Elson Jian (918147110)
Jacob Dominick (917503904)

Submitted files:
proj3.py
proj3_gpt.py

ChatGPT Link

Code:

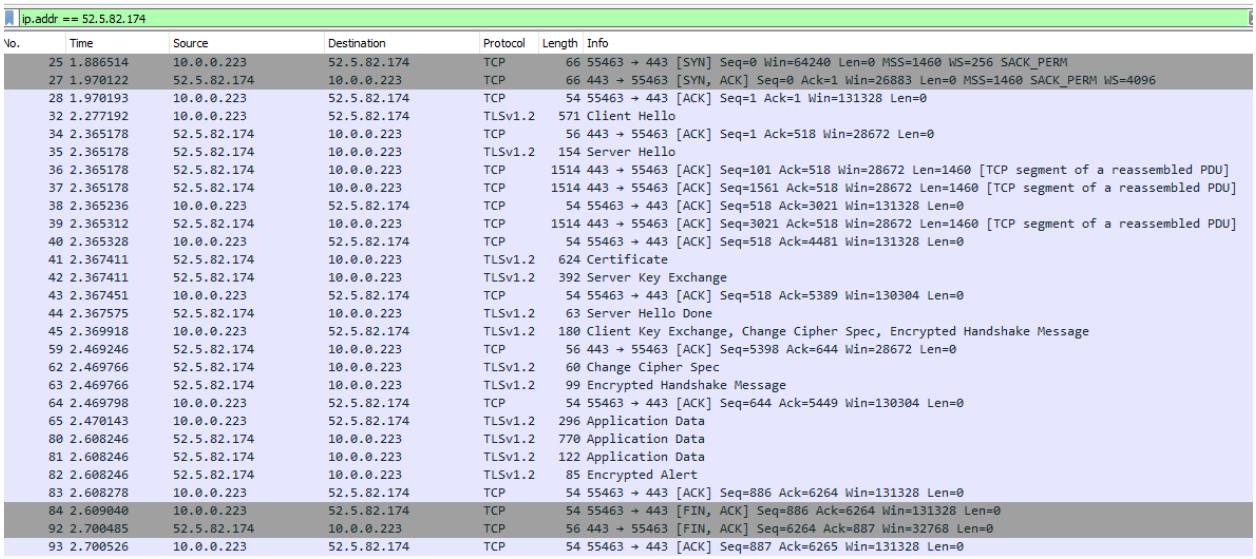
```
import requests

sid = '917503904'
headers = {
    'Student-Id': sid,
}

r =
requests.get('https://kartik-labeling-cvpr-0ed3099180c2.herokuapp.com/ecs1
52a_ass1', headers=headers)
print("Status Code:", r.status_code)
print(r.headers)
```

Output:
Status Code: 200
{'Connection': 'close', 'Server': 'BaseHTTP/0.6 Python/3.11.6', 'Date': 'Fri, 03 Nov 2023 03:51:47 GMT', 'Content-Type': 'text/plain', 'Ecs152a-Resp': '240836237', 'Via': '1.1 vegur'}

Wireshark (no proxy):



ip.addr == 52.5.82.174

No.	Time	Source	Destination	Protocol	Length	Info
25	1.886514	10.0.0.223	52.5.82.174	TCP	66	55463 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
27	1.970122	52.5.82.174	10.0.0.223	TCP	66	443 → 55463 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM WS=4096
28	1.970193	10.0.0.223	52.5.82.174	TCP	54	55463 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
32	2.277192	10.0.0.223	52.5.82.174	TLSv1.2	571	Client Hello
34	2.365178	52.5.82.174	10.0.0.223	TCP	56	443 → 55463 [ACK] Seq=1 Ack=518 Win=28672 Len=0
35	2.365178	52.5.82.174	10.0.0.223	TLSv1.2	154	Server Hello
36	2.365178	52.5.82.174	10.0.0.223	TCP	1514	443 → 55463 [ACK] Seq=101 Ack=518 Win=28672 Len=1460 [TCP segment of a reassembled PDU]
37	2.365178	52.5.82.174	10.0.0.223	TCP	1514	443 → 55463 [ACK] Seq=1561 Ack=518 Win=28672 Len=1460 [TCP segment of a reassembled PDU]
38	2.365236	10.0.0.223	52.5.82.174	TCP	54	55463 → 443 [ACK] Seq=518 Ack=3021 Win=131328 Len=0
39	2.365312	52.5.82.174	10.0.0.223	TCP	1514	443 → 55463 [ACK] Seq=3021 Ack=518 Win=28672 Len=1460 [TCP segment of a reassembled PDU]
40	2.365328	10.0.0.223	52.5.82.174	TCP	54	55463 → 443 [ACK] Seq=518 Ack=4481 Win=131328 Len=0
41	2.367411	52.5.82.174	10.0.0.223	TLSv1.2	624	Certificate
42	2.367411	52.5.82.174	10.0.0.223	TLSv1.2	392	Server Key Exchange
43	2.367451	10.0.0.223	52.5.82.174	TCP	54	55463 → 443 [ACK] Seq=518 Ack=5389 Win=130304 Len=0
44	2.367575	52.5.82.174	10.0.0.223	TLSv1.2	63	Server Hello Done
45	2.369918	10.0.0.223	52.5.82.174	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
59	2.469246	52.5.82.174	10.0.0.223	TCP	56	443 → 55463 [ACK] Seq=5398 Ack=644 Win=28672 Len=0
62	2.469766	52.5.82.174	10.0.0.223	TLSv1.2	60	Change Cipher Spec
63	2.469766	52.5.82.174	10.0.0.223	TLSv1.2	99	Encrypted Handshake Message
64	2.469798	10.0.0.223	52.5.82.174	TCP	54	55463 → 443 [ACK] Seq=644 Ack=5449 Win=130304 Len=0
65	2.470143	10.0.0.223	52.5.82.174	TLSv1.2	296	Application Data
80	2.608246	52.5.82.174	10.0.0.223	TLSv1.2	770	Application Data
81	2.608246	52.5.82.174	10.0.0.223	TLSv1.2	122	Application Data
82	2.608246	52.5.82.174	10.0.0.223	TLSv1.2	85	Encrypted Alert
83	2.608278	10.0.0.223	52.5.82.174	TCP	54	55463 → 443 [ACK] Seq=886 Ack=6264 Win=131328 Len=0
84	2.609040	10.0.0.223	52.5.82.174	TCP	54	55463 → 443 [FIN, ACK] Seq=886 Ack=6264 Win=131328 Len=0
92	2.700485	52.5.82.174	10.0.0.223	TCP	56	443 → 55463 [FIN, ACK] Seq=6264 Ack=887 Win=32768 Len=0
93	2.700526	10.0.0.223	52.5.82.174	TCP	54	55463 → 443 [ACK] Seq=887 Ack=6265 Win=131328 Len=0

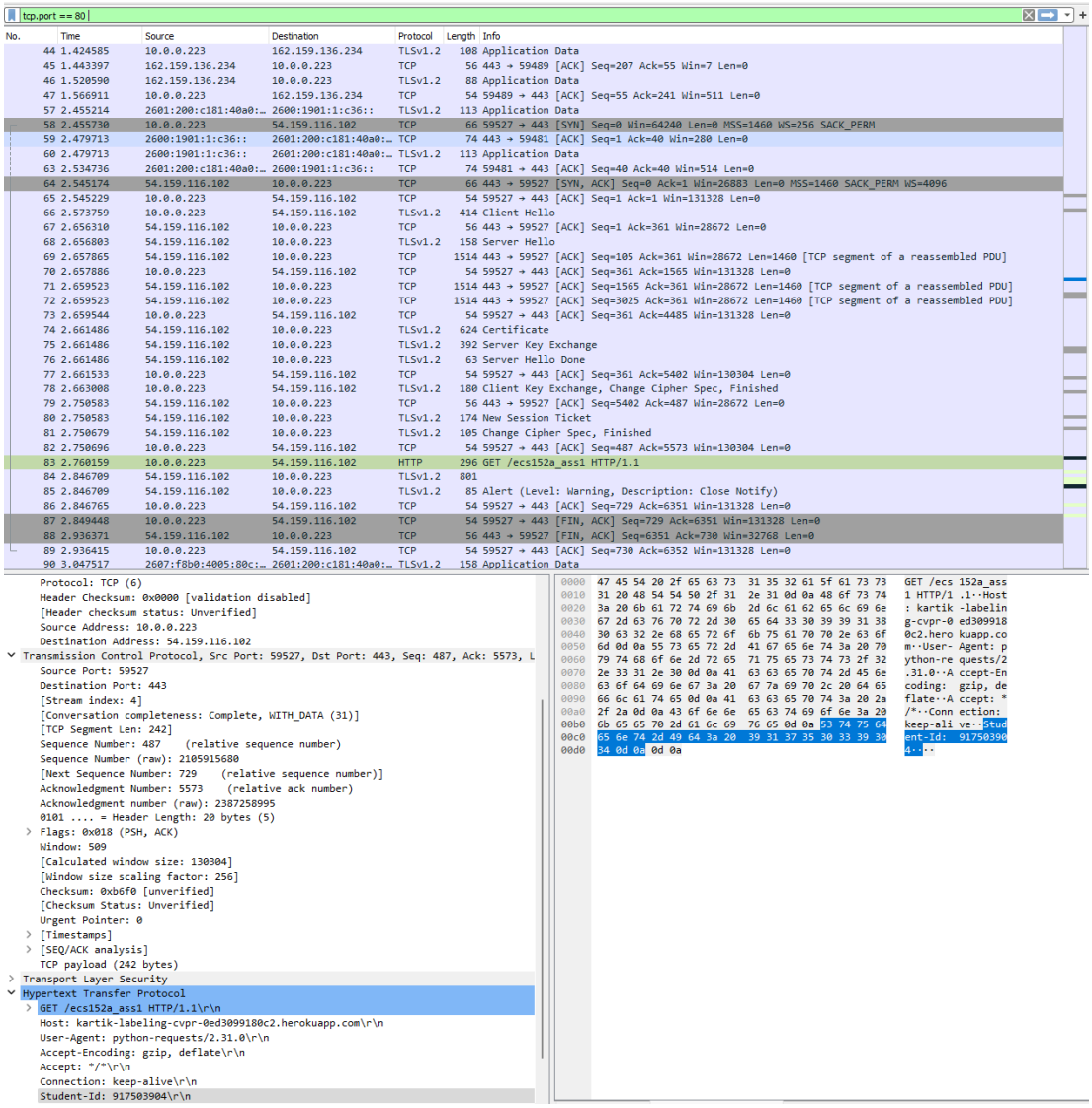
Can I tell what the secret key is?

- Yes. Directly from the Python code, the response headers are printed which include ‘Ecs152a-Resp’ that contains the secret key 240836237

Mitmproxy enabled

```
Flow Details
2023-11-02 21:19:01 GET https://kartik-labeling-cvpr-0ed3099180c2.herokuapp.com/ecs152a_ass1
                    ← 200 OK text/plain 39b 92ms
            Request                 Response                Detail
Report-To:              {"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1698
                        985141&sid=1b10b0ff-8a76-4548-befa-353fc6c6c045&s=i2cwo4pkpCO5dfh0boYrMTf5aS%2ByC2QH1M4wmwKklBg%
                        3D"}]}
Reporting-Endpoints:    heroku-nel=https://nel.heroku.com/reports?ts=1698985141&sid=1b10b0ff-8a76-4548-befa-353fc6c6c045
                        &s=i2cwo4pkpCO5dfh0boYrMTf5aS%2ByC2QH1M4wmwKklBg%3D
Nel:                    {"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"respo
                        nse_headers":["Via"]}
Connection:             close
Server:                 BaseHTTP/0.6 Python/3.11.6
Date:                   Fri, 03 Nov 2023 04:19:01 GMT
Content-Type:           text/plain
Ecs152a-Resp:           240836237
Via:                    1.1 vegur
Raw                                                                                                    [m:auto]
You should look at the response headers
```

Wireshark (with mitmproxy decrypting traffic)



Can I tell what the secret key is?

- From mitmproxy? Yes. You can see the response headers which include the secret key by clicking on the GET request from the terminal. Shown in the above screenshot of mitmproxy.
    - Again it is 'Ecs152a-Resp': '240836237'
- From Wireshark? No. You can see the decrypted GET request that includes the student ID header, but the response is still encrypted.