Covert Channel – Suspicious

Write up by:

John Antone

835 COS

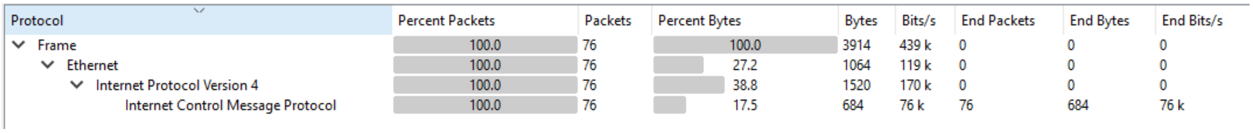
854 CPT

Covert Channel - Suspicious

160

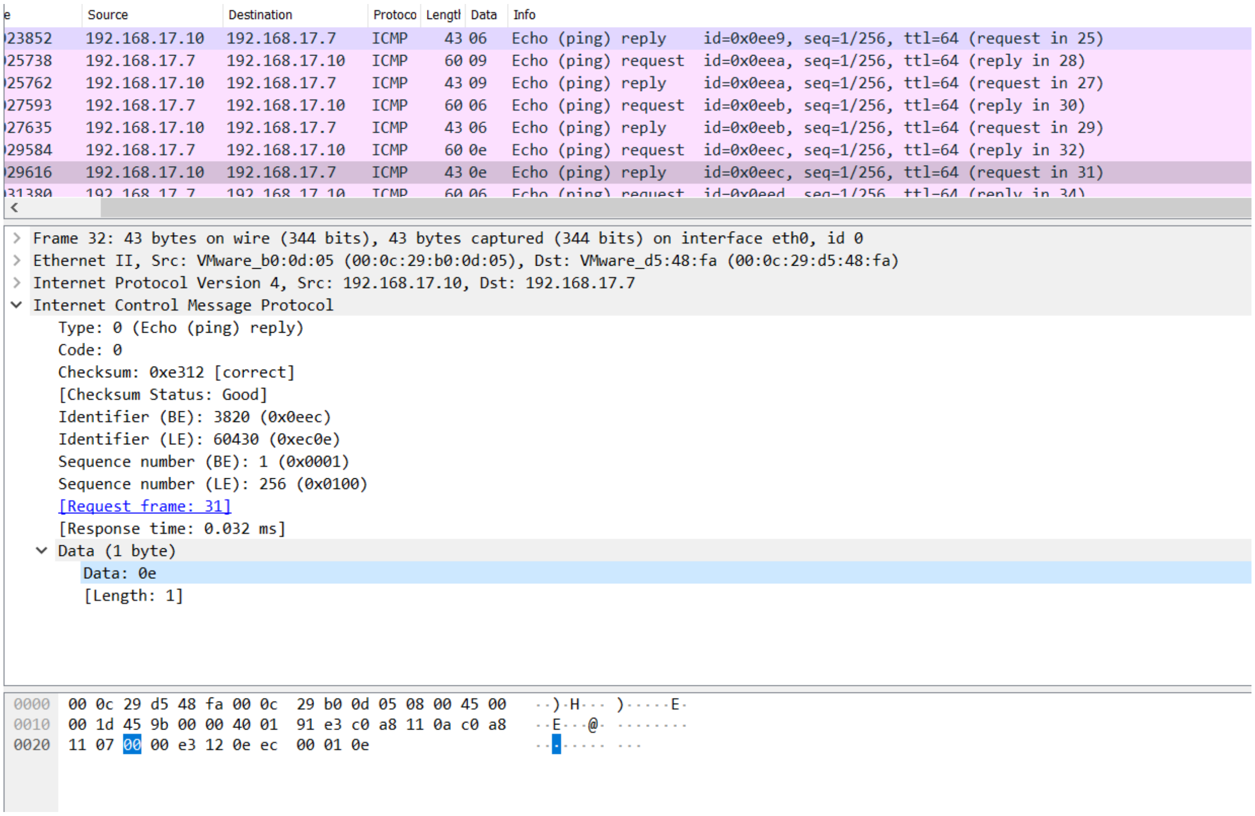
We found some suspicious traffic on our network and think there could be some malware using covert channels to convey messages. We isolated the suspicious traffic for you to take a look. Format: flag{...}

To start off with on this Pcap we look at the Protocol Hierarchy page:



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	76	100.0	3914	439 k	0	0	0
Ethernet	100.0	76	27.2	1064	119 k	0	0	0
Internet Protocol Version 4	100.0	76	38.8	1520	170 k	0	0	0
Internet Control Message Protocol	100.0	76	17.5	684	76 k	76	684	76 k

We see there is only ICMP messages in this pcap, so the answer is in the 76 packets somewhere. And we have Request and Replies that seem to be echoing each other, so to start off we should look at one side of the conversation first. Also all the packets do not look too different from the ASCII section of the hexdump.

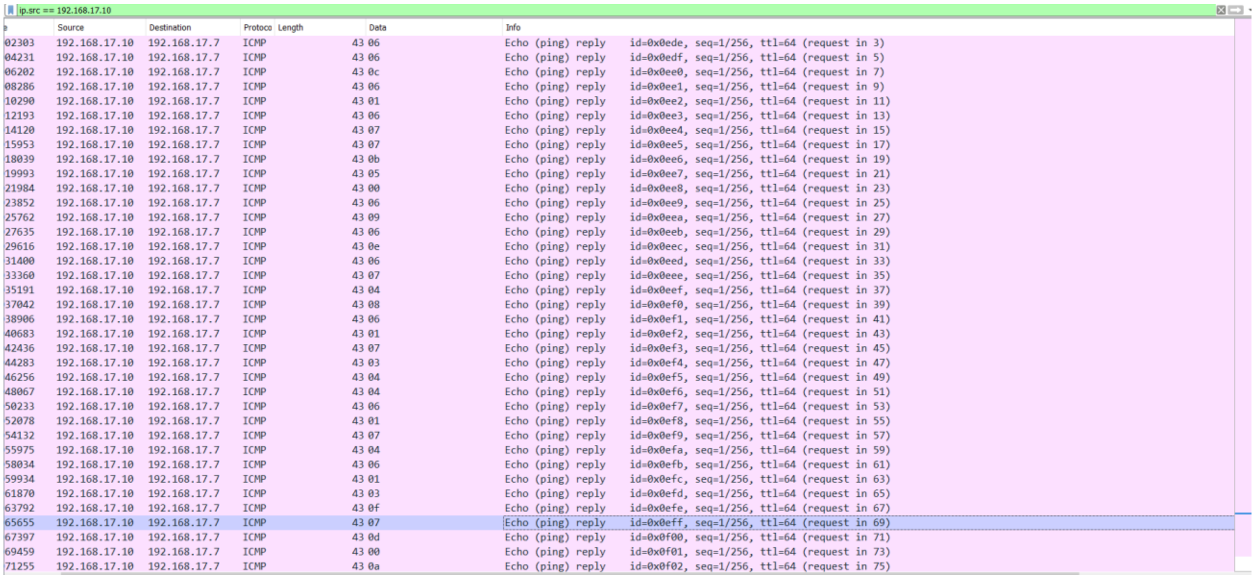


```
e        Source         Destination    Protoco Lengtl Data Info
23852    192.168.17.10  192.168.17.7   ICMP    43     06   Echo (ping) reply    id=0x0ee9, seq=1/256, ttl=64 (request in 25)
25738    192.168.17.7   192.168.17.10  ICMP    60     09   Echo (ping) request  id=0x0eea, seq=1/256, ttl=64 (reply in 28)
25762    192.168.17.10  192.168.17.7   ICMP    43     09   Echo (ping) reply    id=0x0eea, seq=1/256, ttl=64 (request in 27)
27593    192.168.17.7   192.168.17.10  ICMP    60     06   Echo (ping) request  id=0x0eeb, seq=1/256, ttl=64 (reply in 30)
27635    192.168.17.10  192.168.17.7   ICMP    43     06   Echo (ping) reply    id=0x0eeb, seq=1/256, ttl=64 (request in 29)
29584    192.168.17.7   192.168.17.10  ICMP    60     0e   Echo (ping) request  id=0x0eec, seq=1/256, ttl=64 (reply in 32)
29616    192.168.17.10  192.168.17.7   ICMP    43     0e   Echo (ping) reply    id=0x0eec, seq=1/256, ttl=64 (request in 31)
31380    192.168.17.7   192.168.17.10  ICMP    60     06   Echo (ping) request  id=0x0eed, seq=1/256, ttl=64 (reply in 34)
```

```
> Frame 32: 43 bytes on wire (344 bits), 43 bytes captured (344 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_b0:0d:05 (00:0c:29:b0:0d:05), Dst: VMware_d5:48:fa (00:0c:29:d5:48:fa)
> Internet Protocol Version 4, Src: 192.168.17.10, Dst: 192.168.17.7
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xe312 [correct]
    [Checksum Status: Good]
    Identifier (BE): 3820 (0x0eec)
    Identifier (LE): 60430 (0xec0e)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Request frame: 31]
    [Response time: 0.032 ms]
  v Data (1 byte)
      Data: 0e
      [Length: 1]
```

```
0000  00 0c 29 d5 48 fa 00 0c  29 b0 0d 05 08 00 45 00   ··)·H··· )·····E·
0010  00 1d 45 9b 00 00 40 01  91 e3 c0 a8 11 0a c0 a8   ··E···@· ········
0020  11 07 00 00 e3 12 0e ec  00 01 0e                  ········ ···
```

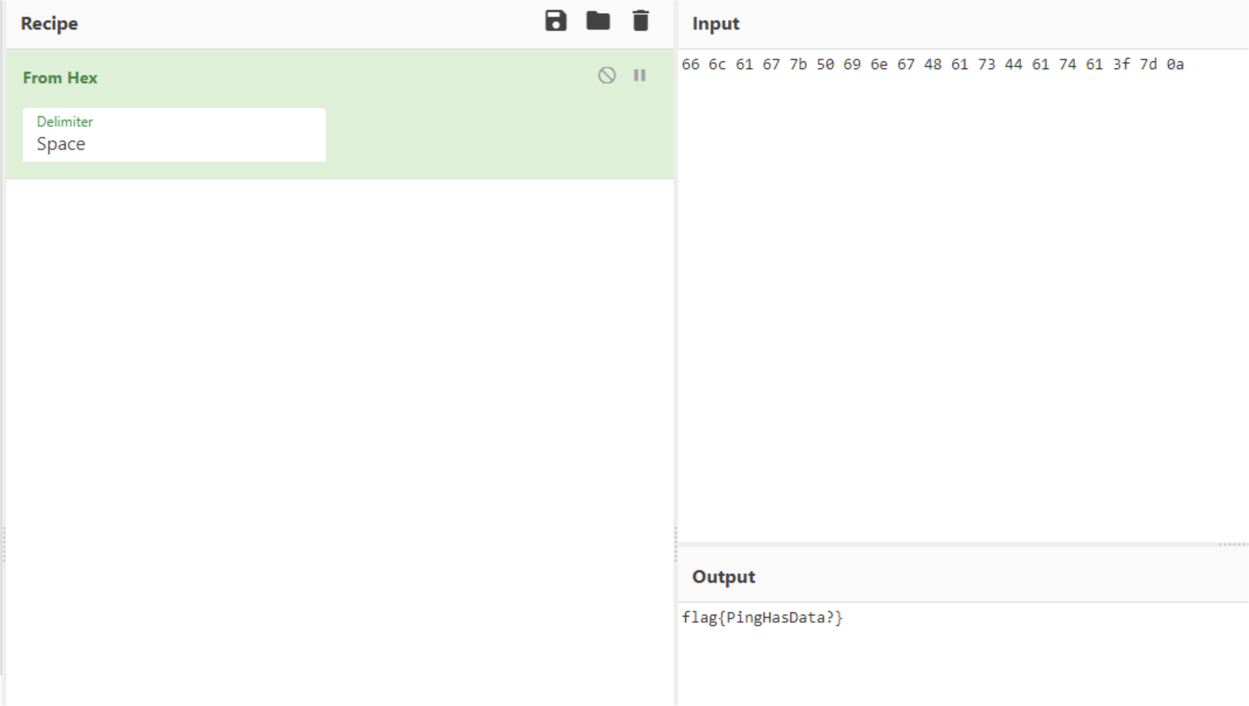
But after looking closer we are seeing information in the Data Section that looks “Suspicious”. But when we add the Data field as a column, we see a pattern in the data field, it looks like Hex.



ip.src == 192.168.17.10

e	Source	Destination	Protoco	Length	Data	Info
02303	192.168.17.10	192.168.17.7	ICMP	43	06	Echo (ping) reply id=0x0ede, seq=1/256, ttl=64 (request in 3)
04231	192.168.17.10	192.168.17.7	ICMP	43	06	Echo (ping) reply id=0x0edf, seq=1/256, ttl=64 (request in 5)
06202	192.168.17.10	192.168.17.7	ICMP	43	0c	Echo (ping) reply id=0x0ee0, seq=1/256, ttl=64 (request in 7)
08286	192.168.17.10	192.168.17.7	ICMP	43	06	Echo (ping) reply id=0x0ee1, seq=1/256, ttl=64 (request in 9)
10290	192.168.17.10	192.168.17.7	ICMP	43	01	Echo (ping) reply id=0x0ee2, seq=1/256, ttl=64 (request in 11)
12193	192.168.17.10	192.168.17.7	ICMP	43	06	Echo (ping) reply id=0x0ee3, seq=1/256, ttl=64 (request in 13)
14120	192.168.17.10	192.168.17.7	ICMP	43	07	Echo (ping) reply id=0x0ee4, seq=1/256, ttl=64 (request in 15)
15953	192.168.17.10	192.168.17.7	ICMP	43	07	Echo (ping) reply id=0x0ee5, seq=1/256, ttl=64 (request in 17)
18039	192.168.17.10	192.168.17.7	ICMP	43	0b	Echo (ping) reply id=0x0ee6, seq=1/256, ttl=64 (request in 19)
19993	192.168.17.10	192.168.17.7	ICMP	43	05	Echo (ping) reply id=0x0ee7, seq=1/256, ttl=64 (request in 21)
21984	192.168.17.10	192.168.17.7	ICMP	43	00	Echo (ping) reply id=0x0ee8, seq=1/256, ttl=64 (request in 23)
23852	192.168.17.10	192.168.17.7	ICMP	43	06	Echo (ping) reply id=0x0ee9, seq=1/256, ttl=64 (request in 25)
25762	192.168.17.10	192.168.17.7	ICMP	43	09	Echo (ping) reply id=0x0eea, seq=1/256, ttl=64 (request in 27)
27635	192.168.17.10	192.168.17.7	ICMP	43	06	Echo (ping) reply id=0x0eeb, seq=1/256, ttl=64 (request in 29)
29616	192.168.17.10	192.168.17.7	ICMP	43	0e	Echo (ping) reply id=0x0eec, seq=1/256, ttl=64 (request in 31)
31400	192.168.17.10	192.168.17.7	ICMP	43	06	Echo (ping) reply id=0x0eed, seq=1/256, ttl=64 (request in 33)
33360	192.168.17.10	192.168.17.7	ICMP	43	07	Echo (ping) reply id=0x0eee, seq=1/256, ttl=64 (request in 35)
35191	192.168.17.10	192.168.17.7	ICMP	43	04	Echo (ping) reply id=0x0eef, seq=1/256, ttl=64 (request in 37)
37042	192.168.17.10	192.168.17.7	ICMP	43	08	Echo (ping) reply id=0x0ef0, seq=1/256, ttl=64 (request in 39)
38906	192.168.17.10	192.168.17.7	ICMP	43	06	Echo (ping) reply id=0x0ef1, seq=1/256, ttl=64 (request in 41)
40683	192.168.17.10	192.168.17.7	ICMP	43	01	Echo (ping) reply id=0x0ef2, seq=1/256, ttl=64 (request in 43)
42436	192.168.17.10	192.168.17.7	ICMP	43	07	Echo (ping) reply id=0x0ef3, seq=1/256, ttl=64 (request in 45)
44283	192.168.17.10	192.168.17.7	ICMP	43	03	Echo (ping) reply id=0x0ef4, seq=1/256, ttl=64 (request in 47)
46256	192.168.17.10	192.168.17.7	ICMP	43	04	Echo (ping) reply id=0x0ef5, seq=1/256, ttl=64 (request in 49)
48067	192.168.17.10	192.168.17.7	ICMP	43	04	Echo (ping) reply id=0x0ef6, seq=1/256, ttl=64 (request in 51)
50233	192.168.17.10	192.168.17.7	ICMP	43	06	Echo (ping) reply id=0x0ef7, seq=1/256, ttl=64 (request in 53)
52078	192.168.17.10	192.168.17.7	ICMP	43	01	Echo (ping) reply id=0x0ef8, seq=1/256, ttl=64 (request in 55)
54132	192.168.17.10	192.168.17.7	ICMP	43	07	Echo (ping) reply id=0x0ef9, seq=1/256, ttl=64 (request in 57)
55975	192.168.17.10	192.168.17.7	ICMP	43	04	Echo (ping) reply id=0x0efa, seq=1/256, ttl=64 (request in 59)
58034	192.168.17.10	192.168.17.7	ICMP	43	06	Echo (ping) reply id=0x0efb, seq=1/256, ttl=64 (request in 61)
59934	192.168.17.10	192.168.17.7	ICMP	43	01	Echo (ping) reply id=0x0efc, seq=1/256, ttl=64 (request in 63)
61870	192.168.17.10	192.168.17.7	ICMP	43	03	Echo (ping) reply id=0x0efd, seq=1/256, ttl=64 (request in 65)
63792	192.168.17.10	192.168.17.7	ICMP	43	0f	Echo (ping) reply id=0x0efe, seq=1/256, ttl=64 (request in 67)
65655	192.168.17.10	192.168.17.7	ICMP	43	07	Echo (ping) reply id=0x0eff, seq=1/256, ttl=64 (request in 69)
67397	192.168.17.10	192.168.17.7	ICMP	43	0d	Echo (ping) reply id=0x0f00, seq=1/256, ttl=64 (request in 71)
69459	192.168.17.10	192.168.17.7	ICMP	43	00	Echo (ping) reply id=0x0f01, seq=1/256, ttl=64 (request in 73)
71255	192.168.17.10	192.168.17.7	ICMP	43	0a	Echo (ping) reply id=0x0f02, seq=1/256, ttl=64 (request in 75)

When we pull out the hex from above (take out the 0 on all the data) we get this: 66 6c 61 67 7b 50 69 6e 67 48 61 73 44 61 74 61 3f 7d 0a



Delimiter
Space

Input

```
66 6c 61 67 7b 50 69 6e 67 48 61 73 44 61 74 61 3f 7d 0a
```

Output

```
flag{PingHasData?}
```

Put that in to a hex decode/cyber chef we get the following flag: flag{PingHasData?}