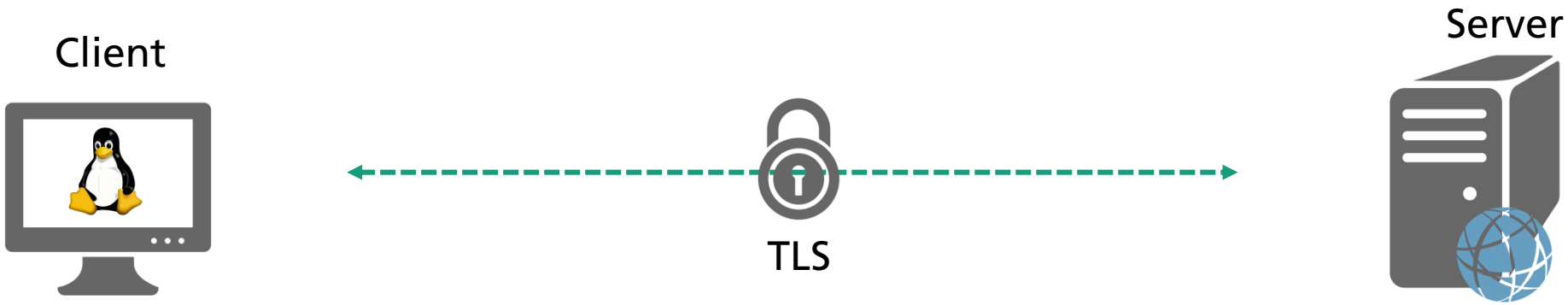
Fraunhofer
FKIE

Daniel Baier & Max Ufer

friTap: Decrypting TLS on the fly

Fraunhofer FKIE

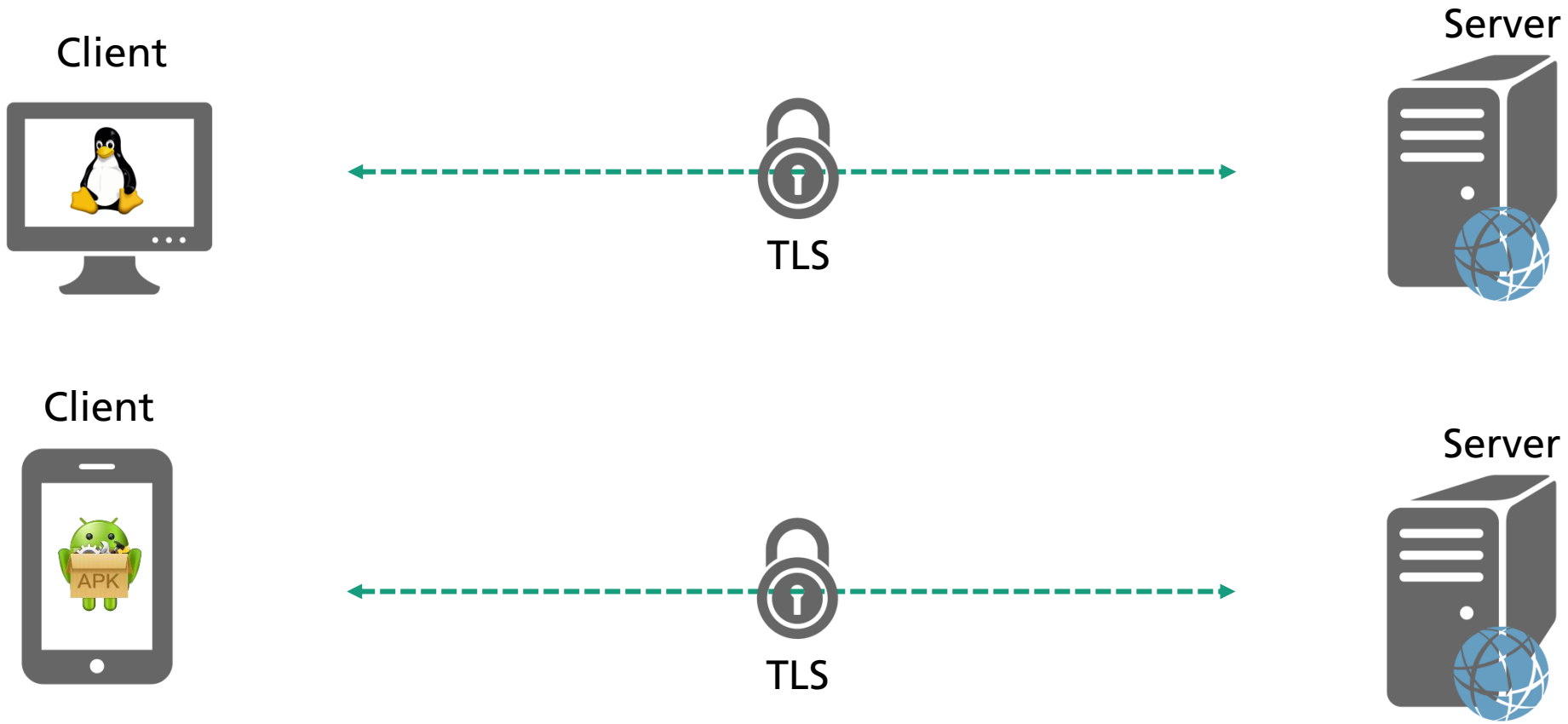
Is a MitM-Proxy enough?



Fraunhofer FKIE

Is a MitM-Proxy enough?

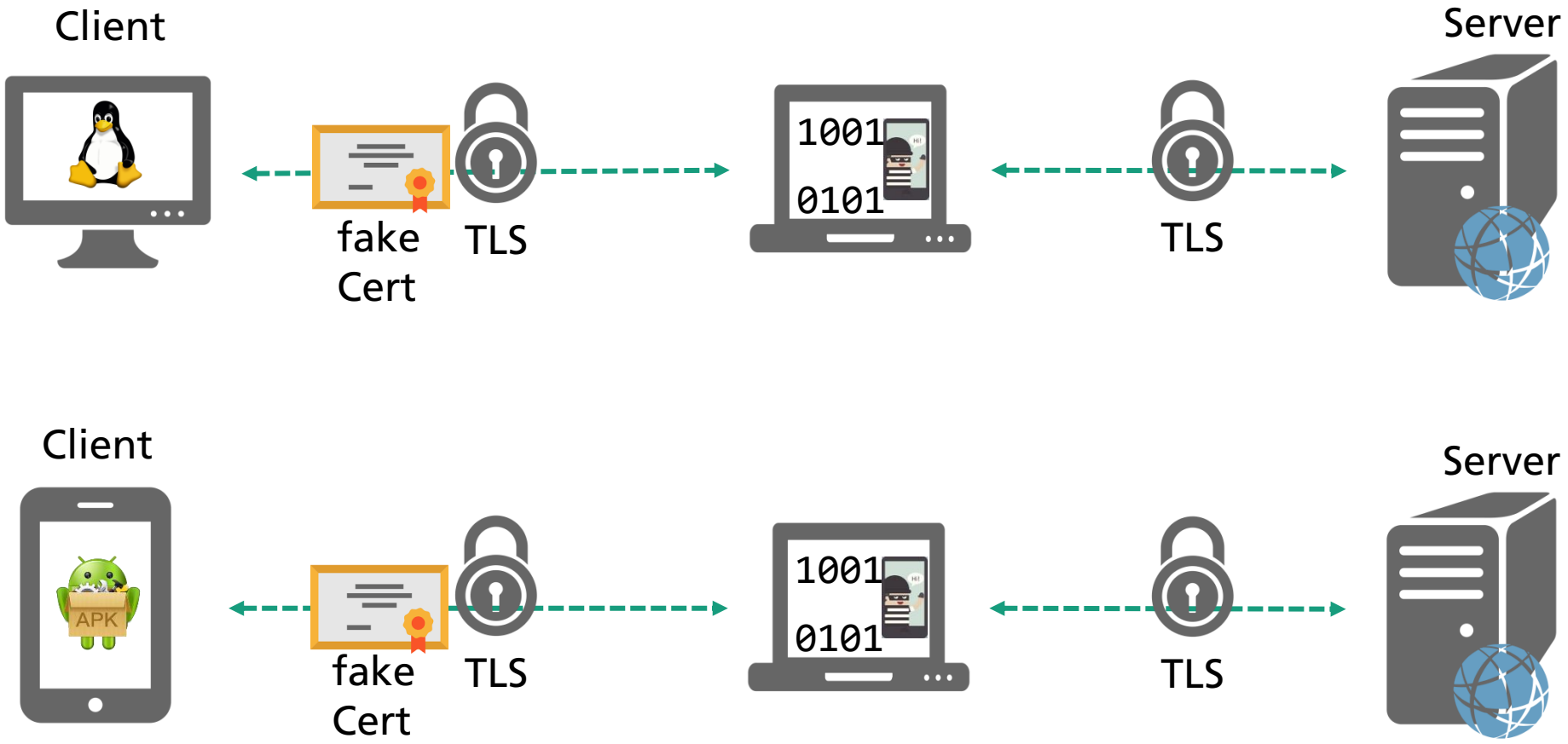
TLS without any attack



Fraunhofer FKIE

Is a MitM-Proxy enough?

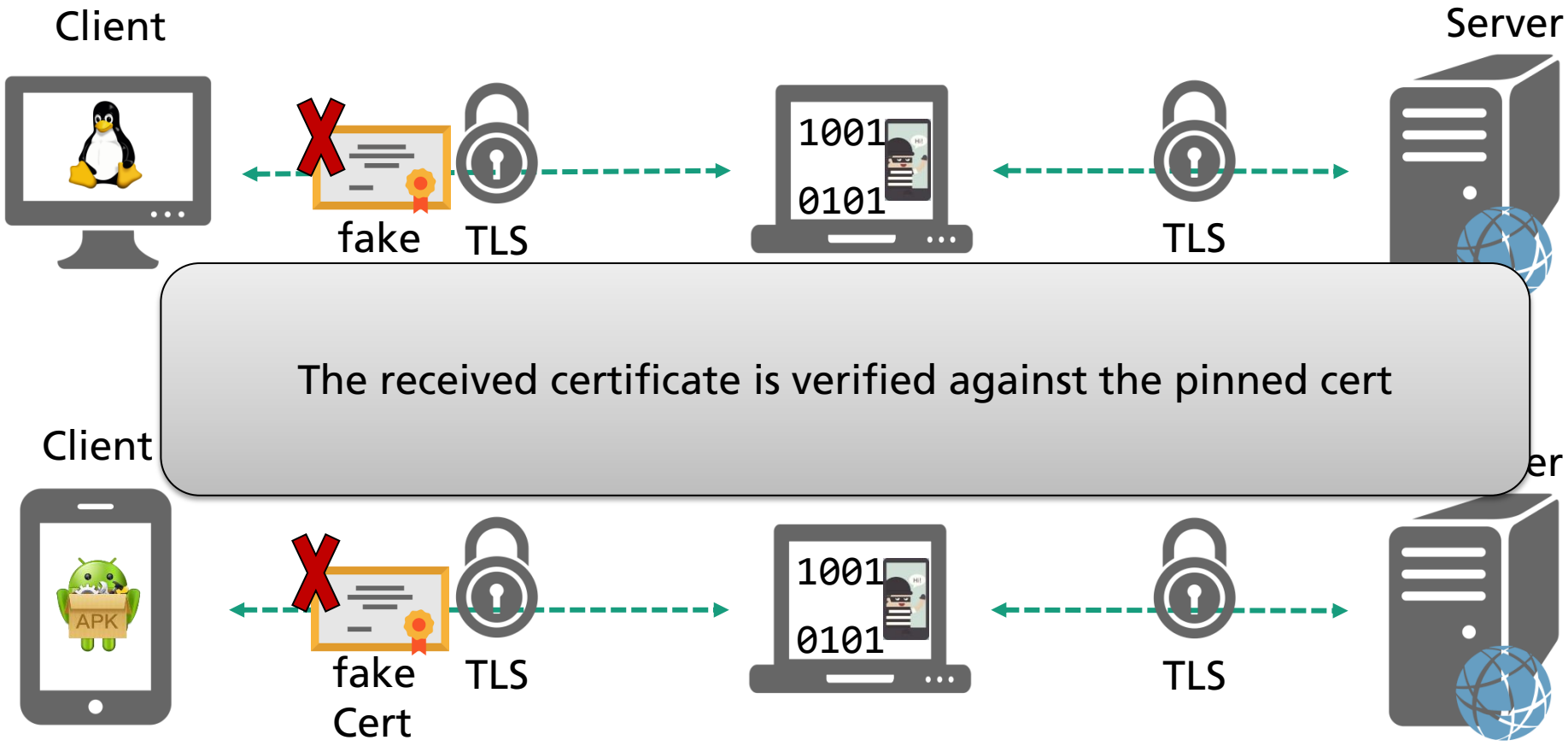
DH-Attack with fake Cert



Fraunhofer FKIE

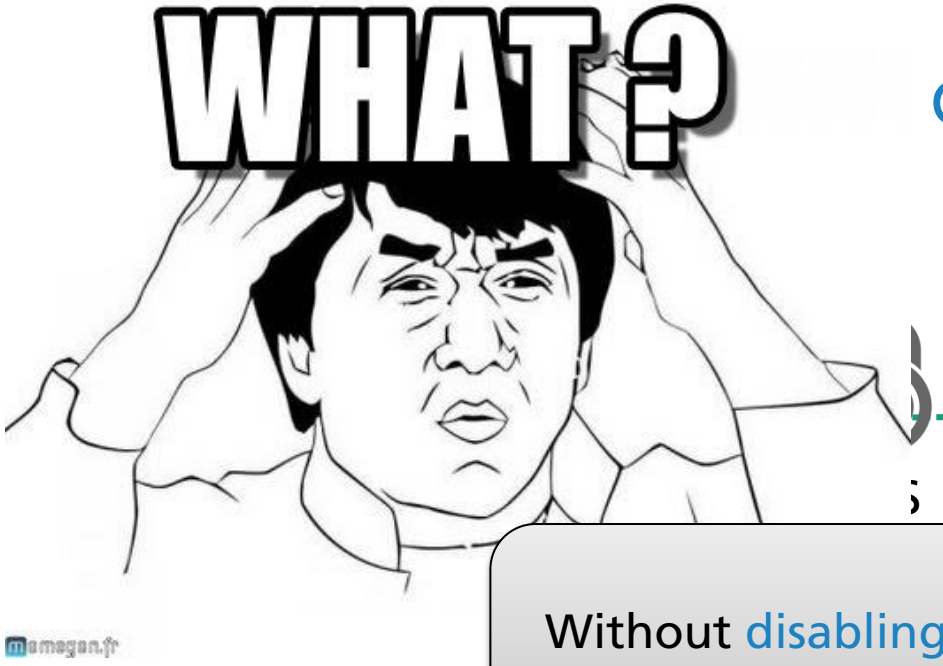
Is a MitM-Proxy enough?

Certificate Pinning

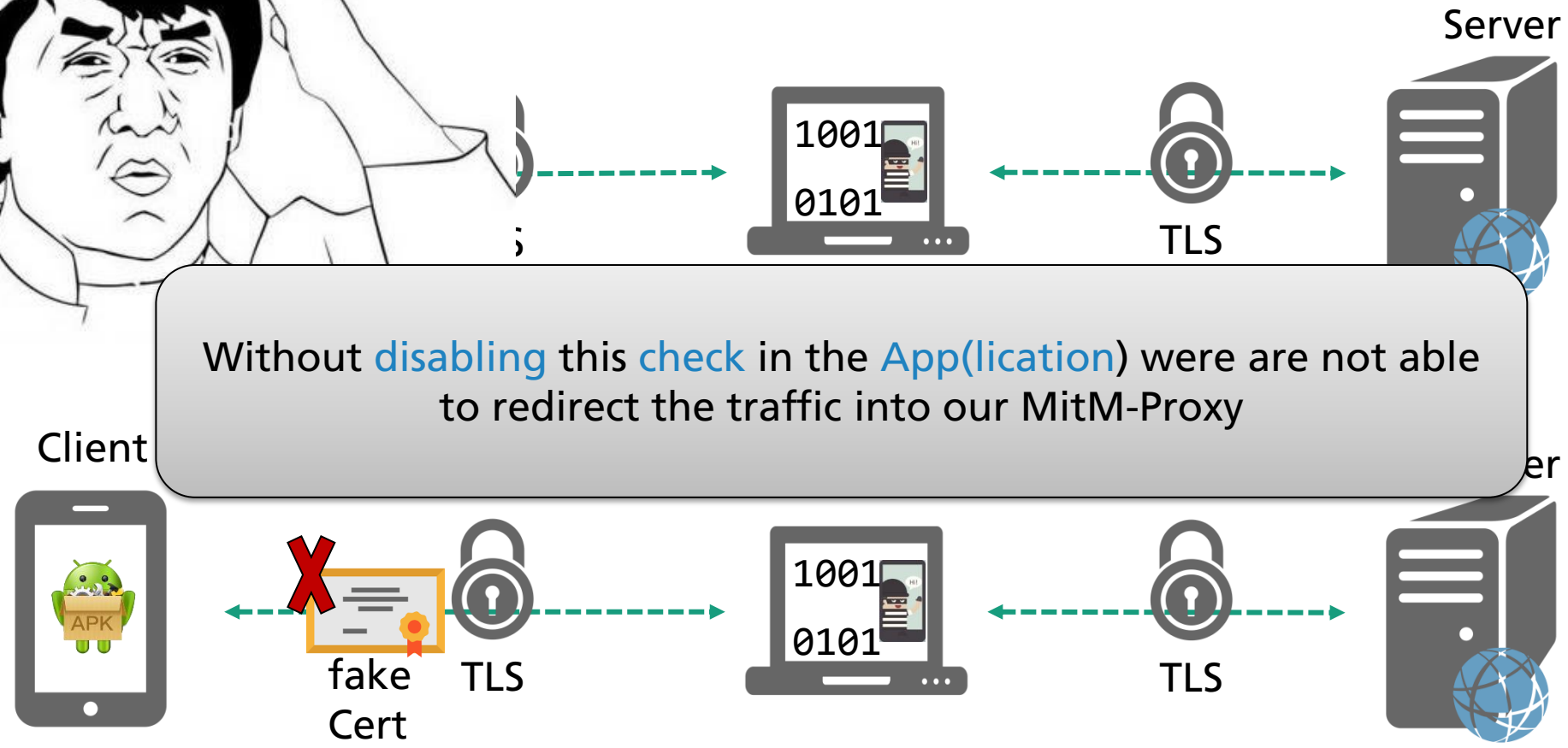


Fraunhofer FKIE

MitM-Proxy is not enough

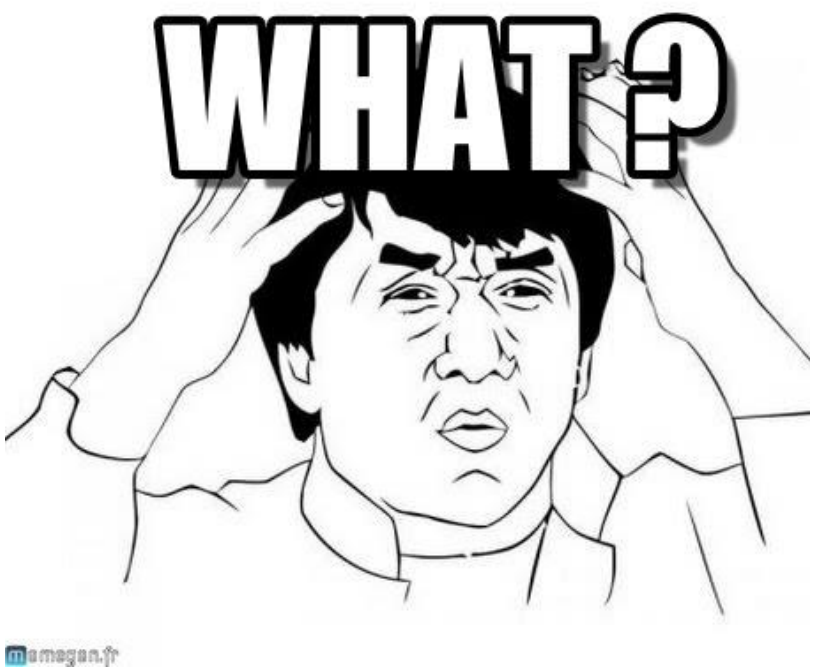


Certificate Pinning



Fraunhofer FKIE

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

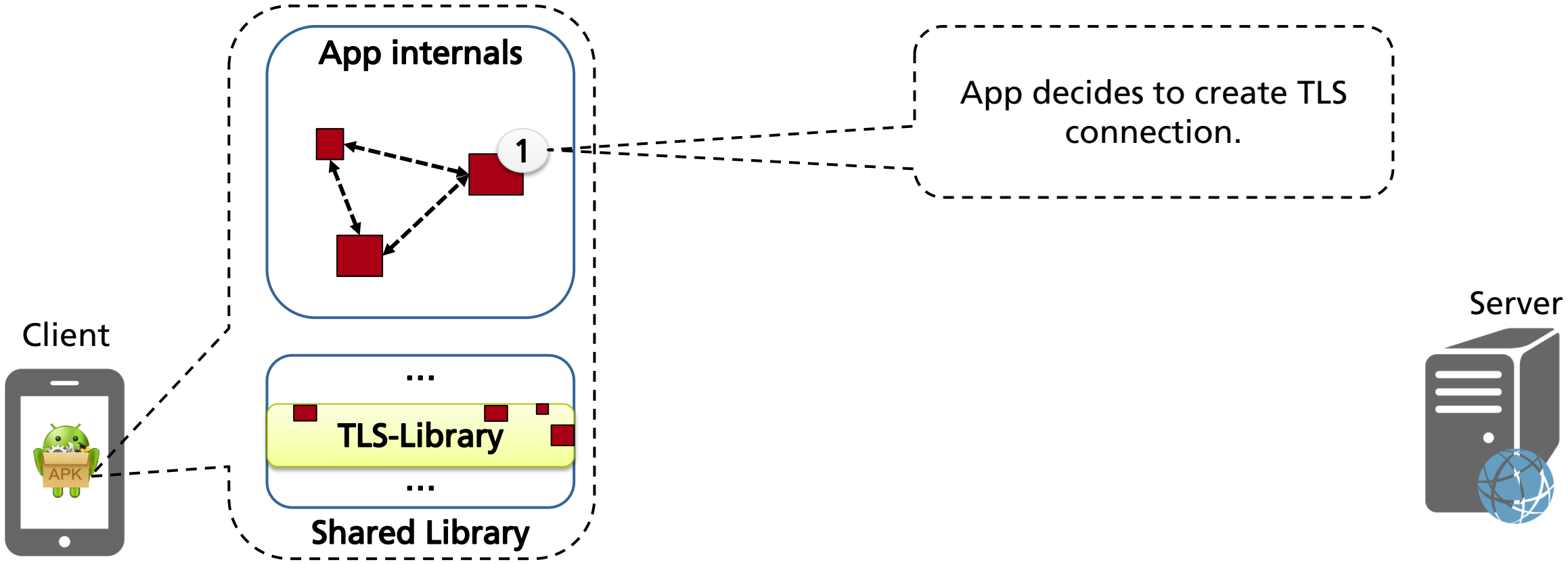
fake Cert

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

Fraunhofer FKIE

friTap: Approach

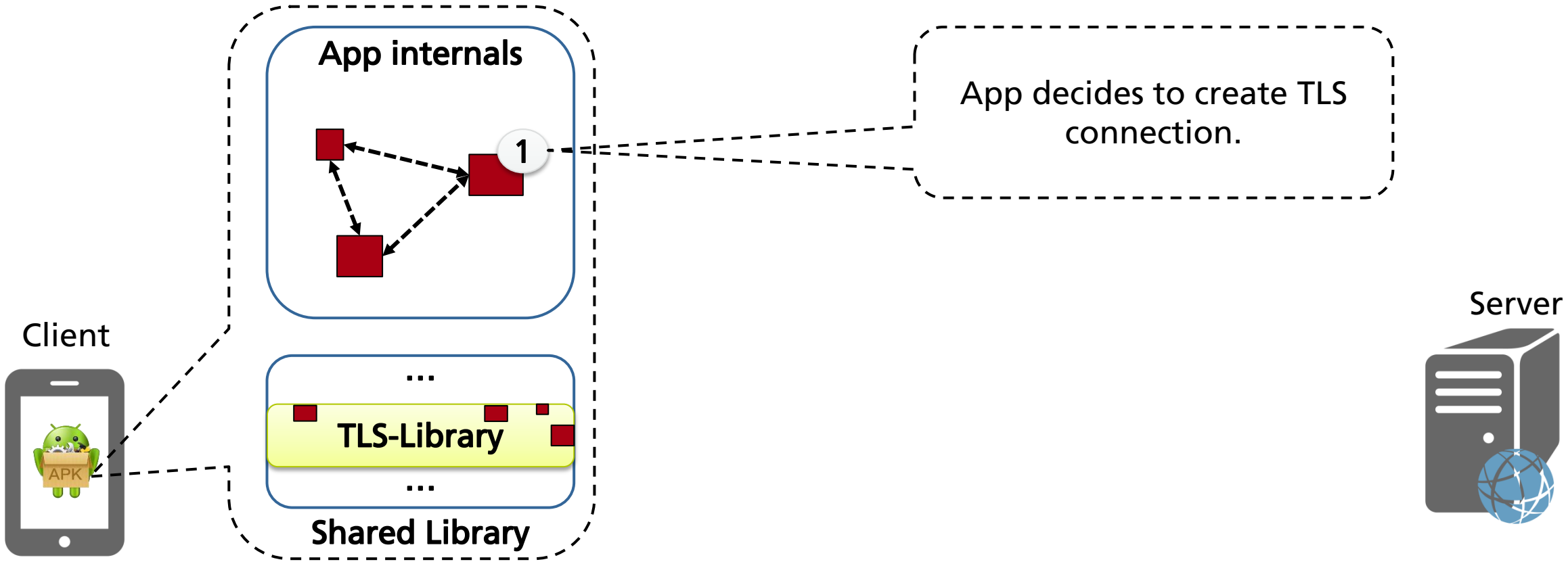
A TLS-stream offers the application to write its decrypted value to it ....



Fraunhofer FKIE

friTap: Approach

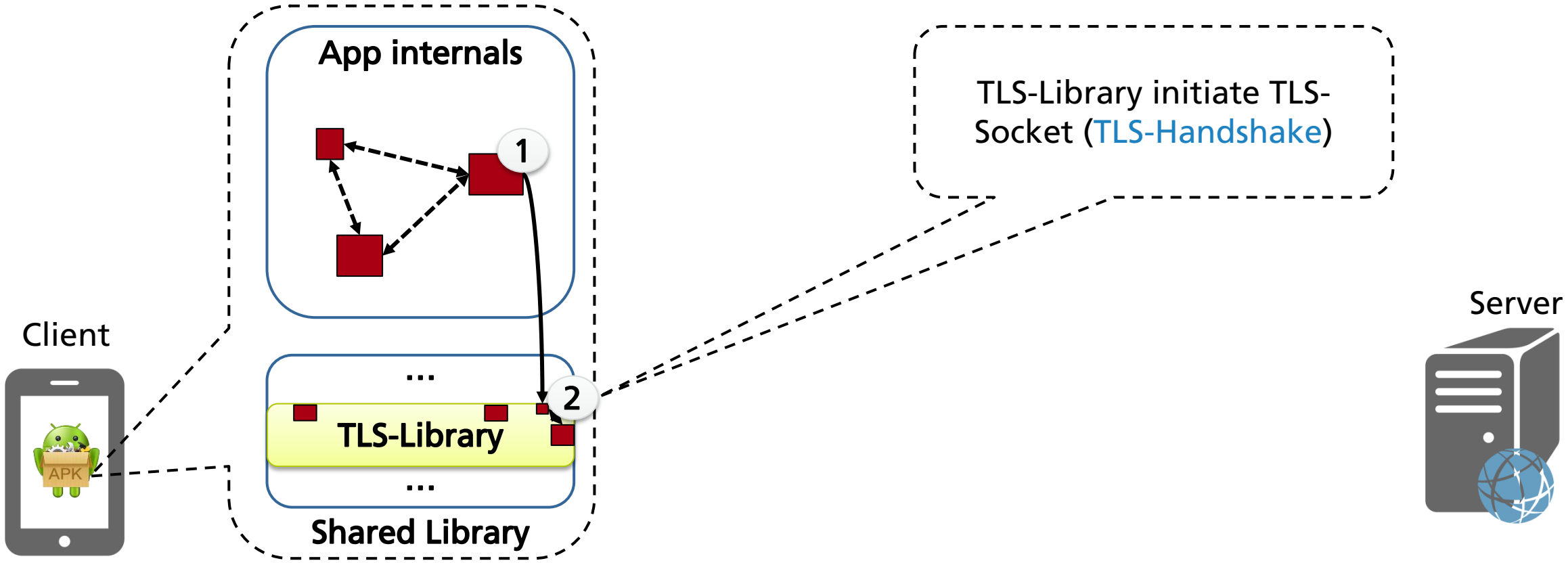
A TLS-stream offers the application to write its decrypted value to it ....



Fraunhofer FKIE

friTap: Approach

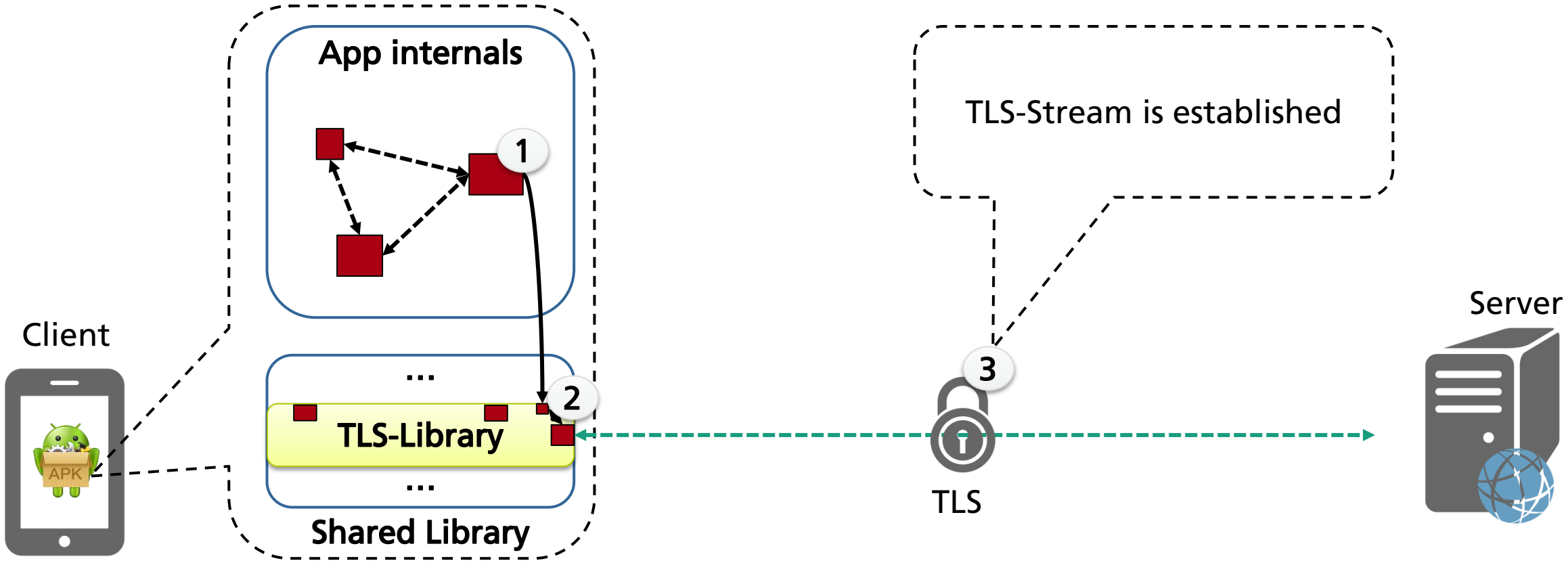
A TLS-stream offers the application to write its decrypted value to it ....



Fraunhofer FKIE

friTap: Approach

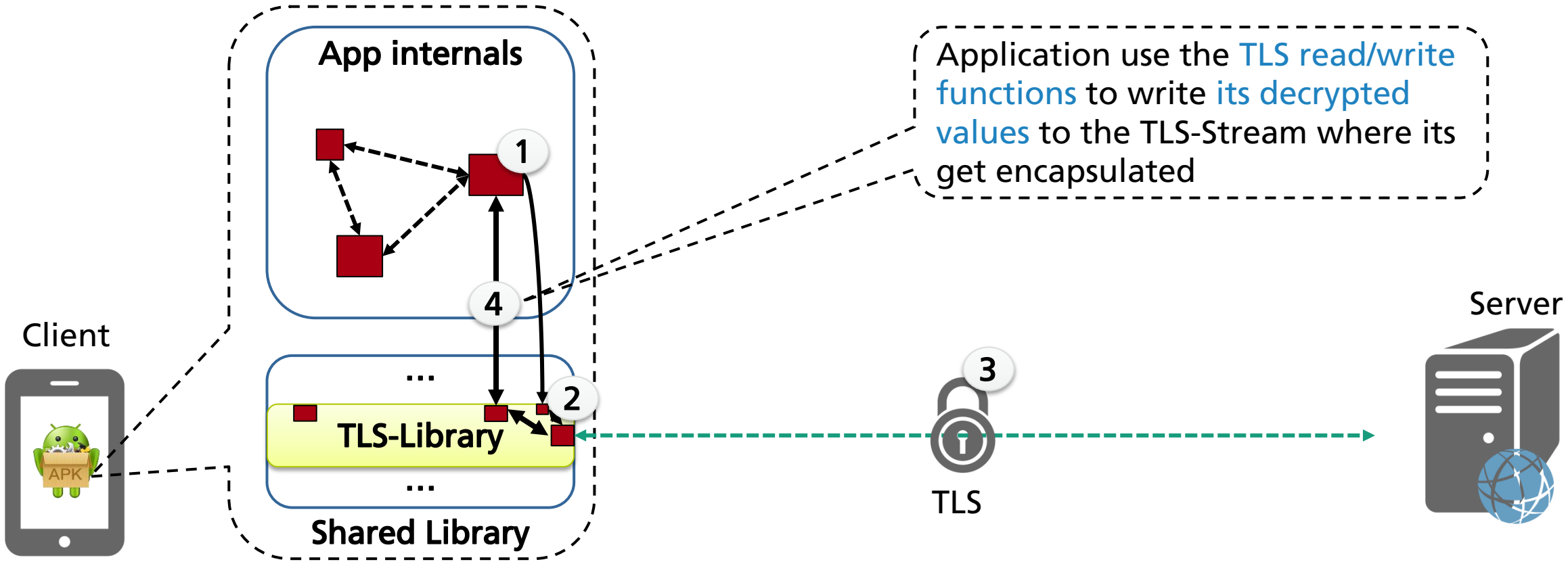
A TLS-stream offers the application to write its decrypted value to it ....



Fraunhofer FKIE

friTap: Approach

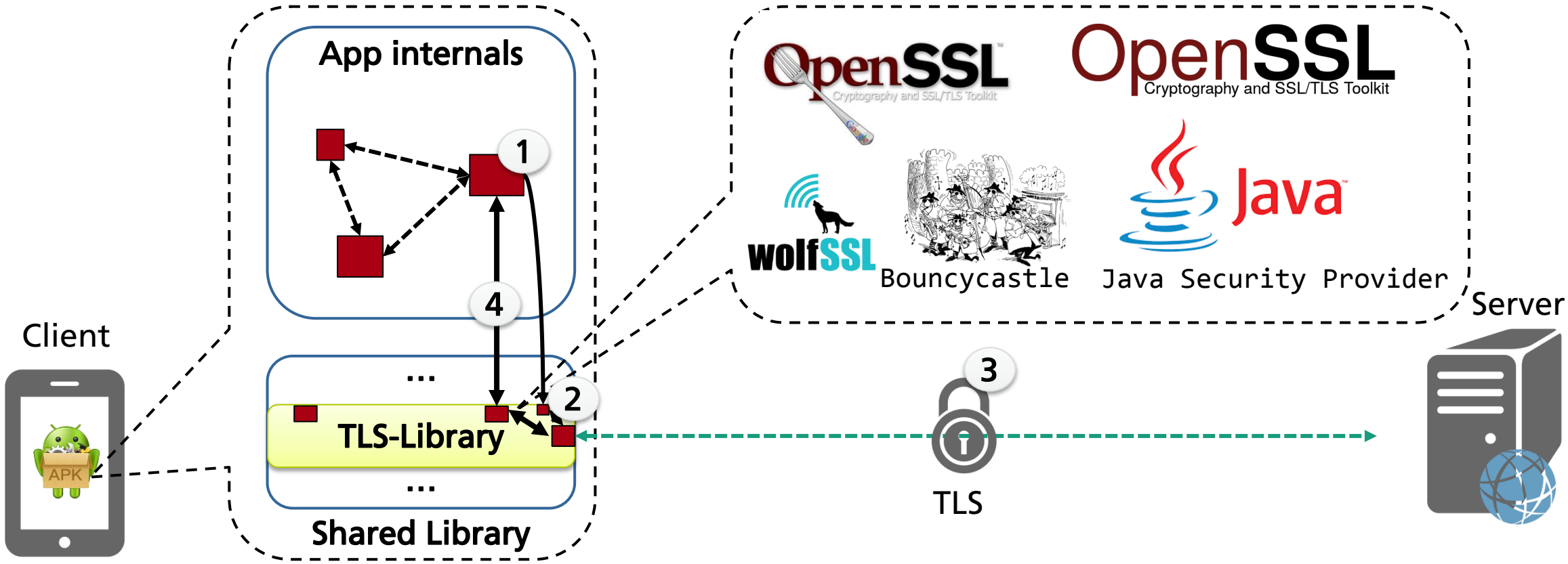
A TLS-stream offers the application to write its decrypted value to it ....



Fraunhofer FKIE

friTap: Approach

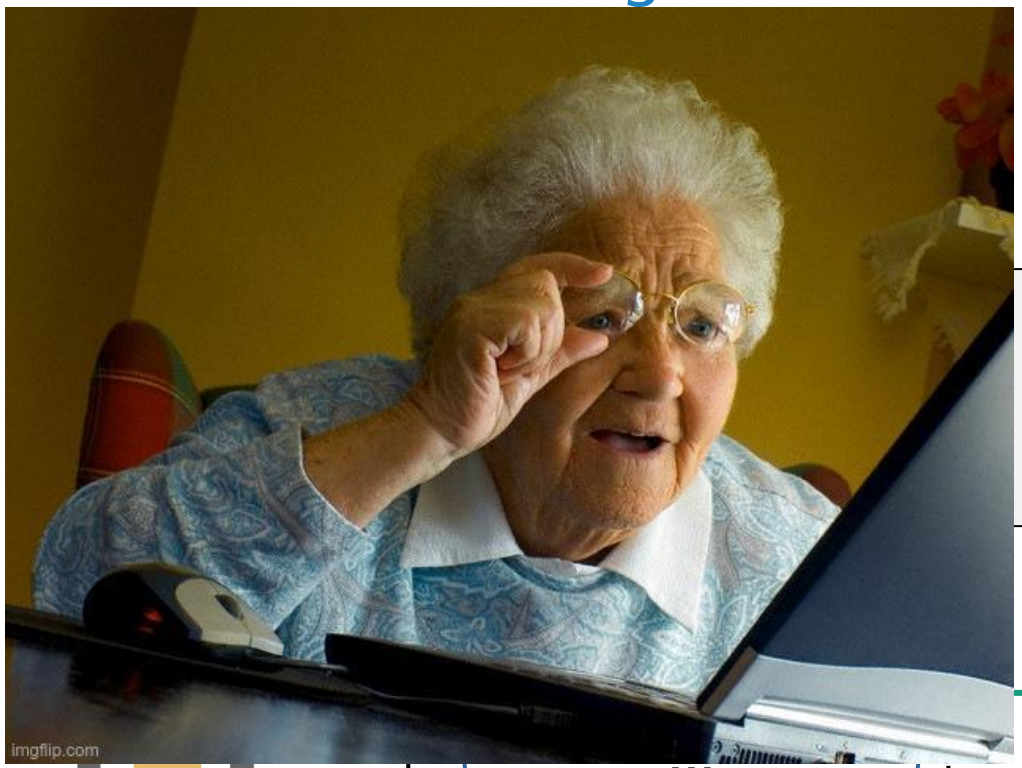
Hooking the TLS read/write functions of the TLS library



Fraunhofer FKIE

friTap: What else?

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

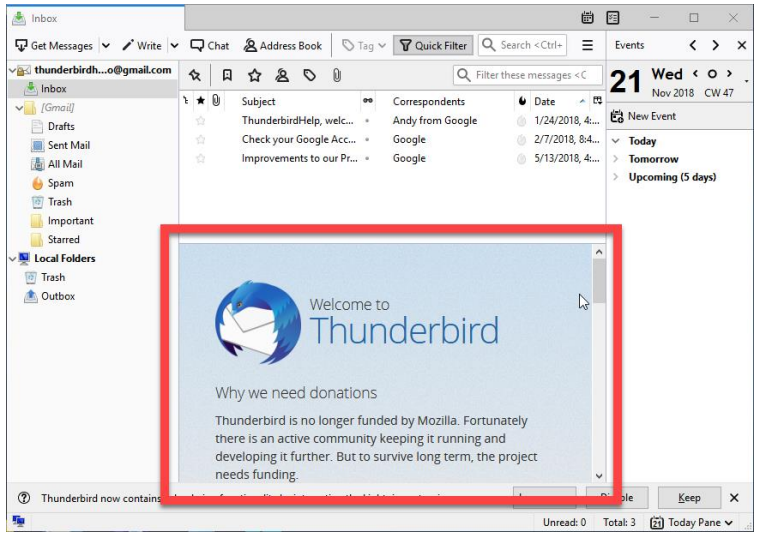


THE SSLKEYLOG-file can also be logged. SSL-Libraries offers ways to write the used keys into a file which can later on used by Wireshark to decrypt the captured traffic.

Fraunhofer FKIE

Demo

Thunderbird



Fraunhofer FKIE

Demo

Different Android APKs from the Playstore

Fraunhofer FKIE

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