2026-01-02 19:49:59.711431365Z  fe80::f6ca:e7ff:feb…   ff02::1      ICMPv6   142 Router Advertisement from f4:ca:e7:b7:fa:3c
  30 2026-01-02 19:49:59.720832281Z  fe80::20c:29ff:fe9a…   ff02::16     ICMPv6   110 Multicast Listener Report Message v2
```

```
▸ Frame 1: Packet, 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▸ Ethernet II, Src: Arcadyan_b7:fa:3c (f4:ca:e7:b7:fa:3c), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
▸ Internet Protocol Version 4, Src: 192.168.29.1, Dst: 224.0.0.1
▸ Internet Group Management Protocol
```

```
0000  01 00 5e 00 00 01 f4 ca  e7 b7 fa 3c 08 00 46 00   ··^·····  ···<··F·
0010  00 24 f8 44 40 00 01 02  2e e4 c0 a8 1d 01 e0 00   ·$·D@···  .·······
0020  00 01 94 04 00 00 11 03  ed f6 00 00 00 00 01 06   ········  ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········  ····
```

2. Analyse network traffic patterns

Conversation → IPv4



ctf.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Conversations · ctf.pcapng
Copy
Follow Stream...
Graph...
I/O Graphs
Filter list for specific type
Close
Help
Packets: 6734
Profile: Default

Conversation Settings

□ Name resolution
☑ Absolute start time
☑ Display raw data
☑ Limit to display filter

	Protocol
□	Bluetooth
□	BPv7
□	DCCP
□	DNP 3.0
✓	Ethernet
□	FC
□	FDDI
□	IEEE 802.11
□	IEEE 802.15.4
□	ILNP

Ethernet · 8 | IPv4 · 6 | IPv6 · 9 | TCP · 2910 | UDP · 15

Address A	Address B	Packets	Bytes	Stream ID	Packets A → B
192.168.29.1	192.168.29.155	48	5 kB	1	24
192.168.29.1	224.0.0.1	29	2 kB	0	29
192.168.29.10	192.168.29.155	5,936	573 kB	2	3,015
192.168.29.155	34.36.137.203	56	23 kB	3	29
192.168.29.155	34.107.221.82	17	2 kB	5	9
192.168.29.155	34.107.243.93	33	11 kB	4	17

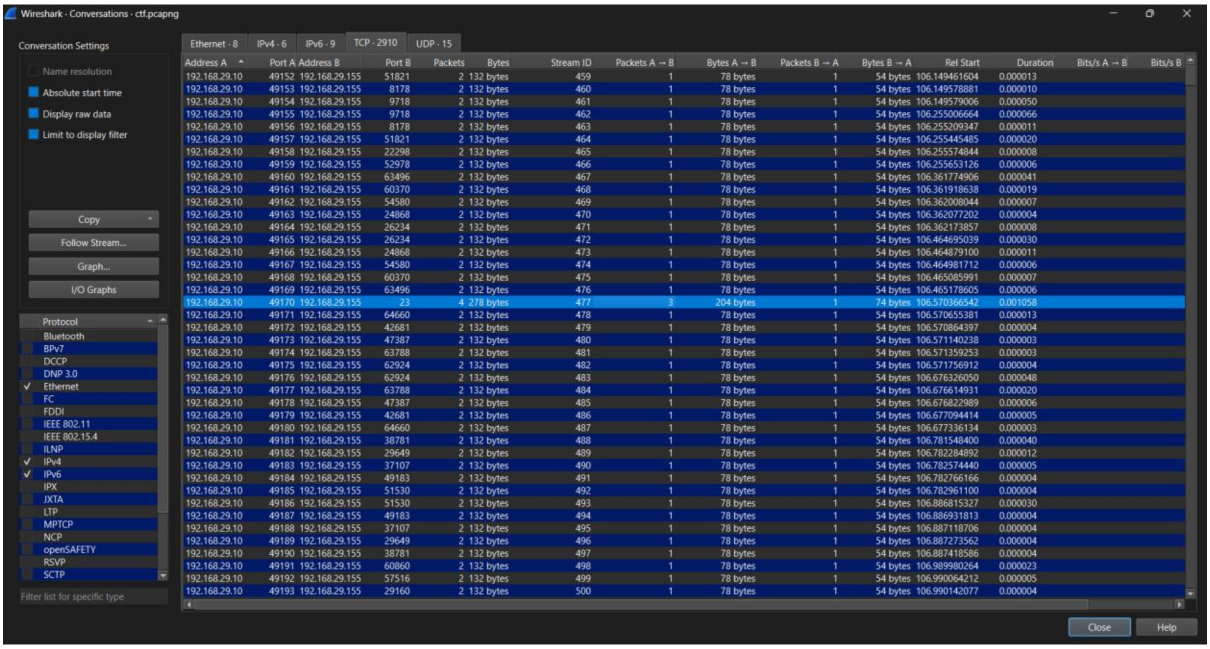
```
No.     Time                             Source
      1 2026-01-02 19:49:26.620295863Z   192.168.29
      2 2026-01-02 19:49:26.621296115Z   fe80::f6ca
      3 2026-01-02 19:49:26.622487636Z   fe80::f6ca
      4 2026-01-02 19:49:26.633009765Z   fe80::20c:
      5 2026-01-02 19:49:32.458464863Z   192.168.29
      6 2026-01-02 19:49:32.462348465Z   fe80::f6ca
      7 2026-01-02 19:49:32.462349048Z   fe80::f6ca
      8 2026-01-02 19:49:32.477086473Z   fe80::20c:
      9 2026-01-02 19:49:32.763996278Z   fe80::f6ca
     10 2026-01-02 19:49:32.777605634Z   fe80::20c:
     11 2026-01-02 19:49:33.632873467Z   fe80::20c:
     12 2026-01-02 19:49:38.425308344Z   192.168.29
     13 2026-01-02 19:49:38.427483366Z   fe80::f6ca
     14 2026-01-02 19:49:38.428689716Z   fe80::f6ca
     15 2026-01-02 19:49:38.441118841Z   fe80::20c:
     16 2026-01-02 19:49:44.435673500Z   192.168.29
     17 2026-01-02 19:49:44.436868935Z   fe80::f6ca
     18 2026-01-02 19:49:44.449065546Z   fe80::20c:
     19 2026-01-02 19:49:44.640572856Z   fe80::f6ca
     20 2026-01-02 19:49:44.653516041Z   fe80::20c:
     21 2026-01-02 19:49:50.428550148Z   192.168.29
     22 2026-01-02 19:49:50.431093040Z   fe80::f6ca
     23 2026-01-02 19:49:50.432382880Z   fe80::f6ca
     24 2026-01-02 19:49:50.441100090Z   fe80::20c:
     25 2026-01-02 19:49:56.431726284Z   192.168.29
     26 2026-01-02 19:49:56.432735076Z   fe80::f6ca
     27 2026-01-02 19:49:56.434008751Z   fe80::f6ca
     28 2026-01-02 19:49:56.453648854Z   fe80::20c:
     29 2026-01-02 19:49:59.711431365Z   fe80::f6ca
     30 2026-01-02 19:49:59.720832281Z   fe80::20c:
```

```
› Frame 1: Packet, 60 bytes on wire (480 bits), 60
› Ethernet II, Src: Arcadyan_b7:fa:3c (f4:ca:e7:b7:
› Internet Protocol Version 4, Src: 192.168.29.1, D
› Internet Group Management Protocol
```

3. Identify the attacker and victim

Conversation → TCP

- Victim → 192.168.29.155
- Attacker → 192.168.29.10



Wireshark · Conversations · ctf.pcapng

Conversation Settings

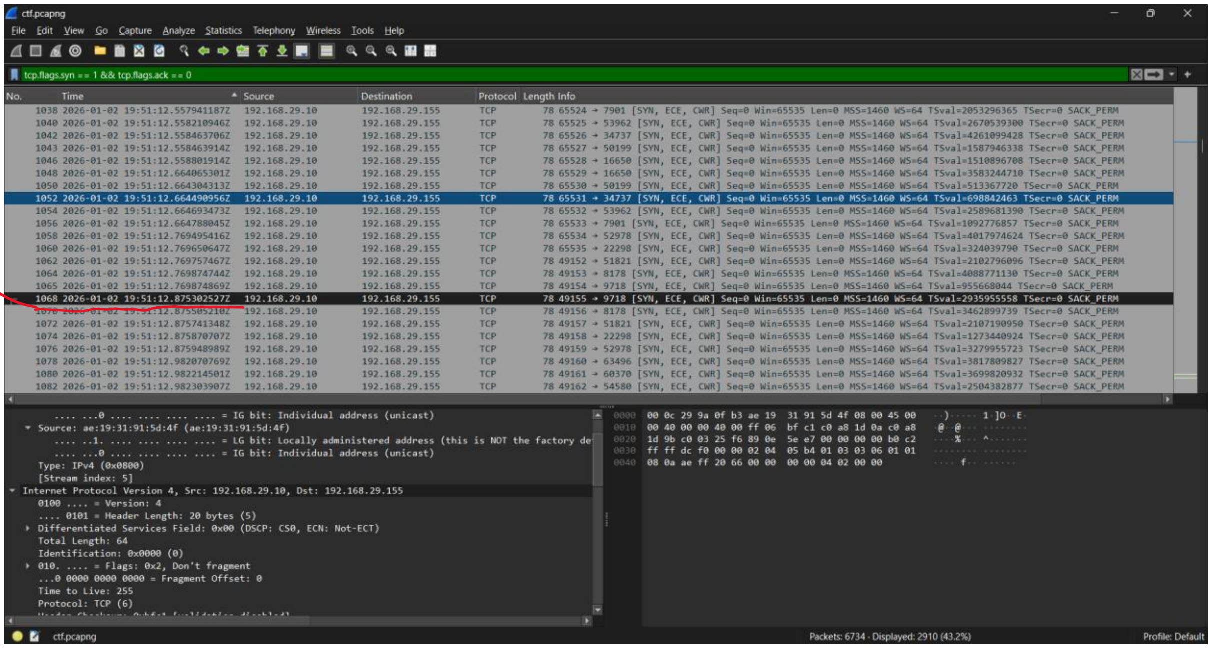
☐ Name resolution
☑ Absolute start time
☑ Display raw data
☑ Limit to display filter

Protocol
☐ Bluetooth
☐ BPv7
☐ DCCP
☐ DNP 3.0
☑ Ethernet
☐ FC
☐ FDDI
☐ IEEE 802.11
☐ IEEE 802.15.4
☐ ILNP
☑ IPv4
☑ IPv6
☐ IPX
☐ JXTA
☐ LTP
☐ MPTCP
☐ NCP
☐ openSAFETY
☐ RSVP
☐ SCTP

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B
192.168.29.10	49152	192.168.29.155	51821	2	132 bytes	459	1	78 bytes	1	54 bytes	106.149461604	0.000013		
192.168.29.10	49153	192.168.29.155	8178	2	132 bytes	460	1	78 bytes	1	54 bytes	106.149578881	0.000010		
192.168.29.10	49154	192.168.29.155	9718	2	132 bytes	461	1	78 bytes	1	54 bytes	106.149579006	0.000050		
192.168.29.10	49155	192.168.29.155	9718	2	132 bytes	462	1	78 bytes	1	54 bytes	106.255006664	0.000066		
192.168.29.10	49156	192.168.29.155	8178	2	132 bytes	463	1	78 bytes	1	54 bytes	106.255209347	0.000011		
192.168.29.10	49157	192.168.29.155	51821	2	132 bytes	464	1	78 bytes	1	54 bytes	106.255445485	0.000020		
192.168.29.10	49158	192.168.29.155	22298	2	132 bytes	465	1	78 bytes	1	54 bytes	106.255574844	0.000008		
192.168.29.10	49159	192.168.29.155	52978	2	132 bytes	466	1	78 bytes	1	54 bytes	106.255653126	0.000006		
192.168.29.10	49160	192.168.29.155	63496	2	132 bytes	467	1	78 bytes	1	54 bytes	106.361774906	0.000041		
192.168.29.10	49161	192.168.29.155	60370	2	132 bytes	468	1	78 bytes	1	54 bytes	106.361918638	0.000019		
192.168.29.10	49162	192.168.29.155	54580	2	132 bytes	469	1	78 bytes	1	54 bytes	106.362008044	0.000007		
192.168.29.10	49163	192.168.29.155	24868	2	132 bytes	470	1	78 bytes	1	54 bytes	106.362077202	0.000004		
192.168.29.10	49164	192.168.29.155	26234	2	132 bytes	471	1	78 bytes	1	54 bytes	106.362173857	0.000008		
192.168.29.10	49165	192.168.29.155	26234	2	132 bytes	472	1	78 bytes	1	54 bytes	106.464695039	0.000030		
192.168.29.10	49166	192.168.29.155	24868	2	132 bytes	473	1	78 bytes	1	54 bytes	106.464879100	0.000011		
192.168.29.10	49167	192.168.29.155	54580	2	132 bytes	474	1	78 bytes	1	54 bytes	106.464981712	0.000006		
192.168.29.10	49168	192.168.29.155	60370	2	132 bytes	475	1	78 bytes	1	54 bytes	106.465085991	0.000007		
192.168.29.10	49169	192.168.29.155	63496	2	132 bytes	476	1	78 bytes	1	54 bytes	106.465178605	0.000006		
192.168.29.10	49170	192.168.29.155	23	4	278 bytes	477	3	204 bytes	1	74 bytes	106.570366542	0.001058		
192.168.29.10	49171	192.168.29.155	64660	2	132 bytes	478	1	78 bytes	1	54 bytes	106.570655381	0.000013		
192.168.29.10	49172	192.168.29.155	42681	2	132 bytes	479	1	78 bytes	1	54 bytes	106.570864397	0.000004		
192.168.29.10	49173	192.168.29.155	47387	2	132 bytes	480	1	78 bytes	1	54 bytes	106.571140238	0.000003		
192.168.29.10	49174	192.168.29.155	63788	2	132 bytes	481	1	78 bytes	1	54 bytes	106.571359253	0.000003		
192.168.29.10	49175	192.168.29.155	62924	2	132 bytes	482	1	78 bytes	1	54 bytes	106.571756912	0.000004		
192.168.29.10	49176	192.168.29.155	62924	2	132 bytes	483	1	78 bytes	1	54 bytes	106.676326050	0.000048		
192.168.29.10	49177	192.168.29.155	63788	2	132 bytes	484	1	78 bytes	1	54 bytes	106.676614931	0.000020		
192.168.29.10	49178	192.168.29.155	47387	2	132 bytes	485	1	78 bytes	1	54 bytes	106.676822989	0.000006		
192.168.29.10	49179	192.168.29.155	42681	2	132 bytes	486	1	78 bytes	1	54 bytes	106.677094414	0.000005		
192.168.29.10	49180	192.168.29.155	64660	2	132 bytes	487	1	78 bytes	1	54 bytes	106.677336134	0.000003		
192.168.29.10	49181	192.168.29.155	38781	2	132 bytes	488	1	78 bytes	1	54 bytes	106.781548400	0.000040		
192.168.29.10	49182	192.168.29.155	29649	2	132 bytes	489	1	78 bytes	1	54 bytes	106.782284892	0.000012		
192.168.29.10	49183	192.168.29.155	37107	2	132 bytes	490	1	78 bytes	1	54 bytes	106.782574440	0.000005		
192.168.29.10	49184	192.168.29.155	49183	2	132 bytes	491	1	78 bytes	1	54 bytes	106.782766166	0.000004		
192.168.29.10	49185	192.168.29.155	51530	2	132 bytes	492	1	78 bytes	1	54 bytes	106.782961100	0.000004		
192.168.29.10	49186	192.168.29.155	51530	2	132 bytes	493	1	78 bytes	1	54 bytes	106.886815327	0.000030		
192.168.29.10	49187	192.168.29.155	49183	2	132 bytes	494	1	78 bytes	1	54 bytes	106.886931813	0.000004		
192.168.29.10	49188	192.168.29.155	37107	2	132 bytes	495	1	78 bytes	1	54 bytes	106.887118706	0.000004		
192.168.29.10	49189	192.168.29.155	29649	2	132 bytes	496	1	78 bytes	1	54 bytes	106.887273562	0.000004		
192.168.29.10	49190	192.168.29.155	38781	2	132 bytes	497	1	78 bytes	1	54 bytes	106.887418586	0.000004		
192.168.29.10	49191	192.168.29.155	60860	2	132 bytes	498	1	78 bytes	1	54 bytes	106.989980264	0.000023		
192.168.29.10	49192	192.168.29.155	57516	2	132 bytes	499	1	78 bytes	1	54 bytes	106.990064212	0.000005		
192.168.29.10	49193	192.168.29.155	29160	2	132 bytes	500	1	78 bytes	1	54 bytes	106.990142077	0.000004		

4.Determine when the attack started

5.Identify reconnaissance activity (port scanning)


ctf.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

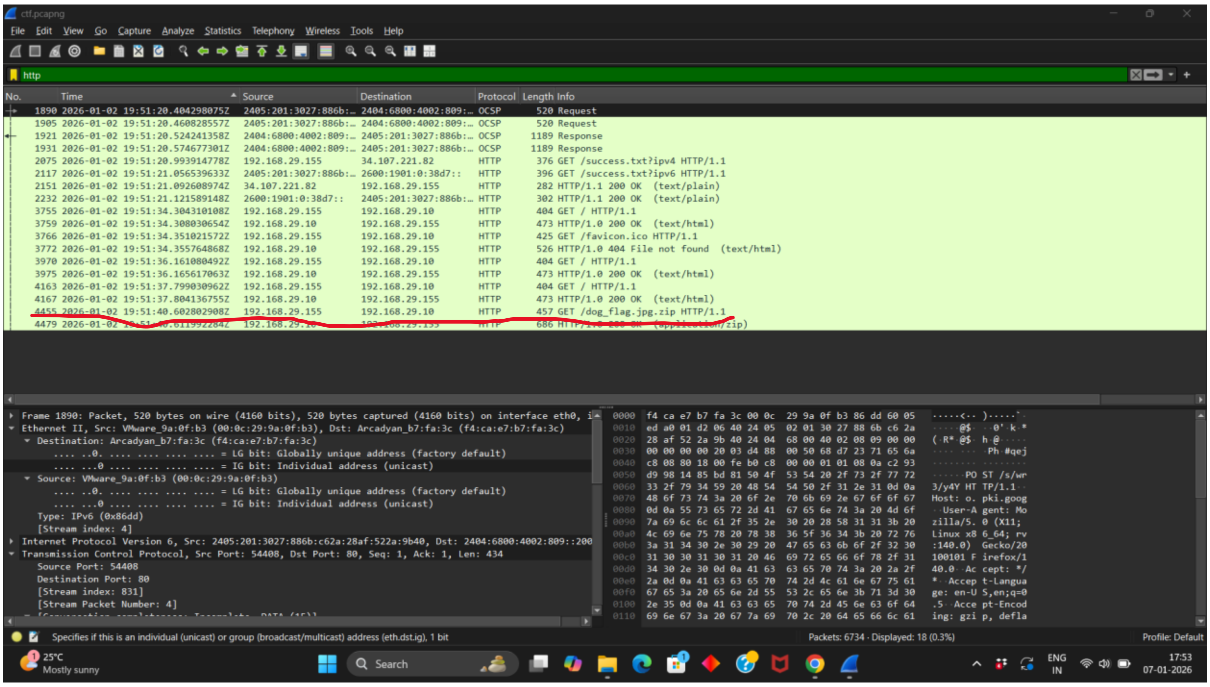
tcp.flags.syn == 1 && tcp.flags.ack == 0

```
No.  Time                            Source          Destination      Protocol Length Info
1038 2026-01-02 19:51:12.557941187Z  192.168.29.10   192.168.29.155   TCP      78 65524 → 7901 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2053296365 TSecr=0 SACK_PERM
1040 2026-01-02 19:51:12.558210946Z  192.168.29.10   192.168.29.155   TCP      78 65525 → 53962 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2670539300 TSecr=0 SACK_PERM
1042 2026-01-02 19:51:12.558463706Z  192.168.29.10   192.168.29.155   TCP      78 65526 → 34737 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=4261099428 TSecr=0 SACK_PERM
1043 2026-01-02 19:51:12.558463914Z  192.168.29.10   192.168.29.155   TCP      78 65527 → 50199 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1587946338 TSecr=0 SACK_PERM
1046 2026-01-02 19:51:12.558801914Z  192.168.29.10   192.168.29.155   TCP      78 65528 → 16650 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1510896708 TSecr=0 SACK_PERM
1048 2026-01-02 19:51:12.664065301Z  192.168.29.10   192.168.29.155   TCP      78 65529 → 16650 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3583244710 TSecr=0 SACK_PERM
1050 2026-01-02 19:51:12.664304313Z  192.168.29.10   192.168.29.155   TCP      78 65530 → 50199 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=513367720 TSecr=0 SACK_PERM
1052 2026-01-02 19:51:12.664490956Z  192.168.29.10   192.168.29.155   TCP      78 65531 → 34737 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=698842463 TSecr=0 SACK_PERM
1054 2026-01-02 19:51:12.664693473Z  192.168.29.10   192.168.29.155   TCP      78 65532 → 53962 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2589681390 TSecr=0 SACK_PERM
1056 2026-01-02 19:51:12.664788045Z  192.168.29.10   192.168.29.155   TCP      78 65533 → 7901 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1092776857 TSecr=0 SACK_PERM
1058 2026-01-02 19:51:12.769495416Z  192.168.29.10   192.168.29.155   TCP      78 65534 → 52978 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=4017974624 TSecr=0 SACK_PERM
1060 2026-01-02 19:51:12.769650647Z  192.168.29.10   192.168.29.155   TCP      78 65535 → 22298 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=324039790 TSecr=0 SACK_PERM
1062 2026-01-02 19:51:12.769757467Z  192.168.29.10   192.168.29.155   TCP      78 49152 → 51821 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2102796096 TSecr=0 SACK_PERM
1064 2026-01-02 19:51:12.769874744Z  192.168.29.10   192.168.29.155   TCP      78 49153 → 8178 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=4088771130 TSecr=0 SACK_PERM
1065 2026-01-02 19:51:12.769874869Z  192.168.29.10   192.168.29.155   TCP      78 49154 → 9718 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=955668044 TSecr=0 SACK_PERM
1068 2026-01-02 19:51:12.875302527Z  192.168.29.10   192.168.29.155   TCP      78 49155 → 9718 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2935955558 TSecr=0 SACK_PERM
1070 2026-01-02 19:51:12.875505210Z  192.168.29.10   192.168.29.155   TCP      78 49156 → 8178 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3462899739 TSecr=0 SACK_PERM
1072 2026-01-02 19:51:12.875741348Z  192.168.29.10   192.168.29.155   TCP      78 49157 → 51821 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2107190950 TSecr=0 SACK_PERM
1074 2026-01-02 19:51:12.875870707Z  192.168.29.10   192.168.29.155   TCP      78 49158 → 22298 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1273440924 TSecr=0 SACK_PERM
1076 2026-01-02 19:51:12.875948989Z  192.168.29.10   192.168.29.155   TCP      78 49159 → 52978 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3279955723 TSecr=0 SACK_PERM
1078 2026-01-02 19:51:12.982070769Z  192.168.29.10   192.168.29.155   TCP      78 49160 → 63496 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3817809827 TSecr=0 SACK_PERM
1080 2026-01-02 19:51:12.982214501Z  192.168.29.10   192.168.29.155   TCP      78 49161 → 60370 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3699820932 TSecr=0 SACK_PERM
1082 2026-01-02 19:51:12.982303907Z  192.168.29.10   192.168.29.155   TCP      78 49162 → 54580 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2504382877 TSecr=0 SACK_PERM
```

```
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: ae:19:31:91:5d:4f (ae:19:31:91:5d:4f)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory de
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 5]
▾ Internet Protocol Version 4, Src: 192.168.29.10, Dst: 192.168.29.155
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 64
    Identification: 0x0000 (0)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: TCP (6)
```

```
0000  00 0c 29 9a 0f b3 ae 19  31 91 5d 4f 08 00 45 00   ··)····· 1·]O··E·
0010  00 40 00 00 40 00 ff 06  bf c1 c0 a8 1d 0a c0 a8   ·@··@··· ········
0020  1d 9b c0 03 25 f6 89 0e  5e e7 00 00 00 00 b0 c2   ····%··· ^·······
0030  ff ff dc f0 00 00 02 04  05 b4 01 03 03 06 01 01   ········ ········
0040  08 0a ae ff 20 66 00 00  00 00 04 02 00 00         ···· f·· ······
```

6.Find the HTTP file download


ctf.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.  Time                            Source                Destination           Protocol Length Info
1890 2026-01-02 19:51:20.404298075Z  2405:201:3027:886b:…  2404:6800:4002:809:…  OCSP      520 Request
1905 2026-01-02 19:51:20.460828557Z  2405:201:3027:886b:…  2404:6800:4002:809:…  OCSP      520 Request
1921 2026-01-02 19:51:20.524241358Z  2404:6800:4002:809:…  2405:201:3027:886b:…  OCSP     1189 Response
1931 2026-01-02 19:51:20.574677301Z  2404:6800:4002:809:…  2405:201:3027:886b:…  OCSP     1189 Response
2075 2026-01-02 19:51:20.993914778Z  192.168.29.155        34.107.221.82         HTTP      376 GET /success.txt?ipv4 HTTP/1.1
2117 2026-01-02 19:51:21.056539633Z  2405:201:3027:886b:…  2600:1901:0:38d7::    HTTP      396 GET /success.txt?ipv6 HTTP/1.1
2151 2026-01-02 19:51:21.092608974Z  34.107.221.82         192.168.29.155        HTTP      282 HTTP/1.1 200 OK  (text/plain)
2232 2026-01-02 19:51:21.121589148Z  2600:1901:0:38d7::    2405:201:3027:886b:…  HTTP      302 HTTP/1.1 200 OK  (text/plain)
3755 2026-01-02 19:51:34.304310108Z  192.168.29.155        192.168.29.10         HTTP      404 GET / HTTP/1.1
3759 2026-01-02 19:51:34.308030654Z  192.168.29.10         192.168.29.155        HTTP      473 HTTP/1.0 200 OK  (text/html)
3766 2026-01-02 19:51:34.351021572Z  192.168.29.155        192.168.29.10         HTTP      425 GET /favicon.ico HTTP/1.1
3772 2026-01-02 19:51:34.355764868Z  192.168.29.10         192.168.29.155        HTTP      526 HTTP/1.0 404 File not found  (text/html)
3970 2026-01-02 19:51:36.161080492Z  192.168.29.155        192.168.29.10         HTTP      404 GET / HTTP/1.1
3975 2026-01-02 19:51:36.165617063Z  192.168.29.10         192.168.29.155        HTTP      473 HTTP/1.0 200 OK  (text/html)
4163 2026-01-02 19:51:37.799030962Z  192.168.29.155        192.168.29.10         HTTP      404 GET / HTTP/1.1
4167 2026-01-02 19:51:37.804136755Z  192.168.29.10         192.168.29.155        HTTP      473 HTTP/1.0 200 OK  (text/html)
4455 2026-01-02 19:51:40.602802908Z  192.168.29.155        192.168.29.10         HTTP      457 GET /dog_flag.jpg.zip HTTP/1.1
4479 2026-01-02 19:51:40.611992284Z  192.168.29.10         192.168.29.155        HTTP      686 HTTP/1.0 200 OK  (application/zip)
```

```
▸ Frame 1890: Packet, 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface eth0, i
▾ Ethernet II, Src: VMware_9a:0f:b3 (00:0c:29:9a:0f:b3), Dst: Arcadyan_b7:fa:3c (f4:ca:e7:b7:fa:3c)
  ▾ Destination: Arcadyan_b7:fa:3c (f4:ca:e7:b7:fa:3c)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: VMware_9a:0f:b3 (00:0c:29:9a:0f:b3)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
    [Stream index: 4]
▸ Internet Protocol Version 6, Src: 2405:201:3027:886b:c62a:28af:522a:9b40, Dst: 2404:6800:4002:809::200
▾ Transmission Control Protocol, Src Port: 54408, Dst Port: 80, Seq: 1, Ack: 1, Len: 434
    Source Port: 54408
    Destination Port: 80
    [Stream index: 831]
    [Stream Packet Number: 4]
```

```
0000  f4 ca e7 b7 fa 3c 00 0c  29 9a 0f b3 86 dd 60 05   ·····<·· )·····`·
0010  ed a0 01 d2 06 40 24 05  02 01 30 27 88 6b c6 2a   ·····@$· ··0'·k·*
0020  28 af 52 2a 9b 40 24 04  68 00 40 02 08 09 00 00   (·R*·@$· h·@·····
0030  00 00 00 00 20 03 d4 88  00 50 68 d7 23 71 65 6a   ···· ··· ·Ph·#qej
0040  c8 08 80 18 00 fe b0 c8  00 00 01 01 08 0a c2 93   ········ ········
0050  d9 98 14 85 bd 81 50 4f  53 54 20 2f 73 2f 77 72   ······PO ST /s/wr
0060  33 2f 79 34 59 20 48 54  54 50 2f 31 2e 31 0d 0a   3/y4Y HT TP/1.1··
0070  48 6f 73 74 3a 20 6f 2e  70 6b 69 2e 67 6f 6f 67   Host: o. pki.goog
0080  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··User-A gent: Mo
0090  7a 69 6c 6c 61 2f 35 2e  30 20 28 58 31 31 3b 20   zilla/5. 0 (X11;
00a0  4c 69 6e 75 78 20 78 38  36 5f 36 34 3b 20 72 76   Linux x8 6_64; rv
00b0  3a 31 34 30 2e 30 29 20  47 65 63 6b 6f 2f 32 30   :140.0)  Gecko/20
00c0  31 30 30 31 30 31 20 46  69 72 65 66 6f 78 2f 31   100101 F irefox/1
00d0  34 30 2e 30 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   40.0··Ac cept: */
00e0  2a 0d 0a 41 63 63 65 70  74 2d 4c 61 6e 67 75 61   *··Accep t-Langua
00f0  67 65 3a 20 65 6e 2d 55  53 2c 65 6e 3b 71 3d 30   ge: en-U S,en;q=0
0100  2e 35 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   .5··Acce pt-Encod
0110  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65 66 6c 61   ing: gzi p, defla
```

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 1 bit

After finding the HTTP

dog_flag.jpg.zip

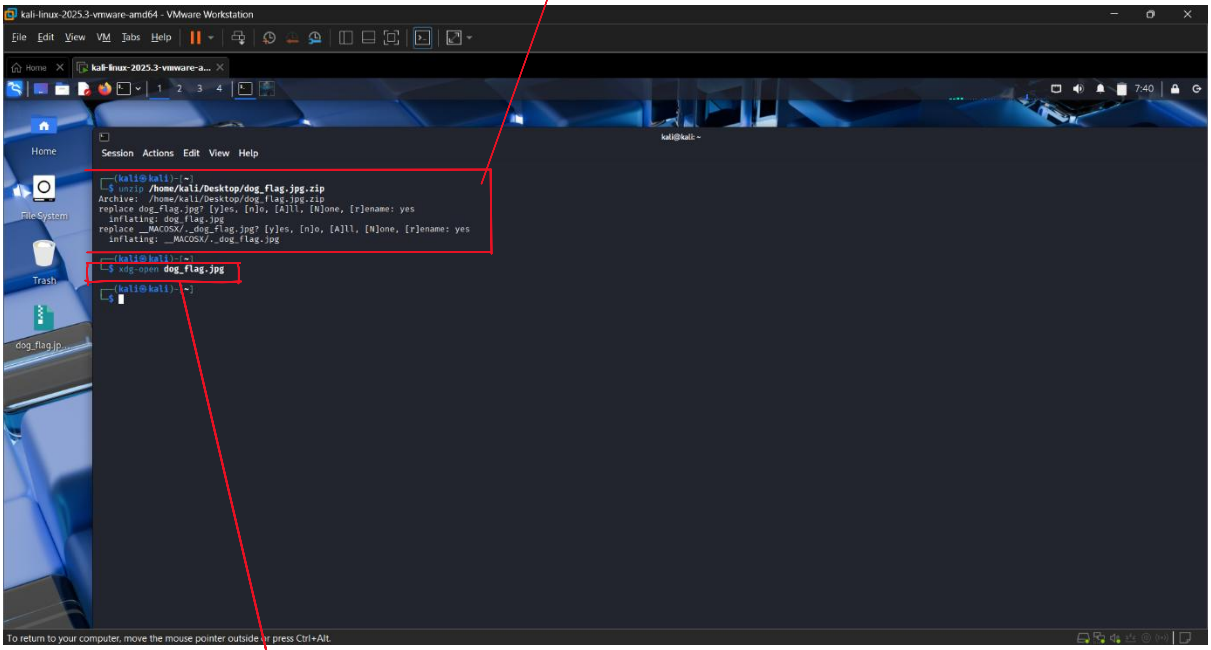
7. Extract the ZIP file from the PCAP

1. Go to file
2. Extract object
3. Choose the fiel (dog_flag.jpg.zip)
4. Save

8. Unzip the file

1. Go to Linux
2. Drag or copy the zip file in Linux OS
3. Open terminal
4. Run command to unzip

Command to unzip

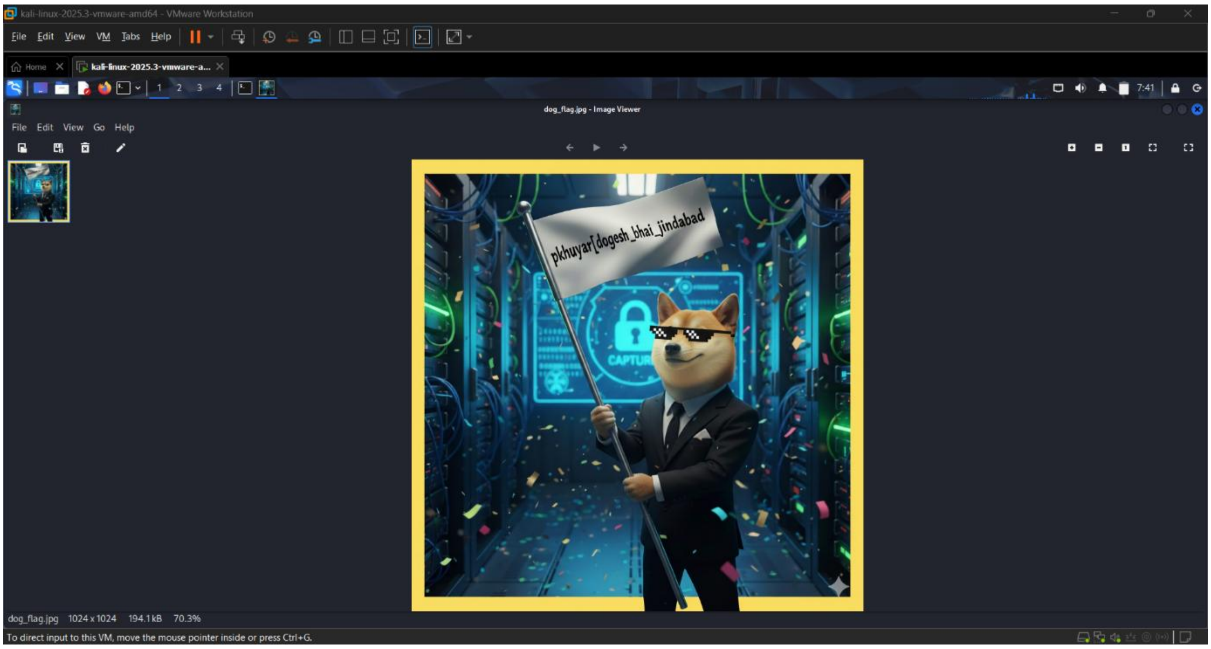

kali-linux-2025.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.3-vmware-a...
1 2 3 4
7:40
Home
File System
Trash
dog_flag.jp...
kali@kali: ~
Session Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ unzip /home/kali/Desktop/dog_flag.jpg.zip
Archive:  /home/kali/Desktop/dog_flag.jpg.zip
replace dog_flag.jpg? [y]es, [n]o, [A]ll, [N]one, [r]ename: yes
  inflating: dog_flag.jpg
replace __MACOSX/._dog_flag.jpg? [y]es, [n]o, [A]ll, [N]one, [r]ename: yes
  inflating: __MACOSX/._dog_flag.jpg

┌──(kali㉿kali)-[~]
└─$ xdg-open dog_flag.jpg

┌──(kali㉿kali)-[~]
└─$ 
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

The command **xdg-open** dog_flag.jpg is used in Linux to open a file using the system's default application. It will open the file in default image viewer.

Retrieve the flag


kali-linux-2025.3-vmware-amd64 - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
kali-linux-2025.3-vmware-a...
1
2
3
4
7:41
dog_flag.jpg - Image Viewer
File
Edit
View
Go
Help
pkhuyar[dogesh_bhai_jindabad
CAPTUR
dog_flag.jpg
1024 x 1024
194.1 kB
70.3%
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Questions to Answer

Answer the following questions one by one in your report:

1. What is the attacker IP address?

Ans→ 192.168.29.10

2. What is the first packet timestamp related to the attack?

Ans→ 2026-01-02 19:51:12.875302527Z

3. What evidence suggests that port scanning (reconnaissance) was performed?

Ans→ TCP 3-way handshake

4. What is the name of the downloaded ZIP file?

Ans → dog_flag.jpg.zip

5. What is the flag obtained after unzipping the file?

FLAG{pkhuyar_[doges_bhai_jindabad}