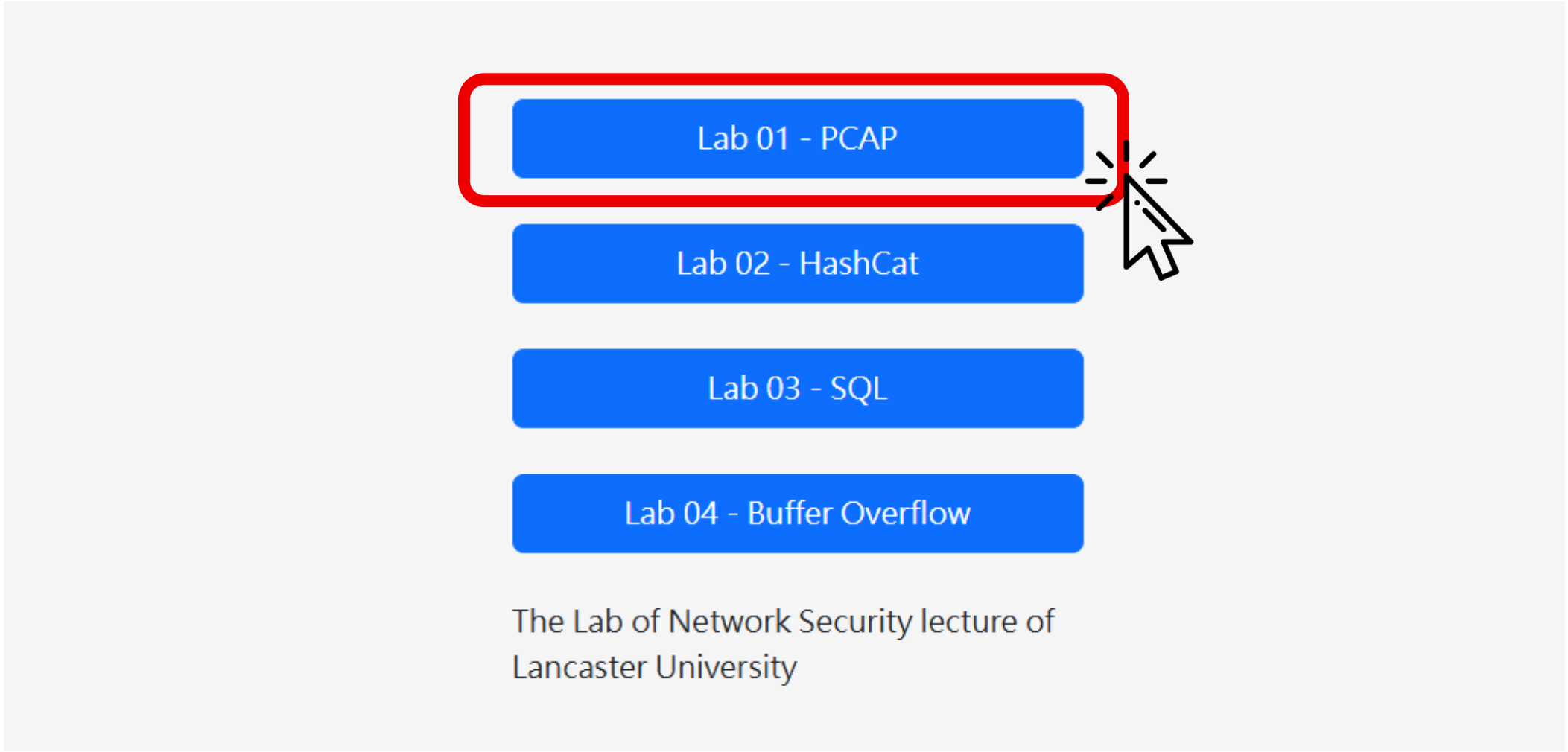
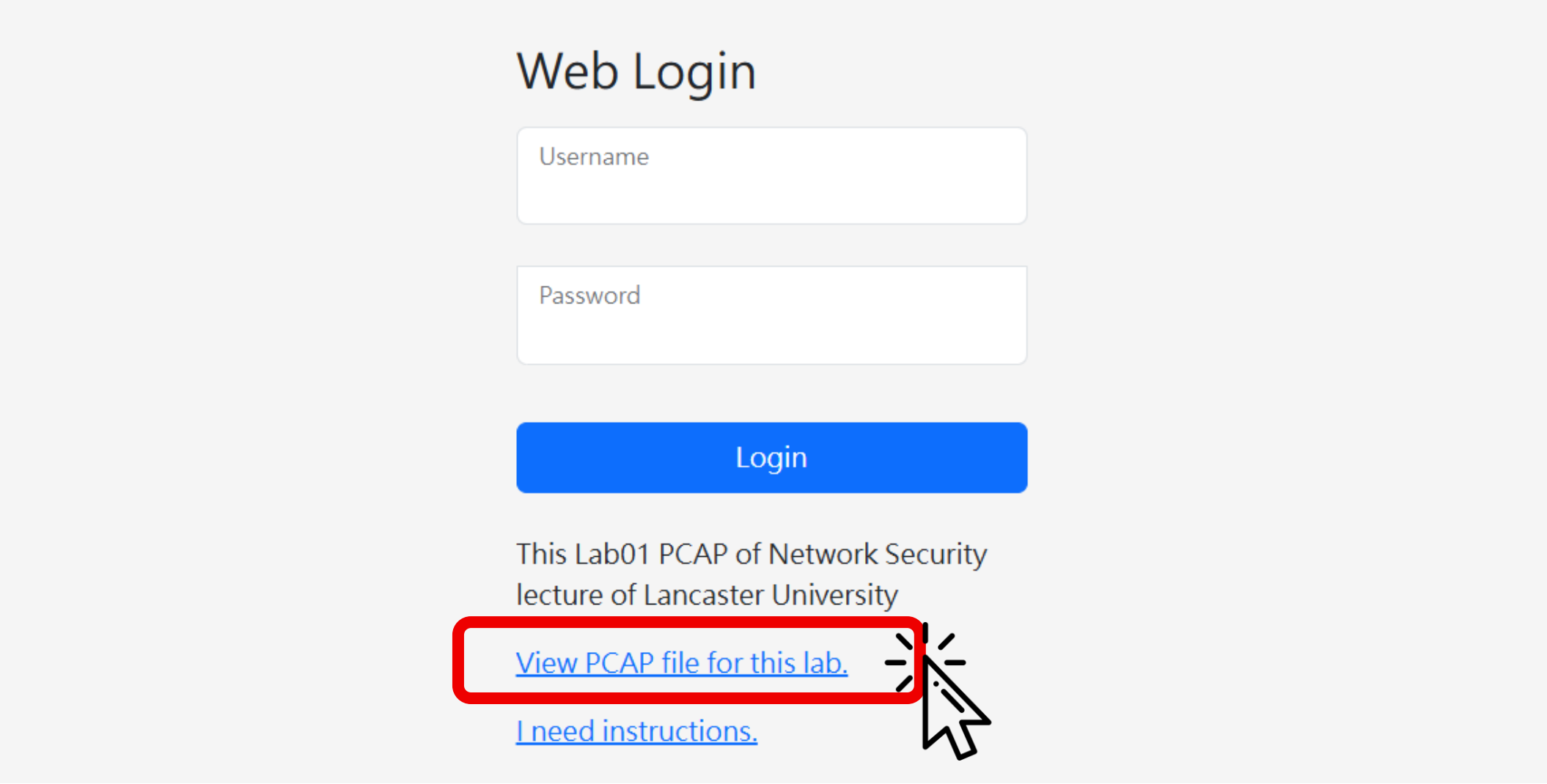
Lancaster University

Network Security Lab 01 Instruction

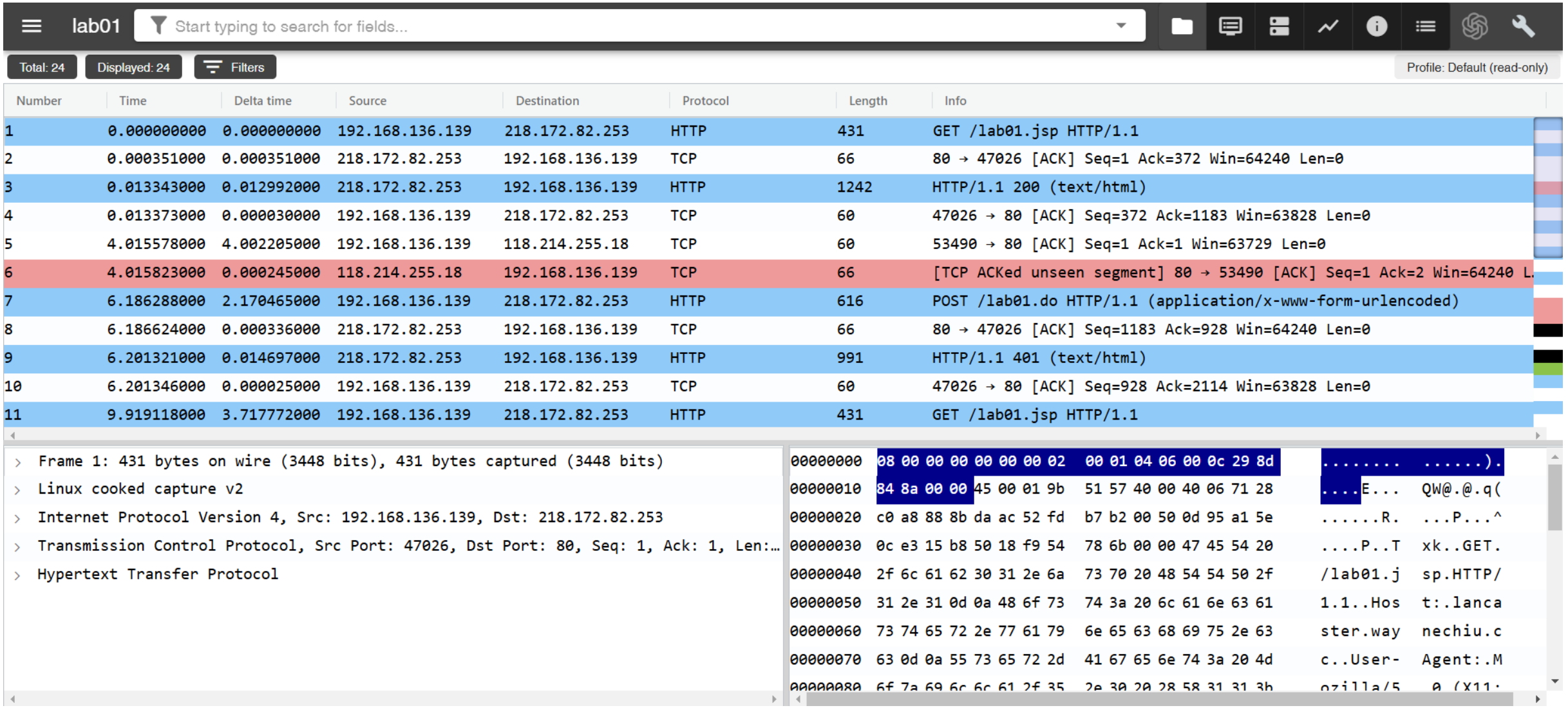
0. Open Lancaster.waynechiu.cc

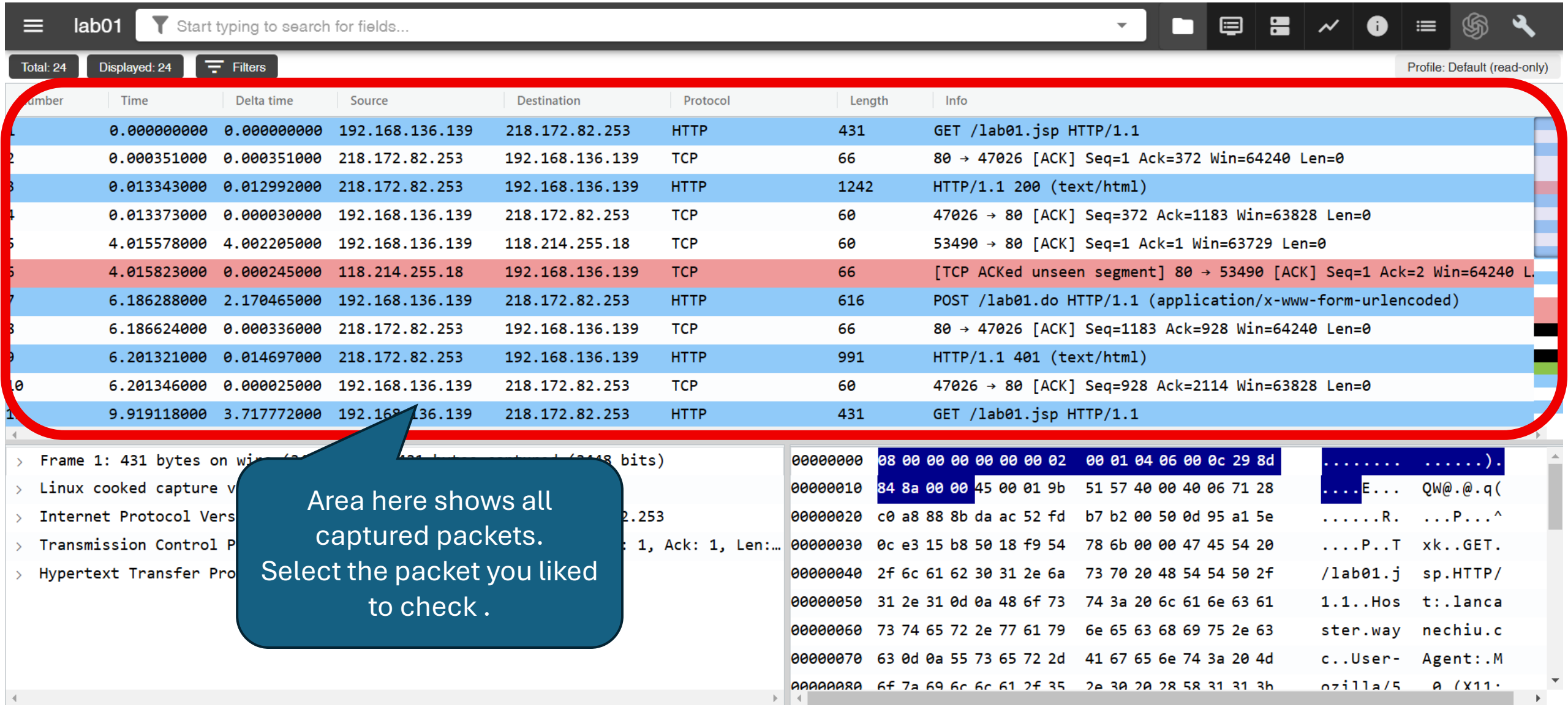


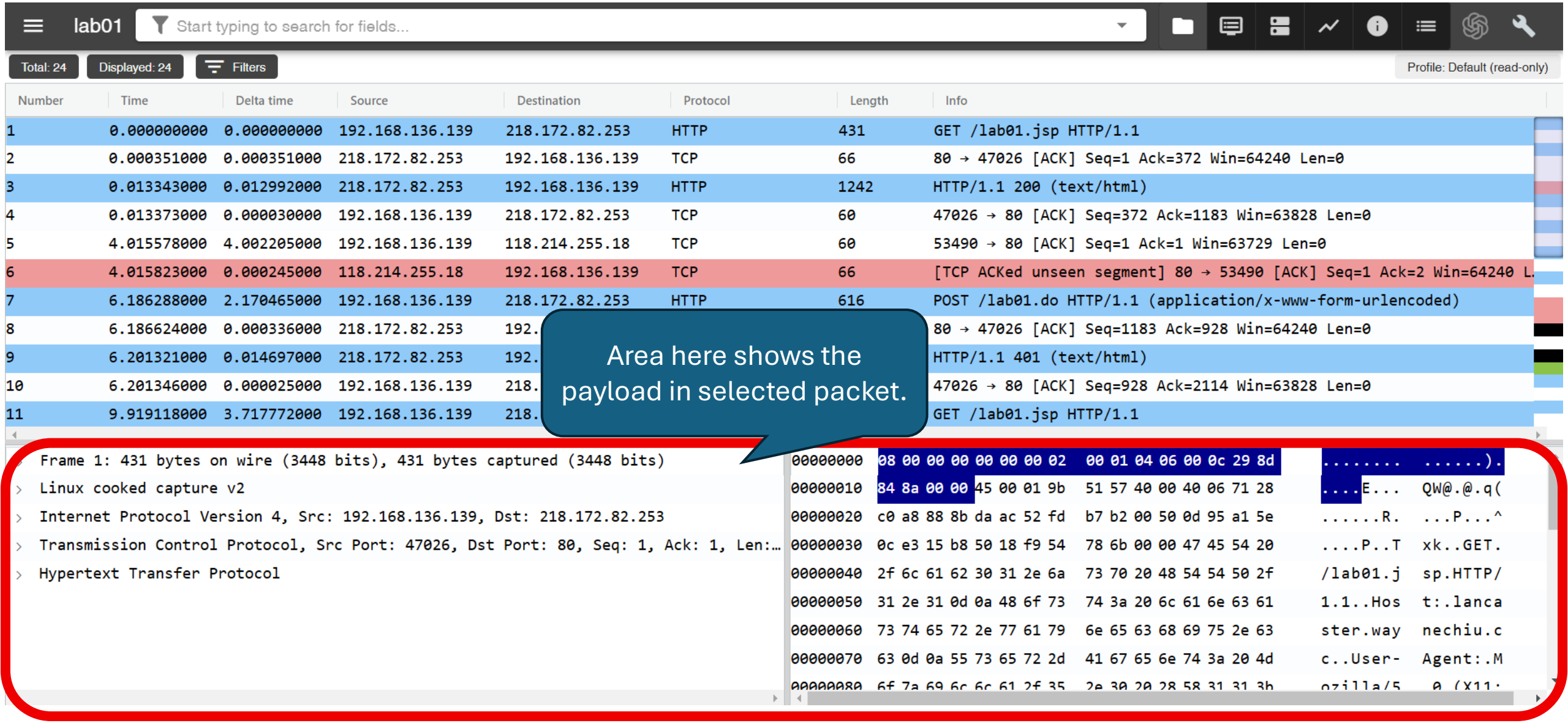
1. View the PCAP file

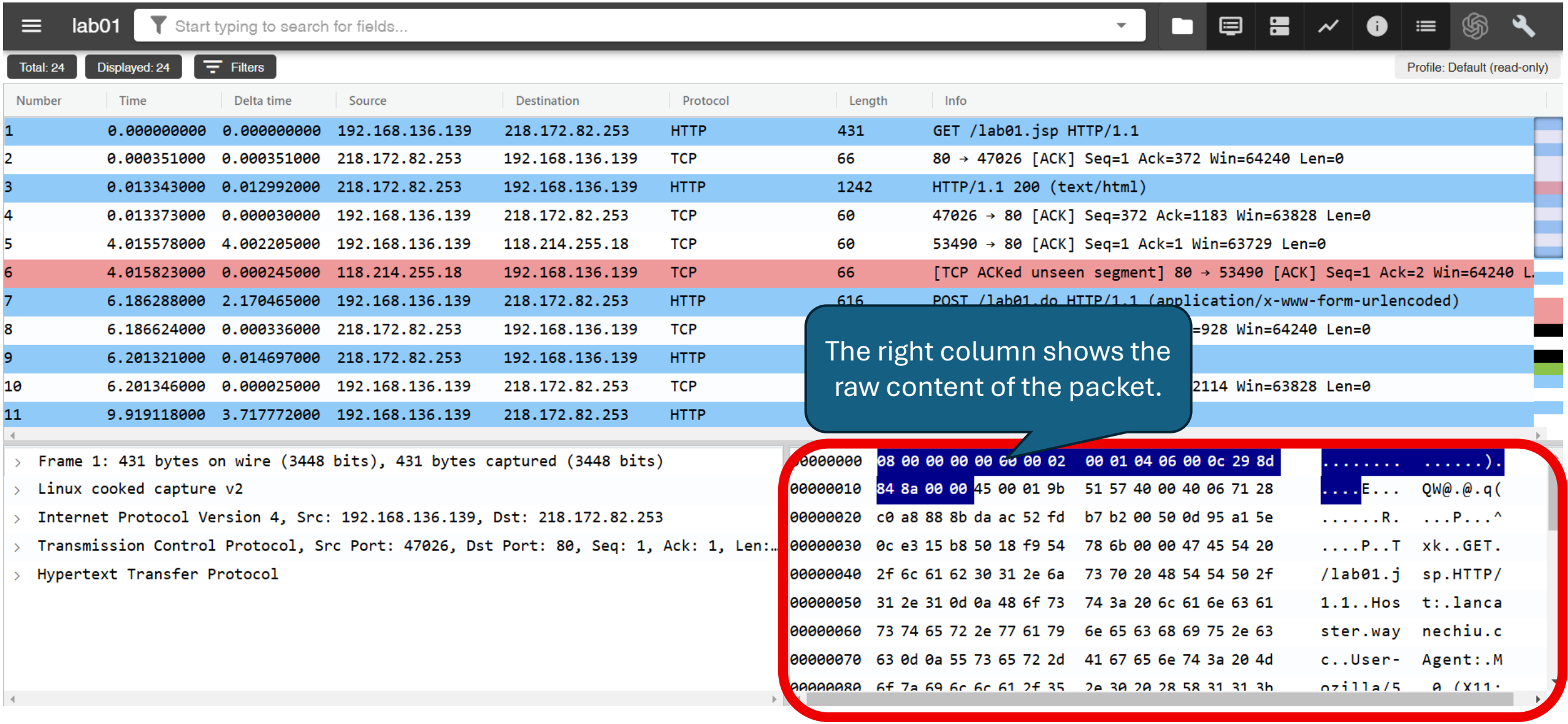


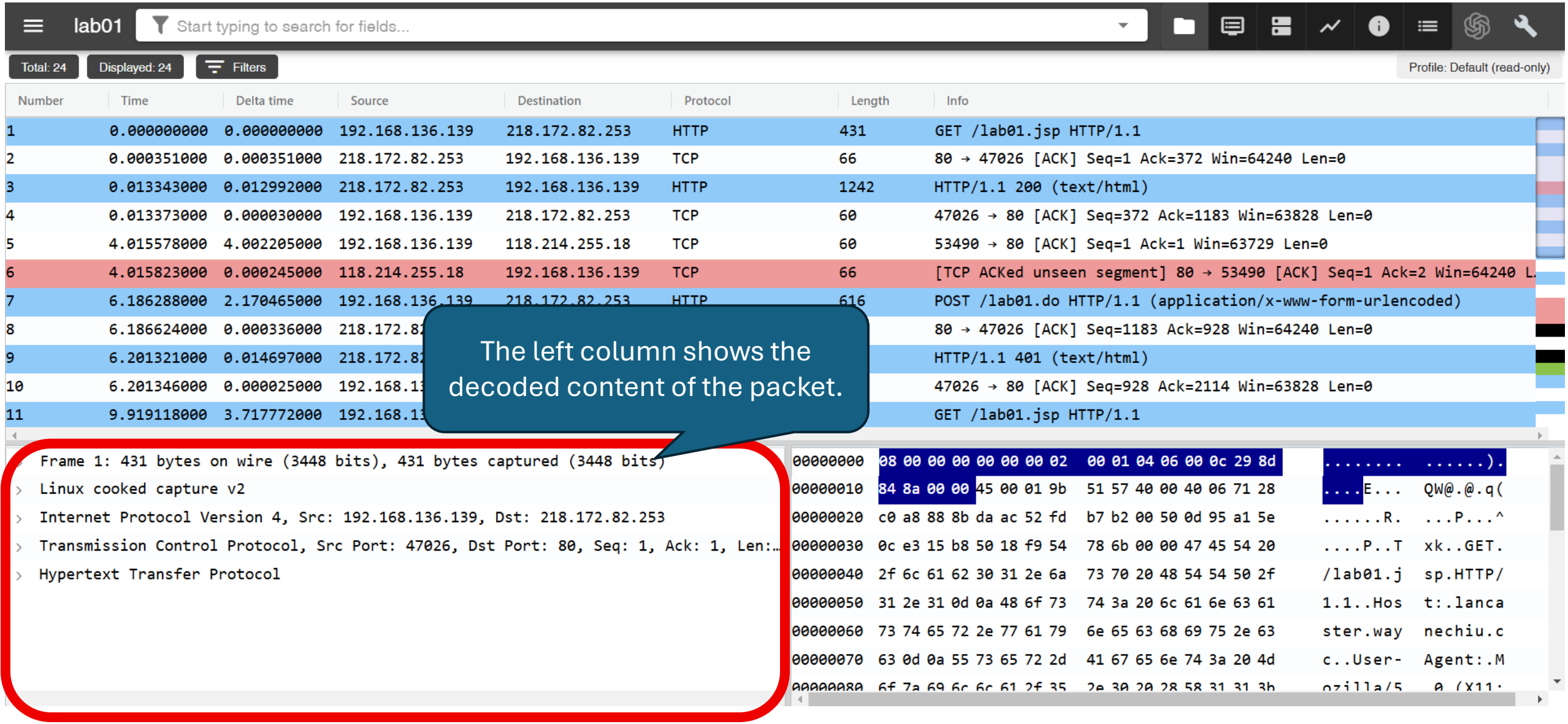
2. Search for useful information.

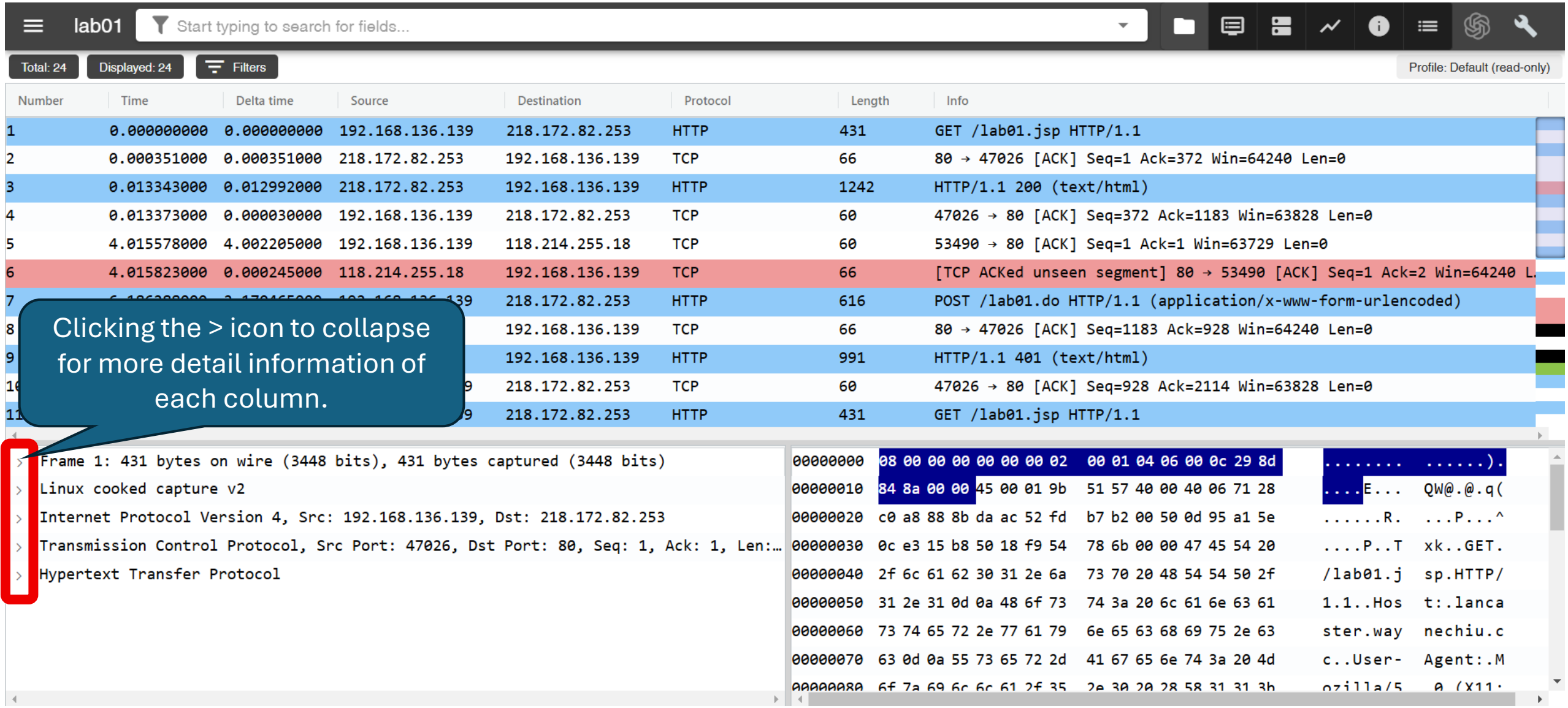


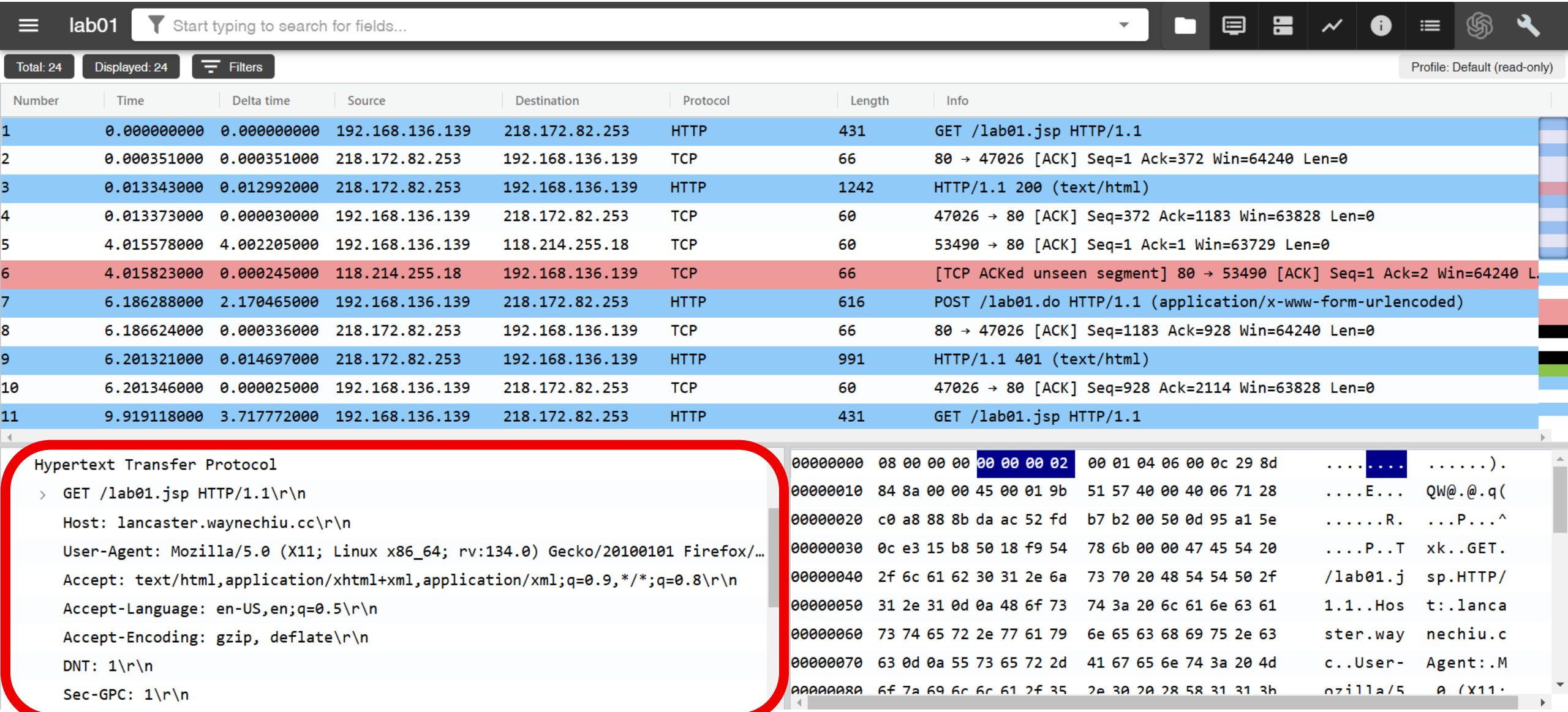

lab01
Start typing to search for fields...
Total: 24
Displayed: 24
Filters
Profile: Default (read-only)
umber Time Delta time Source Destination Protocol Length Info
1 0.000000000 0.000000000 192.168.136.139 218.172.82.253 HTTP 431 GET /lab01.jsp HTTP/1.1
2 0.000351000 0.000351000 218.172.82.253 192.168.136.139 TCP 66 80 → 47026 [ACK] Seq=1 Ack=372 Win=64240 Len=0
3 0.013343000 0.012992000 218.172.82.253 192.168.136.139 HTTP 1242 HTTP/1.1 200 (text/html)
4 0.013373000 0.000030000 192.168.136.139 218.172.82.253 TCP 60 47026 → 80 [ACK] Seq=372 Ack=1183 Win=63828 Len=0
5 4.015578000 4.002205000 192.168.136.139 118.214.255.18 TCP 60 53490 → 80 [ACK] Seq=1 Ack=1 Win=63729 Len=0
6 4.015823000 0.000245000 118.214.255.18 192.168.136.139 TCP 66 [TCP ACKed unseen segment] 80 → 53490 [ACK] Seq=1 Ack=2 Win=64240 L
7 6.186288000 2.170465000 192.168.136.139 218.172.82.253 HTTP 616 POST /lab01.do HTTP/1.1 (application/x-www-form-urlencoded)
8 6.18624000 0.000336000 218.172.82.253 192.168.136.139 TCP 66 80 → 47026 [ACK] Seq=1183 Ack=928 Win=64240 Len=0
9 6.201321000 0.014697000 218.172.82.253 192.168.136.139 HTTP 991 HTTP/1.1 401 (text/html)
10 6.201346000 0.000025000 192.168.136.139 218.172.82.253 TCP 60 47026 → 80 [ACK] Seq=928 Ack=2114 Win=63828 Len=0
11 9.919118000 3.717772000 192.168.136.139 218.172.82.253 HTTP 431 GET /lab01.jsp HTTP/1.1
Frame 1: 431 bytes on wi bits)
Linux cooked capture v
Internet Protocol Vers .253
Transmission Control P 1, Ack: 1, Len:…
Hypertext Transfer Pro
00000000 08 00 00 00 00 00 00 02 00 01 04 06 00 0c 29 8d
00000010 84 8a 00 00 45 00 01 9b 51 57 40 00 40 06 71 28
00000020 c0 a8 88 8b da ac 52 fd b7 b2 00 50 0d 95 a1 5e
00000030 0c e3 15 b8 50 18 f9 54 78 6b 00 00 47 45 54 20
00000040 2f 6c 61 62 30 31 2e 6a 73 70 20 48 54 54 50 2f
00000050 31 2e 31 0d 0a 48 6f 73 74 3a 20 6c 61 6e 63 61
00000060 73 74 65 72 2e 77 61 79 6e 65 63 68 69 75 2e 63
00000070 63 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d
Area here shows all captured packets. Select the packet you liked to check .


lab01
Start typing to search for fields...
Total: 24
Displayed: 24
Filters
Profile: Default (read-only)
Number Time Delta time Source Destination Protocol Length Info
1 0.000000000 0.000000000 192.168.136.139 218.172.82.253 HTTP 431 GET /lab01.jsp HTTP/1.1
2 0.000351000 0.000351000 218.172.82.253 192.168.136.139 TCP 66 80 → 47026 [ACK] Seq=1 Ack=372 Win=64240 Len=0
3 0.013343000 0.012992000 218.172.82.253 192.168.136.139 HTTP 1242 HTTP/1.1 200 (text/html)
4 0.013373000 0.000030000 192.168.136.139 218.172.82.253 TCP 60 47026 → 80 [ACK] Seq=372 Ack=1183 Win=63828 Len=0
5 4.015578000 4.002205000 192.168.136.139 118.214.255.18 TCP 60 53490 → 80 [ACK] Seq=1 Ack=1 Win=63729 Len=0
6 4.015823000 0.000245000 118.214.255.18 192.168.136.139 TCP 66 [TCP ACKed unseen segment] 80 → 53490 [ACK] Seq=1 Ack=2 Win=64240 L
7 6.186288000 2.170465000 192.168.136.139 218.172.82.253 HTTP 616 POST /lab01.do HTTP/1.1 (application/x-www-form-urlencoded)
8 6.186624000 0.000336000 218.172.82.253 192. 80 → 47026 [ACK] Seq=1183 Ack=928 Win=64240 Len=0
9 6.201321000 0.014697000 218.172.82.253 192. HTTP/1.1 401 (text/html)
10 6.201346000 0.000025000 192.168.136.139 218. 47026 → 80 [ACK] Seq=928 Ack=2114 Win=63828 Len=0
11 9.919118000 3.717772000 192.168.136.139 218. GET /lab01.jsp HTTP/1.1
Area here shows the payload in selected packet.
Frame 1: 431 bytes on wire (3448 bits), 431 bytes captured (3448 bits)
Linux cooked capture v2
Internet Protocol Version 4, Src: 192.168.136.139, Dst: 218.172.82.253
Transmission Control Protocol, Src Port: 47026, Dst Port: 80, Seq: 1, Ack: 1, Len:…
Hypertext Transfer Protocol
00000000 08 00 00 00 00 00 00 02 00 01 04 06 00 0c 29 8d ....).
00000010 84 8a 00 00 45 00 01 9b 51 57 40 00 40 06 71 28 ....E... QW@.@.q(
00000020 c0 a8 88 8b da ac 52 fd b7 b2 00 50 0d 95 a1 5e ......R. ...P...^
00000030 0c e3 15 b8 50 18 f9 54 78 6b 00 00 47 45 54 20 ....P..T xk..GET.
00000040 2f 6c 61 62 30 31 2e 6a 73 70 20 48 54 54 50 2f /lab01.j sp.HTTP/
00000050 31 2e 31 0d 0a 48 6f 73 74 3a 20 6c 61 6e 63 61 1.1..Hos t:.lanca
00000060 73 74 65 72 2e 77 61 79 6e 65 63 68 69 75 2e 63 ster.way nechiu.c
00000070 63 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d c..User- Agent:.M
00000080 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b ozilla/5 .0 (X11;


lab01
Start typing to search for fields...
Total: 24
Displayed: 24
Filters
Profile: Default (read-only)
Number Time Delta time Source Destination Protocol Length Info
1 0.000000000 0.000000000 192.168.136.139 218.172.82.253 HTTP 431 GET /lab01.jsp HTTP/1.1
2 0.000351000 0.000351000 218.172.82.253 192.168.136.139 TCP 66 80 → 47026 [ACK] Seq=1 Ack=372 Win=64240 Len=0
3 0.013343000 0.012992000 218.172.82.253 192.168.136.139 HTTP 1242 HTTP/1.1 200 (text/html)
4 0.013373000 0.000030000 192.168.136.139 218.172.82.253 TCP 60 47026 → 80 [ACK] Seq=372 Ack=1183 Win=63828 Len=0
5 4.015578000 4.002205000 192.168.136.139 118.214.255.18 TCP 60 53490 → 80 [ACK] Seq=1 Ack=1 Win=63729 Len=0
6 4.015823000 0.000245000 118.214.255.18 192.168.136.139 TCP 66 [TCP ACKed unseen segment] 80 → 53490 [ACK] Seq=1 Ack=2 Win=64240 L
7 6.186288000 2.170465000 192.168.136.139 218.172.82.253 HTTP 616 POST /lab01.do HTTP/1.1 (application/x-www-form-urlencoded)
8 6.186624000 0.000336000 218.172.82.253 192.168.136.139 TCP =928 Win=64240 Len=0
9 6.201321000 0.014697000 218.172.82.253 192.168.136.139 HTTP
10 6.201346000 0.000025000 192.168.136.139 218.172.82.253 TCP 2114 Win=63828 Len=0
11 9.919118000 3.717772000 192.168.136.139 218.172.82.253 HTTP
The right column shows the raw content of the packet.
Frame 1: 431 bytes on wire (3448 bits), 431 bytes captured (3448 bits)
Linux cooked capture v2
Internet Protocol Version 4, Src: 192.168.136.139, Dst: 218.172.82.253
Transmission Control Protocol, Src Port: 47026, Dst Port: 80, Seq: 1, Ack: 1, Len:
Hypertext Transfer Protocol
00000000 08 00 00 00 00 60 00 02 00 01 04 06 00 0c 29 8d ....).
00000010 84 8a 00 00 45 00 01 9b 51 57 40 00 40 06 71 28 ....E... QW@.@.q(
00000020 c0 a8 88 8b da ac 52 fd b7 b2 00 50 0d 95 a1 5e ......R. ...P...^
00000030 0c e3 15 b8 50 18 f9 54 78 6b 00 00 47 45 54 20 ....P..T xk..GET.
00000040 2f 6c 61 62 30 31 2e 6a 73 70 20 48 54 54 50 2f /lab01.j sp.HTTP/
00000050 31 2e 31 0d 0a 48 6f 73 74 3a 20 6c 61 6e 63 61 1.1..Hos t:.lanca
00000060 73 74 65 72 2e 77 61 79 6e 65 63 68 69 75 2e 63 ster.way nechiu.c
00000070 63 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d c..User- Agent:.M
00000080 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b ozilla/5 .0 (X11;

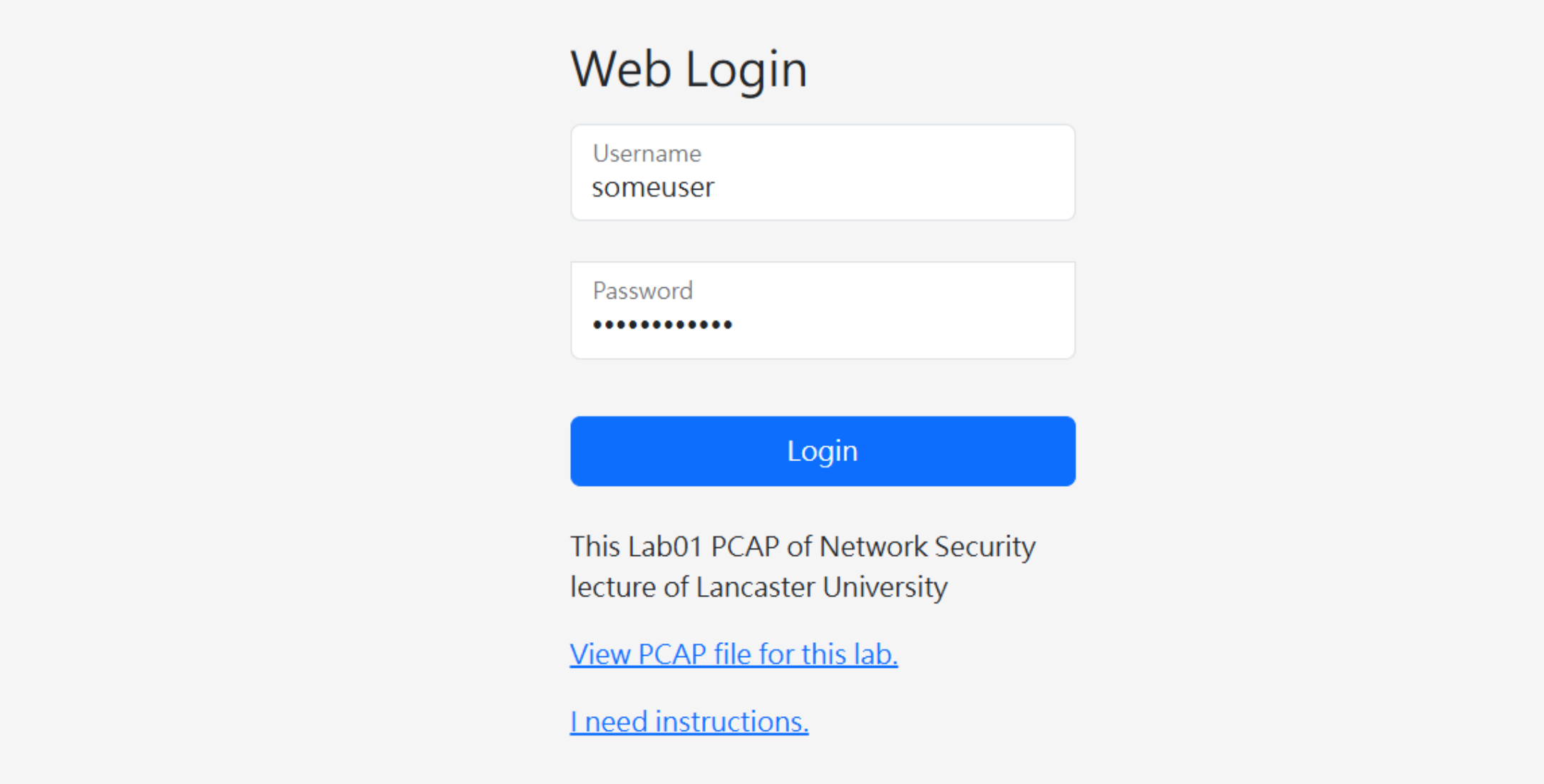

lab01
Start typing to search for fields...
Total: 24
Displayed: 24
Filters
Profile: Default (read-only)
Number Time Delta time Source Destination Protocol Length Info
1 0.000000000 0.000000000 192.168.136.139 218.172.82.253 HTTP 431 GET /lab01.jsp HTTP/1.1
2 0.000351000 0.000351000 218.172.82.253 192.168.136.139 TCP 66 80 → 47026 [ACK] Seq=1 Ack=372 Win=64240 Len=0
3 0.013343000 0.012992000 218.172.82.253 192.168.136.139 HTTP 1242 HTTP/1.1 200 (text/html)
4 0.013373000 0.000030000 192.168.136.139 218.172.82.253 TCP 60 47026 → 80 [ACK] Seq=372 Ack=1183 Win=63828 Len=0
5 4.015578000 4.002205000 192.168.136.139 118.214.255.18 TCP 60 53490 → 80 [ACK] Seq=1 Ack=1 Win=63729 Len=0
6 4.015823000 0.000245000 118.214.255.18 192.168.136.139 TCP 66 [TCP ACKed unseen segment] 80 → 53490 [ACK] Seq=1 Ack=2 Win=64240 L
7 6.186288000 2.170465000 192.168.136.139 218.172.82.253 HTTP 616 POST /lab01.do HTTP/1.1 (application/x-www-form-urlencoded)
8 6.18624000 0.000336000 218.172.82 80 → 47026 [ACK] Seq=1183 Ack=928 Win=64240 Len=0
9 6.201321000 0.014697000 218.172.82 HTTP/1.1 401 (text/html)
10 6.201346000 0.000025000 192.168.13 47026 → 80 [ACK] Seq=928 Ack=2114 Win=63828 Len=0
11 9.919118000 3.717772000 192.168.13 GET /lab01.jsp HTTP/1.1
The left column shows the decoded content of the packet.
Frame 1: 431 bytes on wire (3448 bits), 431 bytes captured (3448 bits)
Linux cooked capture v2
Internet Protocol Version 4, Src: 192.168.136.139, Dst: 218.172.82.253
Transmission Control Protocol, Src Port: 47026, Dst Port: 80, Seq: 1, Ack: 1, Len:
Hypertext Transfer Protocol
00000000 08 00 00 00 00 00 00 02 00 01 04 06 00 0c 29 8d
00000010 84 8a 00 00 45 00 01 9b 51 57 40 00 40 06 71 28
00000020 c0 a8 88 8b da ac 52 fd b7 b2 00 50 0d 95 a1 5e
00000030 0c e3 15 b8 50 18 f9 54 78 6b 00 00 47 45 54 20
00000040 2f 6c 61 62 30 31 2e 6a 73 70 20 48 54 54 50 2f
00000050 31 2e 31 0d 0a 48 6f 73 74 3a 20 6c 61 6e 63 61
00000060 73 74 65 72 2e 77 61 79 6e 65 63 68 69 75 2e 63
00000070 63 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d
00000080 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b


lab01
Start typing to search for fields...
Total: 24
Displayed: 24
Filters
Profile: Default (read-only)
Number Time Delta time Source Destination Protocol Length Info
1 0.000000000 0.000000000 192.168.136.139 218.172.82.253 HTTP 431 GET /lab01.jsp HTTP/1.1
2 0.000351000 0.000351000 218.172.82.253 192.168.136.139 TCP 66 80 → 47026 [ACK] Seq=1 Ack=372 Win=64240 Len=0
3 0.013343000 0.012992000 218.172.82.253 192.168.136.139 HTTP 1242 HTTP/1.1 200 (text/html)
4 0.013373000 0.000030000 192.168.136.139 218.172.82.253 TCP 60 47026 → 80 [ACK] Seq=372 Ack=1183 Win=63828 Len=0
5 4.015578000 4.002205000 192.168.136.139 118.214.255.18 TCP 60 53490 → 80 [ACK] Seq=1 Ack=1 Win=63729 Len=0
6 4.015823000 0.000245000 118.214.255.18 192.168.136.139 TCP 66 [TCP ACKed unseen segment] 80 → 53490 [ACK] Seq=1 Ack=2 Win=64240 L
7 218.172.82.253 HTTP 616 POST /lab01.do HTTP/1.1 (application/x-www-form-urlencoded)
8 192.168.136.139 TCP 66 80 → 47026 [ACK] Seq=1183 Ack=928 Win=64240 Len=0
9 192.168.136.139 HTTP 991 HTTP/1.1 401 (text/html)
218.172.82.253 TCP 60 47026 → 80 [ACK] Seq=928 Ack=2114 Win=63828 Len=0
218.172.82.253 HTTP 431 GET /lab01.jsp HTTP/1.1
Clicking the > icon to collapse for more detail information of each column.
Frame 1: 431 bytes on wire (3448 bits), 431 bytes captured (3448 bits)
Linux cooked capture v2
Internet Protocol Version 4, Src: 192.168.136.139, Dst: 218.172.82.253
Transmission Control Protocol, Src Port: 47026, Dst Port: 80, Seq: 1, Ack: 1, Len:…
Hypertext Transfer Protocol
00000000 08 00 00 00 00 00 00 02 00 01 04 06 00 0c 29 8d ....).
00000010 84 8a 00 00 45 00 01 9b 51 57 40 00 40 06 71 28 ....E... QW@.@.q(
00000020 c0 a8 88 8b da ac 52 fd b7 b2 00 50 0d 95 a1 5e ......R. ...P...^
00000030 0c e3 15 b8 50 18 f9 54 78 6b 00 00 47 45 54 20 ....P..T xk..GET.
00000040 2f 6c 61 62 30 31 2e 6a 73 70 20 48 54 54 50 2f /lab01.j sp.HTTP/
00000050 31 2e 31 0d 0a 48 6f 73 74 3a 20 6c 61 6e 63 61 1.1..Hos t:.lanca
00000060 73 74 65 72 2e 77 61 79 6e 65 63 68 69 75 2e 63 ster.way nechiu.c
00000070 63 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d c..User- Agent:.M
00000080 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b ozilla/5 .0 (X11;


lab01
Start typing to search for fields...
Total: 24
Displayed: 24
Filters
Profile: Default (read-only)
Number Time Delta time Source Destination Protocol Length Info
1 0.000000000 0.000000000 192.168.136.139 218.172.82.253 HTTP 431 GET /lab01.jsp HTTP/1.1
2 0.000351000 0.000351000 218.172.82.253 192.168.136.139 TCP 66 80 → 47026 [ACK] Seq=1 Ack=372 Win=64240 Len=0
3 0.013343000 0.012992000 218.172.82.253 192.168.136.139 HTTP 1242 HTTP/1.1 200 (text/html)
4 0.013373000 0.000030000 192.168.136.139 218.172.82.253 TCP 60 47026 → 80 [ACK] Seq=372 Ack=1183 Win=63828 Len=0
5 4.015578000 4.002205000 192.168.136.139 118.214.255.18 TCP 60 53490 → 80 [ACK] Seq=1 Ack=1 Win=63729 Len=0
6 4.015823000 0.000245000 118.214.255.18 192.168.136.139 TCP 66 [TCP ACKed unseen segment] 80 → 53490 [ACK] Seq=1 Ack=2 Win=64240 L
7 6.186288000 2.170465000 192.168.136.139 218.172.82.253 HTTP 616 POST /lab01.do HTTP/1.1 (application/x-www-form-urlencoded)
8 6.186624000 0.000336000 218.172.82.253 192.168.136.139 TCP 66 80 → 47026 [ACK] Seq=1183 Ack=928 Win=64240 Len=0
9 6.201321000 0.014697000 218.172.82.253 192.168.136.139 HTTP 991 HTTP/1.1 401 (text/html)
10 6.201346000 0.000025000 192.168.136.139 218.172.82.253 TCP 60 47026 → 80 [ACK] Seq=928 Ack=2114 Win=63828 Len=0
11 9.919118000 3.717772000 192.168.136.139 218.172.82.253 HTTP 431 GET /lab01.jsp HTTP/1.1
Hypertext Transfer Protocol
GET /lab01.jsp HTTP/1.1\r\n
Host: lancaster.waynechiu.cc\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:134.0) Gecko/20100101 Firefox/…
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
DNT: 1\r\n
Sec-GPC: 1\r\n
00000000 08 00 00 00 00 00 00 02 00 01 04 06 00 0c 29 8d ....).
00000010 84 8a 00 00 45 00 01 9b 51 57 40 00 40 06 71 28 ....E... QW@.@.q(
00000020 c0 a8 88 8b da ac 52 fd b7 b2 00 50 0d 95 a1 5e ......R. ...P...^
00000030 0c e3 15 b8 50 18 f9 54 78 6b 00 00 47 45 54 20 ....P..T xk..GET.
00000040 2f 6c 61 62 30 31 2e 6a 73 70 20 48 54 54 50 2f /lab01.j sp.HTTP/
00000050 31 2e 31 0d 0a 48 6f 73 74 3a 20 6c 61 6e 63 61 1.1..Hos t:.lanca
00000060 73 74 65 72 2e 77 61 79 6e 65 63 68 69 75 2e 63 ster.way nechiu.c
00000070 63 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d c..User- Agent:.M

Tips: Write down information you figured valuable.

3. Try log into the system



4. Congratulation!

```
Well Done! You have completed the first lab.
```