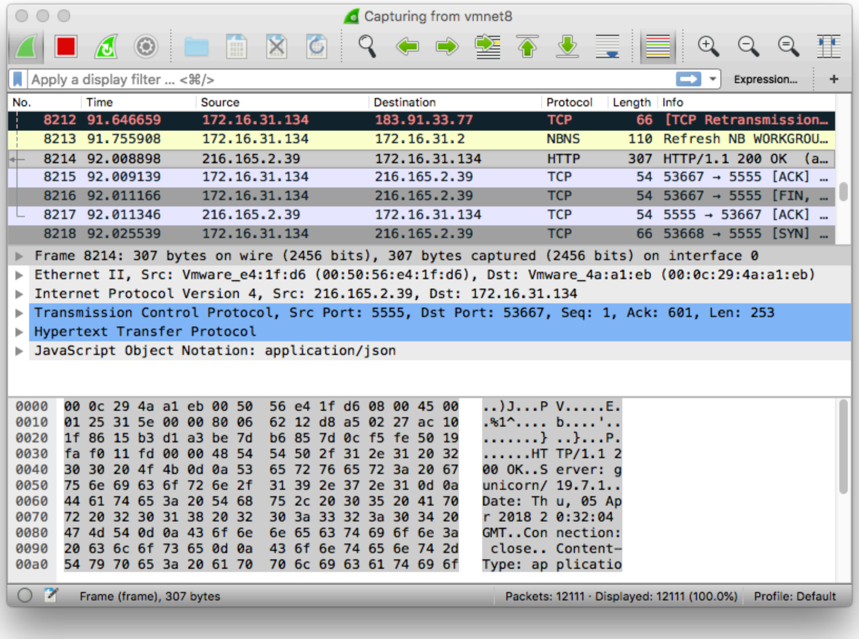
Man-in-the-middle attack

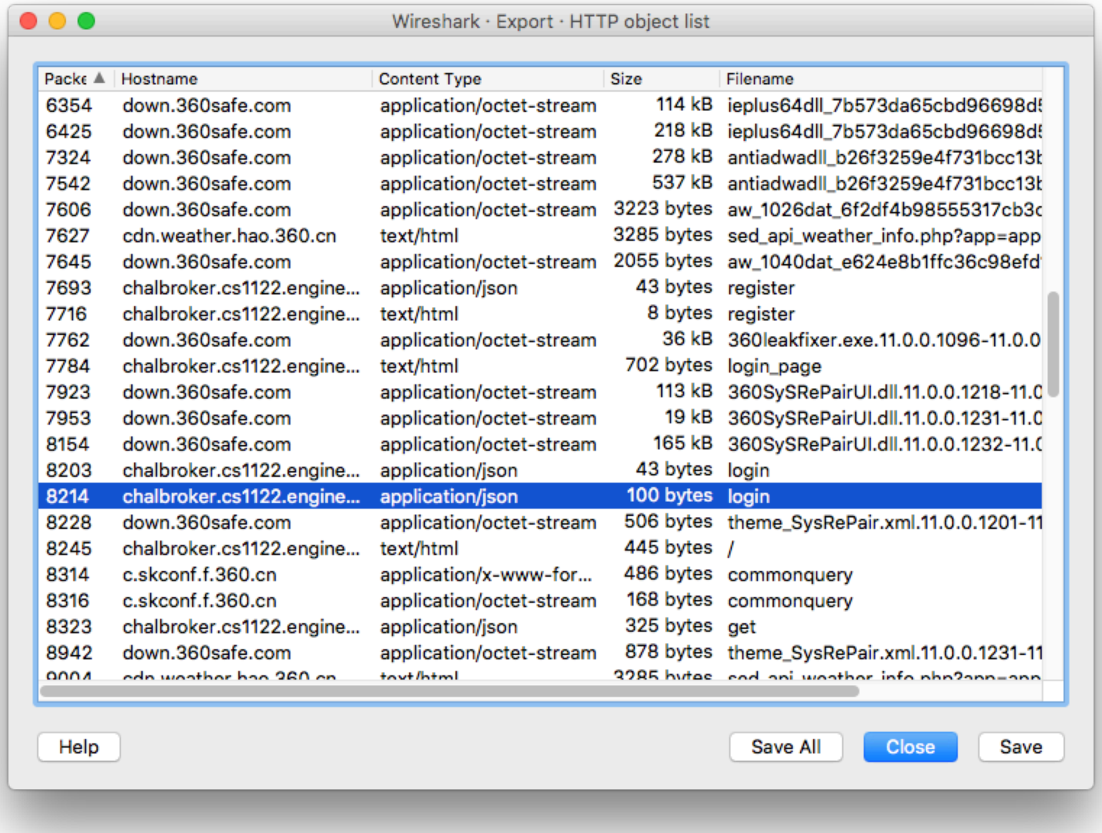
This operation exploits the fact that the website's connection is not encrypted. This way, sensitive data such as username and password is transmitted as plain text. An intruder who can access the same network as the targeted computer is on can intercept the package and steal the data.

1. Open the website on one computer. In my case I ran a virtual machine on VMware.
2. Open Wireshark on another computer. In my case it's the macOS on which the virtual machine is running. Choose the network the targeted computer is on. In my case it's the bridging network between the virtual machine and the host OS. Now Wireshark starts capturing packets on the network.



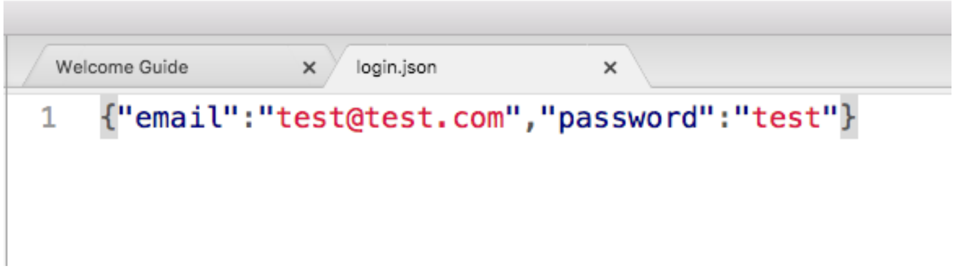
```
No.      Time       Source          Destination     Protocol Length Info
   8212 91.646659  172.16.31.134   183.91.33.77    TCP        66 [TCP Retransmission…
   8213 91.755908  172.16.31.134   172.16.31.2     NBNS      110 Refresh NB WORKGROU…
   8214 92.008898  216.165.2.39    172.16.31.134   HTTP      307 HTTP/1.1 200 OK  (a…
   8215 92.009139  172.16.31.134   216.165.2.39    TCP        54 53667 → 5555 [ACK] …
   8216 92.011166  172.16.31.134   216.165.2.39    TCP        54 53667 → 5555 [FIN, …
   8217 92.011346  216.165.2.39    172.16.31.134   TCP        54 5555 → 53667 [ACK] …
   8218 92.025539  172.16.31.134   216.165.2.39    TCP        66 53668 → 5555 [SYN] …

▶ Frame 8214: 307 bytes on wire (2456 bits), 307 bytes captured (2456 bits) on interface 0
▶ Ethernet II, Src: Vmware_e4:1f:d6 (00:50:56:e4:1f:d6), Dst: Vmware_4a:a1:eb (00:0c:29:4a:a1:eb)
▶ Internet Protocol Version 4, Src: 216.165.2.39, Dst: 172.16.31.134
▶ Transmission Control Protocol, Src Port: 5555, Dst Port: 53667, Seq: 1, Ack: 601, Len: 253
▶ Hypertext Transfer Protocol
▶ JavaScript Object Notation: application/json

0000  00 0c 29 4a a1 eb 00 50  56 e4 1f d6 08 00 45 00   ..)J...P V.....E.
0010  01 25 31 5e 00 00 80 06  62 12 d8 a5 02 27 ac 10   .%1^.... b....'..
0020  1f 86 15 b3 d1 a3 be 7d  b6 85 7d 0c f5 fe 50 19   .......} ..}...P.
0030  fa f0 11 fd 00 00 48 54  54 50 2f 31 2e 31 20 32   ......HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 67   00 OK..S erver: g
0050  75 6e 69 63 6f 72 6e 2f  31 39 2e 37 2e 31 0d 0a   unicorn/ 19.7.1..
0060  44 61 74 65 3a 20 54 68  75 2c 20 30 35 20 41 70   Date: Th u, 05 Ap
0070  72 20 32 30 31 38 20 32  30 3a 33 32 3a 30 34 20   r 2018 2 0:32:04
0080  47 4d 54 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   GMT..Con nection:
0090  20 63 6c 6f 73 65 0d 0a  43 6f 6e 74 65 6e 74 2d    close.. Content-
00a0  54 79 70 65 3a 20 61 70  70 6c 69 63 61 74 69 6f   Type: ap plicatio

Frame (frame), 307 bytes          Packets: 12111 · Displayed: 12111 (100.0%)    Profile: Default
```

3. Register on the website. In my case I entered the username "test@test.com" and the password "test".
4. On Wireshark, click "Export Objects". Now you can see all the objects that can be extracted from the packets.
5. Go to the log-in page of the website. Type in the registered username and password. While logging in, the computer transmits the file "login.json" to the website, which Wireshark captures in a packet. It's shown as an exportable object on the list.



Packe ▲	Hostname	Content Type	Size	Filename
6354	down.360safe.com	application/octet-stream	114 kB	ieplus64dll_7b573da65cbd96698d
6425	down.360safe.com	application/octet-stream	218 kB	ieplus64dll_7b573da65cbd96698d
7324	down.360safe.com	application/octet-stream	278 kB	antiadwadll_b26f3259e4f731bcc13
7542	down.360safe.com	application/octet-stream	537 kB	antiadwadll_b26f3259e4f731bcc13
7606	down.360safe.com	application/octet-stream	3223 bytes	aw_1026dat_6f2df4b98555317cb3
7627	cdn.weather.hao.360.cn	text/html	3285 bytes	sed_api_weather_info.php?app=app
7645	down.360safe.com	application/octet-stream	2055 bytes	aw_1040dat_e624e8b1ffc36c98efd
7693	chalbroker.cs1122.engine...	application/json	43 bytes	register
7716	chalbroker.cs1122.engine...	text/html	8 bytes	register
7762	down.360safe.com	application/octet-stream	36 kB	360leakfixer.exe.11.0.0.1096-11.0.0
7784	chalbroker.cs1122.engine...	text/html	702 bytes	login_page
7923	down.360safe.com	application/octet-stream	113 kB	360SySRePairUI.dll.11.0.0.1218-11.0
7953	down.360safe.com	application/octet-stream	19 kB	360SySRePairUI.dll.11.0.0.1231-11.0
8154	down.360safe.com	application/octet-stream	165 kB	360SySRePairUI.dll.11.0.0.1232-11.0
8203	chalbroker.cs1122.engine...	application/json	43 bytes	login
8214	chalbroker.cs1122.engine...	application/json	100 bytes	login
8228	down.360safe.com	application/octet-stream	506 bytes	theme_SysRePair.xml.11.0.0.1201-11
8245	chalbroker.cs1122.engine...	text/html	445 bytes	/
8314	c.skconf.f.360.cn	application/x-www-for...	486 bytes	commonquery
8316	c.skconf.f.360.cn	application/octet-stream	168 bytes	commonquery
8323	chalbroker.cs1122.engine...	application/json	325 bytes	get
8942	down.360safe.com	application/octet-stream	878 bytes	theme_SysRePair.xml.11.0.0.1231-11
9004	cdn.weather.hao.360.cn	text/html	3285 bytes	sed_api_weather_info.php?app=app

6. Save the highlighted file as “login.json”. Open the file in a code editor, and you can see the username and password.



```
{"email":"test@test.com","password":"test"}
```