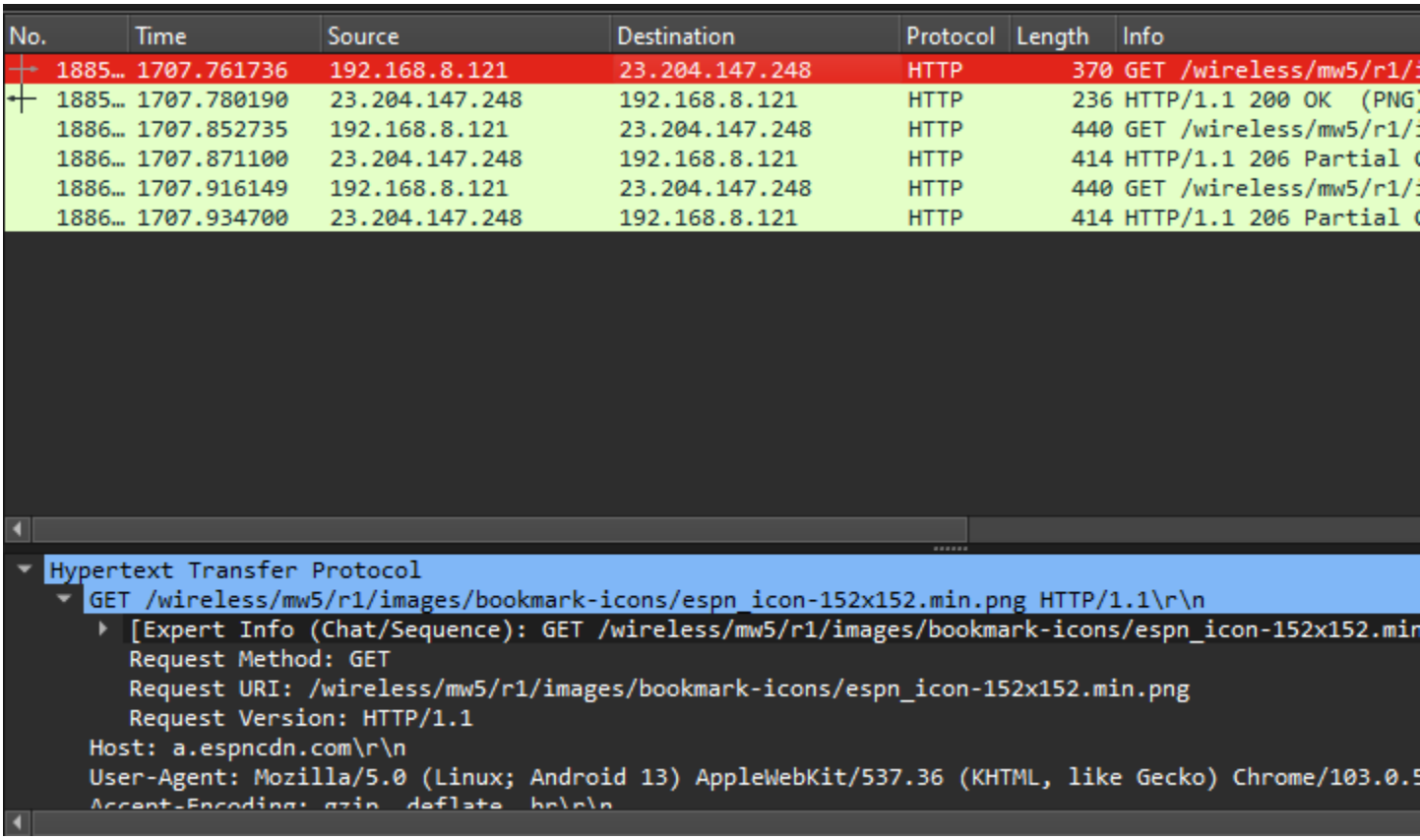
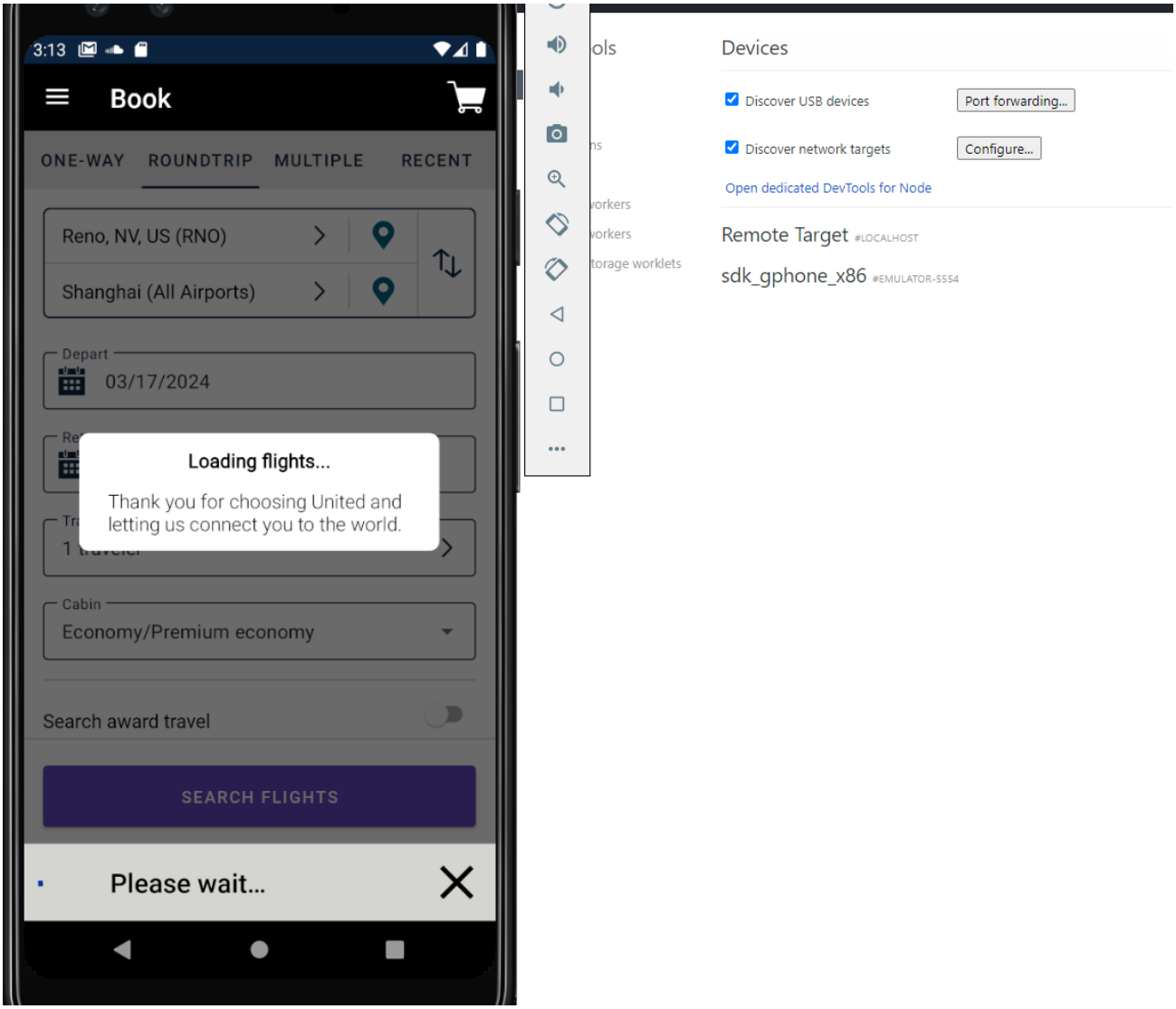


Wireshark is not capturing any traffic from the untied airlines app. Above is the example of it capturing test ESPN traffic.



According to MobSF reports there are webviews for the united airlines app however I could not find the app functionality that triggered the webview.

749	https://js.appboycdn.com	GET	/web-sdk/5.0/braze.min.js				
750	https://d.impactradius-event...	GET	/A1323623-ff1f-47da-bf87-01a656...				
751	https://sb.scorecardresearc...	GET	/cs/3000005/beacon.js				
752	https://vision.fn-pz.com	OPTIO...	/v2/config/wdgespcom				
753	https://vision.fn-pz.com	OPTIO...	/v2/event				
754	https://www.facebook.com	GET	/tr/?id=504412503408123&ev=Pa...	✓		200	447
755	https://www.espn.com	GET	/service-worker.js			304	403
756	https://secure.espn.com	GET	/core/nfl/?xhr=1&render=true&d...	✓		200	173
757	https://sw88.espn.com	GET	/b/ss/wdgespcom,wdgespge/1/JS...	✓			
758	https://www.facebook.com	GET	/tr/?id=504412503408123&ev=Pa...	✓		200	447
759	https://sw88.espn.com	GET	/b/ss/wdgespcom,wdgespge/1/JS...	✓			
760	https://cdn.taboola.com	GET	/libtrc/espn-network/loader.js				
761	https://site.api.espn.com	GET	/apis/personalized/v2/scoreboard...	✓		200	103
762	https://dcf.espn.com	GET	/TWDC-DTCI/prod/serverCompon...	✓		200	152
763	https://vision.fn-pz.com	OPTIO...	/v2/event				
764	https://sb.scorecardresearc...	GET	/cs/3000005/beacon.js				
765	https://vision.fn-pz.com	OPTIO...	/v2/event				
767	http://redirector.gvt1.com	GET	/edgedl/release2/chrome_compo...			302	122
770	https://update.googleapis.c...	POST	/service/update2/json	✓		200	918
773	https://update.googleapis.c...	POST	/service/update2/json	✓		200	902
774	https://vision.fn-pz.com	OPTIO...	/v2/event				
777	https://update.googleapis.c...	POST	/service/update2/json	✓		200	902

Same situation with the proxying http + adding ca certificate. Only test espn traffic was captured.

network_security_config.xml

C: > Users > migue > Documents > CS435-Mobile_Sec > Module-6 > united-airlines > res > xml >

```xml
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <base-config cleartextTrafficPermitted="false" />
    <domain-config cleartextTrafficPermitted="true">
        <domain includeSubdomains="true">127.0.0.1</domain>
        <domain includeSubdomains="true">172.27.4.91</domain>
        <domain includeSubdomains="true">192.168.1.1</domain>
        <domain includeSubdomains="true">localhost</domain>
        <domain includeSubdomains="true">airpana.com</domain>
        <domain includeSubdomains="true">gogoinflight.com</domain>
        <domain includeSubdomains="true">inflightinternet.com</domain
        <domain includeSubdomains="true">ideanovatech.com</domain>
        <domain includeSubdomains="true">inflightpanasonic.aero</doma
        <domain includeSubdomains="true">ufs.ltv</domain>
        <domain includeSubdomains="true">jcb-card.jp</domain>
    </domain-config>
</network-security-config>
```

Evidence of preconfigured clear text traffic of the above domains

Event detail

Time:	22:06:45 9 Mar 2024
Type:	Error
Source:	Proxy
Message:	[2] Unknown host: airbornemedia.inflightinternet.com

Error from on of the above domains when using the proxy

NO	ISSUE	SEVERITY	STANDARDS
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK

This app uses SSL Pinning and therefore I've been prevented from seeing any traffic from the united airlines app, I will have to test the ssl pinning work around.