

GET_CON

The screenshot shows a Wireshark interface titled "Capturing from tun0 (as superuser)". The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capturing, analyzing, and displaying packets.

The main display area shows a list of captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	aaaa::1	aaaa::212:4b00:1205:2269	CoAP	65	CON, MID:22637, GET, End of Block #0, /test/hello
2	0.272405277	aaaa::212:4b00:1205:2269	aaaa::1	CoAP	70	ACK, MID:22637, 2.05 Content, End of Block #0
3	257.236438...	aaaa::1	aaaa::212:4b00:1205:2269	CoAP	67	CON, MID:58611, POST, /led/red/toggle
4	258.229415...	aaaa::212:4b00:1205:2269	aaaa::1	CoAP	52	ACK, MID:58611, 2.05 Content

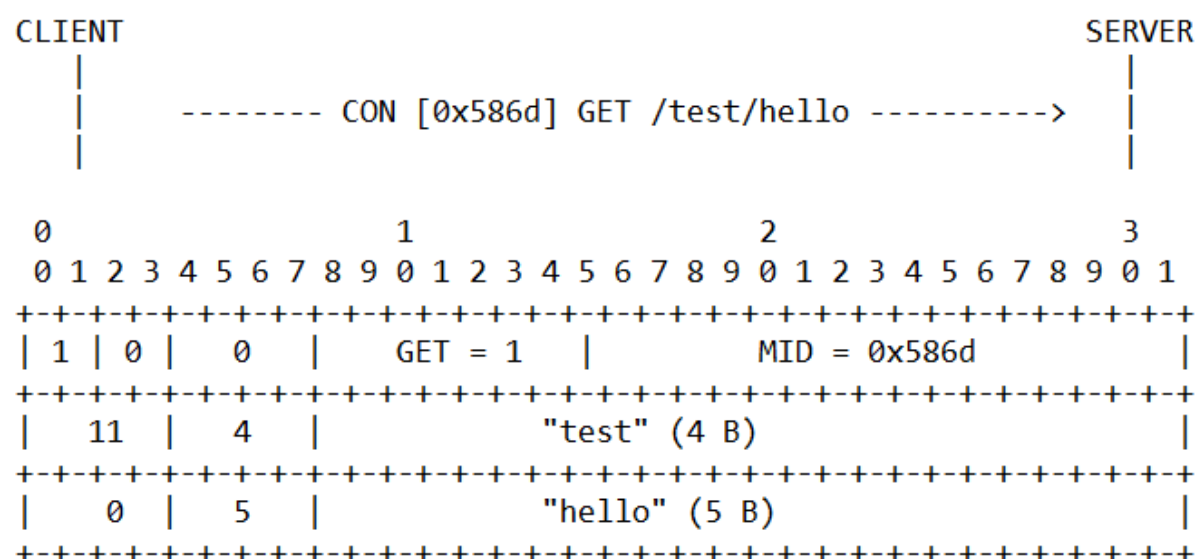
The selected packet (No. 1) is expanded, showing the following details:

- Frame 1:** 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface 0
- Raw packet data**
- Internet Protocol Version 6,** Src: aaaa::1, Dst: aaaa::212:4b00:1205:2269
- User Datagram Protocol,** Src Port: 45360, Dst Port: 5683
- Constrained Application Protocol,** Confirmable, GET, MID:22637
 - 01... = Version: 1
 - ..00 = Type: Confirmable (0)
 - 0000 = Token Length: 0
 - Code: GET (1)
 - Message ID: 22637
 - Opt Name: #1: Uri-Path: test
 - Opt Desc: Type 11, Critical, Unsafe
 - 1011 = Opt Delta: 11
 - 0100 = Opt Length: 4
 - Uri-Path: test
 - Opt Name: #2: Uri-Path: hello
 - Opt Desc: Type 11, Critical, Unsafe
 - 0000 = Opt Delta: 0
 - 0101 = Opt Length: 5
 - Uri-Path: hello
 - Opt Name: #3: Block2: NUM:0, M:0, SZX:64
 - Opt Desc: Type 23, Critical, Unsafe
 - 1100 = Opt Delta: 12
 - 0001 = Opt Length: 1
 - Block Number: 0
 - 0... = More Flag: 0
 - Block Size: 64 (2 encoded)
 - [Uri-Path: /test/hello]

The bottom pane displays the raw packet data in hexadecimal and ASCII format:

```

0000  60 00 00 00 00 19 11 40 aa aa 00 00 00 00 00 00  @.....
0010  00 00 00 00 00 00 00 01 aa aa 00 00 00 00 00 00 
0020  02 12 4b 00 12 05 22 69 b1 30 16 33 00 19 f4 92  ..K...i -0-3...
0030  40 01 58 6d b4 74 65 73 74 05 68 65 6c 6c 6f c1  @Xm tes t.hello
0040  02
  
```



GET_ACK

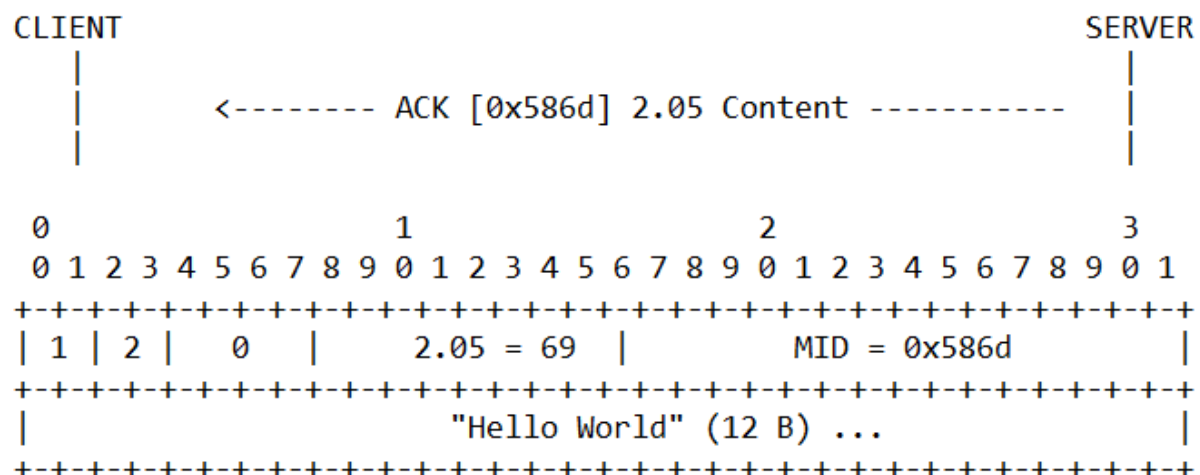
The image shows a Wireshark packet capture analysis of an HTTP GET request and response. The top pane displays a list of four packets. The second packet, at time 0.272405277, is a CoAP message from source address ::212:4b00:1205:2269 to destination address ::1. The third packet, at time 0.257236438, is a CoAP message from source address ::1 to destination address ::212:4b00:1205:2269. The fourth packet, at time 0.258229415, is a CoAP message from source address ::212:4b00:1205:2269 to destination address ::1.

The middle pane shows the details of the selected packet (Frame 2). It is a CoAP message of type Acknowledgement (2). The token length is 0. The code is 2.05 Content (69). The message ID is 22637. The options include:

- Opt Name: #1: Etag: 0c
 - Opt Desc: Type 4, Elective, Safe
 - 0100 = Opt Delta: 4
 - 0001 = Opt Length: 1
 - Etag: 0c
- Opt Name: #2: Content-Format: text/plain; charset=utf-8
 - Opt Desc: Type 12, Elective, Safe
 - 1000 = Opt Delta: 8
 - 0000 = Opt Length: 0
 - Content-type: text/plain; charset=utf-8
- Opt Name: #3: Block2: NUM:0, M:0, SZX:32
 - Opt Desc: Type 23, Critical, Unsafe
 - 1011 = Opt Delta: 11
 - 0001 = Opt Length: 1
 - Block Number: 0
 - 0... = More Flag: 0
 - Block Size: 32 (1 encoded)
 - End of options marker: 255

The payload is a text/plain message with a length of 12 bytes. The content is "Hello World!".

The bottom pane shows the raw packet data in hexadecimal and ASCII. The ASCII column shows the text "Hello World!".



POST_CON

Capturing from tun0 (as superuser)

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

Apply a display filter ... <Ctrl-/>

Express

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	aaaa::1	aaaa::212:4b00:1205:2269	CoAP	65	CON, MID:22637, GET, End of Block
2	0.272405277	aaaa::212:4b00:1205:2269	aaaa::1	CoAP	70	ACK, MID:22637, 2.05 Content, End
3	257.236438...	aaaa::1	aaaa::212:4b00:1205:2269	CoAP	67	CON, MID:58611, POST, /led/red/tog
4	258.229415...	aaaa::212:4b00:1205:2269	aaaa::1	CoAP	52	ACK, MID:58611, 2.05 Content

Frame 3: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0

Raw packet data

Internet Protocol Version 6, Src: aaaa::1, Dst: aaaa::212:4b00:1205:2269

User Datagram Protocol, Src Port: 45258, Dst Port: 5683

Constrained Application Protocol, Confirmable, POST, MID:58611

01... = Version: 1

..00... = Type: Confirmable (0)

.... 0000 = Token Length: 0

Code: POST (2)

Message ID: 58611

Opt Name: #1: Uri-Path: led

Opt Desc: Type 11, Critical, Unsafe

1011... = Opt Delta: 11

.... 0011 = Opt Length: 3

Uri-Path: led

Opt Name: #2: Uri-Path: red

Opt Desc: Type 11, Critical, Unsafe

0000... = Opt Delta: 0

.... 0011 = Opt Length: 3

Uri-Path: red

Opt Name: #3: Uri-Path: toggle

Opt Desc: Type 11, Critical, Unsafe

0000... = Opt Delta: 0

.... 0110 = Opt Length: 6

Uri-Path: toggle

[Uri-Path: /led/red/toggle]

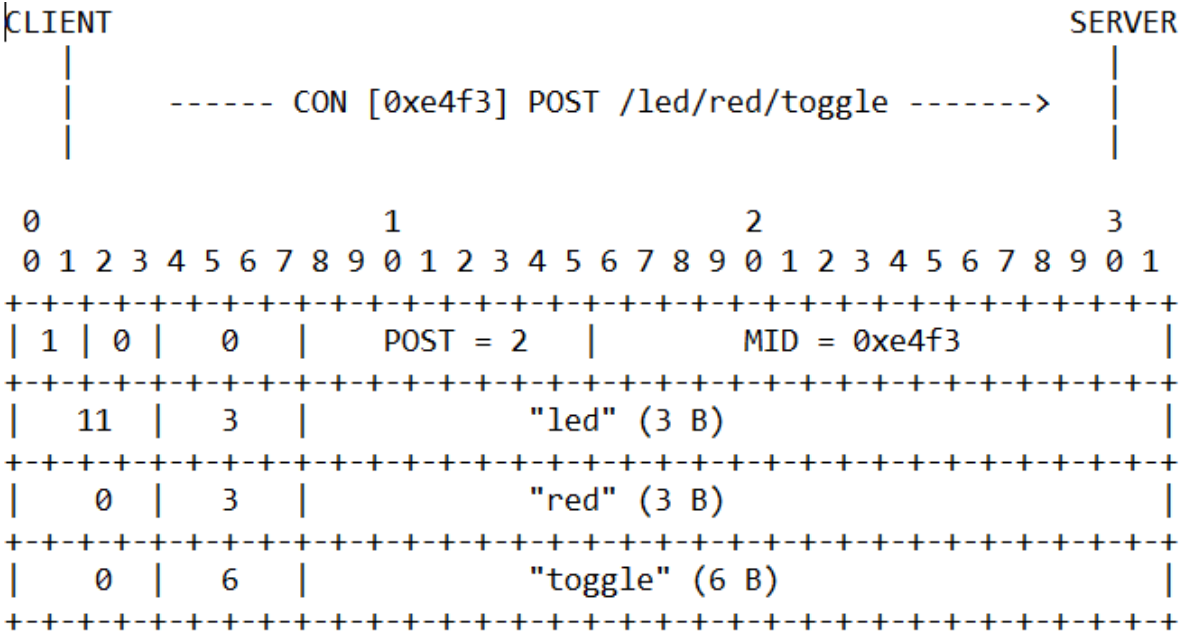
0000 60 00 00 00 00 1b 11 40 aa aa 00 00 00 00 00 00@.....

0010 00 00 00 00 00 00 00 01 aa aa 00 00 00 00 00 00K.....

0020 02 12 4b 00 12 05 22 69 b0 ca 16 33 00 1b 78 fe @...led...red-tog

0030 40 02 e4 f3 b3 6c 65 64 03 72 65 64 06 74 6f 67 @...led...red-tog

0040 67 6c 65 gle



The screenshot shows the Wireshark network protocol analyzer interface. The title bar reads "Capturing from tun0 (as user)". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, packet selection, and zooming.

A filter bar at the top contains the text "Apply a display filter ... <Ctrl-/>" and a search icon. To its right is a field labeled "Expression..." with a plus sign.

The main packet list pane displays four captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	aaaa::1	aaaa::212:4b00:1205:2269	CoAP	65	CON, MID:22637, GET, End of Block #0, /test/hej
2	0.272405277	aaaa::212:4b00:1205:2269	aaaa::1	CoAP	70	ACK, MID:22637, 2.05 Content, End of Block #0 (
3	257.236438...	aaaa::1	aaaa::212:4b00:1205:2269	CoAP	67	CON, MID:58611, POST, /led/red/toggle
4	258.229415...	aaaa::212:4b00:1205:2269	aaaa::1	CoAP	52	ACK, MID:58611, 2.05 Content

Packets 1 through 3 are collapsed. Packet 4 is expanded, showing details:

- Frame 4: 52 bytes on wire (416 bits), 52 bytes captured (416 bits) on interface 0
- Raw packet data
- Internet Protocol Version 6, Src: aaaa::212:4b00:1205:2269, Dst: aaaa::1
- User Datagram Protocol, Src Port: 5683, Dst Port: 45258
- Constrained Application Protocol, Acknowledgement, 2.05 Content, MID:58611**
 - 01.. = Version: 1
 - ...10 = Type: Acknowledgement (2)
 - 0000 = Token Length: 0
 - Code: 2.05 Content (69)
 - Message ID: 58611

The bottom pane shows the hex dump of the selected packet (packet 4):

```

0000  60 00 00 00 00 0c 11 3f aa aa 00 00 00 00 00 00  ~.....? .....
0010  02 12 4b 00 12 05 22 69 aa aa 00 00 00 00 00 00  ..K..."i .....
0020  00 00 00 00 00 00 00 01 16 33 b0 ca 00 0c 1c c9  .....3.....
0030  60 45 e4 f3                                     E..
  
```

