

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>



<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)

Capture 2. Appuie sur Capture



- Step 2: View of a frame captured by Wireshark

Adresse IP émetteur (API)	Adresse IP Recepteur (PC)	Protocole de communication	Longueur de trame	Type de trame
5160 63.480057	10.10.3.3	10.10.5.2	Modbus/TCP	64 Query: Trans: 47425; Unit: 0, Func: 90: Unity (Schneider)
5163 63.500940	10.10.5.2	10.10.3.3	Modbus/TCP	64 Response: Trans: 47426; Unit: 0, Func: 90: Unity (Schneider)
5165 63.522260	10.10.5.2	10.10.3.3	Modbus/TCP	64 Response: Trans: 47427; Unit: 0, Func: 90: Unity (Schneider)
5171 63.617948	10.10.5.2	10.10.3.3	Modbus/TCP	64 Response: Trans: 47430; Unit: 0, Func: 90: Unity (Schneider)

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 58Z.X
0040	07 01 80 00 00 00 00 fb 03

Trame en format
Hexadécimale

Frame analysis

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

```

> 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 00 03  .....

```

Trame en format Hexadécimale

IP level (layer 3)

- ✓ Internet Protocol Version 4, Src: 10.10.3.3, Dst: 10.10.5.2
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 59
 - Identification: 0x0fe2 (4066)
 - > Flags: 0x4000, Don't fragment
 - Time to live: 128
 - Protocol: TCP (6)
 - Header checksum: 0xcec2 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 10.10.3.3
 - Destination: 10.10.5.2

MODBUS TCP

- Wireshark décode complètement Modbus TCP

dump-20200511-2bbe5f6295b19afc171a5dfa7af09cd4-1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <<Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	172.16.1.100	Modbus/TCP	55	

<

> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)

Raw packet data

- > Internet Protocol Version 4, Src: 192.168.1.100, Dst: 172.16.1.100
- > Transmission Control Protocol, Src Port: 49678, Dst Port: 502, Seq: 1, Ack: 1, Len: 15
- ▼ Modbus/TCP
 - Transaction Identifier: 0
 - Protocol Identifier: 0
 - Length: 9
 - Unit Identifier: 255
- ▼ Modbus
 - .001 0000 - Function Code: Write Multiple Registers (16)
 - Reference Number: 1014
 - Word Count: 1
 - Byte Count: 2
 - > Register 1014 (UINT16): 100

```

0000 45 00 00 37 5b 0c 40 00 80 06 30 34 c0 a8 01 64  E-7[ @ --04--d
0010 ac 10 01 64 c2 0e 01 f6 37 d8 12 be 75 87 ef 9c  --d--- 7---u---
0020 50 18 04 02 5f 6e 00 00 00 00 00 00 ff 18  P---j--- .....
0030 03 f6 00 01 02 00 64  .....d
  
```

The screenshot displays the Wireshark interface with a packet capture of a Modbus communication. The main packet list shows a Modbus query (Frame 145) and its corresponding response (Frame 146). The packet details pane for Frame 145 shows a Modbus/TCP packet with Transaction Identifier 13797, Protocol Identifier 0, and Unit Identifier 1. The Modbus data field indicates a 'Read Discrete Inputs' request (Function Code 01) for 1 bit.

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)

Packet 145 Details:

- 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
 - Bit 2 : 1
 - Bit 3 : 0
 - Bit 4 : 0
 - Bit 5 : 0
 - Bit 6 : 1

Packet 146 Details:

- Frame 146: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{3F387C1E-BFD9-49DD-B3D1-281B65F5B364}, id 0
- Ethernet II, Src: Broadcom_4d:93:52 (00:0a:f7:4d:93:52), Dst: Telemech_1c:5c:8d (00:80:f4:1c:5c:8d)
- Internet Protocol Version 4, Src: 10.10.3.2, Dst: 10.10.5.61
- Transmission Control Protocol, Src Port: 1075, Dst Port: 502, Seq: 25, Ack: 11, Len: 10
- Modbus/TCP
 - Transaction Identifier: 13797
 - Protocol Identifier: 0
 - Length: 4
 - Unit Identifier: 1
- Modbus
 - .000 0010 = Function Code: Read Discrete Inputs (2)
 - [Response Frame: 145]
 - [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