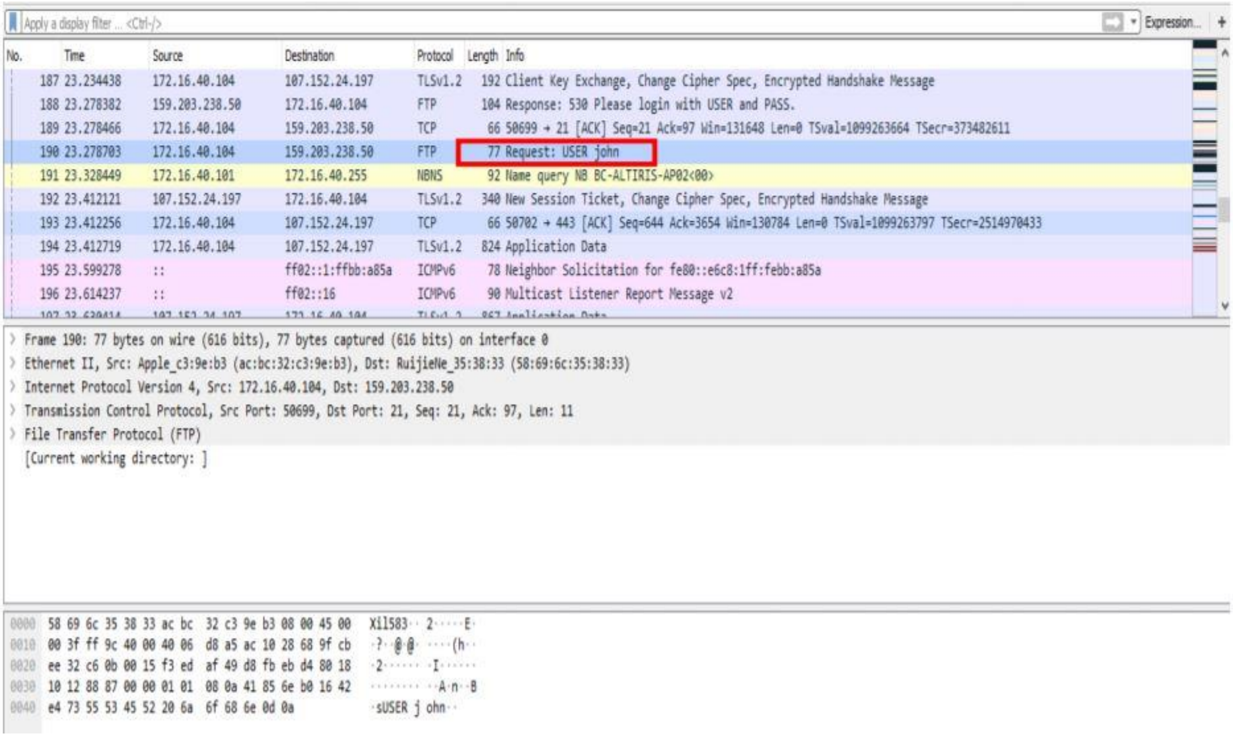
CFAI: ASSIGNMETN 3:

DARSHAN CHOUHAN

The file F_Step_1. pcapng

Username – johan

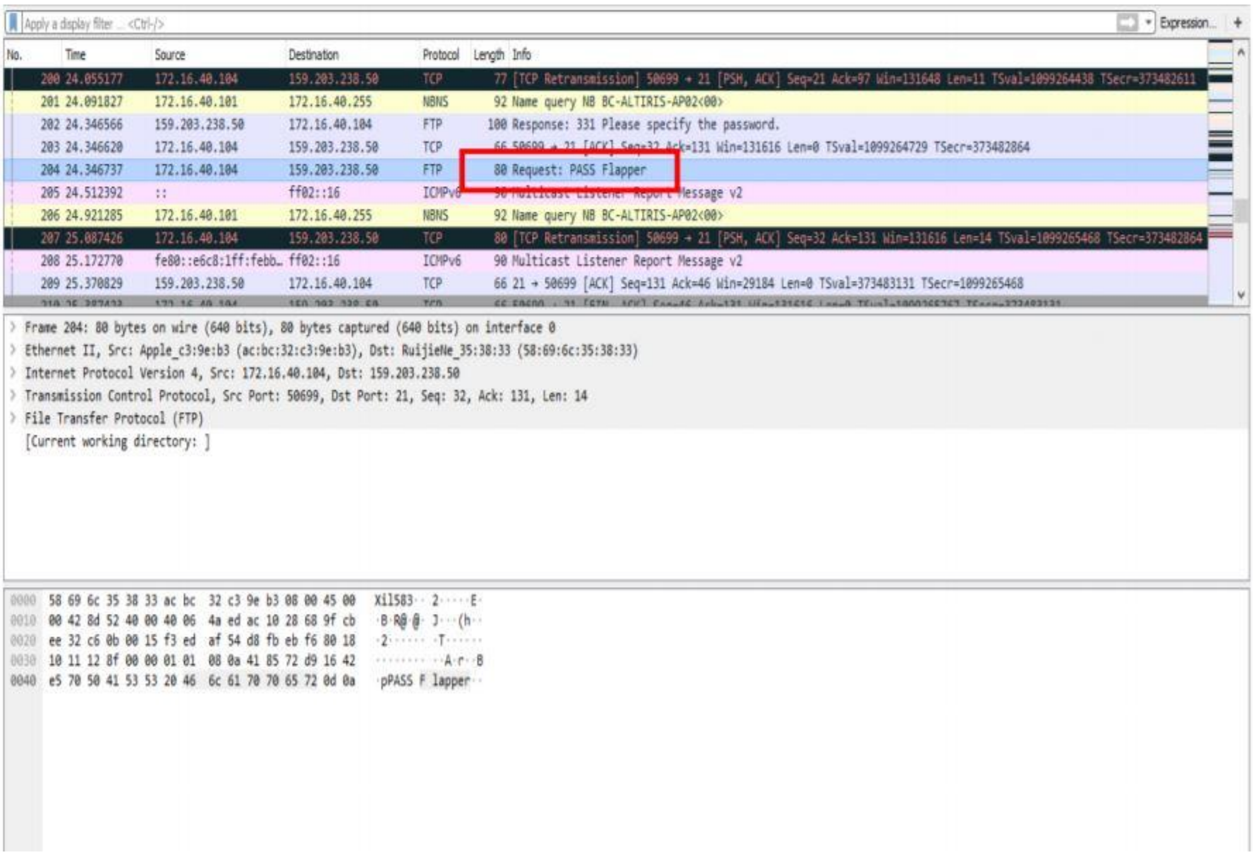
Password – Flapper



No.	Time	Source	Destination	Protocol	Length	Info
187	23.234438	172.16.40.104	107.152.24.197	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
188	23.278382	159.203.238.50	172.16.40.104	FTP	104	Response: 530 Please login with USER and PASS.
189	23.278466	172.16.40.104	159.203.238.50	TCP	66	50699 → 21 [ACK] Seq=21 Ack=97 Win=131648 Len=0 TSval=1099263664 TSecr=373482611
190	23.278703	172.16.40.104	159.203.238.50	FTP	77	Request: USER john
191	23.328449	172.16.40.101	172.16.40.255	NBNS	92	Name query NB BC-ALTIRIS-AP02<00>
192	23.412121	107.152.24.197	172.16.40.104	TLSv1.2	340	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
193	23.412256	172.16.40.104	107.152.24.197	TCP	66	50702 → 443 [ACK] Seq=644 Ack=3654 Win=130784 Len=0 TSval=1099263797 TSecr=2514970433
194	23.412719	172.16.40.104	107.152.24.197	TLSv1.2	824	Application Data
195	23.599278	::	ff02::1:ffbb:a85a	ICMPv6	78	Neighbor Solicitation for fe80::e6c8:1ff:febb:a85a
196	23.614237	::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
197	23.630414	107.152.24.197	172.16.40.104	TLSv1.2	867	Application Data

```
> Frame 190: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
> Ethernet II, Src: Apple_c3:9e:b3 (ac:bc:32:c3:9e:b3), Dst: RuijieNe_35:38:33 (58:69:6c:35:38:33)
> Internet Protocol Version 4, Src: 172.16.40.104, Dst: 159.203.238.50
> Transmission Control Protocol, Src Port: 50699, Dst Port: 21, Seq: 21, Ack: 97, Len: 11
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  58 69 6c 35 38 33 ac bc  32 c3 9e b3 08 00 45 00   Xil583·· 2·····E·
0010  00 3f ff 9c 40 00 40 06  d8 a5 ac 10 28 68 9f cb   ·?··@·@· ····(h··
0020  ee 32 c6 0b 00 15 f3 ed  af 49 d8 fb eb d4 80 18   ·2······ ·I······
0030  10 12 88 87 00 00 01 01  08 0a 41 85 6e b0 16 42   ········ ··A·n··B
0040  e4 73 55 53 45 52 20 6a  6f 68 6e 0d 0a            ·sUSER j ohn··
```



```
No.   Time        Source                   Destination      Protocol  Length Info
  200 24.055177   172.16.40.104            159.203.238.50   TCP        77 [TCP Retransmission] 50699 → 21 [PSH, ACK] Seq=21 Ack=97 Win=131648 Len=11 TSval=1099264438 TSecr=373482611
  201 24.091827   172.16.40.101            172.16.40.255    NBNS       92 Name query NB BC-ALTIRIS-AP02<00>
  202 24.346566   159.203.238.50           172.16.40.104    FTP       100 Response: 331 Please specify the password.
  203 24.346620   172.16.40.104            159.203.238.50   TCP        66 50699 → 21 [ACK] Seq=32 Ack=131 Win=131616 Len=0 TSval=1099264729 TSecr=373482864
  204 24.346737   172.16.40.104            159.203.238.50   FTP        80 Request: PASS Flapper
  205 24.512392   ::                       ff02::16         ICMPv6     90 Multicast Listener Report Message v2
  206 24.921285   172.16.40.101            172.16.40.255    NBNS       92 Name query NB BC-ALTIRIS-AP02<00>
  207 25.087426   172.16.40.104            159.203.238.50   TCP        80 [TCP Retransmission] 50699 → 21 [PSH, ACK] Seq=32 Ack=131 Win=131616 Len=14 TSval=1099265468 TSecr=373482864
  208 25.172770   fe80::e6c8:1ff:febb…     ff02::16         ICMPv6     90 Multicast Listener Report Message v2
  209 25.370829   159.203.238.50           172.16.40.104    TCP        66 21 → 50699 [ACK] Seq=131 Ack=46 Win=29184 Len=0 TSval=373483131 TSecr=1099265468
  210 25.387433   172.16.40.104            159.203.238.50   TCP        66 50699 → 21 [FIN, ACK] Seq=46 Ack=131 Win=131616 Len=0 TSval=1099265767 TSecr=373483131
```

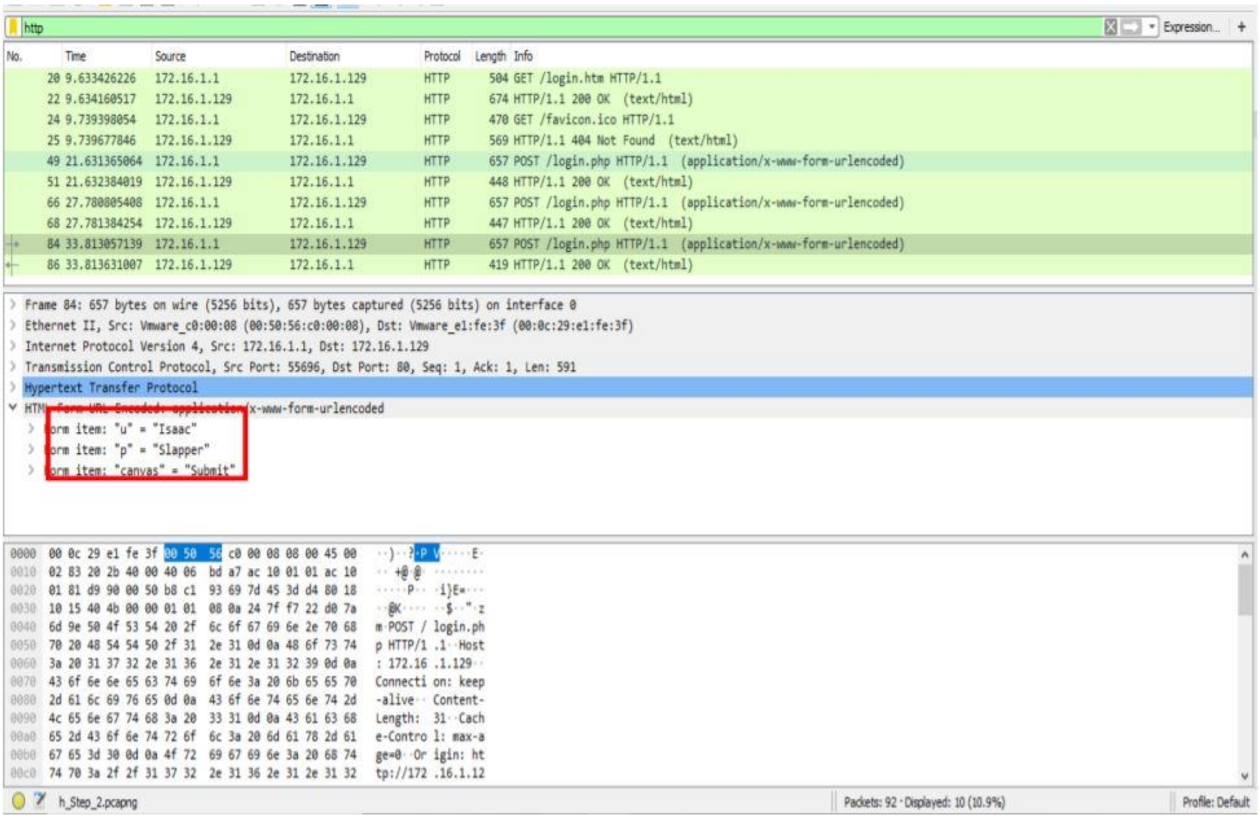
```
> Frame 204: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
> Ethernet II, Src: Apple_c3:9e:b3 (ac:bc:32:c3:9e:b3), Dst: RuijieNe_35:38:33 (58:69:6c:35:38:33)
> Internet Protocol Version 4, Src: 172.16.40.104, Dst: 159.203.238.50
> Transmission Control Protocol, Src Port: 50699, Dst Port: 21, Seq: 32, Ack: 131, Len: 14
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  58 69 6c 35 38 33 ac bc  32 c3 9e b3 08 00 45 00   Xil583·· 2·····E·
0010  00 42 8d 52 40 00 40 06  4a ed ac 10 28 68 9f cb   ·B·R@·@· J···(h··
0020  ee 32 c6 0b 00 15 f3 ed  af 54 d8 fb eb f6 80 18   ·2······ ·T······
0030  10 11 12 8f 00 00 01 01  08 0a 41 85 72 d9 16 42   ········ ··A·r··B
0040  e5 70 50 41 53 53 20 46  6c 61 70 70 65 72 0d 0a   ·pPASS F lapper··
```

File h_Step_2.pcapng

Username – Isaac

Password – Slapper



```
No.    Time          Source        Destination   Protocol Length Info
    20 9.633426226   172.16.1.1    172.16.1.129  HTTP      504 GET /login.htm HTTP/1.1
    22 9.634160517   172.16.1.129  172.16.1.1    HTTP      674 HTTP/1.1 200 OK  (text/html)
    24 9.739398054   172.16.1.1    172.16.1.129  HTTP      470 GET /favicon.ico HTTP/1.1
    25 9.739677846   172.16.1.129  172.16.1.1    HTTP      569 HTTP/1.1 404 Not Found  (text/html)
    49 21.631365064  172.16.1.1    172.16.1.129  HTTP      657 POST /login.php HTTP/1.1  (application/x-www-form-urlencoded)
    51 21.632384019  172.16.1.129  172.16.1.1    HTTP      448 HTTP/1.1 200 OK  (text/html)
    66 27.780805408  172.16.1.1    172.16.1.129  HTTP      657 POST /login.php HTTP/1.1  (application/x-www-form-urlencoded)
    68 27.781384254  172.16.1.129  172.16.1.1    HTTP      447 HTTP/1.1 200 OK  (text/html)
    84 33.813057139  172.16.1.1    172.16.1.129  HTTP      657 POST /login.php HTTP/1.1  (application/x-www-form-urlencoded)
    86 33.813631007  172.16.1.129  172.16.1.1    HTTP      419 HTTP/1.1 200 OK  (text/html)
```

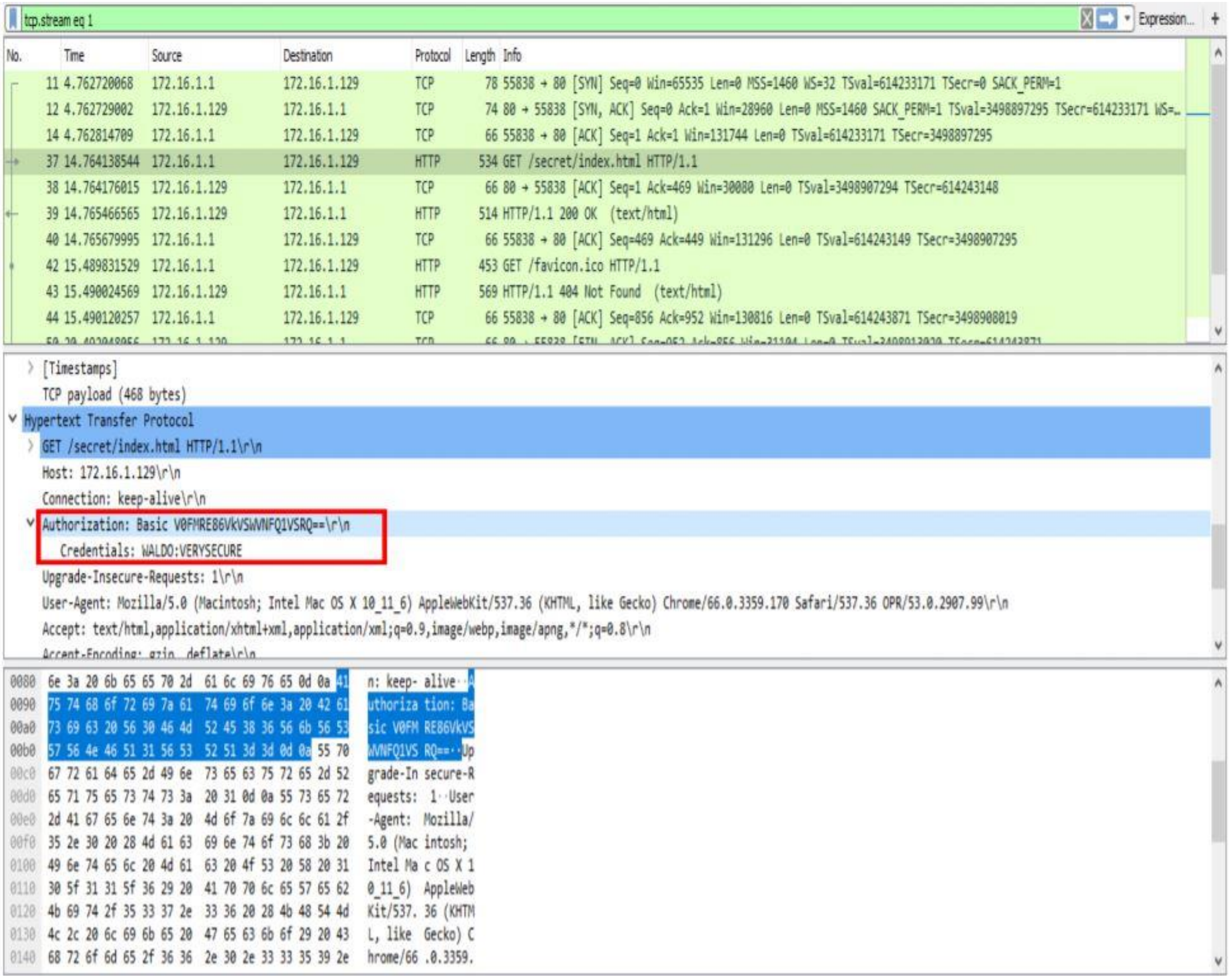
```
> Frame 84: 657 bytes on wire (5256 bits), 657 bytes captured (5256 bits) on interface 0
> Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Vmware_e1:fe:3f (00:0c:29:e1:fe:3f)
> Internet Protocol Version 4, Src: 172.16.1.1, Dst: 172.16.1.129
> Transmission Control Protocol, Src Port: 55696, Dst Port: 80, Seq: 1, Ack: 1, Len: 591
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "u" = "Isaac"
  > Form item: "p" = "Slapper"
  > Form item: "canvas" = "Submit"
```

```
0000  00 0c 29 e1 fe 3f 00 50  56 c0 00 08 08 00 45 00   ··)··?·P V·····E·
0010  02 83 20 2b 40 00 40 06  bd a7 ac 10 01 01 ac 10   ·· +@·@· ········
0020  01 81 d9 90 00 50 b8 c1  93 69 7d 45 3d d4 80 18   ·····P·· ·i}E=···
0030  10 15 40 4b 00 00 01 01  08 0a 24 7f f7 22 d0 7a   ··@K···· ··$··"·z
0040  6d 9e 50 4f 53 54 20 2f  6c 6f 67 69 6e 2e 70 68   m·POST / login.ph
0050  70 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   p HTTP/1 .1··Host
0060  3a 20 31 37 32 2e 31 36  2e 31 2e 31 32 39 0d 0a   : 172.16 .1.129··
0070  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 6b 65 65 70   Connecti on: keep
0080  2d 61 6c 69 76 65 0d 0a  43 6f 6e 74 65 6e 74 2d   -alive·· Content-
0090  4c 65 6e 67 74 68 3a 20  33 31 0d 0a 43 61 63 68   Length:  31··Cach
00a0  65 2d 43 6f 6e 74 72 6f  6c 3a 20 6d 61 78 2d 61   e-Contro l: max-a
00b0  67 65 3d 30 0d 0a 4f 72  69 67 69 6e 3a 20 68 74   ge=0··Or igin: ht
00c0  74 70 3a 2f 2f 31 37 32  2e 31 36 2e 31 2e 31 32   tp://172 .16.1.12
```

BasicLogin_intermediate.pcapng

Username –WALDO

Password – VERYSECURE



```
No.  Time          Source        Destination   Protocol Length Info
  11 4.762720068   172.16.1.1    172.16.1.129  TCP        78 55838 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=614233171 TSecr=0 SACK_PERM=1
  12 4.762729002   172.16.1.129  172.16.1.1    TCP        74 80 → 55838 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3498897295 TSecr=614233171 WS=…
  14 4.762814709   172.16.1.1    172.16.1.129  TCP        66 55838 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=614233171 TSecr=3498897295
  37 14.764138544  172.16.1.1    172.16.1.129  HTTP      534 GET /secret/index.html HTTP/1.1
  38 14.764176015  172.16.1.129  172.16.1.1    TCP        66 80 → 55838 [ACK] Seq=1 Ack=469 Win=30080 Len=0 TSval=3498907294 TSecr=614243148
  39 14.765466565  172.16.1.129  172.16.1.1    HTTP      514 HTTP/1.1 200 OK  (text/html)
  40 14.765679995  172.16.1.1    172.16.1.129  TCP        66 55838 → 80 [ACK] Seq=469 Ack=449 Win=131296 Len=0 TSval=614243149 TSecr=3498907295
  42 15.489831529  172.16.1.1    172.16.1.129  HTTP      453 GET /favicon.ico HTTP/1.1
  43 15.490024569  172.16.1.129  172.16.1.1    HTTP      569 HTTP/1.1 404 Not Found  (text/html)
  44 15.490120257  172.16.1.1    172.16.1.129  TCP        66 55838 → 80 [ACK] Seq=856 Ack=952 Win=130816 Len=0 TSval=614243871 TSecr=3498908019
  50 20.402048056  172.16.1.129  172.16.1.1    TCP        66 80 → 55838 [FIN, ACK] Seq=952 Ack=856 Win=31104 Len=0 TSval=3498913020 TSecr=614243871
```

```
  > [Timestamps]
    TCP payload (468 bytes)
v Hypertext Transfer Protocol
  > GET /secret/index.html HTTP/1.1\r\n
    Host: 172.16.1.129\r\n
    Connection: keep-alive\r\n
  v Authorization: Basic V0FMRE86VkVSWVNFQ1VSRQ==\r\n
      Credentials: WALDO:VERYSECURE
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.170 Safari/537.36 OPR/53.0.2907.99\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
```

```
0080  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 41   n: keep- alive··A
0090  75 74 68 6f 72 69 7a 61  74 69 6f 6e 3a 20 42 61   uthoriza tion: Ba
00a0  73 69 63 20 56 30 46 4d  52 45 38 36 56 6b 56 53   sic V0FM RE86VkVS
00b0  57 56 4e 46 51 31 56 53  52 51 3d 3d 0d 0a 55 70   WVNFQ1VS RQ==··Up
00c0  67 72 61 64 65 2d 49 6e  73 65 63 75 72 65 2d 52   grade-In secure-R
00d0  65 71 75 65 73 74 73 3a  20 31 0d 0a 55 73 65 72   equests:  1··User
00e0  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
00f0  35 2e 30 20 28 4d 61 63  69 6e 74 6f 73 68 3b 20   5.0 (Mac intosh;
0100  49 6e 74 65 6c 20 4d 61  63 20 4f 53 20 58 20 31   Intel Ma c OS X 1
0110  30 5f 31 31 5f 36 29 20  41 70 70 6c 65 57 65 62   0_11_6)  AppleWeb
0120  4b 69 74 2f 35 33 37 2e  33 36 20 28 4b 48 54 4d   Kit/537. 36 (KHTM
0130  4c 2c 20 6c 69 6b 65 20  47 65 63 6b 6f 29 20 43   L, like  Gecko) C
0140  68 72 6f 6d 65 2f 36 36  2e 30 2e 33 33 35 39 2e   hrome/66 .0.3359.
```