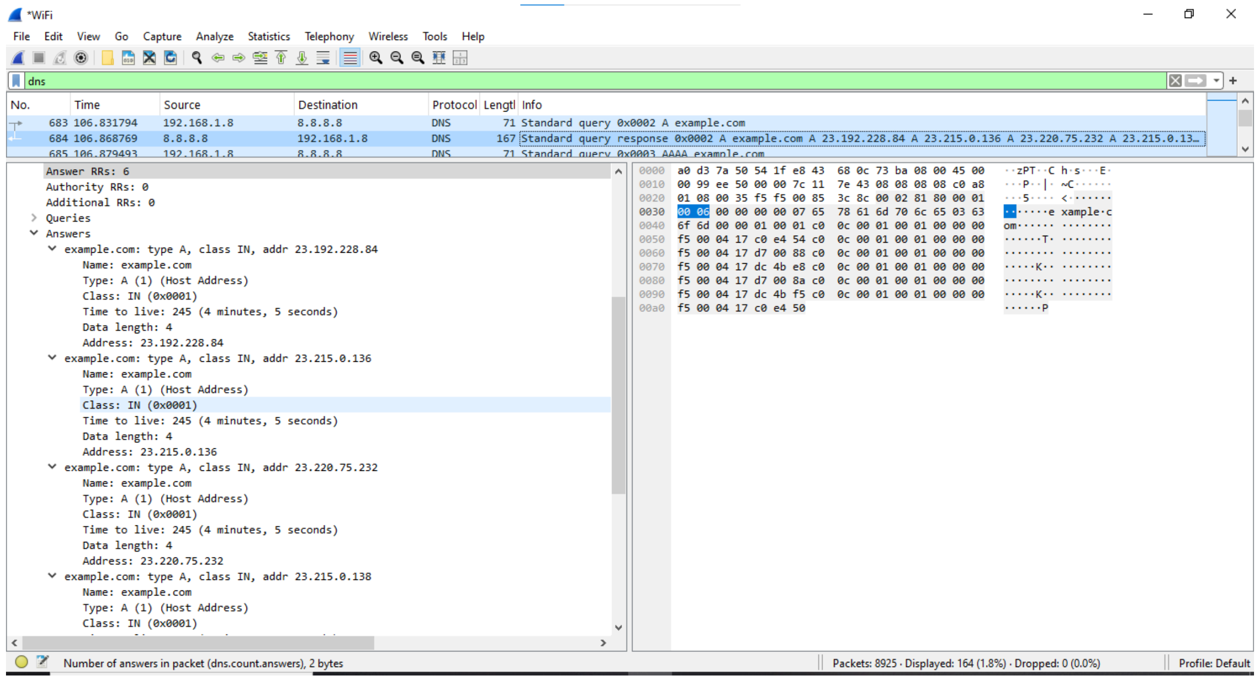
# A — DNS lookup for example.com

Open Wireshark → Start Capture → Apply filter: dns → Visit example.com (in browser) → Locate DNS response → Expand 'Answers' → Find A record (IPv4 address) .

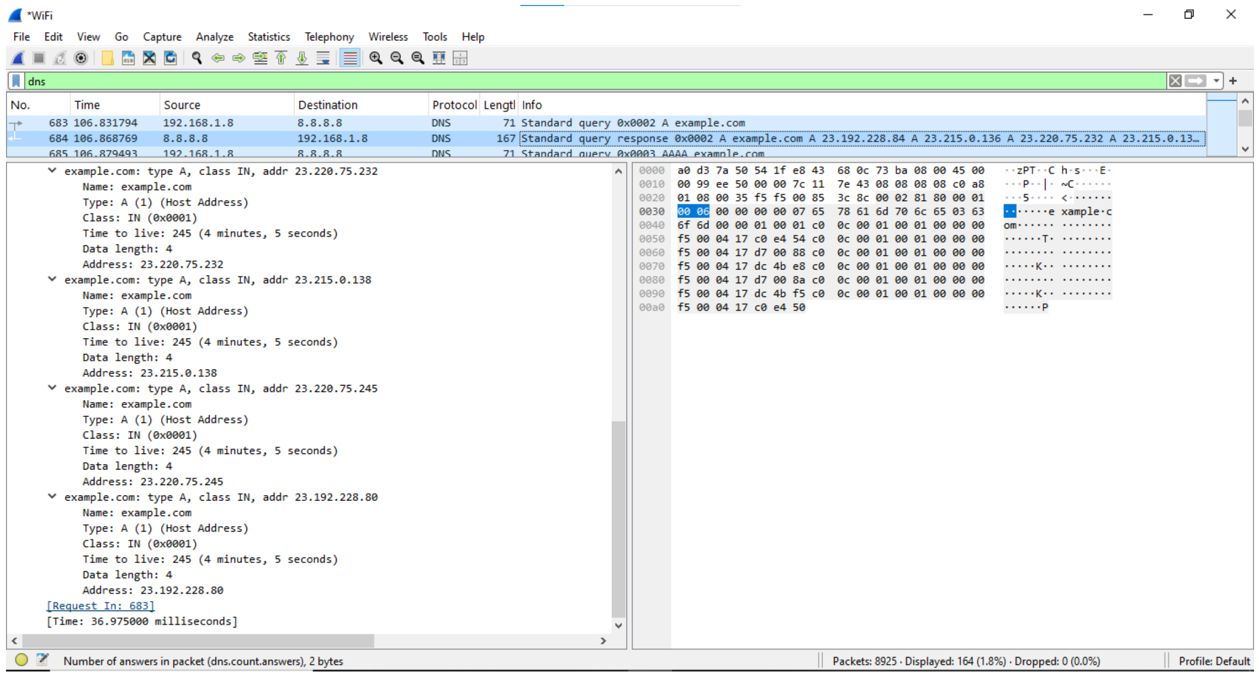


```
dns

No.   Time        Source        Destination   Protocol Lengtl Info
  683 106.831794  192.168.1.8   8.8.8.8       DNS         71 Standard query 0x0002 A example.com
  684 106.868769  8.8.8.8       192.168.1.8   DNS        167 Standard query response 0x0002 A example.com A 23.192.228.84 A 23.215.0.136 A 23.220.75.232 A 23.215.0.13…
  685 106.879493  192.168.1.8   8.8.8.8       DNS         71 Standard query 0x0003 AAAA example.com
```

```
      Answer RRs: 6
      Authority RRs: 0
      Additional RRs: 0
    > Queries
    v Answers
      v example.com: type A, class IN, addr 23.192.228.84
            Name: example.com
            Type: A (1) (Host Address)
            Class: IN (0x0001)
            Time to live: 245 (4 minutes, 5 seconds)
            Data length: 4
            Address: 23.192.228.84
      v example.com: type A, class IN, addr 23.215.0.136
            Name: example.com
            Type: A (1) (Host Address)
            Class: IN (0x0001)
            Time to live: 245 (4 minutes, 5 seconds)
            Data length: 4
            Address: 23.215.0.136
      v example.com: type A, class IN, addr 23.220.75.232
            Name: example.com
            Type: A (1) (Host Address)
            Class: IN (0x0001)
            Time to live: 245 (4 minutes, 5 seconds)
            Data length: 4
            Address: 23.220.75.232
      v example.com: type A, class IN, addr 23.215.0.138
            Name: example.com
            Type: A (1) (Host Address)
            Class: IN (0x0001)
```

```
0000  a0 d3 7a 50 54 1f e8 43  68 0c 73 ba 08 00 45 00   ··zPT··C h·s···E·
0010  00 99 ee 50 00 00 7c 11  7e 43 08 08 08 08 c0 a8   ···P··|· ~C······
0020  01 08 00 35 f5 f5 00 85  3c 8c 00 02 81 80 00 01   ···5···· <·······
0030  00 06 00 00 00 00 07 65  78 61 6d 70 6c 65 03 63   ·······e xample·c
0040  6f 6d 00 00 01 00 01 c0  0c 00 01 00 01 00 00 00   om······ ········
0050  f5 00 04 17 c0 e4 54 c0  0c 00 01 00 01 00 00 00   ······T· ········
0060  f5 00 04 17 d7 00 88 c0  0c 00 01 00 01 00 00 00   ········ ········
0070  f5 00 04 17 dc 4b e8 c0  0c 00 01 00 01 00 00 00   ·····K·· ········
0080  f5 00 04 17 d7 00 8a c0  0c 00 01 00 01 00 00 00   ········ ········
0090  f5 00 04 17 dc 4b f5 c0  0c 00 01 00 01 00 00 00   ·····K·· ········
00a0  f5 00 04 17 c0 e4 50                               ······P
```

Number of answers in packet (dns.count.answers), 2 bytes | Packets: 8925 · Displayed: 164 (1.8%) · Dropped: 0 (0.0%) | Profile: Default



```
dns

No.   Time        Source        Destination   Protocol Lengtl Info
  683 106.831794  192.168.1.8   8.8.8.8       DNS         71 Standard query 0x0002 A example.com
  684 106.868769  8.8.8.8       192.168.1.8   DNS        167 Standard query response 0x0002 A example.com A 23.192.228.84 A 23.215.0.136 A 23.220.75.232 A 23.215.0.13…
  685 106.879493  192.168.1.8   8.8.8.8       DNS         71 Standard query 0x0003 AAAA example.com
```

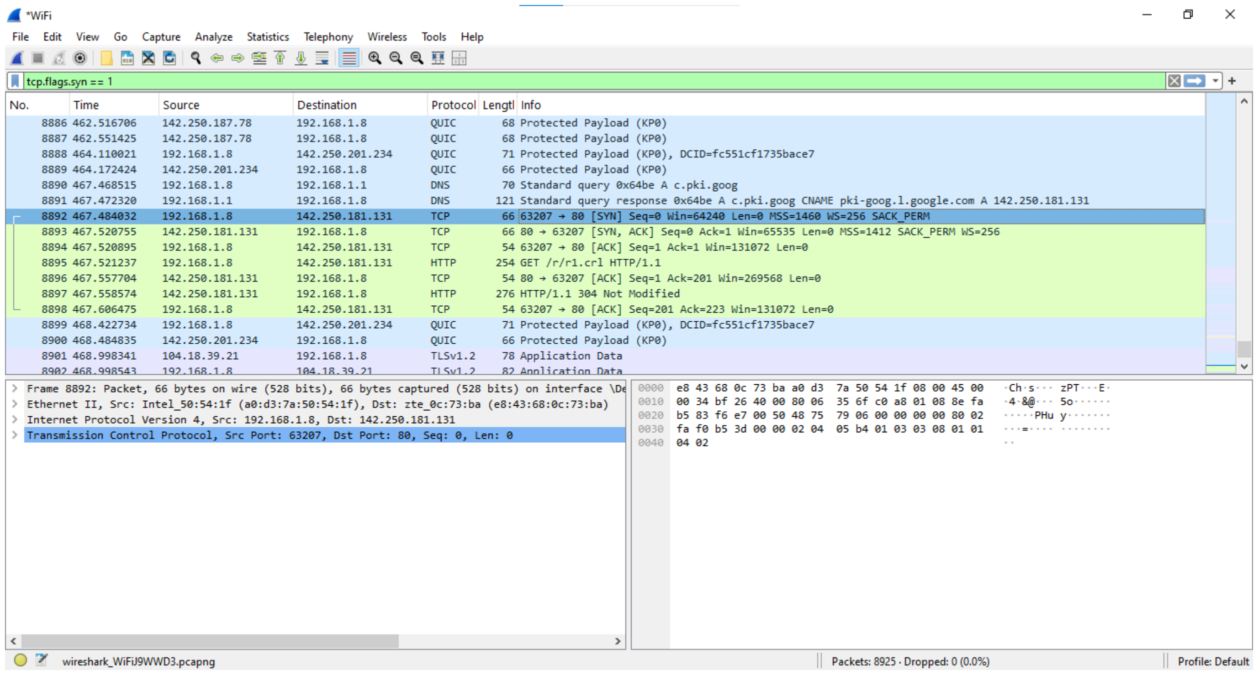
```
      v example.com: type A, class IN, addr 23.220.75.232
            Name: example.com
            Type: A (1) (Host Address)
            Class: IN (0x0001)
            Time to live: 245 (4 minutes, 5 seconds)
            Data length: 4
            Address: 23.220.75.232
      v example.com: type A, class IN, addr 23.215.0.138
            Name: example.com
            Type: A (1) (Host Address)
            Class: IN (0x0001)
            Time to live: 245 (4 minutes, 5 seconds)
            Data length: 4
            Address: 23.215.0.138
      v example.com: type A, class IN, addr 23.220.75.245
            Name: example.com
            Type: A (1) (Host Address)
            Class: IN (0x0001)
            Time to live: 245 (4 minutes, 5 seconds)
            Data length: 4
            Address: 23.220.75.245
      v example.com: type A, class IN, addr 23.192.228.80
            Name: example.com
            Type: A (1) (Host Address)
            Class: IN (0x0001)
            Time to live: 245 (4 minutes, 5 seconds)
            Data length: 4
            Address: 23.192.228.80
      [Request In: 683]
      [Time: 36.975000 milliseconds]
```

```
0000  a0 d3 7a 50 54 1f e8 43  68 0c 73 ba 08 00 45 00   ··zPT··C h·s···E·
0010  00 99 ee 50 00 00 7c 11  7e 43 08 08 08 08 c0 a8   ···P··|· ~C······
0020  01 08 00 35 f5 f5 00 85  3c 8c 00 02 81 80 00 01   ···5···· <·······
0030  00 06 00 00 00 00 07 65  78 61 6d 70 6c 65 03 63   ·······e xample·c
0040  6f 6d 00 00 01 00 01 c0  0c 00 01 00 01 00 00 00   om······ ········
0050  f5 00 04 17 c0 e4 54 c0  0c 00 01 00 01 00 00 00   ······T· ········
0060  f5 00 04 17 d7 00 88 c0  0c 00 01 00 01 00 00 00   ········ ········
0070  f5 00 04 17 dc 4b e8 c0  0c 00 01 00 01 00 00 00   ·····K·· ········
0080  f5 00 04 17 d7 00 8a c0  0c 00 01 00 01 00 00 00   ········ ········
0090  f5 00 04 17 dc 4b f5 c0  0c 00 01 00 01 00 00 00   ·····K·· ········
00a0  f5 00 04 17 c0 e4 50                               ······P
```

Number of answers in packet (dns.count.answers), 2 bytes | Packets: 8925 · Displayed: 164 (1.8%) · Dropped: 0 (0.0%) | Profile: Default

## B — TCP SYN (handshake) observation

Open Wireshark → Start Capture → Apply filter: tcp.flags.syn == 1 → Visit a website → Locate the three packets (SYN, SYN-ACK, ACK)



*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags.syn == 1
```

```
No.   Time        Source           Destination      Protocol Lengtl Info
 8886 462.516706  142.250.187.78   192.168.1.8      QUIC      68 Protected Payload (KP0)
 8887 462.551425  142.250.187.78   192.168.1.8      QUIC      68 Protected Payload (KP0)
 8888 464.110021  192.168.1.8      142.250.201.234  QUIC      71 Protected Payload (KP0), DCID=fc551cf1735bace7
 8889 464.172424  142.250.201.234  192.168.1.8      QUIC      66 Protected Payload (KP0)
 8890 467.468515  192.168.1.8      192.168.1.1      DNS       70 Standard query 0x64be A c.pki.goog
 8891 467.472320  192.168.1.1      192.168.1.8      DNS      121 Standard query response 0x64be A c.pki.goog CNAME pki-goog.l.google.com A 142.250.181.131
 8892 467.484032  192.168.1.8      142.250.181.131  TCP       66 63207 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 8893 467.520755  142.250.181.131  192.168.1.8      TCP       66 80 → 63207 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
 8894 467.520895  192.168.1.8      142.250.181.131  TCP       54 63207 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
 8895 467.521237  192.168.1.8      142.250.181.131  HTTP     254 GET /r/r1.crl HTTP/1.1
 8896 467.557704  142.250.181.131  192.168.1.8      TCP       54 80 → 63207 [ACK] Seq=1 Ack=201 Win=269568 Len=0
 8897 467.558574  142.250.181.131  192.168.1.8      HTTP     276 HTTP/1.1 304 Not Modified
 8898 467.606475  192.168.1.8      142.250.181.131  TCP       54 63207 → 80 [ACK] Seq=201 Ack=223 Win=131072 Len=0
 8899 468.422734  192.168.1.8      142.250.201.234  QUIC      71 Protected Payload (KP0), DCID=fc551cf1735bace7
 8900 468.484835  142.250.201.234  192.168.1.8      QUIC      66 Protected Payload (KP0)
 8901 468.998341  104.18.39.21     192.168.1.8      TLSv1.2   78 Application Data
 8902 468.998543  192.168.1.8      104.18.39.21     TLSv1.2   82 Application Data
```

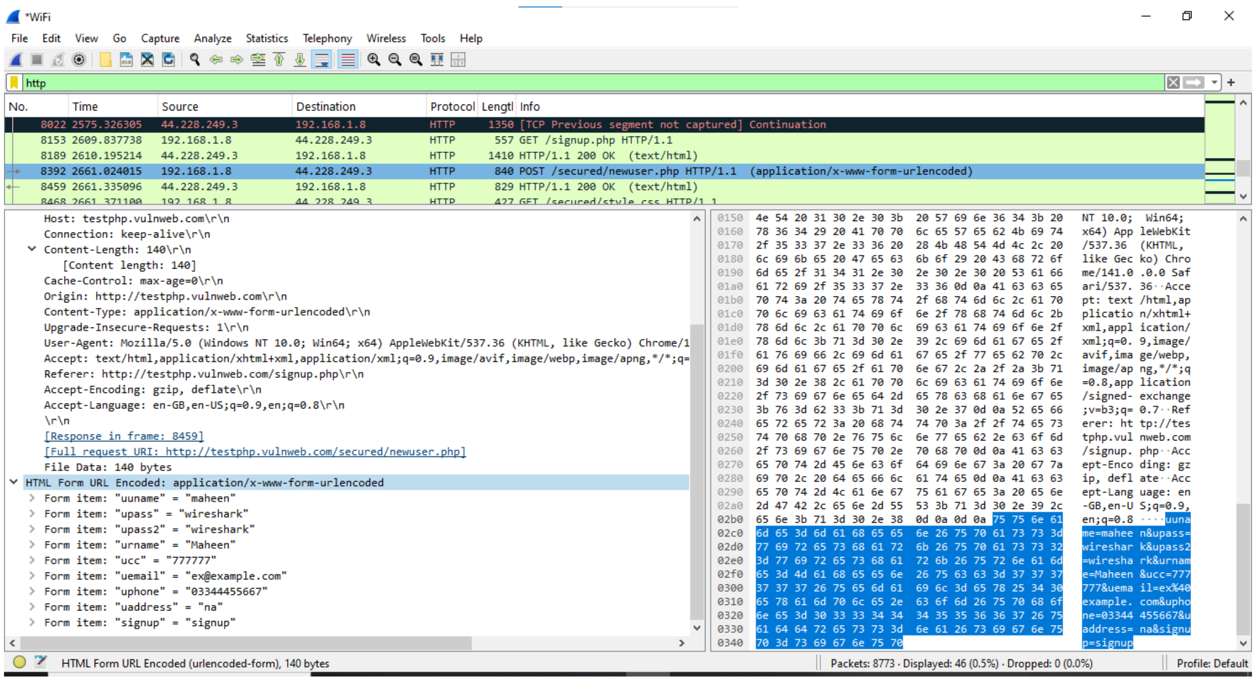
```
> Frame 8892: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \De
> Ethernet II, Src: Intel_50:54:1f (a0:d3:7a:50:54:1f), Dst: zte_0c:73:ba (e8:43:68:0c:73:ba)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 142.250.181.131
> Transmission Control Protocol, Src Port: 63207, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  e8 43 68 0c 73 ba a0 d3  7a 50 54 1f 08 00 45 00   ·Ch·s···  zPT···E·
0010  00 34 bf 26 40 00 80 06  35 6f c0 a8 01 08 8e fa   ·4·&@···  5o······
0020  b5 83 f6 e7 00 50 48 75  79 06 00 00 00 00 80 02   ·····PHu  y·······
0030  fa f0 b5 3d 00 00 02 04  05 b4 01 03 03 08 01 01   ···=····  ········
0040  04 02                                              ··
```

```
wireshark_WiFiJ9WWD3.pcapng        Packets: 8925 · Dropped: 0 (0.0%)        Profile: Default
```

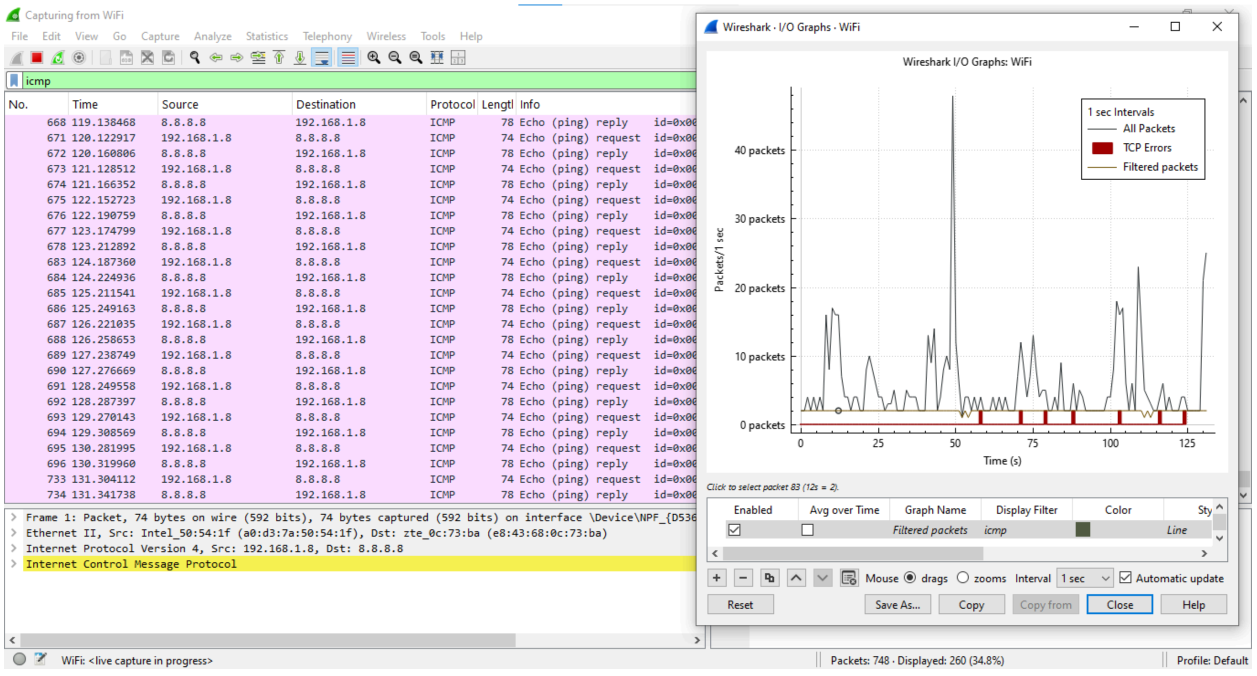
## C — Capture HTTP plaintext credentials (http filter)

Open Wireshark → Start Capture → Apply filter: http → Visit [http://testphp.vulnweb.com/login.php](http://testphp.vulnweb.com/login.php) → Submit fake login → Locate HTTP POST packet → Expand 'HTML Form URL Encoded'



```
*WiFi
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
http

No.   Time          Source         Destination    Protocol Lengtl Info
 8022 2575.326305   44.228.249.3   192.168.1.8    HTTP     1350 [TCP Previous segment not captured] Continuation
 8153 2609.837738   192.168.1.8    44.228.249.3   HTTP      557 GET /signup.php HTTP/1.1
 8189 2610.195214   44.228.249.3   192.168.1.8    HTTP     1410 HTTP/1.1 200 OK  (text/html)
 8392 2661.024015   192.168.1.8    44.228.249.3   HTTP      840 POST /secured/newuser.php HTTP/1.1  (application/x-www-form-urlencoded)
 8459 2661.335096   44.228.249.3   192.168.1.8    HTTP      829 HTTP/1.1 200 OK  (text/html)
 8468 2661.371100   192.168.1.8    44.228.249.3   HTTP      427 GET /secured/style.css HTTP/1.1

    Host: testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
  v Content-Length: 140\r\n
       [Content length: 140]
    Cache-Control: max-age=0\r\n
    Origin: http://testphp.vulnweb.com\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
    Referer: http://testphp.vulnweb.com/signup.php\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    \r\n
    [Response in frame: 8459]
    [Full request URI: http://testphp.vulnweb.com/secured/newuser.php]
    File Data: 140 bytes
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "uuname" = "maheen"
  > Form item: "upass" = "wireshark"
  > Form item: "upass2" = "wireshark"
  > Form item: "urname" = "Maheen"
  > Form item: "ucc" = "777777"
  > Form item: "uemail" = "ex@example.com"
  > Form item: "uphone" = "03344455667"
  > Form item: "uaddress" = "na"
  > Form item: "signup" = "signup"

0150  4e 54 20 31 30 2e 30 3b  20 57 69 6e 36 34 3b 20   NT 10.0;  Win64;
0160  78 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   x64) App leWebKit
0170  2f 35 33 37 2e 33 36 20  28 4b 48 54 4d 4c 2c 20   /537.36  (KHTML,
0180  6c 69 6b 65 20 47 65 63  6b 6f 29 20 43 68 72 6f   like Gec ko) Chro
0190  6d 65 2f 31 34 31 2e 30  2e 30 2e 30 20 53 61 66   me/141.0 .0.0 Saf
01a0  61 72 69 2f 35 33 37 2e  33 36 0d 0a 41 63 63 65   ari/537. 36··Acce
01b0  70 74 3a 20 74 65 78 74  2f 68 74 6d 6c 2c 61 70   pt: text /html,ap
01c0  70 6c 69 63 61 74 69 6f  6e 2f 78 68 74 6d 6c 2b   plicatio n/xhtml+
01d0  78 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   xml,appl ication/
01e0  78 6d 6c 3b 71 3d 30 2e  39 2c 69 6d 61 67 65 2f   xml;q=0. 9,image/
01f0  61 76 69 66 2c 69 6d 61  67 65 2f 77 65 62 70 2c   avif,ima ge/webp,
0200  69 6d 61 67 65 2f 61 70  6e 67 2c 2a 2f 2a 3b 71   image/ap ng,*/*;q
0210  3d 30 2e 38 2c 61 70 70  6c 69 63 61 74 69 6f 6e   =0.8,app lication
0220  2f 73 69 67 6e 65 64 2d  65 78 63 68 61 6e 67 65   /signed- exchange
0230  3b 76 3d 62 33 3b 71 3d  30 2e 37 0d 0a 52 65 66   ;v=b3;q= 0.7··Ref
0240  65 72 65 72 3a 20 68 74  74 70 3a 2f 2f 74 65 73   erer: ht tp://tes
0250  74 70 68 70 2e 76 75 6c  6e 77 65 62 2e 63 6f 6d   tphp.vul nweb.com
0260  2f 73 69 67 6e 75 70 2e  70 68 70 0d 0a 41 63 63   /signup. php··Acc
0270  65 70 74 2d 45 6e 63 6f  64 69 6e 67 3a 20 67 7a   ept-Enco ding: gz
0280  69 70 2c 20 64 65 66 6c  61 74 65 0d 0a 41 63 63   ip, defl ate··Acc
0290  65 70 74 2d 4c 61 6e 67  75 61 67 65 3a 20 65 6e   ept-Lang uage: en
02a0  2d 47 42 2c 65 6e 2d 55  53 3b 71 3d 30 2e 39 2c   -GB,en-U S;q=0.9,
02b0  65 6e 3b 71 3d 30 2e 38  0d 0a 0d 0a 75 75 6e 61   en;q=0.8 ····uuna
02c0  6d 65 3d 6d 61 68 65 65  6e 26 75 70 61 73 73 3d   me=mahee n&upass=
02d0  77 69 72 65 73 68 61 72  6b 26 75 70 61 73 73 32   wireshar k&upass2
02e0  3d 77 69 72 65 73 68 61  72 6b 26 75 72 6e 61 6d   =wiresha rk&urnam
02f0  65 3d 4d 61 68 65 65 6e  26 75 63 63 3d 37 37 37   e=Maheen &ucc=777
0300  37 37 37 26 75 65 6d 61  69 6c 3d 65 78 25 34 30   777&uema il=ex%40
0310  65 78 61 6d 70 6c 65 2e  63 6f 6d 26 75 70 68 6f   example. com&upho
0320  6e 65 3d 30 33 33 34 34  34 35 35 36 36 37 26 75   ne=03344 455667&u
0330  61 64 64 72 65 73 73 3d  6e 61 26 73 69 67 6e 75   address= na&signu
0340  70 3d 73 69 67 6e 75 70                            p=signup

HTML Form URL Encoded (urlencoded-form), 140 bytes   Packets: 8773 · Displayed: 46 (0.5%) · Dropped: 0 (0.0%)   Profile: Default
```

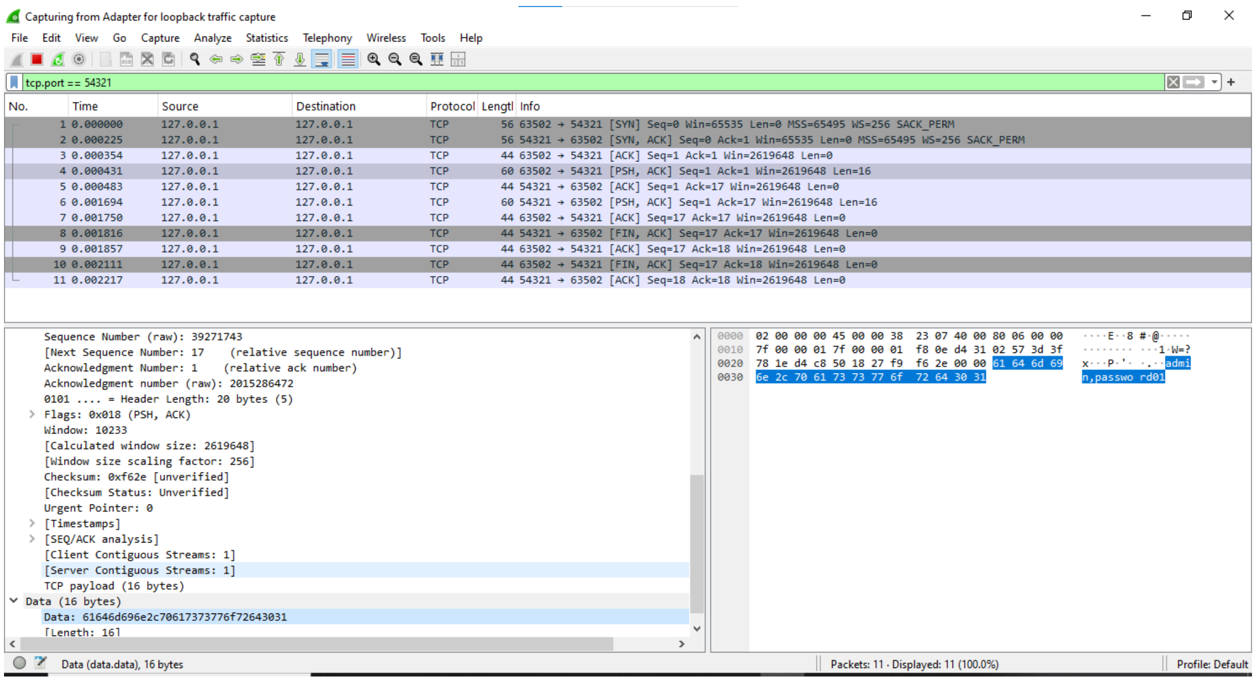
## D — ICMP ping and detecting ICMP flood



```
Capturing from WiFi
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
icmp

No.  Time         Source        Destination   Protocol Lengtl Info
 668 119.138468   8.8.8.8       192.168.1.8   ICMP     78 Echo (ping) reply    id=0x00
 671 120.122917   192.168.1.8   8.8.8.8       ICMP     74 Echo (ping) request  id=0x00
 672 120.160806   8.8.8.8       192.168.1.8   ICMP     78 Echo (ping) reply    id=0x00
 673 121.128512   192.168.1.8   8.8.8.8       ICMP     74 Echo (ping) request  id=0x00
 674 121.166352   8.8.8.8       192.168.1.8   ICMP     78 Echo (ping) reply    id=0x00
 675 122.152723   192.168.1.8   8.8.8.8       ICMP     74 Echo (ping) request  id=0x00
 676 122.190759   8.8.8.8       192.168.1.8   ICMP     78 Echo (ping) reply    id=0x00
 677 123.174799   192.168.1.8   8.8.8.8       ICMP     74 Echo (ping) request  id=0x00
 678 123.212892   8.8.8.8       192.168.1.8   ICMP     78 Echo (ping) reply    id=0x00
 683 124.187360   192.168.1.8   8.8.8.8       ICMP     74 Echo (ping) request  id=0x00
 684 124.224936   8.8.8.8       192.168.1.8   ICMP     78 Echo (ping) reply    id=0x00
 685 125.211541   192.168.1.8   8.8.8.8       ICMP     74 Echo (ping) request  id=0x00
 686 125.249163   8.8.8.8       192.168.1.8   ICMP     78 Echo (ping) reply    id=0x00
 687 126.221035   192.168.1.8   8.8.8.8       ICMP     74 Echo (ping) request  id=0x00
 688 126.258653   8.8.8.8       192.168.1.8   ICMP     78 Echo (ping) reply    id=0x00
 689 127.238749   192.168.1.8   8.8.8.8       ICMP     74 Echo (ping) request  id=0x00
 690 127.276669   8.8.8.8       192.168.1.8   ICMP     78 Echo (ping) reply    id=0x00
 691 128.249558   192.168.1.8   8.8.8.8       ICMP     74 Echo (ping) request  id=0x00
 692 128.287397   8.8.8.8       192.168.1.8   ICMP     78 Echo (ping) reply    id=0x00
 693 129.270143   192.168.1.8   8.8.8.8       ICMP     74 Echo (ping) request  id=0x00
 694 129.308569   8.8.8.8       192.168.1.8   ICMP     78 Echo (ping) reply    id=0x00
 695 130.281995   192.168.1.8   8.8.8.8       ICMP     74 Echo (ping) request  id=0x00
 696 130.319960   8.8.8.8       192.168.1.8   ICMP     78 Echo (ping) reply    id=0x00
 733 131.304112   192.168.1.8   8.8.8.8       ICMP     74 Echo (ping) request  id=0x00
 734 131.341738   8.8.8.8       192.168.1.8   ICMP     78 Echo (ping) reply    id=0x00

> Frame 1: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D536
> Ethernet II, Src: Intel_50:54:1f (a0:d3:7a:50:54:1f), Dst: zte_0c:73:ba (e8:43:68:0c:73:ba)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 8.8.8.8
> Internet Control Message Protocol

WiFi: <live capture in progress>   Packets: 748 · Displayed: 260 (34.8%)   Profile: Default

Wireshark · I/O Graphs · WiFi
Click to select packet 83 (12s = 2).
Enabled  Avg over Time  Graph Name        Display Filter  Color  Sty
[✓]      [ ]            Filtered packets  icmp            ■      Line
Mouse (●) drags  ( ) zooms   Interval 1 sec   [✓] Automatic update
Reset   Save As...   Copy   Copy from   Close   Help
```

## E — Local TCP server & client (capture SYN, SYN-ACK, ACK)

Open Wireshark → Select Loopback Interface → Apply filter: tcp.port == 54321 → Run python server.py → Run python client.py → Locate SYN→SYN-ACK→ACK → Locate Data (PSH, ACK) packet → Expand TCP Payload/Data


Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 54321

```
No.  Time      Source     Destination Protocol Lengtl Info
   1 0.000000  127.0.0.1  127.0.0.1   TCP      56 63502 → 54321 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
   2 0.000225  127.0.0.1  127.0.0.1   TCP      56 54321 → 63502 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
   3 0.000354  127.0.0.1  127.0.0.1   TCP      44 63502 → 54321 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
   4 0.000431  127.0.0.1  127.0.0.1   TCP      60 63502 → 54321 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=16
   5 0.000483  127.0.0.1  127.0.0.1   TCP      44 54321 → 63502 [ACK] Seq=1 Ack=17 Win=2619648 Len=0
   6 0.001694  127.0.0.1  127.0.0.1   TCP      60 54321 → 63502 [PSH, ACK] Seq=1 Ack=17 Win=2619648 Len=16
   7 0.001750  127.0.0.1  127.0.0.1   TCP      44 63502 → 54321 [ACK] Seq=17 Ack=17 Win=2619648 Len=0
   8 0.001816  127.0.0.1  127.0.0.1   TCP      44 54321 → 63502 [FIN, ACK] Seq=17 Ack=17 Win=2619648 Len=0
   9 0.001857  127.0.0.1  127.0.0.1   TCP      44 63502 → 54321 [ACK] Seq=17 Ack=18 Win=2619648 Len=0
  10 0.002111  127.0.0.1  127.0.0.1   TCP      44 63502 → 54321 [FIN, ACK] Seq=17 Ack=18 Win=2619648 Len=0
  11 0.002217  127.0.0.1  127.0.0.1   TCP      44 54321 → 63502 [ACK] Seq=18 Ack=18 Win=2619648 Len=0
```

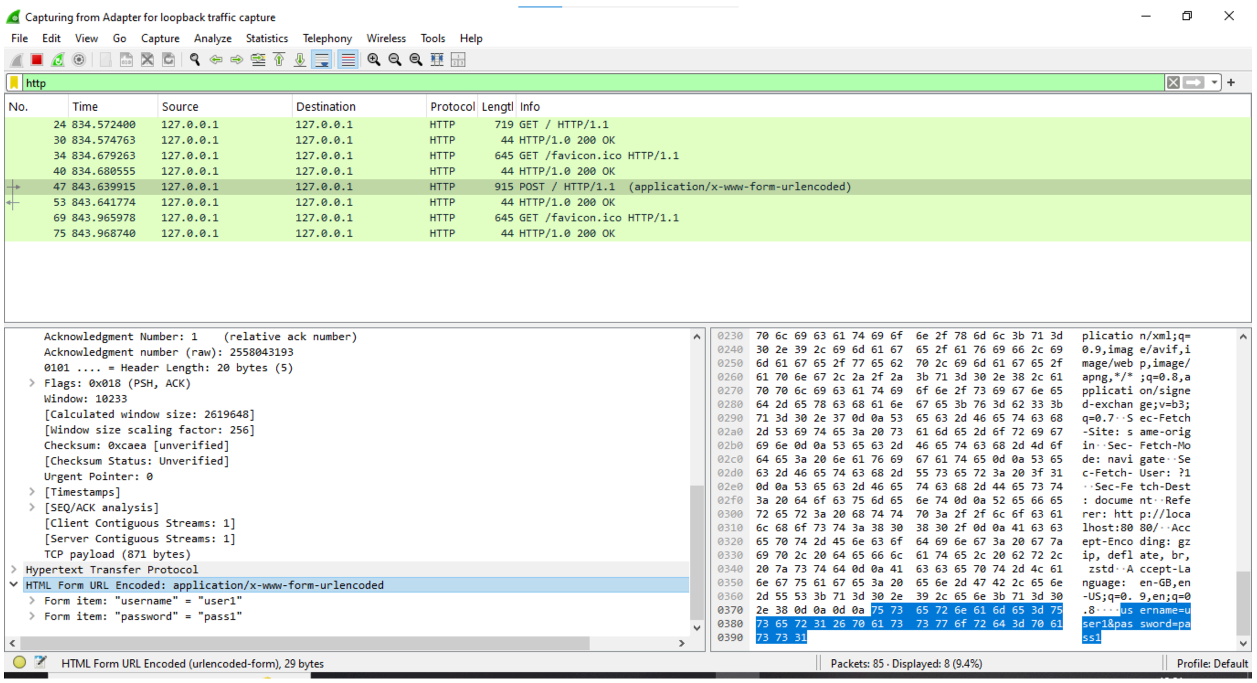
```
    Sequence Number (raw): 39271743
    [Next Sequence Number: 17    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2015286472
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 10233
    [Calculated window size: 2619648]
    [Window size scaling factor: 256]
    Checksum: 0xf62e [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    [Client Contiguous Streams: 1]
    [Server Contiguous Streams: 1]
    TCP payload (16 bytes)
v Data (16 bytes)
    Data: 61646d696e2c70617373776f72643031
    [Length: 16]
```

```
0000  02 00 00 00 45 00 00 38  23 07 40 00 80 06 00 00   ····E··8 #·@·····
0010  7f 00 00 01 7f 00 00 01  f8 0e d4 31 02 57 3d 3f   ········ ···1·W=?
0020  78 1e d4 c8 50 18 27 f9  f6 2e 00 00 61 64 6d 69   x···P·'· ·.··admi
0030  6e 2c 70 61 73 73 77 6f  72 64 30 31               n,passwo rd01
```

Data (data.data), 16 bytes | Packets: 11 · Displayed: 11 (100.0%) | Profile: Default

## F — Local Python HTTP server and submit dummy login (capture with `http`)

Open Wireshark → Select Loopback Interface → Apply filter: http → Run python http_server.py → Visit http://localhost:8080 → Submit fake login → Locate HTTP POST packet → Expand HTML Form URL Encoded


Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time        Source      Destination  Protocol Lengtl Info
   24 834.572400  127.0.0.1   127.0.0.1    HTTP      719 GET / HTTP/1.1
   30 834.574763  127.0.0.1   127.0.0.1    HTTP       44 HTTP/1.0 200 OK
   34 834.679263  127.0.0.1   127.0.0.1    HTTP      645 GET /favicon.ico HTTP/1.1
   40 834.680555  127.0.0.1   127.0.0.1    HTTP       44 HTTP/1.0 200 OK
   47 843.639915  127.0.0.1   127.0.0.1    HTTP      915 POST / HTTP/1.1  (application/x-www-form-urlencoded)
   53 843.641774  127.0.0.1   127.0.0.1    HTTP       44 HTTP/1.0 200 OK
   69 843.965978  127.0.0.1   127.0.0.1    HTTP      645 GET /favicon.ico HTTP/1.1
   75 843.968740  127.0.0.1   127.0.0.1    HTTP       44 HTTP/1.0 200 OK
```

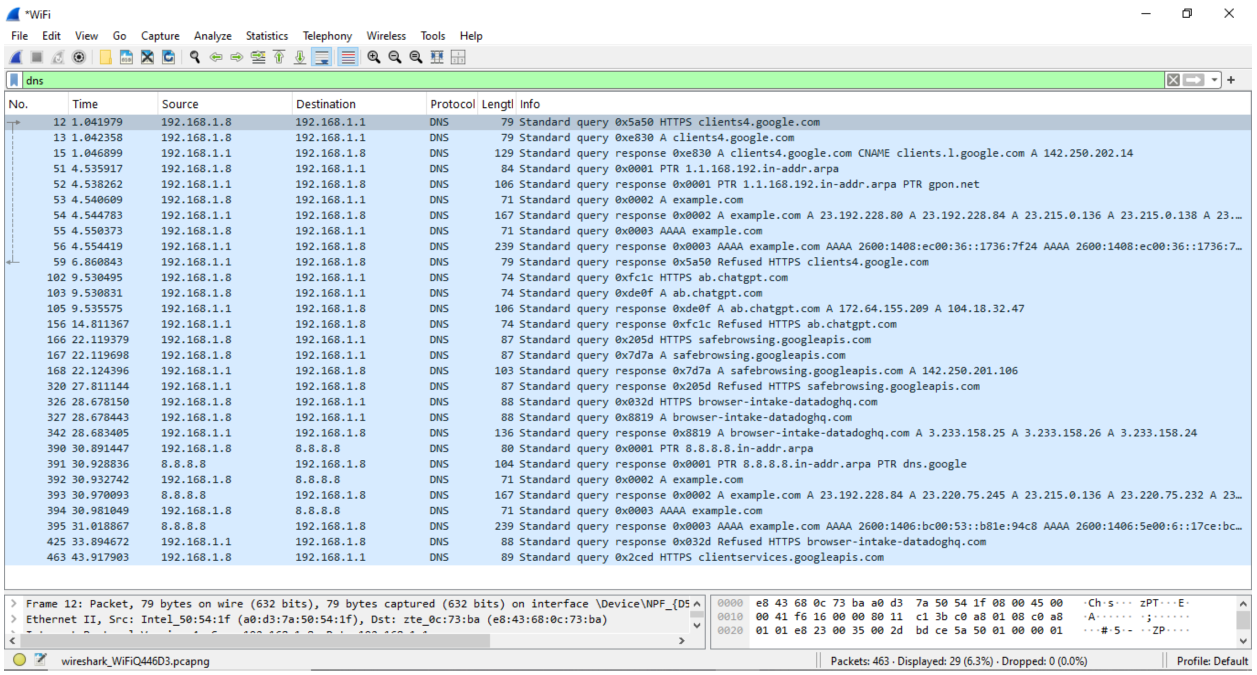
```
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2558043193
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 10233
    [Calculated window size: 2619648]
    [Window size scaling factor: 256]
    Checksum: 0xcaea [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    [Client Contiguous Streams: 1]
    [Server Contiguous Streams: 1]
    TCP payload (871 bytes)
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "username" = "user1"
  > Form item: "password" = "pass1"
```

```
0230  70 6c 69 63 61 74 69 6f  6e 2f 78 6d 6c 3b 71 3d   plicatio n/xml;q=
0240  30 2e 39 2c 69 6d 61 67  65 2f 61 76 69 66 2c 69   0.9,imag e/avif,i
0250  6d 61 67 65 2f 77 65 62  70 2c 69 6d 61 67 65 2f   mage/web p,image/
0260  61 70 6e 67 2c 2a 2f 2a  3b 71 3d 30 2e 38 2c 61   apng,*/* ;q=0.8,a
0270  70 70 6c 69 63 61 74 69  6f 6e 2f 73 69 67 6e 65   pplicati on/signe
0280  64 2d 65 78 63 68 61 6e  67 65 3b 76 3d 62 33 3b   d-exchan ge;v=b3;
0290  71 3d 30 2e 37 0d 0a 53  65 63 2d 46 65 74 63 68   q=0.7··S ec-Fetch
02a0  2d 53 69 74 65 3a 20 73  61 6d 65 2d 6f 72 69 67   -Site: s ame-orig
02b0  69 6e 0d 0a 53 65 63 2d  46 65 74 63 68 2d 4d 6f   in··Sec- Fetch-Mo
02c0  64 65 3a 20 6e 61 76 69  67 61 74 65 0d 0a 53 65   de: navi gate··Se
02d0  63 2d 46 65 74 63 68 2d  55 73 65 72 3a 20 3f 31   c-Fetch- User: ?1
02e0  0d 0a 53 65 63 2d 46 65  74 63 68 2d 44 65 73 74   ··Sec-Fe tch-Dest
02f0  3a 20 64 6f 63 75 6d 65  6e 74 0d 0a 52 65 66 65   : docume nt··Refe
0300  72 65 72 3a 20 68 74 74  70 3a 2f 2f 6c 6f 63 61   rer: htt p://loca
0310  6c 68 6f 73 74 3a 38 30  38 30 2f 0d 0a 41 63 63   lhost:80 80/··Acc
0320  65 70 74 2d 45 6e 63 6f  64 69 6e 67 3a 20 67 7a   ept-Enco ding: gz
0330  69 70 2c 20 64 65 66 6c  61 74 65 2c 20 62 72 2c   ip, defl ate, br,
0340  20 7a 73 74 64 0d 0a 41  63 63 65 70 74 2d 4c 61    zstd··A ccept-La
0350  6e 67 75 61 67 65 3a 20  65 6e 2d 47 42 2c 65 6e   nguage:  en-GB,en
0360  2d 55 53 3b 71 3d 30 2e  39 2c 65 6e 3b 71 3d 30   -US;q=0. 9,en;q=0
0370  2e 38 0d 0a 0d 0a 75 73  65 72 6e 61 6d 65 3d 75   .8····us ername=u
0380  73 65 72 31 26 70 61 73  73 77 6f 72 64 3d 70 61   ser1&pas sword=pa
0390  73 73 31                                           ss1
```

```
HTML Form URL Encoded (urlencoded-form), 29 bytes    Packets: 85 · Displayed: 8 (9.4%)    Profile: Default
```

## G — nslookup and DNS spoof explanation

Open Wireshark → Start Capture → Apply filter: dns → Run nslookup example.com → Run nslookup example.com 8.8.8.8


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time        Source        Destination  Protocol Lengtl Info
   12 1.041979    192.168.1.8   192.168.1.1  DNS       79 Standard query 0x5a50 HTTPS clients4.google.com
   13 1.042358    192.168.1.8   192.168.1.1  DNS       79 Standard query 0xe830 A clients4.google.com
   15 1.046899    192.168.1.1   192.168.1.8  DNS      129 Standard query response 0xe830 A clients4.google.com CNAME clients.l.google.com A 142.250.202.14
   51 4.535917    192.168.1.8   192.168.1.1  DNS       84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
   52 4.538262    192.168.1.1   192.168.1.8  DNS      106 Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR gpon.net
   53 4.540609    192.168.1.8   192.168.1.1  DNS       71 Standard query 0x0002 A example.com
   54 4.544783    192.168.1.1   192.168.1.8  DNS      167 Standard query response 0x0002 A example.com A 23.192.228.80 A 23.192.228.84 A 23.215.0.136 A 23.215.0.138 A 23…
   55 4.550373    192.168.1.8   192.168.1.1  DNS       71 Standard query 0x0003 AAAA example.com
   56 4.554419    192.168.1.1   192.168.1.8  DNS      239 Standard query response 0x0003 AAAA example.com AAAA 2600:1408:ec00:36::1736:7f24 AAAA 2600:1408:ec00:36::1736:7…
   59 6.860843    192.168.1.1   192.168.1.8  DNS       79 Standard query response 0x5a50 Refused HTTPS clients4.google.com
  102 9.530495    192.168.1.8   192.168.1.1  DNS       74 Standard query 0xfc1c HTTPS ab.chatgpt.com
  103 9.530831    192.168.1.8   192.168.1.1  DNS       74 Standard query 0xde0f A ab.chatgpt.com
  105 9.535575    192.168.1.1   192.168.1.8  DNS      106 Standard query response 0xde0f A ab.chatgpt.com A 172.64.155.209 A 104.18.32.47
  156 14.811367   192.168.1.1   192.168.1.8  DNS       74 Standard query response 0xfc1c Refused HTTPS ab.chatgpt.com
  166 22.119379   192.168.1.8   192.168.1.1  DNS       87 Standard query 0x205d HTTPS safebrowsing.googleapis.com
  167 22.119698   192.168.1.8   192.168.1.1  DNS       87 Standard query 0x7d7a A safebrowsing.googleapis.com
  168 22.124396   192.168.1.1   192.168.1.8  DNS      103 Standard query response 0x7d7a A safebrowsing.googleapis.com A 142.250.201.106
  320 27.811144   192.168.1.1   192.168.1.8  DNS       87 Standard query response 0x205d Refused HTTPS safebrowsing.googleapis.com
  326 28.678150   192.168.1.8   192.168.1.1  DNS       88 Standard query 0x032d HTTPS browser-intake-datadoghq.com
  327 28.678443   192.168.1.8   192.168.1.1  DNS       88 Standard query 0x8819 A browser-intake-datadoghq.com
  342 28.683405   192.168.1.1   192.168.1.8  DNS      136 Standard query response 0x8819 A browser-intake-datadoghq.com A 3.233.158.25 A 3.233.158.26 A 3.233.158.24
  390 30.891447   192.168.1.8   8.8.8.8      DNS       80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
  391 30.928836   8.8.8.8       192.168.1.8  DNS      104 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
  392 30.932742   192.168.1.8   8.8.8.8      DNS       71 Standard query 0x0002 A example.com
  393 30.970093   8.8.8.8       192.168.1.8  DNS      167 Standard query response 0x0002 A example.com A 23.192.228.84 A 23.220.75.245 A 23.215.0.136 A 23.220.75.232 A 23…
  394 30.981049   192.168.1.8   8.8.8.8      DNS       71 Standard query 0x0003 AAAA example.com
  395 31.018867   8.8.8.8       192.168.1.8  DNS      239 Standard query response 0x0003 AAAA example.com AAAA 2600:1406:bc00:53::b81e:94c8 AAAA 2600:1406:5e00:6::17ce:bc…
  425 33.894672   192.168.1.1   192.168.1.8  DNS       88 Standard query response 0x032d Refused HTTPS browser-intake-datadoghq.com
  463 43.917903   192.168.1.8   192.168.1.1  DNS       89 Standard query 0x2ced HTTPS clientservices.googleapis.com
```

```
> Frame 12: Packet, 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{D5
> Ethernet II, Src: Intel_50:54:1f (a0:d3:7a:50:54:1f), Dst: zte_0c:73:ba (e8:43:68:0c:73:ba)
```

```
0000  e8 43 68 0c 73 ba a0 d3  7a 50 54 1f 08 00 45 00   ·Ch·s··· zPT···E·
0010  00 41 f6 16 00 00 80 11  c1 3b c0 a8 01 08 c0 a8   ·A······ ·;······
0020  01 01 e8 23 00 35 00 2d  bd ce 5a 50 01 00 00 01   ···#·5·- ··ZP····
```

```
wireshark_WiFiQ446D3.pcapng    Packets: 463 · Displayed: 29 (6.3%) · Dropped: 0 (0.0%)    Profile: Default
```

### How attackers could spoof DNS responses (simple):

- DNS spoofing (a.k.a. cache poisoning) tricks a resolver into storing a forged answer. If an attacker can send a fake DNS response to your resolver before the real one arrives, your machine may be given a malicious IP for a domain (so you get sent to a fake site). Attackers can also run a rogue DNS server on a LAN and intercept/answer queries with fake addresses.

## H — Difference: Display vs Capture Filters & Why HTTPS is needed

**Display filters (Wireshark):**

- Applied after capture. They only *hide/show* packets in the GUI — they do not change what packets were captured.
- Example: `http` or `tcp.port == 54321`

**Capture filters (when you start capturing):**

- Specify which packets to actually save while capturing. Fewer packets means smaller captures and less load.
- Uses BPF syntax. Example: `port 80` or `icmp` as capture filter when starting capture.

**Why HTTPS is needed (simple):**

- HTTPS encrypts data between your browser and the server. This prevents eavesdroppers (anyone capturing network traffic) from reading usernames, passwords, session cookies, or page content. It also ensures the server you talk to is the real server (certificate verification), helping prevent man-in-the-middle attacks.