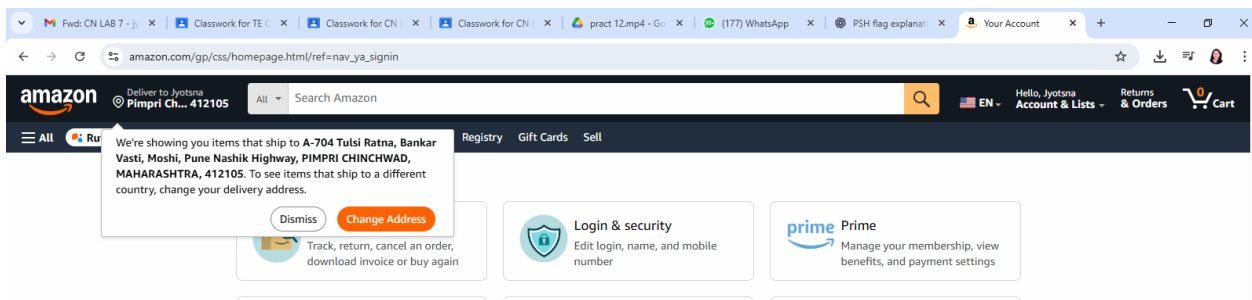


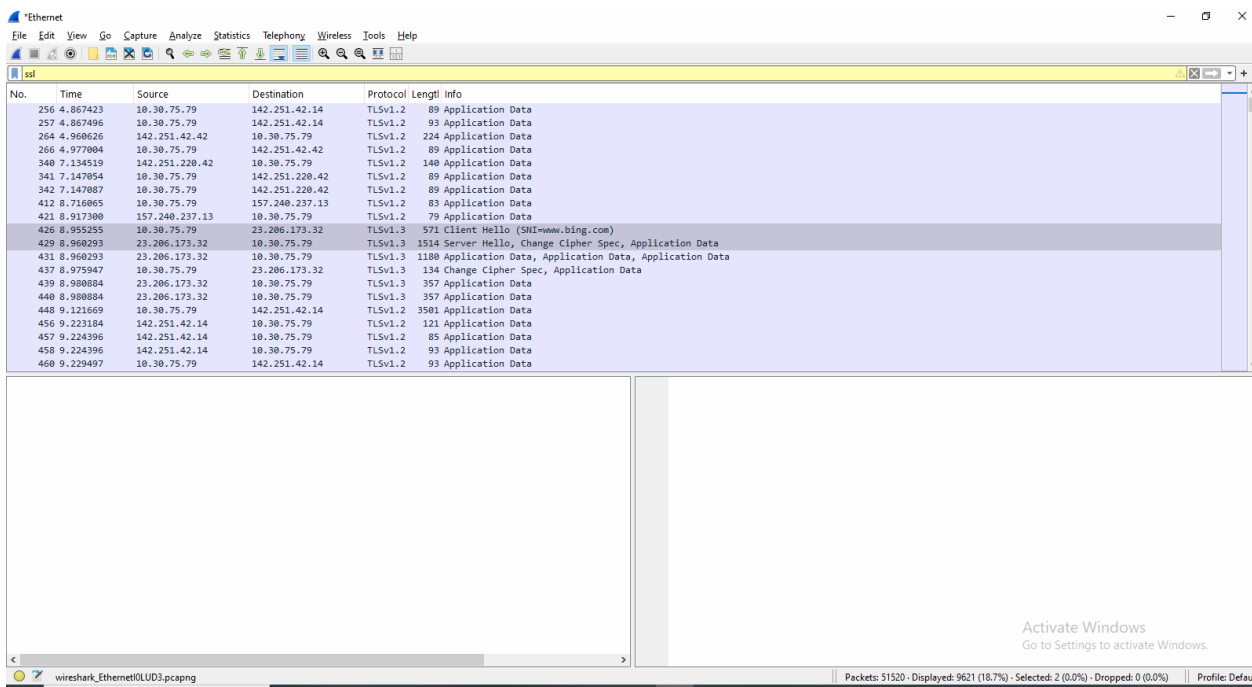
12. To study the SSL protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e-commerce etc.).

1. Open Wireshark first

2. Open Amazon and login



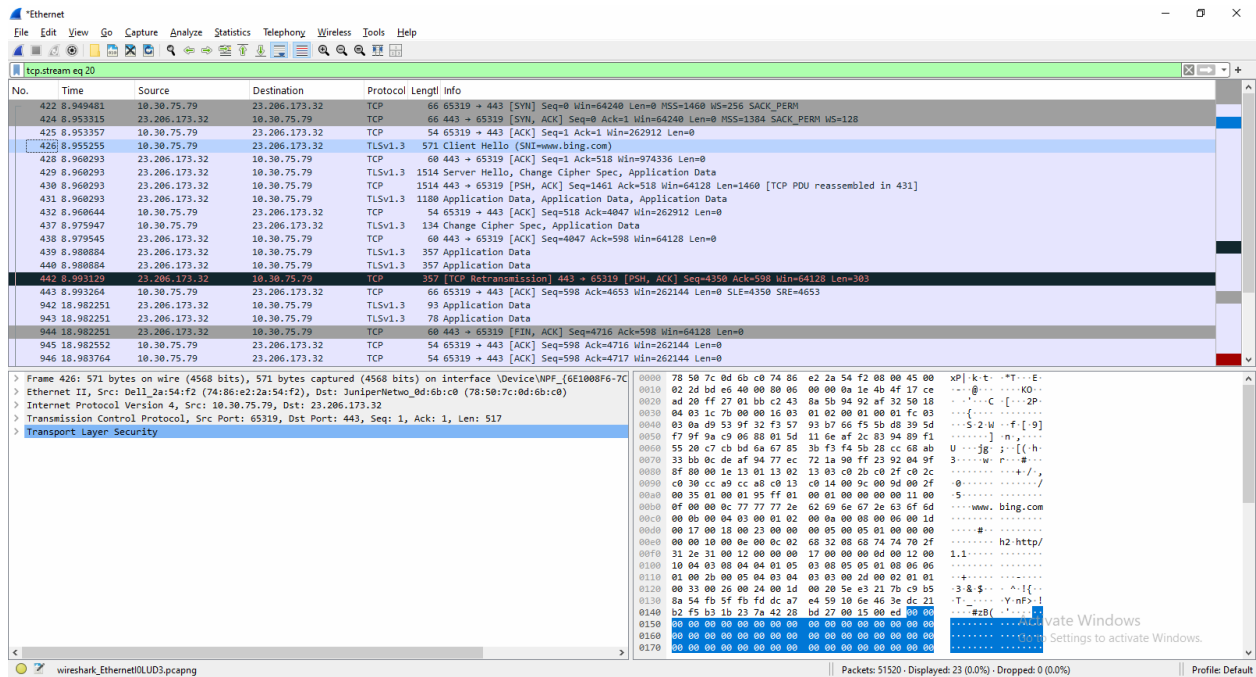
3. Stop packet capturing on Wireshark



4. Right click on → Client hello → follow → TLS Stream → you will get a popup close that

by doing this you will get one command on Wireshark as follows

tcp.stream eq 20



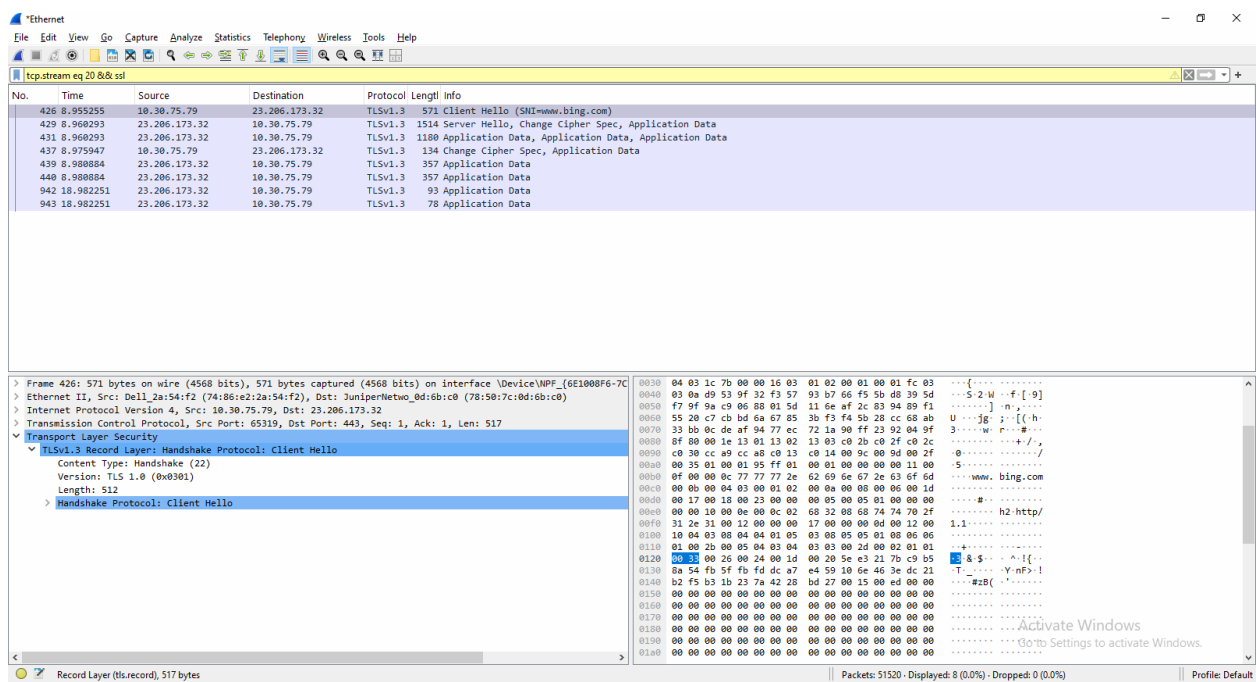
The image shows a Wireshark packet capture of a TCP stream (eq 20). The packet list on the left shows a sequence of packets from 422 to 946. The packet details pane on the right shows the structure of the captured data, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Transport Layer Security (TLS).

Packet 426 (751 bytes) is highlighted, showing the following details:

- Frame 426: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{6E1008F6-7C} (78:50:7c:0d:6b:c0)
- Ethernet II, Src: Dell_2a:54:f2 (74:8b:e2:2a:54:f2), Dst: JuniperNetwo_0d:6b:c0 (78:50:7c:0d:6b:c0)
- Internet Protocol Version 4, Src: 10.30.75.79, Dst: 23.206.173.32
- Transmission Control Protocol, Src Port: 65319, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
- Transport Layer Security

The packet bytes pane on the right shows the raw data of the captured packet, including the TLS record structure.

5. tcp.stream eq 20 && ssl



The image shows a Wireshark packet capture of a TCP stream (eq 20 && ssl). The packet list on the left shows a sequence of packets from 426 to 943. The packet details pane on the right shows the structure of the captured data, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Transport Layer Security (TLS).

Packet 426 (751 bytes) is highlighted, showing the following details:

- Frame 426: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{6E1008F6-7C} (78:50:7c:0d:6b:c0)
- Ethernet II, Src: Dell_2a:54:f2 (74:8b:e2:2a:54:f2), Dst: JuniperNetwo_0d:6b:c0 (78:50:7c:0d:6b:c0)
- Internet Protocol Version 4, Src: 10.30.75.79, Dst: 23.206.173.32
- Transmission Control Protocol, Src Port: 65319, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
- Transport Layer Security
- TLSv1.3 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 512
 - Handshake Protocol: Client Hello

The packet bytes pane on the right shows the raw data of the captured packet, including the TLS record structure.

Wireshark interface showing a TLS handshake capture. The packet list on the left shows packets 426 through 943. Packet 426 is selected, showing details for the TLSv1.3 Client Hello. The details pane on the right shows the structure of the Client Hello, including the random value, session ID, cipher suites, and extensions. The packet bytes pane on the right shows the raw data of the Client Hello.

No.	Time	Source	Destination	Protocol	Length	Info
426	8.955255	10.30.75.79	23.206.173.32	TLSv1.3	571	Client Hello (SNI=www.bing.com)
429	8.968293	23.206.173.32	10.30.75.79	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
431	8.968293	23.206.173.32	10.30.75.79	TLSv1.3	1180	Application Data, Application Data, Application Data
437	8.975947	10.30.75.79	23.206.173.32	TLSv1.3	134	Change Cipher Spec, Application Data
439	8.980884	23.206.173.32	10.30.75.79	TLSv1.3	357	Application Data
448	8.980884	23.206.173.32	10.30.75.79	TLSv1.3	357	Application Data
942	18.982251	23.206.173.32	10.30.75.79	TLSv1.3	93	Application Data
943	18.982251	23.206.173.32	10.30.75.79	TLSv1.3	78	Application Data

Details for Packet 426 (Client Hello):

- Version: TLS 1.0 (0x0301)
- Length: 512
- Handshake Protocol: Client Hello
- Handshake Type: Client Hello (1)
- Length: 508
- Version: TLS 1.2 (0x0303)
- Random: 0ad9539f32f35793b766f55bd8395df79f9ac90688015d116eaf2c839489f155
- Session ID Length: 32
- Session ID: c7cbbd6a67853bf3f45b28cc68ab33b0cdeaf9477ec721a90ff2392049f8f80
- Cipher Suites Length: 30
- Cipher Suites (15 suites)
- Compression Methods Length: 1
- Extensions Length: 405
- Extension: renegotiation_info (len=1)
- Extension: server_name (len=17) name=www.bing.com
- Extension: ec_point_formats (len=4)
- Extension: supported_groups (len=8)
- Extension: session_ticket (len=0)
- Extension: status_request (len=5)
- Extension: application_layer_protocol_negotiation (len=14)

Wireshark interface showing the same TLS handshake capture. The packet list on the left shows packets 426 through 943. Packet 426 is selected, showing details for the TLSv1.3 Client Hello. The details pane on the right shows the structure of the Client Hello, including the random value, session ID, cipher suites, and extensions. The packet bytes pane on the right shows the raw data of the Client Hello.

No.	Time	Source	Destination	Protocol	Length	Info
426	8.955255	10.30.75.79	23.206.173.32	TLSv1.3	571	Client Hello (SNI=www.bing.com)
429	8.968293	23.206.173.32	10.30.75.79	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
431	8.968293	23.206.173.32	10.30.75.79	TLSv1.3	1180	Application Data, Application Data, Application Data
437	8.975947	10.30.75.79	23.206.173.32	TLSv1.3	134	Change Cipher Spec, Application Data
439	8.980884	23.206.173.32	10.30.75.79	TLSv1.3	357	Application Data
448	8.980884	23.206.173.32	10.30.75.79	TLSv1.3	357	Application Data
942	18.982251	23.206.173.32	10.30.75.79	TLSv1.3	93	Application Data
943	18.982251	23.206.173.32	10.30.75.79	TLSv1.3	78	Application Data

Details for Packet 426 (Client Hello):

- Random: 0ad9539f32f35793b766f55bd8395df79f9ac90688015d116eaf2c839489f155
- Session ID Length: 32
- Session ID: c7cbbd6a67853bf3f45b28cc68ab33b0cdeaf9477ec721a90ff2392049f8f80
- Cipher Suites Length: 30
- Cipher Suites (15 suites)
 - Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
 - Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
 - Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc030)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc031)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc032)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc013)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc014)
 - Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
 - Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
 - Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
 - Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- Compression Methods Length: 1

(Click on bottom Transport layer security then again click on arrow you will get all details)

7.If you do right click on server hello →follow → TLS Stream → you will get popup close that

by doing this you will get one command on Wireshark as follow

The screenshot displays the Wireshark interface with a packet capture of a TCP stream (eq 20). The packet list on the left shows a series of packets from 422 to 946. Packet 429 is highlighted, showing a TLSv1.3 record layer. The packet details pane on the right shows the structure of the TLSv1.3 record layer, including the handshake protocol, server hello, and application data. The packet bytes pane on the right shows the raw hex and ASCII data of the selected packet.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
422	8.949481	10.30.75.79	23.206.173.32	TCP	66	65319 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
424	8.953315	23.206.173.32	10.30.75.79	TCP	66	443 → 65319 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1384 SACK_PERM WS=128
425	8.953357	10.30.75.79	23.206.173.32	TCP	54	65319 → 443 [ACK] Seq=1 Ack=1 Win=262912 Len=0
426	8.955255	10.30.75.79	23.206.173.32	TLSv1.3	571	Client Hello (SNL=mmar.bing.com)
428	8.960293	23.206.173.32	10.30.75.79	TCP	60	443 → 65319 [ACK] Seq=1 Ack=518 Win=974336 Len=0
429	8.960293	23.206.173.32	10.30.75.79	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
430	8.960293	23.206.173.32	10.30.75.79	TCP	1514	443 → 65319 [PSH, ACK] Seq=1461 Ack=518 Win=64128 Len=1460 [TCP PDU reassembled in 431]
431	8.960293	23.206.173.32	10.30.75.79	TLSv1.3	1180	Application Data, Application Data, Application Data
432	8.960644	10.30.75.79	23.206.173.32	TCP	54	65319 → 443 [ACK] Seq=518 Ack=4047 Win=262912 Len=0
437	8.975947	10.30.75.79	23.206.173.32	TLSv1.3	134	Change Cipher Spec, Application Data
438	8.979545	23.206.173.32	10.30.75.79	TCP	60	443 → 65319 [ACK] Seq=4047 Ack=598 Win=64128 Len=0
439	8.980884	23.206.173.32	10.30.75.79	TLSv1.3	357	Application Data
440	8.980884	23.206.173.32	10.30.75.79	TLSv1.3	357	Application Data
442	8.993324	23.206.173.32	10.30.75.79	TCP	66	65319 → 443 [ACK] Seq=598 Ack=4653 Win=262144 Len=0 SLE=4358 SRE=4653
942	18.982251	23.206.173.32	10.30.75.79	TLSv1.3	93	Application Data
943	18.982251	23.206.173.32	10.30.75.79	TLSv1.3	78	Application Data
944	18.982251	23.206.173.32	10.30.75.79	TCP	60	443 → 65319 [FIN, ACK] Seq=4716 Ack=598 Win=64128 Len=0
945	18.982552	10.30.75.79	23.206.173.32	TCP	54	65319 → 443 [ACK] Seq=598 Ack=4716 Win=262144 Len=0
946	18.983764	10.30.75.79	23.206.173.32	TCP	54	65319 → 443 [ACK] Seq=598 Ack=4717 Win=262144 Len=0

Packet Details (429):

- Frame 429: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{6E10E...}
- Ethernet II, Src: JuniperNetwo_8d:8b:c0 (78:5b:7c:8d:8b:c0), Dst: Dell_2a:54:f2 (74:86:e2:2a:54:f2)
- Internet Protocol Version 4, Src: 23.206.173.32, Dst: 10.30.75.79
- Transmission Control Protocol, Src Port: 443, Dst Port: 65319, Seq: 1, Ack: 518, Len: 1460
- Transport Layer Security
 - TLSv1.3 Record Layer: Handshake Protocol: Server Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 122
 - Handshake Protocol: Server Hello
 - Handshake Type: Server Hello (2)
 - Length: 118
 - Version: TLS 1.2 (0x0303)
 - Random: a8e9c51447fac815a46af424f7b2582b6033cdce8d38dc7234fa892f4aff674
 - Session ID Length: 32
 - Session ID: c7cbbd6a67853bf3f45b28cc68ab33b0cdeaf9477ec721a90ff2392049f8f80
 - Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
 - Compression Method: null (0)
 - Extensions Length: 46
 - Extension: supported_versions (len=2) TLS 1.3
 - Extension: raw_data (len=36) v25510

Packet Bytes:

```
0000 03 00 e9 c5 1d 47 fa c8 15 a4 6a f4 24 f7 b2 58 .....G...j$X
0001 2b 68 33 cd ce 8d d3 bd c7 23 4f a8 92 f4 af f6 ...h3.....00....
0002 74 20 c7 cb bd 6a 67 85 3b f3 f4 5b 28 cc 68 ab t...jg...:[(h
0003 33 bb 0c de af 94 77 ec 72 1a 90 ff 23 92 04 9f 3...w...r...#...
0004 8f 80 13 02 00 00 2e 00 20 00 02 03 04 00 33 00 .....r...3...
0005 24 00 1d 00 20 06 13 eb 61 30 53 17 00 09 e8 0d $...r...05.....
0006 8b 71 2f cd 22 d4 12 5b f8 06 a3 b0 38 c8 53 e5 q/...[...8'S
0007 b8 e8 31 65 67 14 03 00 01 17 03 03 00 2e .....leg.....
0008 b3 a5 df 13 ef 91 bd e5 35 bf 85 16 03 d7 b6 93 .....S.....
0009 7f 04 b7 d5 90 99 23 55 29 99 3e da 73 a4 c7 .....U Z)>...
000a eb 99 6a d9 ca 18 18 33 38 ae a2 44 51 ee 17 03 .....3 8'DQ...
000b 03 0e 63 a7 4c 85 30 8b 78 c9 2f 05 3b 01 cb 8e ...C.L0: x/r/j...
000c 07 e5 33 2e 15 7e ea 32 39 7d 00 c9 17 01 1e 7d ...372).....
000d 50 a5 33 2e 15 7e ea 32 39 7d 00 c9 17 01 1e 7d ...3...2 9)...1...
000e f3 7a 88 3d c2 f5 36 77 6c c2 ee 88 21 ca 7a d5 ...m...dw 1...1...
000f 02 e2 a5 85 f2 5d 2d 73 1f bb e8 6a e5 cc 01 bc .....]s.....
0010 ac e5 db db fc 95 bf c0 54 98 07 dc 26 1f ce 91 .....T...1k...
0011 7a 68 1a b3 05 5c 64 81 ce a9 d1 d8 78 62 a7 88 zh...Vd...x...
0012 f0 02 f9 54 d8 97 1e 44 88 d8 1f 38 03 38 75 6b ...T...D...8-Buk
0013 ef b3 5c d7 34 3f b2 6d 15 21 22 8b a4 8a 35 0e ...43m...1...5...
0014 f0 a5 20 70 9f b0 30 a5 42 c7 e1 01 14 40 f0 d0 ...j...B...g...
0015 f9 6c c7 ab 4f 99 5c d1 a0 8e 18 54 d9 ef cc c7 ...1...0...v...
0016 f1 d2 50 73 02 64 d6 1b 0c e4 4a 1c 23 c7 0e 2f ...Ps...d...3...
0017 0d ad cd 4c fc 04 f7 2f b5 ba 66 09 07 bc 01 5a ...L.../...f...2...
```