

## Reg : nProbe collector output

Lavanya Singaravelan <lavanya.singaravelan@tatacommunications.com>

Tue 10/12/2019 17:50

To: Sriram Ramanujam <sriram.ramanujam@tatacommunications.com>

Hi Sriram,

I'm getting the below output for nProbe collector

```
10/Dec/2019 17:09:19 [collect.c:183] Flow collector listening on port 2055 (IPv4/v6)
10/Dec/2019 17:09:19 [nprobe.c:9472] WARNING: *****
*****
10/Dec/2019 17:09:19 [nprobe.c:9473] WARNING: ** You're running nprobe in DEBUG mode **
10/Dec/2019 17:09:19 [nprobe.c:9474] WARNING: *****
*****
10/Dec/2019 17:09:19 [nprobe.c:9620] nProbe started successfully
10/Dec/2019 17:10:41 [collect.c:2346] NETFLOW_DEBUG: Received 60 bytes flow
10/Dec/2019 17:10:41 [collect.c:896] +++ Dissecting packet 1
10/Dec/2019 17:12:41 [collect.c:2346] NETFLOW_DEBUG: Received 60 bytes flow
10/Dec/2019 17:12:41 [collect.c:896] +++ Dissecting packet 2
```

This is the output which I'm getting in Wireshark

### For template

```
> Frame 132: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
> Ethernet II, Src: ca:02:06:7d:00:00 (ca:02:06:7d:00:00), Dst: PcsCompu_dd:91:f4 (08:00:27:dd:91:f4)
> Internet Protocol Version 4, Src: 192.168.56.105, Dst: 192.168.56.106
> User Datagram Protocol, Src Port: 62087, Dst Port: 2055
< Cisco NetFlow/IPFIX
  Version: 9
  Count: 1
  SysUptime: 1495.420000000 seconds
  Timestamp: Dec 10, 2019 22:44:41.000000000 India Standard Time
  FlowSequence: 56
  SourceId: 0
  < FlowSet 1 [Id=0] (Data Template): 256
    FlowSet Id: Data Template (V9) (0)
    FlowSet Length: 40
    < Template (Id = 256, Count = 8)
      Template Id: 256
      Field Count: 8
      > Field (1/8): IP_SRC_ADDR
      > Field (2/8): IP_DST_ADDR
      > Field (3/8): L4_SRC_PORT
      > Field (4/8): L4_DST_PORT
      > Field (5/8): IP_TOS
      > Field (6/8): PROTOCOL
      > Field (7/8): BYTES
      > Field (8/8): PKTS
```

```
> Frame 257: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 0
> Ethernet II, Src: ca:02:06:7d:00:00 (ca:02:06:7d:00:00), Dst: PcsCompu_dd:91:f4 (08:00:27:dd:91:f4)
> Internet Protocol Version 4, Src: 192.168.56.105, Dst: 192.168.56.106
> User Datagram Protocol, Src Port: 62087, Dst Port: 2055
< Cisco NetFlow/IPFIX
  Version: 9
  Count: 1
  SysUptime: 1878.420000000 seconds
  Timestamp: Dec 10, 2019 22:51:03.000000000 India Standard Time
  FlowSequence: 62
  SourceId: 0
  < FlowSet 1 [Id=256] (1 flows)
    FlowSet Id: (Data) (256)
    FlowSet Length: 34
    < [Template Frame: 34]
      < Flow 1
        SrcAddr: 192.168.56.106
        DstAddr: 192.168.56.105
        SrcPort: 0
        DstPort: 0
        IP ToS: 0x00
        Protocol: ICMP (1)
        Octets: 1000
        Packets: 10
```

Thanks and Regards,  
Lavanya Singaravelan