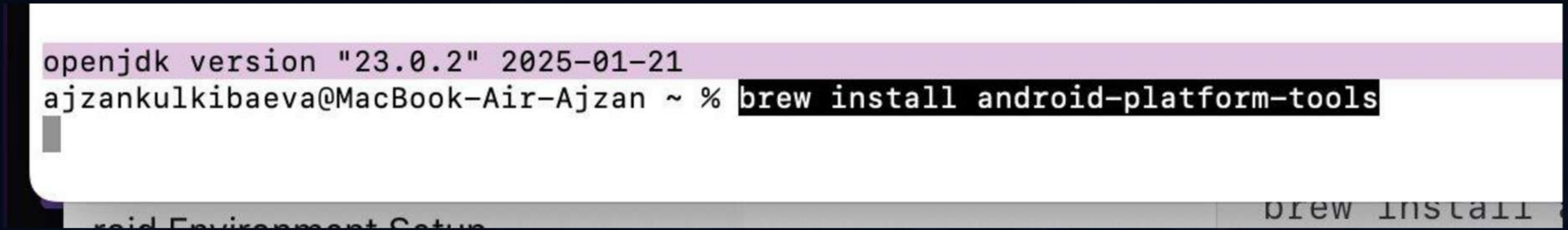
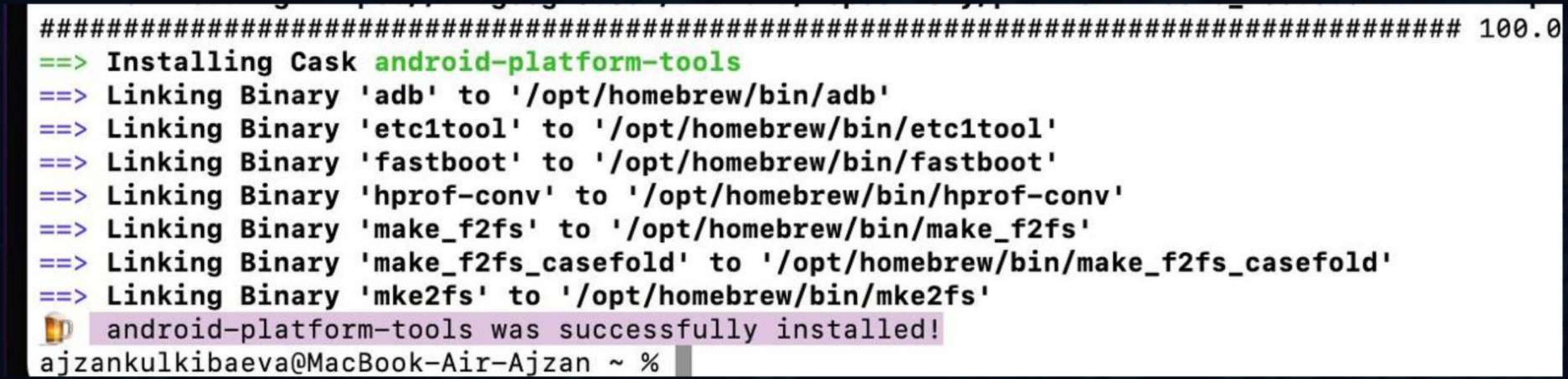
THYNK UNLIMITED

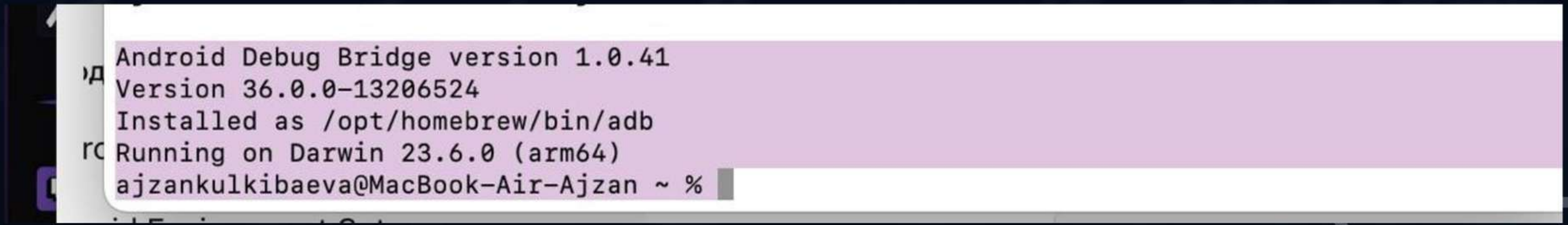
MOBILE APPLICATION SECURITY ANALYSIS



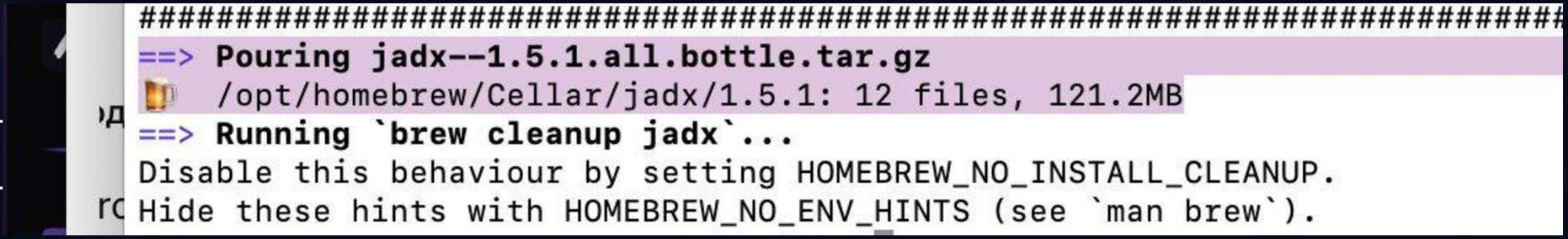
```
openjdk version "23.0.2" 2025-01-21
ajzankulkibaeva@MacBook-Air-Ajzan ~ % brew install android-platform-tools
```



```
######################################################################################## 100.0
==> Installing Cask android-platform-tools
==> Linking Binary 'adb' to '/opt/homebrew/bin/adb'
==> Linking Binary 'etc1tool' to '/opt/homebrew/bin/etc1tool'
==> Linking Binary 'fastboot' to '/opt/homebrew/bin/fastboot'
==> Linking Binary 'hprof-conv' to '/opt/homebrew/bin/hprof-conv'
==> Linking Binary 'make_f2fs' to '/opt/homebrew/bin/make_f2fs'
==> Linking Binary 'make_f2fs_casefold' to '/opt/homebrew/bin/make_f2fs_casefold'
==> Linking Binary 'mke2fs' to '/opt/homebrew/bin/mke2fs'
🍺  android-platform-tools was successfully installed!
ajzankulkibaeva@MacBook-Air-Ajzan ~ %
```

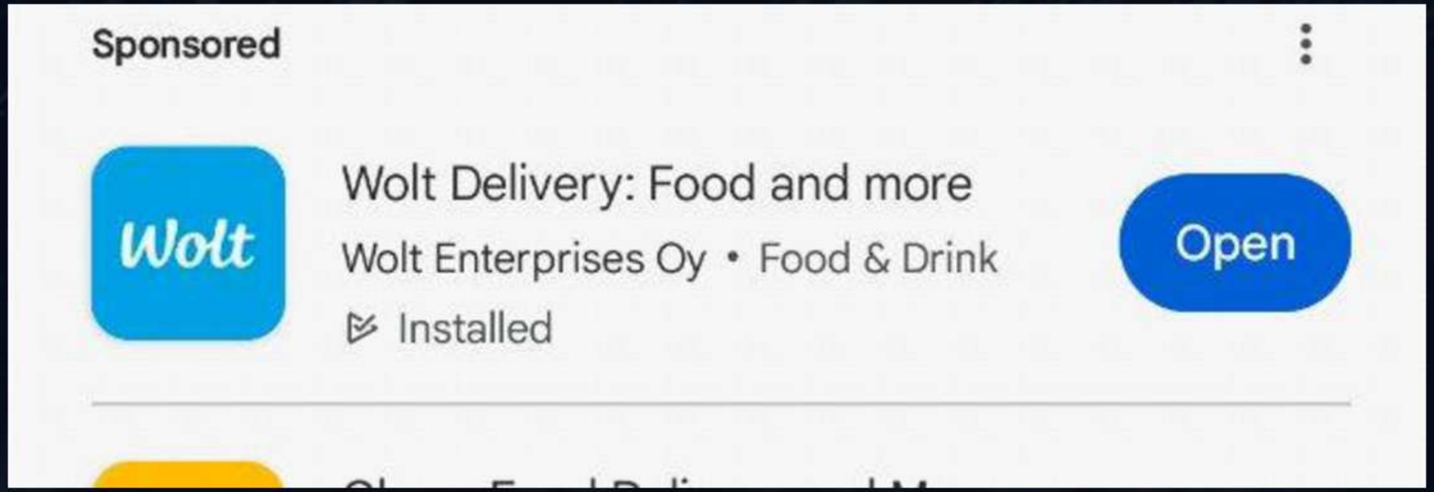


```
Android Debug Bridge version 1.0.41
Version 36.0.0-13206524
Installed as /opt/homebrew/bin/adb
Running on Darwin 23.6.0 (arm64)
ajzankulkibaeva@MacBook-Air-Ajzan ~ %
```



```
#########################################################################
==> Pouring jadx--1.5.1.all.bottle.tar.gz
🍺  /opt/homebrew/Cellar/jadx/1.5.1: 12 files, 121.2MB
==> Running `brew cleanup jadx`...
Disable this behaviour by setting HOMEBREW_NO_INSTALL_CLEANUP.
Hide these hints with HOMEBREW_NO_ENV_HINTS (see `man brew`).
```

PHASE 2: WOLT



Sponsored

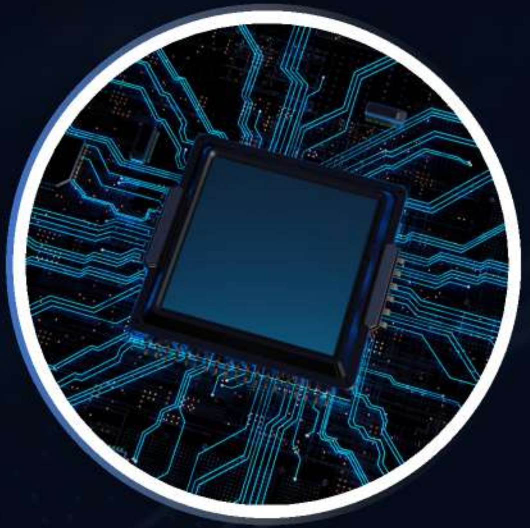
Wolt Delivery: Food and more

Wolt Enterprises Oy • Food & Drink

Installed

PHASE 3

```
1.adb devices

List of devices attached
emulator-5554 device
```

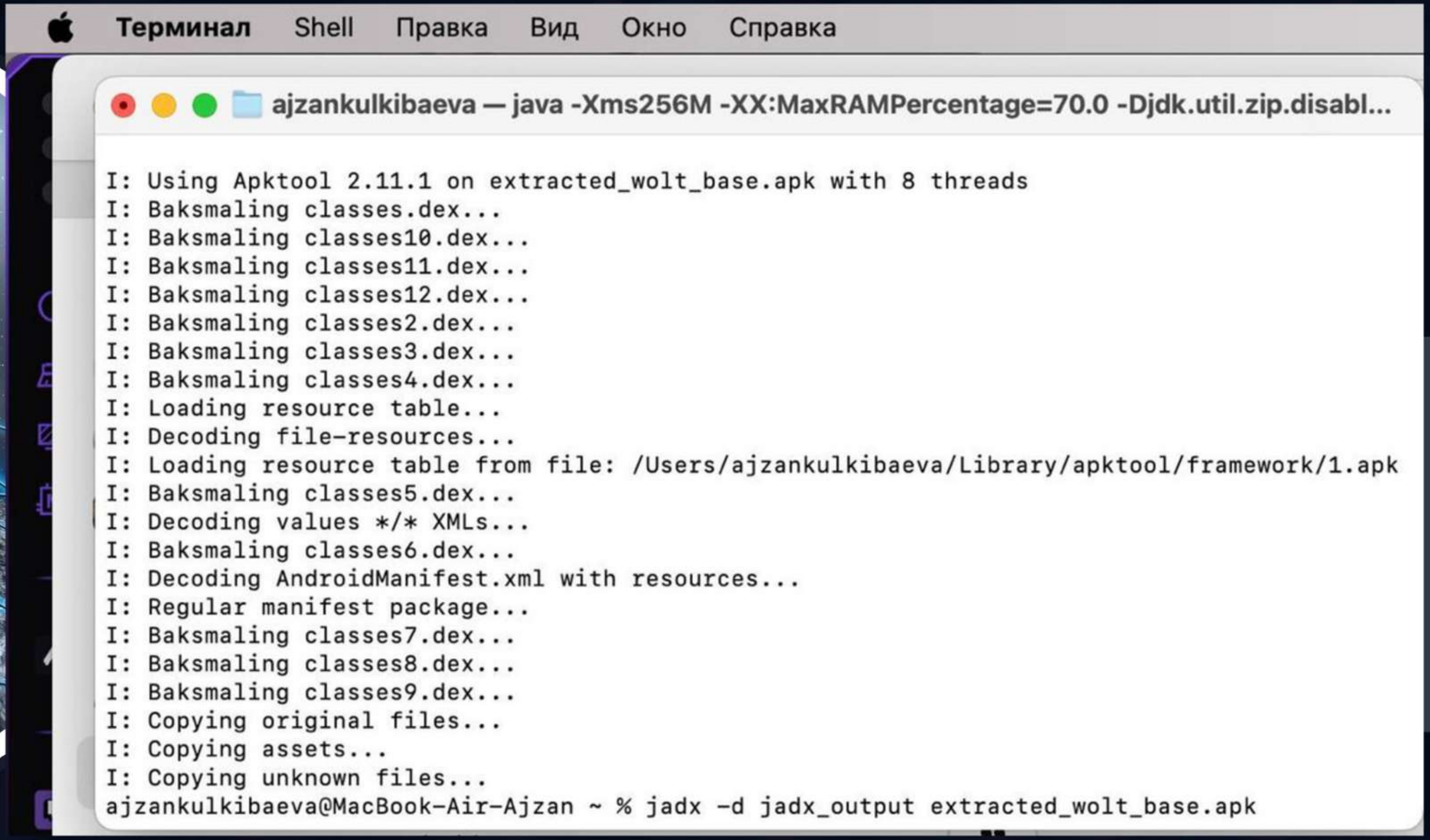


```
2.adb shell pm list packages | grep wolt
package:com.wolt.android
```

```
3.adb shell pm path com.wolt.android
```

```
4.adb pull /data/app/~~0_Oft10KOzysVmnAQbIUlw==/com.wolt.android-
rXJxXkLQWZDece2CZTWxJA==/base.apk ./extracted_wolt_base.apk

/data/app/~~0_Oft10KOzysVmnAQbIUlw==/com.wol...ipped. 65.0 MB/s (136851690 bytes in 2.007s)
```

PHASE 4: DECOMPILING THE APPLICATION

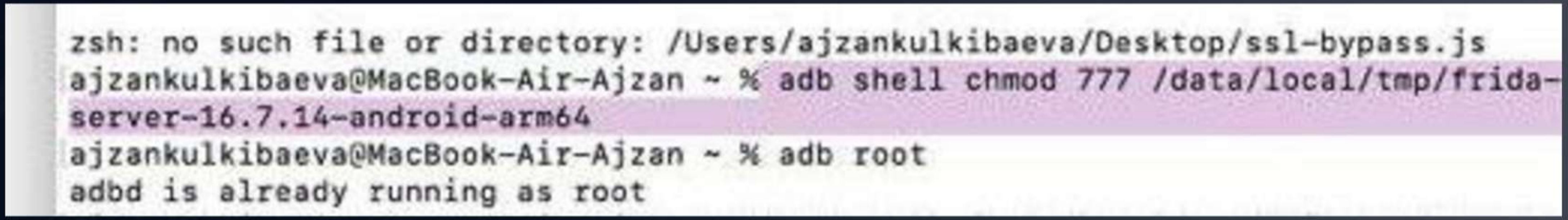

Терминал
Shell
Правка
Вид
Окно
Справка
ajzankulkibaeva — java -Xms256M -XX:MaxRAMPercentage=70.0 -Djdk.util.zip.disabl...

```
I: Using Apktool 2.11.1 on extracted_wolt_base.apk with 8 threads
I: Baksmaling classes.dex...
I: Baksmaling classes10.dex...
I: Baksmaling classes11.dex...
I: Baksmaling classes12.dex...
I: Baksmaling classes2.dex...
I: Baksmaling classes3.dex...
I: Baksmaling classes4.dex...
I: Loading resource table...
I: Decoding file-resources...
I: Loading resource table from file: /Users/ajzankulkibaeva/Library/apktool/framework/1.apk
I: Baksmaling classes5.dex...
I: Decoding values */* XMLs...
I: Baksmaling classes6.dex...
I: Decoding AndroidManifest.xml with resources...
I: Regular manifest package...
I: Baksmaling classes7.dex...
I: Baksmaling classes8.dex...
I: Baksmaling classes9.dex...
I: Copying original files...
I: Copying assets...
I: Copying unknown files...
ajzankulkibaeva@MacBook-Air-Ajzan ~ % jadx -d jadx_output extracted_wolt_base.apk
```

www.reallygreatsite.com

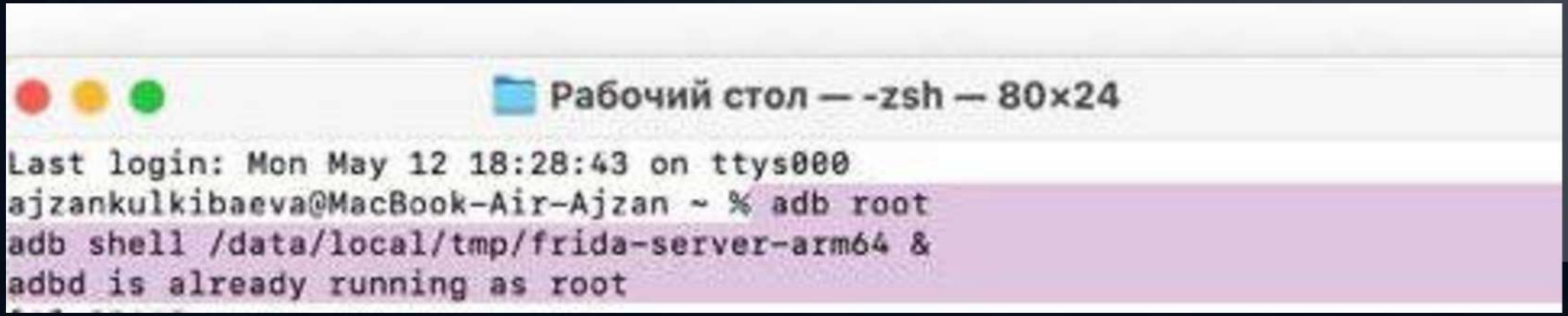
METHOD 2: FRIDA HOOKING

Rapid Detection and Containment

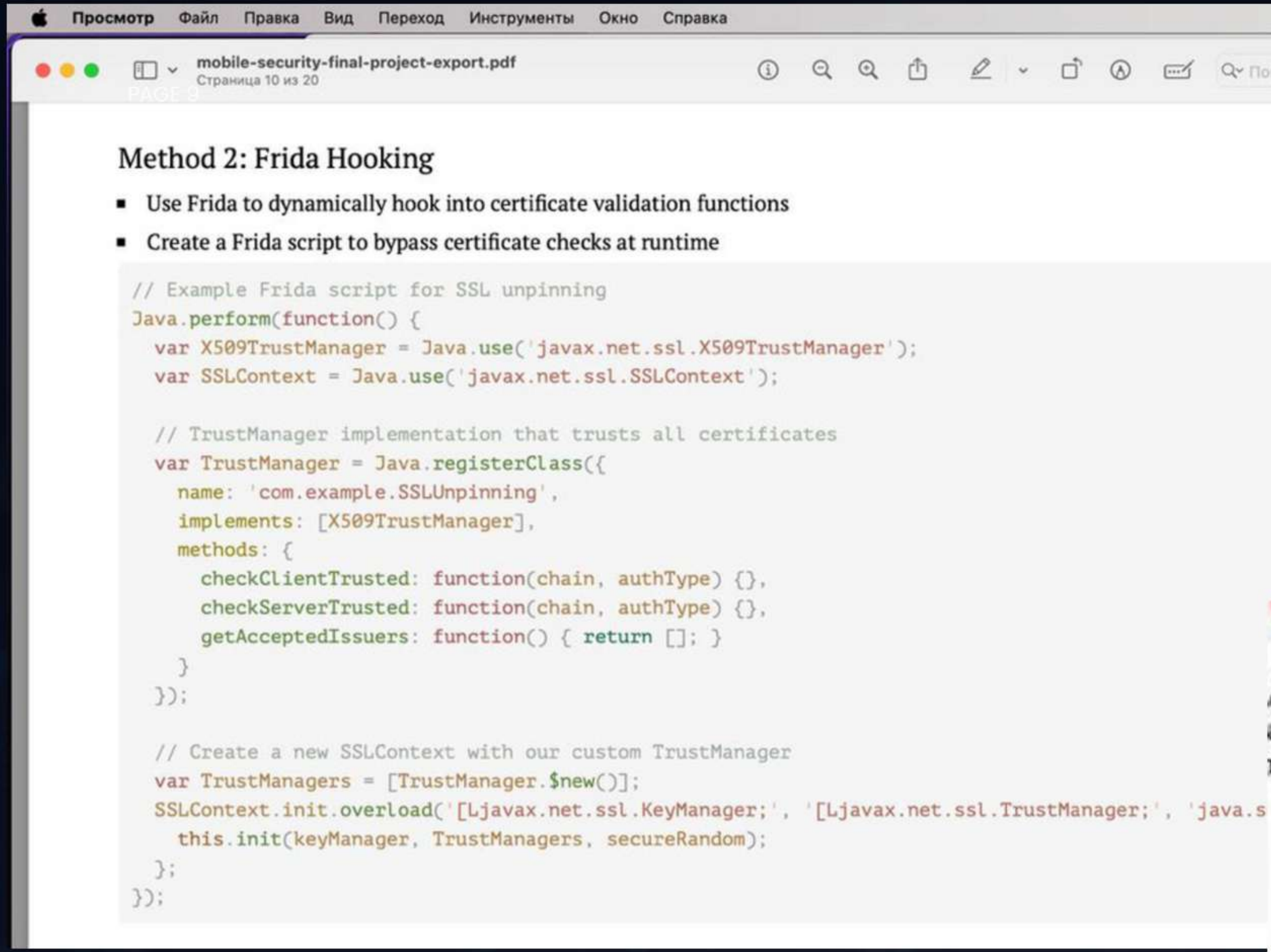


```
zsh: no such file or directory: /Users/ajzankulkibaeva/Desktop/ssl-bypass.js
ajzankulkibaeva@MacBook-Air-Ajzan ~ % adb shell chmod 777 /data/local/tmp/frida-
server-16.7.14-android-arm64
ajzankulkibaeva@MacBook-Air-Ajzan ~ % adb root
adbd is already running as root
```

Post-Incident Analysis and Recovery:



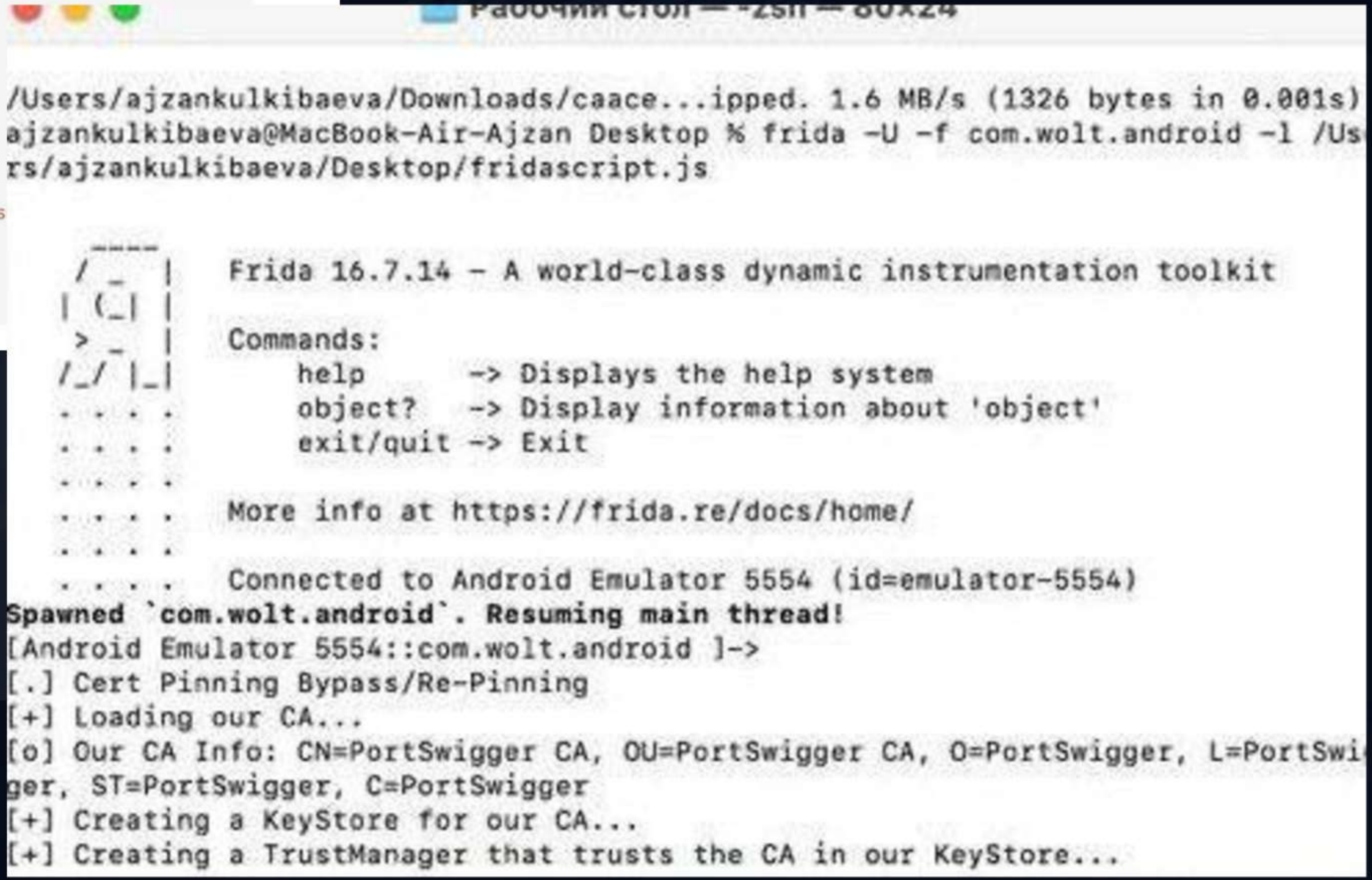
```
Last login: Mon May 12 18:28:43 on ttys000
ajzankulkibaeva@MacBook-Air-Ajzan ~ % adb root
adb shell /data/local/tmp/frida-server-arm64 &
adbd is already running as root
```



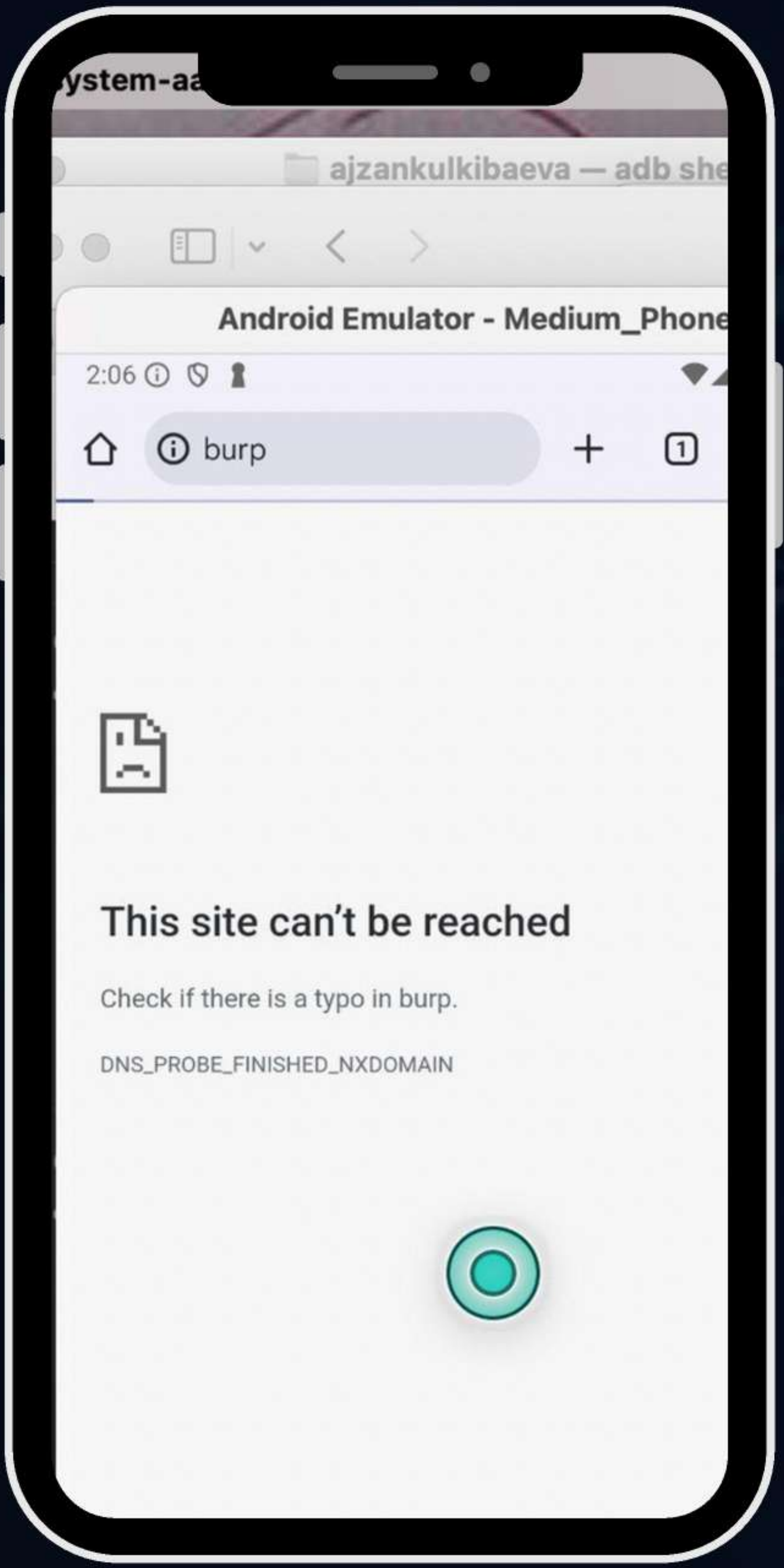
Method 2: Frida Hooking

- Use Frida to dynamically hook into certificate validation functions
- Create a Frida script to bypass certificate checks at runtime

```
// Example Frida script for SSL unpinning
Java.perform(function() {
  var X509TrustManager = Java.use('javax.net.ssl.X509TrustManager');
  var SSLContext = Java.use('javax.net.ssl.SSLContext');

  // TrustManager implementation that trusts all certificates
  var TrustManager = Java.registerClass({
    name: 'com.example.SSLUnpinning',
    implements: [X509TrustManager],
    methods: {
      checkClientTrusted: function(chain, authType) {},
      checkServerTrusted: function(chain, authType) {},
      getAcceptedIssuers: function() { return []; }
    }
  });

  // Create a new SSLContext with our custom TrustManager
  var TrustManagers = [TrustManager.$new()];
  SSLContext.init.overload('[Ljavax.net.ssl.KeyManager;', '[Ljavax.net.ssl.TrustManager;', 'java.s
    this.init(keyManager, TrustManagers, secureRandom);
  };
});
```



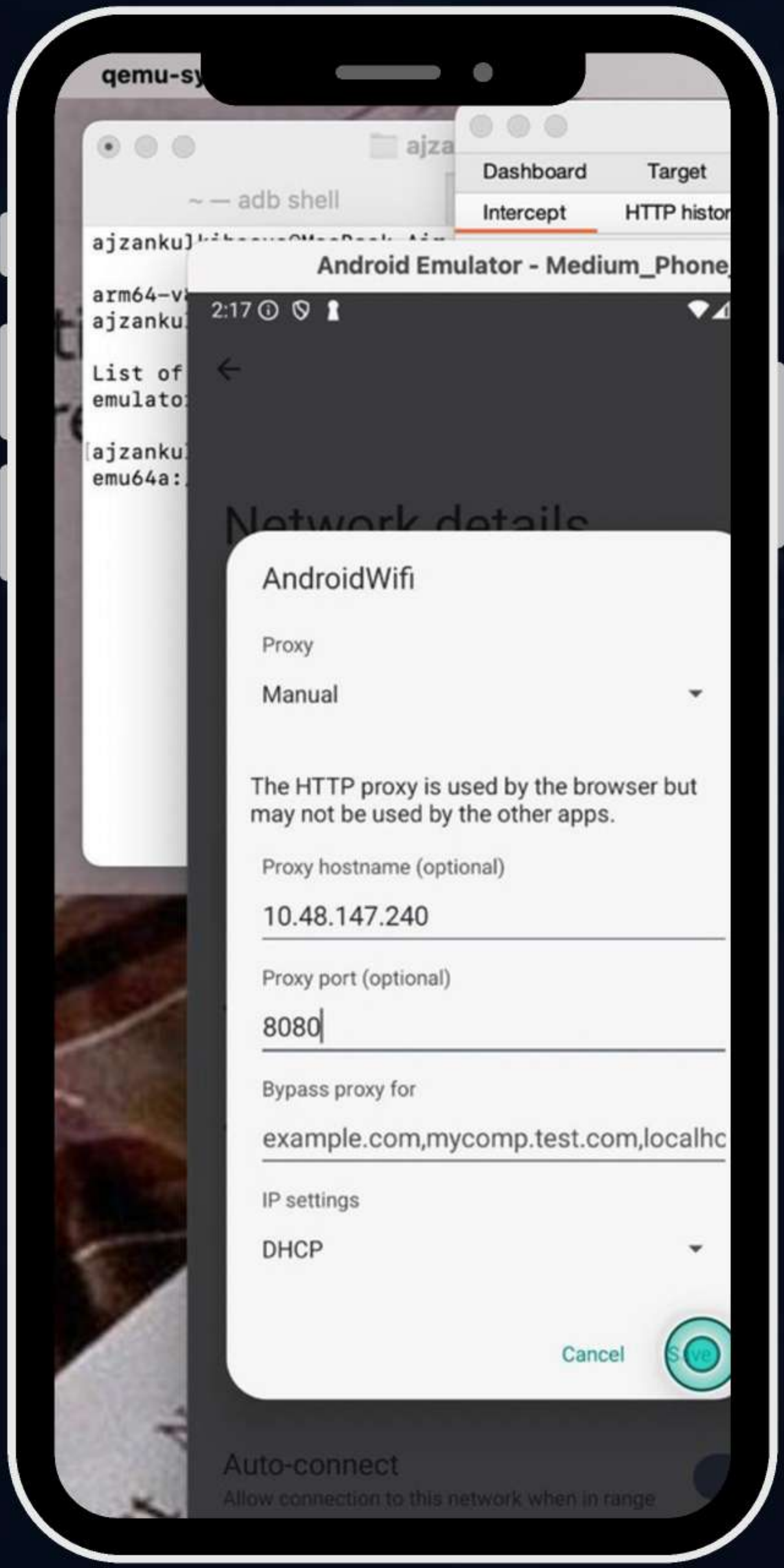
```
/Users/ajzankulkibaeva/Downloads/caace...ipped. 1.6 MB/s (1326 bytes in 0.001s)
ajzankulkibaeva@MacBook-Air-Ajzan Desktop % frida -U -f com.wolt.android -l /Us
rs/ajzankulkibaeva/Desktop/fridascript.js

     ____
    / _  |   Frida 16.7.14 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
   . . . .
   . . . .   Connected to Android Emulator 5554 (id=emulator-5554)
Spawned `com.wolt.android`. Resuming main thread!
[Android Emulator 5554::com.wolt.android ]->
[.] Cert Pinning Bypass/Re-Pinning
[+] Loading our CA...
[o] Our CA Info: CN=PortSwigger CA, OU=PortSwigger CA, O=PortSwigger, L=PortSwi
ger, ST=PortSwigger, C=PortSwigger
[+] Creating a KeyStore for our CA...
[+] Creating a TrustManager that trusts the CA in our KeyStore...
```



This site can't be reached

Check if there is a typo in burp.

DNS_PROBE_FINISHED_NXDOMAIN


Dashboard
Target
Intercept
HTTP histor
Android Emulator - Medium_Phone
2:17
Network details
Cancel
Save
Auto-connect
Allow connection to this network when in range

AndroidWifi

Proxy: Manual

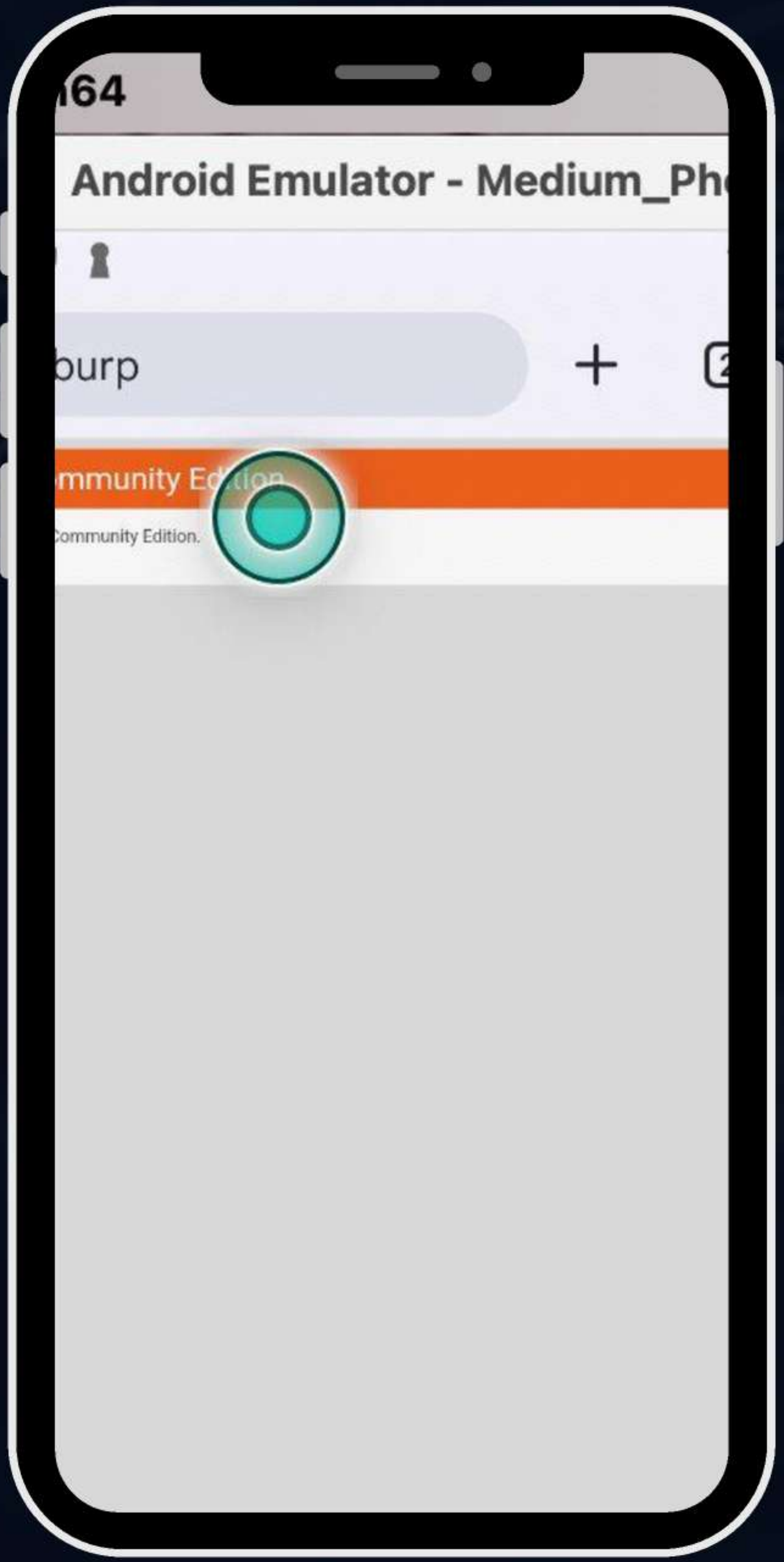
The HTTP proxy is used by the browser but may not be used by the other apps.

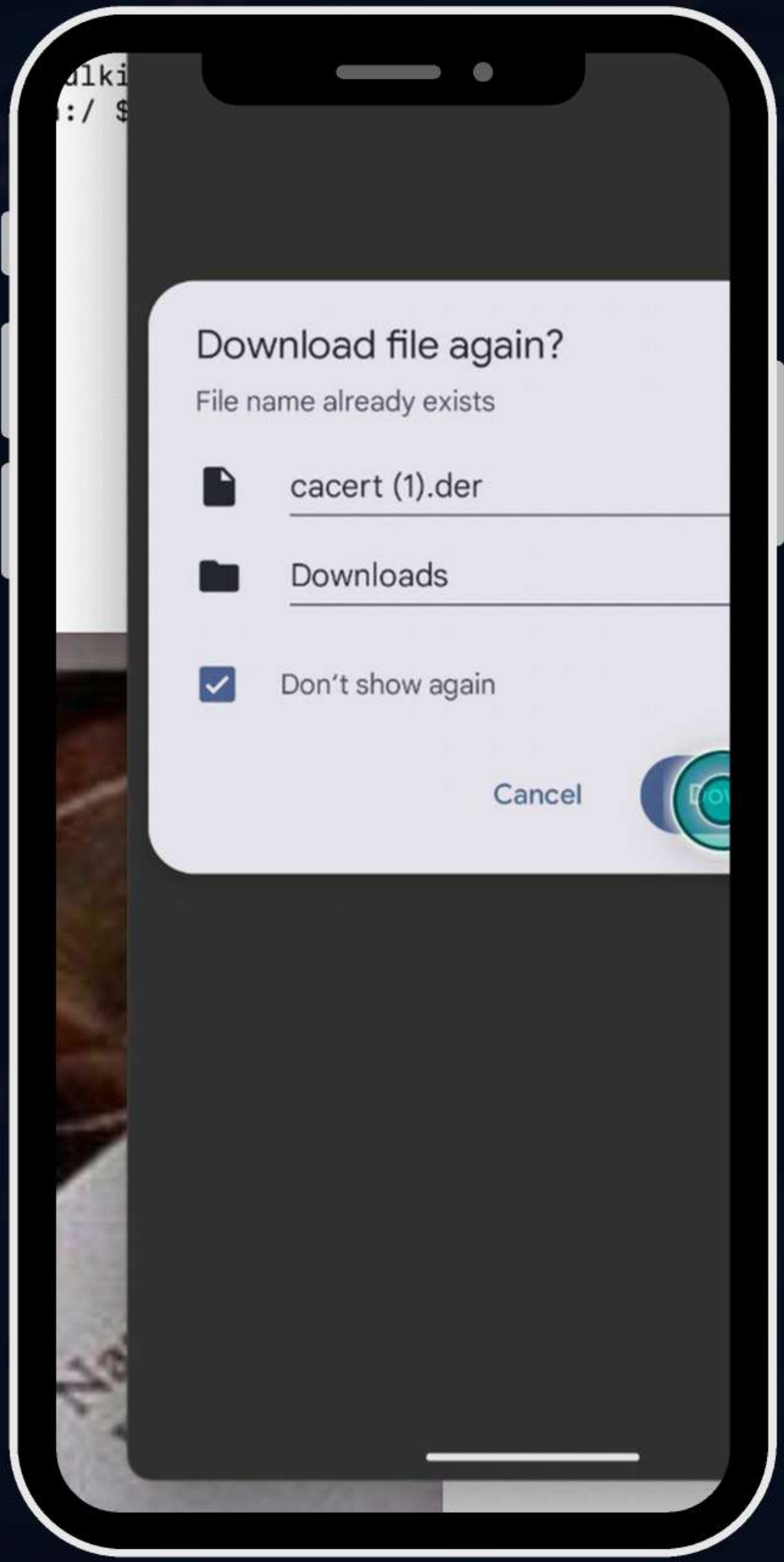
Proxy hostname (optional): 10.48.147.240

Proxy port (optional): 8080

Bypass proxy for: example.com,mycomp.test.com,localhc

IP settings: DHCP





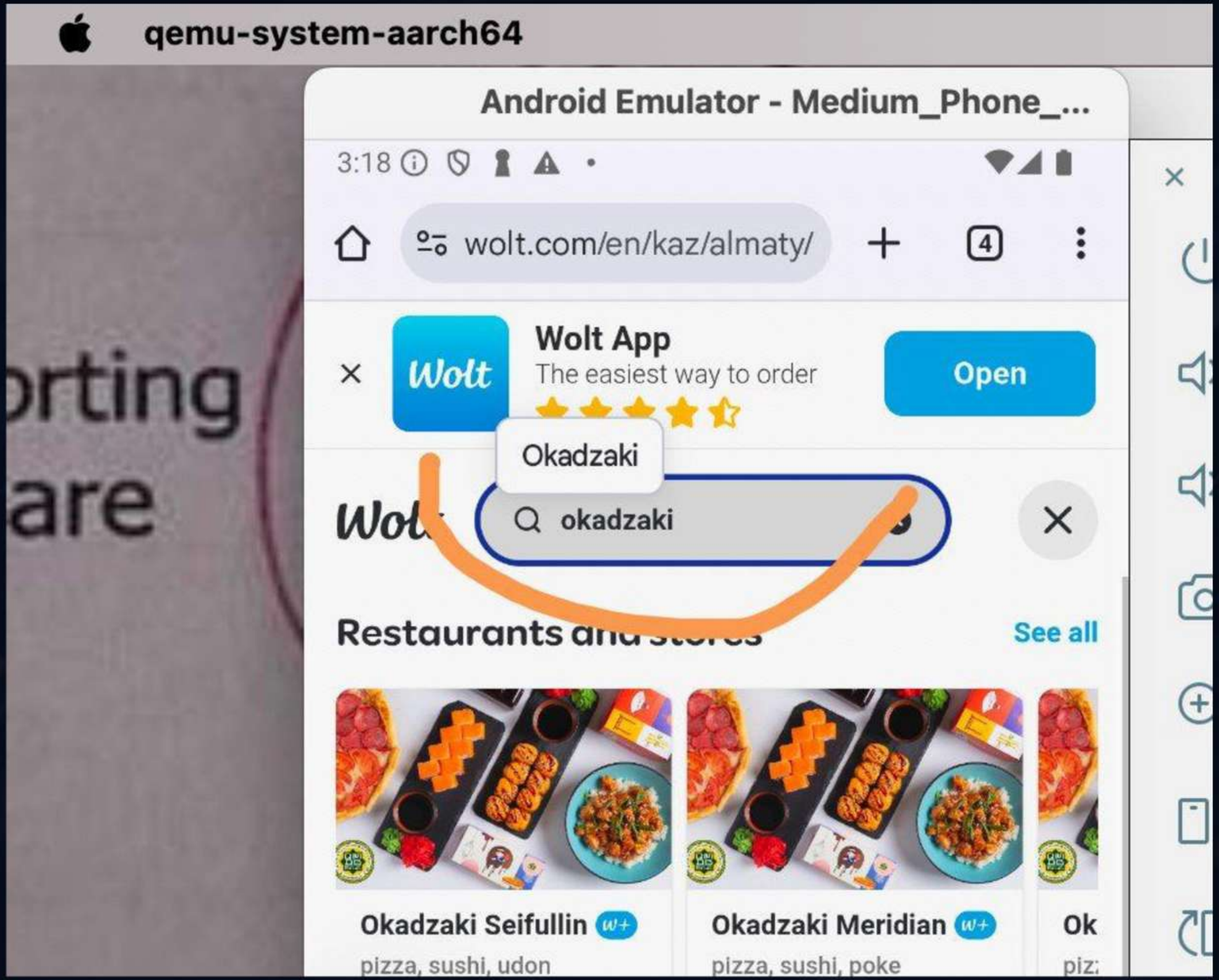
Download file again?

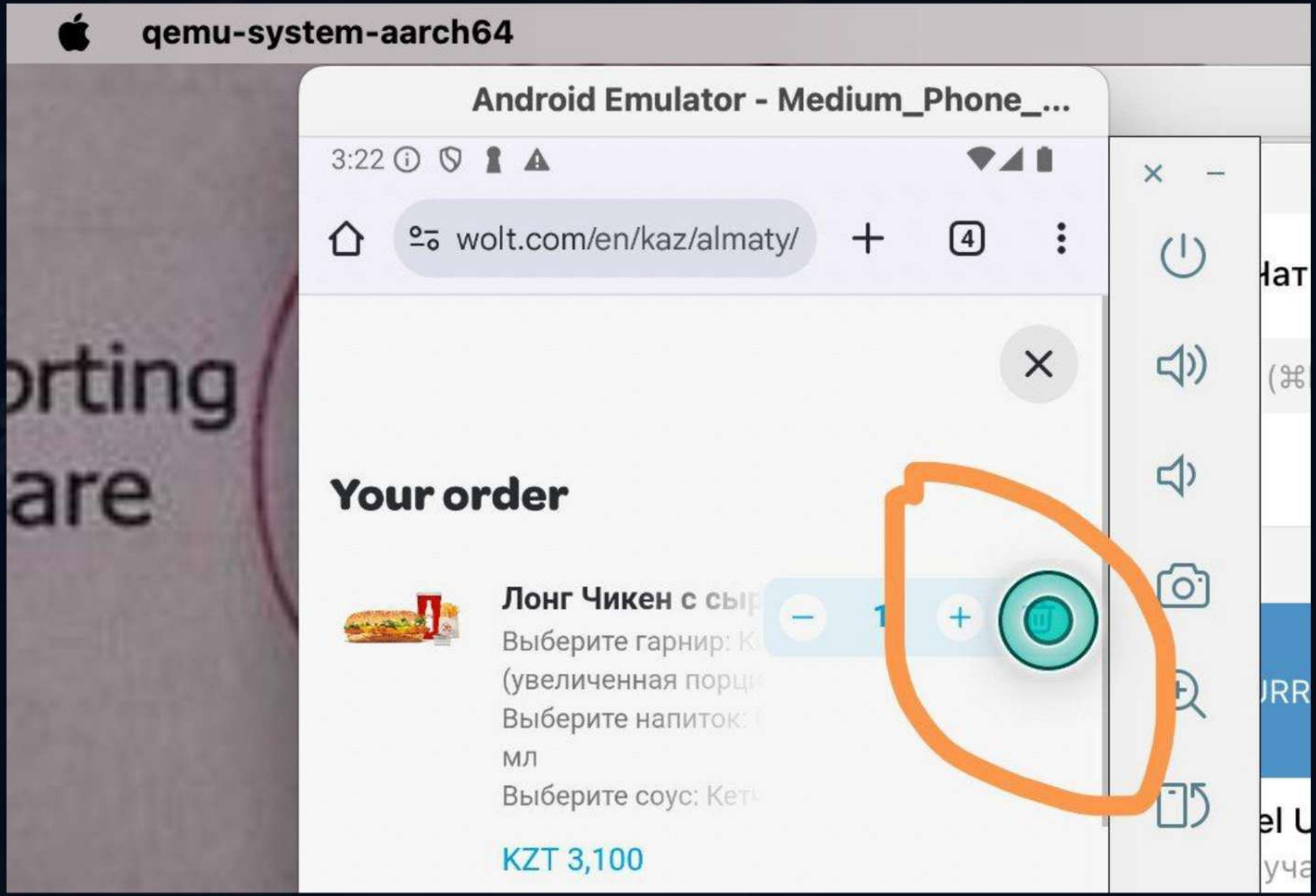
File name already exists

cacert (1).der

Downloads

☑ Don't show again


qemu-system-aarch64
Android Emulator - Medium_Phone_...
3:18
wolt.com/en/kaz/almaty/
4
Wolt App
The easiest way to order
Open
Okadzaki
okadzaki
Restaurants and stores
See all
Okadzaki Seifullin
pizza, sushi, udon
Okadzaki Meridian
pizza, sushi, poke
Ok
piz


qemu-system-aarch64
Android Emulator - Medium_Phone_...
3:22
wolt.com/en/kaz/almaty/
4
Your order
Лонг Чикен с сыр
Выберите гарнир: К
(увеличенная порц
Выберите напиток:
мл
Выберите соус: Кет
1
KZT 3,100

The https://authentication.wolt.com/v1/wauth2/access_token endpoint is used in the OAuth 2.0 authentication flow to obtain access and refresh tokens.

Method: POST

Purpose: Exchange an authorization code for an access token (for API requests) and a refresh token (to renew the access token).

Parameters: grant_type (authorization_code), code (authorization code), redirect_uri (same as used during authorization).

Response: Access token, refresh token, and expiration time.

REQUESTMETHOD: GET
ENDPOINT: /V1/PAGES/RESTAURANTS
QUERY PARAMETERS:

LAT=43.245132
LON=76.954158

PURPOSE

- FETCH A LIST OF RESTAURANTS NEAR THE PROVIDED COORDINATES.