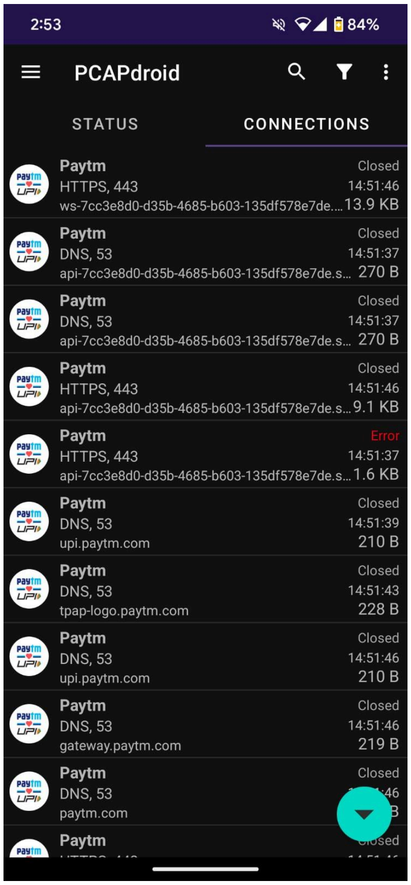
Digital Payment Apps : Week 1

Shreejeet Golhait and Tushman Khalse

Tasks Completed

- **Create a github repo**: Digital Payment Systems

- **Collect logs while running PCAPdroid for a payment on Paytm and analyze the data**: We tried to collect network traffic for various applications and found that PCAPdroid captures most of the traffic including Paytm traffic, but was unable to capture the connection involving a transaction due to Paytm's security measures.



2:53 84%

PCAPdroid

Paytm HTTPS, 443 ws-7cc3e8d0-d35b-4685-b603-135df578e7de.... Closed 14:51:46 13.9 KB

Paytm DNS, 53 api-7cc3e8d0-d35b-4685-b603-135df578e7de.s... Closed 14:51:37 270 B

Paytm DNS, 53 api-7cc3e8d0-d35b-4685-b603-135df578e7de.s... Closed 14:51:37 270 B

Paytm HTTPS, 443 api-7cc3e8d0-d35b-4685-b603-135df578e7de.s... Closed 14:51:46 9.1 KB

Paytm HTTPS, 443 api-7cc3e8d0-d35b-4685-b603-135df578e7de.s... Error 14:51:37 1.6 KB

Paytm DNS, 53 upi.paytm.com Closed 14:51:39 210 B

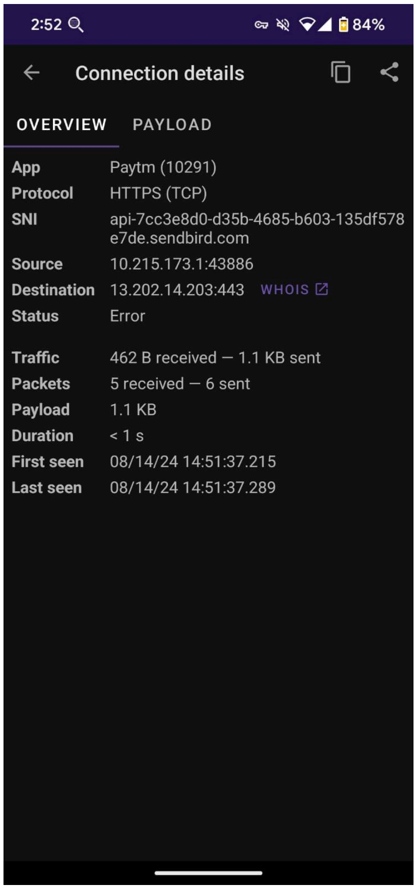
Paytm DNS, 53 tpap-logo.paytm.com Closed 14:51:43 228 B

Paytm DNS, 53 upi.paytm.com Closed 14:51:46 210 B

Paytm DNS, 53 gateway.paytm.com Closed 14:51:46 219 B

Paytm DNS, 53 paytm.com Closed 46 B

Paytm Closed

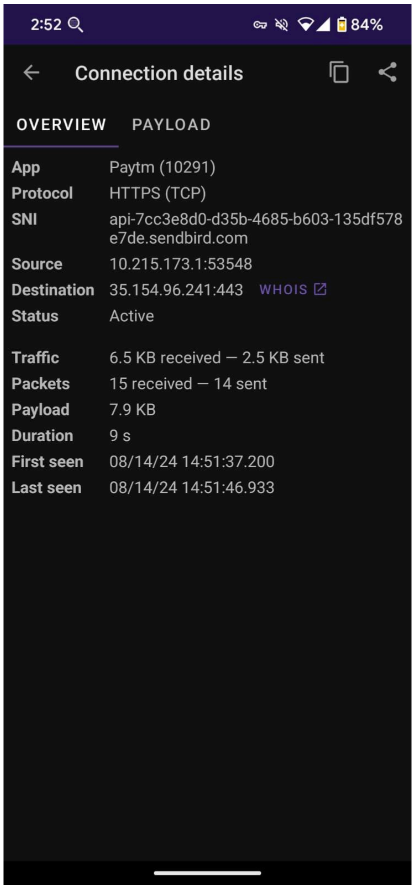


2:52 84%

Connection details

App Paytm (10291)
Protocol HTTPS (TCP)
SNI api-7cc3e8d0-d35b-4685-b603-135df578e7de.sendbird.com
Source 10.215.173.1:43886
Destination 13.202.14.203:443 WHOIS
Status Error

Traffic 462 B received — 1.1 KB sent
Packets 5 received — 6 sent
Payload 1.1 KB
Duration < 1 s
First seen 08/14/24 14:51:37.215
Last seen 08/14/24 14:51:37.289



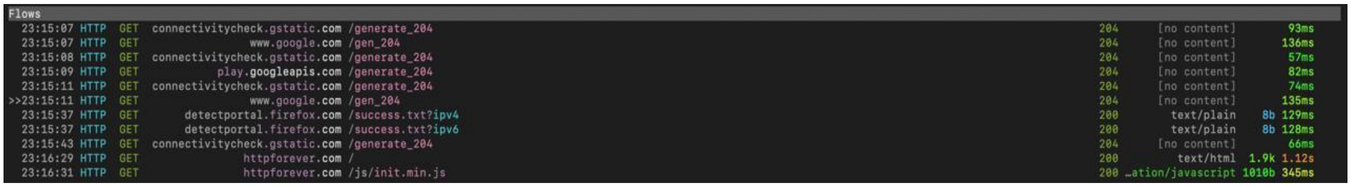
2:52 84%

Connection details

App Paytm (10291)
Protocol HTTPS (TCP)
SNI api-7cc3e8d0-d35b-4685-b603-135df578e7de.sendbird.com
Source 10.215.173.1:53548
Destination 35.154.96.241:443 WHOIS
Status Active

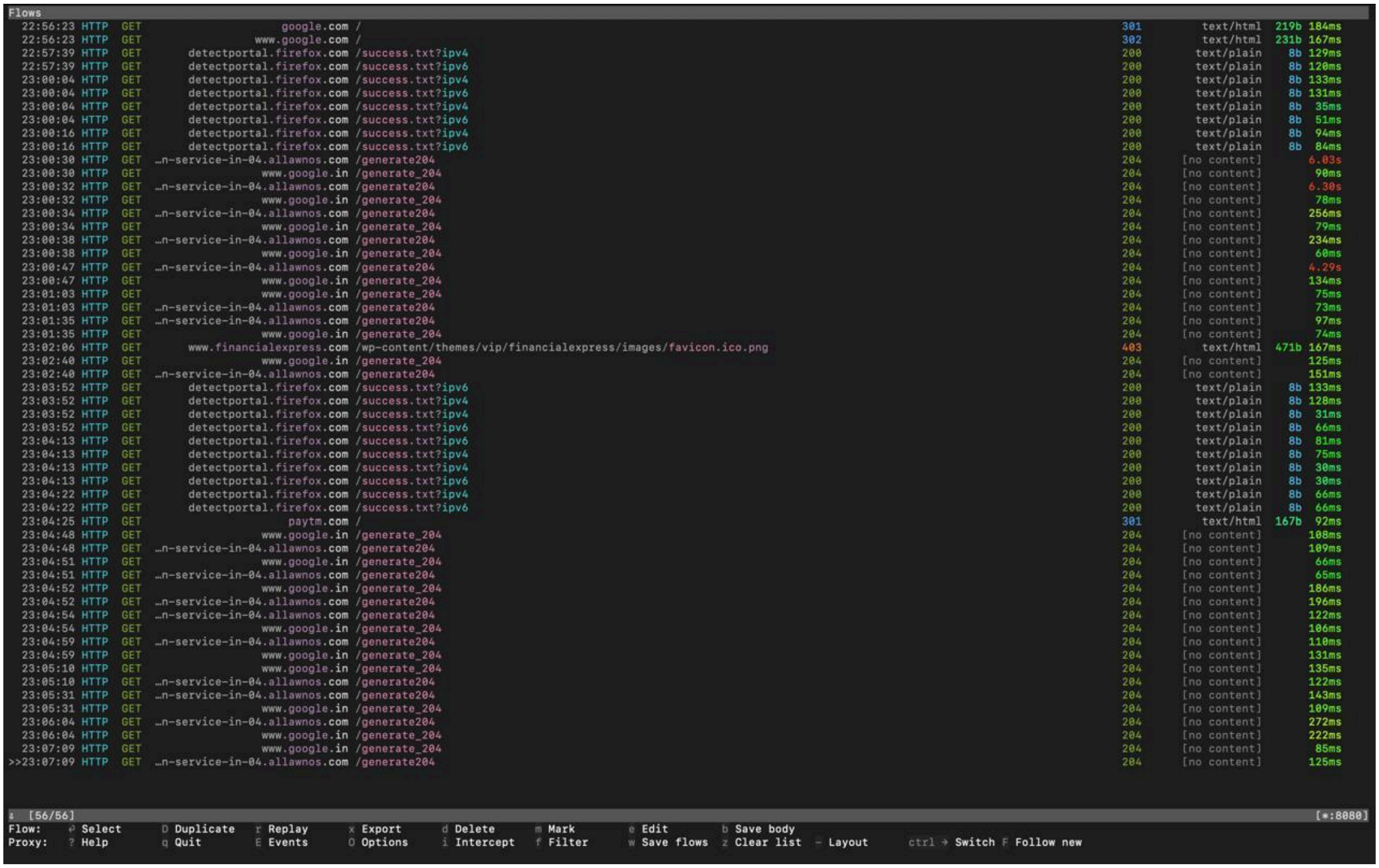
Traffic 6.5 KB received — 2.5 KB sent
Packets 15 received — 14 sent
Payload 7.9 KB
Duration 9 s
First seen 08/14/24 14:51:37.200
Last seen 08/14/24 14:51:46.933

- **Set up MITM Proxy, configure proxy on phone and collect traffic with a non-trusted proxy**: We were successful in setting up MITMProxy on our computer device and even collected network traffic from the computer. Then we connected our Android device to the MITMProxy without trusting it in order to capture traffic, and we could capture the initial calls for http packets, and the calls failed to proceed beyond that point.



```
Flows
  23:15:07 HTTP  GET  connectivitycheck.gstatic.com /generate_204          204   [no content]         93ms
  23:15:07 HTTP  GET                 www.google.com /gen_204               204   [no content]        136ms
  23:15:08 HTTP  GET  connectivitycheck.gstatic.com /generate_204          204   [no content]         57ms
  23:15:09 HTTP  GET             play.googleapis.com /generate_204          204   [no content]         82ms
  23:15:11 HTTP  GET  connectivitycheck.gstatic.com /generate_204          204   [no content]         74ms
>>23:15:11 HTTP  GET                 www.google.com /gen_204               204   [no content]        135ms
  23:15:37 HTTP  GET      detectportal.firefox.com /success.txt?ipv4      200     text/plain     8b 129ms
  23:15:37 HTTP  GET      detectportal.firefox.com /success.txt?ipv6      200     text/plain     8b 128ms
  23:15:43 HTTP  GET  connectivitycheck.gstatic.com /generate_204          204   [no content]         66ms
  23:16:29 HTTP  GET              httpforever.com /                       200      text/html   1.9k 1.12s
  23:16:31 HTTP  GET              httpforever.com /js/init.min.js         200 …ation/javascript 1010b 345ms
```

- **Configure it to be a trusted proxy and then try to collect Paytm traffic**: We then trusted the proxy by adding the certificate for it in our Android device, which still didn't allow us to capture https traffic resulting in a similar capture.



```
Flows
  22:56:23 HTTP  GET                 google.com /                                                               301      text/html  219b 184ms
  22:56:23 HTTP  GET             www.google.com /                                                               302      text/html  231b 167ms
  22:57:39 HTTP  GET   detectportal.firefox.com /success.txt?ipv4                                               200     text/plain    8b 129ms
  22:57:39 HTTP  GET   detectportal.firefox.com /success.txt?ipv6                                               200     text/plain    8b 120ms
  23:00:04 HTTP  GET   detectportal.firefox.com /success.txt?ipv4                                               200     text/plain    8b 133ms
  23:00:04 HTTP  GET   detectportal.firefox.com /success.txt?ipv6                                               200     text/plain    8b 131ms
  23:00:04 HTTP  GET   detectportal.firefox.com /success.txt?ipv4                                               200     text/plain    8b  35ms
  23:00:04 HTTP  GET   detectportal.firefox.com /success.txt?ipv6                                               200     text/plain    8b  51ms
  23:00:16 HTTP  GET   detectportal.firefox.com /success.txt?ipv4                                               200     text/plain    8b  94ms
  23:00:16 HTTP  GET   detectportal.firefox.com /success.txt?ipv6                                               200     text/plain    8b  84ms
  23:00:30 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]       6.03s
  23:00:30 HTTP  GET              www.google.in /generate_204                                                   204   [no content]        90ms
  23:00:32 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]       6.30s
  23:00:32 HTTP  GET              www.google.in /generate_204                                                   204   [no content]        78ms
  23:00:34 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]       256ms
  23:00:34 HTTP  GET              www.google.in /generate_204                                                   204   [no content]        79ms
  23:00:38 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]       234ms
  23:00:38 HTTP  GET              www.google.in /generate_204                                                   204   [no content]        60ms
  23:00:47 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]       4.29s
  23:00:47 HTTP  GET              www.google.in /generate_204                                                   204   [no content]       134ms
  23:01:03 HTTP  GET              www.google.in /generate_204                                                   204   [no content]        75ms
  23:01:03 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]        73ms
  23:01:35 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]        97ms
  23:01:35 HTTP  GET              www.google.in /generate_204                                                   204   [no content]        74ms
  23:02:06 HTTP  GET   www.financialexpress.com /wp-content/themes/vip/financialexpress/images/favicon.ico.png  403      text/html  471b 167ms
  23:02:40 HTTP  GET              www.google.in /generate_204                                                   204   [no content]       125ms
  23:02:40 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]       151ms
  23:03:52 HTTP  GET   detectportal.firefox.com /success.txt?ipv6                                               200     text/plain    8b 133ms
  23:03:52 HTTP  GET   detectportal.firefox.com /success.txt?ipv4                                               200     text/plain    8b 128ms
  23:03:52 HTTP  GET   detectportal.firefox.com /success.txt?ipv4                                               200     text/plain    8b  31ms
  23:03:52 HTTP  GET   detectportal.firefox.com /success.txt?ipv6                                               200     text/plain    8b  66ms
  23:04:13 HTTP  GET   detectportal.firefox.com /success.txt?ipv6                                               200     text/plain    8b  81ms
  23:04:13 HTTP  GET   detectportal.firefox.com /success.txt?ipv4                                               200     text/plain    8b  75ms
  23:04:13 HTTP  GET   detectportal.firefox.com /success.txt?ipv4                                               200     text/plain    8b  30ms
  23:04:13 HTTP  GET   detectportal.firefox.com /success.txt?ipv6                                               200     text/plain    8b  30ms
  23:04:22 HTTP  GET   detectportal.firefox.com /success.txt?ipv4                                               200     text/plain    8b  66ms
  23:04:22 HTTP  GET   detectportal.firefox.com /success.txt?ipv6                                               200     text/plain    8b  66ms
  23:04:25 HTTP  GET                  paytm.com /                                                               301      text/html  167b  92ms
  23:04:48 HTTP  GET              www.google.in /generate_204                                                   204   [no content]       108ms
  23:04:48 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]       109ms
  23:04:51 HTTP  GET              www.google.in /generate_204                                                   204   [no content]        66ms
  23:04:51 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]        65ms
  23:04:52 HTTP  GET              www.google.in /generate_204                                                   204   [no content]       186ms
  23:04:52 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]       196ms
  23:04:54 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]       122ms
  23:04:54 HTTP  GET              www.google.in /generate_204                                                   204   [no content]       106ms
  23:04:59 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]       110ms
  23:04:59 HTTP  GET              www.google.in /generate_204                                                   204   [no content]       131ms
  23:05:10 HTTP  GET              www.google.in /generate_204                                                   204   [no content]       135ms
  23:05:10 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]       122ms
  23:05:31 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]       143ms
  23:05:31 HTTP  GET              www.google.in /generate_204                                                   204   [no content]       109ms
  23:06:04 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]       272ms
  23:06:04 HTTP  GET              www.google.in /generate_204                                                   204   [no content]       222ms
  23:07:09 HTTP  GET              www.google.in /generate_204                                                   204   [no content]        85ms
>>23:07:09 HTTP  GET …n-service-in-04.allawnos.com /generate204                                                 204   [no content]       125ms

⇕  [56/56]                                                                                                                         [*:8080]
Flow:    ↵ Select    D Duplicate  r Replay   x Export   d Delete     m Mark     e Edit        b Save body
Proxy:   ? Help      q Quit       E Events   O Options  i Intercept  f Filter   w Save flows  z Clear list  - Layout    ctrl → Switch F Follow new
```

Conclusion

We completed all the steps and tried to trace Paytm payment data as instructed. We were able to set up MITMproxy with both the laptop and mobile devices connected to another mobile hotspot since we were unable to set up a proxy on the campus wifi. This could be due to enhanced security measures present in the campus wifi. We were able to capture general Paytm traffic via PCAPdroid but when we tried to capture the traffic involving a transaction, we were unable to do so. At the same time, MITMProxy did not allow us to capture general traffic from Paytm either probably due to being secured by https protocol.