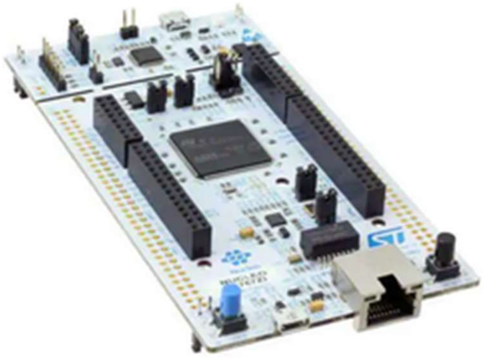
Ping request bug in Nucleo-F767ZI

Ingmar Pätzold

24th Sept 2020



Label on backside:	MB1137 B-01 A20172920
Hardware:	MB1137 Rev B

Setup

The Nucleo Board basically runs the Webserver Example from the recent ST firmware package:

…\STM32Cube_FW_F7_V1.16.0\Projects\STM32F767ZI-Nucleo\Applications\LwIP\LwIP_HTTP_Server_Netconn_RTOS

Changes:

Ping.c added from

https://git.savannah.nongnu.org/cgit/lwip.git/tree/contrib/apps/ping

- ➔ My application sends out echo requests (ping) to my computer
- ➔ On the computer, wireshark is capturing the ethernet interface.

Observation

- ➔ The ping request arrives at the computer, but it does not answer, since the ICMP checksum is incorrect (0x0000), see below.
- ➔ Vice versa, thus when the computer pings the Nucleo board, both request and answer are OK.

I have tracked down the problem through ping, lwip and eventually the HAL_ETH code.

- ➔ The message buffer is correct until the content is given to the DMA.

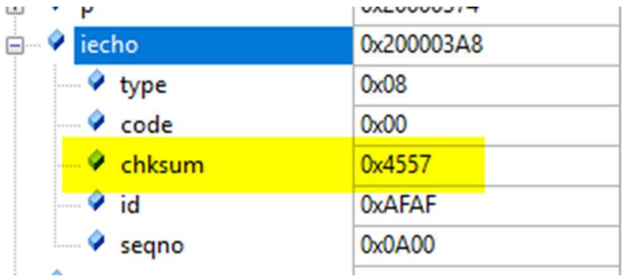
Assumption

The lower levels or the hardware (MAC? PHY?)

- ○ Set the ICMP checksum to 0x0000
- ○ Calculate the IP packet checksum (correctly)

Tracking down the bug

1. The checksum is (correctly) calculated for the ICMP message in ping.c

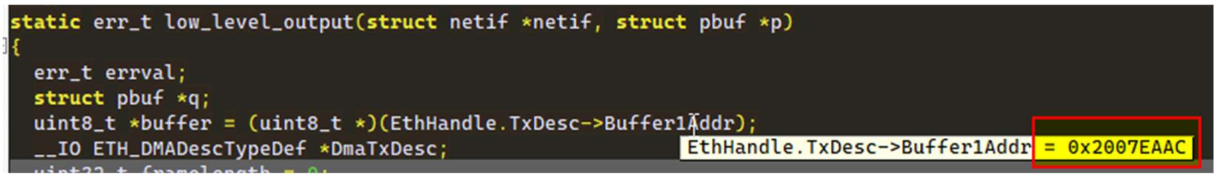


```
iecho      0x200003A8
  type     0x08
  code     0x00
  chksum   0x4557
  id       0xAFAF
  seqno    0x0A00
```

2. Eventually, inside lwip, the buffer address from the EthHandler is retrieved and the message content is copied to that address.

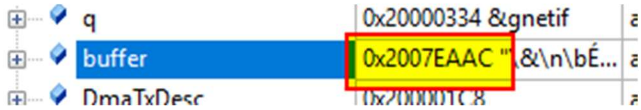
```
static err_t low_level_output(struct netif *netif, struct pbuf *p)
{
  err_t errval;
  struct pbuf *q;
  uint8_t *buffer = (uint8_t *)(EthHandle.TxDesc->Buffer1Addr);
```

3. Here the Address in the Debugger:



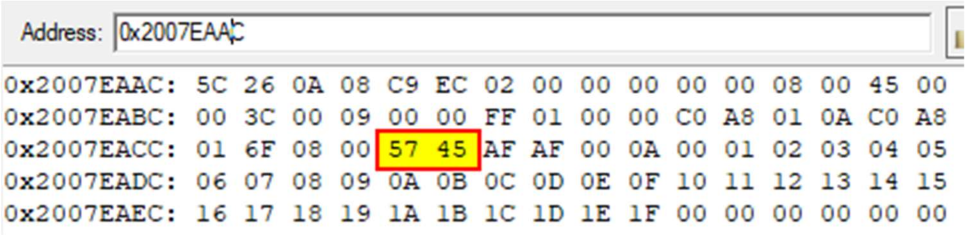
```
static err_t low_level_output(struct netif *netif, struct pbuf *p)
{
  err_t errval;
  struct pbuf *q;
  uint8_t *buffer = (uint8_t *)(EthHandle.TxDesc->Buffer1Addr);
  __IO ETH_DMADescTypeDef *DmaTxDesc;          EthHandle.TxDesc->Buffer1Addr = 0x2007EAAC
```

Assigned to buffer (pointer):



```
q          0x20000334 &gnetif
buffer     0x2007EAAC "\&\n\bÉ...
DmaTxDesc  0x200001C8
```

4. Memory view after the memcpy (yellow: the ICMP checksum):



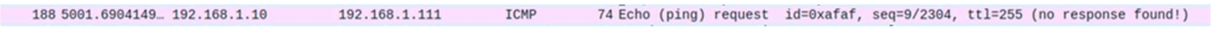
```
Address: 0x2007EAAC

0x2007EAAC: 5C 26 0A 08 C9 EC 02 00 00 00 00 00 08 00 45 00
0x2007EABC: 00 3C 00 09 00 00 FF 01 00 00 C0 A8 01 0A C0 A8
0x2007EACC: 01 6F 08 00 57 45 AF AF 00 0A 00 01 02 03 04 05
0x2007EADC: 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15
0x2007EAEC: 16 17 18 19 1A 1B 1C 1D 1E 1F 00 00 00 00 00 00
```

5. This Buffer / EthHandle is then passed to the HAL_ETH-Layer

In stm32f7xx_hal_eth.c: `HAL_ETH_TransmitFrame(&EthHandle, framelength);`

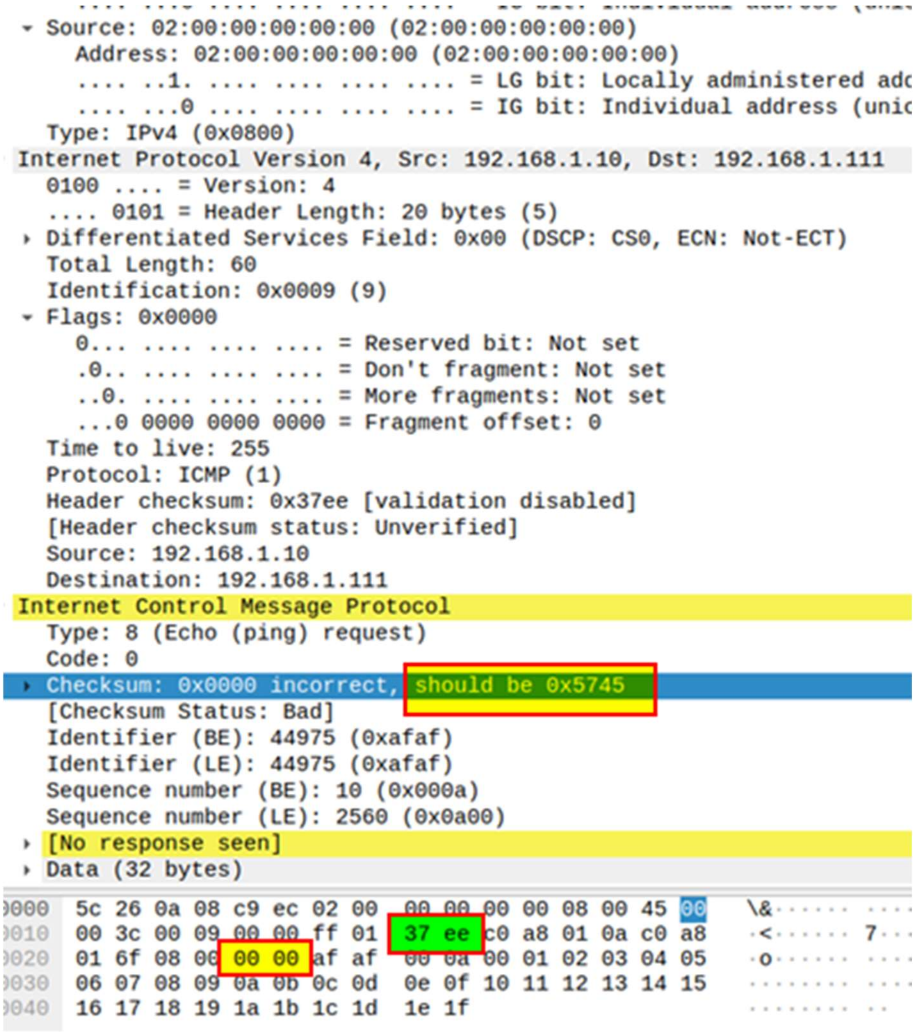
The function drives the DMA that eventually transmits the message to the Ethernet hardware.

6. This is what arrives on the computer (wireshark):



```
188 5001.6904149… 192.168.1.10          192.168.1.111         ICMP        74 Echo (ping) request  id=0xafaf, seq=9/2304, ttl=255 (no response found!)
```

- The checksum is 0x0000 (yellow)
- The IP packet checksum has been calculated

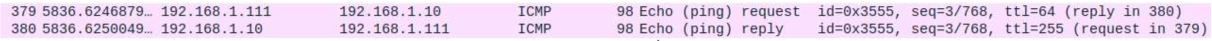


```
 ▾ Source: 02:00:00:00:00:00 (02:00:00:00:00:00)
     Address: 02:00:00:00:00:00 (02:00:00:00:00:00)
     .... ..1. .... .... .... .... = LG bit: Locally administered adc
     .... ...0 .... .... .... .... = IG bit: Individual address (unic
   Type: IPv4 (0x0800)
 Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.111
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 60
   Identification: 0x0009 (9)
 ▾ Flags: 0x0000
     0... .... .... .... = Reserved bit: Not set
     .0.. .... .... .... = Don't fragment: Not set
     ..0. .... .... .... = More fragments: Not set
     ...0 0000 0000 0000 = Fragment offset: 0
   Time to live: 255
   Protocol: ICMP (1)
   Header checksum: 0x37ee [validation disabled]
   [Header checksum status: Unverified]
   Source: 192.168.1.10
   Destination: 192.168.1.111
 Internet Control Message Protocol
   Type: 8 (Echo (ping) request)
   Code: 0
 ▸ Checksum: 0x0000 incorrect, should be 0x5745
   [Checksum Status: Bad]
   Identifier (BE): 44975 (0xafaf)
   Identifier (LE): 44975 (0xafaf)
   Sequence number (BE): 10 (0x000a)
   Sequence number (LE): 2560 (0x0a00)
 ▸ [No response seen]
 ▸ Data (32 bytes)

0000  5c 26 0a 08 c9 ec 02 00  00 00 00 00 08 00 45 00   \&······ ····
0010  00 3c 00 09 00 00 ff 01  37 ee c0 a8 01 0a c0 a8   ·<······ 7···
0020  01 6f 08 00 00 00 af af  00 0a 00 01 02 03 04 05   ·o······ ····
0030  06 07 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ········ ····
0040  16 17 18 19 1a 1b 1c 1d  1e 1f                     ········ ··
```

Vice Versa

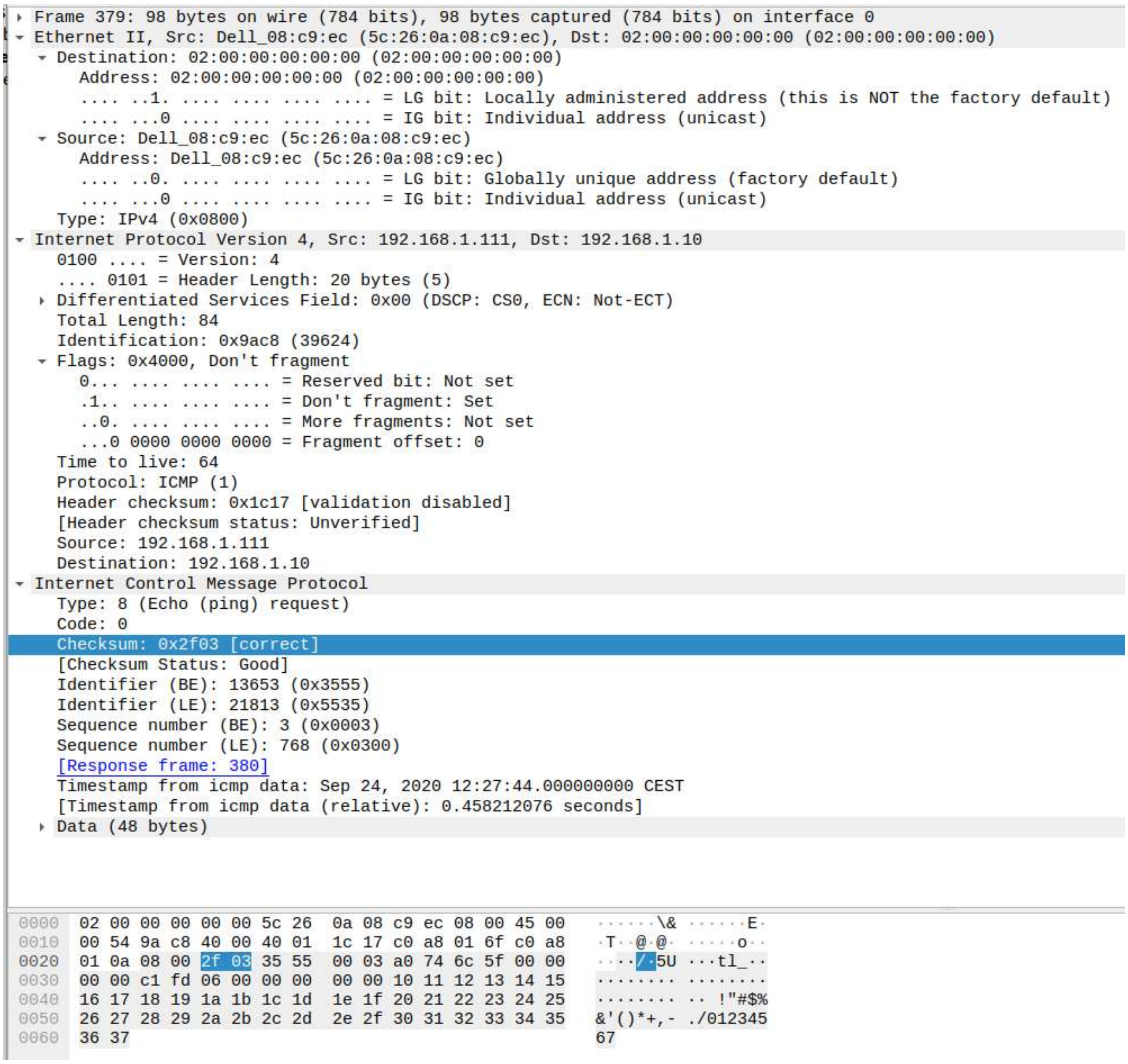
This is the opposite case:

The computer pings the Nucleo-Board, which perfectly answers.



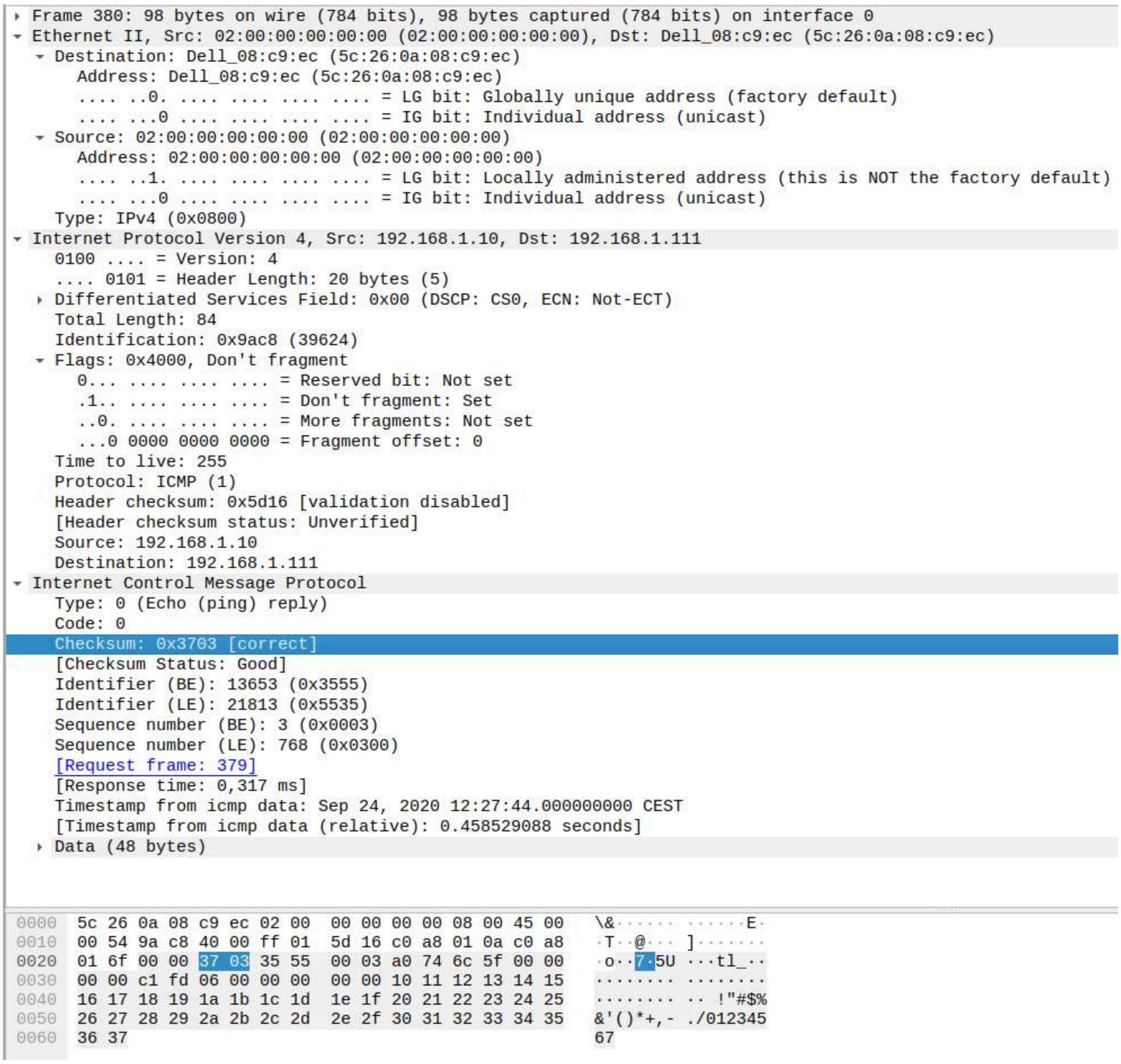
```
379 5836.6246879… 192.168.1.111         192.168.1.10          ICMP        98 Echo (ping) request  id=0x3555, seq=3/768, ttl=64 (reply in 380)
380 5836.6250049… 192.168.1.10          192.168.1.111         ICMP        98 Echo (ping) reply    id=0x3555, seq=3/768, ttl=255 (request in 379)
```

Request from computer



```
▸ Frame 379: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▾ Ethernet II, Src: Dell_08:c9:ec (5c:26:0a:08:c9:ec), Dst: 02:00:00:00:00:00 (02:00:00:00:00:00)
  ▾ Destination: 02:00:00:00:00:00 (02:00:00:00:00:00)
      Address: 02:00:00:00:00:00 (02:00:00:00:00:00)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: Dell_08:c9:ec (5c:26:0a:08:c9:ec)
      Address: Dell_08:c9:ec (5c:26:0a:08:c9:ec)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 192.168.1.111, Dst: 192.168.1.10
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x9ac8 (39624)
  ▾ Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x1c17 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.111
    Destination: 192.168.1.10
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x2f03 [correct]
    [Checksum Status: Good]
    Identifier (BE): 13653 (0x3555)
    Identifier (LE): 21813 (0x5535)
    Sequence number (BE): 3 (0x0003)
    Sequence number (LE): 768 (0x0300)
    [Response frame: 380]
    Timestamp from icmp data: Sep 24, 2020 12:27:44.000000000 CEST
    [Timestamp from icmp data (relative): 0.458212076 seconds]
  ▸ Data (48 bytes)

0000  02 00 00 00 00 00 5c 26  0a 08 c9 ec 08 00 45 00   ······\& ······E·
0010  00 54 9a c8 40 00 40 01  1c 17 c0 a8 01 6f c0 a8   ·T··@·@· ·····o··
0020  01 0a 08 00 2f 03 35 55  00 03 a0 74 6c 5f 00 00   ····/·5U ···tl_··
0030  00 00 c1 fd 06 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Answer from Nucleo: OK



```
▸ Frame 380: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▾ Ethernet II, Src: 02:00:00:00:00:00 (02:00:00:00:00:00), Dst: Dell_08:c9:ec (5c:26:0a:08:c9:ec)
  ▾ Destination: Dell_08:c9:ec (5c:26:0a:08:c9:ec)
      Address: Dell_08:c9:ec (5c:26:0a:08:c9:ec)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: 02:00:00:00:00:00 (02:00:00:00:00:00)
      Address: 02:00:00:00:00:00 (02:00:00:00:00:00)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.111
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x9ac8 (39624)
  ▾ Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x5d16 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.10
    Destination: 192.168.1.111
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x3703 [correct]
    [Checksum Status: Good]
    Identifier (BE): 13653 (0x3555)
    Identifier (LE): 21813 (0x5535)
    Sequence number (BE): 3 (0x0003)
    Sequence number (LE): 768 (0x0300)
    [Request frame: 379]
    [Response time: 0,317 ms]
    Timestamp from icmp data: Sep 24, 2020 12:27:44.000000000 CEST
    [Timestamp from icmp data (relative): 0.458529088 seconds]
  ▸ Data (48 bytes)

0000  5c 26 0a 08 c9 ec 02 00  00 00 00 00 08 00 45 00   \&······ ······E·
0010  00 54 9a c8 40 00 ff 01  5d 16 c0 a8 01 0a c0 a8   ·T··@··· ]·······
0020  01 6f 00 00 37 03 35 55  00 03 a0 74 6c 5f 00 00   ·o··7·5U ···tl_··
0030  00 00 c1 fd 06 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```