1. Install Frida on local PC
2. Install Android studio and create an Android Open Source AVD
3. Install the Xbox APK
4. Install Frida server – this needs to match the AVD’s architecture and be the same version as the Frida version installed on local client
   1. adb push ~/Downloads/frida-server-16.6.6-android-arm64 /data/local/tmp/frida-server
5. Start Xbox
   1. adb shell monkey -p com.microsoft.xboxone.smartglass -c android.intent.category.LAUNCHER 1
6. In one terminal tab, launch Frida-server
   1. adb shell /data/local/tmp/frida-server
7. Use Frida-trace to identify the right SNI, e.g. searching with
   1. frida-trace -U -n Xbox -i "\*SSL\*" or using the script below
8. Launch Frida with the hooks necessary to identify, log, and process the correct API call(s)
   1. frida -U -n Xbox -l ~/Desktop/my\_hook.js

## Login to playstation

adb shell input tap 518 2150 # click “sign in”

adb shell input tap 440 870 # click email box

adb shell input text "nick@nickballou.com"  
adb shell input tap 513 1000 # click next

adb shell input tap 480 970 # click email box

adb shell input text "docbuz-Duwce4-woshib"

adb shell input tap 770 1100 # click “sign in”

adb shell input tap 650 2000 # click “confirm and continue”

## Login to xbox

adb shell input tap 550 1950

adb shell input tap 280 530 # click email box

adb shell input text "nick@nickballou.com"

adb shell input tap 870 812 # click next

adb shell input tap 360 570 # click password box

adb shell input text “guqtin-Conjen-turni6”

adb shell input tap 900 920 # click sign in

adb shell input tap 550 2145 # click “let’s go”

### GET SNI

var getServerName = Module.findExportByName("libssl.so", "SSL\_get\_servername");

if (getServerName) {

Interceptor.attach(getServerName, {

onEnter: function(args) {

// nothing to do on enter

},

onLeave: function(retval) {

if (!retval.isNull()) {

var serverName = Memory.readUtf8String(retval);

console.log("Server name (SNI) is: " + serverName);

}

}

});

console.log("Hooked SSL\_get\_servername at: " + getServerName);

} else {

console.log("Could not find SSL\_get\_servername");

}