Generate and Analyze HAR files

Important: This feature is available only for limited release, to add support for the feature contact support.

What is a HAR file

HTTP Archive (HAR) file is a JSON-formatted archive file format for logging an application’s (either browser or a native/hybrid app) interaction with HTTP servers. The HAR file format is an evolving standard and the information contained within it is both flexible and extensible. You can expect a HAR file to include a breakdown of timings including:

1. How long it takes to fetch DNS information.
2. How long each object takes to be requested.
3. How long it takes to connect to the server.
4. How long it takes to transfer assets from the server to the browser of each object.

In addition to the timing information, the HAR file may include details regarding any HTTP events generated during the script execution.

Perfecto provides support to generate a HAR file from an automation-script run, by activating the Network Virtualization functionality of the Perfecto CQ Lab. The HAR file will be included in the Reporting artifacts for the automation report.

Installing the Certificate

When generating the HAR file, Perfecto uses a proxy to capture the information and generate the HAR entries. Use of the proxy requires that a ***mitm*** certificate is installed on the Perfecto Lab device.

Installing the certificate involves:

1. Select the device to install the mitm certificate on.
   The certificate must be installed on the device used later for the HAR file generation.
2. Running a short Perfecto Automation script (see below).
   The script browses to the certificate installation wizard.
3. Suspending the Automation script,
4. Use Interactive mode to follow the certificate installation wizard.
5. Complete the Automation script.

Perfecto Automation Script

```
Network virtualization start(generateHarFile: true)
Wait(Wait duration: 2)
Browser go to(URL: http://mitm.it)
Wait(Wait duration:180)
<< during this three minute suspension follow the Wizard instructions, see
below >>
Network virtualization stop
```

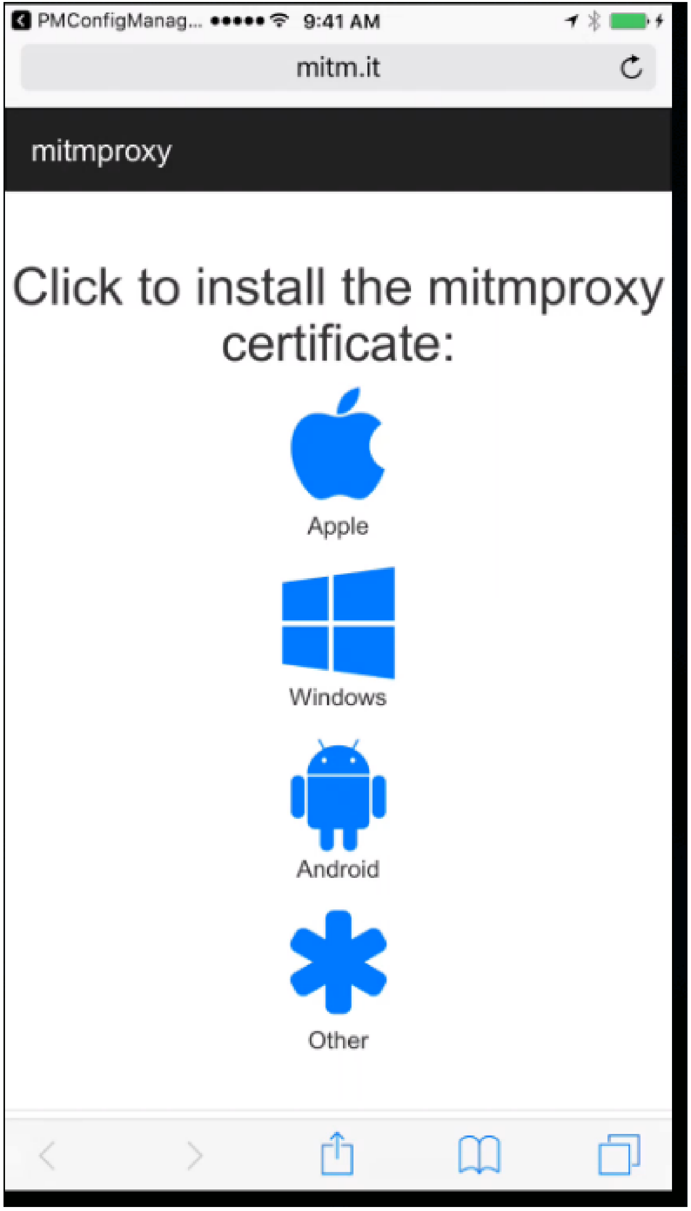
Selenium Automation Script

```
{...
        Map<String, Object> params = new HashMap<>();
    params.put("generateHarFile", "true");
    // Start the network virtualization
    driver.executeScript("mobile:vnetwork:start", params);
    // browse to the mitm site
    driver.get("http://mitm.it");

        Thread.sleep(18000);  //three minute suspension, perform Wizard
installation in manual mode, see below

        //End the network virtualization
        params.clear();
        driver.executeScript("mobile:vnetwork:stop", params);
...
}
```

Wizard Installation

During the Wait period, after the device browser navigates to the ***mitm.it*** site, perform the following steps in **Interactive** mode:

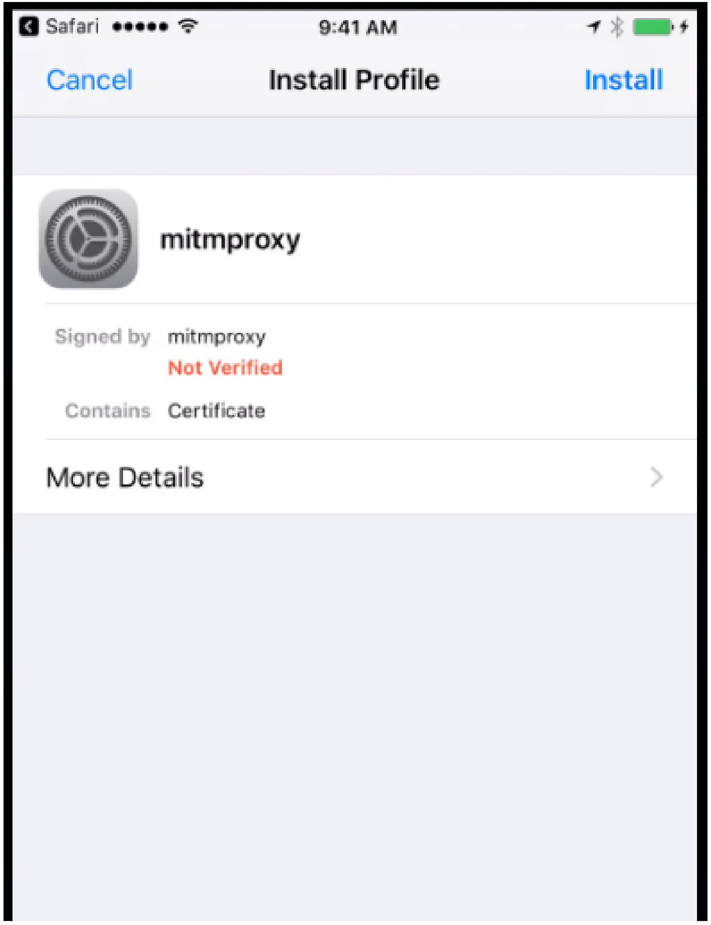
1. Select the OS of the device as the proxy version to install:



Click to install the mitmproxy certificate:

For *Android* devices continue with Android installation.
For *iOS* devices continue with the following steps.

2. The wizard displays information on the proxy trust status - Click **Install** (upper right)

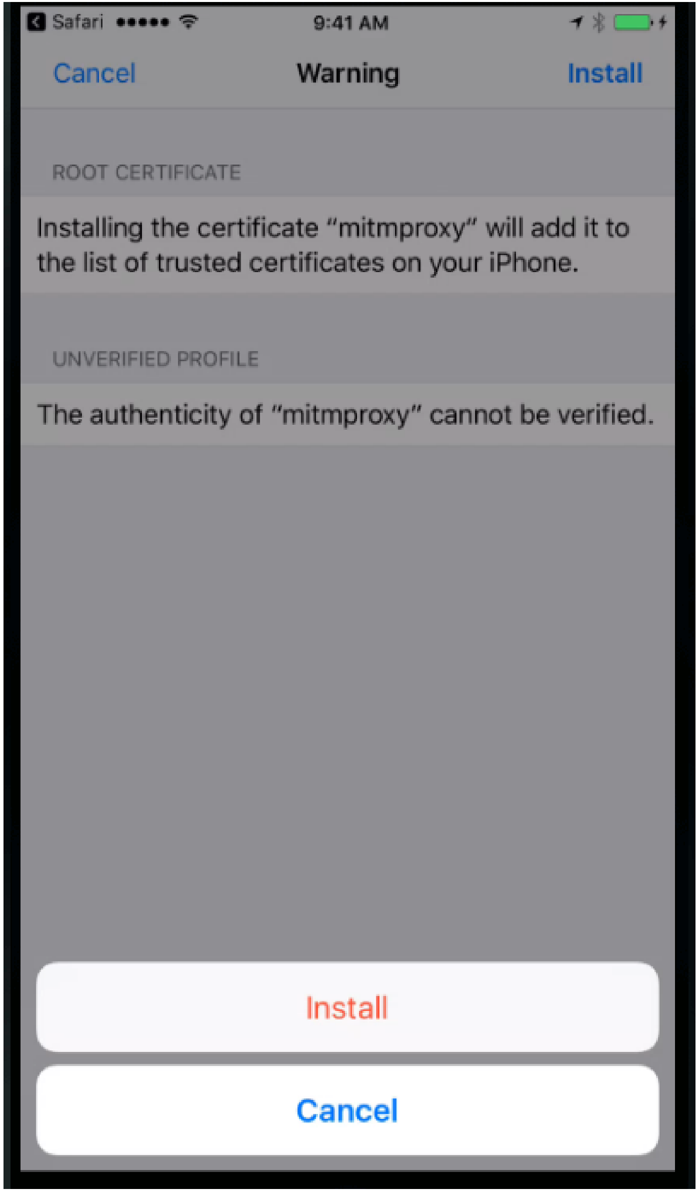


mitmproxy

Signed by mitmproxy
Not Verified

Contains Certificate

3. Wizard displays a warning message regarding the Trust status of the installation, Click **Install**



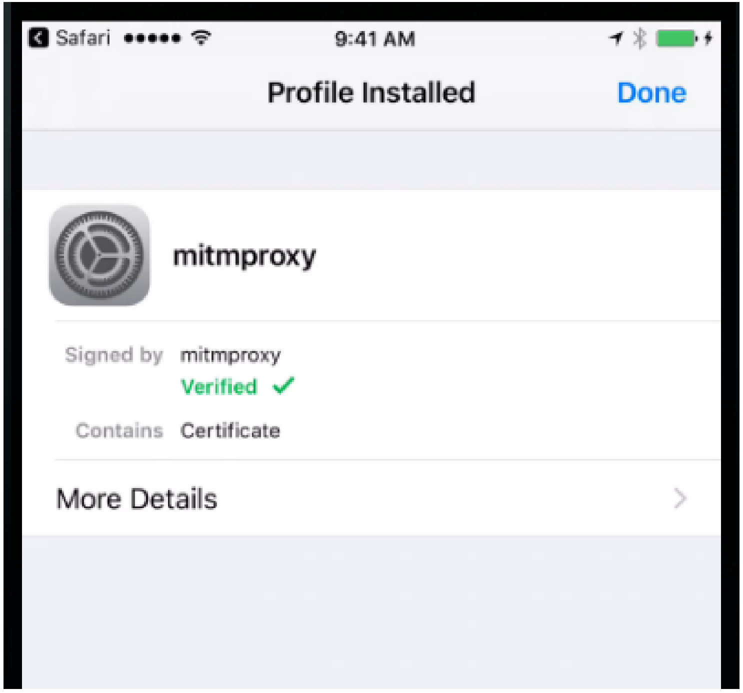
ROOT CERTIFICATE

Installing the certificate "mitmproxy" will add it to the list of trusted certificates on your iPhone.

UNVERIFIED PROFILE

The authenticity of "mitmproxy" cannot be verified.

4. When installation completes, the Wizard displays the updated Certificate status of the proxy, Click **Done**



Profile Installed

mitmproxy

Signed by mitmproxy
Verified ✓

Contains Certificate

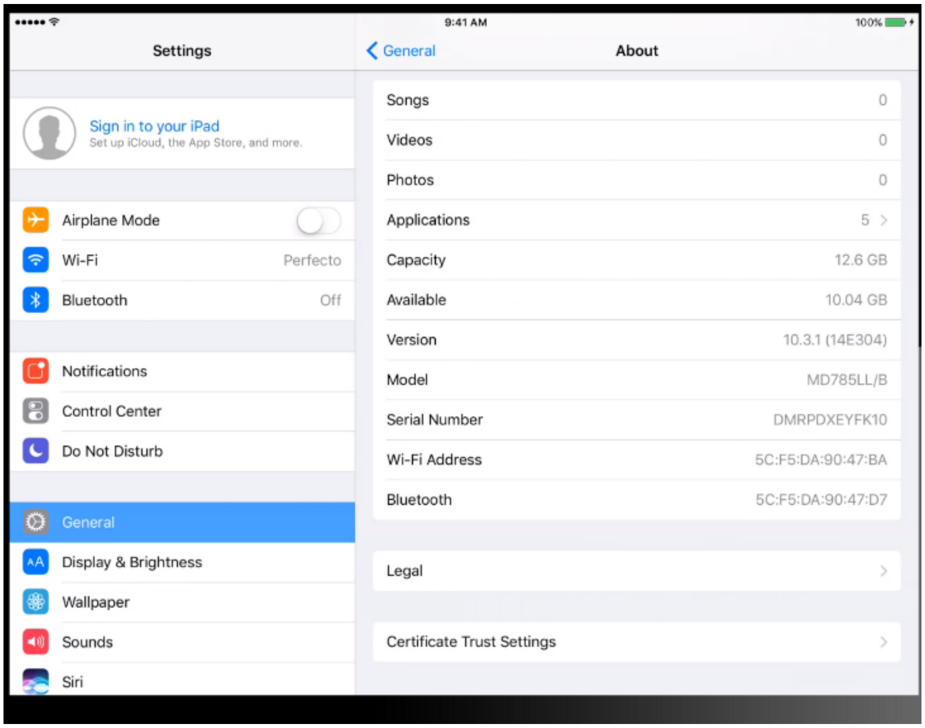
More Details

5. For Apple devices running iOS 10.3 or later continue with the Trust Proxy procedure. Other devices are ready to run.

Trusting the MITM Proxy

On iOS devices, you may need to verify that the system Trusts the installed proxy.

1. After installing the Proxy with the Wizard (as detailed above), Open the **Settings** application.
2. Click on **General > About**



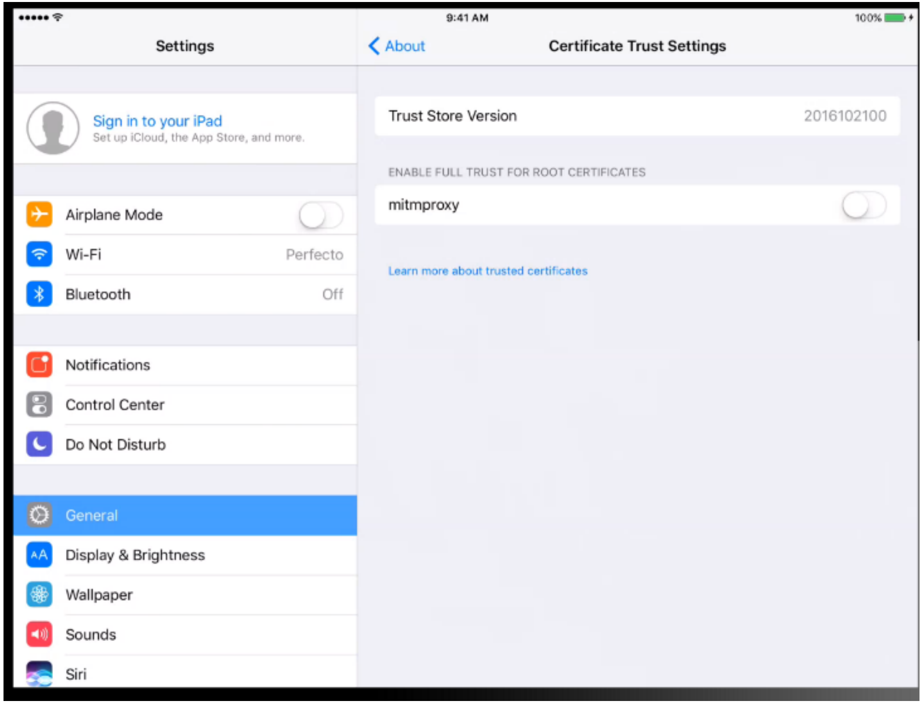
About

Songs 0
Videos 0
Photos 0
Applications 5
Capacity 12.6 GB
Available 10.04 GB
Version 10.3.1 (14E304)
Model MD785LL/B
Serial Number DMRPDXEYFK10
Wi-Fi Address 5C:F5:DA:90:47:BA
Bluetooth 5C:F5:DA:90:47:D7

Legal

Certificate Trust Settings

3. Click **Certificate Trust Settings**



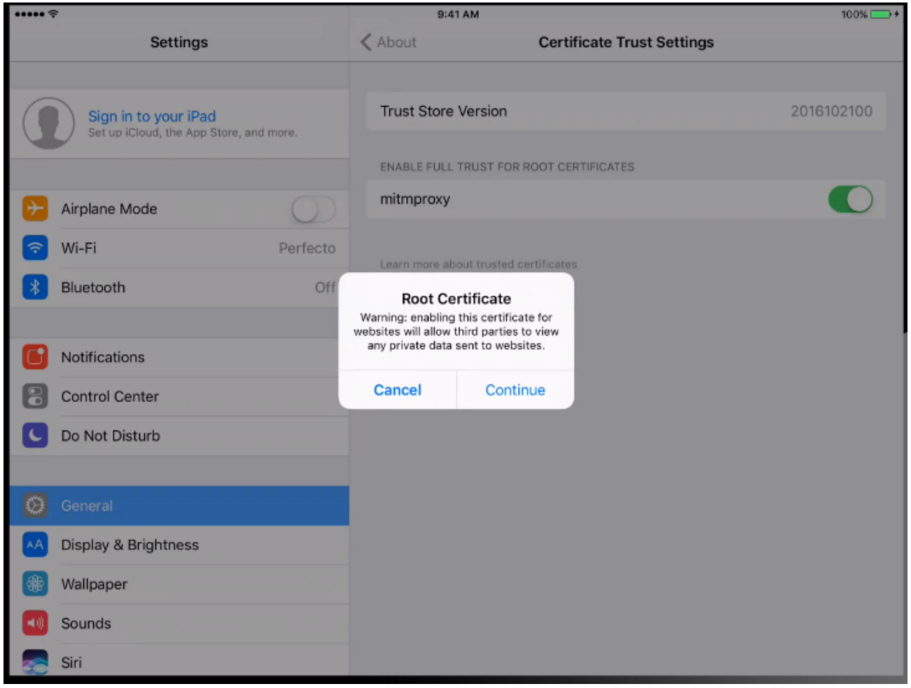
Trust Store Version 2016102100

ENABLE FULL TRUST FOR ROOT CERTIFICATES

mitmproxy

Learn more about trusted certificates

4. Set the trust setting for ***mitmproxy*** to True (selected). The system displays a warning message:



Trust Store Version 2016102100

ENABLE FULL TRUST FOR ROOT CERTIFICATES

mitmproxy

Learn more about trusted certificates

Root Certificate

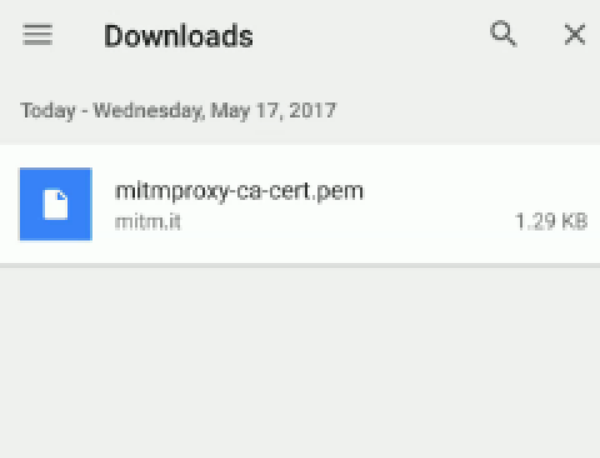
Warning: enabling this certificate for websites will allow third parties to view any private data sent to websites.

5. Click **Continue,** Proxy is now trusted.

Android Certificate Manual Install

To install the certificate on an Android device - perform the Automation script, and navigate to the mitm.it site and select Android.:

1. Open the downloaded file, by either clicking on the ***Open*** when filename is displayed at the bottom of the browser, or by opening the *Downloads* window of the browser (from the browser options menu)

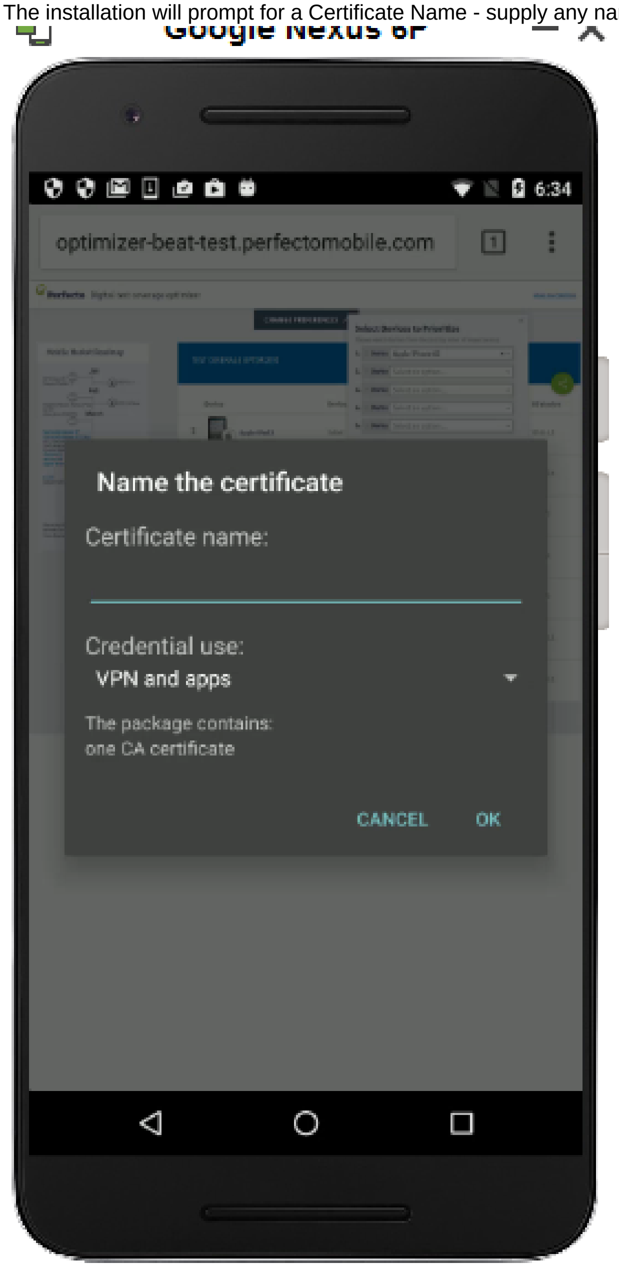


Downloads

Today - Wednesday, May 17, 2017

mitmproxy-ca-cert.pem
mitm.it
1.29 KB

2. The installation will prompt for a Certificate Name - supply any name (for example "mitm") and click OK.



Name the certificate

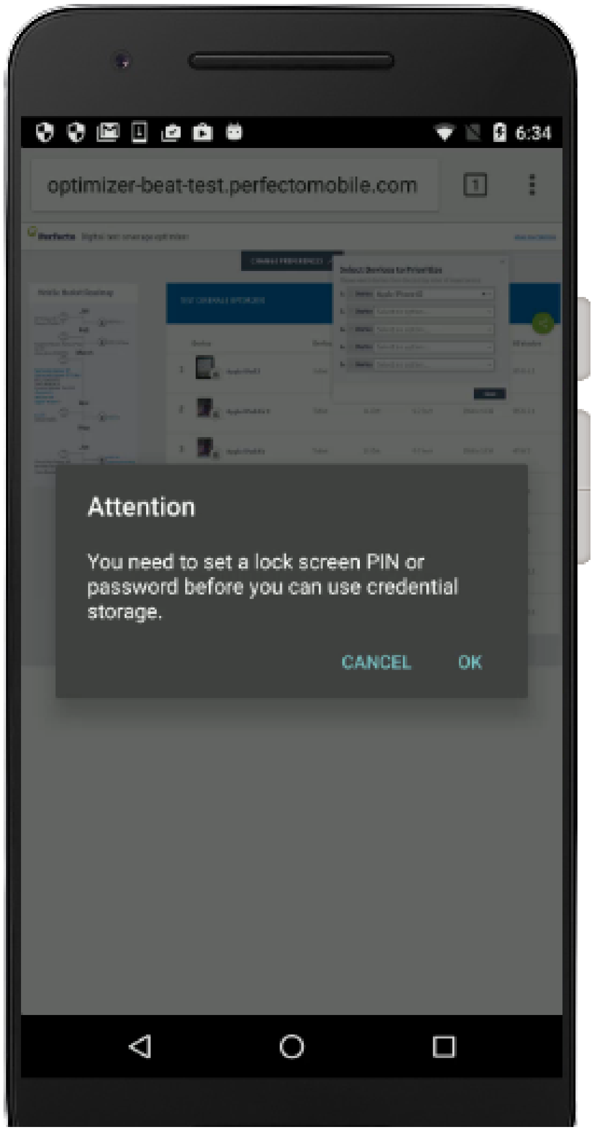
Certificate name:

Credential use:
VPN and apps

The package contains:
one CA certificate

3. Android may require that you setup an unlock credential PIN for the device -
   if you receive the following message continue to the next step.

If you do not continue to Step #9



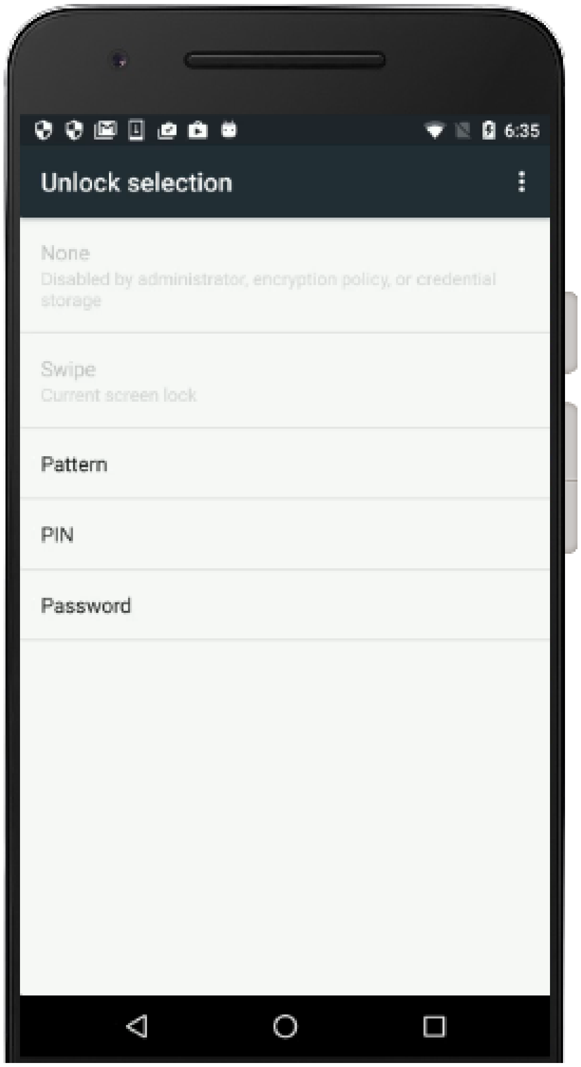
Attention

You need to set a lock screen PIN or password before you can use credential storage.

CANCEL OK

4. Click **OK** on the message and the system will present different options for the unlock credentials

> **Note**: If the device you are working with supports fingerprint identification, the system will present options that include use of *Android Imprint*. Select the option to not use Imprint.



Unlock selection

None
Disabled by administrator, encryption policy, or credential storage

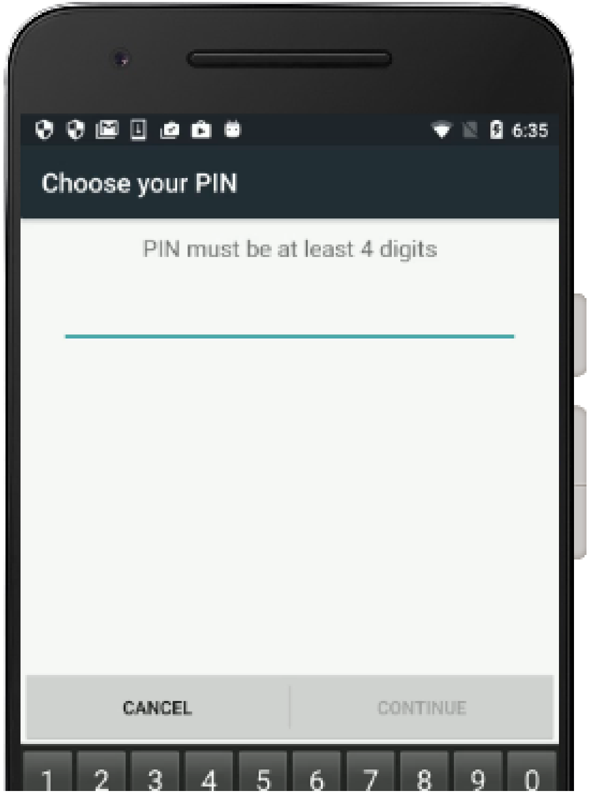
Swipe
Current screen lock

Pattern

PIN

Password

5. Select **PIN** option, and the system prompts to enter a new four-digit PIN code. Click **CONTINUE**.



Choose your PIN

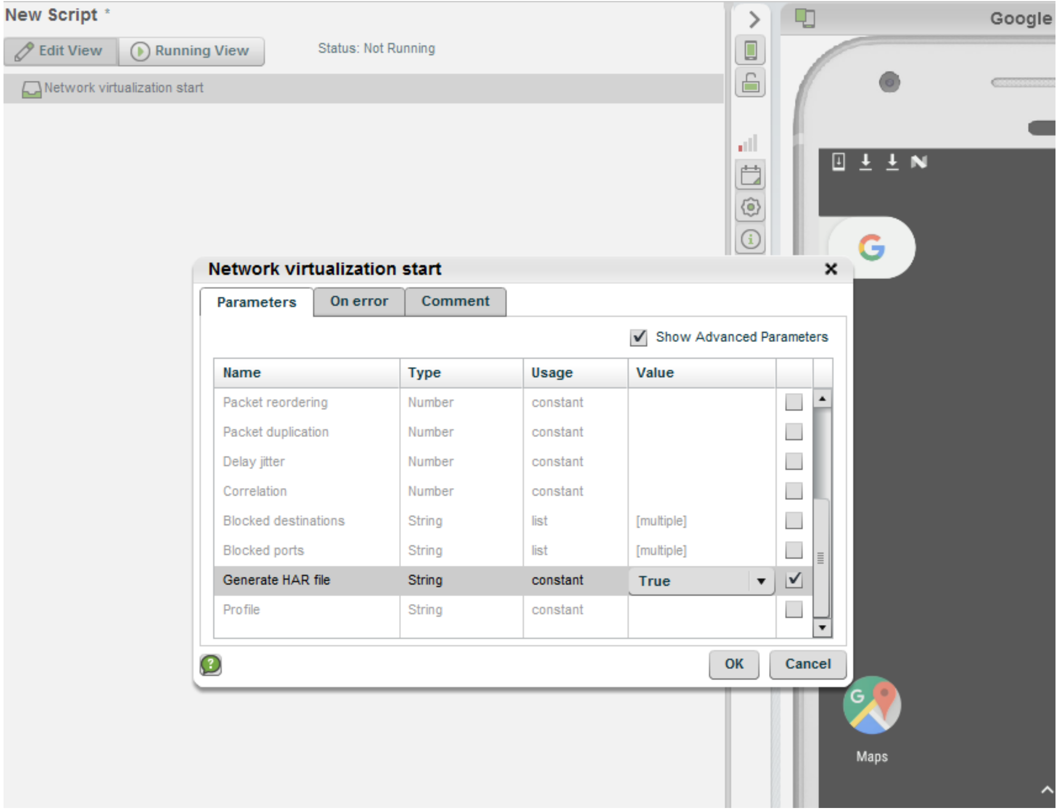
PIN must be at least 4 digits

6. Confirm the PIN on the next screen, Click **OK**.
7. The certificate is automatically installed.

When you are finished recording the HAR file you can disable the Screen Unlock PIN code - use **SettingsSecurityScreen Lock,** and select **None**
However, Passcode can be removed without uninstalling the MITM certificate from the devices based on the Android 6 and up only.
If you need to remove PIN from Android 5.1.1 device MITM certificate should be removed first.

Activating the Network Virtualization

- Use the Network virtualization start command in your automation script, setting the ***generateHarFile*** parameter to **True**. In Native Automation use the command from the *Services/Network Virtualization* folder in the **Functions** tab.



Status: Not Running

Network virtualization start

Network virtualization start

☑ Show Advanced Parameters

Name	Type	Usage	Value	
Packet reordering	Number	constant		□
Packet duplication	Number	constant		□
Delay jitter	Number	constant		□
Correlation	Number	constant		□
Blocked destinations	String	list	[multiple]	□
Blocked ports	String	list	[multiple]	□
Generate HAR file	String	constant	True	☑
Profile	String	constant		□

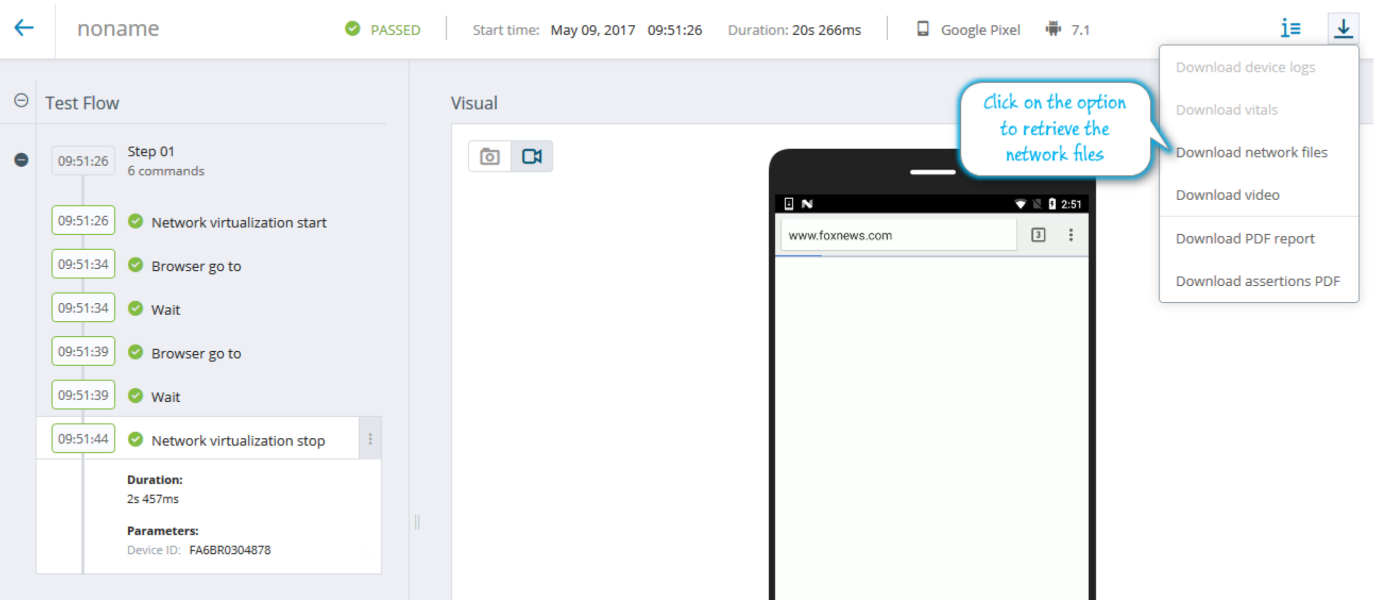
- For Selenium/Appium scripts use the **mobile:vnetwork:start** command in the *driver.executeScript()* method.

```
Map<String, Object> params = new HashMap<>();
params.put("generateHarFile", "true");
// Start the network virtualization
driver.executeScript("mobile:vnetwork:start", params);

// Add your script code here

//End the network virutalization
params.clear();
driver.executeScript("mobile:vnetwork:stop", params);
```

- Include whatever network navigation steps needed in your automation script.
- Add the Network virtualization stop command at the end of your script.
- Run the script.

Retrieving the HAR file

After completing the automation script, open the Single Test Report for the execution. In the upper right corner of the STR View, open the Retrieve artifacts menu and select the **Download network files** option.



Start time: May 09, 2017 09:51:26 Duration: 20s 266ms

09:51:26 Step 01
6 commands

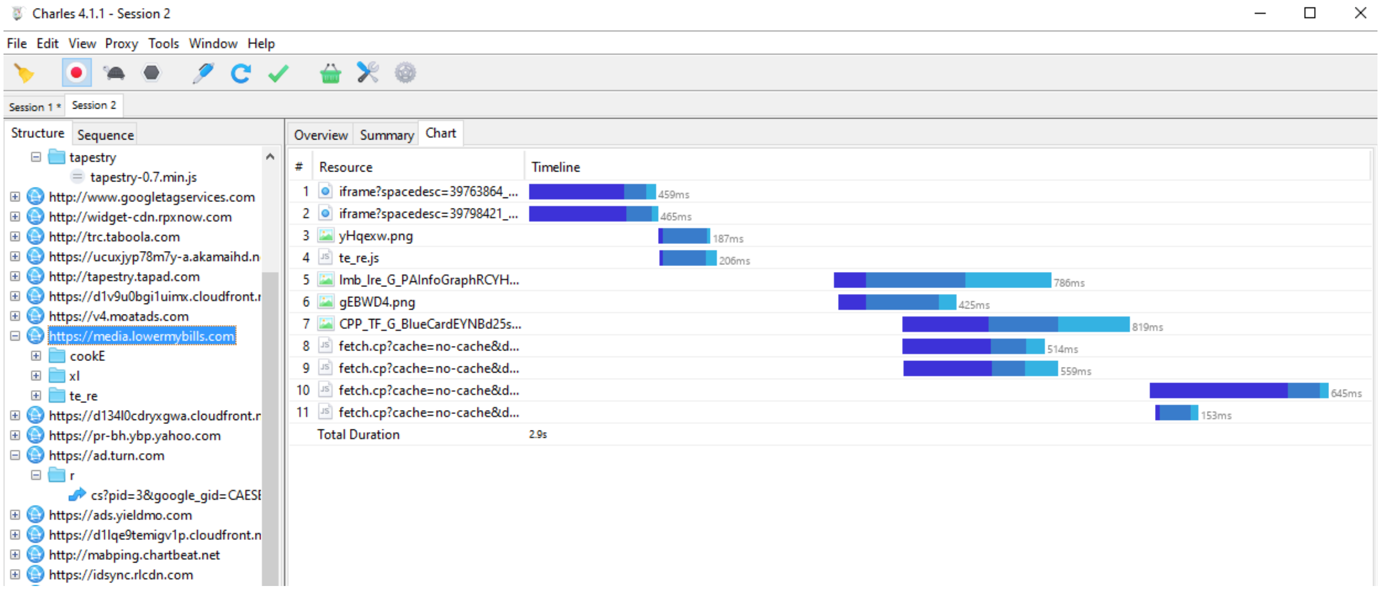
09:51:26 Network virtualization start
09:51:34 Browser go to
09:51:34 Wait
09:51:39 Browser go to
09:51:39 Wait
09:51:44 Network virtualization stop

Duration:
2s 457ms

Parameters:
Device ID: FA6BR0304878

Click on the option to retrieve the network files

Save the files to a known location and view the *.har* file with an appropriate viewer, either a browser developer tool (Chrome, Firefox tools) or an external tool like Charles (used in the example below). Import the har file and examine the timing information, request/response content, etc.


Charles 4.1.1 - Session 2
File Edit View Proxy Tools Window Help
Session 1 *
Session 2
Structure
Sequence
Overview
Summary
Chart

tapestry
tapestry-0.7.min.js
http://www.googletagservices.com
http://widget-cdn.rpxnow.com
http://trc.taboola.com
https://ucuxjyp78m7y-a.akamaihd.n
http://tapestry.tapad.com
https://d1v9u0bgi1uimx.cloudfront.r
https://v4.moatads.com
https://media.lowermybills.com
cookE
xl
te_re
https://d134l0cdryxgwa.cloudfront.r
https://pr-bh.ybp.yahoo.com
https://ad.turn.com
r
cs?pid=3&google_gid=CAESE
https://ads.yieldmo.com
https://d1lqe9temigv1p.cloudfront.n
http://mabping.chartbeat.net
https://idsync.rlcdn.com

#	Resource	Timeline
1	iframe?spacedesc=39763864_...	459ms
2	iframe?spacedesc=39798421_...	465ms
3	yHqexw.png	187ms
4	te_re.js	206ms
5	Imb_Ire_G_PAInfoGraphRCYH...	786ms
6	gEBWD4.png	425ms
7	CPP_TF_G_BlueCardEYNBd25s...	819ms
8	fetch.cp?cache=no-cache&d...	514ms
9	fetch.cp?cache=no-cache&d...	559ms
10	fetch.cp?cache=no-cache&d...	645ms
11	fetch.cp?cache=no-cache&d...	153ms
	Total Duration	2.9s

Known Limitations

- When using this feature together with Network Virtualization Profiles - the HAR file will not reflect the traffic on the virtual network, only the traffic to the actual Internet is included in the HAR file.