**Coloring rule:**

http: 1

tcp: 2

**Protocols in frame:**

eth:ethertype:ip:tcp:http:data:data:data - 1

eth:ethertype:ip:tcp:http - 2

eth:ethertype:ip:tcp:http:data - 3

eth:ethertype:ip:tcp:http:urlencoded-form - 4

eth:ethertype:ip:tcp:tls - 5

eth:ethertype:ip:tcp:tls:tls - 6

eth:ethertype:ip:tcp:tls:oscp:tls -7

eth:ethertype:ip:tcp:tls:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509ce:x509ce:x509ce:x509ce:x509ce:x509ce:x509ce:pkix1explicit:pkix1implicit:x509ce:t - 8

eth:ethertype:ip:tcp:tls:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509ce:x509ce:x509ce:x509ce:x509ce:x509ce:x509ce:pkix1explicit:pkix1implicit:x509ce:tls:x509sat:x509sat:x509sat:x509s - 9

eth:ethertype:ip:tcp:tls:x509sat:x509sat:x509sat:x509sat:x509sat:x509ce:x509ce:x509ce:x509ce:x509ce:x509ce:x509ce:pkix1implicit:x509ce:tls:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509ce:x509 - 10

eth:ethertype:ip:tcp:tls:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509ce:x509ce:x509ce:x509ce:x509ce:x509ce:pkix1explicit:x509ce:pkix1implicit:x509ce:x509sat:x509sat:x509sat:x509sat:x – 11

eth:ethertype:ip:tcp:tls:ocsp:ocsp:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509ce:x509ce:x509ce:x509ce:x509ce:x509ce:ocsp:tls – 12

eth:ethertype:ip:tcp:tls:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:pkcs-1:x509ce:x509ce:x509ce:x509ce:x509ce:x509ce:pkix1implicit:x509ce:x509sat:x509sat:x509sat - 13

eth:ethertype:ip:tcp:http:data-text-lines – 14

**Coloring rule string:**

http || tcp.port == 80 || http2 - 1

tcp - 2

**Label:**

http - 1

http get- 2

http post - 3

Client hello – 4

Server hello ,– 5

Server hello, change cipher spec – 6

Certificate,certificate status, server key exchange, server hello done – 7

Client key exchange,change cipher spec, encrypted handshake message – 8

Certificate, server key exchange, server hello done – 9

Certificate status, server key exchange,server hello done – 10

Server key exchange, server hello done – 11

New session ticket, change cipher spec, encrypted handshake message – 12

Change cipher spec,encrypted handshake message – 13

Server hello, change cipher spec, encrypted handshake msg – 14

Application data, change cipher spec application data – 15

Server hello, certificate, server key exchange, server hello done – 16

Http malicious - 20

Http get malicious – 21

Http ok malicious – 22(only this will contain tcp segment data and file data)

Encrypted alert - 23

Client hello malicious – 24

Server hello malicious – 25

Client key exchange,change cipher spec, encrypted handshake message malicious – 26

New session ticket, change cipher spec, encrypted handshake message malicious – 27

Application data malicious - 28

Certificate status, server key exchange,server hello done malicious – 29

Certificate [TCP segment of a reassembled PDU] – 30

Server hello, certificate, server key exchange, server hello done malicious – 31

Server hello, change cipher spec – 32