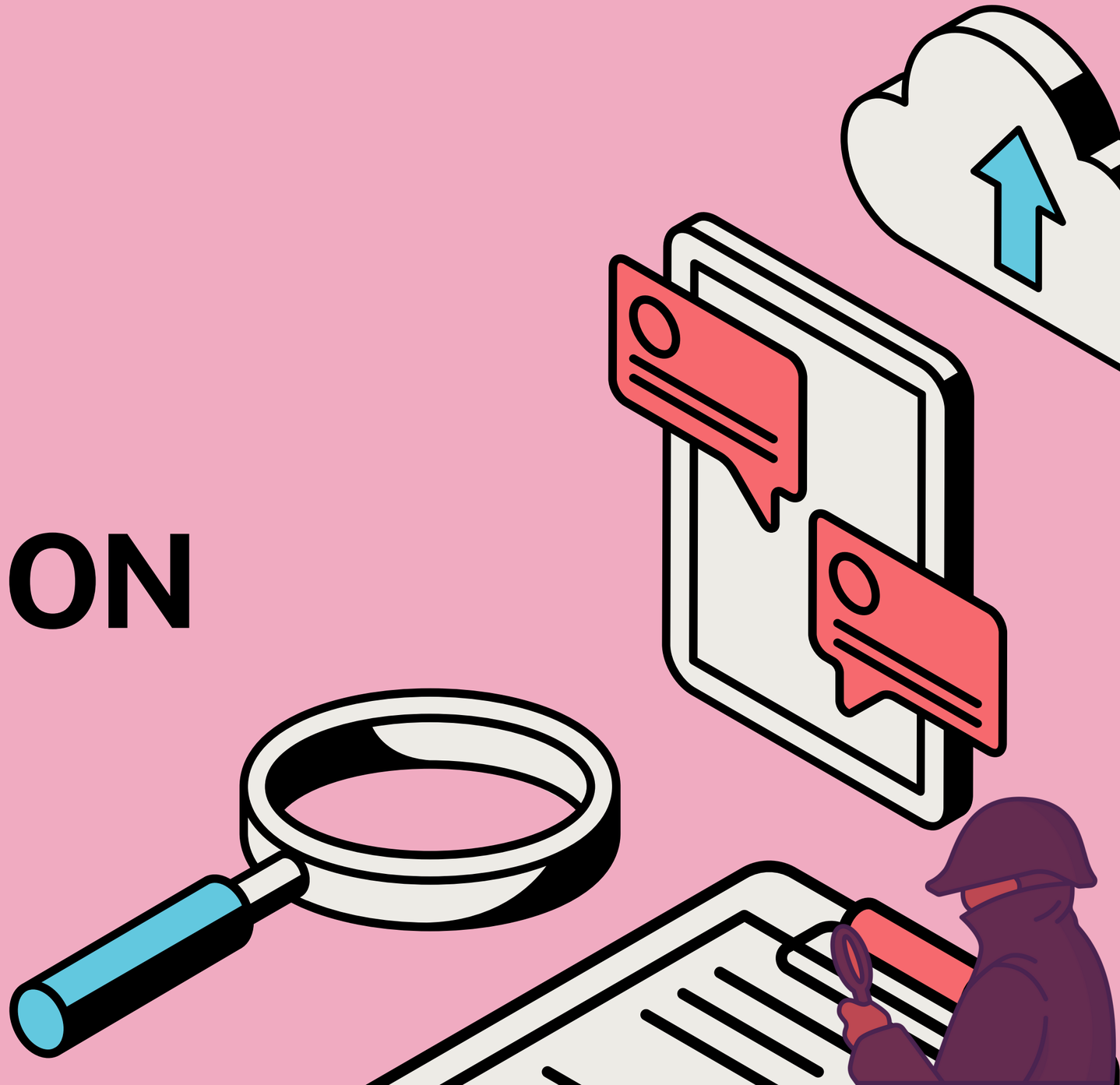
TEAM

INSE 6110 PROJECT PRESENTATION

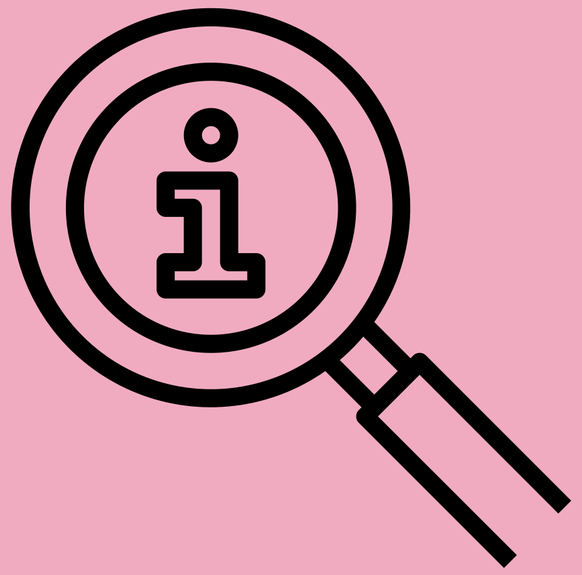


Date: April 17, 2023

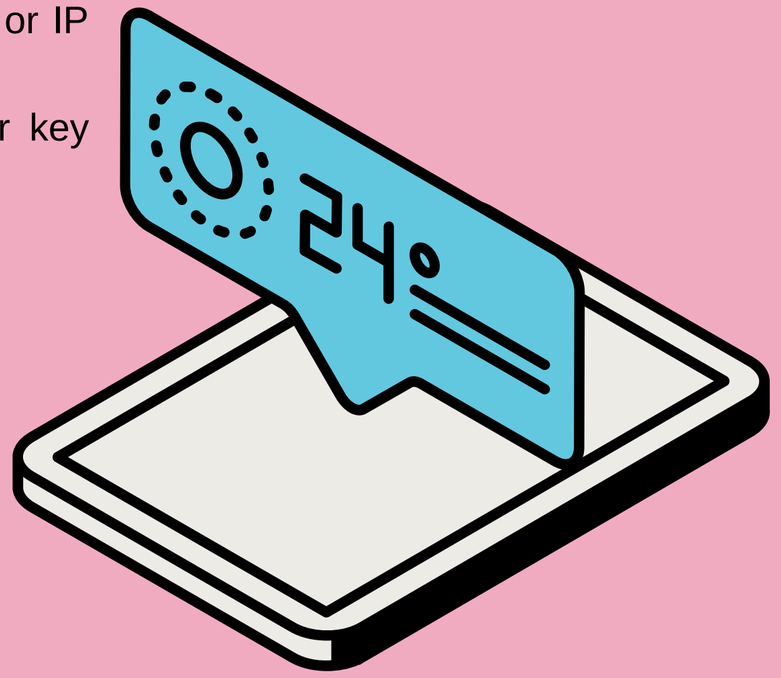
In this document:

1.

What is TLS Pinning?



- TLS (Transport Layer Security) : secure communication between websites and servers.
- involves associating a specific TLS certificate or public key
  - with a particular domain name or IP address, instead of relying on the trusted certificate authorities.
- Goal: prevent man-in-the-middle attacks.
- Client application stores the trusted certificate or public key for a specific domain or IP address
  - Only accepts connections from servers that present that exact certificate or key during the TLS handshake.



2. Static Analysis for TLS Pinning

Here we use ApkTool

- Download apktool files (.bat and .jar) from the internet (Link provided in document)
- Save them in C://Windows folder
- Download the android app (You can use uptodown)
- Open terminal - navigate to downloaded application
- Decompile app using apktool - apktool -d <appname.apk>
- This should generate a folder with decompiled files
- Open the folder > Go to android manifest file
- Open the file, search for Network Security Config file or NSC -> Check the link stated with it
- Navigate to the link and note down the subdomains and hashed certificate entries

2. Static Analysis for TLS Pinning

```
PS C:\Users\rahul\Downloads\Tes> apktool d .\instagram.apk
I: Using Apktool 2.7.0 on instagram.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\rahul\AppData\Local\apktool\framework\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Baksmaling classes3.dex...
I: Baksmaling classes4.dex...
I: Baksmaling classes5.dex...
I: Baksmaling classes6.dex...
I: Baksmaling classes7.dex...
I: Baksmaling classes8.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
Press any key to continue . . .
```

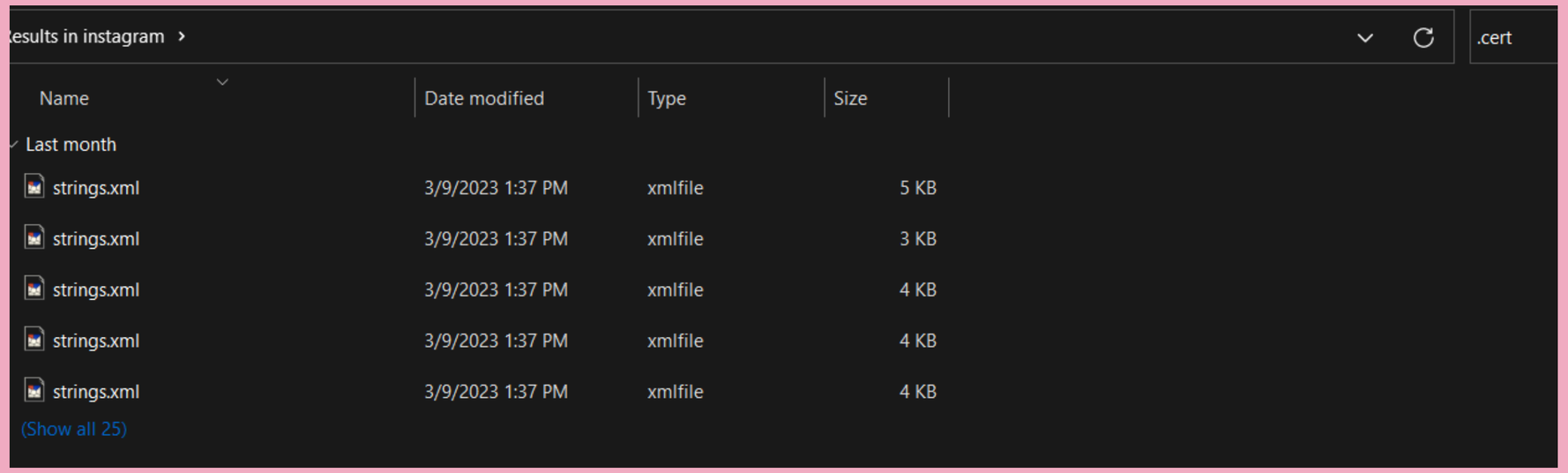
```
llowTaskReparenting="true" android:appComponentFactory="androidx.c
" android:networkSecurityConfig="@xml/fb_network_security_config"
d.channel" android:value="playstore"/>
```

```
<network-security-config>
    <base-config cleartextTrafficPermitted="true">
        <trust-anchors>
            <certificates src="system" />
            <certificates overridePins="true" src="user" />
        </trust-anchors>
    </base-config>
    <domain-config cleartextTrafficPermitted="false">
        <domain includeSubdomains="true">facebook.com</domain>
        <domain includeSubdomains="true">fbcdn.net</domain>
        <domain includeSubdomains="true">fbsbx.com</domain>
        <domain includeSubdomains="true">facebookcorewwwi.onion</domain>
        <domain includeSubdomains="true">fbcdn23dssr3jqnq.onion</domain>
        <domain includeSubdomains="true">fbsbx2q4mvcl63pw.onion</domain>
        <domain includeSubdomains="true">instagram.com</domain>
        <domain includeSubdomains="true">cdninstagram.com</domain>
        <domain includeSubdomains="true">workplace.com</domain>
        <domain includeSubdomains="true">oculus.com</domain>
        <domain includeSubdomains="true">facebookvirtualassistant.com</domain>
        <domain includeSubdomains="true">discoverapp.com</domain>
        <domain includeSubdomains="true">freebasics.com</domain>
        <domain includeSubdomains="true">internet.org</domain>
        <domain includeSubdomains="true">viewpointsfromfacebook.com</domain>
        <pin-set expiration="2024-03-05">
            <pin digest="SHA-256">lCppFqbkrlJ3EcVFAkeip0+44VaoJUymbnOaEUk7tEU=</pin>
            <pin digest="SHA-256">grX4Ta9HpZx6tSHkmCrvpApTQGo67CYDnvprLg5yRME=</pin>
            <pin digest="SHA-256">I/Lt/z7ekCWanjD0Cvj5EqXls2lOaThEA0H2Bg4BT/o=</pin>
            <pin digest="SHA-256">8ca6Zwz8iOTfUpc8rkIPCgid1HQUT+WAbEIAZOFZEik=</pin>
            <pin digest="SHA-256">Fe7TOVlLME+M+Ee0dzcdjW/sYfTbKwGvWJ58U7Ncrkw=</pin>
            <pin digest="SHA-256">r/mIkG3eEpVdm+u/ko/cwxzOMo1bk4TyHIlByibiA5E=</pin>
```

2. Static Analysis for TLS Pinning

Searching for certificates

- You manually search for certificates here in the decompiled folder, using wildcards such as .cert, .pem, .cer
- You should see certificates show up, if you dont, its simple -> This method was not used



2. Static Analysis for TLS Pinning

Using crt.sh

- Open the android manifest file
- Navigate to the domain host entry and note down the host link - should be something like www.<application>.com
- Open a web browser and navigate to crt.sh
- Search for this domain on it
- It should give you a list of certificate entries, the latest one is the active one, select it
- It should give you information about the certifier.

2. Static Analysis for TLS Pinning

```
<data android:host="instagram.com"/>
<data android:host="www.instagram.com"/>
<data android:host="applink.instagram.com"/>
<data android:host="familycenter.instagram.com"/>
ntent-filter>
```

crt.sh Identity Search

Group by Issuer

Criteria	Type: Identity	Match: ILIKE	Search: 'www.instagram.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
9151882553	2023-04-15	2023-04-15	2023-07-14	*.www.instagram.com	*.www.instagram.com www.instagram.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
9142046825	2023-04-14	2023-04-14	2023-07-13	*.www.instagram.com	*.www.instagram.com www.instagram.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
9132271400	2023-04-13	2023-04-13	2023-07-12	*.www.instagram.com	*.www.instagram.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA

SHA-256 931FFFFFA2A54632DAC84D80CE506546F3F24BF408D1B6AA4B62004EC32814BF SHA-1 8

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0d:b9:3e:ca:10:f7:94:3d:36:3c:67:bc:fe:7b:e0:e7
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 1397)
            commonName                = DigiCert SHA2 High Assurance Server CA
            organizationalUnitName    = www.digicert.com
            organizationName          = DigiCert Inc
            countryName               = US
```

2. Static Analysis for TLS Pinning

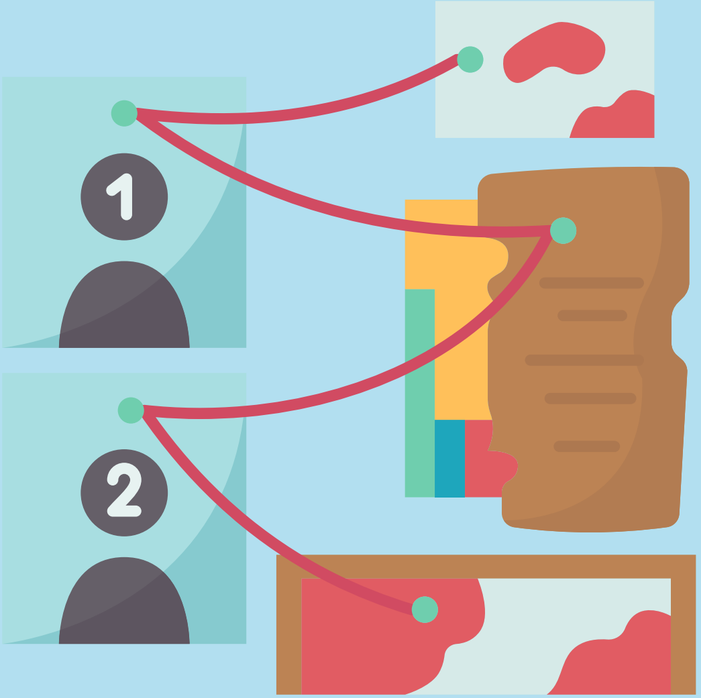
Third Party Analysis

- You do crt.sh for multiple applications
- See if you find a common certifier - this means it should be a trusted CA.

3: Dynamic Analysis

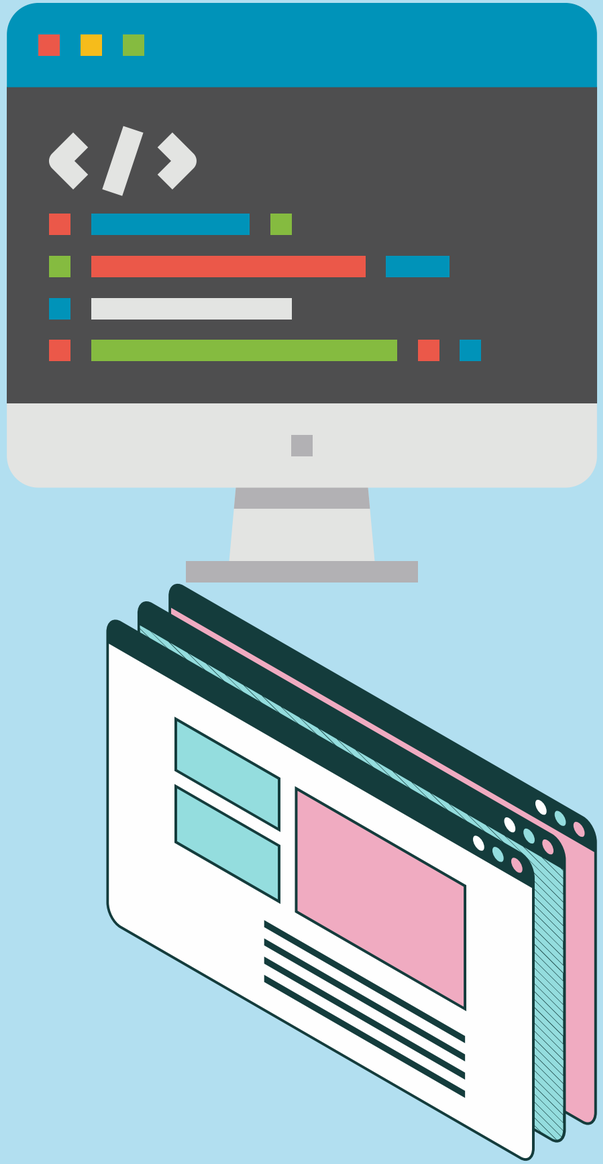
Setup required

- Download MITM proxy tool
- Download android studio
- Setup emulator on android studio with playstore, we selected Pixel 4
- MITM certificate. Store it in system certificates.



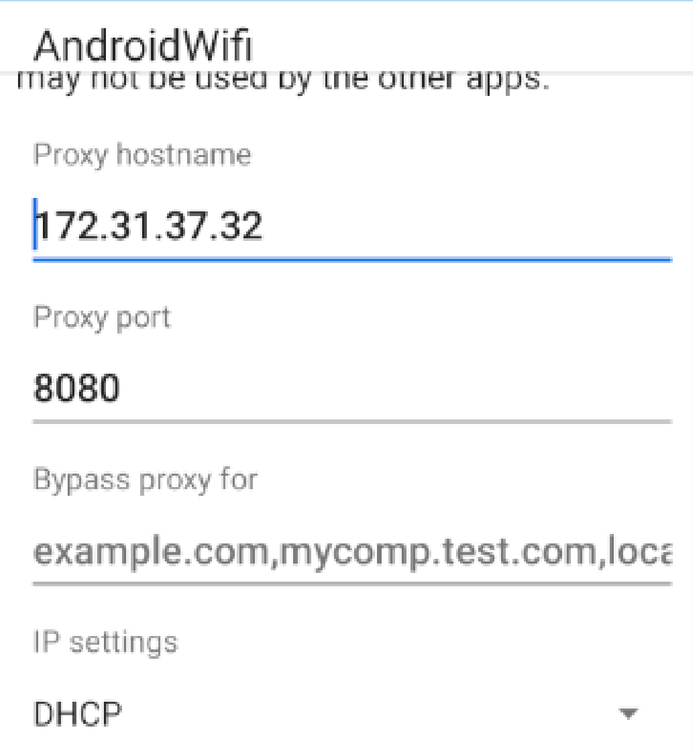
3: Dynamic Analysis

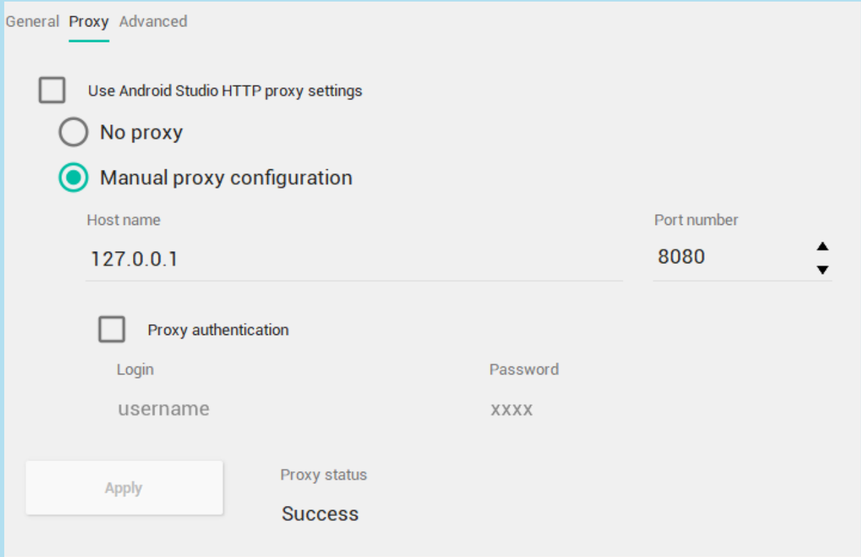
- Run the mitm proxy via terminal - mitmweb
- You should see the IP and port the mitm is hosted on
- Open android studio and run the emulator
- Setup the phone proxy to the one as the system
- Install the same application as the static one
- Go to settings of the emulator > Network > Proxy
- Uncheck (No Proxy needed) option and enter the IP and port that is provided by the mitmweb, select apply - it should say success.
- Open the installed application and observe how mitmweb captures traffic.
- There will be a point where the application tries to contact its server via port 443 (SSH) and its TLS pinned certificate stops it with the error, the certificate is not recognised - evidence of certificate pinning.



3: Dynamic Analysis

```
[02:54:06.588][127.0.0.1:54367] client connect
[02:54:06.592][127.0.0.1:54367] server connect 172.217.13.99:443
[02:54:50.674][127.0.0.1:54318] server disconnect 31.13.80.34:443
[02:54:50.675][127.0.0.1:54318] client disconnect
[02:54:55.580][127.0.0.1:54418] client connect
[02:54:55.585][127.0.0.1:54418] server connect 31.13.80.52:443
[02:54:56.100][127.0.0.1:54418] Client TLS handshake failed. The client does
 not trust the proxy's certificate for i.instagram.com (sslv3 alert bad cert
ificate)
[02:54:56.101][127.0.0.1:54418] client disconnect
[02:54:56.102][127.0.0.1:54418] server disconnect 31.13.80.52:443
```





4
Conclusion

Following is the conclusion of the project

1	Using static analysis, we observe how certificates are embedded via different methods
2	Decompiling the application provides all the details about the configurations of the application
3	TLS pinning prevents the application against MITM attacks, which was observed via dynamic analysis

Questions?

Thank you.