Billy Ouattara (920603707)
Jose Gavidia (921477055)
part3.py, part3_gpt.py

Part I:

1. When analyzing the communication happening between our device and the destination IP corresponding to the request made in the python file. We notice that we do not have access to either the request or response content. Therefore, we can't tell what the secret key is.
2. We can't tell the secret key because we are performing an HTTPS request which is done through the use of TLS encryption protocols. In encryption protocols, the requests and responses are encrypted before sending them to server or client.

Part II:

1. We are able to tell the secret key. On the mitmproxy interface we clicked on the get request to the corresponding url which displayed the information about the request and response. When clicking on response, we were able to analyze the header and reveal the secret.
2. The secret key is: Ecs152a-Resp: 253936030
3. mitmoroxy acts as a middle point between the client host and the server. The client host sends the request to the MITM proxy while sharing trusted keys. The Proxy then forwards that request as a new request to the server. Since the client shares its trusted keys with the proxy, the proxy is able to encrypt and decrypt requests and responses. Hence, allowing us to analyze the header and extract the secret key.

ChatGPT link: https://chat.openai.com/share/15369bc7-3374-474a-aa4f-604139e5f785