# 9-Network Interception

هنتكلم بقي عن Network Interception ازاي نحاول ان احنا capturing, analyzing, and manipulating network traffic between the Android application and its backend server

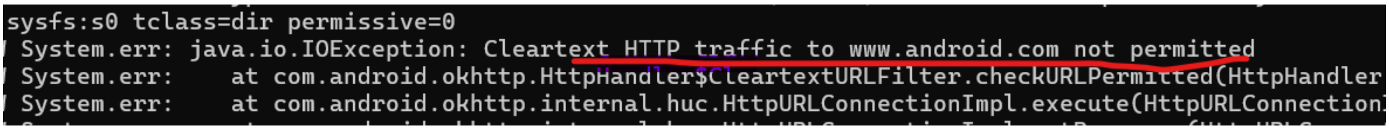
## 1-The INTERNET Permission

ايه الصلاحيات اللي محتاجنها لو عاوزين مثلا نخلي app يبعت Request ل website ايه اللي لازم نعمله علشان الطلب يكتمل فمثلا لو run this code

```
   ExecutorService executorService = Executors.newSingleThreadExecutor();
                executorService.execute(()->{
                    try {
                            URL url=new URL("http://www.android.com/");
                        HttpURLConnection urlConnection=(HttpURLConnection)
url.openConnection();
                        InputStream in=new
BufferedInputStream(urlConnection.getInputStream());
                        BufferReader reader=new BufferReader(new
InputStreamReader(in));
                        StringBuilder sb=new StringBuilder();
                        String line;
                        while ((line=reader.readLine())!=null){
                            sb.append(line).append("\n");

                        }
                        String result=sb.toString();
                        BreakIterator homeText = null;
                        runOnUiThread(()->homeText.setText(result));
                    }catch (Exception e){
                        e.printStackTrace();
                    }
                });

                }

        });
```

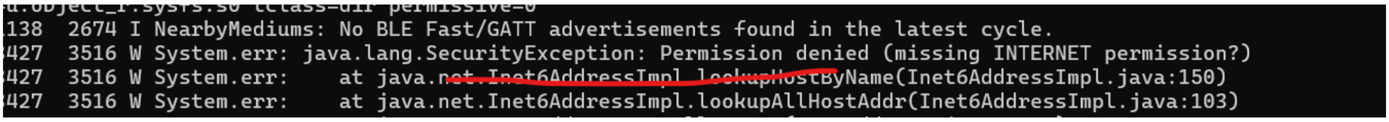
هنلاقي ان هو مش بيسمح ان هو يبعت http

1- ودي اول حاجة لو بنستخدم  default network on android هيمنعني ان اطلب http



```
sysfs:s0 tclass=dir permissive=0
/ System.err: java.io.IOException: Cleartext HTTP traffic to www.android.com not permitted
/ System.err:     at com.android.okhttp.HttpHandler$CleartextURLFilter.checkURLPermitted(HttpHandler
/ System.err:     at com.android.okhttp.internal.huc.HttpURLConnectionImpl.execute(HttpURLConnectionI
```

بس لو غيرنا ل https برده مش هيرسل request

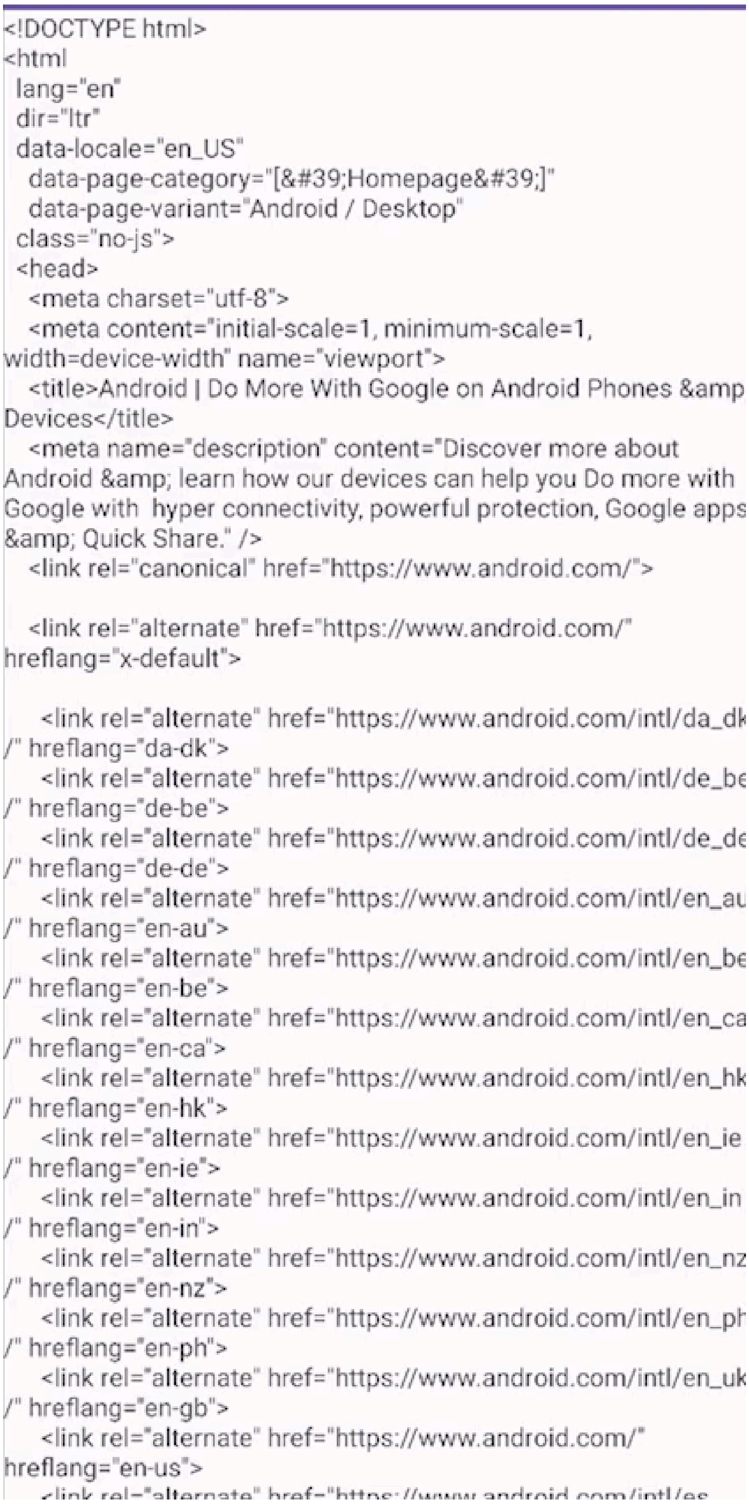


```
138  2674 I NearbyMediums: No BLE Fast/GATT advertisements found in the latest cycle.
427  3516 W System.err: java.lang.SecurityException: Permission denied (missing INTERNET permission?)
427  3516 W System.err:     at java.net.Inet6AddressImpl.lookupHostByName(Inet6AddressImpl.java:150)
427  3516 W System.err:     at java.net.Inet6AddressImpl.lookupAllHostAddr(Inet6AddressImpl.java:103)
```

2- علشان لازم نحط في androidMeniFast.xml تحط صلاحيات ان احنا نستخدم Internet ودي تاني حاجة لازم ناخد بالنا منها

```
    <uses-permission android:name="android.permission.INTERNET"/>
```

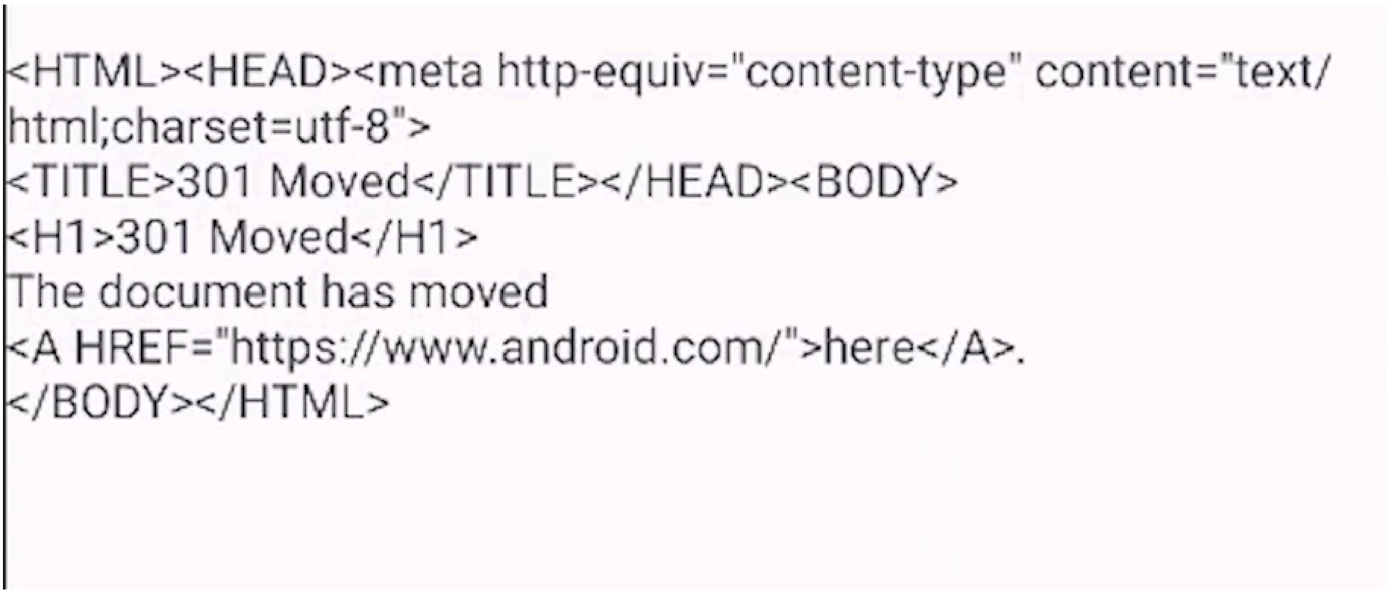
هلناقيه بيبعت Request عادي



```
<!DOCTYPE html>
<html
 lang="en"
 dir="ltr"
 data-locale="en_US"
   data-page-category="[&#39;Homepage&#39;]"
   data-page-variant="Android / Desktop"
 class="no-js">
 <head>
   <meta charset="utf-8">
   <meta content="initial-scale=1, minimum-scale=1,
width=device-width" name="viewport">
   <title>Android | Do More With Google on Android Phones &amp
Devices</title>
   <meta name="description" content="Discover more about
Android &amp; learn how our devices can help you Do more with
Google with  hyper connectivity, powerful protection, Google apps
&amp; Quick Share." />
   <link rel="canonical" href="https://www.android.com/">

   <link rel="alternate" href="https://www.android.com/"
hreflang="x-default">

     <link rel="alternate" href="https://www.android.com/intl/da_dk
/" hreflang="da-dk">
     <link rel="alternate" href="https://www.android.com/intl/de_be
/" hreflang="de-be">
     <link rel="alternate" href="https://www.android.com/intl/de_de
/" hreflang="de-de">
     <link rel="alternate" href="https://www.android.com/intl/en_au
/" hreflang="en-au">
     <link rel="alternate" href="https://www.android.com/intl/en_be
/" hreflang="en-be">
     <link rel="alternate" href="https://www.android.com/intl/en_ca
/" hreflang="en-ca">
     <link rel="alternate" href="https://www.android.com/intl/en_hk
/" hreflang="en-hk">
     <link rel="alternate" href="https://www.android.com/intl/en_ie
/" hreflang="en-ie">
     <link rel="alternate" href="https://www.android.com/intl/en_in
/" hreflang="en-in">
     <link rel="alternate" href="https://www.android.com/intl/en_nz
/" hreflang="en-nz">
     <link rel="alternate" href="https://www.android.com/intl/en_ph
/" hreflang="en-ph">
     <link rel="alternate" href="https://www.android.com/intl/en_uk
/" hreflang="en-gb">
     <link rel="alternate" href="https://www.android.com/"
hreflang="en-us">
     <link rel="alternate" href="https://www.android.com/intl/es
```

3- لو احنا بقي عاوزين نستخدم http ممكن نضيف flat يسمح ب استخدام Cleartext Traffic

```
android:usesCleartextTraffic="true"
```



```
<HTML><HEAD><meta http-equiv="content-type" content="text/
html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="https://www.android.com/">here</A>.
</BODY></HTML>
```

ممكن برضه نستخدم مكتبة socket علشان نرسل request

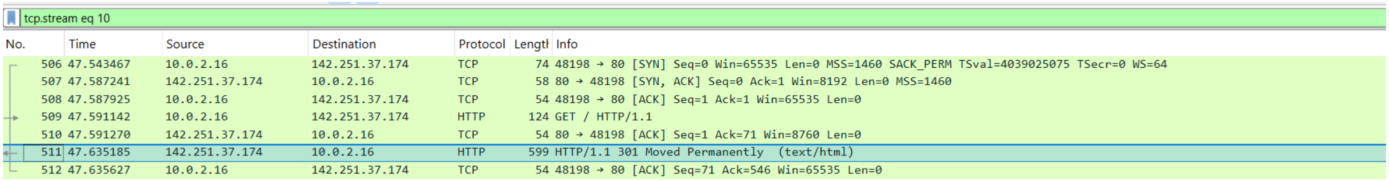
```
ExecutorService executorService = Executors.newSingleThreadExecutor();
                executorService.execute(()->{
                    try {
                        Socket socket=new Socket("www.android.com",80);
                        OutputStream outputStream=socket.getOutputStream();
                        BufferReader reader=new BufferReader(new
InputStreamReader(socket.getInputStream()));
                        String request ="GET /
HTTP/1.1\r\nHost:www.android.com\r\nUser-Agent: app\r\nAccept: */*\r\n\r\n";
                        outputStream.write(request.getBytes());
                        outputStream.flush();
                        StringBuilder sb=new StringBuilder();
                        String line;
                        StringBuffer homeText;
                        while ((line=reader.readLine())!=null){
                            String finalline=line;

                            runOnUiThread(()->homeText.append(finalline));

                        }
                        String result=sb.toString();

                    }catch (Exception e){
                        e.printStackTrace();
                    }
                });
```

يبقيكده ايه اللي ممكن نستفاده ان لو لاقيت flag ده `"android:usesCleartextTraffic="true` فمعني كده ان app use cleartext traffic

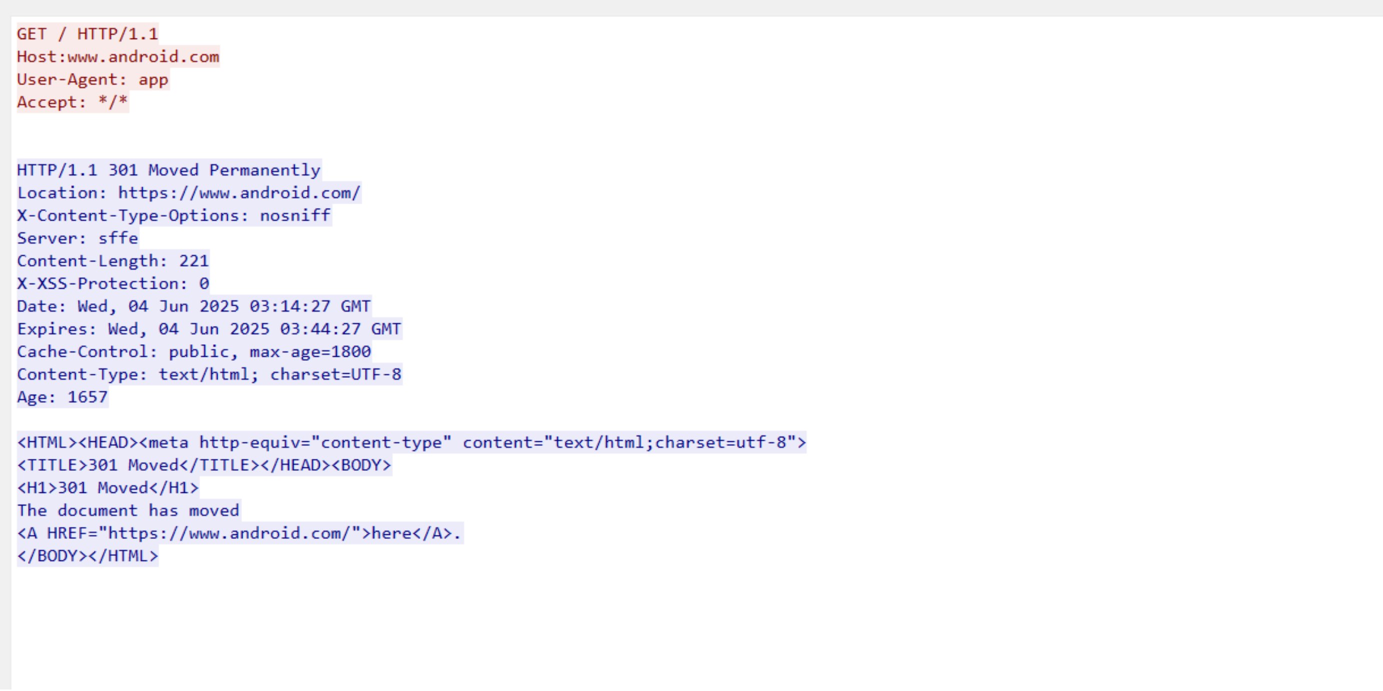
## 2- Packet Logging with tcpdump

عاوزين بقي ان احنا نحاول نشوف traffic فمحتاجين بقي نخلي emulator يشتغل وناخد traffic نخزنها في file

```
emulator -tcpdump emulator.cap -avd Pixel_9_API_30
```



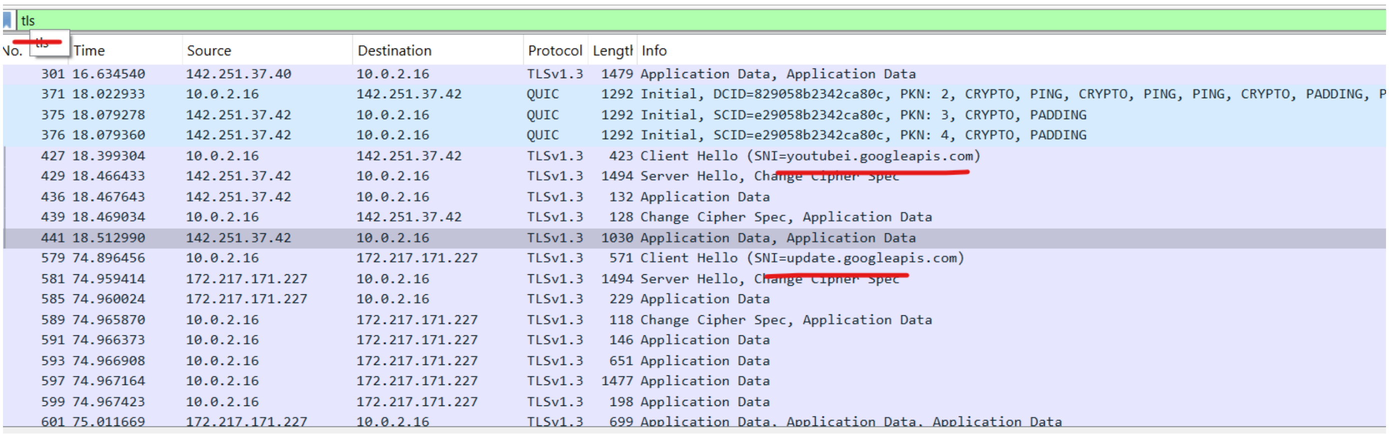
```
tcp.stream eq 10
No.  Time       Source          Destination     Protocol Length Info
506 47.543467  10.0.2.16       142.251.37.174  TCP       74 48198 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=4039025075 TSecr=0 WS=64
507 47.587241  142.251.37.174  10.0.2.16       TCP       58 80 → 48198 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
508 47.587925  10.0.2.16       142.251.37.174  TCP       54 48198 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
509 47.591142  10.0.2.16       142.251.37.174  HTTP     124 GET / HTTP/1.1
510 47.591270  142.251.37.174  10.0.2.16       TCP       54 80 → 48198 [ACK] Seq=1 Ack=71 Win=8760 Len=0
511 47.635185  142.251.37.174  10.0.2.16       HTTP     599 HTTP/1.1 301 Moved Permanently  (text/html)
512 47.635627  10.0.2.16       142.251.37.174  TCP       54 48198 → 80 [ACK] Seq=71 Ack=546 Win=65535 Len=0
```



```
GET / HTTP/1.1
Host:www.android.com
User-Agent: app
Accept: */*


HTTP/1.1 301 Moved Permanently
Location: https://www.android.com/
X-Content-Type-Options: nosniff
Server: sffe
Content-Length: 221
X-XSS-Protection: 0
Date: Wed, 04 Jun 2025 03:14:27 GMT
Expires: Wed, 04 Jun 2025 03:44:27 GMT
Cache-Control: public, max-age=1800
Content-Type: text/html; charset=UTF-8
Age: 1657

<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="https://www.android.com/">here</A>.
</BODY></HTML>
```

كده ممكن نعرف ايه هي التطبيقات اللي بيستخدم http

برده لو عاوزين نعرف ايه التطبيقات اللي متتواصل مع domain معينة او مواقع معينة : هلناقيهم بيستخدمو https بس ممكن نعرف ايه هو domain اللي بيتواصلو معاه



```
tls
No.  Time       Source           Destination      Protocol Length Info
301 16.634540  142.251.37.40    10.0.2.16        TLSv1.3  1479 Application Data, Application Data
371 18.022933  10.0.2.16        142.251.37.42    QUIC     1292 Initial, DCID=829058b2342ca80c, PKN: 2, CRYPTO, PING, CRYPTO, PING, PING, CRYPTO, PADDING, P
375 18.079278  142.251.37.42    10.0.2.16        QUIC     1292 Initial, SCID=e29058b2342ca80c, PKN: 3, CRYPTO, PADDING
376 18.079360  142.251.37.42    10.0.2.16        QUIC     1292 Initial, SCID=e29058b2342ca80c, PKN: 4, CRYPTO, PADDING
427 18.399304  10.0.2.16        142.251.37.42    TLSv1.3   423 Client Hello (SNI=youtubei.googleapis.com)
429 18.466433  142.251.37.42    10.0.2.16        TLSv1.3  1494 Server Hello, Change Cipher Spec
436 18.467643  142.251.37.42    10.0.2.16        TLSv1.3   132 Application Data
439 18.469034  10.0.2.16        142.251.37.42    TLSv1.3   128 Change Cipher Spec, Application Data
441 18.512990  142.251.37.42    10.0.2.16        TLSv1.3  1030 Application Data, Application Data
579 74.896456  10.0.2.16        172.217.171.227  TLSv1.3   571 Client Hello (SNI=update.googleapis.com)
581 74.959414  172.217.171.227  10.0.2.16        TLSv1.3  1494 Server Hello, Change Cipher Spec
585 74.960024  172.217.171.227  10.0.2.16        TLSv1.3   229 Application Data
589 74.965870  10.0.2.16        172.217.171.227  TLSv1.3   118 Change Cipher Spec, Application Data
591 74.966373  10.0.2.16        172.217.171.227  TLSv1.3   146 Application Data
593 74.966908  10.0.2.16        172.217.171.227  TLSv1.3   651 Application Data
597 74.967164  10.0.2.16        172.217.171.227  TLSv1.3  1477 Application Data
599 74.967423  10.0.2.16        172.217.171.227  TLSv1.3   198 Application Data
601 75.011669  172.217.171.227  10.0.2.16        TLSv1.3   699 Application Data, Application Data, Application Data
```

## Flag  Analyze the PocketHexMap HTTP traffic

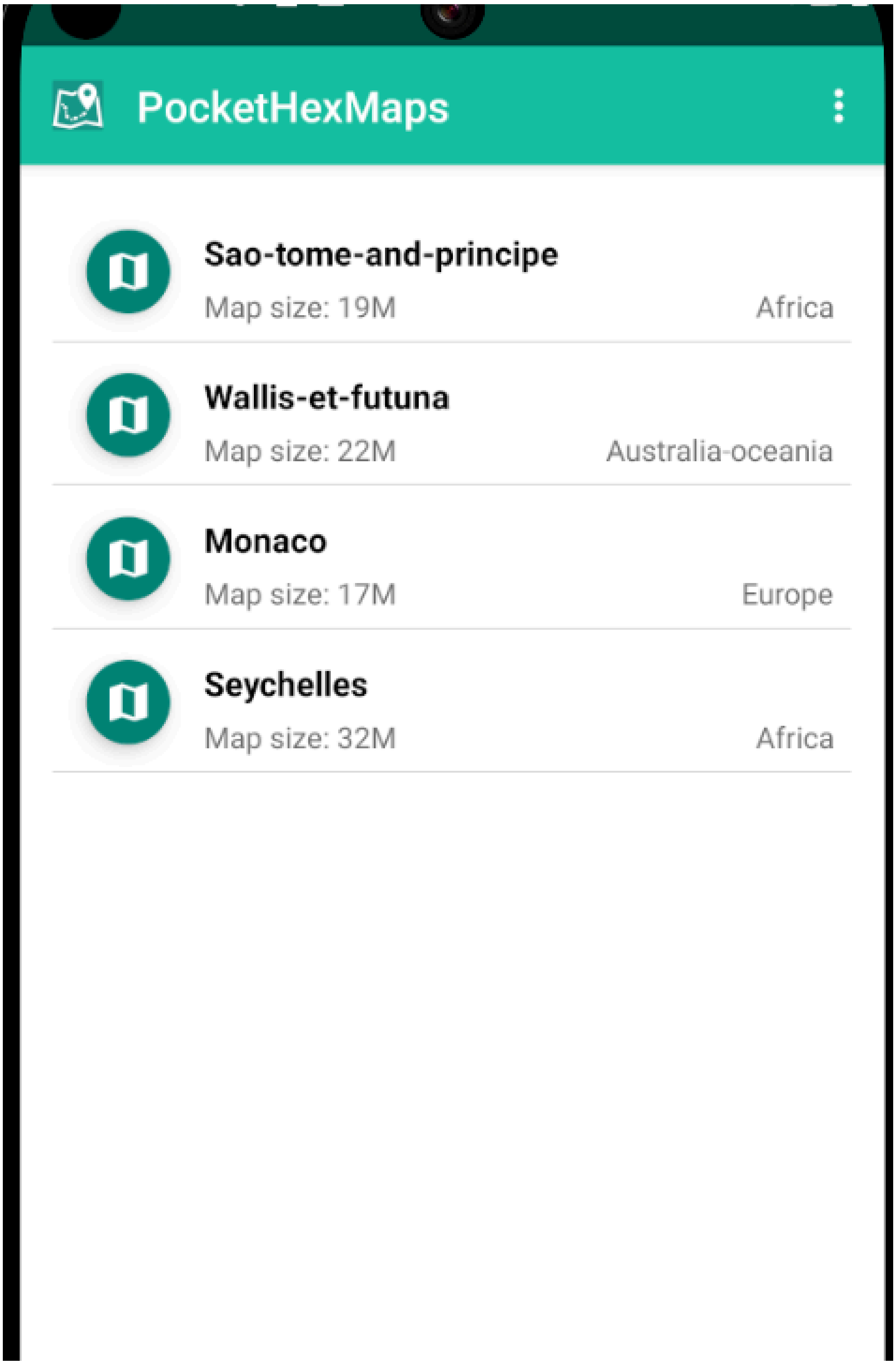
دلوقتي بقي علشان capture traffic لازم ان نشغل emulator ونستخدم tcpdump-

```
emulator -tcpdump catprue.cap @device
```

### open file with wireshark

لو جينا بقي خلينا filter=http علشنا نشوف ايه التطبيقات اللي بيتسخدم http هنلاقي ان التطبيق اللي نزلناه بيستخدم http

app

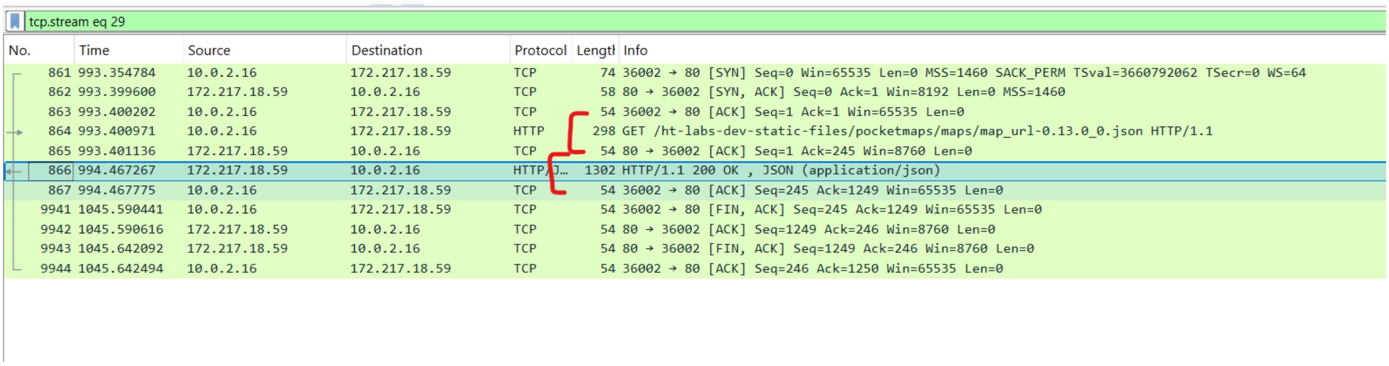


Sao-tome-and-principe
Map size: 19M Africa

Wallis-et-futuna
Map size: 22M Australia-oceania

Monaco
Map size: 17M Europe

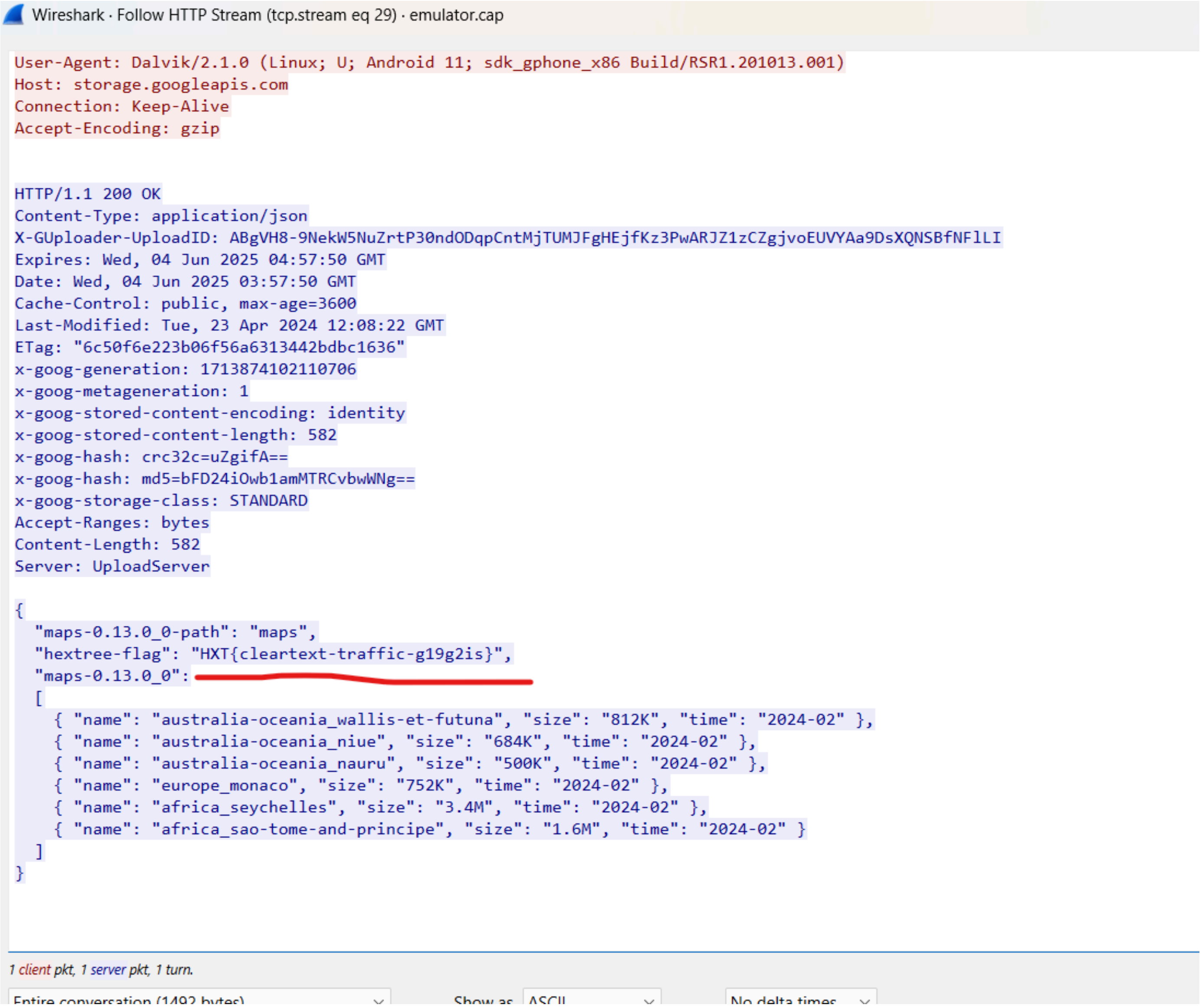
Seychelles
Map size: 32M Africa



```
tcp.stream eq 29
No.   Time         Source         Destination    Protocol Lengtl Info
 861 993.354784   10.0.2.16      172.217.18.59  TCP        74 36002 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=3660792062 TSecr=0 WS=64
 862 993.399600   172.217.18.59  10.0.2.16      TCP        58 80 → 36002 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
 863 993.400202   10.0.2.16      172.217.18.59  TCP        54 36002 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
 864 993.400971   10.0.2.16      172.217.18.59  HTTP      298 GET /ht-labs-dev-static-files/pocketmaps/maps/map_url-0.13.0_0.json HTTP/1.1
 865 993.401136   172.217.18.59  10.0.2.16      TCP        54 80 → 36002 [ACK] Seq=1 Ack=245 Win=8760 Len=0
 866 994.467267   172.217.18.59  10.0.2.16      HTTP/J…  1302 HTTP/1.1 200 OK , JSON (application/json)
 867 994.467775   10.0.2.16      172.217.18.59  TCP        54 36002 → 80 [ACK] Seq=245 Ack=1249 Win=65535 Len=0
9941 1045.590441  10.0.2.16      172.217.18.59  TCP        54 36002 → 80 [FIN, ACK] Seq=245 Ack=1249 Win=65535 Len=0
9942 1045.590616  172.217.18.59  10.0.2.16      TCP        54 80 → 36002 [ACK] Seq=1249 Ack=246 Win=8760 Len=0
9943 1045.642092  172.217.18.59  10.0.2.16      TCP        54 80 → 36002 [FIN, ACK] Seq=1249 Ack=246 Win=8760 Len=0
9944 1045.642494  10.0.2.16      172.217.18.59  TCP        54 36002 → 80 [ACK] Seq=246 Ack=1250 Win=65535 Len=0
```

لو عملنا follow  stream http stream

## flag is HXT{cleartext-traffic-g19g2is}



Wireshark · Follow HTTP Stream (tcp.stream eq 29) · emulator.cap

```
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; sdk_gphone_x86 Build/RSR1.201013.001)
Host: storage.googleapis.com
Connection: Keep-Alive
Accept-Encoding: gzip


HTTP/1.1 200 OK
Content-Type: application/json
X-GUploader-UploadID: ABgVH8-9NekW5NuZrtP30ndODqpCntMjTUMJFgHEjfKz3PwARJZ1zCZgjvoEUVYAa9DsXQNSBfNFlLI
Expires: Wed, 04 Jun 2025 04:57:50 GMT
Date: Wed, 04 Jun 2025 03:57:50 GMT
Cache-Control: public, max-age=3600
Last-Modified: Tue, 23 Apr 2024 12:08:22 GMT
ETag: "6c50f6e223b06f56a6313442bdbc1636"
x-goog-generation: 1713874102110706
x-goog-metageneration: 1
x-goog-stored-content-encoding: identity
x-goog-stored-content-length: 582
x-goog-hash: crc32c=uZgifA==
x-goog-hash: md5=bFD24iOwb1amMTRCvbwWNg==
x-goog-storage-class: STANDARD
Accept-Ranges: bytes
Content-Length: 582
Server: UploadServer

{
  "maps-0.13.0_0-path": "maps",
  "hextree-flag": "HXT{cleartext-traffic-g19g2is}",
  "maps-0.13.0_0":
  [
    { "name": "australia-oceania_wallis-et-futuna", "size": "812K", "time": "2024-02" },
    { "name": "australia-oceania_niue", "size": "684K", "time": "2024-02" },
    { "name": "australia-oceania_nauru", "size": "500K", "time": "2024-02" },
    { "name": "europe_monaco", "size": "752K", "time": "2024-02" },
    { "name": "africa_seychelles", "size": "3.4M", "time": "2024-02" },
    { "name": "africa_sao-tome-and-principe", "size": "1.6M", "time": "2024-02" }
  ]
}
```

1 client pkt, 1 server pkt, 1 turn.

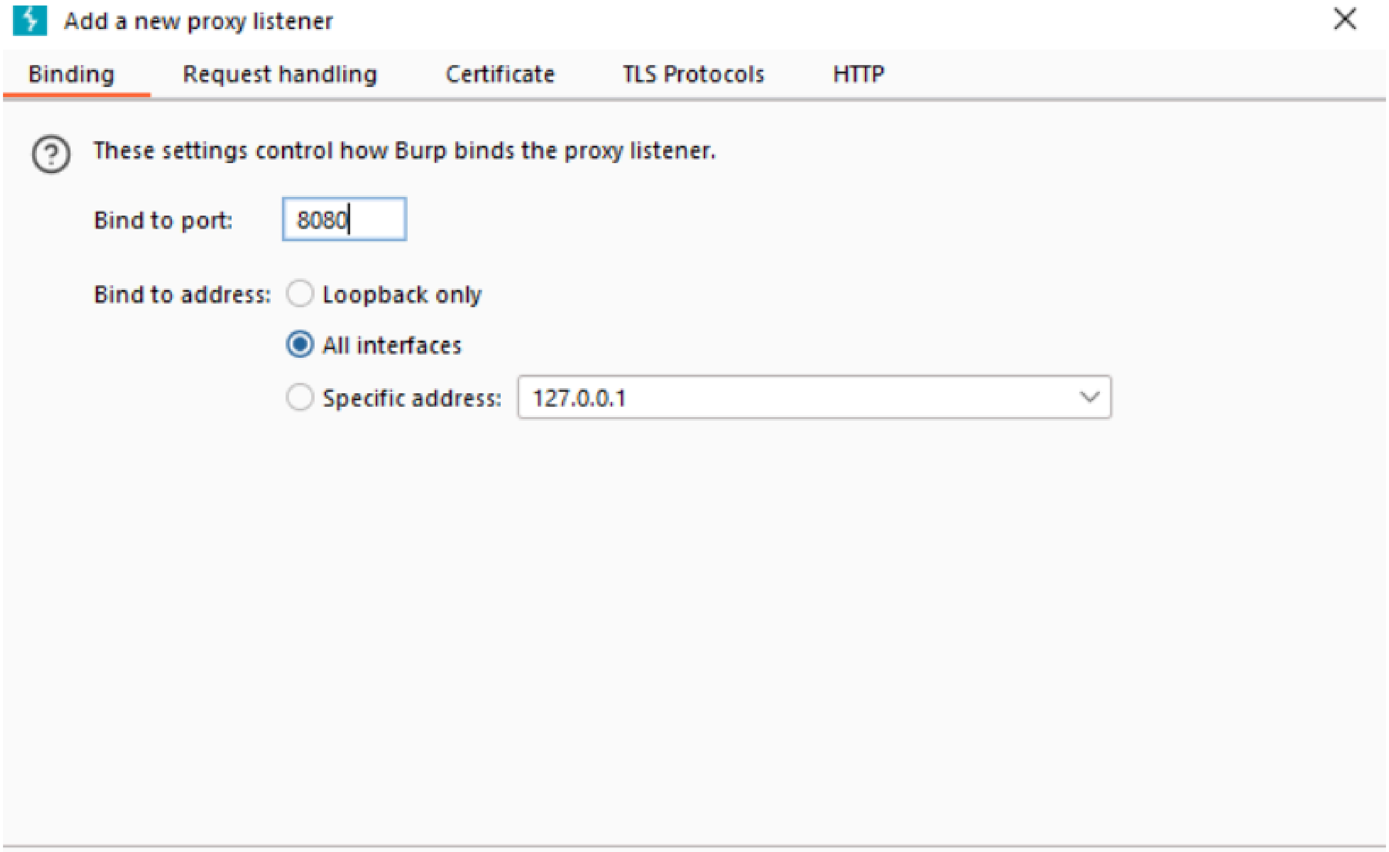
How to connect burpsuite to emulator

1- install burpsuite

## 1. Setup the Burp Suite Proxy

1. **Start Burp Suite**:

   - Launch Burp Suite and go to **Proxy > Options**.
   - Note the **Proxy Listener** details, typically set to `127.0.0.1:8080`.
2. **Bind to All Interfaces**:
   - To allow connections from the emulator, click **Edit** in the Proxy Listeners.
   - Select **"Bind to address > All interfaces"**, and click **OK**.



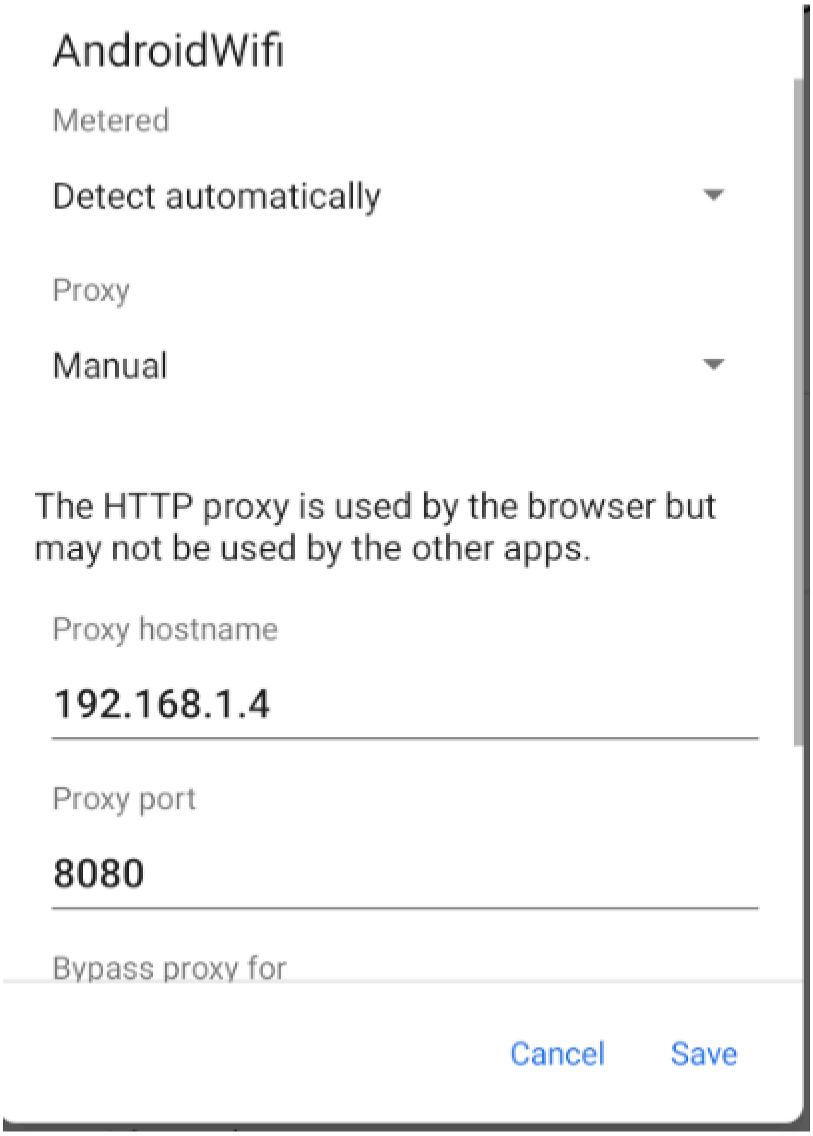
These settings control how Burp binds the proxy listener.

Bind to port: 8080

Bind to address: ○ Loopback only
● All interfaces
○ Specific address: 127.0.0.1

## 2. Configure the Android Emulator

1. **Access Emulator Settings**:
   - Open the emulator.
   - Navigate to **Settings > Network & Internet > Wi-Fi**.
2. **Set Up the Proxy**:
   - Long-press the active Wi-Fi network and select **Modify Network**.
   - Enable **Show advanced options**.
   - Under **Proxy**, select **Manual**:
     - **Proxy hostname**: The IP address of your host machine running Burp Suite.
     - **Proxy port**: `8080` (or the port set in Burp Suite).



AndroidWifi

Metered

Detect automatically

Proxy

Manual

The HTTP proxy is used by the browser but may not be used by the other apps.

Proxy hostname

192.168.1.4

Proxy port

8080

Bypass proxy for

دلوقتي هو بيعمل intercept http traffic only لازم بقي ننزل certificate

### 3. Install the Burp Certificate

1. **Export the Certificate**:
   - In Burp Suite, go to **Proxy > Options > Import / Export CA Certificate**.
   - Export the certificate in **DER format** (e.g., `burp_cert.cer`).
2. **Transfer the Certificate to the Emulator**:
   - Drag and drop the `burp_cert.cer` file onto the emulator screen.
   - Alternatively, use `adb`:

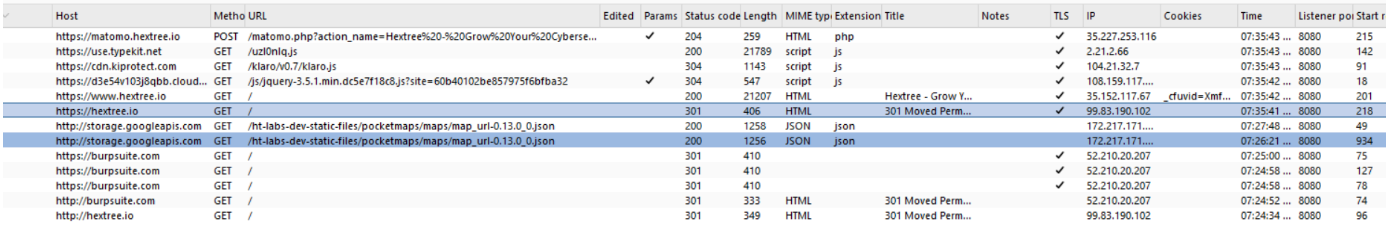
     bash

     CopyEdit

     ```
     adb push burp_cert.cer /sdcard/Download/
     ```
3. **Install the Certificate**:
   - Open **Settings > Security > Encryption & credentials > Install a certificate > CA certificate**.
   - Select the `burp_cert.cer` file from the **Download** folder.

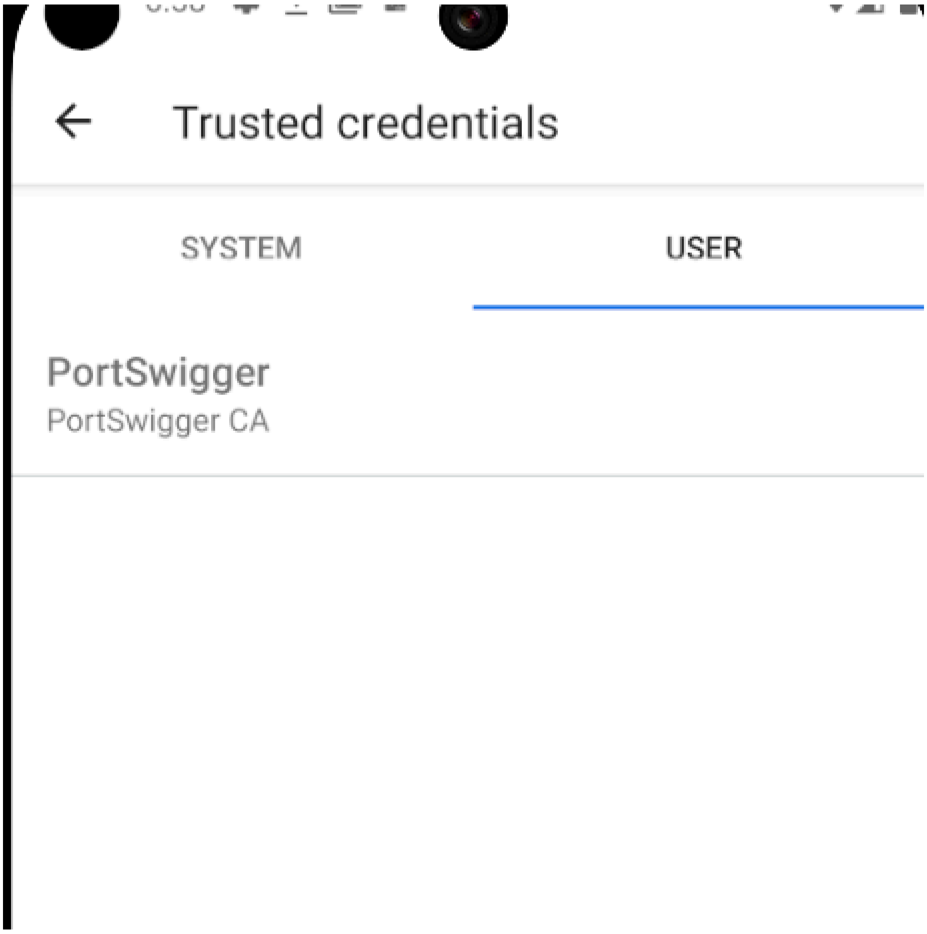
- Confirm the installation.

### search for any https website like hextree.io and so the burp history



| | Host | Metho | URL | Edited | Params | Status code | Length | MIME typ | Extension | Title | Notes | TLS | IP | Cookies | Time | Listener po | Start r |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | https://matomo.hextree.io | POST | /matomo.php?action_name=Hextree%20-%20Grow%20Your%20Cyberse... | | ✓ | 204 | 259 | HTML | php | | | ✓ | 35.227.253.116 | | 07:35:43 ... | 8080 | 215 |
| | https://use.typekit.net | GET | /uzl0nlq.js | | | 200 | 21789 | script | js | | | ✓ | 2.21.2.66 | | 07:35:43 ... | 8080 | 142 |
| | https://cdn.kiprotect.com | GET | /klaro/v0.7/klaro.js | | | 304 | 1143 | script | js | | | ✓ | 104.21.32.7 | | 07:35:43 ... | 8080 | 91 |
| | https://d3e54v103j8qbb.cloud... | GET | /js/jquery-3.5.1.min.dc5e7f18c8.js?site=60b40102be857975f6bfba32 | | ✓ | 304 | 547 | script | js | | | ✓ | 108.159.117.... | | 07:35:42 ... | 8080 | 18 |
| | https://www.hextree.io | GET | / | | | 200 | 21207 | HTML | | Hextree - Grow Y... | | ✓ | 35.152.117.67 | _cfuvid=Xmf... | 07:35:42 ... | 8080 | 201 |
| | https://hextree.io | GET | / | | | 301 | 406 | HTML | | 301 Moved Perm... | | ✓ | 99.83.190.102 | | 07:35:41 ... | 8080 | 218 |
| | http://storage.googleapis.com | GET | /ht-labs-dev-static-files/pocketmaps/maps/map_url-0.13.0_0.json | | | 200 | 1258 | JSON | json | | | | 172.217.171.... | | 07:27:48 ... | 8080 | 49 |
| | http://storage.googleapis.com | GET | /ht-labs-dev-static-files/pocketmaps/maps/map_url-0.13.0_0.json | | | 200 | 1256 | JSON | json | | | | 172.217.171.... | | 07:26:21 ... | 8080 | 934 |
| | https://burpsuite.com | GET | / | | | 301 | 410 | | | | | ✓ | 52.210.20.207 | | 07:25:00 ... | 8080 | 75 |
| | https://burpsuite.com | GET | / | | | 301 | 410 | | | | | ✓ | 52.210.20.207 | | 07:24:58 ... | 8080 | 127 |
| | https://burpsuite.com | GET | / | | | 301 | 410 | | | | | ✓ | 52.210.20.207 | | 07:24:58 ... | 8080 | 78 |
| | http://burpsuite.com | GET | / | | | 301 | 333 | HTML | | 301 Moved Perm... | | | 52.210.20.207 | | 07:24:52 ... | 8080 | 74 |
| | http://hextree.io | GET | / | | | 301 | 349 | HTML | | 301 Moved Perm... | | | 99.83.190.102 | | 07:24:34 ... | 8080 | 96 |

دلوقتي بقي لو جينا نشوف اي تطبيق مثبت بيستخدم https مش هنعرف نعترضه ده في 2 options من الثقة هو SYSTEM , USER ده يعني ان system بيبقي ليه certificate و user بيبقي ليه certificate وان لما بنزل burpsuite certifcate دي بتبقي تبع user مش system



Trusted credentials

SYSTEM USER

PortSwigger
PortSwigger CA

من android 6 كان بيثق في certificates بتاعت system, user ولكن من بعد android 6 بقي بيثق في certificate بتاعت system بس علشان كده لما نيجي intercept اي تطبيق مثبت بيستخدم https مش هنعرف نعترضه

ولكن في chrome ممكن عادي نعترض https or http علشان chrome بيثق في system user

## Installing Certificate in System Store burpsuite بس تبقي تبع system هنزل شهادة

in adb shell the path of system certificate is `/system/etc/security/cacerts` path of user certificates is : `/data/misc/user/0/cacerts-added/`

```
generic_x86_arm:/ $ ls -lah /system/etc/security/cacerts
total 520K
drwxr-xr-x 2 root root 4.0K 2009-01-01 02:00 .
drwxr-xr-x 5 root root 4.0K 2009-01-01 02:00 ..
-rw-r--r-- 1 root root 4.6K 2009-01-01 02:00 00673b5b.0
-rw-r--r-- 1 root root 2.8K 2009-01-01 02:00 04f60c28.0
-rw-r--r-- 1 root root 2.2K 2009-01-01 02:00 0d69c7e1.0
-rw-r--r-- 1 root root 4.5K 2009-01-01 02:00 10531352.0
-rw-r--r-- 1 root root 4.6K 2009-01-01 02:00 111e6273.0
-rw-r--r-- 1 root root 4.2K 2009-01-01 02:00 12d55845.0
```

بس هنلاقي ان هما كلهم بعمولين root user فلازم نبقي root

get root on emulator

1- download rootavd ( tool for get root access ) [https://gitlab.com/newbit/rootAVD](https://gitlab.com/newbit/rootAVD)

2- go the directory of rootavd and open cmd and run tool.bat on windows and .sh on linux

```
PS C:\Users\Dell\Downloads\rootAVD-master (1)\rootAVD-master> .\rootAVD.bat
ListAllAVDS

rootAVD.bat system-images\android-
35\google_apis_playstore\x86_64\ramdisk.img
rootAVD.bat system-images\android-
35\google_apis_playstore\x86_64\ramdisk.img FAKEBOOTIMG
rootAVD.bat system-images\android-
35\google_apis_playstore\x86_64\ramdisk.img DEBUG PATCHFSTAB GetUSBHPmodZ
rootAVD.bat system-images\android-
35\google_apis_playstore\x86_64\ramdisk.img restore
rootAVD.bat system-images\android-
35\google_apis_playstore\x86_64\ramdisk.img InstallKernelModules
rootAVD.bat system-images\android-
35\google_apis_playstore\x86_64\ramdisk.img InstallPrebuiltKernelModules
rootAVD.bat system-images\android-
35\google_apis_playstore\x86_64\ramdisk.img InstallPrebuiltKernelModules
GetUSBHPmodZ PATCHFSTAB DEBUG

rootAVD.bat system-images\android-30\google_apis_playstore\x86\ramdisk.img
rootAVD.bat system-images\android-30\google_apis_playstore\x86\ramdisk.img
FAKEBOOTIMG
rootAVD.bat system-images\android-30\google_apis_playstore\x86\ramdisk.img
```

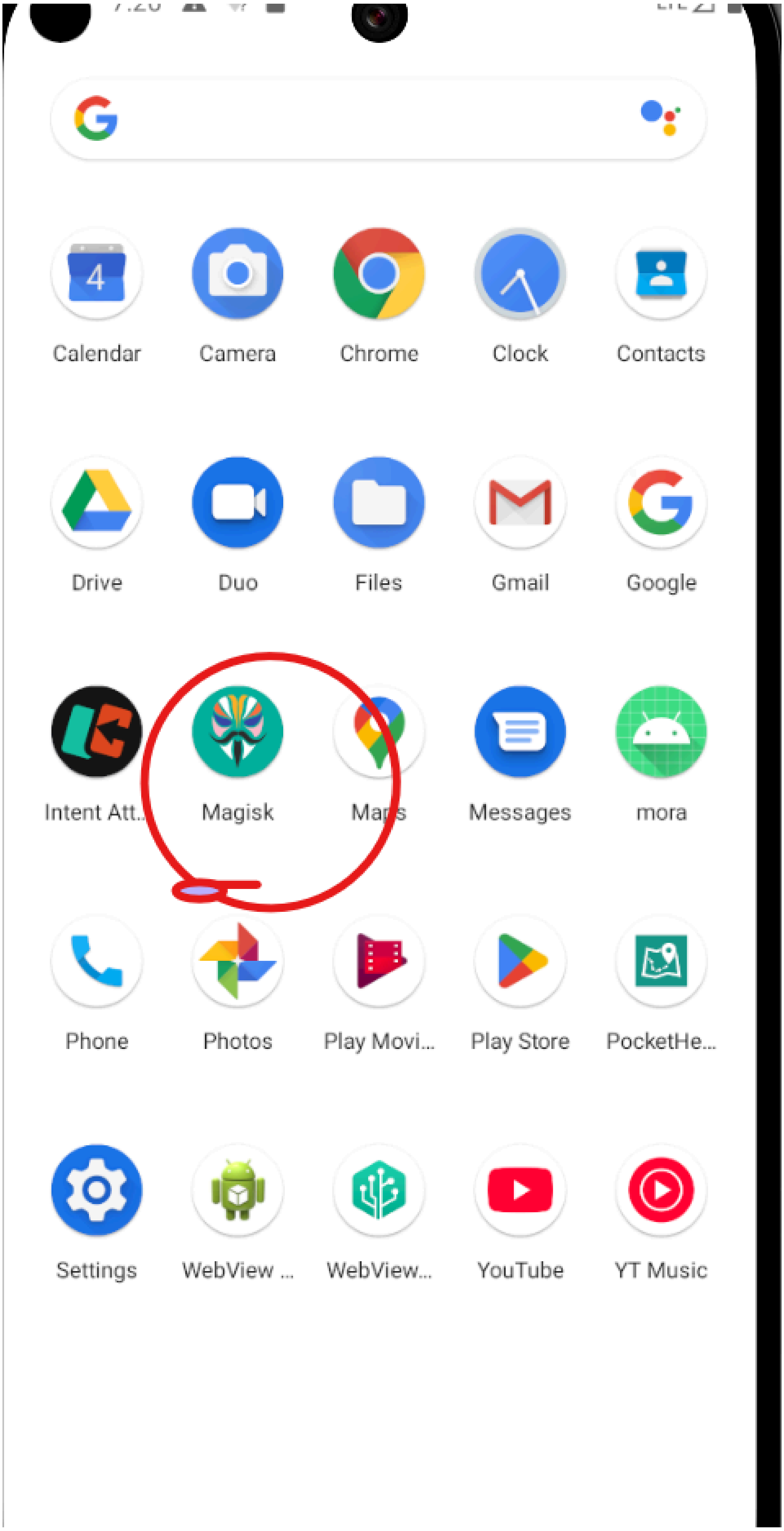
```
DEBUG PATCHFSTAB GetUSBHPmodZ
rootAVD.bat system-images\android-30\google_apis_playstore\x86\ramdisk.img
restore
rootAVD.bat system-images\android-30\google_apis_playstore\x86\ramdisk.img
InstallKernelModules
rootAVD.bat system-images\android-30\google_apis_playstore\x86\ramdisk.img
InstallPrebuiltKernelModules
rootAVD.bat system-images\android-30\google_apis_playstore\x86\ramdisk.img
InstallPrebuiltKernelModules GetUSBHPmodZ PATCHFSTAB DEBUG
```

According to the type of android  like android-30 or android-35 choose the same type of the device running

```
rootAVD.bat system-images\android-30\google_apis_playstore\x86\ramdisk.img

choose 1
```

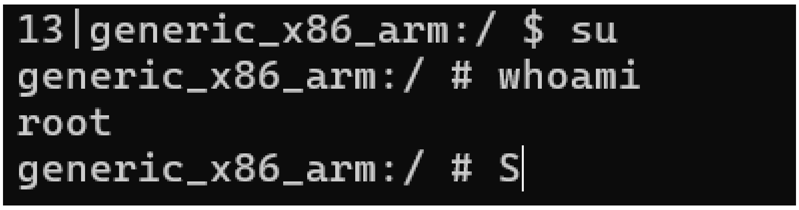
restart the device

Magisk is installed



open the app and click ok for message

after reboot, open the app and open adb ( run : su )  the message will appear click grant and will became the root



```
13|generic_x86_arm:/ $ su
generic_x86_arm:/ # whoami
root
generic_x86_arm:/ # S
```

دلوقتي بعد ما بقينا root عاوين بقي ننقل burpsuite certificate from user to system

```
1|generic_x86_arm:/ # cp  /data/misc/user/0/cacerts-added/9a5ba575.0
/system/etc/security/cacerts
cp: /system/etc/security/cacerts/9a5ba575.0: Read-only file system
1|generic_x86_arm:/ #
```

مش هيمح علشان هو read only علشان كده هناخد كل certificate in system ونحطها عند user

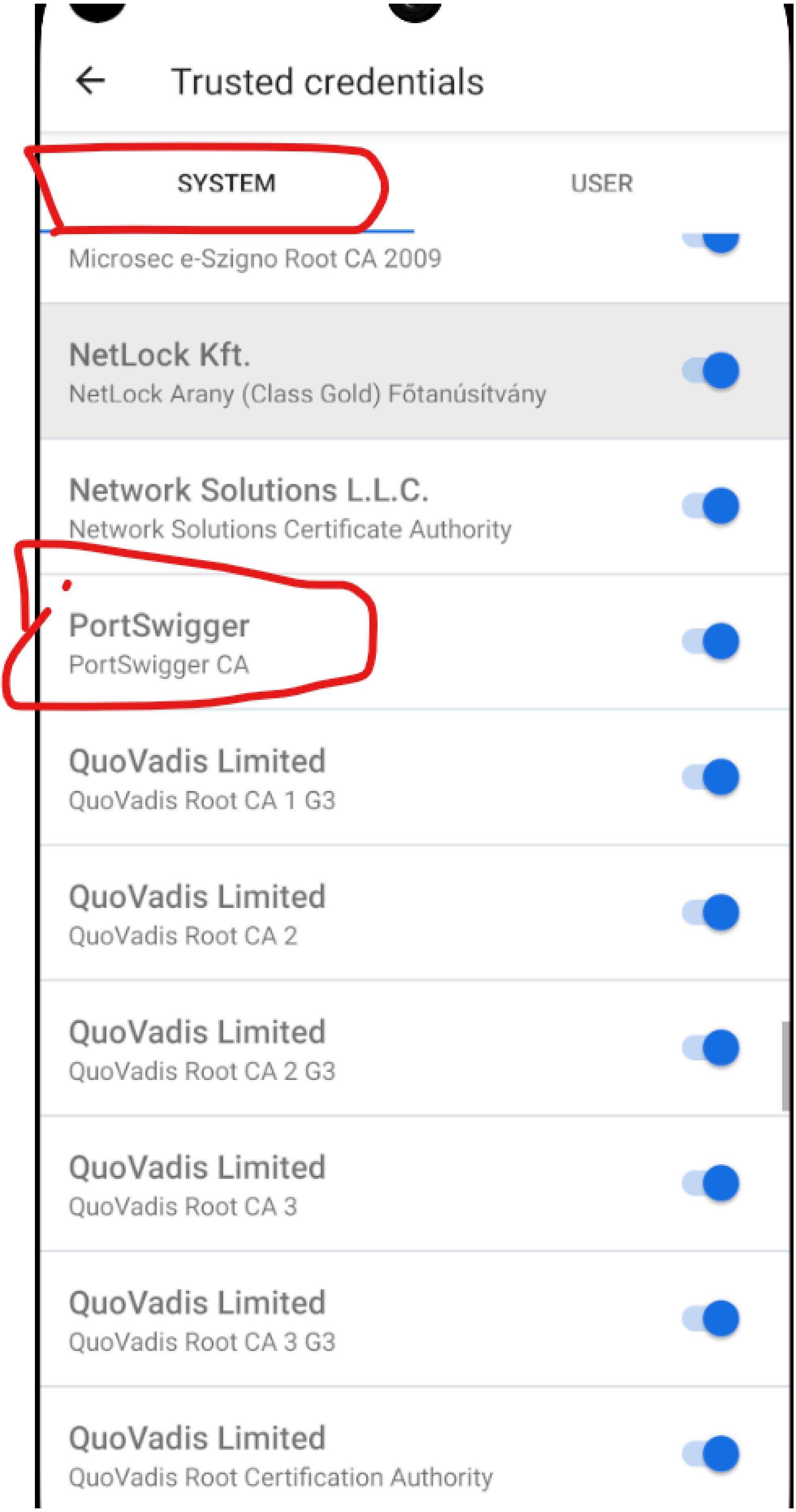
```
1|generic_x86_arm:/ #  cp /system/etc/security/cacerts/*
/data/misc/user/0/cacerts-added/
```

set /system/etc/secuity/cacerts/ to temporary file

```
generic_x86_arm:/ # mount -t tmpfs tmpfs /system/etc/security/cacerts
```

cp all cert in user to system

```
generic_x86_arm:/ # cp /data/misc/user/0/cacerts-added/*
/system/etc/security/cacerts/
```



Trusted credentials

SYSTEM USER

Microsec e-Szigno Root CA 2009

NetLock Kft.
NetLock Arany (Class Gold) Főtanúsítvány

Network Solutions L.L.C.
Network Solutions Certificate Authority

PortSwigger
PortSwigger CA

QuoVadis Limited
QuoVadis Root CA 1 G3

QuoVadis Limited
QuoVadis Root CA 2

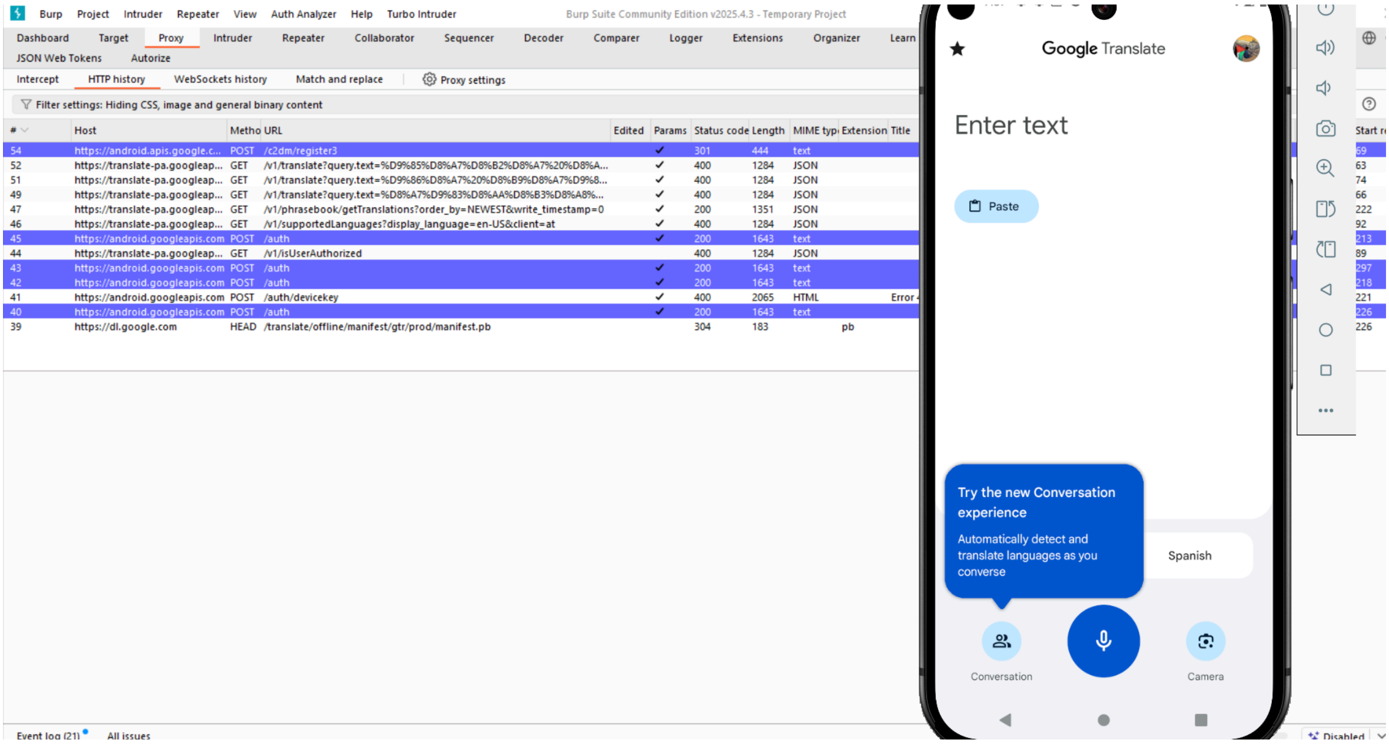
QuoVadis Limited
QuoVadis Root CA 2 G3

QuoVadis Limited
QuoVadis Root CA 3

QuoVadis Limited
QuoVadis Root CA 3 G3

QuoVadis Limited
QuoVadis Root Certification Authority

هنا اهو بقي اول ما افتح اي app هيظهر عادي في burpsuite



Filter settings: Hiding CSS, image and general binary content

| # | Host | Metho | URL | Edited | Params | Status code | Length | MIME typ | Extension | Title | Start r |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 54 | https://android.apis.google.c... | POST | /c2dm/register3 | | ✓ | 301 | 444 | text | | | 69 |
| 52 | https://translate-pa.googleap... | GET | /v1/translate?query.text=%D9%85%D8%A7%D8%B2%D8%A7%20%D8%A... | | ✓ | 400 | 1284 | JSON | | | 63 |
| 51 | https://translate-pa.googleap... | GET | /v1/translate?query.text=%D9%86%D8%A7%20%D8%B9%D8%A7%D9%8... | | ✓ | 400 | 1284 | JSON | | | 74 |
| 49 | https://translate-pa.googleap... | GET | /v1/translate?query.text=%D8%A7%D9%83%D8%AA%D8%B3%D8%A8%... | | ✓ | 400 | 1284 | JSON | | | 66 |
| 47 | https://translate-pa.googleap... | GET | /v1/phrasebook/getTranslations?order_by=NEWEST&write_timestamp=0 | | ✓ | 200 | 1351 | JSON | | | 222 |
| 46 | https://translate-pa.googleap... | GET | /v1/supportedLanguages?display_language=en-US&client=at | | ✓ | 400 | 1284 | JSON | | | 92 |
| 45 | https://android.googleapis.com | POST | /auth | | ✓ | 200 | 1643 | text | | | 213 |
| 44 | https://translate-pa.googleap... | GET | /v1/isUserAuthorized | | | 400 | 1284 | JSON | | | 89 |
| 43 | https://android.googleapis.com | POST | /auth | | ✓ | 200 | 1643 | text | | | 297 |
| 42 | https://android.googleapis.com | POST | /auth | | ✓ | 200 | 1643 | text | | | 218 |
| 41 | https://android.googleapis.com | POST | /auth/devicekey | | ✓ | 400 | 2065 | HTML | | Error | 221 |
| 40 | https://android.googleapis.com | POST | /auth | | ✓ | 200 | 1643 | text | | | 226 |
| 39 | https://dl.google.com | HEAD | /translate/offline/manifest/gtr/prod/manifest.pb | | | 304 | 183 | | pb | | 226 |

Try the new Conversation experience

Automatically detect and translate languages as you converse

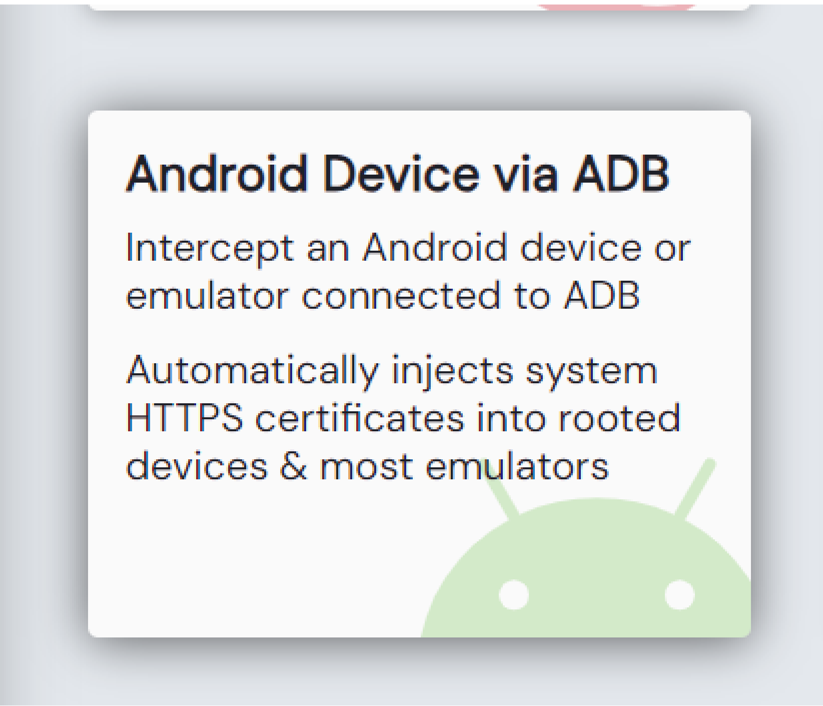
## HTTP Toolkit

**HTTP Toolkit** is a developer tool used for intercepting, debugging, and testing HTTP and HTTPS traffic. It provides an easy-to-use interface for capturing and analyzing HTTP requests and responses between a client (like a browser, app, or API client) and a server.

دي tool زي burpsuite كده بس احسن منها لو هنستخدمها android

download from here : https://httptoolkit.com/download/win-exe/

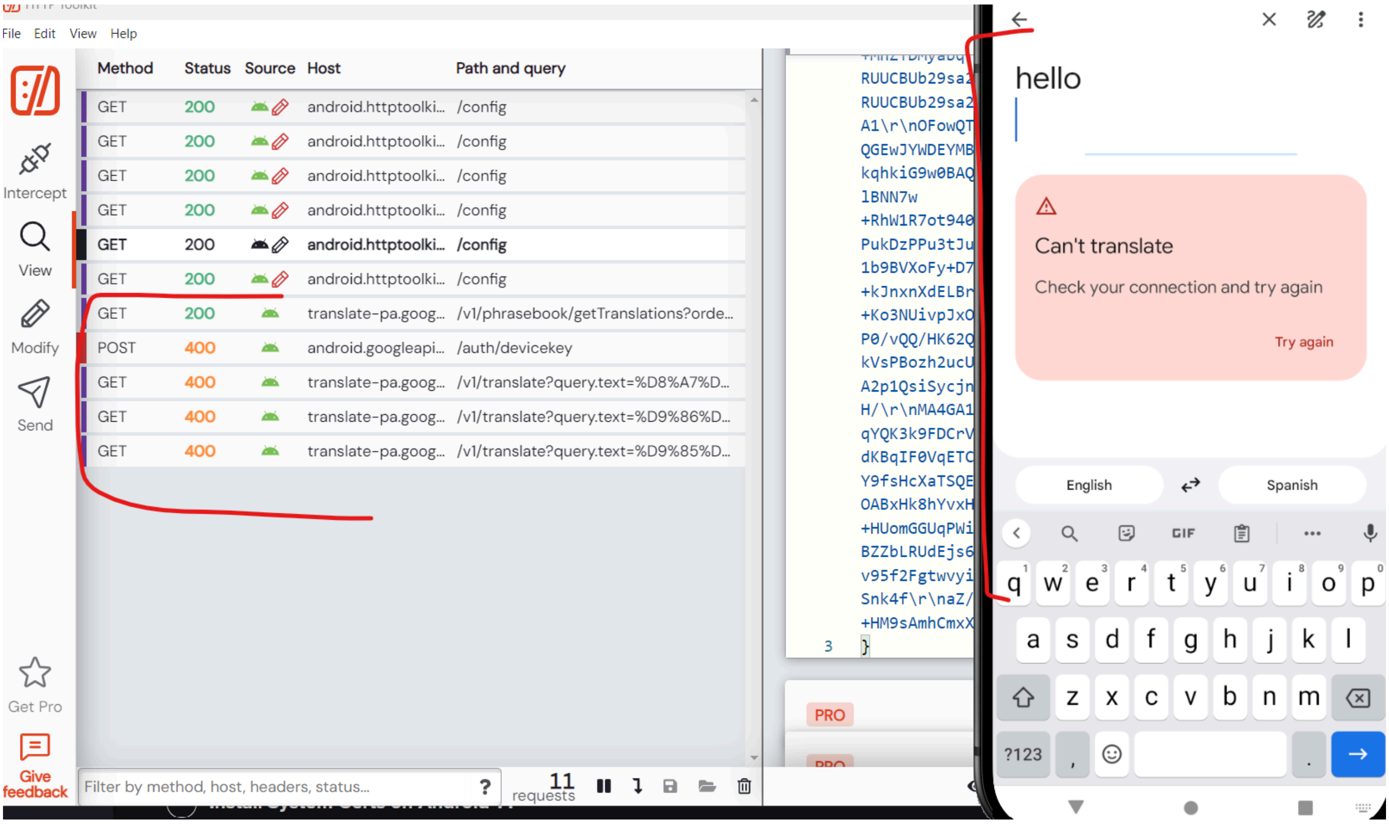
choose Android Device via ADB



### Android Device via ADB

Intercept an Android device or emulator connected to ADB

Automatically injects system HTTPS certificates into rooted devices & most emulators



| Method | Status | Source | Host | Path and query |
|---|---|---|---|---|
| GET | 200 | | android.httptoolki... | /config |
| GET | 200 | | android.httptoolki... | /config |
| GET | 200 | | android.httptoolki... | /config |
| GET | 200 | | android.httptoolki... | /config |
| GET | 200 | | android.httptoolki... | /config |
| GET | 200 | | android.httptoolki... | /config |
| GET | 200 | | translate-pa.goog... | /v1/phrasebook/getTranslations?orde... |
| POST | 400 | | android.googleapi... | /auth/devicekey |
| GET | 400 | | translate-pa.goog... | /v1/translate?query.text=%D8%A7%D... |
| GET | 400 | | translate-pa.goog... | /v1/translate?query.text=%D9%86%D... |
| GET | 400 | | translate-pa.goog... | /v1/translate?query.text=%D9%85%D... |

Filter by method, host, headers, status...

11 requests

RUUCBUb29sa2
RUUCBUb29sa2
A1\r\nOFowQT
QGEwJYWDEYMB
kqhkiG9w0BAQ
lBNN7w
+RhW1R7ot940
PukDzPPu3tJu
1b9BVXoFy+D7
+kJnxnXdELBr
+Ko3NUivpJxO
P0/vQQ/HK62Q
kVsPBozh2ucU
A2p1QsiSycjn
H/\r\nMA4GA1
qYQK3k9FDCrV
dKBqIF0VqETC
Y9fsHcXaTSQE
OABxHk8hYvxH
+HUomGGUqPWi
BZZbLRUdEjs6
v95f2Fgtwvyi
Snk4f\r\naZ/
+HM9sAmhCmxX
}

hello

Can't translate

Check your connection and try again

ممكن برضه لو عاوزين نخليه يستخدم certificate بتاعت user فكده احنا محاجين نعدل app ونضيف فيه user

Steps for config any app to use user certificate

1- decompile the app by appktool

2- change the configration to use user certificate and system certificate

3- build the app

4- sign app

```
# unpack the target .apk
apktool d translate.apk

# modify the AndroidManifest.xml to add a networkSecurityConfig
# create a permissive xml/network_security_config.xml
cd translate

# repackage the .apk
apktool b

# ensure the .apk is zipaligned
[...]/build-tools/34.0.0/zipalign -p -f -v 4 ./dist/translate.apk
```

```
translate2.apk

# create a keystore to sign the apk
keytool -genkey -v -keystore research.keystore -alias research_key -keyalg
RSA -keysize 2048 -validity 10000

# sign the apk with apksigner
[...]/build-tools/34.0.0/apksigner sign --ks ./research.keystore
./translate2.apk
```

for network_security_config.xml

1- add in AndroidMeniFast.xml

```
android:networkSecurityConfig="@xml/network_security_config"
```

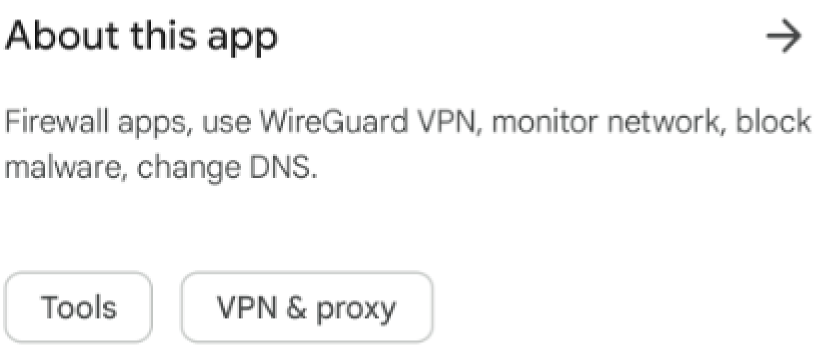
2- network_securiyt_config

```
<network-security-config>
    <base-config>
        <trust-anchors>
            <certificates src="user"/>
            <certificates src="system"/>
        </trust-anchors>
    </base-config>
</network-security-config>
```

## Advanced HTTP Interception with VPN

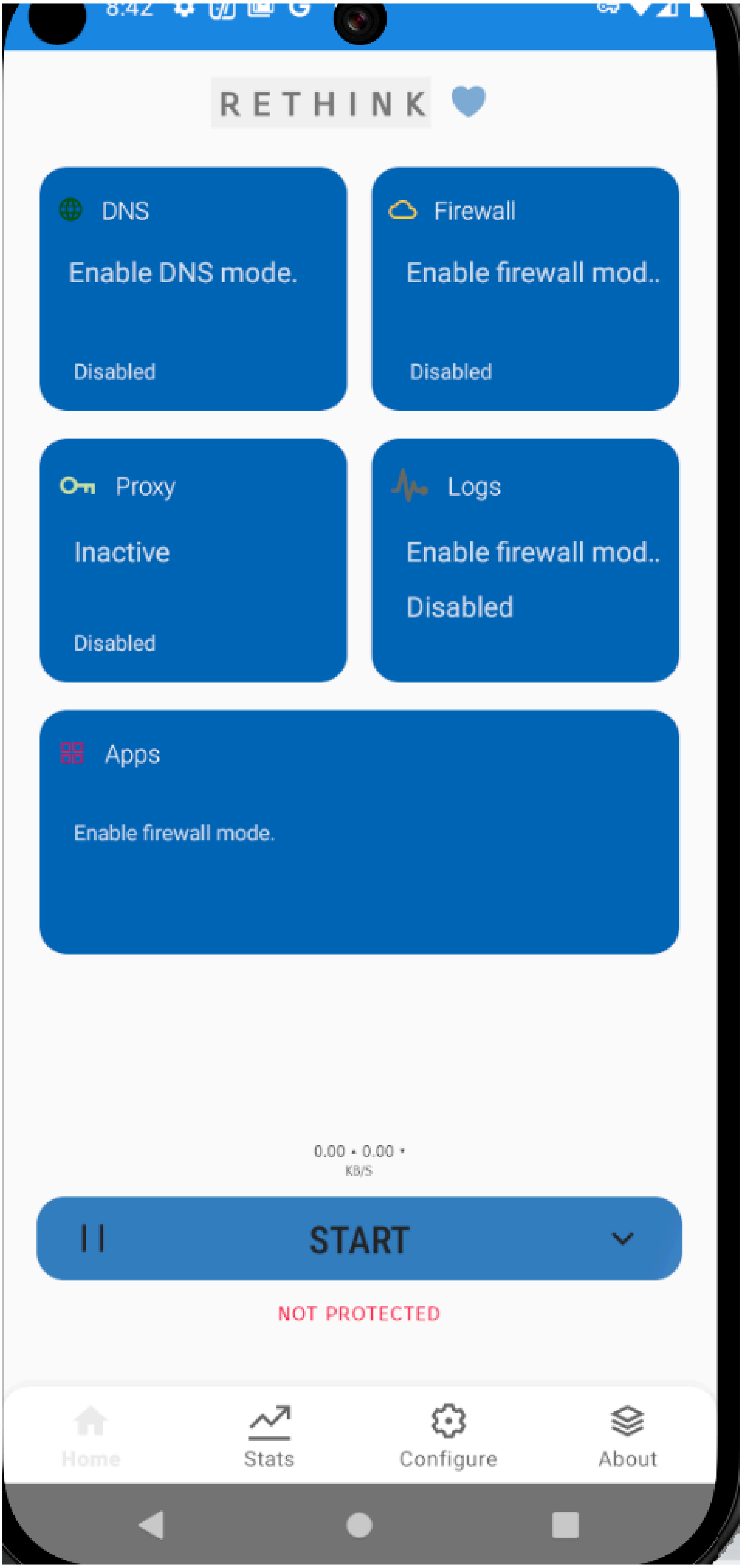
هنعرف ازاي نعمل intercept بس باستخدام  vpn علشان بعض apps بتتجاهل proxy فكده احنا مش هنعرف نعترض اي حاجة فهنشوف ازاي نعمله باستخدام vpn

1- use Rethink app : https://github.com/celzero/rethink-app



About this app →

Firewall apps, use WireGuard VPN, monitor network, block malware, change DNS.



DNS

Enable DNS mode.

Disabled

Firewall

Enable firewall mod..

Disabled

Proxy

Inactive

Disabled

Logs

Enable firewall mod..

Disabled

Apps

Enable firewall mode.

0.00 • 0.00 •
KB/S

START

NOT PROTECTED

configure HTTPS CONNECT proxy

1-Choose Inactive

2-Setup HTTP(S) Connect proxy

3- add the ip of windows and port 80

Configure DNS

1- go to Configuration

2- choose DNS

3- use System DNS

START vpn

---