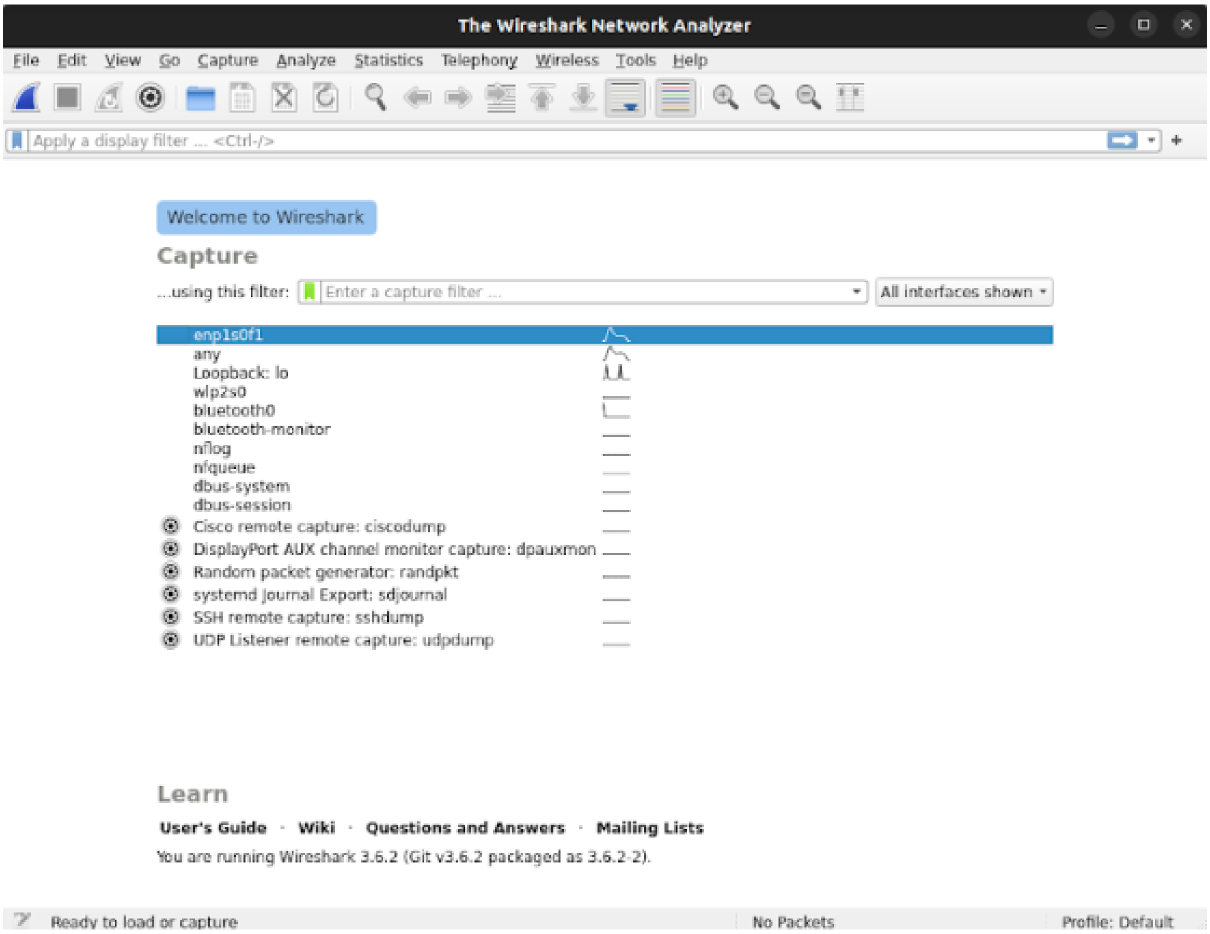
Experiment 7

Output:

Nonprimiscous mode: a screenshot of Wireshark.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

Welcome to Wireshark

Capture

…using this filter: Enter a capture filter … All interfaces shown

```
enp1s0f1
any
Loopback: lo
wlp2s0
bluetooth0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
```

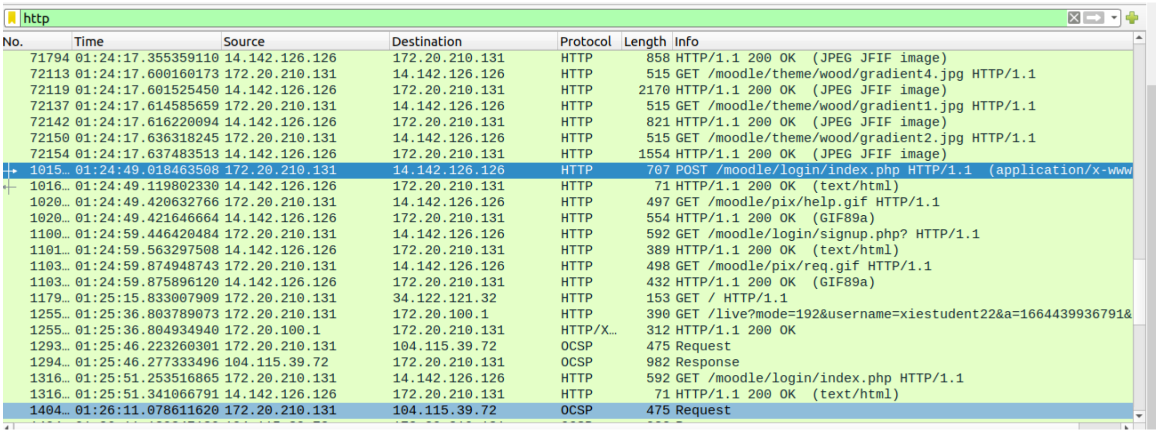
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

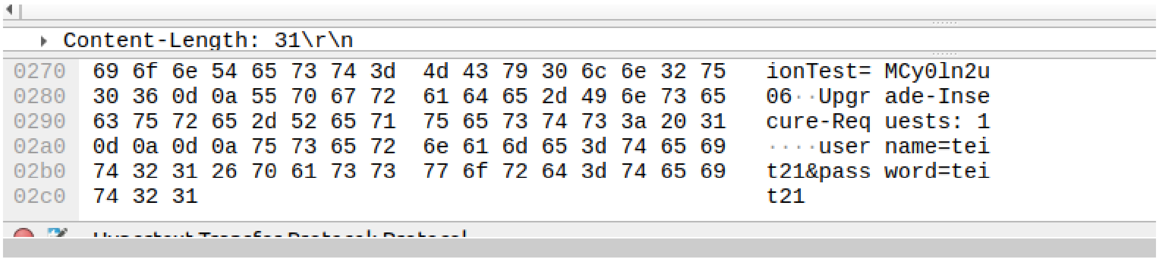
You are running Wireshark 3.6.2 (Git v3.6.2 packaged as 3.6.2-2).

Ready to load or capture   No Packets   Profile: Default

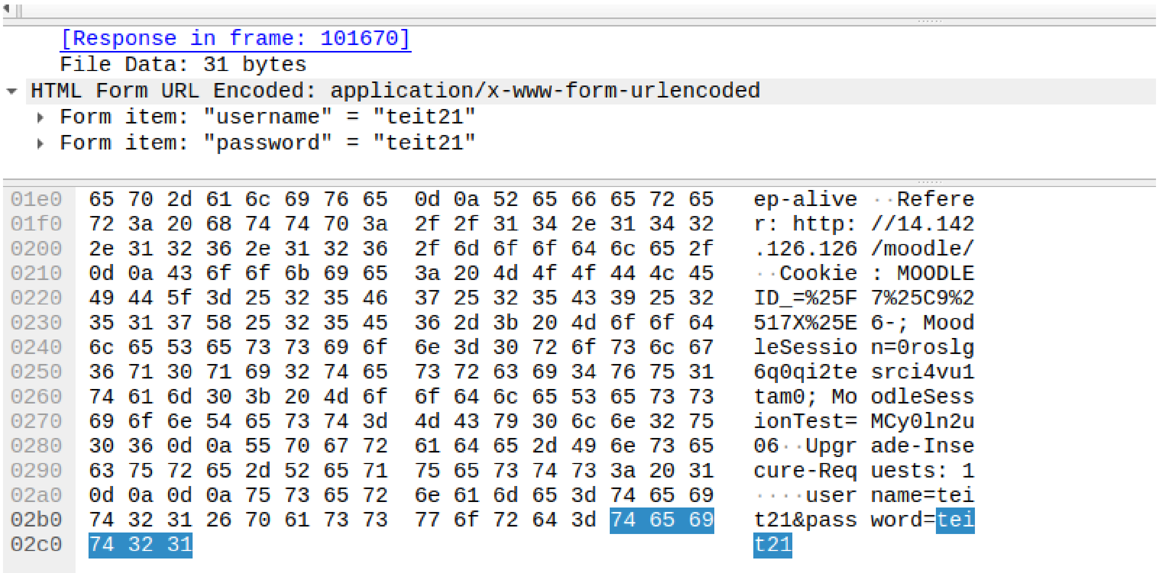
Primiscous mode :http :go to ip address



```
http
No.   Time               Source         Destination     Protocol Length Info
71794 01:24:17.355359110 14.142.126.126 172.20.210.131  HTTP      858 HTTP/1.1 200 OK  (JPEG JFIF image)
72113 01:24:17.600160173 172.20.210.131 14.142.126.126  HTTP      515 GET /moodle/theme/wood/gradient4.jpg HTTP/1.1
72119 01:24:17.601525450 14.142.126.126 172.20.210.131  HTTP     2170 HTTP/1.1 200 OK  (JPEG JFIF image)
72137 01:24:17.614585659 172.20.210.131 14.142.126.126  HTTP      515 GET /moodle/theme/wood/gradient1.jpg HTTP/1.1
72142 01:24:17.616220094 14.142.126.126 172.20.210.131  HTTP      821 HTTP/1.1 200 OK  (JPEG JFIF image)
72150 01:24:17.636318245 172.20.210.131 14.142.126.126  HTTP      515 GET /moodle/theme/wood/gradient2.jpg HTTP/1.1
72154 01:24:17.637483513 14.142.126.126 172.20.210.131  HTTP     1554 HTTP/1.1 200 OK  (JPEG JFIF image)
1015… 01:24:49.018463508 172.20.210.131 14.142.126.126  HTTP      707 POST /moodle/login/index.php HTTP/1.1  (application/x-www
1016… 01:24:49.119802330 14.142.126.126 172.20.210.131  HTTP       71 HTTP/1.1 200 OK  (text/html)
1020… 01:24:49.420632766 172.20.210.131 14.142.126.126  HTTP      497 GET /moodle/pix/help.gif HTTP/1.1
1020… 01:24:49.421646664 14.142.126.126 172.20.210.131  HTTP      554 HTTP/1.1 200 OK  (GIF89a)
1100… 01:24:59.446420484 172.20.210.131 14.142.126.126  HTTP      592 GET /moodle/login/signup.php? HTTP/1.1
1101… 01:24:59.563297508 14.142.126.126 172.20.210.131  HTTP      389 HTTP/1.1 200 OK  (text/html)
1103… 01:24:59.874948743 172.20.210.131 14.142.126.126  HTTP      498 GET /moodle/pix/req.gif HTTP/1.1
1103… 01:24:59.875896120 14.142.126.126 172.20.210.131  HTTP      432 HTTP/1.1 200 OK  (GIF89a)
1179… 01:25:15.833007909 172.20.210.131 34.122.121.32   HTTP      153 GET / HTTP/1.1
1255… 01:25:36.803789073 172.20.210.131 172.20.100.1    HTTP      390 GET /live?mode=192&username=xiestudent22&a=1664439936791&
1255… 01:25:36.804934940 172.20.100.1   172.20.210.131  HTTP/X…   312 HTTP/1.1 200 OK
1293… 01:25:46.223260301 172.20.210.131 104.115.39.72   OCSP      475 Request
1294… 01:25:46.277333496 104.115.39.72  172.20.210.131  OCSP      982 Response
1316… 01:25:51.253516865 172.20.210.131 14.142.126.126  HTTP      592 GET /moodle/login/index.php HTTP/1.1
1316… 01:25:51.341066791 14.142.126.126 172.20.210.131  HTTP       71 HTTP/1.1 200 OK  (text/html)
1404… 01:26:11.078611620 172.20.210.131 104.115.39.72   OCSP      475 Request
```

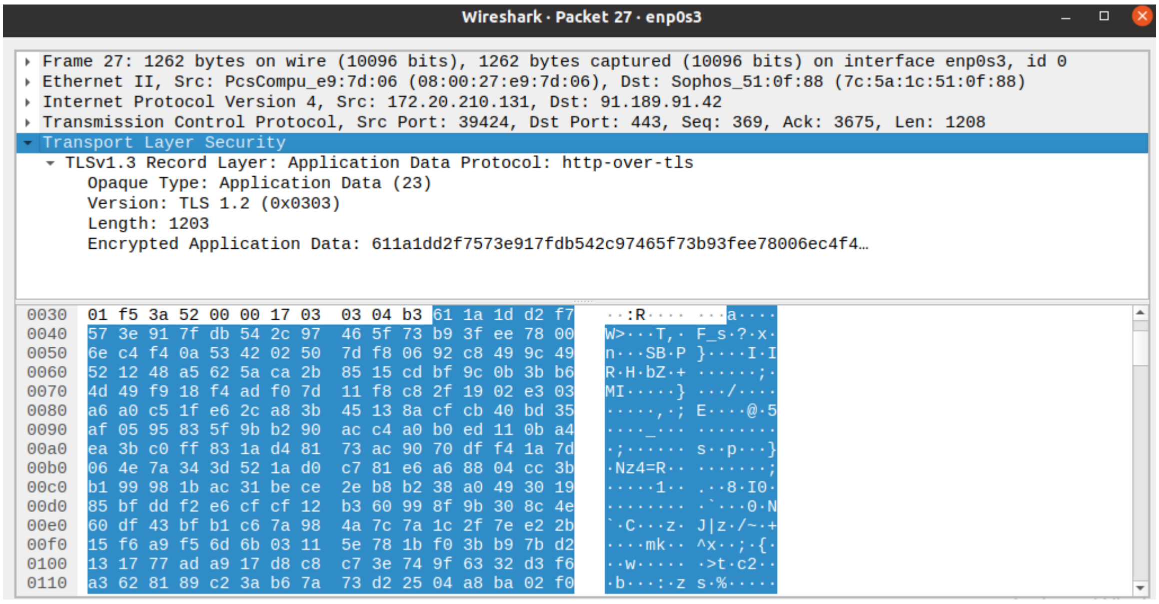


```
  Content-Length: 31\r\n
0270  69 6f 6e 54 65 73 74 3d  4d 43 79 30 6c 6e 32 75   ionTest= MCy0ln2u
0280  30 36 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   06··Upgr ade-Inse
0290  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31   cure-Req uests: 1
02a0  0d 0a 0d 0a 75 73 65 72  6e 61 6d 65 3d 74 65 69   ····user name=tei
02b0  74 32 31 26 70 61 73 73  77 6f 72 64 3d 74 65 69   t21&pass word=tei
02c0  74 32 31                                           t21
```

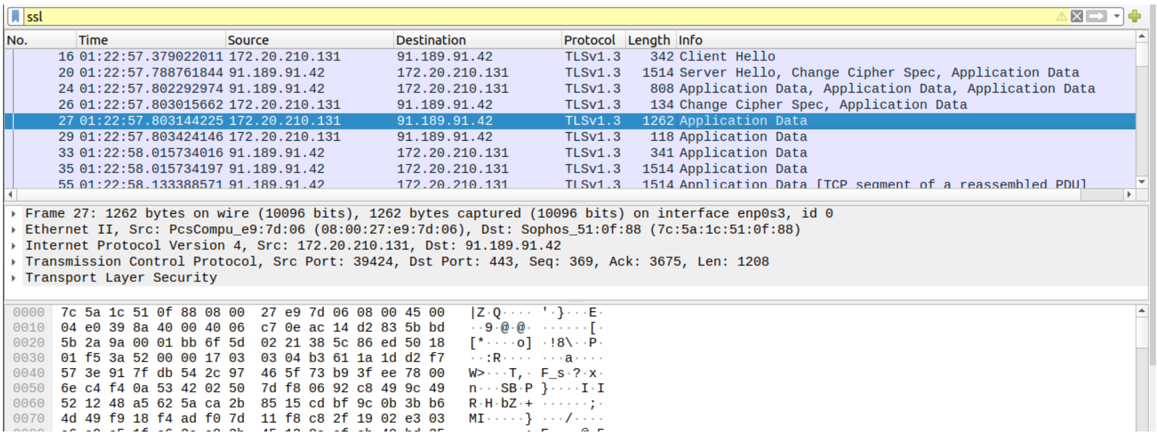


```
    [Response in frame: 101670]
    File Data: 31 bytes
 HTML Form URL Encoded: application/x-www-form-urlencoded
    Form item: "username" = "teit21"
    Form item: "password" = "teit21"

01e0  65 70 2d 61 6c 69 76 65  0d 0a 52 65 66 65 72 65   ep-alive ··Refere
01f0  72 3a 20 68 74 74 70 3a  2f 2f 31 34 2e 31 34 32   r: http: //14.142
0200  2e 31 32 36 2e 31 32 36  2f 6d 6f 6f 64 6c 65 2f   .126.126 /moodle/
0210  0d 0a 43 6f 6f 6b 69 65  3a 20 4d 4f 4f 44 4c 45   ··Cookie : MOODLE
0220  49 44 5f 3d 25 32 35 46  37 25 32 35 43 39 25 32   ID_=%25F 7%25C9%2
0230  35 31 37 58 25 32 35 45  36 2d 3b 20 4d 6f 6f 64   517X%25E 6-; Mood
0240  6c 65 53 65 73 73 69 6f  6e 3d 30 72 6f 73 6c 67   leSessio n=0roslg
0250  36 71 30 71 69 32 74 65  73 72 63 69 34 76 75 31   6q0qi2te srci4vu1
0260  74 61 6d 30 3b 20 4d 6f  6f 64 6c 65 53 65 73 73   tam0; Mo odleSess
0270  69 6f 6e 54 65 73 74 3d  4d 43 79 30 6c 6e 32 75   ionTest= MCy0ln2u
0280  30 36 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   06··Upgr ade-Inse
0290  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31   cure-Req uests: 1
02a0  0d 0a 0d 0a 75 73 65 72  6e 61 6d 65 3d 74 65 69   ····user name=tei
02b0  74 32 31 26 70 61 73 73  77 6f 72 64 3d 74 65 69   t21&pass word=tei
02c0  74 32 31                                           t21
```

https:ssl



```
 Frame 27: 1262 bytes on wire (10096 bits), 1262 bytes captured (10096 bits) on interface enp0s3, id 0
 Ethernet II, Src: PcsCompu_e9:7d:06 (08:00:27:e9:7d:06), Dst: Sophos_51:0f:88 (7c:5a:1c:51:0f:88)
 Internet Protocol Version 4, Src: 172.20.210.131, Dst: 91.189.91.42
 Transmission Control Protocol, Src Port: 39424, Dst Port: 443, Seq: 369, Ack: 3675, Len: 1208
 Transport Layer Security
   TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 1203
      Encrypted Application Data: 611a1dd2f7573e917fdb542c97465f73b93fee78006ec4f4…

0030  01 f5 3a 52 00 00 17 03  03 04 b3 61 1a 1d d2 f7   ··:R···· ···a····
0040  57 3e 91 7f db 54 2c 97  46 5f 73 b9 3f ee 78 00   W>···T,· F_s·?·x·
0050  6e c4 f4 0a 53 42 02 50  7d f8 06 92 c8 49 9c 49   n···SB·P }····I·I
0060  52 12 48 a5 62 5a ca 2b  85 15 cd bf 9c 0b 3b b6   R·H·bZ·+ ······;·
0070  4d 49 f9 18 f4 ad f0 7d  11 f8 c8 2f 19 02 e3 03   MI·····} ···/····
0080  a6 a0 c5 1f e6 2c a8 3b  45 13 8a cf cb 40 bd 35   ·····,·; E····@·5
0090  af 05 95 83 5f 9b b2 90  ac c4 a0 b0 ed 11 0b a4   ····_··· ········
00a0  ea 3b c0 ff 83 1a d4 81  73 ac 90 70 df f4 1a 7d   ·;······ s··p···}
00b0  06 4e 7a 34 3d 52 1a d0  c7 81 e6 a6 88 04 cc 3b   ·Nz4=R·· ·······;
00c0  b1 99 98 1b ac 31 be ce  2e b8 b2 38 a0 49 30 19   ·····1·· .··8·I0·
00d0  85 bf dd f2 e6 cf cf 12  b3 60 99 8f 9b 30 8c 4e   ········ ·`···0·N
00e0  60 df 43 bf b1 c6 7a 98  4a 7c 7a 1c 2f 7e e2 2b   `·C···z· J|z·/~·+
00f0  15 f6 a9 f5 6d 6b 03 11  5e 78 1b f0 3b b9 7b d2   ····mk·· ^x··;·{·
0100  13 17 77 ad a9 17 d8 c8  c7 3e 74 9f 63 32 d3 f6   ··w····· ·>t·c2··
0110  a3 62 81 89 c2 3a b6 7a  73 d2 25 04 a8 ba 02 f0   ·b···:·z s·%·····
```



```
No.   Time               Source         Destination    Protocol Length Info
   16 01:22:57.379022011 172.20.210.131 91.189.91.42   TLSv1.3   342 Client Hello
   20 01:22:57.788761844 91.189.91.42   172.20.210.131 TLSv1.3  1514 Server Hello, Change Cipher Spec, Application Data
   24 01:22:57.802292974 91.189.91.42   172.20.210.131 TLSv1.3   808 Application Data, Application Data, Application Data
   26 01:22:57.803015662 172.20.210.131 91.189.91.42   TLSv1.3   134 Change Cipher Spec, Application Data
   27 01:22:57.803144225 172.20.210.131 91.189.91.42   TLSv1.3  1262 Application Data
   29 01:22:57.803424146 172.20.210.131 91.189.91.42   TLSv1.3   118 Application Data
   33 01:22:58.015734016 91.189.91.42   172.20.210.131 TLSv1.3   341 Application Data
   35 01:22:58.015734197 91.189.91.42   172.20.210.131 TLSv1.3  1514 Application Data
   55 01:22:58.133388571 91.189.91.42   172.20.210.131 TLSv1.3  1514 Application Data [TCP segment of a reassembled PDU]
```

```
▸ Frame 27: 1262 bytes on wire (10096 bits), 1262 bytes captured (10096 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_e9:7d:06 (08:00:27:e9:7d:06), Dst: Sophos_51:0f:88 (7c:5a:1c:51:0f:88)
▸ Internet Protocol Version 4, Src: 172.20.210.131, Dst: 91.189.91.42
▸ Transmission Control Protocol, Src Port: 39424, Dst Port: 443, Seq: 369, Ack: 3675, Len: 1208
▸ Transport Layer Security
```

```
0000  7c 5a 1c 51 0f 88 08 00  27 e9 7d 06 08 00 45 00   |Z·Q····  '·}···E·
0010  04 e0 39 8a 40 00 40 06  c7 0e ac 14 d2 83 5b bd   ··9·@·@·  ······[·
0020  5b 2a 9a 00 01 bb 6f 5d  02 21 38 5c 86 ed 50 18   [*····o]  ·!8\··P·
0030  01 f5 3a 52 00 00 17 03  03 04 b3 61 1a 1d d2 f7   ··:R····  ···a····
0040  57 3e 91 7f db 54 2c 97  46 5f 73 b9 3f ee 78 00   W>···T,·  F_s·?·x·
0050  6e c4 f4 0a 53 42 02 50  7d f8 06 92 c8 49 9c 49   n···SB·P  }····I·I
0060  52 12 48 a5 62 5a ca 2b  85 15 cd bf 9c 0b 3b b6   R·H·bZ·+  ······;·
0070  4d 49 f9 18 f4 ad f0 7d  11 f8 c8 2f 19 02 e3 03   MI·····}  ···/····
```