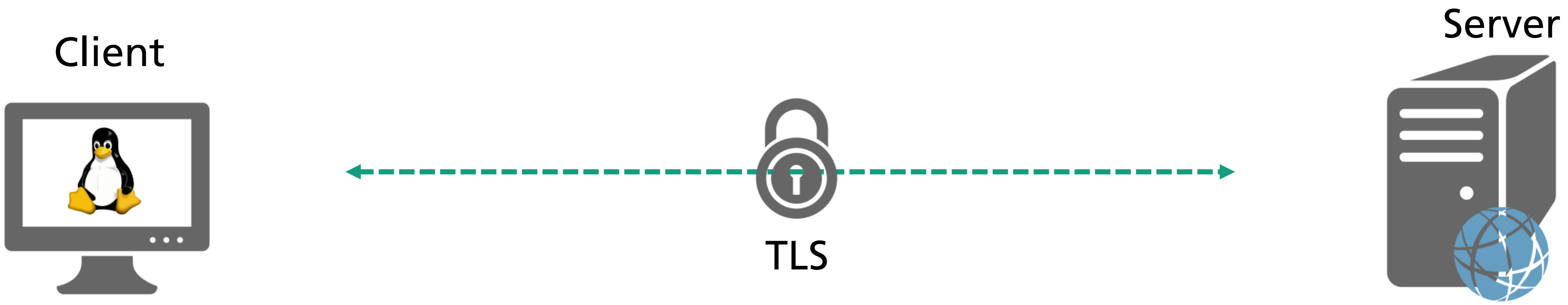
Fraunhofer
FKIE

Daniel Baier & Max Ufer

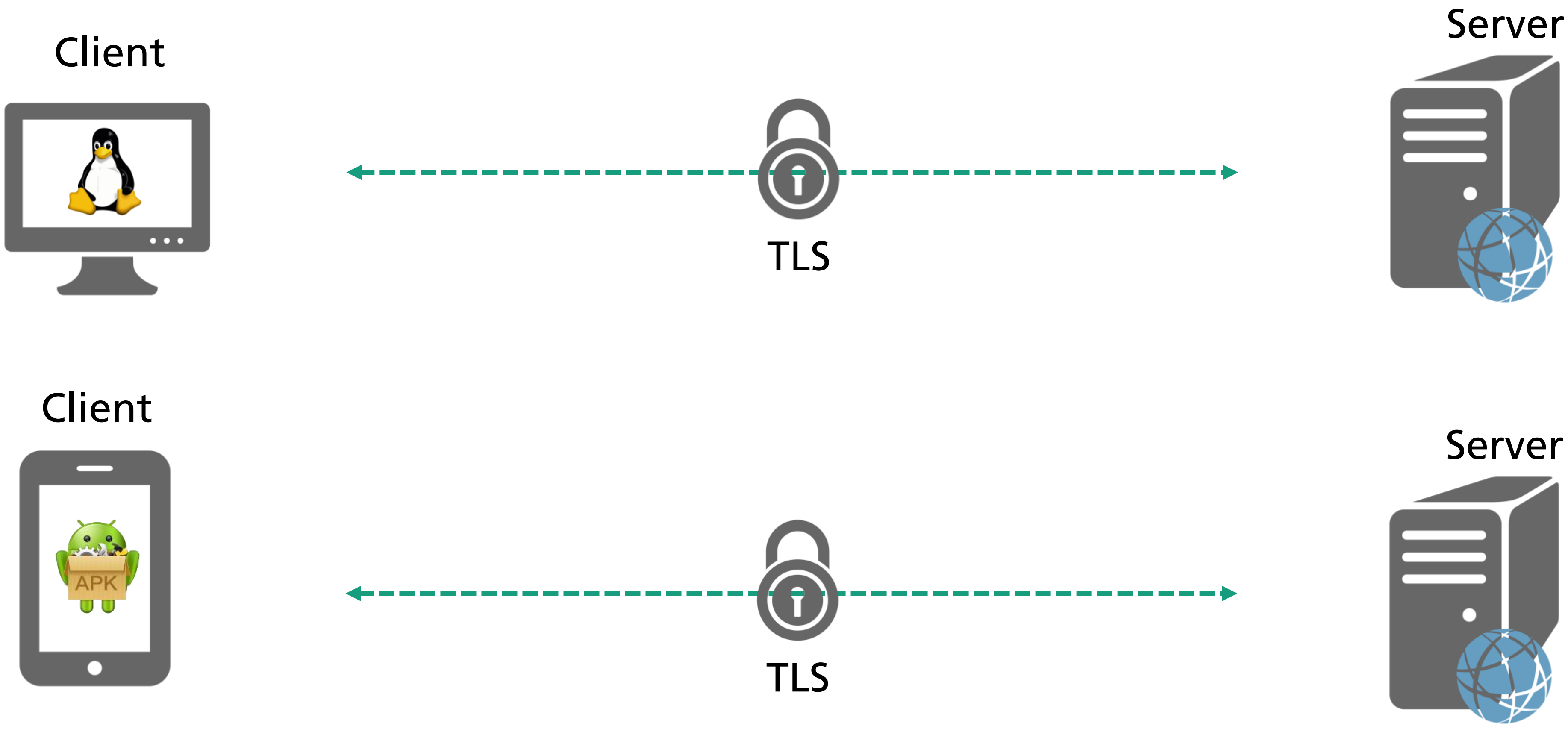
friTap: Decrypting TLS on the fly

Is a MitM-Proxy enough?



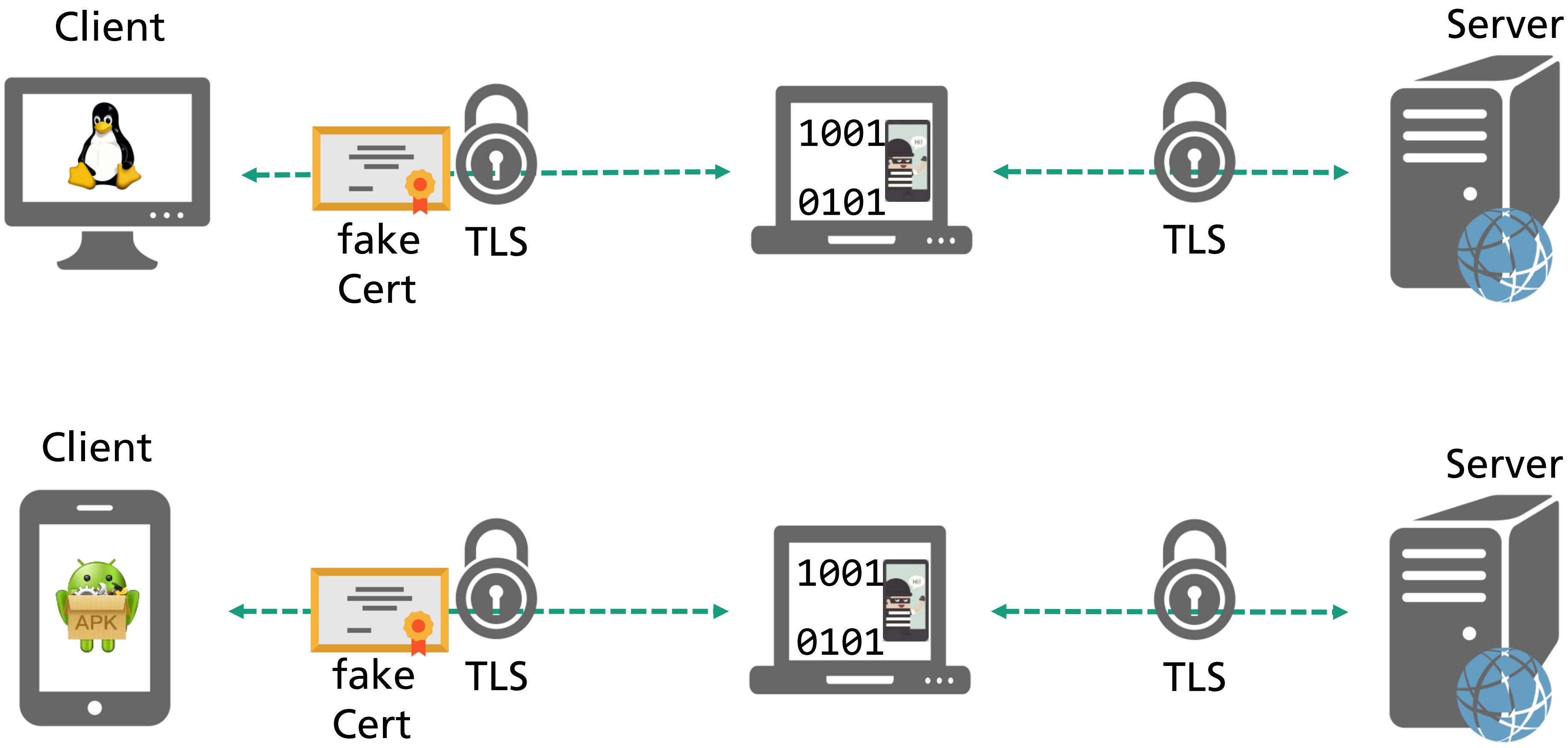
Is a MitM-Proxy enough?

TLS without any attack



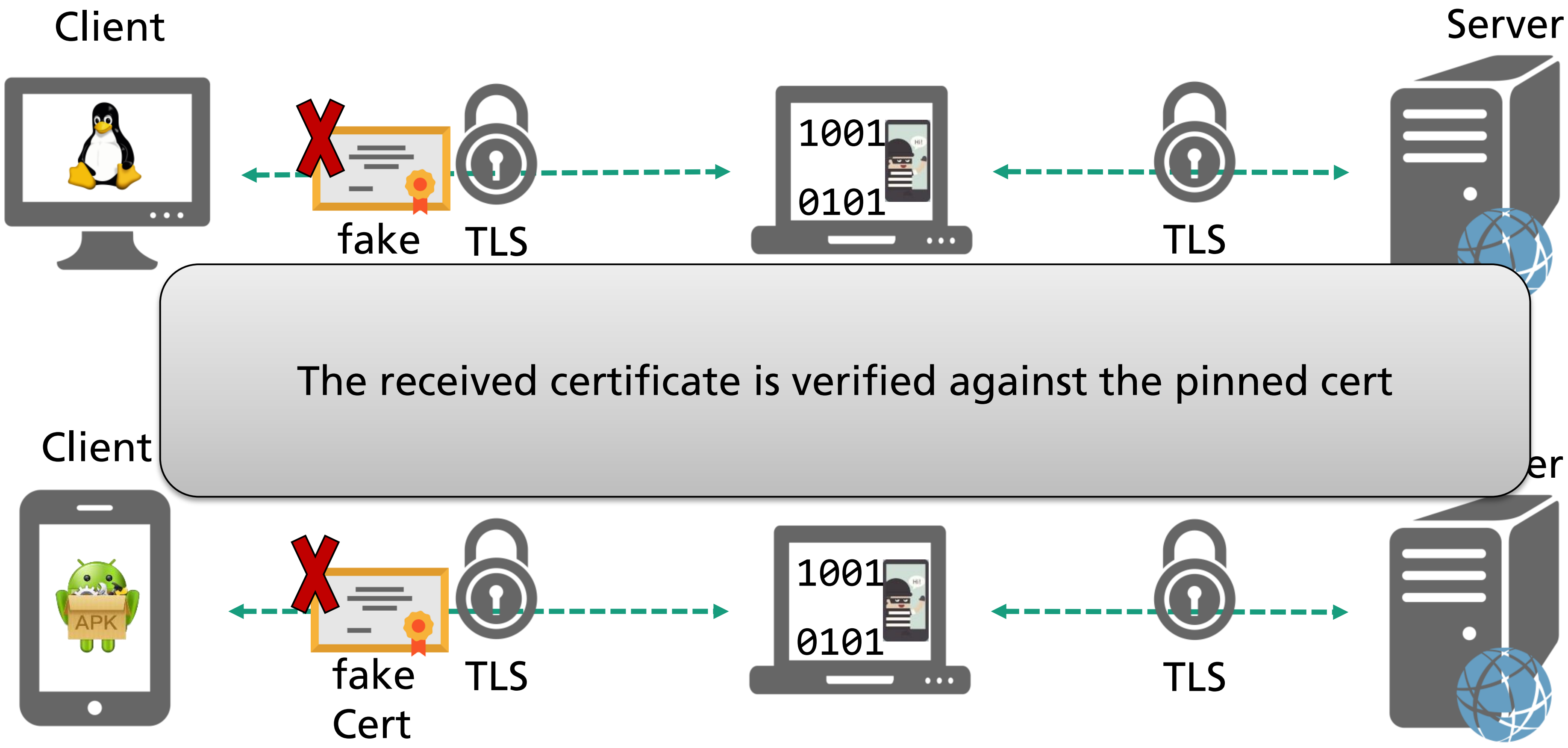
Is a MitM-Proxy enough?

DH-Attack with fake Cert



Is a MitM-Proxy enough?

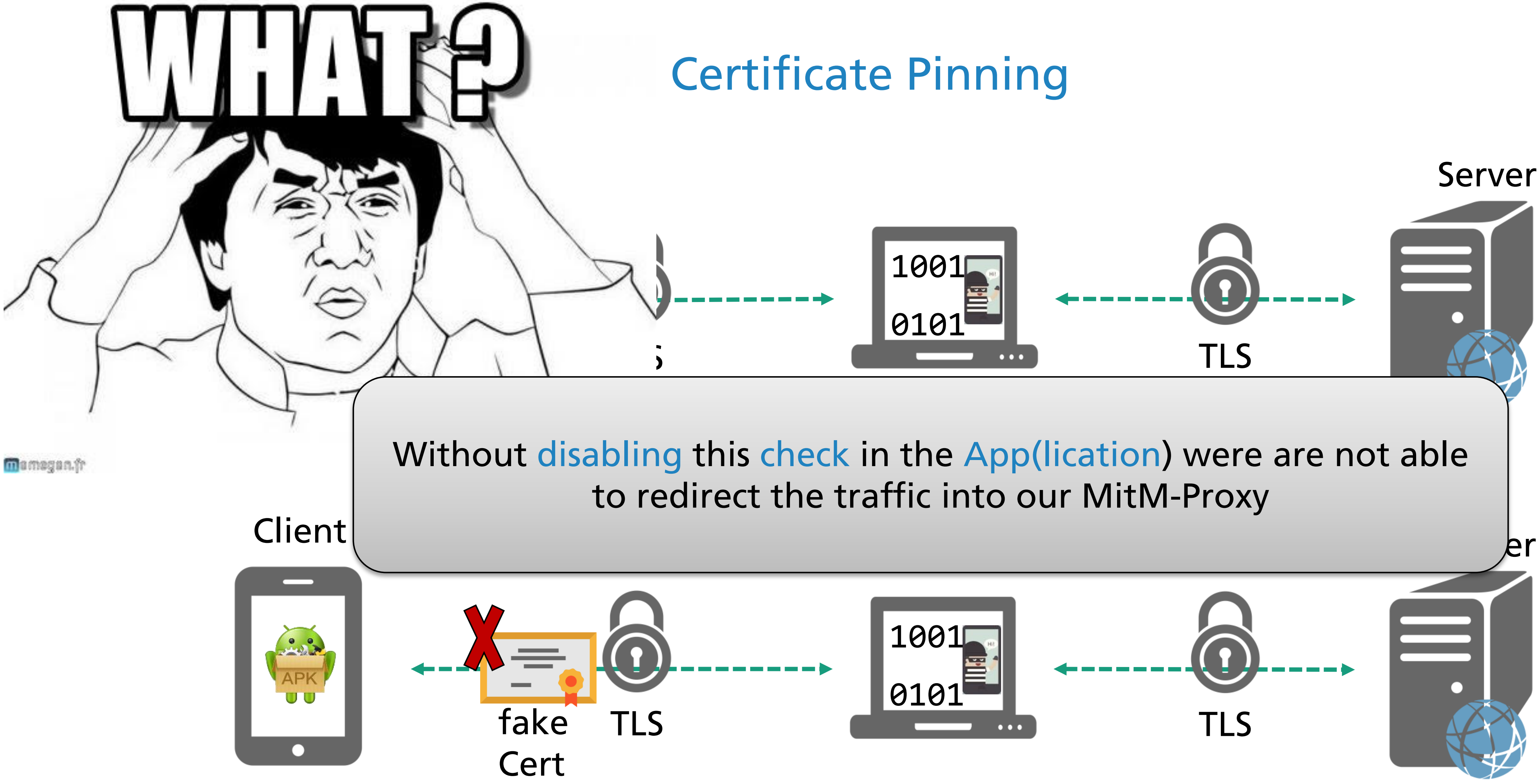
Certificate Pinning



The received certificate is verified against the pinned cert

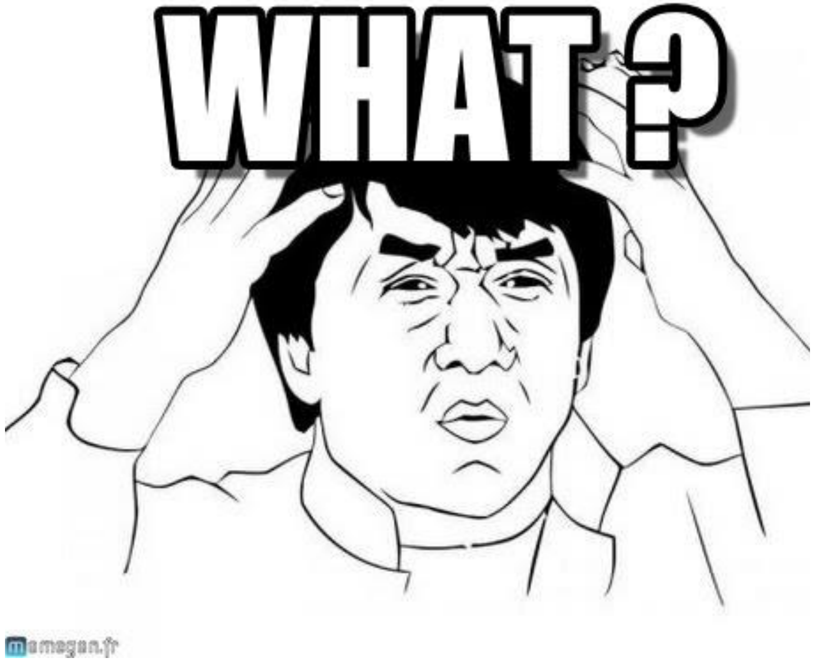
MitM-Proxy is not enough

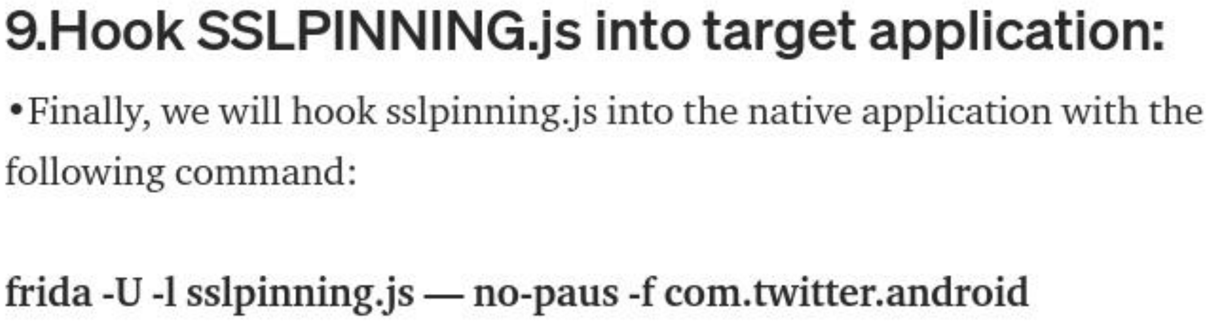
Certificate Pinning



Without disabling this check in the App(lication) were are not able to redirect the traffic into our MitM-Proxy

Solution: Disable the check

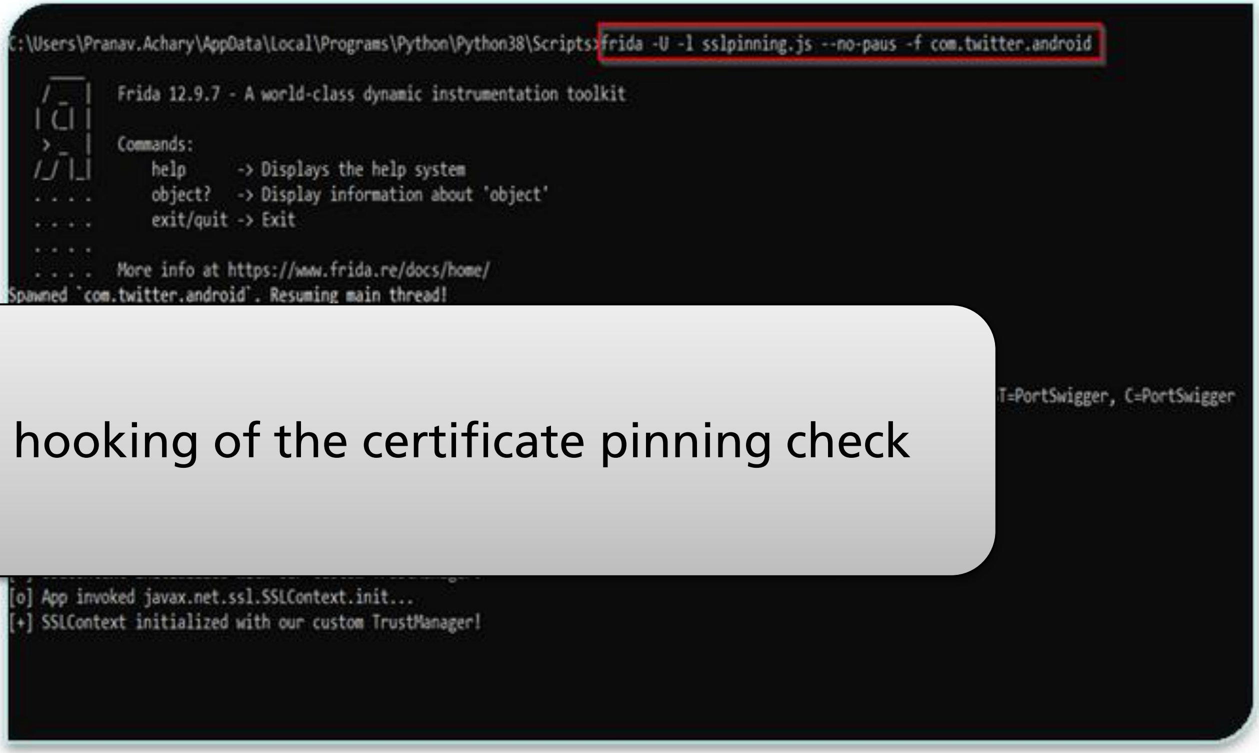




9.Hook SSLPINNING.js into target application:

- Finally, we will hook sslpinning.js into the native application with the following command:

frida -U -l sslpinning.js — no-paus -f com.twitter.android



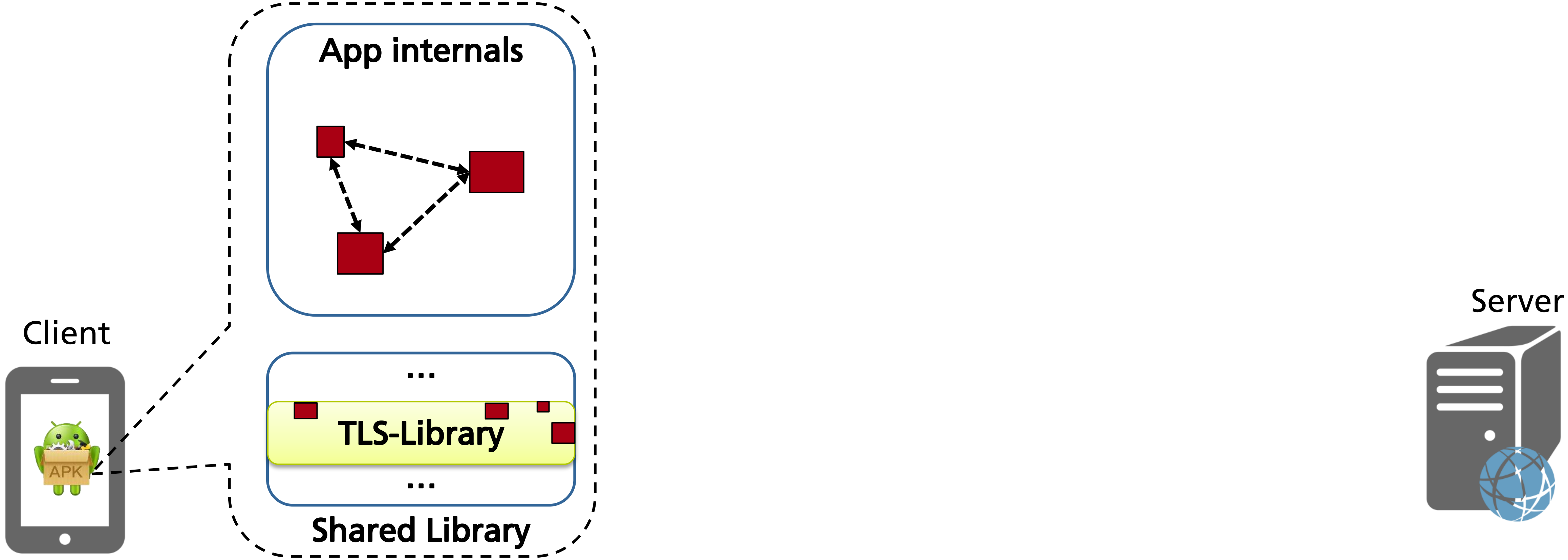
```
C:\Users\Pranav.Achary\AppData\Local\Programs\Python\Python38\Scripts>frida -U -l sslpinning.js --no-paus -f com.twitter.android
     ____
    / _  |   Frida 12.9.7 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://www.frida.re/docs/home/
Spawned `com.twitter.android`. Resuming main thread!
                                                                                   T=PortSwigger, C=PortSwigger
[o] App invoked javax.net.ssl.SSLContext.init...
[+] SSLContext initialized with our custom TrustManager!
```

We have to apply some hooking of the certificate pinning check

When we have to „attack“ the App why not directly extract the payload of the TLS-stream?

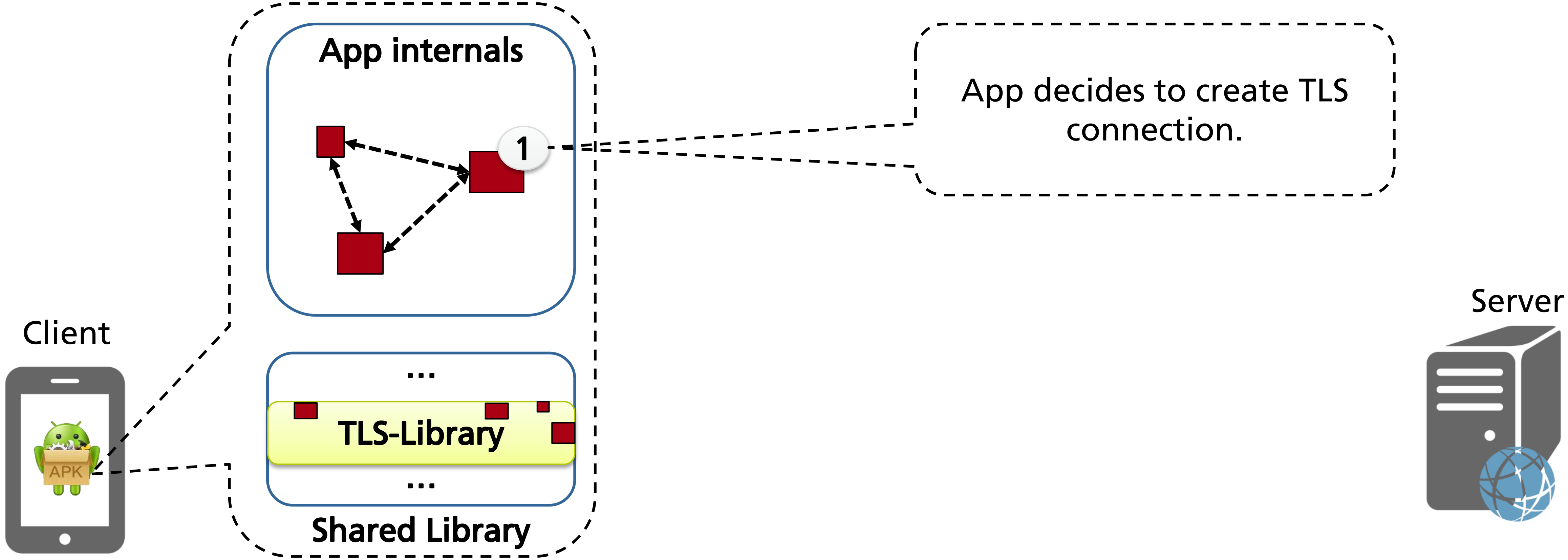
friTap: Approach

A TLS-stream offers the application to write its decrypted value to it ....



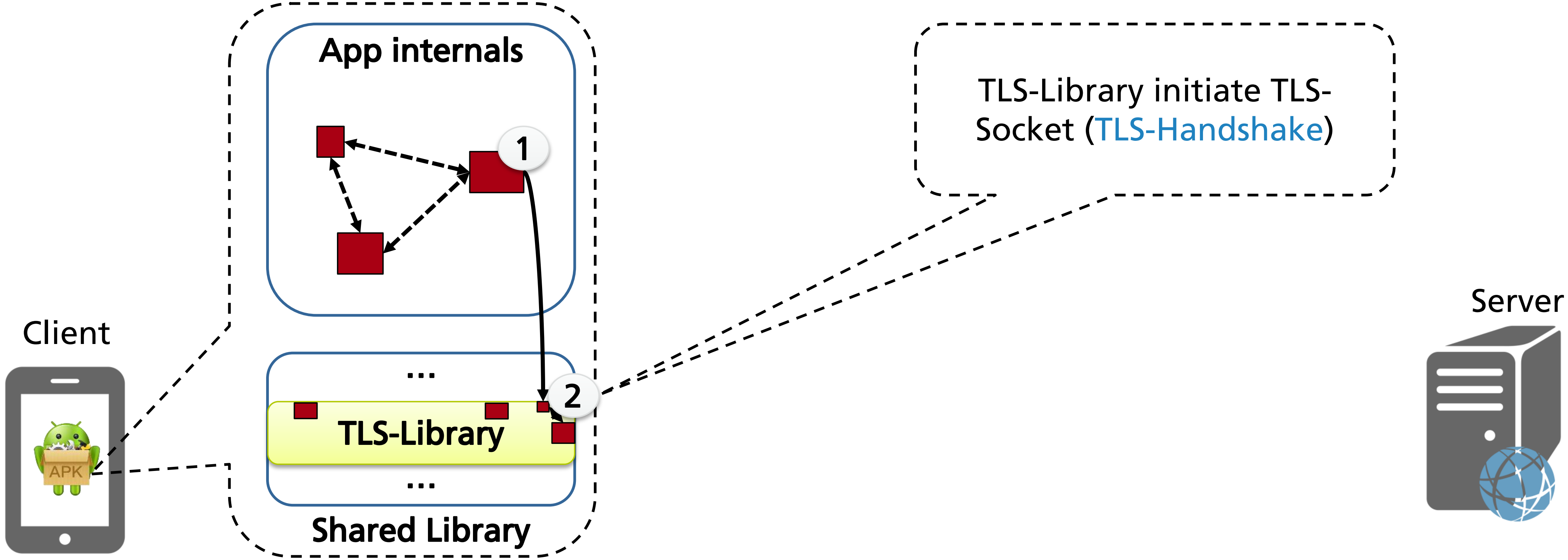
friTap: Approach

A TLS-stream offers the application to write its decrypted value to it ....



friTap: Approach

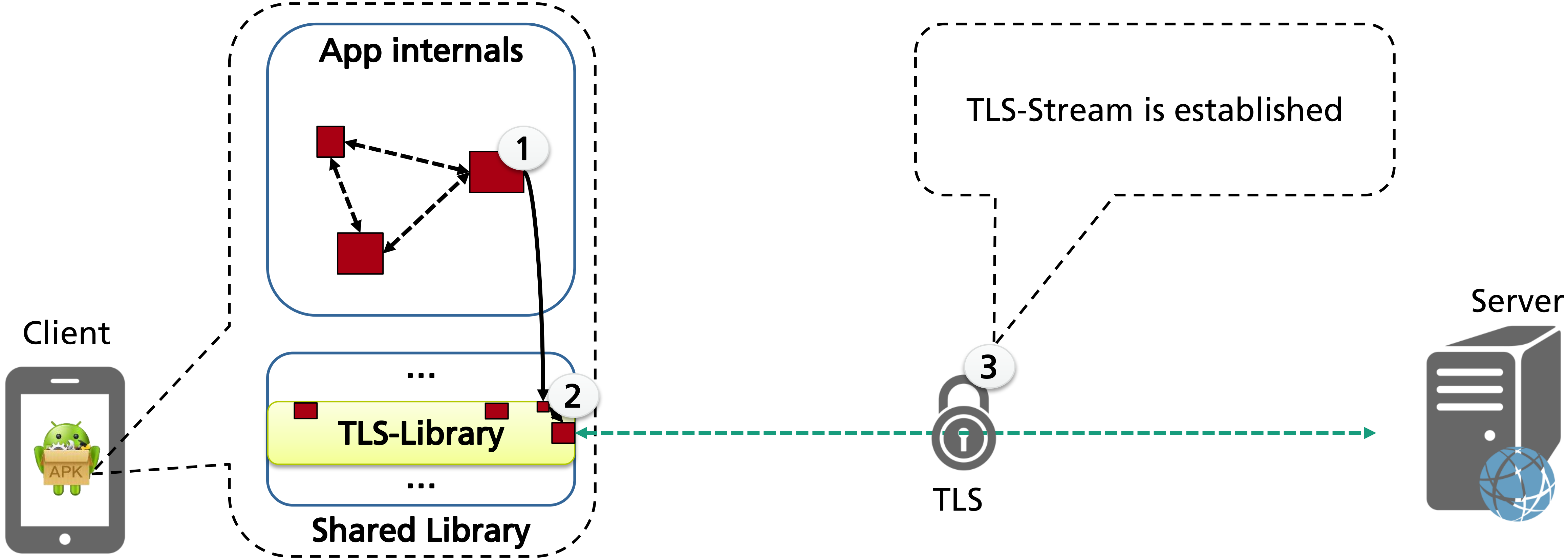
A TLS-stream offers the application to write its decrypted value to it ....



TLS-Library initiate TLS-Socket (TLS-Handshake)

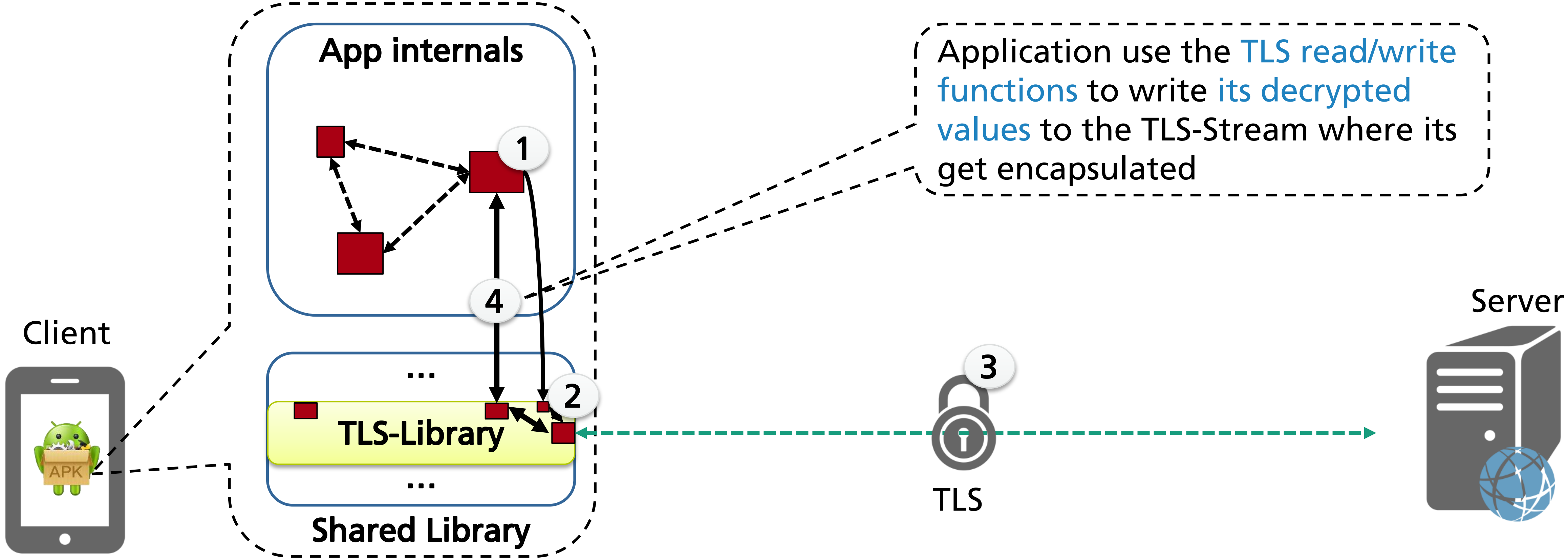
friTap: Approach

A TLS-stream offers the application to write its decrypted value to it ....



friTap: Approach

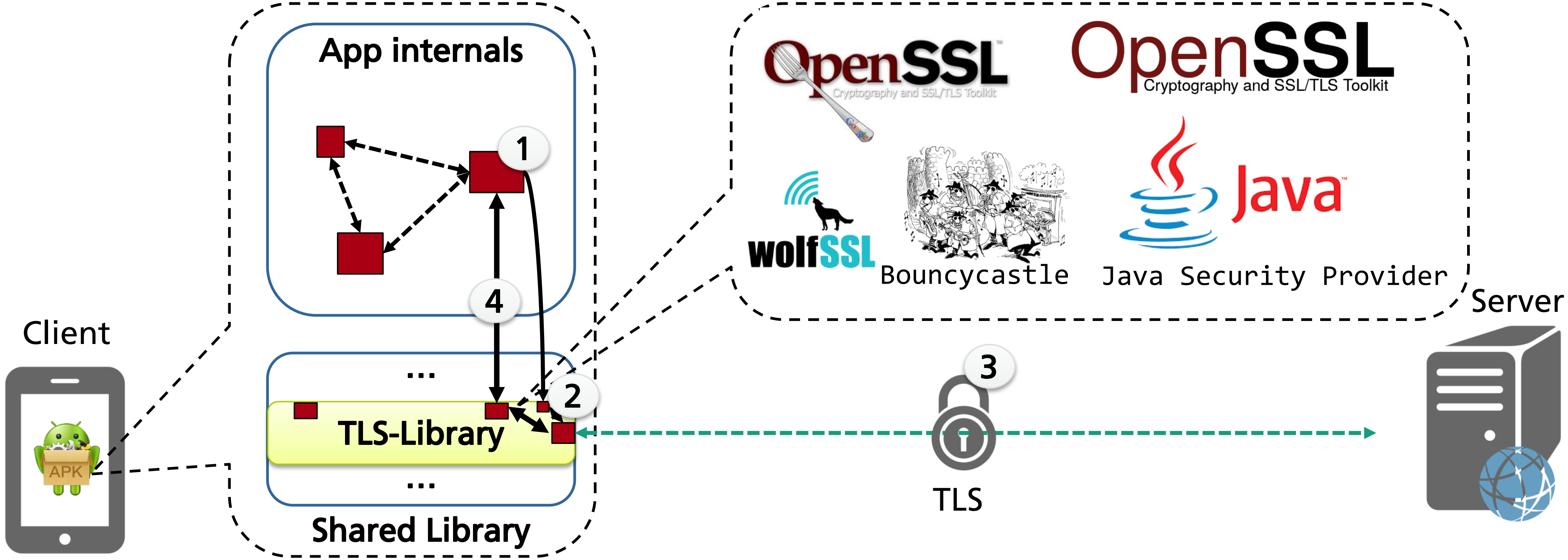
A TLS-stream offers the application to write its decrypted value to it ….



Application use the TLS read/write functions to write its decrypted values to the TLS-Stream where its get encapsulated

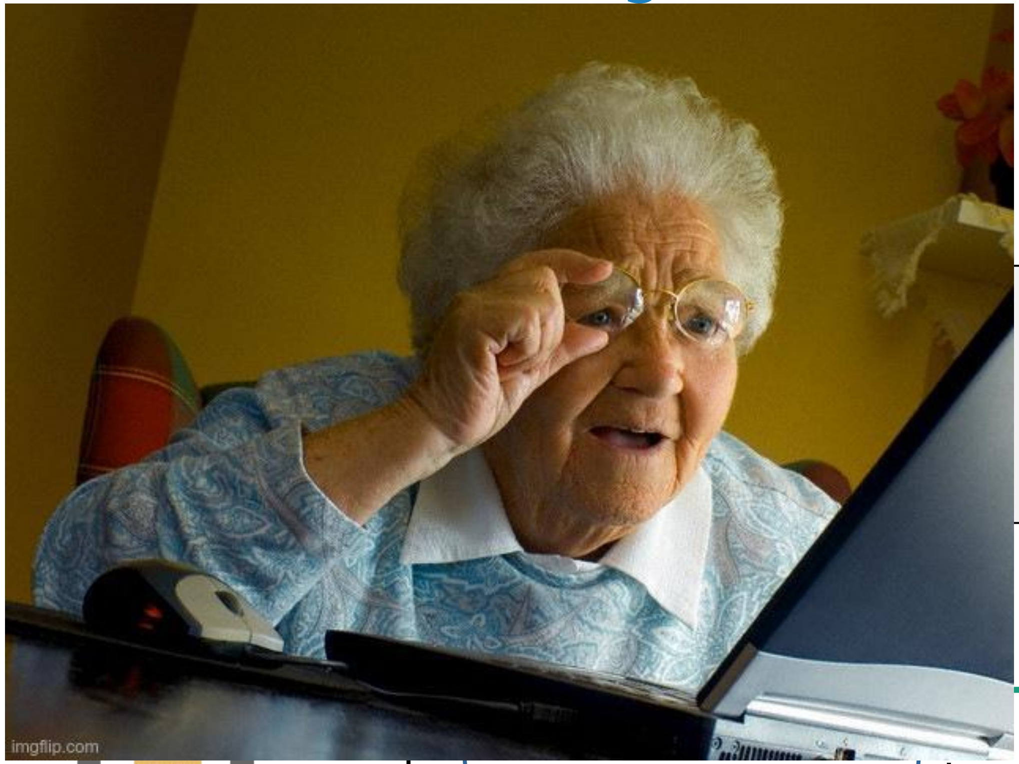
friTap: Approach

Hooking the TLS read/write functions of the TLS library



friTap: What else?

Hooking the TLS functions of the TLS-library to extract TLS-Keys

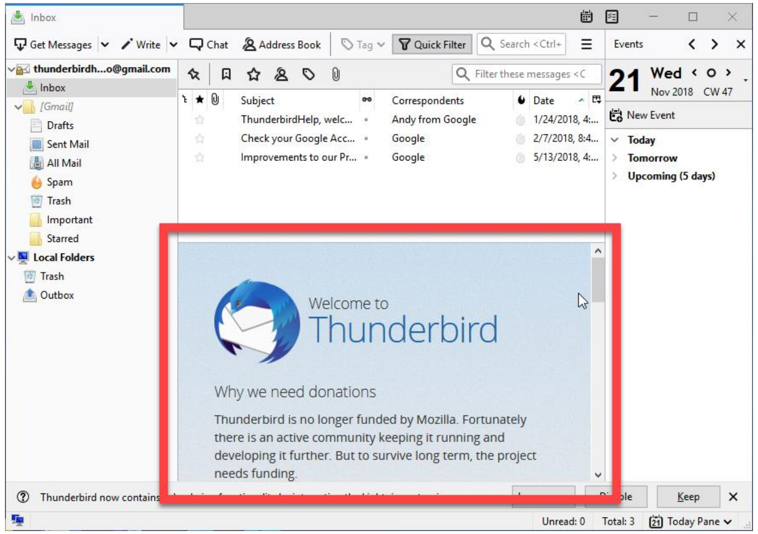


THE SSLKEYLOG-file can also be logged. SSL-Libraries offers ways to write the used keys into a file which can later on used by Wireshark to decrypt the captured traffic.

...
Shared Library
3
TLS

Demo

Thunderbird



Subject	Correspondents	Date
ThunderbirdHelp, welc...	Andy from Google	1/24/2018, 4:...
Check your Google Acc...	Google	2/7/2018, 8:4...
Improvements to our Pr...	Google	5/13/2018, 4:...

Welcome to Thunderbird

Why we need donations

Thunderbird is no longer funded by Mozilla. Fortunately there is an active community keeping it running and developing it further. But to survive long term, the project needs funding.

Thunderbird now contains

Demo

- Different Android APKs from the Playstore

Google Play

Future Work

There is still a lot of work to do….

- Add fully Linux support
- Support for other Operating Systems
- Capturing all traffic of an Application directly with friTap