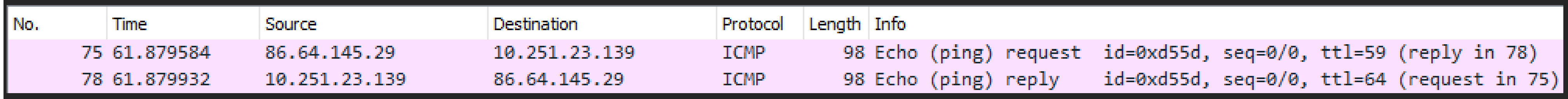
THM_Wireshark 101 [Task 8 IMCP]

I learned about packet types, timestamps, and data strings
from ICMP packets

dns+icmp.pcapng 8 kB

ICMP or Internet Control Message Protocol is used to analyze various nodes on a network. This is most commonly used with utilities like ping and traceroute. You should already be familiar with how ICMP works; however, if you need a refresher, read the IETF documentation.

Below you can see a sample of what a ping would look like, we can see a request to the server from ICMP, then a reply from the server.



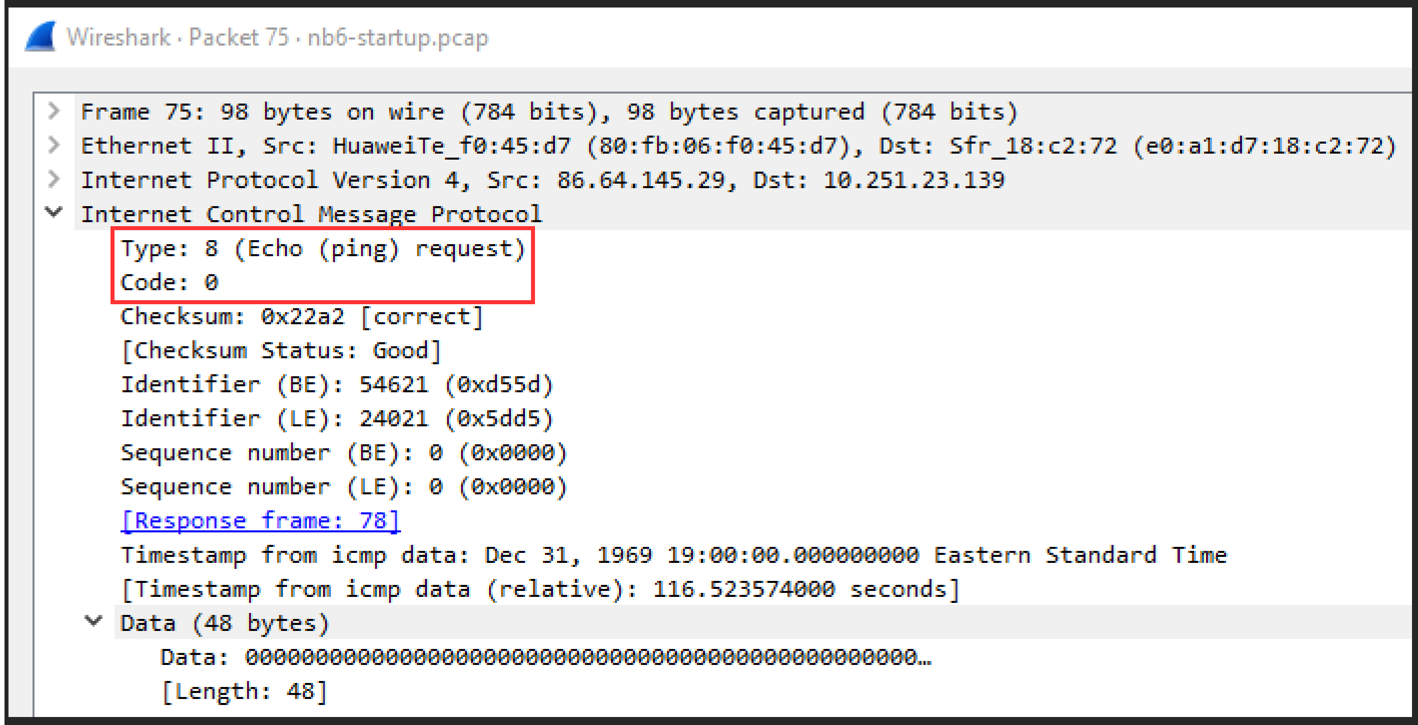
```
No.   Time        Source          Destination     Protocol  Length Info
   75 61.879584   86.64.145.29    10.251.23.139   ICMP          98 Echo (ping) request  id=0xd55d, seq=0/0, ttl=59 (reply in 78)
   78 61.879932   10.251.23.139   86.64.145.29    ICMP          98 Echo (ping) reply    id=0xd55d, seq=0/0, ttl=64 (request in 75)
```

ICMP Traffic Overview

ICMP request:

Below we see packet details for a ping request packet. There are a few important things within the packet details that we can take note of first being the type and code of the packet. A type that equals 8 means that it is a request packet, if it is equal to 0 it is a reply packet. When these codes are altered or do not seem correct that is typically a sign of suspicious activity.

There are two other details within the packet that are useful to analyze: timestamp and data. The timestamp can be useful for identifying the time the ping was requested it can also be useful to identify suspicious activity in some cases. We can also look at the data string which will typically just be a random data string.



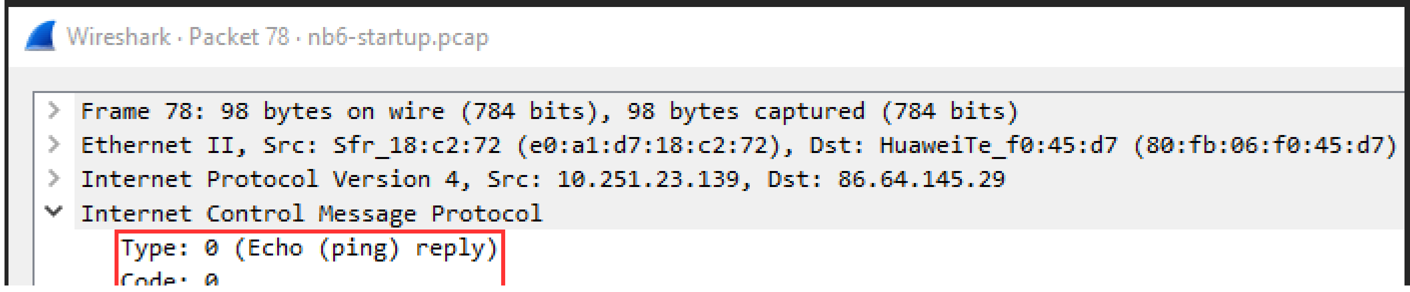
Wireshark · Packet 75 · nb6-startup.pcap

```
> Frame 75: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: HuaweiTe_f0:45:d7 (80:fb:06:f0:45:d7), Dst: Sfr_18:c2:72 (e0:a1:d7:18:c2:72)
> Internet Protocol Version 4, Src: 86.64.145.29, Dst: 10.251.23.139
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x22a2 [correct]
    [Checksum Status: Good]
    Identifier (BE): 54621 (0xd55d)
    Identifier (LE): 24021 (0x5dd5)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Response frame: 78]
    Timestamp from icmp data: Dec 31, 1969 19:00:00.000000000 Eastern Standard Time
    [Timestamp from icmp data (relative): 116.523574000 seconds]
  v Data (48 bytes)
      Data: 000000000000000000000000000000000000000000000000…
      [Length: 48]
```

ICMP Reply:

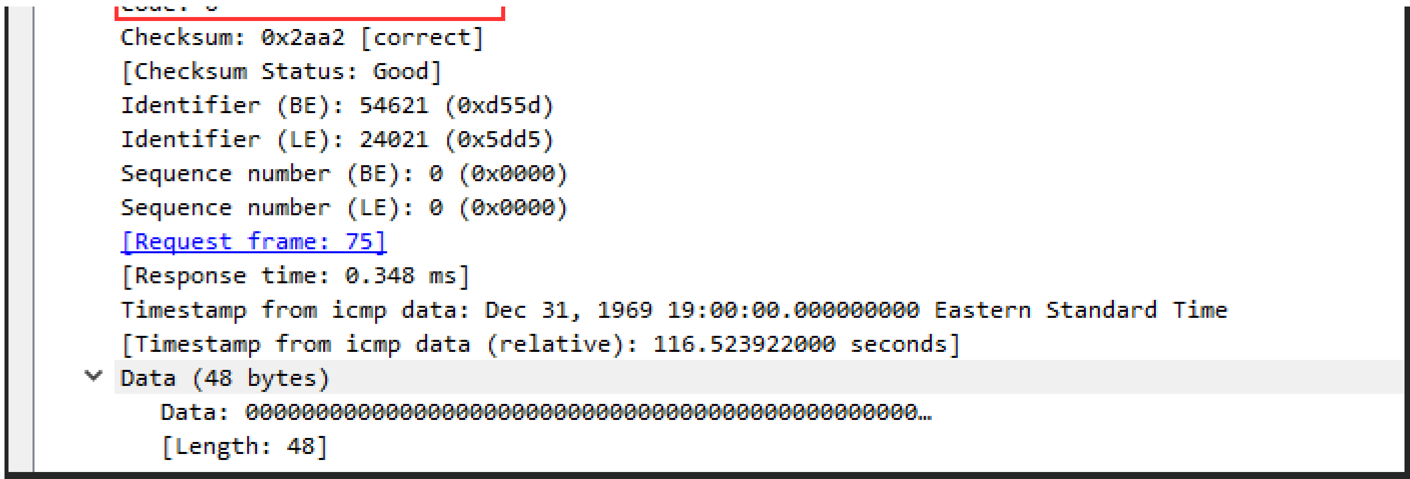
Below you can see that the reply packet is very similar to the request packet. One of the main difference that distinguishes a reply packet is the code, in this case, you can see it is 0, confirming that it is a reply packet.

The same analysis techniques for Request packets apply here as well, again the main difference will be the packet type.



Wireshark · Packet 78 · nb6-startup.pcap

```
> Frame 78: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: Sfr_18:c2:72 (e0:a1:d7:18:c2:72), Dst: HuaweiTe_f0:45:d7 (80:fb:06:f0:45:d7)
> Internet Protocol Version 4, Src: 10.251.23.139, Dst: 86.64.145.29
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
```

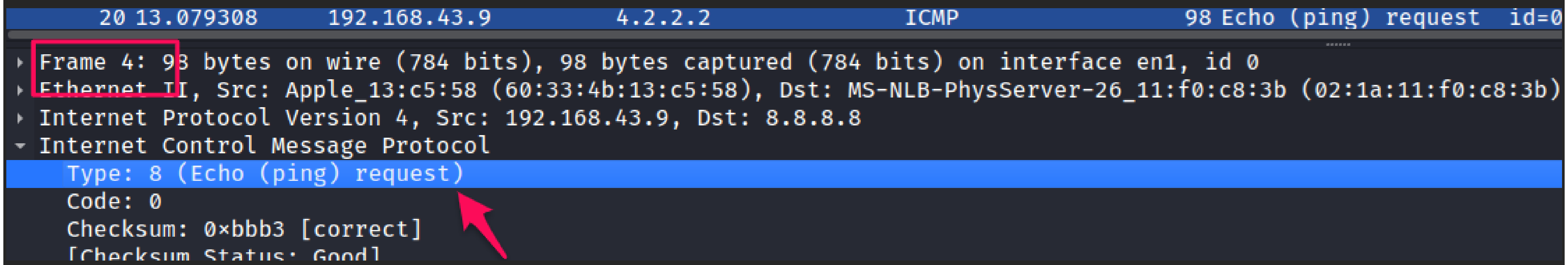


```
    Code: 0
    Checksum: 0x2aa2 [correct]
    [Checksum Status: Good]
    Identifier (BE): 54621 (0xd55d)
    Identifier (LE): 24021 (0x5dd5)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Request frame: 75]
    [Response time: 0.348 ms]
    Timestamp from icmp data: Dec 31, 1969 19:00:00.000000000 Eastern Standard Time
    [Timestamp from icmp data (relative): 116.523922000 seconds]
  ˅ Data (48 bytes)
      Data: 000000000000000000000000000000000000000000000000…
      [Length: 48]
```

Answer the questions below

What is the type for packet 4?

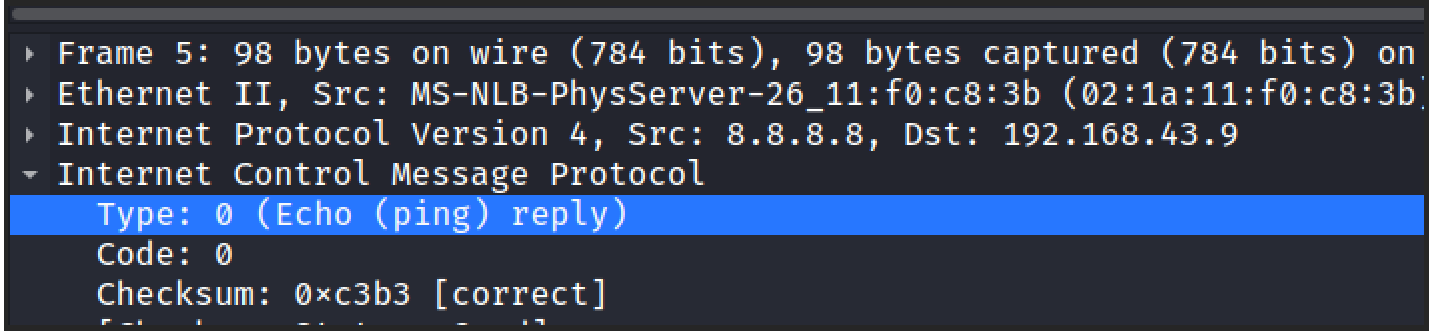
8



```
   20 13.079308      192.168.43.9          4.2.2.2                ICMP                 98 Echo (ping) request  id=0
› Frame 4: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en1, id 0
› Ethernet II, Src: Apple_13:c5:58 (60:33:4b:13:c5:58), Dst: MS-NLB-PhysServer-26_11:f0:c8:3b (02:1a:11:f0:c8:3b)
› Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8
˅ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0×bbb3 [correct]
    [Checksum Status: Good]
```

What is the type for packet 5?

0

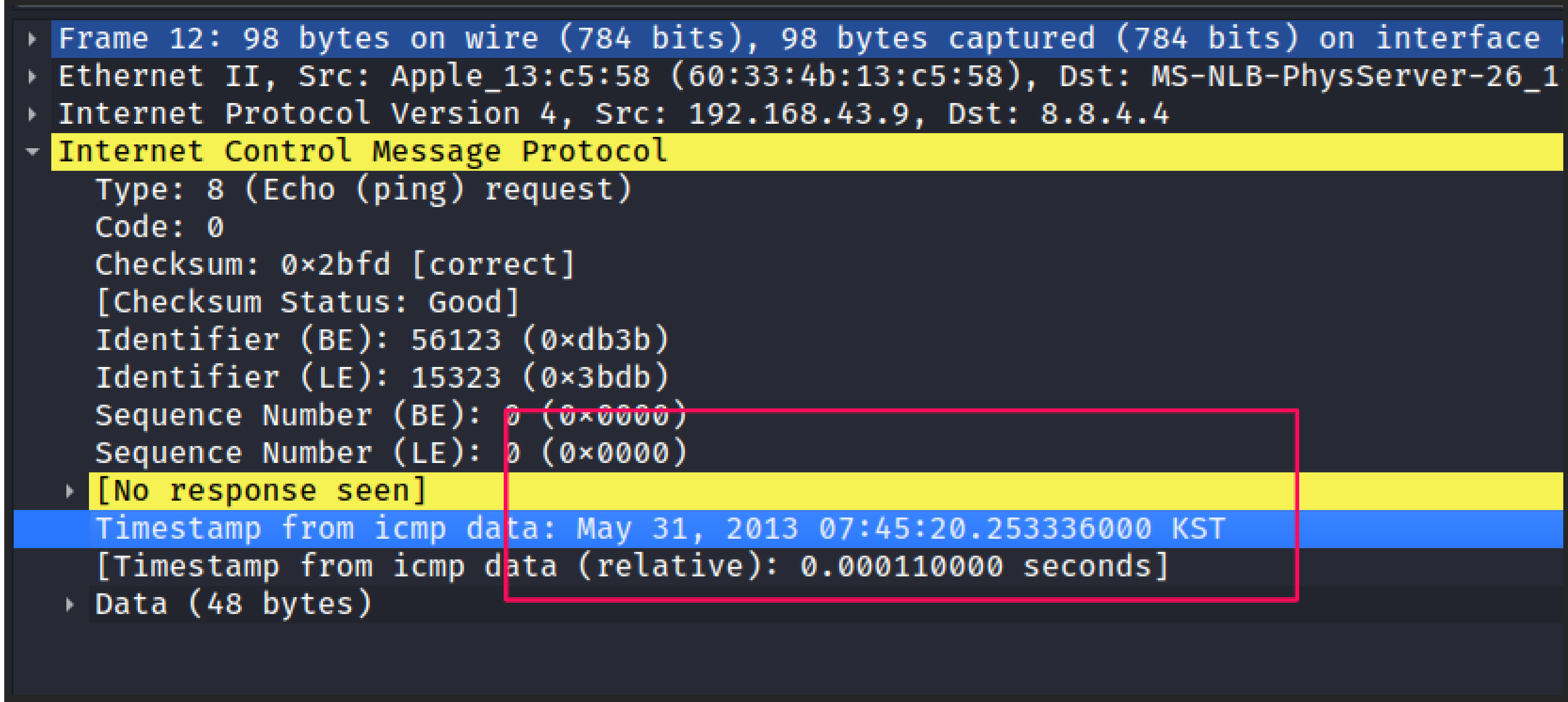


```
› Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on
› Ethernet II, Src: MS-NLB-PhysServer-26_11:f0:c8:3b (02:1a:11:f0:c8:3b)
› Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.43.9
˅ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0×c3b3 [correct]
```

What is the timestamp for packet 12, only including month day and year?

note: Wireshark bases it's time off of your devices time zone, if your answer is wrong try one day more or less.

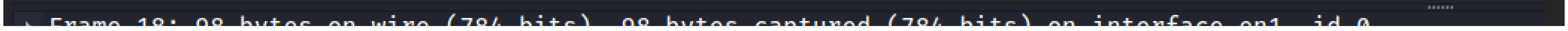
May 30, 2013



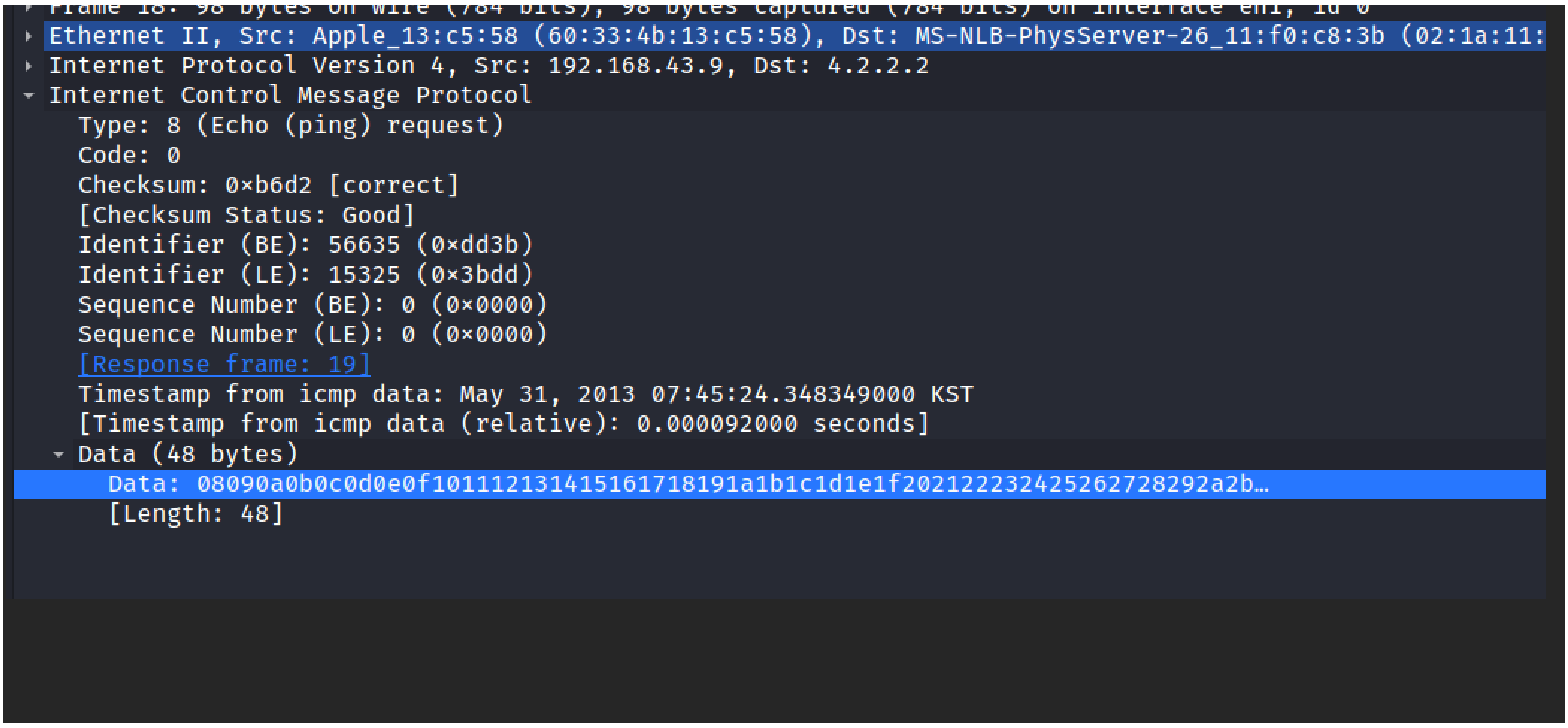
```
› Frame 12: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface
› Ethernet II, Src: Apple_13:c5:58 (60:33:4b:13:c5:58), Dst: MS-NLB-PhysServer-26_1
› Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.4.4
˅ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0×2bfd [correct]
    [Checksum Status: Good]
    Identifier (BE): 56123 (0×db3b)
    Identifier (LE): 15323 (0×3bdb)
    Sequence Number (BE): 0 (0×0000)
    Sequence Number (LE): 0 (0×0000)
  › [No response seen]
    Timestamp from icmp data: May 31, 2013 07:45:20.253336000 KST
    [Timestamp from icmp data (relative): 0.000110000 seconds]
  › Data (48 bytes)
```

What is the full data string for packet 18?

08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637



```
› Frame 18: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en1, id 0
```



```
▸ Frame 18: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en1, id 0
▸ Ethernet II, Src: Apple_13:c5:58 (60:33:4b:13:c5:58), Dst: MS-NLB-PhysServer-26_11:f0:c8:3b (02:1a:11:
▸ Internet Protocol Version 4, Src: 192.168.43.9, Dst: 4.2.2.2
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x b6d2 [correct]
    [Checksum Status: Good]
    Identifier (BE): 56635 (0xdd3b)
    Identifier (LE): 15325 (0x3bdd)
    Sequence Number (BE): 0 (0x0000)
    Sequence Number (LE): 0 (0x0000)
    [Response frame: 19]
    Timestamp from icmp data: May 31, 2013 07:45:24.348349000 KST
    [Timestamp from icmp data (relative): 0.000092000 seconds]
  ▾ Data (48 bytes)
      Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b…
      [Length: 48]
```