Wireshark – Image Extraction

Host IP: 192.168.159.129

The given capture file is opened.

Upon analysis, they are several HTTP Get requests from the host.

The capture is filtered for HTTP for easier inspection.

7	0.010413	192.168.159.129	10.10.20.129	HTTP	516 GET / HTTP/1.1
11	0.012962	10.10.20.129	192.168.159.129	HTTP	545 HTTP/1.0 200 OK (text/html)
40	1.110099	192.168.159.129	10.10.20.129	HTTP	516 GET / HTTP/1.1
43	1.111673	10.10.20.129	192.168.159.129	HTTP	545 HTTP/1.0 200 OK (text/html)
83	3.078789	192.168.159.129	10.10.20.129	HTTP	516 GET / HTTP/1.1
86	3.082240	10.10.20.129	192.168.159.129	HTTP	545 HTTP/1.0 200 OK (text/html)
155	10.711362	192.168.159.129	10.10.20.129	HTTP	376 GET /http_with_jpegs.cap HTTP/1.1
464	10.730608	10.10.20.129	192.168.159.129	HTTP	424 HTTP/1.0 200 OK (application/vnd.tcpdump.pcap)
526	18.849965	192.168.159.129	10.10.20.129	HTTP	365 GET /htb.jpeg HTTP/1.1
531	18.851428	10.10.20.129	192.168.159.129	HTTP	726 HTTP/1.0 200 OK (JPEG JFIF image)
577	24.128988	192.168.159.129	10.10.20.129	HTTP	368 GET /Rise-Up.jpg HTTP/1.1
657	24.137398	10.10.20.129	192.168.159.129	HTTP	1153 HTTP/1.0 200 OK (JPEG JFIF image)
721	31.653720	192.168.159.129	10.10.20.129	HTTP	366 GET /water.jpg HTTP/1.1

Each Get request is followed by a 200 OK packet from a server.

These requests include ones for 3 image files of type JPEG.

When following the TCP Stream of these responses, it is confirmed that the images were successfully sent to the host.

```
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.9.1+
Date: Thu, 22 Apr 2021 17:10:07 GMT
Content-type: image/jpeg
Content-Length: 3592
Last-Modified: Thu, 22 Apr 2021 15:52:54 GMT
```

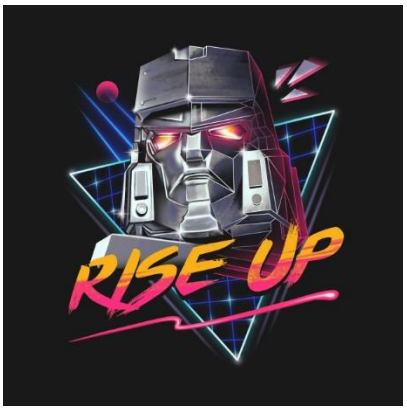
Using the Export Objects option in Wireshark and selecting HTTP, the images sent from the server can be pulled from the captured packets and saved locally.

Packet	Hostname	Content Type	Size	Filename
531	10.10.20.129	image/jpeg	3592 bytes	htb.jpeg
657	10.10.20.129	image/jpeg	89 kB	Rise-Up.jpg
997	10.10.20.129	image/jpeg	301 kB	water.jpg

Below are the extracted images:

htb.jpeg

Rise-Up.jpg



water.jpg