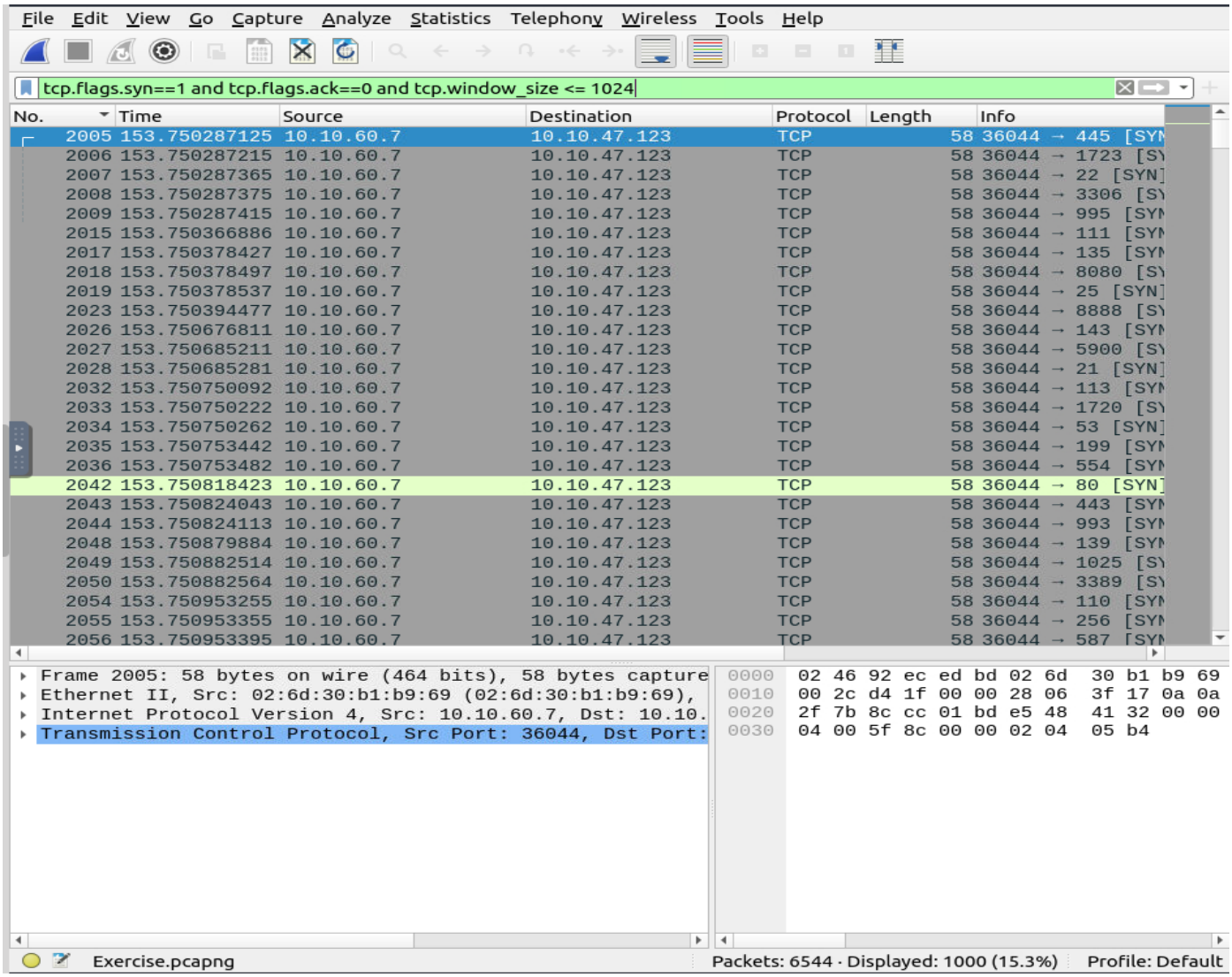
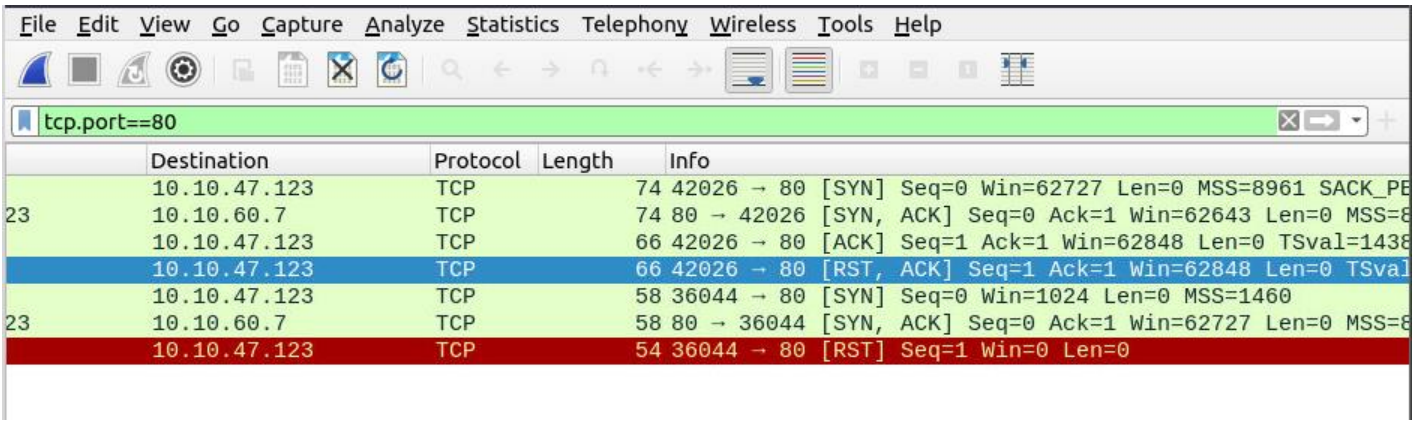
Analysis NMAP scans by potential adversary:

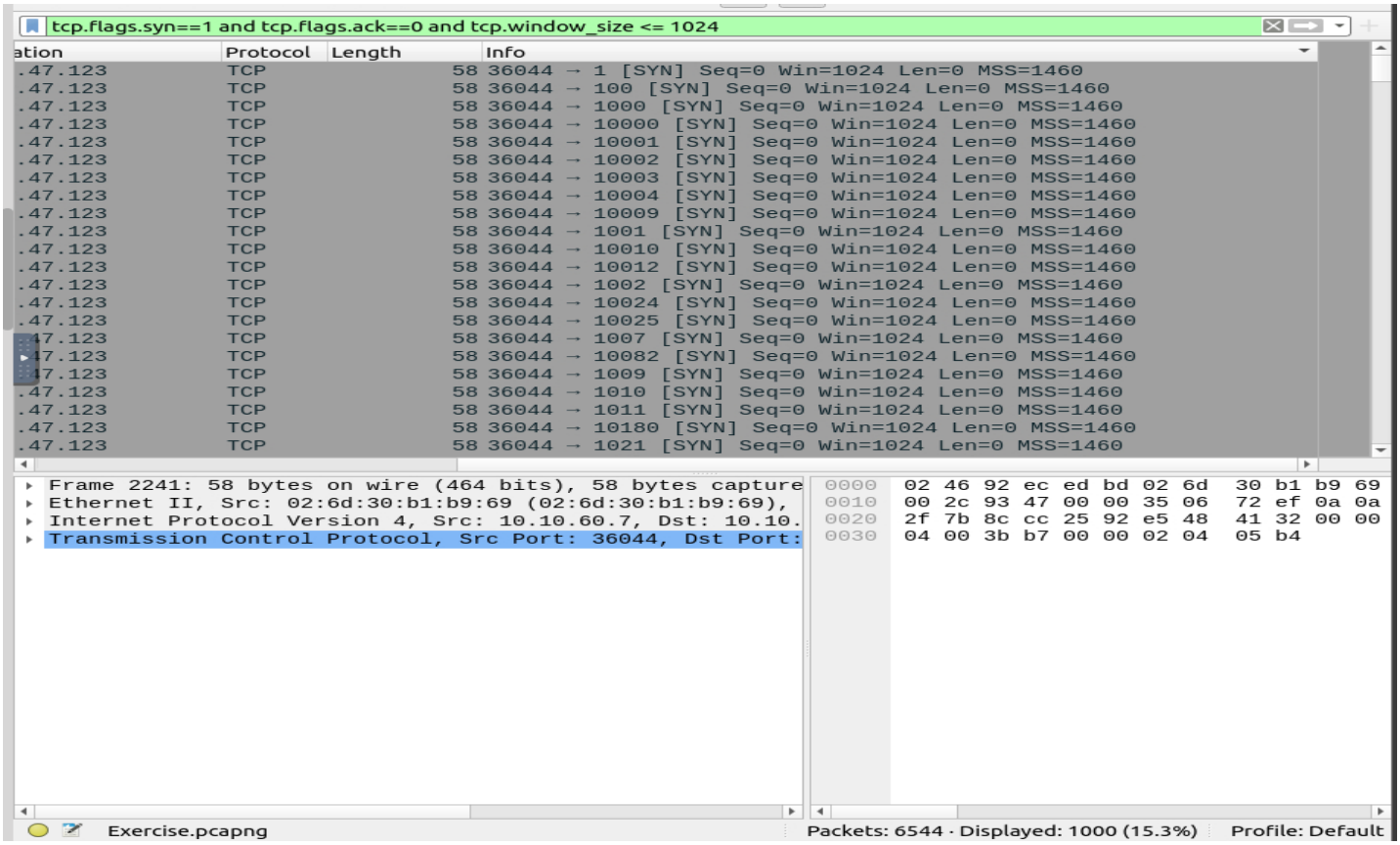
1. Number of TCP Connect is 1000



2. The type is used to scan the TCP port 80 and it's a open TCP port connection because of the full handshake



3. The number of sys pacakets by the syn scan is 1000



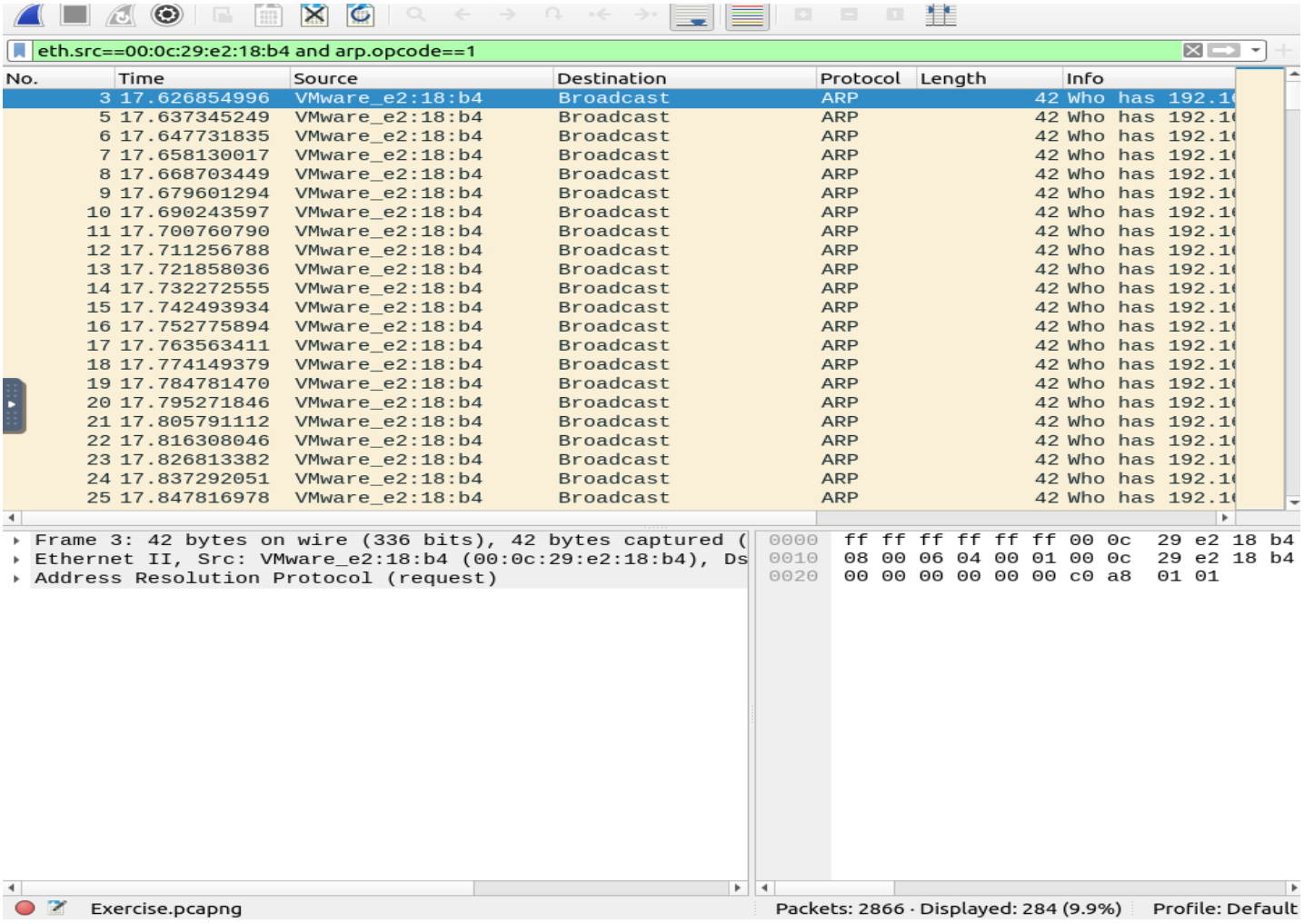
+==========+

ARP poisoning and MITM:

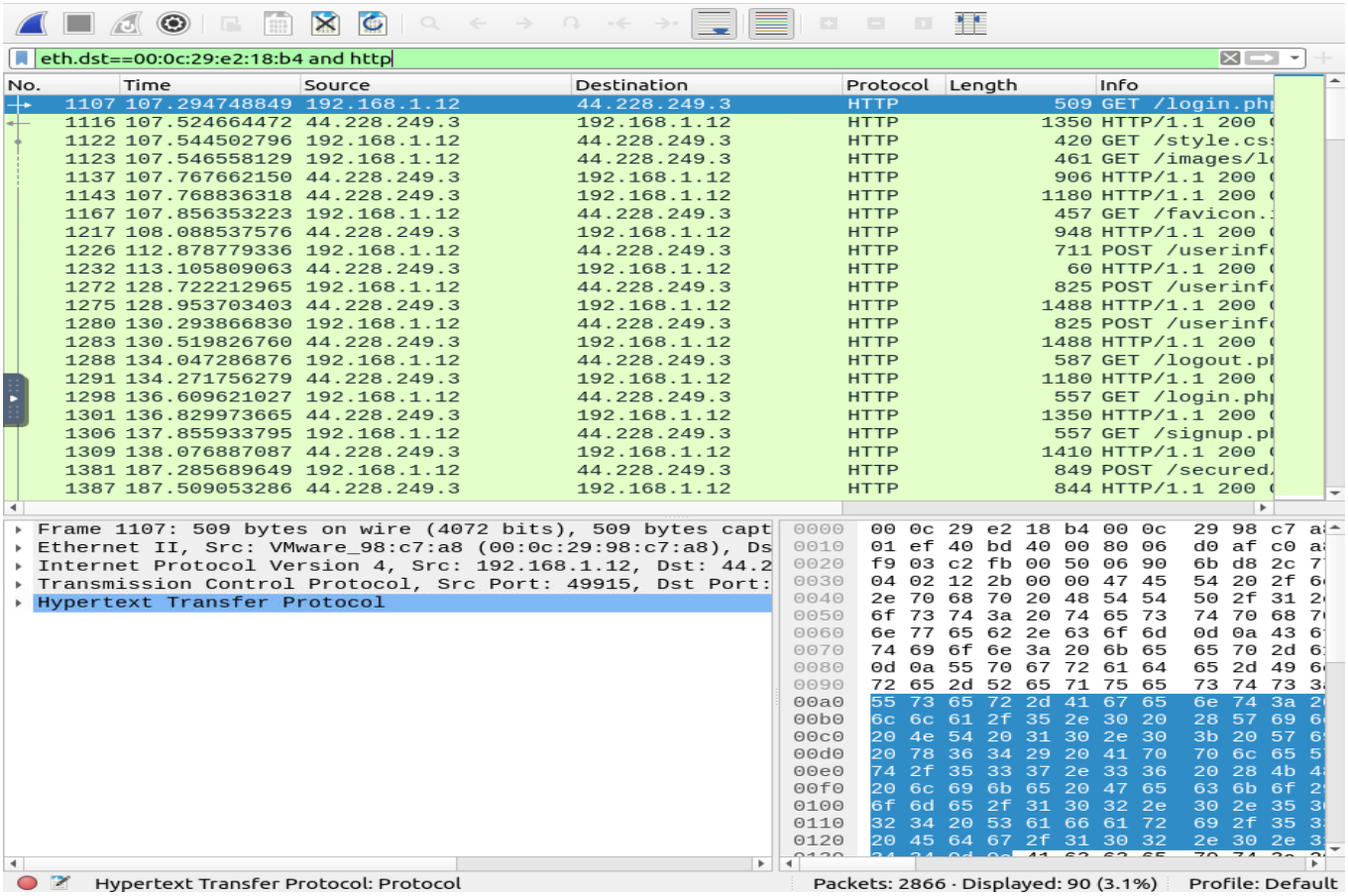
Scenario: The work is divided among your teammates and your teammates found some evidence of a potential attacker. Here is what they found.

Detection Notes	Findings	
IP to MAC matches.	3 IP to MAC address matches.	• MAC: 00:0c:29:e2:18:b4 = IP: 192.168.1.25 • MAC: 50:78:b3:f3:cd:f4 = IP: 192.1681.1 • MAC: 00:0c:29:98:c7:a8 = IP: 192.168.1.12
Attacker	The attacker created noise with ARP packets.	• MAC: 00:0c:29:e2:18:b4 = IP: 192.168.1.25
Router/gateway	Gateway address.	• MAC: 50:78:b3:f3:cd:f4 = IP: 192.1681.1
Victim	The attacker sniffed all traffic of the victim.	• MAC: 50:78:b3:f3:cd:f4 = IP: 192.1681.12

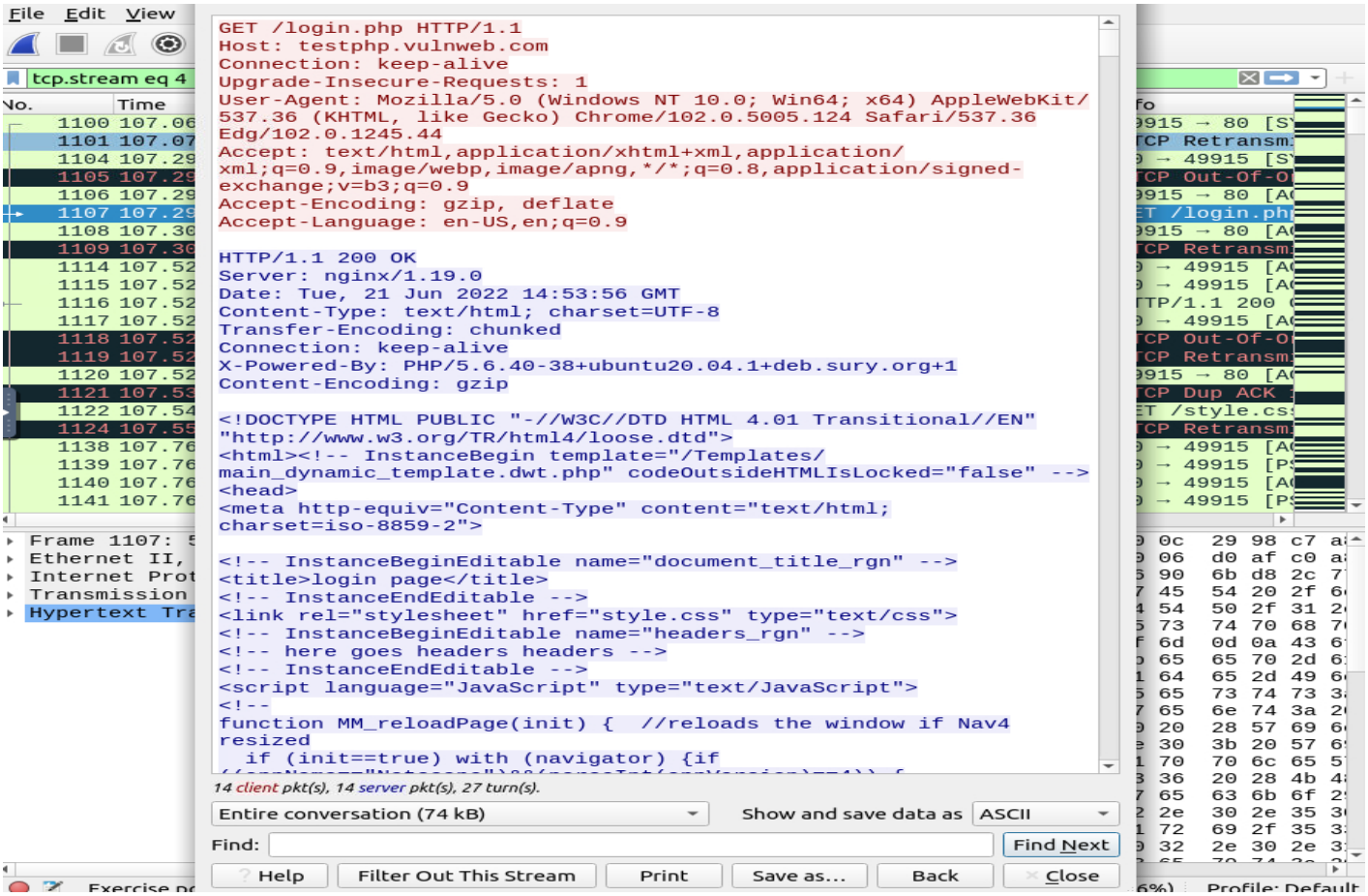
What is the number of ARP requests crafted by the attacker? It's 284 packets.

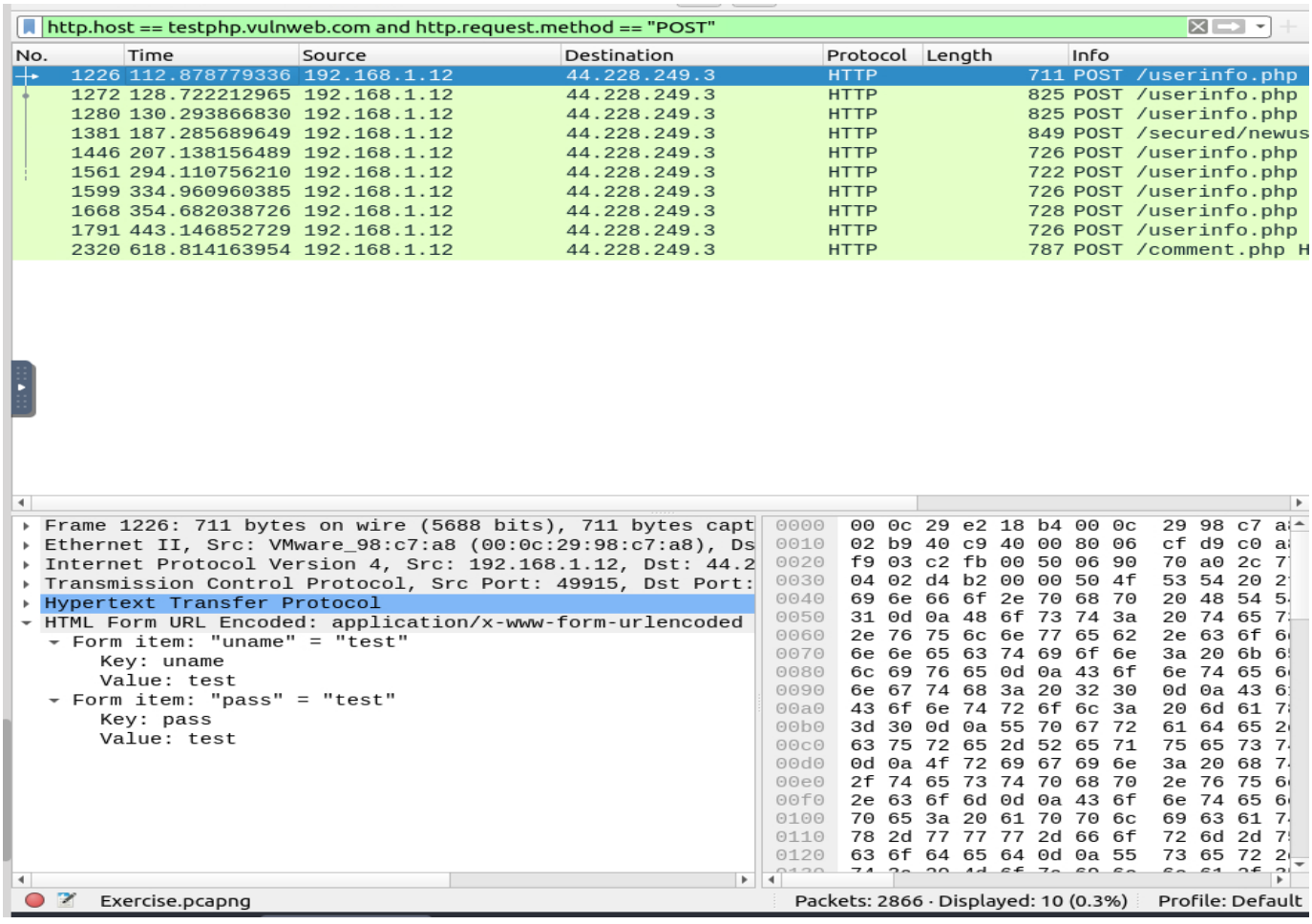

eth.src==00:0c:29:e2:18:b4 and arp.opcode==1
No. Time Source Destination Protocol Length Info
3 17.626854996 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
5 17.637345249 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
6 17.647731835 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
7 17.658130017 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
8 17.668703449 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
9 17.679601294 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
10 17.690243597 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
11 17.700760790 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
12 17.711256788 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
13 17.721858036 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
14 17.732272555 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
15 17.742493934 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
16 17.752775894 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
17 17.763563411 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
18 17.774149379 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
19 17.784781470 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
20 17.795271846 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
21 17.805791112 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
22 17.816308046 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
23 17.826813382 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
24 17.837292051 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
25 17.847816978 VMware_e2:18:b4 Broadcast ARP 42 Who has 192.1
Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (
Ethernet II, Src: VMware_e2:18:b4 (00:0c:29:e2:18:b4), Ds
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 0c 29 e2 18 b4
0010 08 00 06 04 00 01 00 0c 29 e2 18 b4
0020 00 00 00 00 00 00 c0 a8 01 01
Exercise.pcapng
Packets: 2866 · Displayed: 284 (9.9%)
Profile: Default

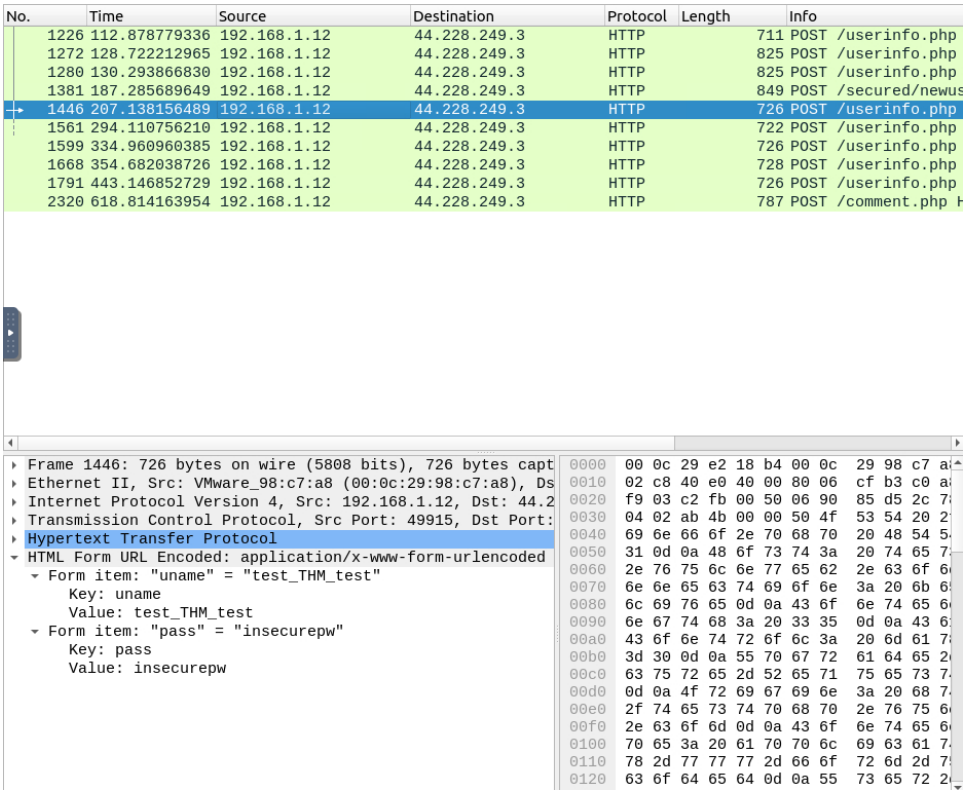
What is the number of HTTP packets received by the attacker? It’s 90 packets



What is the number of sniffed username&password entries? Followed the HTTP stream and found vulnerable web FQDN and the 6 accounts were sniffed.


File Edit View
tcp.stream eq 4
GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.124 Safari/537.36 Edg/102.0.1245.44
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Tue, 21 Jun 2022 14:53:56 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>login page</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
14 client pkt(s), 14 server pkt(s), 27 turn(s).
Entire conversation (74 kB)
Show and save data as ASCII
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close

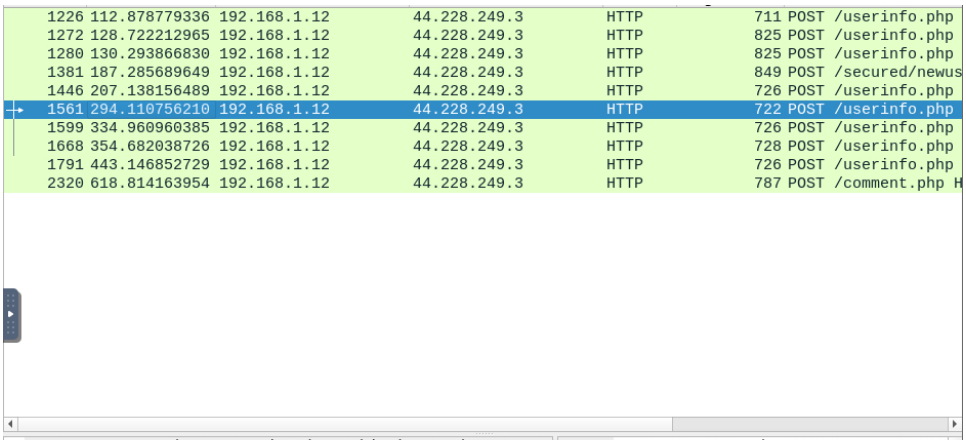

http.host == testphp.vulnweb.com and http.request.method == "POST"
No. Time Source Destination Protocol Length Info
1226 112.878779336 192.168.1.12 44.228.249.3 HTTP 711 POST /userinfo.php
1272 128.722212965 192.168.1.12 44.228.249.3 HTTP 825 POST /userinfo.php
1280 130.293866830 192.168.1.12 44.228.249.3 HTTP 825 POST /userinfo.php
1381 187.285689649 192.168.1.12 44.228.249.3 HTTP 849 POST /secured/newus
1446 207.138156489 192.168.1.12 44.228.249.3 HTTP 726 POST /userinfo.php
1561 294.110756210 192.168.1.12 44.228.249.3 HTTP 722 POST /userinfo.php
1599 334.960960385 192.168.1.12 44.228.249.3 HTTP 726 POST /userinfo.php
1668 354.682038726 192.168.1.12 44.228.249.3 HTTP 728 POST /userinfo.php
1791 443.146852729 192.168.1.12 44.228.249.3 HTTP 726 POST /userinfo.php
2320 618.814163954 192.168.1.12 44.228.249.3 HTTP 787 POST /comment.php H
Frame 1226: 711 bytes on wire (5688 bits), 711 bytes capt
Ethernet II, Src: VMware_98:c7:a8 (00:0c:29:98:c7:a8), Ds
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 44.2
Transmission Control Protocol, Src Port: 49915, Dst Port:
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uname" = "test"
Key: uname
Value: test
Form item: "pass" = "test"
Key: pass
Value: test
0000 00 0c 29 e2 18 b4 00 0c 29 98 c7 a
0010 02 b9 40 c9 40 00 80 06 cf d9 c0 a
0020 f9 03 c2 fb 00 50 06 90 70 a0 2c 7
0030 04 02 d4 b2 00 00 50 4f 53 54 20 2
0040 69 6e 66 6f 2e 70 68 70 20 48 54 5
0050 31 0d 0a 48 6f 73 74 3a 20 74 65 7
0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6
0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 6
0080 6c 69 76 65 0d 0a 43 6f 6e 74 65 6
0090 6e 67 74 68 3a 20 32 30 0d 0a 43 6
00a0 43 6f 6e 74 72 6f 6c 3a 20 6d 61 7
00b0 3d 30 0d 0a 55 70 67 72 61 64 65 2
00c0 63 75 72 65 2d 52 65 71 75 65 73 7
00d0 0d 0a 4f 72 69 67 69 6e 3a 20 68 7
00e0 2f 74 65 73 74 70 68 70 2e 76 75 6
00f0 2e 63 6f 6d 0d 0a 43 6f 6e 74 65 6
0100 70 65 3a 20 61 70 70 6c 69 63 61 7
0110 78 2d 77 77 77 2d 66 6f 72 6d 2d 7
0120 63 6f 64 65 64 0d 0a 55 73 65 72 2
Exercise.pcapng
Packets: 2866 · Displayed: 10 (0.3%)
Profile: Default



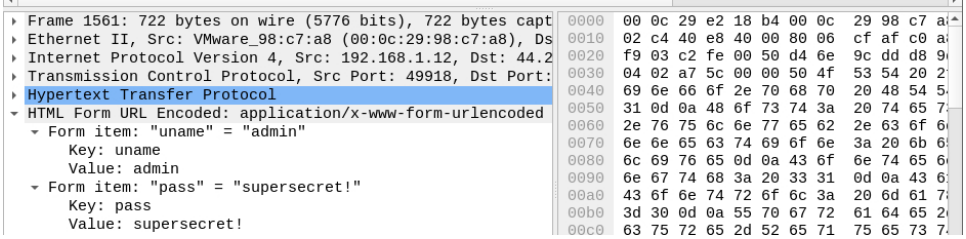
No.	Time	Source	Destination	Protocol	Length	Info
1226	112.878779336	192.168.1.12	44.228.249.3	HTTP	711	POST /userinfo.php
1272	128.722212965	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo.php
1280	130.293866830	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo.php
1381	187.285689649	192.168.1.12	44.228.249.3	HTTP	849	POST /secured/newus
1446	207.138156489	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
1561	294.110756210	192.168.1.12	44.228.249.3	HTTP	722	POST /userinfo.php
1599	334.960960385	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
1668	354.682038726	192.168.1.12	44.228.249.3	HTTP	728	POST /userinfo.php
1791	443.146852729	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
2320	618.814163954	192.168.1.12	44.228.249.3	HTTP	787	POST /comment.php H


```
Frame 1446: 726 bytes on wire (5808 bits), 726 bytes capt
Ethernet II, Src: VMware_98:c7:a8 (00:0c:29:98:c7:a8), Ds
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 44.2
Transmission Control Protocol, Src Port: 49915, Dst Port:
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "uname" = "test_THM_test"
      Key: uname
      Value: test_THM_test
  Form item: "pass" = "insecurepw"
      Key: pass
      Value: insecurepw
```

```
0000  00 0c 29 e2 18 b4 00 0c  29 98 c7 a
0010  02 c8 40 e0 40 00 80 06  cf b3 c0 a
0020  f9 03 c2 fb 00 50 06 90  85 d5 2c 7
0030  04 02 ab 4b 00 00 50 4f  53 54 20 2
0040  69 6e 66 6f 2e 70 68 70  20 48 54 5
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 7
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 6
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6
0090  6e 67 74 68 3a 20 33 35  0d 0a 43 6
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 7
00b0  3d 30 0d 0a 55 70 67 72  61 64 65 2
00c0  63 75 72 65 2d 52 65 71  75 65 73 7
00d0  0d 0a 4f 72 69 67 69 6e  3a 20 68 7
00e0  2f 74 65 73 74 70 68 70  2e 76 75 6
00f0  2e 63 6f 6d 0d 0a 43 6f  6e 74 65 6
0100  70 65 3a 20 61 70 70 6c  69 63 61 7
0110  78 2d 77 77 77 2d 66 6f  72 6d 2d 7
0120  63 6f 64 65 64 0d 0a 55  73 65 72 2
```



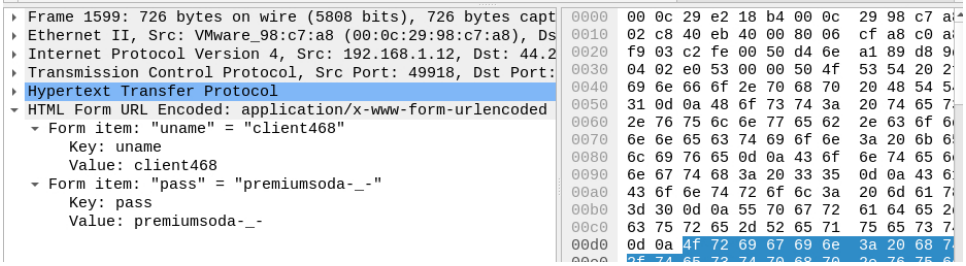
No.	Time	Source	Destination	Protocol	Length	Info
1226	112.878779336	192.168.1.12	44.228.249.3	HTTP	711	POST /userinfo.php
1272	128.722212965	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo.php
1280	130.293866830	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo.php
1381	187.285689649	192.168.1.12	44.228.249.3	HTTP	849	POST /secured/newus
1446	207.138156489	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
1561	294.110756210	192.168.1.12	44.228.249.3	HTTP	722	POST /userinfo.php
1599	334.960960385	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
1668	354.682038726	192.168.1.12	44.228.249.3	HTTP	728	POST /userinfo.php
1791	443.146852729	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
2320	618.814163954	192.168.1.12	44.228.249.3	HTTP	787	POST /comment.php H



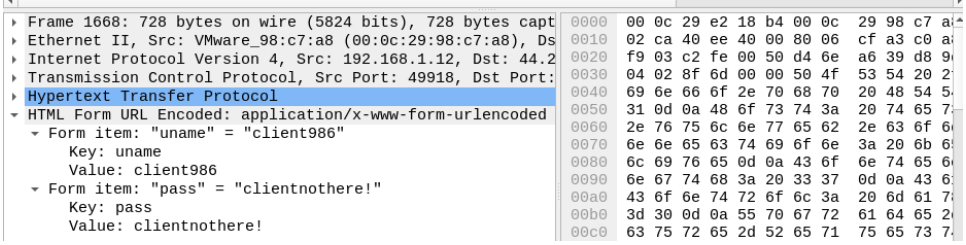
```
Frame 1561: 722 bytes on wire (5776 bits), 722 bytes capt
Ethernet II, Src: VMware_98:c7:a8 (00:0c:29:98:c7:a8), Ds
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 44.2
Transmission Control Protocol, Src Port: 49918, Dst Port:
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "uname" = "admin"
      Key: uname
      Value: admin
  Form item: "pass" = "supersecret!"
      Key: pass
      Value: supersecret!
```

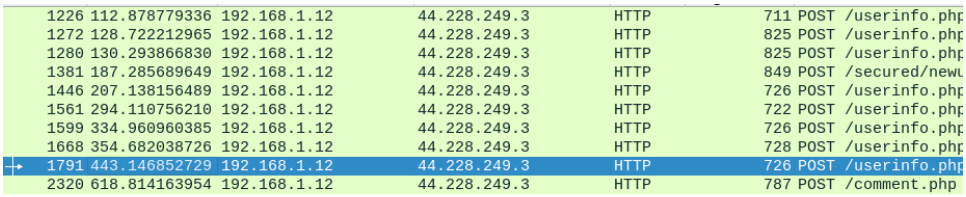
```
0000  00 0c 29 e2 18 b4 00 0c  29 98 c7 a
0010  02 c4 40 e8 40 00 80 06  cf af c0 a
0020  f9 03 c2 fe 00 50 d4 6e  9c dd d8 9
0030  04 02 a7 5c 00 00 50 4f  53 54 20 2
0040  69 6e 66 6f 2e 70 68 70  20 48 54 5
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 7
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 6
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6
0090  6e 67 74 68 3a 20 33 31  0d 0a 43 6
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 7
00b0  3d 30 0d 0a 55 70 67 72  61 64 65 2
00c0  63 75 72 65 2d 52 65 71  75 65 73 7
```

No.	Time	Source	Destination	Protocol	Length	Info
1226	112.878779336	192.168.1.12	44.228.249.3	HTTP	711	POST /userinfo.php
1272	128.722212965	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo.php
1280	130.293866830	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo.php
1381	187.285689649	192.168.1.12	44.228.249.3	HTTP	849	POST /secured/newus
1446	207.138156489	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
1561	294.110756210	192.168.1.12	44.228.249.3	HTTP	722	POST /userinfo.php
1599	334.960960385	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
1668	354.682038726	192.168.1.12	44.228.249.3	HTTP	728	POST /userinfo.php
1791	443.146852729	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
2320	618.814163954	192.168.1.12	44.228.249.3	HTTP	787	POST /comment.php

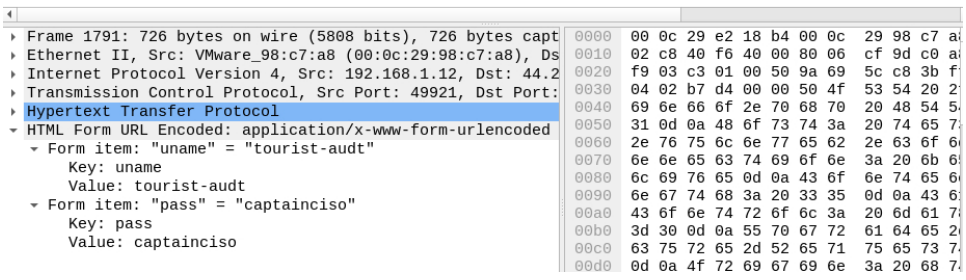


No.	Time	Source	Destination	Protocol	Length	Info
1226	112.878779336	192.168.1.12	44.228.249.3	HTTP	711	POST /userinfo.php
1272	128.722212965	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo.php
1280	130.293866830	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo.php
1381	187.285689649	192.168.1.12	44.228.249.3	HTTP	849	POST /secured/newus
1446	207.138156489	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
1561	294.110756210	192.168.1.12	44.228.249.3	HTTP	722	POST /userinfo.php
1599	334.960960385	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
1668	354.682038726	192.168.1.12	44.228.249.3	HTTP	728	POST /userinfo.php
1791	443.146852729	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
2320	618.814163954	192.168.1.12	44.228.249.3	HTTP	787	POST /comment.php





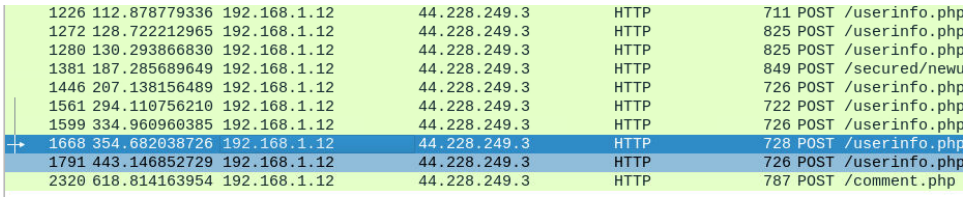
```
1226 112.878779336 192.168.1.12 44.228.249.3 HTTP 711 POST /userinfo.php
1272 128.722212965 192.168.1.12 44.228.249.3 HTTP 825 POST /userinfo.php
1280 130.293866830 192.168.1.12 44.228.249.3 HTTP 825 POST /userinfo.php
1381 187.285689649 192.168.1.12 44.228.249.3 HTTP 849 POST /secured/newu
1446 207.138156489 192.168.1.12 44.228.249.3 HTTP 726 POST /userinfo.php
1561 294.110756210 192.168.1.12 44.228.249.3 HTTP 722 POST /userinfo.php
1599 334.960960385 192.168.1.12 44.228.249.3 HTTP 726 POST /userinfo.php
1668 354.682038726 192.168.1.12 44.228.249.3 HTTP 728 POST /userinfo.php
1791 443.146852729 192.168.1.12 44.228.249.3 HTTP 726 POST /userinfo.php
2320 618.814163954 192.168.1.12 44.228.249.3 HTTP 787 POST /comment.php
```



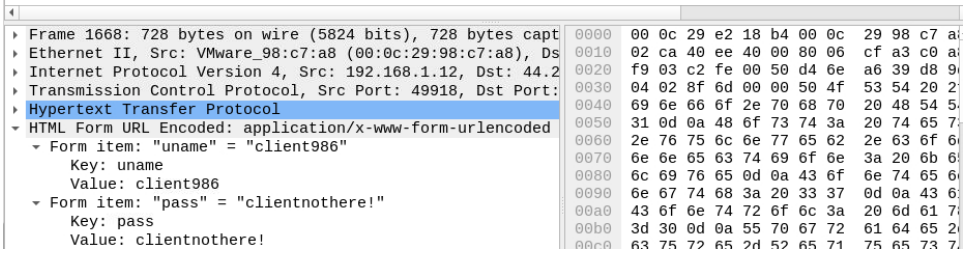
```
Frame 1791: 726 bytes on wire (5808 bits), 726 bytes capt
Ethernet II, Src: VMware_98:c7:a8 (00:0c:29:98:c7:a8), Ds
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 44.2
Transmission Control Protocol, Src Port: 49921, Dst Port:
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "uname" = "tourist-audt"
    Key: uname
    Value: tourist-audt
  Form item: "pass" = "captainciso"
    Key: pass
    Value: captainciso
```

```
0000  00 0c 29 e2 18 b4 00 0c  29 98 c7 a
0010  02 c8 40 f6 40 00 80 06  cf 9d c0 a
0020  f9 03 c3 01 00 50 9a 69  5c c8 3b f
0030  04 02 b7 d4 00 00 50 4f  53 54 20 2
0040  69 6e 66 6f 2e 70 68 70  20 48 54 5
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 7
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 6
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6
0090  6e 67 74 68 3a 20 33 35  0d 0a 43 6
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 7
00b0  3d 30 0d 0a 55 70 67 72  61 64 65 2
00c0  63 75 72 65 2d 52 65 71  75 65 73 7
00d0  0d 0a 4f 72 69 67 69 6e  3a 20 68 7
```

What is the password of the "Client986"? It's clientnothere!



```
1226 112.878779336 192.168.1.12 44.228.249.3 HTTP 711 POST /userinfo.php
1272 128.722212965 192.168.1.12 44.228.249.3 HTTP 825 POST /userinfo.php
1280 130.293866830 192.168.1.12 44.228.249.3 HTTP 825 POST /userinfo.php
1381 187.285689649 192.168.1.12 44.228.249.3 HTTP 849 POST /secured/newu
1446 207.138156489 192.168.1.12 44.228.249.3 HTTP 726 POST /userinfo.php
1561 294.110756210 192.168.1.12 44.228.249.3 HTTP 722 POST /userinfo.php
1599 334.960960385 192.168.1.12 44.228.249.3 HTTP 726 POST /userinfo.php
1668 354.682038726 192.168.1.12 44.228.249.3 HTTP 728 POST /userinfo.php
1791 443.146852729 192.168.1.12 44.228.249.3 HTTP 726 POST /userinfo.php
2320 618.814163954 192.168.1.12 44.228.249.3 HTTP 787 POST /comment.php
```



```
Frame 1668: 728 bytes on wire (5824 bits), 728 bytes capt
Ethernet II, Src: VMware_98:c7:a8 (00:0c:29:98:c7:a8), Ds
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 44.2
Transmission Control Protocol, Src Port: 49918, Dst Port:
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "uname" = "client986"
    Key: uname
    Value: client986
  Form item: "pass" = "clientnothere!"
    Key: pass
    Value: clientnothere!
```

```
0000  00 0c 29 e2 18 b4 00 0c  29 98 c7 a
0010  02 ca 40 ee 40 00 80 06  cf a3 c0 a
0020  f9 03 c2 fe 00 50 d4 6e  a6 39 d8 9
0030  04 02 8f 6d 00 00 50 4f  53 54 20 2
0040  69 6e 66 6f 2e 70 68 70  20 48 54 5
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 7
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 6
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6
0090  6e 67 74 68 3a 20 33 37  0d 0a 43 6
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 7
00b0  3d 30 0d 0a 55 70 67 72  61 64 65 2
00c0  63 75 72 65 2d 52 65 71  75 65 73 7
```

What is the comment provided by the "Client354"? The message is nice work!

1226	112.878779336	192.168.1.12	44.228.249.3	HTTP	711	POST /userinfo.php
1272	128.722212965	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo.php
1280	130.293866830	192.168.1.12	44.228.249.3	HTTP	825	POST /userinfo.php
1381	187.285689649	192.168.1.12	44.228.249.3	HTTP	849	POST /secured/newu
1446	207.138156489	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
1561	294.110756210	192.168.1.12	44.228.249.3	HTTP	722	POST /userinfo.php
1599	334.960960385	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
1668	354.682038726	192.168.1.12	44.228.249.3	HTTP	728	POST /userinfo.php
1791	443.146852729	192.168.1.12	44.228.249.3	HTTP	726	POST /userinfo.php
2320	618.814163954	192.168.1.12	44.228.249.3	HTTP	787	POST /comment.php