Generating LoadRunner script from Real Mobile Devices

Author – Vishal , India Presales Team, HP Software

Contents

Background

There are 2 types of Mobile Applications.

1) Browser Based

2) Native

To determine the performance of applications, we have to create a script in vugen which controller can use for generating load. For browser based applications, we can use the mobile truclient protocol to capture the traffic between the client browser and the server to generate the loadrunner script. The challenge is with native applications.

To capture the network traffic of a native application is a cumbersome task today. Capturing traffic for native applications cannot be done with truclient and we have to use Mobile Application protocol. There are 2 ways to capture the traffic here for Mobile Application protocol:

The Mobile App (HTTP/HTML) protocol provides two methods for script generation:

Create a Script With a Capture File

You can analyze a capture file that was created with either an external capture file utilities, such as Wireshark, or VuGen's Mobile Sniffer Agent. The **Recording Wizard** > **Analyze Traffic** option enables you to point to the capture file, specify the source or destination IP address to include, and generate the script.

Create a Script Using an Emulator

For many mobile devices, there are third party emulators that you can install on your computer. Once installed, you can use the **Emulate Record** method to record and generate a script.

Customers for practical reasons don't prefer emulators for capturing network communication between native mobile application and server.

Standard Procedure to capture communication from Real Devices:

This procedure is also listed in Loadrunner guide.

Recording Traffic into a Capture (Sniffer) File

Recording application traffic to a capture file is effective when you are unable to record an application using VuGen as is the case with mobile applications. A capture file is a trace file containing a log of all TCP traffic over the network. Using a sniffer application, you obtain a dump of all of the network traffic. The sniffer captures all of the events on the network and saves them to a capture file. To generate a smaller, more manageable script, try to capture the network traffic only for the time that you perform actions in your application. Depending on your OS and device, you have many options on where and how to record a capture file. The table below lists the some of the locations and their related advantages and disadvantages

Capture File Source	Supported by Mobile Sniffer Agent	Advantages	Disadvantages
Mobile device		Record the real traffic that comes from the device	Requires administrator permissions on most devices

Capture File Source	Supported by Mobile Sniffer Agent	Advantages	Disadvantages
VuGen with configured "hot spot[1]"	✓	• Easy and intuitive • Administrator permission not an issue	• Not all devices support "ad hoc" • Captures WiFi only (Not capturing cellular network traffic)
Server	✓	Record real traffic (both WiFi and cellular network traffic)	• Requires administrator permissions • Requires installation of a software on the server.

Challenge

As you can see from the table, default Mobile Sniffer agent we provide in LR is not supported(not installable) in real mobiles devices. Mobile sniffer agent **ONLY** works with VUgen machine configured with hotspot or when deployed on server. You can see that either of the methods for capturing traffic have following disadvantages:

Disadvantages when Vugen is configured as hotspot:

1) Doesnot support capturing of traffic over mobile network. Only Wifi supported.
2) Configuring Vugen with hotspot is a tedious and cumbersome task involving hot spot and adhoc network creation and tethering mobile devices.

Disadvantages of having sniffer agent in server:

1) Require administrative permission on servers.
2) If the end customer is service provider/third party services in most cases, then he will not be given access to server to install the sniffer agent.
3) Customer is hesitant to install any software in testing/production systems.

In summary, it is impractical in some scenarios and tedious in other scenarios to capture traffic using above methods.

Solution

Install a network traffic capture mobile application and capture the network traffic going from the real mobile device. One such app available in android playstore called tPacketCapture can be used to capture entire network traffic. tPacketCapture does packet capturing without using any root permissions. tPacketCapture uses VpnService provided by Android OS. Captured data are saved as a PCAP file format in the external storage of your mobile. If you want a more detailed analysis, please transfer the file to your PC and use the software handles PCAP format(such as Wireshark). There is also an advanced version of this application tPacketCapture Pro which can be used to capture filtered traffic from specific application.

★ Differences between tPacketCapture and tPacketCapture Pro ★
Pro Version include an Application filtering feature. Application filtering is able to capture only a specific application communication.

Below youtube URL can be used for understanding how to run the application to capture the real mobile traffic on real networks:

https://www.youtube.com/watch?feature=player_embedded&v=PjJbfYfDsX4
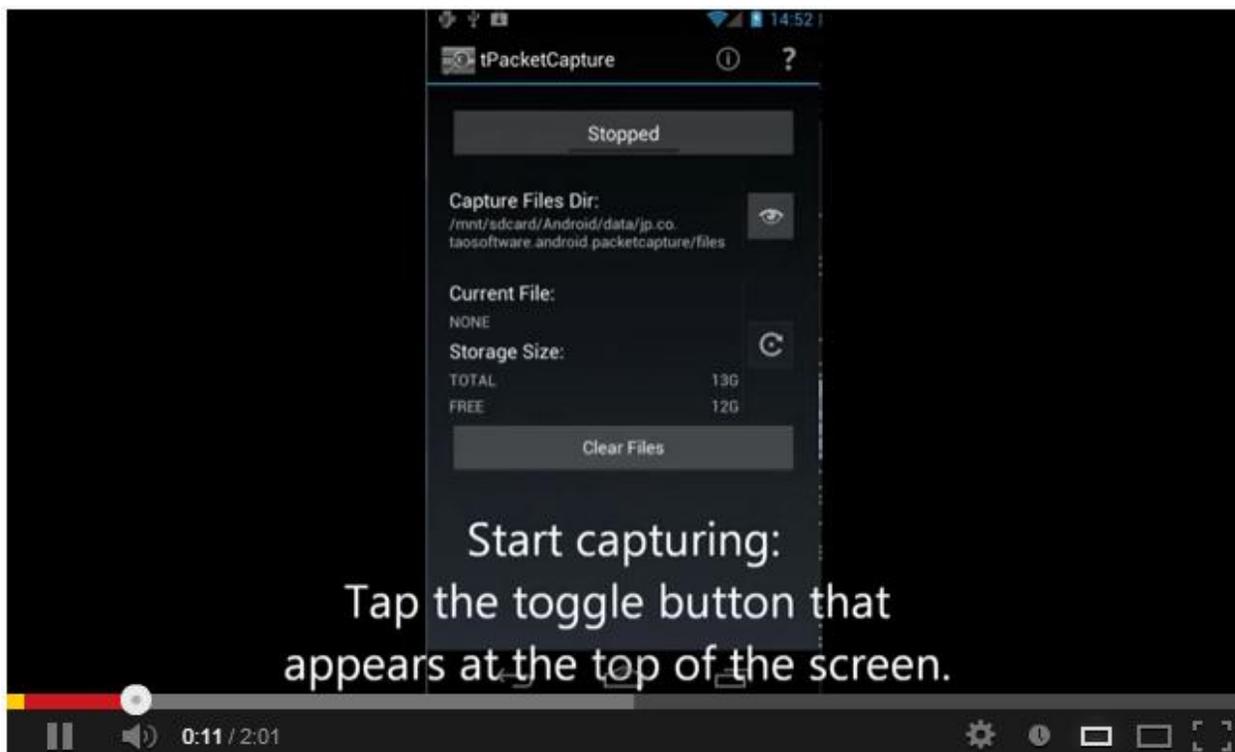
Steps to generate vugen script from pcap file:

1. **Transfer your pcap file from mobile to desktop machine**

   Once you create the pcap file from the tPacketCapture application share it to the machine where you have Vugen installed
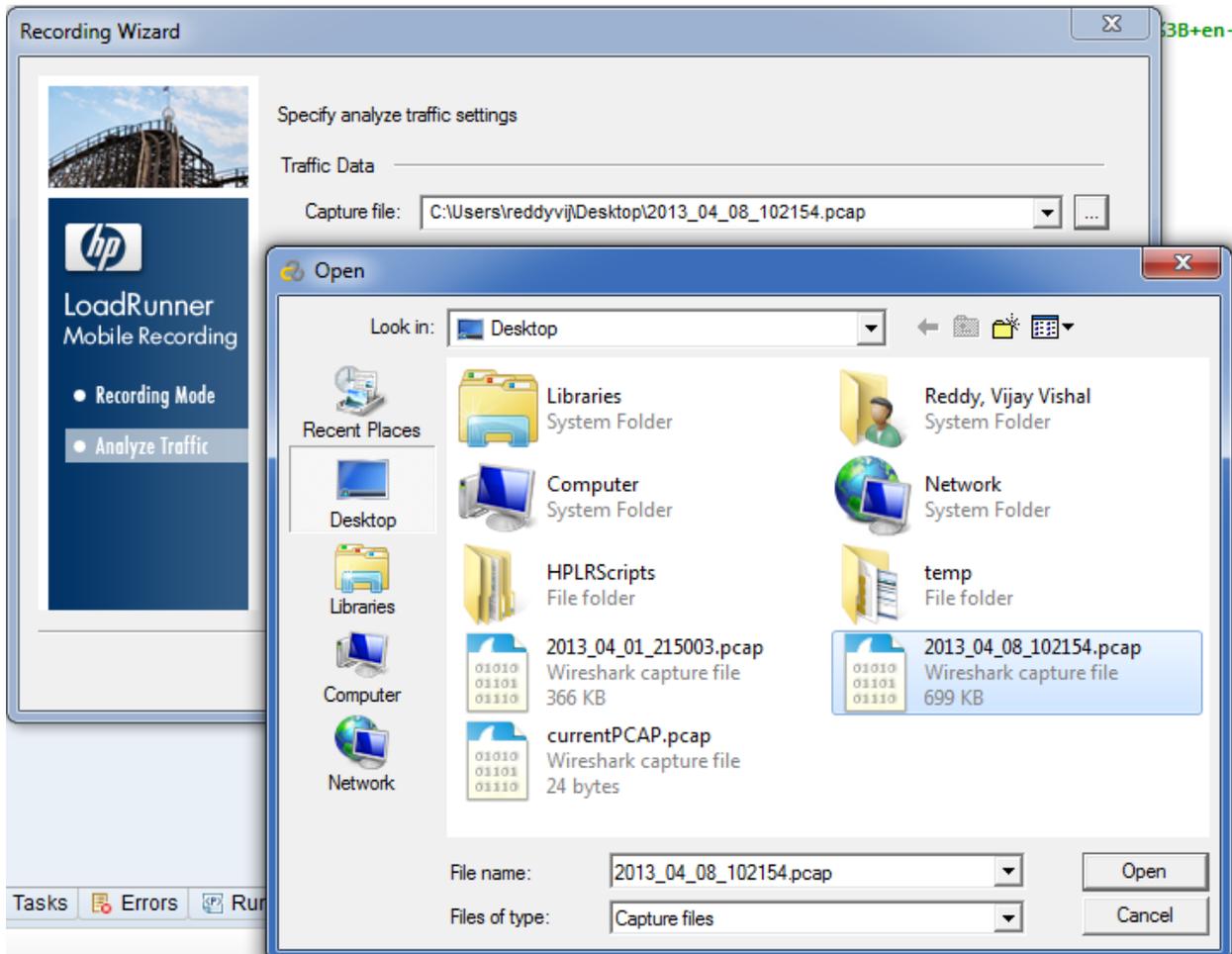
2. **Start the Recording Wizard**
   Click the **Start Record** button after choosing mobile application protocol. Select the **Analyze Traffic** method.
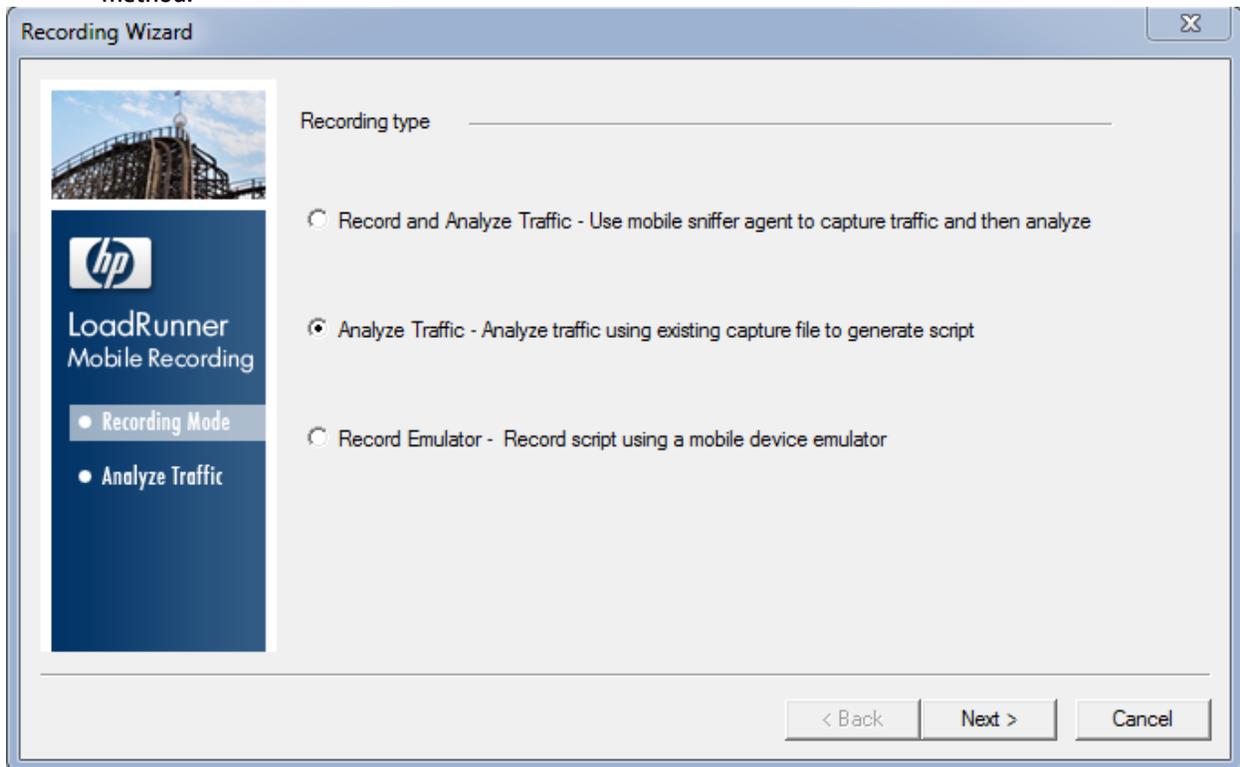
3. Specify the location of the Capture File

Enter or browse to the location of the capture file.

4. Enter Mobile IP:

Enter the client IP to filter

5. Finish

Click Finish button and the script gets generated

```
Mobile...rRecording : Action.c ✕
632      web_url("subscription_details_ajax.asp_32",
633          "URL=http://mobile-net.hp.com:8080/subscription_details_ajax.asp?time=1365396886820",
634          "Resource=0",
635          "RecContentType=text/html",
636          "Referer=http://mobile-net.hp.com:8080/session.asp",
637          "Snapshot=t69.inf",
638          "Mode=HTML",
639          LAST);
640
641      web_url("search",
642          "URL=http://www.google.co.in/search?hl=en&site=&source=hp&ei=Yk1iUZSwA8OjigLm9ICYDA&q=mobile+application+load+runner&btnG=",
643          "Resource=0",
644          "RecContentType=text/html",
645          "Referer=",
646          "Snapshot=t70.inf",
647          "Mode=HTML",
648          LAST);
649
650      web_url("session_ajax.asp_33",
651          "URL=http://mobile-net.hp.com:8080/session_ajax.asp?time=1365396891898",
652          "Resource=0",
```

Conclusion

Using tPacketCapture application you can capture the real mobile traffic on real network for native applications overcoming some of the tedious and cumbersome process prevalent today. Advantages of this method are as below:

Technical Benefits

1) Less Effort
2) Less component dependencies
3) No rooting required
4) Real Device and Real Network usage means more confidence
5) Simple & easy approach to testing native mobile applications

Business Benefits

1. Organizations are able to effectively and efficiently address the challenges of mobile testing
2. This reality makes performance testing for mobile applications not just a nice thing to have, but an essential activity for success in the age of the instant-on enterprise—a time when people expect instantaneous access to your organization and the services you provide.

There are others apps in the market similar to this and can be used after due diligence.