Asean-factori

3.2. Networks: Complements Wireshark

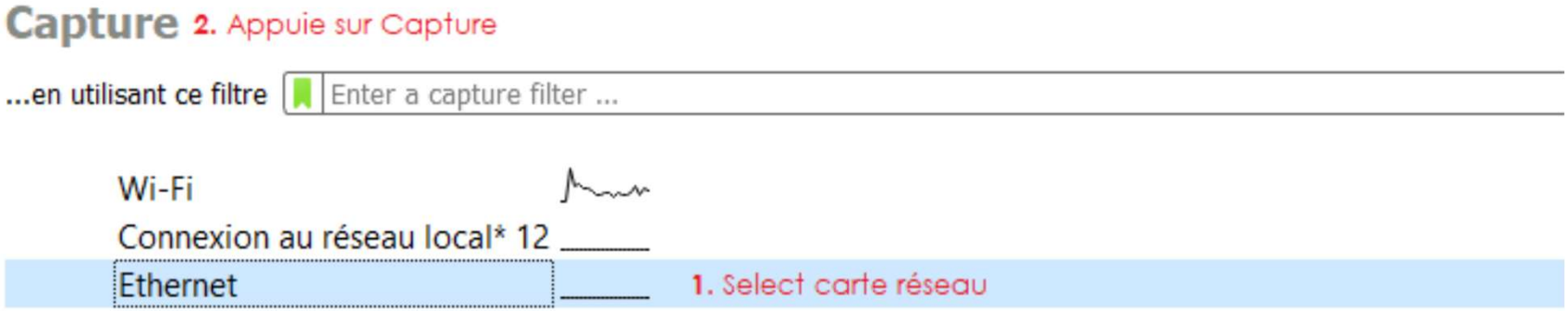
Jean-Marc THIRIET

jean-marc.thiriet@univ-grenoble-alpes.fr

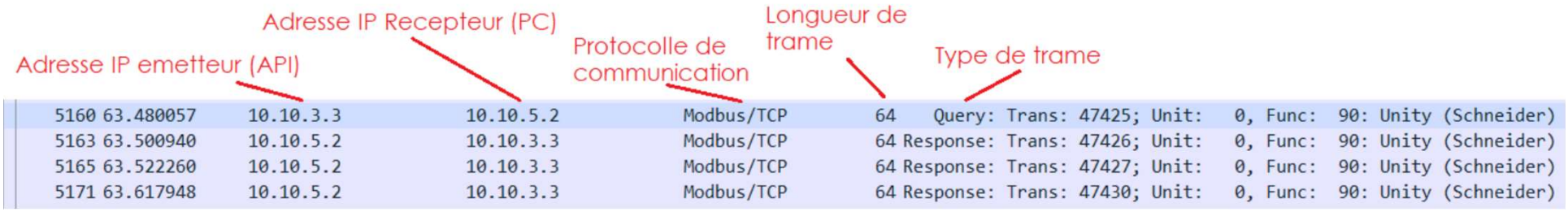
http://www.gipsa-lab.grenoble-inp.fr/~jean-marc.thiriet/asean/asean.html

Wireshark is a software to analyse networks packets (packet sniffer; layer 3)

- Step 1: starting the capture (choosing the interface)



- Step 2: View of a frame captured by Wireshark



Frame analysis

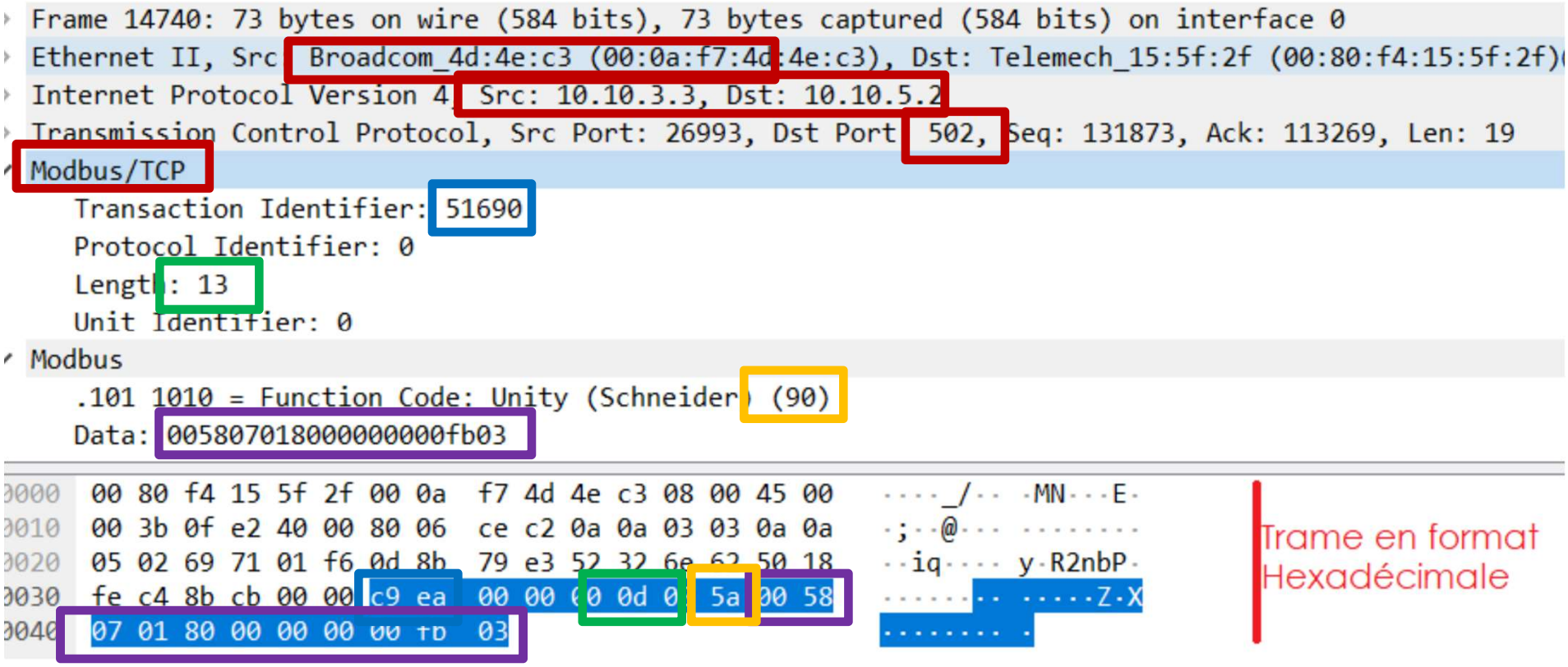
```
Frame 14740: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
Ethernet II, Src: Broadcom_4d:4e:c3 (00:0a:f7:4d:4e:c3), Dst: Telemech_15:5f:2f (00:80:f4:15:5f:2f)
Internet Protocol Version 4, Src: 10.10.3.3, Dst: 10.10.5.2
Transmission Control Protocol, Src Port: 26993, Dst Port: 502, Seq: 131873, Ack: 113269, Len: 19
Modbus/TCP
    Transaction Identifier: 51690
    Protocol Identifier: 0
    Length: 13
    Unit Identifier: 0
Modbus
    .101 1010 = Function Code: Unity (Schneider) (90)
    Data: 005807018000000000fb03
```

```
0000  00 80 f4 15 5f 2f 00 0a  f7 4d 4e c3 08 00 45 00   ····_/·· ·MN···E·
0010  00 3b 0f e2 40 00 80 06  ce c2 0a 0a 03 03 0a 0a   ·;··@··· ········
0020  05 02 69 71 01 f6 0d 8b  79 e3 52 32 6e 62 50 18   ··iq···· y·R2nbP·
0030  fe c4 8b cb 00 00 c9 ea  00 00 00 0d 00 5a 00 58   ········ ·····Z·X
0040  07 01 80 00 00 00 00 fb  03                       ········ ·
```

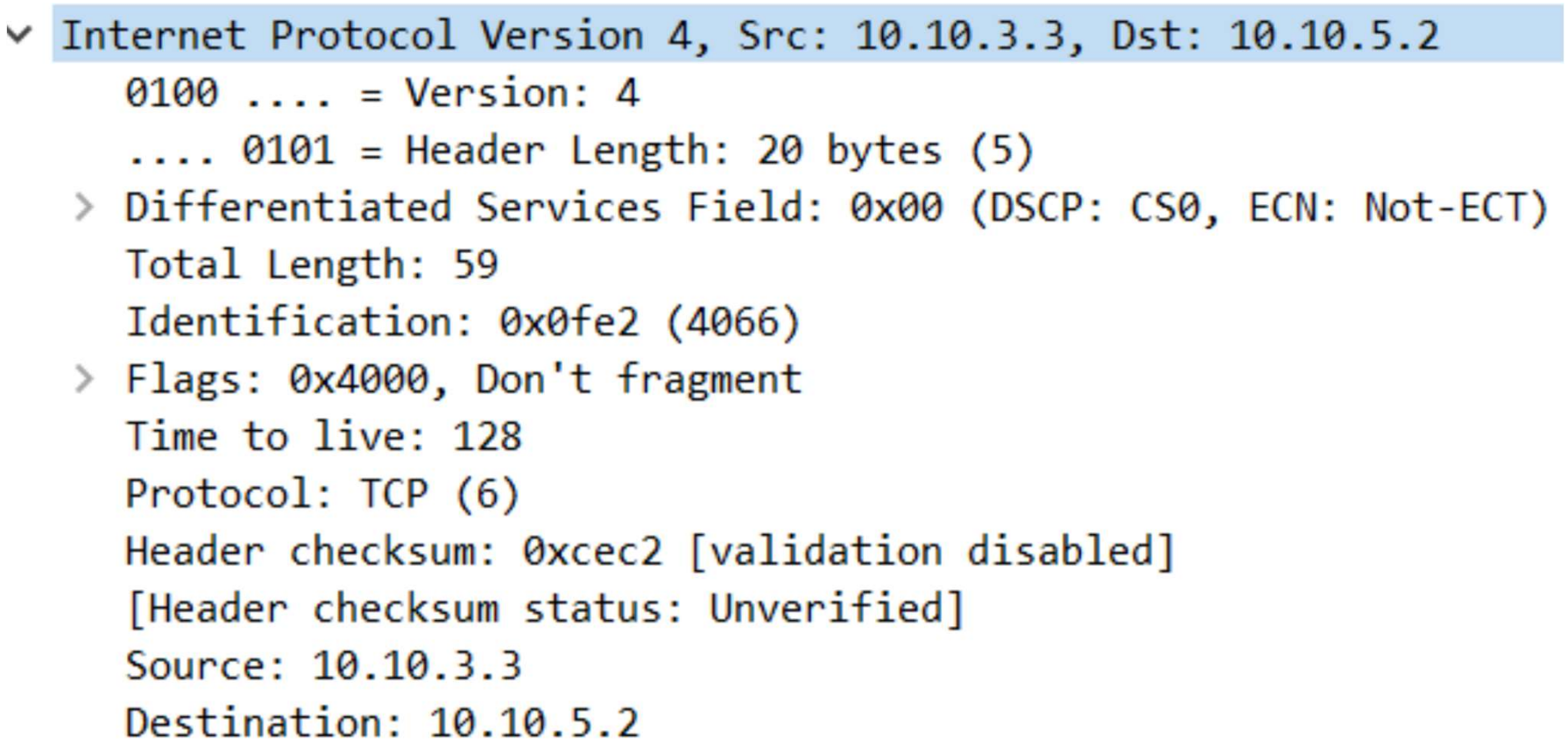
Trame en format Hexadécimale

Frame analysis

- 12(c)*16^3+9*16^2+14(e)*16+10(a)=51690
- 5*16+10(a)=90

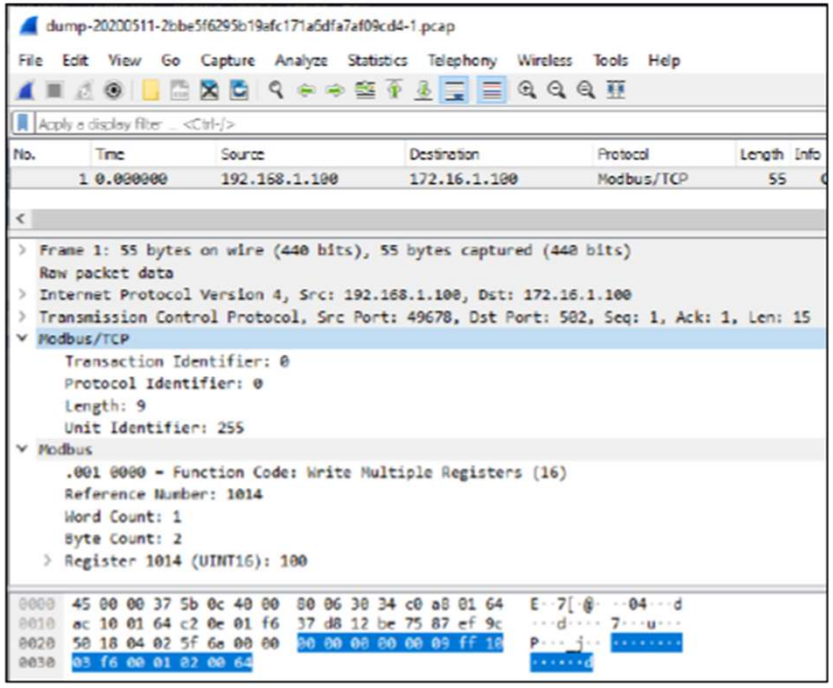


IP level (layer 3)



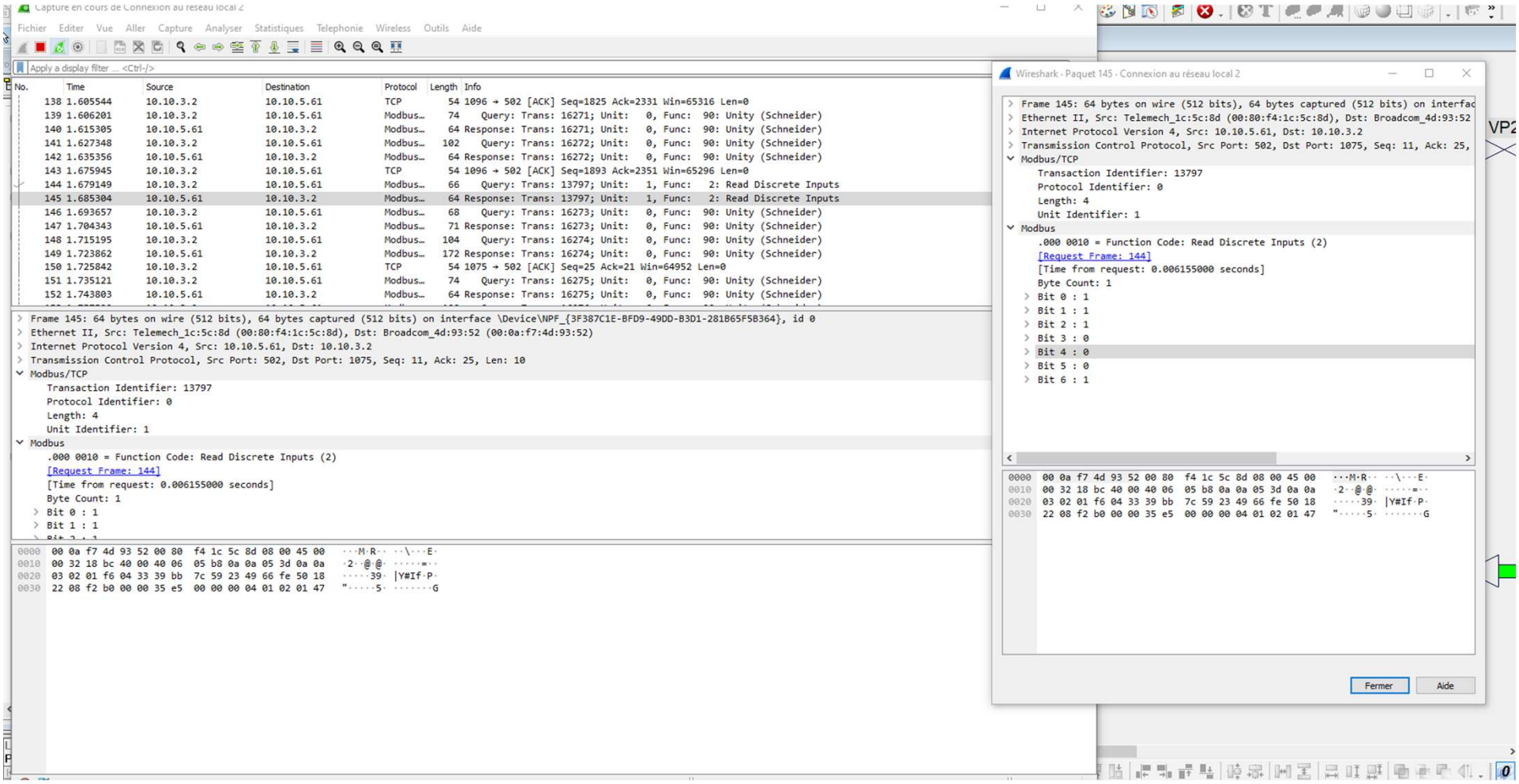
MODBUS TCP

- Wireshark décode complètement Modbus TCP



STORMSHIELD

10


Capture en cours de Connexion au réseau local 2
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
138 1.605544 10.10.3.2 10.10.5.61 TCP 54 1096 → 502 [ACK] Seq=1825 Ack=2331 Win=65316 Len=0
139 1.606201 10.10.3.2 10.10.5.61 Modbus… 74 Query: Trans: 16271; Unit: 0, Func: 90: Unity (Schneider)
140 1.615305 10.10.5.61 10.10.3.2 Modbus… 64 Response: Trans: 16271; Unit: 0, Func: 90: Unity (Schneider)
141 1.627348 10.10.3.2 10.10.5.61 Modbus… 102 Query: Trans: 16272; Unit: 0, Func: 90: Unity (Schneider)
142 1.635356 10.10.5.61 10.10.3.2 Modbus… 64 Response: Trans: 16272; Unit: 0, Func: 90: Unity (Schneider)
143 1.675945 10.10.3.2 10.10.5.61 TCP 54 1096 → 502 [ACK] Seq=1893 Ack=2351 Win=65296 Len=0
144 1.679149 10.10.3.2 10.10.5.61 Modbus… 66 Query: Trans: 13797; Unit: 1, Func: 2: Read Discrete Inputs
145 1.685304 10.10.5.61 10.10.3.2 Modbus… 64 Response: Trans: 13797; Unit: 1, Func: 2: Read Discrete Inputs
146 1.693657 10.10.3.2 10.10.5.61 Modbus… 68 Query: Trans: 16273; Unit: 0, Func: 90: Unity (Schneider)
147 1.704343 10.10.5.61 10.10.3.2 Modbus… 71 Response: Trans: 16273; Unit: 0, Func: 90: Unity (Schneider)
148 1.715195 10.10.3.2 10.10.5.61 Modbus… 104 Query: Trans: 16274; Unit: 0, Func: 90: Unity (Schneider)
149 1.723862 10.10.5.61 10.10.3.2 Modbus… 172 Response: Trans: 16274; Unit: 0, Func: 90: Unity (Schneider)
150 1.725842 10.10.3.2 10.10.5.61 TCP 54 1075 → 502 [ACK] Seq=25 Ack=21 Win=64952 Len=0
151 1.735121 10.10.3.2 10.10.5.61 Modbus… 74 Query: Trans: 16275; Unit: 0, Func: 90: Unity (Schneider)
152 1.743803 10.10.5.61 10.10.3.2 Modbus… 64 Response: Trans: 16275; Unit: 0, Func: 90: Unity (Schneider)
Frame 145: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF_{3F387C1E-BFD9-49DD-B3D1-281B65F5B364}, id 0
Ethernet II, Src: Telemech_1c:5c:8d (00:80:f4:1c:5c:8d), Dst: Broadcom_4d:93:52 (00:0a:f7:4d:93:52)
Internet Protocol Version 4, Src: 10.10.5.61, Dst: 10.10.3.2
Transmission Control Protocol, Src Port: 502, Dst Port: 1075, Seq: 11, Ack: 25, Len: 10
Modbus/TCP
Transaction Identifier: 13797
Protocol Identifier: 0
Length: 4
Unit Identifier: 1
Modbus
.000 0010 = Function Code: Read Discrete Inputs (2)
[Request Frame: 144]
[Time from request: 0.006155000 seconds]
Byte Count: 1
Bit 0 : 1
Bit 1 : 1
0000 00 0a f7 4d 93 52 00 80 f4 1c 5c 8d 08 00 45 00
0010 00 32 18 bc 40 00 40 06 05 b8 0a 0a 05 3d 0a 0a
0020 03 02 01 f6 04 33 39 bb 7c 59 23 49 66 fe 50 18
0030 22 08 f2 b0 00 00 35 e5 00 00 00 04 01 02 01 47
Wireshark · Paquet 145 · Connexion au réseau local 2
Frame 145: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interfac
Ethernet II, Src: Telemech_1c:5c:8d (00:80:f4:1c:5c:8d), Dst: Broadcom_4d:93:52
Internet Protocol Version 4, Src: 10.10.5.61, Dst: 10.10.3.2
Transmission Control Protocol, Src Port: 502, Dst Port: 1075, Seq: 11, Ack: 25,
Modbus/TCP
Transaction Identifier: 13797
Protocol Identifier: 0
Length: 4
Unit Identifier: 1
Modbus
.000 0010 = Function Code: Read Discrete Inputs (2)
[Request Frame: 144]
[Time from request: 0.006155000 seconds]
Byte Count: 1
Bit 0 : 1
Bit 1 : 1
Bit 2 : 1
Bit 3 : 0
Bit 4 : 0
Bit 5 : 0
Bit 6 : 1
0000 00 0a f7 4d 93 52 00 80 f4 1c 5c 8d 08 00 45 00
0010 00 32 18 bc 40 00 40 06 05 b8 0a 0a 05 3d 0a 0a
0020 03 02 01 f6 04 33 39 bb 7c 59 23 49 66 fe 50 18
0030 22 08 f2 b0 00 00 35 e5 00 00 00 04 01 02 01 47
Fermer
Aide