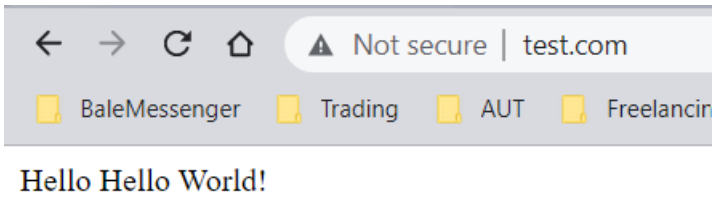
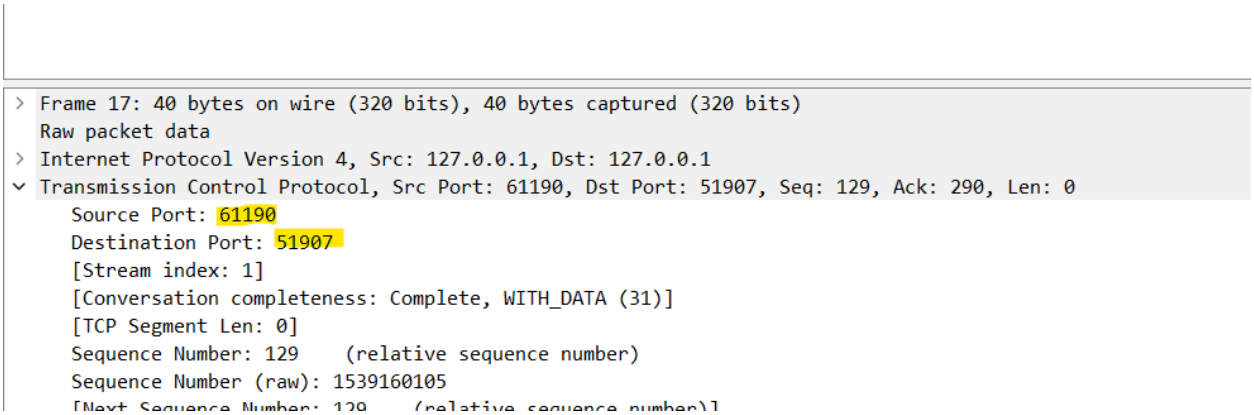
گزارش کار سوم – Web & FTP

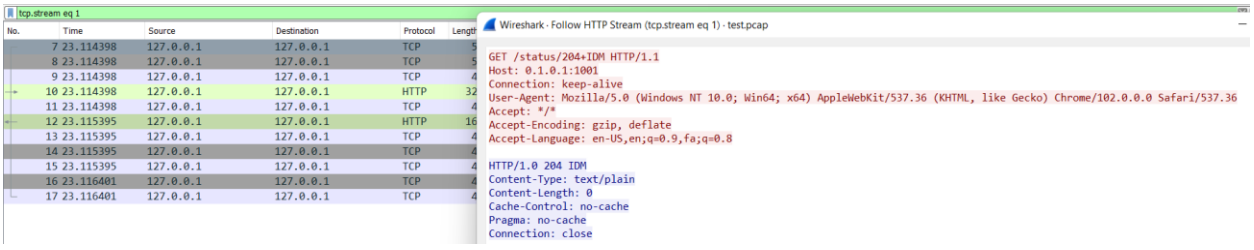
سوال اول) زیرا ما صرفا Host را تعریف کردیم اما آنرا به IP Address متصل نکردیم. پس زمانی که آدرس سایت را در مرور گر وارد کنیم Host را شناخته اما نمیداند آن را به کدام IP وصل کند. از طرفی بعد از حل این مشکل همچنان می تواند مشکل از DNS Cache هم باشد که با Hard Refresh و پاک کردن آن درست می شود.

سوال دوم) بعد از انجام عملیات های گفته شده سایت در مرور گر باز می شود، اما نمی توان با Wireshark ارتباط را شنود کرد زیرا این نرم افزار ترافیک localhost را شنود نمیکند (به آن اصطلاحا 127.0.0.1 یا Loopback هم گفته می شود)



سوال سوم) پورت مبدا برابر ۶۱۱۹۰ و پرت مقصد برابر ۵۱۹۰۷ است (مطابق عکس زیر). با وارد کردن آدرس www.test.com مطابق شکل سوال قبل آدرس به DNS محلی در دستگاه رفته و دنبال IP Address متناظر با این Host میگردد. پس از یافتن آن محتویات index.html را نمایش می دهد.





سوال چهارم) مقدار Connection از نوع Keep-Alive است که بیانگر Persistent بودن ارتباط است. نوع درخواستی GET بوده زیرا در load کردن محتویات سایت همیشه پروتکل GET استفاده می شود. مقدار User-Agent همانند شکل بالا

برابر Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36 است که اشاره به مرور گر و مشخصات سیستم عامل و جزئیات دیگر دارد.

سوال پنجم) مقادیر Flag اولین بسته مطابق شکل زیر است:

```
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
   000. .... .... = Reserved: Not set
   ...0 .... .... = Nonce: Not set
   .... 0... .... = Congestion Window Reduced (CWR): Not set
   .... .0.. .... = ECN-Echo: Not set
   .... ..0. .... = Urgent: Not set
   .... ...0 .... = Acknowledgment: Not set
   .... .... 0... = Push: Not set
   .... .... .0.. = Reset: Not set
   .... .... ..1. = Syn: Set
   .... .... ...0 = Fin: Not set
   [TCP Flags: ·····S·]
Window: 65535
```

سوال ششم) سایت دیگری با نام test2 و Host www.test2.com ساخته و تست شد. تمام مراحل گفته شده برای سایت اول ساخته شده برای دومی نیز تکرار میشوند، اما برخی متغیر ها مانند پورت های مبدا و مقصد متفاوت است. برای مثال پورت های جدید برابر:

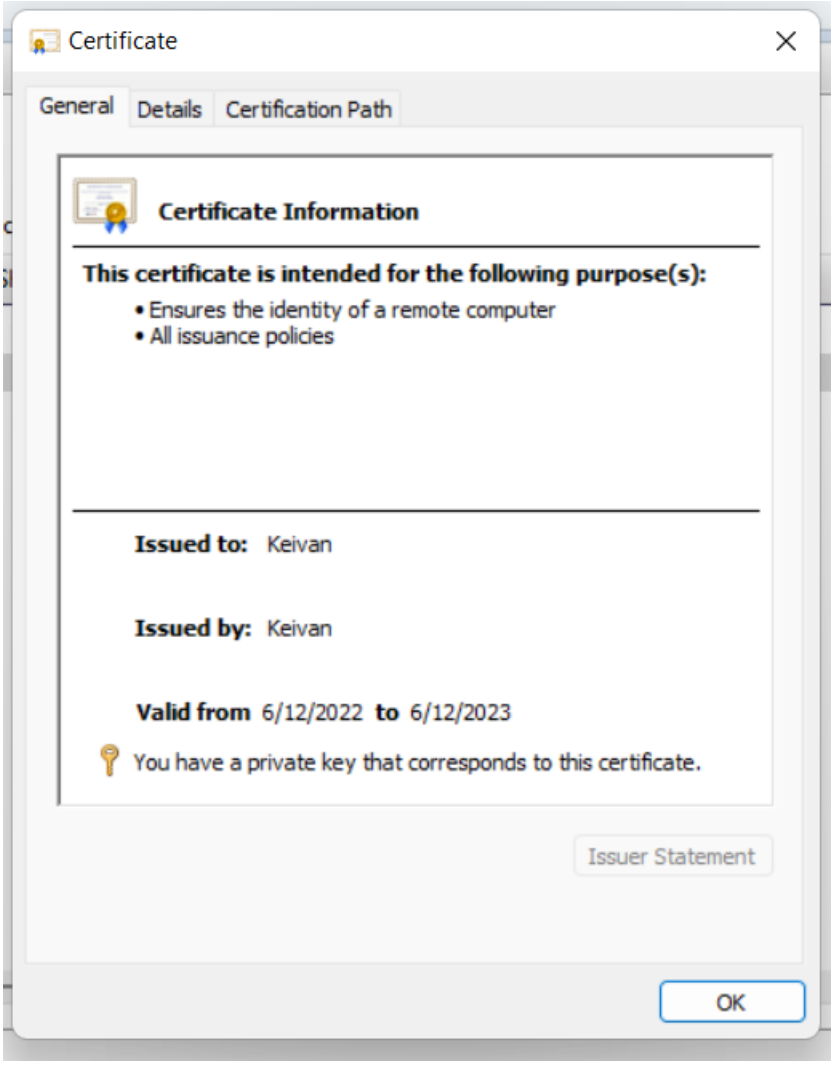
```
Frame 57: 328 bytes on wire (2624 bits), 328 bytes captured (2624 bits)
Raw packet data
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 52190, Dst Port: 61190, Seq: 1, Ack: 1, Len: 288
   Source Port: 52190
   Destination Port: 61190
   [Stream index: 6]
   [Conversation completeness: Complete, WITH_DATA (31)]
```

سوال هفتم) زیرا با استفاده از این IP Address نمی توان به سایت مورد نظر رسید. این به آن دلیل است که هر دو سایت www.test.com و www.test2.com که ساختیم به این IP وصل شده اند. پس سوالی که پیش می آید آن است که زمانی که این IP را وارد کنیم کدام سایت باید load شوند؟ پس در نتیجه چیزی load نخواهد شد.

سوال هشتم) مشکلی که با آن میخوریم HTTP بودن این Certificate است که مشکل ساز است، زیرا باید HTTPS باشد. پس می توان دو کار کرد: ۱) آن را در white list قرار داد یا به عبارتی exception گذاشت و یا نوع HTTPS را برای گواهی آن انتخاب کرد.

از طرفی باید موقع وارد کردن سایت در مرور گر پورت آنرا مشخص کنیم. پورت انتخاب من ۱۲۳۴ بود پس در مرور گر http://www.test.com:1234/ وارد کردم.

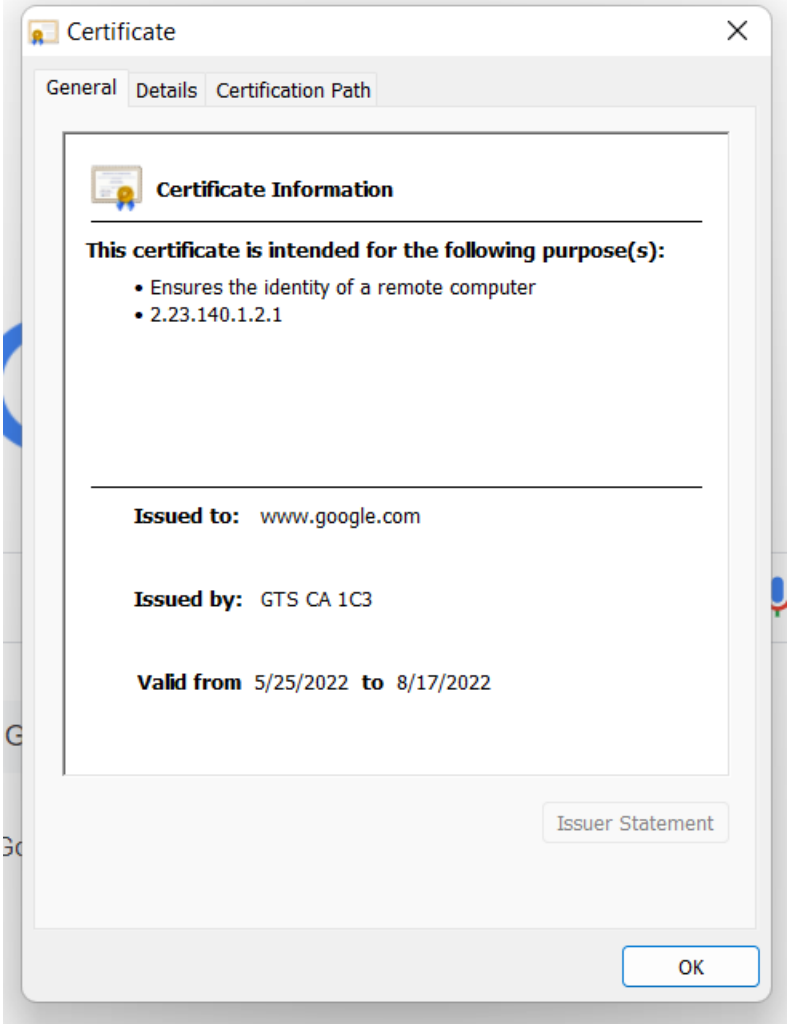
سوال نهم) مطابق عکس زیر:



این گواهی توسط این بنده حقیر ساخته شده و به خودم تخصیص داده شده است. از طرفی از الگوریتم SHA256RSA برای ساختن Private Key آن استفاده شده است.

سوال دهم) خیر نمیتوان زیرا HTTPS است و محتویات رمزنگاری شده است :(

سوال یازدهم) مطابق عکس:



توسط GTS CA 1C3 ساخته شده و به www.google.com تخصیص شده است.

نکته خیلی مهم: متاسفانه chrome و Microsoft edge دیگر اجازه اتصال به سرور FTP را نمیدهند و هر دو مرور گر این قابلیت را به دلایلی به کلی حذف کرده اند! امکان اتصال به FTP از این طریق برای منم ممکن نبود.

لینک های اطلاع رسانی هر دو مرور گر بدین شرح است:

https://answers.microsoft.com/en-us/windows/forum/all/open-ftp-site-in-microsot-edge/a6c3dbdc-d48d-4664-acc6-01161e43622d

https://superuser.com/questions/1634495/how-can-i-open-an-ftp-server-in-chrome#answer-1689941

پاسخ سوالات بر اساس دانش و جست و جو اینترنتی داده شده اند.

سوال دوازدهم) در لایه انتقال از پروتکل TCP استفاده شده است. برای لیست کردن فایل های دایرکتوری از دستور LIST استفاده میشود. متاسفانه پورت ها قابل مشاهده نیستند (دلیل بالاتر ذکر شد)

سوال سیزدهم) خیر در پروتکل FTP username و password رمز گزاری شده اند.

سوال چهاردهم) در بخش FTP Authentication از نوع Basic بوده و FTP Authorization برای تمامی کاربران از نوع READ بوده است.

سوال پانزدهم) خیر این عمل ممکن نیست زیرا به SSL Credentials نیاز داریم.

سوال شانزدهم) ارور نمایش داده شده حاکی از نداشتن SSL Credentials است زیرا از SSL Policy استفاده میکنیم به آن گواهی نیز نیاز داریم.

سوالات بخش پروتکل HTTP

دستور همانطور که بالاتر توضیح داده شد از نوع GET است و در User-Agent برابر Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36 است که حاوی جزییاتی از سیستم عامل و مرورگر استفاده شده برای دسترسی به سایت بوده است.