Additional Material for Android OS Privacy under the Lens – A Tale from the East

Haoyu Liu
The University of edinburgh
Edinburgh, United Kindgom
haoyu.liu@ed.ac.uk

Douglas J. Leith
Trinity College Dublin
Dublin, Ireland
Doug.Leith@tcd.ie

Paul Patras
The University of edinburgh
Edinburgh, United Kindgom
paul.patras@ed.ac.uk

1 XIAOMI

Summary:

(1) Device details, aaid and oaid are sent to cn.register.xmpush.xiaomi.com for device registration after factory reset. aaid and oaid are temporary identifiers. Hashed android ID (temporary), hashed IMEI, cpuid and device details are are post to update.miui.com.
(2) Temporary identifiers including cloudsp_fid and cloudsp_devId are transmitted to find.api.micloud.xiaomi.net.
(3) Xiaomi device sends an request to data.mistat.xiaomi.com/key_get, which negotiates an encryption key (RSA encrypted) and sid with the server. The device further sends request to data.mistat.xiaomi.com/idservice/deviceid_get and data.mistat.xiaomi.com/mistats/v3 in which the message is encrypted with the key aforementioned and contains the sid, so that the server can look up associated key for decryption. The message to /idservice/deviceid_get incorporates hashed IMEI, MEID, MAC address and serial number, and AAID, android ID and OAID in plaintext. Any connections to data.mistat.xiaomi.com/mistats/v3 contains the same group of identifiers and also telemetry information that logs the access time of some activities including UsbDebuggingActivity, com.miui.notes.ui.NotesListActivity, and com.miui.notes.ui.activity.EditActivity.
(4) Traffic to diagnosis.ad.xiaomi.com and api.ad.xiaomi.com contains device details, aaid, oaid, hashed MAC address and IMEIs. Besides, connections to the latter incorporate local IP address, android ID and also the field 'isPersonalizedAdEnable' is set to true despite the fact that all opt-outs are selected during device setup. The traces collected from EU firmware populate this field as false.
(5) An request to api.developer.xiaomi.com uploads a range of system package names and jar filenames to check update. A smaller batch of xiaomi-related package names is uploaded to de.idm.iot.mi.com. However, the device also sends all the installed package names to auth.be.sec.miui.com, which is weird in the sense that the content does not match the domain/endpoint name at all.
(6) GUID, OAID and device details are sent to api.hybrid.xiaomi.com.
(7) The package com.xiaomi.metoknlp initiates a request to a baidu API api.map.baidu.com that contains the current geolocation. Note that during setup, Xiaomi provides the option of using location service or not, but disabling it does not turn off the location switch in settings.
(8) Traffic to tracking.miui.com consists of aaid, oaid, cpuid, hashed MAC, IMEI and devices details. Moreover, the handset collects a series of telemetry and location information which are also posted to this domain. Location-wise, geolocation, MCC, MNC, nearby wifi name and wifi mac address are transmitted. com.miui.analytics collects telemetry about xiaomi preinstalled app, including settings, recording, note, phone, message and camera. App first launch time, usage start time and end time are logged. The timestamps of calling key activities are logged as well, such as WifiProvisionSettingsActivity, NotesListActivity, EditActivity, Camera, and GrantPermissionsActivity.

Pre-installed Non-Xiaomi System Apps

(1) **China Mobile SDK** The handset sends multiple requests to a.fxltsbl.com which belongs to a self-registering platform managed by China Mobile. The requests contains IMEI, MEID, device details, and all the installed apps. If a sim card is inserted, CellId and lac are also populated.
(2) **China Unicom SDK** The handset send a request to dm.wo.com.cn:18080 for registration after factory reset, in which device details, IMEI, ICCID, IMSI, phone number, MNC, CellID and LAC are populated.
(3) **Baidu** The device requests baidu.com right after factory reset and the response routinely sets a few cookies, but they never appear elsewhere.

1.1 Selected Connections During Startup After Factory Reset and When Idle

```
POST https://cn.register.xmpush.xiaomi.com/pass/v2/register/encrypt
Headers
*Content-Type: application/x-www-form-urlencoded*
*Accept-Encoding: gzip*
**request body**
{"aaid":"68ddb591-8735-4d2d-8cae-ea790500e349","appid":"1000271","apptoken":"420100086271","appversion":"40009001","board":"evergo","brand":"Redmi","devid":"a-C895F74DC36426C4AE68E135B2FB9E6788C0D95D","model":"21091116AC","oaid":"6b13ae725b3af2dd","oaid_type":"1","os":"11-V12.5.4.0.RGBCNXM","packagename":"com.xiaomi.xmsf","ram":"4.0GB","rom":"128.0GB","sdkversion":"40001","space_id":"0","vaid":"0fc054a378bc1439"}

POST https://find.api.micloud.xiaomi.net/mic/find/v4/anonymous/device/key?cloudsp_fid=2828357e28403a4e6d577531512c20443a5b244c617046246622414326..&cloudsp_devId=ZDWVOTeL_xHsl8T1&cloudsp_service=allService
Headers
*User-Agent: 21091116AC; MIUI/V12.5.4.0.RGBCNXM*
*X-Micloud-Date: Tue, 04 Jan 2022 13:31:59 +0000*
*Accept-Language: zh_CN*
*Accept-Encoding: gzip*

POST https://data.mistat.xiaomi.com/get_all_config
Headers
*Content-Type: application/x-www-form-urlencoded*
```

```
*Accept-Encoding: gzip*
**request body**
rc=S&sv=3.0.16&t=2&av=20201109.0&rg=CN&ai
=2882303761517402087&m=21091116AC
ai is hashed android id.

POST https://update.miui.com/updates/miotaV3.php
Headers
*Cookie: serviceToken=;*
*Cache-Control: no-cache*
*Content-Type: application/x-www-form-urlencoded*
*Accept-Encoding: gzip*
**request body**
b'miuiotavalided11'={"a":"0","b":"F","c":"11","unlock
":"1","d":"evergo","lockZoneChannel":"","f":"5","
g":"790dc28bfd1e2f6d8fa62c99ec890ab3","channel":"","
i":"fb583af8b75156052b1bf57b1c4570b329c248c3a6f2dd4
d9acebd37b9457643","isR":"0","l":"zh_CN","sys":"0","n
":"ct","p":"evergo","r":"CN","bv":"125","v":"MIUI-V12
.5.4.0.RGBCNXM","id":"","sn":"0
xc60874bdc67fd88d4d96b41131ca00e279f9c22cff508563a5c080

82","sdk":"30","pn":"evergo","options":{"zone":1,"
hashId":"3f10ddcfb7b0813b","ab":"1","previewPlan
":"0"}}

g: hashed android Id (MD5), i: hased IMEI (SHA-256),
sn: cpuid


POST http://diagnosis.ad.xiaomi.com/track/d/v1.0
Headers
*gzip: 0*
*Content-Type: application/x-www-form-urlencoded*
*Accept-Encoding: gzip*
**request body**
value={"H":{"model":"21091116AC","android":"11","miui
":"V12.5.4.0.RGBCNXM","bn":"S","product":"evergo","
device":"evergo","cv":"4.6.0","lang":"zh_CN","region
":"CN","mi":"0","sender":"com.miui.analytics","userid
":0,"oa":"522c2e284e3699b7","n":"10","aaid":"61d0d6ee
-9974-410f-a9e2-ccd6863641b3","mac":"
b03c43d7e4c64fb5ba6ddd1b3a45b516","imei":"
a35f8d0fee9d2e444c8bfddf0b70af19","st
":"1641303127131"},"B":[{"H":{"sid":"","pk":"com.miui.
systemAdSolution","key":"
systemadsolution_sdkdiagnosislog","eventTime
":"1641303127027","sn":"28072637231","retryCnt":0},"B
":{"_event_id_":"REQUEST","e":"REQUEST","r":"
splash_config","biz":"init","pkg":"com.miui.
systemAdSolution","avc":2021092600,"avn
":"2021.09.26.00-release","ts":1641303127027}}]}
sign=061d1a7e0658aaa8bff68dc79e4fd652
ts=1641303127128
nonce=2a23476f4890215ca6846c0f714eabcb

POST https://find.api.micloud.xiaomi.net/mic/find/v4
.7/anonymous/device/report
Headers
*User-Agent: 21091116AC; MIUI/V12.5.4.0.RGBCNXM*
*X-Micloud-Date: Tue, 04 Jan 2022 13:32:04 +0000*
*Accept-Language: zh_CN*
*Content-Type: application/x-www-form-urlencoded*
** request body **
cloudsp_status=off&cloudsp_nonce=
_gUAE7LIYu6AIDYzYTVjMDgwODIBjXZI28lOKEhzSyiExQuErjcF2w
&cloudsp_fid=2828357e28403a4e6d57...&cloudp_sign
=304402...&cloudsp_devId=ZDWVOTeL_xHsl8T1&

POST https://tracking.miui.com/track/v1
Headers
*gzip: 0*
*Content-Type: application/x-www-form-urlencoded*
*Accept-Encoding: gzip*
**request body**
value={"H":{"model":"21091116AC","android":"11","miui
":"V12.5.4.0.RGBCNXM","bn":"S","product":"evergo","
device":"evergo","cv":"4.6.0","lang":"zh_CN","region
":"CN","mi":"0","sender":"com.miui.analytics","userid
":0,"oa":"522c2e284e3699b7","n":"10","aaid":"61d0d6ee
-9974-410f-a9e2-ccd6863641b3","mac":"
b03c43d7e4c64fb5ba6ddd1b3a45b516","imei":"
a35f8d0fee9d2e444c8bfddf0b70af19","st
":"1641303142813"},"B":[{"H":{"sid":"","pk":"com.miui.
systemAdSolution","key":"systemadsolution_monitor","
eventTime":"1641303142797","sn":"43752981540","
retryCnt":0},"B":{"e":"activate","pkg":"com.miui.
systemAdSolution","version":2021092600,"avc
":2021092600,"avn":"2021.09.26.00-release","ts
":1641303142797}}]}
sign=99e9dda6ca22912b017c9f55d9306a2f
ts=1641303142811
nonce=4f458592d4948de37cc3ac4d5b4a8e63

GET https://api.ad.xiaomi.com/track/pi/v1.0?
Headers
*gzip: 0*
*Accept-Encoding: gzip*
decoded query string:
{"adv":"11","androidId":"5a7e72f118faac59","at
":1641303142889,"cfgId":"null","cv":2021092600,"
device":"evergo","ile":"system","imei":"","make":"
xiaomi","mi":false,"miui":"V12.5.4.0.RGBCNXM","model
":"21091116AC","n":-1,"nonce":"
f8c082b11cc9c985ef0ac7af8b2cf10c","oaId":"522
c2e284e3699b7","region":"CN","st":1641303142904,"
pilist":["com.ss.android.ugc.aweme","com.tencent.mtt
","com.android.email","com.eg.android.AlipayGphone","
com.mipay.wallet","com.xiaomi.drivemode","com.xiaomi.
mibrain.speech","com.sina.weibo","com.mfashiongallery.
emag","com.xunmeng.pinduoduo","com.miui.cleanmaster
","com.xiaomi.vipaccount","cn.wps.moffice_eng.xiaomi.
lite","com.miui.notes","com.miui.newmidrive","com.
xiaomi.shop","com.miui.mediaeditor","com.xiaomi.
youpin","com.xiaomi.gamecenter","com.mi.health","com.
taobao.taobao","com.miui.huanji","com.miui.
smarttravel","com.miui.newhome","com.autonavi.minimap
","com.miui.calculator","com.miui.thirdappassistant
","com.mi.liveassistant","com.miui.virtualsim","com.
xiaomi.scanner","com.xiaomi.jr","com.miui.weather2","
com.ss.android.article.news","com.xiaomi.smarthome","
com.taobao.litetao","com.baidu.searchbox","com.duokan.
reader","com.miui.fm","com.baidu.input_mi","com.
iflytek.inputmethod.miui","com.dragon.read","tv.
danmaku.bili","com.duokan.phone.remotecontroller","
com.miui.screenrecorder","com.youku.phone","com.
android.soundrecorder","com.UCMobile"],"event":"list"}


GET https://api.ad.xiaomi.com/track/pi/v1.0?
Headers
*gzip: 0*
*Accept-Encoding: gzip*
decoded query string:
{"adv":"11","androidId":"5a7e72f118faac59","at
":1641227067609,"cfgId":"null","channel":"oobe","cv
":2021092600,"device":"evergo","ile":"unknown","imei
":"","make":"xiaomi","mi":false,"miui":"V12.5.4.0.
RGBCNXM","model":"21091116AC","n":-1,"nonce":"4
b200f32fe04a612563a226508ab54b1","oaId":"522
c2e284e3699b7","region":"CN","st":1641307299093,"apn
":"com.android.email","event":"active"}

GET https://api.ad.xiaomi.com/track/pi/v1.0?
Headers
*gzip: 0*
*Accept-Encoding: gzip*
decoded query string:
```

```
{"adv":"11","androidId":"5a7e72f118faac59","at
":1641227067244,"cfgId":"null","channel":"oobe","cv
":2021092600,"device":"evergo","ile":"unknown","imei
":"","make":"xiaomi","mi":false,"miui":"V12.5.4.0.
RGBCNXM","model":"21091116AC","n":-1,"nonce":"95
bb5d0d1f75030b652815470c938bf9","oaId":"522
c2e284e3699b7","region":"CN","st":1641307314753,"apn
":"com.xiaomi.mibrain.speech","event":"active"}

followed by a few consecutive requests containing
different package names

POST https://api.ad.xiaomi.com/brand/splashConfig
Headers
*content-type: application/x-www-form-urlencoded*
*accept-encoding: gzip*
**request body**
clientInfo={"context":{"approvePersonalizedAd":true,"
supportFocusVideo":true,"supportMaterialRender":false
},"adSdkInfo":{"version":"2021092600"},"deviceInfo
":{"androidVersion":"11","bc":"S","device":"evergo","
isInter":false,"make":"xiaomi","miuiVersion":"V12
.5.4.0.RGBCNXM","miuiVersionName":"V125","model
":"21091116AC","os":"android","restrictImei":false,"
screenDensity":2,"screenHeight":2400,"screenWidth
":1080},"userInfo":{"aaid":"61d0d6ee-9974-410f-a9e2-
ccd6863641b3","androidId":"
f42a12d7781eaf2dc9fea63818e88e0f","connectionType":"
WIFI","country":"CN","customization":"ct","imei":"","
ip":"192.168.1.90","language":"zh","locale":"zh_CN","
mac":"c95a595b9214b52ba77ac28b8406e367","networkType
":-1,"oaId":"522c2e284e3699b7","serviceProvider":"","
triggerId":"5a3019700233ca550f1475eea2c0d65f","ua":"
Dalvik/2.1.0 (Linux; U; Android 11; 21091116AC Build/
RP1A.200720.011)","vaId":"d17288e27a110f71"}}&nonce
=140ecfc3103a5e5e2624731b63948e41&sv=sv&packageName=
com.miui.systemAdSolution&isbase64=false&appKey=
system_splash&sign=2d47fa6c6b292c8d2a6cb3444c615f5e

POST https://api.ad.xiaomi.com/splash/predict
Headers
*content-type: application/x-www-form-urlencoded*
*accept-encoding: gzip*
**request body**
clientInfo={"context":{"approvePersonalizedAd":true,"
supportFocusVideo":true,"supportMaterialRender":false
},"adSdkInfo":{"version":"2021092600"},"deviceInfo
":{"androidVersion":"11","bc":"S","device":"evergo","
isInter":false,"make":"xiaomi","miuiVersion":"V12
.5.4.0.RGBCNXM","miuiVersionName":"V125","model
":"21091116AC","os":"android","restrictImei":false,"
screenDensity":2,"screenHeight":2400,"screenWidth
":1080},"userInfo":{"aaid":"61d0d6ee-9974-410f-a9e2-
ccd6863641b3","androidId":"
f42a12d7781eaf2dc9fea63818e88e0f","connectionType":"
WIFI","country":"CN","customization":"ct","imei":"","
ip":"192.168.1.90","language":"zh","locale":"zh_CN","
mac":"c95a595b9214b52ba77ac28b8406e367","networkType
":-1,"oaId":"522c2e284e3699b7","serviceProvider":"","
triggerId":"1e70dab00727fa0248ab35a877b681a1","ua":"
Dalvik/2.1.0 (Linux; U; Android 11; 21091116AC Build/
RP1A.200720.011)","vaId":"d17288e27a110f71"}}&appKey=
system_splash&sign=44d1f6f0be018ace3a197bb1f63456f4

POST https://api.ad.xiaomi.com/remoteConfig
Headers
*Content-Type: application/x-www-form-urlencoded; UTF
-8*
*Cache-Control: no-cache*
*Accept-Encoding: gzip*
**request body**
clientInfo={"deviceInfo":{"screenWidth":1080,"
screenHeight":2400,"screenDensity":2,"model
":"21091116AC","device":"evergo","androidVersion
":"11","miuiVersion":"V12.5.4.0.RGBCNXM","
miuiVersionName":"V125","bc":"S","make":"xiaomi","
isInter":false,"os":"android","restrictImei":false},"
userInfo":{"locale":"zh_CN","language":"zh","country
":"CN","customization":"ct","networkType":-1,"
connectionType":"WIFI","ua":"Dalvik\/2.1.0+(Linux;+U;+
Android+11;+21091116AC+Build\/RP1A.200720.011)","
serviceProvider":"","triggerId":"
c964454088e65dccd5f8a4a9393e714a","
isPersonalizedAdEnabled":true,"imei":"","mac":"
c95a595b9214b52ba77ac28b8406e367","aaid":"61d0d6ee
-9974-410f-a9e2-ccd6863641b3","androidId":"
f42a12d7781eaf2dc9fea63818e88e0f","ip
":"192.168.1.90","oaId":"522c2e284e3699b7","vaId":"
d17288e27a110f71"},"applicationInfo":{"platform":"
xiaomi","packageName":"com.miui.systemAdSolution","
version":2021092600},"context":{"hasUc":0}}&isbase64=
false&appKey=APP_STORE_DESKTOPFOLDER&sign=5
fdf0edee999168d093fc412db8a8af1


POST https://api.hybrid.xiaomi.com/api/topn/fetch.v2
Headers
*accept-language: zh-CN,zh;q=0.9,en;q=0.8*
*content-type: application/x-www-form-urlencoded*
*accept-encoding: gzip*
**request body**
device_model=evergo&is_global=false&device_type=phone
&check_whitelist=false&hybrid_version_code=10810405&
os_version_type=V12.5.4.0.RGBCNXM(stable)&
android_os_version=30&platform_version=1081&imei_md5
=&guid=8d6bdde1-0150-4c27-ab37-43c8cea7a2d7&region=CN
&network_type=wifi&oaid=522c2e284e3699b7&screen_width
=1080&screen_height=2260&screen_density=2.75

POST https://api.hybrid.xiaomi.com/api/redirect/query.
v4
Headers
*accept-language: zh-CN,zh;q=0.9,en;q=0.8*
*content-type: application/x-www-form-urlencoded*
*accept-encoding: gzip*
**request body**
device_model=evergo&is_global=false&device_type=phone
&check_whitelist=false&hybrid_version_code=10810405&
os_version_type=V12.5.4.0.RGBCNXM(stable)&
android_os_version=30&platform_version=1081&imei_md5
=&guid=8d6bdde1-0150-4c27-ab37-43c8cea7a2d7&region=CN
&network_type=wifi&oaid=522c2e284e3699b7

GET https://resolver.msg.xiaomi.net/gslb/?ver=4.0&
type=wifi&reserved=1&uuid=0&list=cn.app.chat.xiaomi.
net%2Cresolver.msg.xiaomi.net&countrycode=CN&sdkver
=46&osver=30&os=21091116AC%3AV12.5.4.0.RGBCNXM&mi=3&
key=d30c1a48d9744f5669c7fd944dda0ea5

POST https://api.sec.miui.com/common/whiteList/
listByModule
Headers
*Accept-Charset: utf-8*
*Content-Type: application/x-www-form-urlencoded*
*Accept-Encoding: gzip*
**request body**
appVersion=30&carrier=unknown&dataVersion=0&device=
evergo&imei=6C76C7EABBD49CB16DB3B7009416DF2B&initdev=
false&isDiff=true&miuiVersion=V12.5.4.0.RGBCNXM&
module=RestrictAppControl&param=dXBkYXRl&region=CN&t=
stable&sign=8BECAEB947E70D64887B76EE2DFB459B

POST https://data.sec.miui.com/data/cloud
Headers
*Content-Type: application/x-www-form-urlencoded*
*Accept-Encoding: gzip*
```

```
POST https://auth.be.sec.miui.com/v1/auth/permissions?versionType=stable&cta=false&carrier=ct&appVersion=166&androidVersion=30&miuiVersion=MIUI-V12.5.4.0.RGBCNXM&region=CN&mi=d17288e27a110f71&lang=zh&device=evergo
Headers
*Content-Type: UTF-8*
*Accept-Encoding: gzip*
['com.android.storagemanager', 'com.android.printspooler', 'com.mi.AutoTest', 'com.goodix.fingerprint', 'com.mediatek.frameworkresoverlay', 'com.android.pacprocessor', 'com.mediatek.capctrl.service', 'com.android.wifi.resources.xiaomi', 'com.android.permissioncontroller', 'com.miui.guardprovider', 'com.miui.huanji', 'com.android.wallpaper.livepicker', 'com.miui.newhome', 'com.android.internal.systemui.navbar.gestural_narrow_back', 'com.miui.calculator', 'com.android.providers.telephony', 'com.unionpay.tsmservice.mi', 'com.android.contacts', 'com.android.internal.display.cutout.emulation.waterfall', 'com.miui.catcherpatch', 'com.android.deskclock', 'com.miui.micloudsync', 'com.miui.wmsvc', 'com.mediatek.systemuiresoverlay', 'com.miui.translation.youdao', 'com.baidu.searchbox', 'com.xiaomi.finddevice', 'com.android.cts.ctsshim', 'com.android.mtp', 'com.android.systemui.overlay.miui', 'com.duokan.phone.remotecontroller', 'com.miui.hybrid.accessory', .... (all installed apps)

POST https://tracking.miui.com/track/v4
Headers
*Content-Type: application/octet-stream*
*OT_SID: 7e3bc06fd5f2b3021c8ad01899dc83353c13efdf47977ccd9a7cad864e59520495d0652512a3be5fe63e43374afd02d6*
*OT_ts: 1641330974892*
*OT_net: WIFI*
*OT_sender: com.miui.analytics*
*OT_protocol: 3.0*
*Accept-Encoding: gzip*
[
{
...
   "B":
   {
      "real_model": "21091116AC",
      "product": "evergo",
      "device": "evergo",
      "device_type": "Phone",
      "screen": "2400*1080",
      "sn": "",
      "android_id": "d42520ff64e66d42",
      "vaid": "b703a91ca6baa940",
      "udid": "",
      "mac": "b03c43d7e4c64fb5ba6ddd1b3a45b516",
      "imeis": "[a35f8d0fee9d2e444c8bfddf0b70af19,6c76c7eabbd49cb16db3b7009416df2b]",
      "meids": "[ba1573ba7923062e8eb0dcf30ca16c74]",
      "imsis": "[b2d5c6783e3fa6eef38ff1fc7dedfb10,]",
      "oaid_stat": 1,
      "language": "zh_CN",
      "ram": "4GB",
      "rom": "128GB",
      "free_rom": "104.10GB",
      "ui_ver": "V125",
      "android_ver_int": 30,
      "uep": false,
      "sign": "701478a1",
      "cust_variant": "cn_chinatelecom",
      "intl": false,
      "desc": "evergo-user 11 RP1A.200720.011 V12.5.4.0.RGBCNXM release-keys",
      "radio": "23415", //MCC+MNC
      "radio2": "",
      "first_boot": false,
      "bind_stats": "0",
      "release_time": 1470758400000,
      "first_conect_time": 1666818468000,
      "lock_state": "unlocked",
      "rootable": "0",
      "tz_content": "f6mGXHX...",
      "tz_sign": "3044022...",
      "tz_fid": "2828357...",
      "tz_support": true,
      "tz_cpuid": "0xc60874bdc67fd88d4d96b41131ca00e279f9c22cff508563a5c08082",
      "loc": "{\"b\":\"234,15,850,60937383,-93\",\"w\":\"d4:5d:64:db:04:24,androidprivacy,-37,5500\",\"s\":[\"234,15,850,60937383,-89\",
      \"234,15,850,60937383,-95\"],\"wl\":[\"5c:02:14:89:8d:ef,Xiaomi_8DEE,-31,2422\",\"d4:5d:64:db:04:24,androidprivacy,-37,5500\",\"00:08:32:8e:ed:e9,,-79,5260\",\"00:08:32:8e:ed:ec,uS-Glide,-79,5260\",\"00:08:32:8e:ed:ee,UNITE-Staff,-79,5260\",\"00:08:32:8e:ed:ef,UNITE-Corporate,-79,5260\",\"00:08:32:91:dd:2f,UNITE-Corporate,-80,5200\",\"00:08:32:91:dd:2e,UNITE-Staff,-81,5200\",\"00:08:32:91:dd:2c,uS-Glide,-81,5200\"],\"wlt\":1666819355063,\"g\":[{\"loc_type\":\"network\",\"lat\":55.941304,\"lng\":-3.179206,\"cc\":\"51603\",\"cn\":\"Scotland\",\"aa\":\"Edinburgh\",\"loc\":\"Edinburgh\",\"sl\":\"\",\"tho\":\"Bernard Terrace\",\"loc_t\":1666819356263}],\"ss\":{\"gss\":1,\"wss\":1}}",
      "allow_report_usage": 0,
      "protocol_ver": 1,
      "ot_activation": false
   }
},
{
   "H":
   {
      "event": "onetrack_id",
      "imei": "a35f8d0fee9d2e444c8bfddf0b70af19",
      "oaid": "e6864b18e5150073",
      "instance_id": "fe2c5a3d-df93-4281-bd9a-394b050702d3",
      "mfrs": "Xiaomi",
      "model": "21091116AC",
      "platform": "Android",
      "miui": "V12.5.4.0.RGBCNXM",
      "build": "S",
      "os_ver": "11",
      "app_ver": "5.1.0",
      "e_ts": 1666819361207,
      "tz": "GMT+00:00",
      "net": "WIFI",
      "region": "CN",
      "user_id": 0,
      "app_id": "001",
      "pkg": "com.miui.analytics",
      "market_name": "Redmi Note 11 5G"
   },
   "B":
   {
      "sn": "",
      "imeis": "[a35f8d0fee9d2e444c8bfddf0b70af19,6c76c7eabbd49cb16db3b7009416df2b]",
      "imsis": "[b2d5c6783e3fa6eef38ff1fc7dedfb10,]",
      "meids": "[ba1573ba7923062e8eb0dcf30ca16c74]",
      "oaid": "e6864b18e5150073",
      "vaid": "b703a91ca6baa940",
      "udid": "",
      "android_id": "d42520ff64e66d42",
      "mac": "b03c43d7e4c64fb5ba6ddd1b3a45b516",
      "oaid_stat": 1
   }
},
...
}]
```

a broad range of telemetry are collected and post to this url, including the app first launch time, start time, end time, note creation time, edit time, recording time... The following activities are logged when created (not limited to them):

```
com.android.settings.wifi.
WifiProvisionSettingsActivity
com.android.settings.MiuiSettings
com.android.settings.Settings$WifiSettingsActivity
com.miui.notes.ui.NotesListActivity
com.miui.notes.ui.activity.EditActivity
com.android.calendar.homepage.AllInOneActivity
com.android.camera.Camera
com.android.packageinstaller.permission.ui.
GrantPermissionsActivity
...


POST https://data.mistat.xiaomi.com/key_get
Headers
*Content-Type: application/x-www-form-urlencoded*
*Accept-Encoding: gzip*
**request body**
skey_rsa=CF7QO7pE6M0i7m9vsPn7lW9aeomeya/
QvjEiia7SbEpwAcqDpx/
G1EMKo4qbvzVQLsKyy67ZVpGQ6GTVUnp2rZnzRqSRQTw++0
HdgyKQOf76V0fsqLFk1DyFzFfAYyTa1r4RL/mO6/GbWa/
FpB92ZbETNsAR7s7LTe7zzticzoE=

key encrypted with RSA, and would be used in
following request

POST https://data.mistat.xiaomi.com/idservice/
deviceid_get
Headers
*Content-Type: application/x-www-form-urlencoded*
*Accept-Encoding: gzip*
**request body**
decrypted
{
   "ia": "a35f8d0fee9d2e444c8bfddf0b70af19", imei1
   "ib": "6c76c7eabbd49cb16db3b7009416df2b", imei2
   "md": "ba1573ba7923062e8eb0dcf30ca16c74", meid
   "mm": "b03c43d7e4c64fb5ba6ddd1b3a45b516", mac
   "bm": "fb8e5e7fbe3bfea840263b075e517d3a", serial
number
   "aa": "0c5300d8-2069-44ff-9708-f4444b1080c8", aaid
 changes after factory reset
   "ai": "daa30bab43de5109", android_id changes after
 factory reset
   "oa": "d428f037d79e4310" oaid changes after
factory reset
}


POST https://data.mistat.xiaomi.com/mistats/v3
Headers
*Content-Type: application/x-www-form-urlencoded*
*Accept-Encoding: gzip*
**request body**
decrypted
{
   "id": "MB03C43D7E4C64FB5BA6DDD1B3A45B516", //
device_id from xiaomi
   "aii": "8e9dd3dc-309f-4cc4-877f-1a4806436a81",
   "rc": "S",
   "av": "20201109.0",
   "ac": "MIUI12.5",
   "os": "Android",
   "rd": "",
   "pp": 15000,
   "st": "1666796063707",
   "tz": "GMT+00:00",
   "cc": 1,
   "ob": "V12.5.4.0.RGBCNXM",
   "n": "WIFI",
   "es": [
   {
      "e": "mistat_dau",
      "eg": "mistat_basic",
      "tp": "track",
      "ts": 1666795753344,
      "eid": 1,
      "ps":
      {
         "fo": 1,
         "ia": "a35f8d0fee9d2e444c8bfddf0b70af19", //
 imei
         "i1": "
fb583af8b75156052b1bf57b1c4570b329c248c3a6
         f2dd4d9acebd37b9457643",
         "ib": "6c76c7eabbd49cb16db3b7009416df2b", //
imei2
         "i2": "
e6c6d2f45111be97ce711c519c2059f649e5d73
         1df044da46a696ac8b2368bb6",
         "md": "ba1573ba7923062e8eb0dcf30ca16c74", //
 meid
         "ms": "5113
c1359c1a6faeeed9e46cc6c2c6430182f02a
         eb1f27a38e58619b87e0599d",
         "ii": "8e9dd3dc-309f-4cc4-877f-1a4806436a81",
 // pref_instance_id
         "mcm": "b03c43d7e4c64fb5ba6ddd1b3a45b516", //
 mac
         "mcs": "5
e00c329cd48b3b71b507b6df7e26a8389b43bc
         8aaa9cb5088072a8d98e559c4",
         "bm": "fb8e5e7fbe3bfea840263b075e517d3a", //
 serial number
         "bs": "
b7a55ce3d1e1ca4a45de45c7ac00bc4ffa9817d4c
         41ff29dbd1b00e9ab7c7c43",
         "aa": "9861b5d6-2a32-42bc-9847-7d75dabc026b",

         "ai": "47eaefe5bc381ade", // android_id
         "od": "null",
         "oa": "d090195932e9f8a0", // OAID
         "va": "a8fb7d26baeb047d", // VAID
         "mi_av": "20201109.0",
         "mi_sv": "3.0.16",
         "mi_ov": "11",
         "mi_ob": "V12.5.4.0.RGBCNXM",
         "mi_n": "NOT_CONNECTED",
         "mi_rd": "",
         "mi_mf": "Xiaomi",
         "mi_m": "21091116AC",
         "mi_os": "Android"
      }
   },
   {
      "e": "mistat_pa",
      "eg": "mistat_basic",
      "tp": "track",
      "ts": 1666795754854,
      "eid": 2,
      "ps":
      {
         "pg": "
com.android.systemui.usb.UsbDebuggingActivity",
         "bt": 1666795753339,
         "et": 1666795754854,
         "mi_av": "20201109.0",
         "mi_sv": "3.0.16",
         "mi_ov": "11",
         "mi_ob": "V12.5.4.0.RGBCNXM",
         "mi_n": "NOT_CONNECTED",
         "mi_rd": "",
         "mi_mf": "Xiaomi",
         "mi_m": "21091116AC",
         "mi_os": "Android"
      }
   },
   {
      "e": "mistat_page_monitor",
      "eg": "mistat_basic",
      "tp": "track",
      "ts": 1666795754881,
      "eid": 3,
      "ps":
      {
```

```
          "rc": 1,
          "pc": 1,
          "sts": 1666795753338,
          "ets": 1666795754880,
          "mi_av": "20201109.0",
          "mi_sv": "3.0.16",
          "mi_ov": "11",
          "mi_ob": "V12.5.4.0.RGBCNXM",
          "mi_n": "NOT_CONNECTED",
          "mi_rd": "",
          "mi_mf": "Xiaomi",
          "mi_m": "21091116AC",
          "mi_os": "Android"
      }
   }]
}
```


such logging of activities also exists in phone, message, note, recording, ...


```
POST https://api.developer.xiaomi.com/autoupdate/updateself
Headers
*Content-Type: application/x-www-form-urlencoded*
*Accept-Encoding: gzip*
**request body**
androidId=5a7e72f118faac59&apkHash=bd6fddbc200db7422201e2d9b5652f5e&co=CN&debug=0&info={"screenSize":"1080*2260","resolution":"2260*1080","density":440,"touchScreen":3,"glEsVersion":"3.2","feature":"[android.hardware.audio.low_latency,+android.hardware.audio.output,+android.hardware.bluetooth,+android.hardware.bluetooth_le,+android.hardware.camera,+android.hardware.camera.any,+android.hardware.camera.autofocus,+android.hardware.camera.capability.manual_post_processing,+android.hardware.camera.capability.manual_sensor,+android.hardware.camera.capability.raw,+android.hardware.camera.flash,+android.hardware.camera.front,+android.hardware.camera.level.full,+android.hardware.consumerir,+android.hardware.ethernet,+android.hardware.faketouch,+android.hardware.fingerprint,+android.hardware.location,+android.hardware.location.gps,+android.hardware.location.network,+android.hardware.microphone,+android.hardware.opengles.aep,+android.hardware.ram.normal,+android.hardware.screen.landscape,+android.hardware.screen.portrait,+android.hardware.sensor.accelerometer,+android.hardware.sensor.compass,+android.hardware.sensor.gyroscope,+android.hardware.sensor.light,+android.hardware.sensor.proximity,+android.hardware.sensor.stepcounter,+android.hardware.sensor.stepdetector,+android.hardware.telephony,+android.hardware.telephony.cdma,+android.hardware.telephony.gsm,...


GET https://api.map.baidu.com/geocoder/v2/?
queries are below:
ak=qZNFtSET5KfZiv4mSnV2eGjC
build=845
channel=nl.1269e
coordtype=wgs84ll
cu=54B1C87D656D116392668FE36723444B|0
from=BaiduNLP
language=zh-CN
language_auto=1
latest_admin=1
location=55.941324,-3.179302
mb=21091116AC
oem=xiaomi
os=Android30
output=jsonaes
pois=1
prod=SDKXM5.5.10:build845:com.xiaomi.metoknlp
sn=0dc22eb9c95a66033d6d5ed261fbc770
```


1.2 Connections initiated by Non-Xiaomi Apps


```

POST https://www.baidu.com/
Headers
*Accept-Encoding: gzip*

GET https://a.fxltsbl.com/getIpAddr&appkey=A100000005&version=v2&imei=866490057599967&timestr=1666554424159&token=a7bd562d60a94ff0552a2e6bb8430f8e
Headers
*Accept-Encoding: gzip*

POST https://a.fxltsbl.com/TerminalConfigService/terminalConf?func=tsdk:termimalfullconfig&brand=Redmi&model=21091116AC&mac=null&imei=866490057599967&imei2=866490057599975&version=v2&sdkver=2.1.2&dynamicVer=0&action=heart&timestr=1666554489158&token=c49cf99ff433ae7aa13bc344721e30f5&appkey=A100000005
Headers
*Content-Type: application/json; charset=utf-8*
*Accept-Encoding: gzip*
**request body**
{"brand":"Redmi","model":"21091116AC","imei":"866490057599967","appkey":"A100000005","func":"tsdk:termimalfullconfig"}


POST https://a.fxltsbl.com/accept/sdkService?func=tsdk:posthblog&appkey=A100000005&timestr=1666554490036&imei=866490057599967&version=v2&token=31a2c68403db07f375be38f1c69e28e4
Headers
*Content-Type: application/json; charset=utf-8*
*Accept-Encoding: gzip*
**request body**
{"sdkVersion":"2.1.2","deviceId":"866490057599967","imei1":"866490057599967","imei2":"866490057599975","meid":"990018293799 98","brand":"Redmi","model":"21091116AC","firmwareVer":"MIUI 12.5.4 |\n12.5.4.0(RGBCNXM)","systemVer":"11","type":"1","mac":"fc:d9:08:ee:5e:8a","cellId":"-1","lac":"-1","channel":"18","dataCard":"0","masterStatus":"-1","soltQuantity":"2","dataCard2":"0","soltService1":"1","soltService2":"1","soltNetwork1":"0","soltNetwork2":"0","cellId2":"-1","lac2":"-1","volte":"0","volteShow":"unknown","niticeContent":"unknown","volte2":"0","volteShow2":"unknown","niticeContent2":"unknown","inType":"21091116AC","verify":"imei_866490057599967#imsi_#mac_null#brand_Redmi#model_21091116AC#version_11#totalRam_4GB#SDFreeSpace_99543.26171875#cpu_MT6833P#screen_1080*2260#simSerialNumber_null#romSpace_115 GB#battery_100#ROTATION_VECTOR:Y||GYROSCOPE_UNCALIBRATED:Y||GAME_ROTATION_VECTOR:Y||AMBIENT_TEMPERATURE:N||GYROSCOPE:Y||LIGHT:Y||STEP_COUNTER:Y||LINEAR_ACCELERATION:Y||GRAVITY:Y||RELATIVE_HUMIDITY:N||MAGNETIC_FIELD_UNCALIBRATED:Y||GEOMAGNETIC_ROTATION_VECTOR:Y||PRESSURE:N||TEMPERATURE:N||ORIENTATION:Y||ACCELEROMETER:Y||SIGNIFICANT_MOTION:Y||STEP_DETECTOR:Y||PROXIMITY:Y||#","totalFlowW":"2291234","totalFlowD":"0","totalFlowD2":"0","cpu":"MT6833P","rom":"128GB","ram":"4.00GB","mobileFirst":"1","sendTime":"1666554490006","longitude":"unknown","latitude":"unknown","address":"-1|-1|-1","switchState":"1101100000111","addrFrom":"-1","phoneNumber1":"unknown","phoneNumber2":"unknown"}


POST https://a.fxltsbl.com/accept/sdkService?func=tsdk:postapplylog&appkey=A100000005&timestr=1666554492829&imei=866490057599967&version=v2&token=7f00ab6f2cb231470d576b175ef377ae
Headers
*Content-Type: application/json; charset=utf-8*
*Accept-Encoding: gzip*
```

```
**request body**
{"imei1":"866490057599967","imei2
":"866490057599975","meid":"99001829379998","brand":"
Redmi","model":"21091116AC","sdkVersion":"2.1.2","
deviceId":"866490057599967","sendTime
":1666554492827,"totalFlowW":2291234,"totalFlowD":0,"
logAppAry":"|0|0|0|0|com.android.printspooler\r\n
|0|0|0|0|com.mi.AutoTest\r\nGFManager|0|0|0|0|com.
goodix.fingerprint\r\ncom.mediatek.
frameworkresoverlay|0|0|0|0|com.mediatek.
frameworkresoverlay\r\nPacProcessor|0|0|0|0|com.
android.pacprocessor\r\nRilCap|0|0|0|0|com.mediatek.
capctrl.service\r\ncom.android.wifi.resources.xiaomi
|0|0|0|0|com.android.wifi.resources.xiaomi\r\n
|0|0|0|0|com.android.permissioncontroller\r\n
|0|0|0|0|com.miui.guardprovider\r\n|0|0|0|0|com.miui.
huanji\r\n|0|0|0|0|com.android.internal.systemui.
navbar.gestural_narrow_back\r\nGFManager|0|0|0|0|com.
unionpay.tsmservice.mi\r\nJoyose|0|0|0|0|com.android.
internal.display.cutout.emulation.waterfall\r\n
|0|0|0|0|com.android.providers.telephony\r\ncom.miui.
catcherpatch.BaseApplication|0|0|0|0|com.miui.
catcherpatch\r\n|0|0|0|0|com.android.deskclock\r\
nMiCloudSync|0|0|0|0|com.miui.micloudsync\r\
nWMService|0|0|0|0|com.miui.wmsvc\r\ncom.mediatek.
systemuiresoverlay|0|0|0|0|com.mediatek.
systemuiresoverlay\r\ncom.miui.translation.youdao
|0|0|0|0|com.miui.translation.youdao\r\n|0|0|25214|0|
com.xiaomi.finddevice... (all the installed app)

POST http://dm.wo.com.cn:18080/registerv3?ver=3.0&
model=21091116AC&manuf=Xiaomi&sign=qw78SISjawaQ%2
BR134g96cPHf7zQSBiWfGIp3s0etOjGn3zreBE4trxfUuskdpq
fBDvkbJUf7SRbX%0ANlRo1fZao2a3xx0PZe%2FeJiF%2
BRjtd47uM30TupXZEqyjTtZr6aK%2FIr%2FFLCPhSy%2
FQhObHEKtpURa5L%0AGO7X9GVZtInFB2Onjno%3D%0A
Headers
*Content-Type: application/encrypted-json*
*Accept-Encoding: gzip*

{"Manuf":"Xiaomi","Model":"21091116AC","HWVersion":"
V1","SWVersion":"V12.5.4.0.RGBCNXM","OS":"Android","
OSVersion":"11","IMEI1":"866490057599967","ICCID1
":"89860114851034217836","IMSI1":"460013434948555","
MSISDN1":"+86131xxxxxxxx","MNC1":"46001","NCLS1":"LTE
","CellID1":"129303075","LAC1":"41105","VolteEnabled1
":"1","5GEnabled1":"1","IMEI2":"866490057599975","
ICCID2":"","IMSI2":"","MSISDN2":"","MNC2":"","NCLS2
":"","CellID2":"","LAC2":"","VolteEnabled2":"","5
GEnabled2":"","DataSlot":"1","AccType":"WiFi","
SubType":{"RAM":"4G","ROM":"128G","FREE":"97G"},"
DeviceType":"000005","RegType":"F","SpecVersion
":"3.0","RegVersion":"1.2-20210817","Time
":"2022-10-29 22:34:45","AppInfo":""}
```

2 ONEPLUS

Summary:

(1) Weather app sends OID, VAID, and OAID to oppo server i6.weather.oppomobile.com. Geo-location (latitude and longitude) is transmitted in subsequent requests. parameters mcc, ssid and lac exists in the requests but no values are filled in.
(2) The handset sends encrypted guid and IMEI to moa-upload-online.coloros.com, sends devID to lang.coloros.com and transmits openId to tobcustomize.coloros.com and component-ota.coloros.com. IMEI and openID (=guid) are persistent identifiers while devID changes after factory reset. Although heytapmobi and coloros nominally belong to two companies, they are deeply related in terms of the traffic generated after factory reset. The handset sends device details to https://data.sms.heytapmobi.com and receives a list of URLs starting with https://tedsyncfs.coloros.com/, which is accessed later.
(3) A subset of preinstalled apps are sent to icosa.coloros.com, classify.apps.coloros.com and moa-upload-online.coloros.com.
(4) The handset transmits encrypted contents to log.avlyun.com with the package name com.coloros.wifisecuredetect in the requests. The package would be launched as soon as wifi is enabled and initiates those requests. The time gap between 'enabling wifi' and 'posting requests' is extremely small. By the time frida hooked the functions in this package, the requests are already sent. contents are still unknown.
(5) The handset sends deviceId and vaid to httpdns.push.heytapmobi.com, sends duId and ouId to stg-data.ads.heytapmobi.com, and sends device details and ouId to data.sms.heytapmobi.com. DeviceId is a persistent identifier while the rest of them changes after factory reset. There is no evidence yet that heytapmobi can use deviceId to relink devices after factory reset, because vaid/deviceId never appear in the requests that contains duId or ouId. It is worth noting that in one request to api-cn.open.heytapmobi.com a header named openId is added but the value actually is vaid. Besides, the vaid that appears in heytap requests is the same as the one in i6.weather.oppomobile.com
(6) When a sim card is inserted, observed requests to sms.ads.heytapmobi.com/new/v5/phones, sms.ads.heytapmobi.com/new/api/get_sms_menu and log.avlyun.com with encrypted messages. The phone number and ouID is sent to sms.ads.heytapmobi.com/new/v5/phones for registration. Local wifi name, mac address, device details and AVLUDID are sent to log.avlyun.com.
(7) When making or receiving a phone call, my mobile number and ouId is post to sms.ads.heytapmobi.com. Phone numbers can be considered as a semi-persistent identifier, since in China each number is registered with the user's citizen ID. When receiving a phone call or a text, the caller/sender's phone number is also posted.
(8) The handset sends ouId and auId to u.bot.heytapmobi.com when opening clock app.

Pre-installed Non-Oneplus System Apps

(1) **Amap** transmits encrypted contents to aps.amap.com, offline.aps.amap.com, apsrgeo.amap.com and cgicol.amap.com. A unique CSID is associated with http requests to aps.amap.com but would change upon factory reset. Decrypting the post contents to apsrgeo.amap.com, we found that current geo-location is embedded in the message. I could not decrypt messages to aps.amap.com directly since it calls a JNI native function for encryption. Instead I hook an intermediate function to print out all the values, which contains nearby Wi-Fi names and their MAC addresses. Payload to cgicol.amap.com is loaded from a local database with some timestamps. Looks like regular logging without sensitive information.
(2) **China Mobile SDK** The handset sends requests to a.fxltsbl.com which belongs to a self-registering platform managed by China Mobile. The requests contains IMEI, device details, and deviceId (different from the deviceID sent to heytapmobi). Mac, lac, cellId and iccid exist in the posted json string but are not populated. The requests can be captured right after factory reset without a sim card, but cannot be observed if a sim card is inserted after factory reset.
(3) **China Unicom SDK** sends device details and IMEI to dm.wo.com.cn for device registration if no sim card is inserted. With a sim card, additional contents including encrypted ICCID, CellID, LAC, IMSI, MISIDN and MNC would be posted, which contains the coarse location information. At the moment that the user press 'reset this device', another request to dm.wo.com.cn would be made with IMEI and device details populated.
(4) **Sogo** The handset made a GET request to m.sogo.com which returns status code 302 and a cookie, but no subsequent requests is observed nor the cookie.
(5) **QQ** sends an empty request to tools.3g.qq.com which returns cookies, but never observe them in other connections.

2.1 Selected Connections During Startup After Factory Reset and When Idle

```
1
2  POST https://i6.weather.oppomobile.com/weather/
   location/v0/sdk?appId=app-weather&authCode=335736
   bf737176c4a9b840b40497ab31429a423bb4385f64826a..
3  Headers
4  *otaVersion: le2100_11_a.05*
5  *romVersion: LE2100_11_A.05*
6  *isForeign: 0*
7  *h: 2400*
8  *oid: f0E=%IV1%y91eRX+4nAcbESd9laGm9g==%AESK1%8
   zTyvgPf/+IMz21kIy2c7
9  ...
10 **request body**
11 {'mnc': '-1', 'bssid': '02:00:00:00:00:00', '
   latitude': '55.941', 'nid': '0', 'language': 'ZH-CN',
    'source': 'Google', 'mcc': '-1', 'ssid': '<unknown
   ssid>', 'lac': '0', 'sid': '0', 'vaid': '3
   DF103D64C9B4F6BBDCF93148C33676DEC7D424979CC
12 9C514F9390DE9C4D56D6', 'imei': '-1', 'bid': '0', '
   udid': '', 'oaid': '
   D601C6CC81A6467C979907FC27664CE6d63abc4491c9
13 997842600ab216af9138', 'longitude': '-3.179', 'cid':
   '0', 'ts': '2021-12-30 16:14:11 GMT'}
14
15 POST https://lang.coloros.com/enum/v1/child
```

```
{"aids":[{"aid":"single-language","versionCode":0}],"condition":{"brand":"oppo","otaVersionPrefix":"LE2100"},"devId":"3fa1159509fe997de556c5f9b889e156","mode":1}

POST https://log.avlyun.com/logupload?channel=coloros_wifi&pkg=com.coloros.wifisecuredetect

Headers
*X-Log-Version: 1.1*
*Charset: UTF-8*
*Content-Type: multipart/form-data;boundary=*******
*Accept-Encoding: gzip*
**request body**
decrypted:
#SYSINFO;{"kernel_version":"","name":"OnePlus9R_CH","security_patch":"2021-03-05","sdk":"30","incremental":"1618459936301","base_os":"","platform":"kona","manufacturer":"OnePlus"}
#ID;02C093E7B7E846D8FDC79D37C8CD3984 (AVLUDID);ERR_D;ERR_D;ERR_D;ERR_D;D52C9771-2B2F-447E-B273-2C0D1E004270 (random UUID);ERR_D;;;
#INFO;errUID_Java;coloros_wifi;11/OnePlus/LE2100_11_A.05;LE2100;FEEB1D874027AF97034D5EDD1E96F583;5fedf844;1.6.6;;GMT+00:00;zh_CN;;;;7
#WIFI;635eb9bf(timestamp in hex);androidprivacy;d4:5d:64:db:04:24;PSK;;;
#SERVERSTATUS;1609431108;1.1.17;00000;16;1;;;;;0;0;0;0;57721203274;;;;


GET tobcustomize.coloros.com
https://tobcustomize.coloros.com/cer/serverTime?openId=77283e2f97e308fd02604fd980232117ef1d975e3d10...&imei=&licenseCode=
Headers

POST https://moa-upload-online.coloros.com/cflLog/distributeTask
Headers
imei: RfT1FAuVXgoZfLWgvUJ56yZXhHFkJzKzi4IoU+sixbVZss0r6Dq+3wh825B21je6uTJZI/f7DbUheU+4mUrU8kgEhRYzX7TrrZK2oehzsdr1daOWqFkGpi4V1CuvVgRFb5QGPfL6hTZWtciSdBcI2Kra3tGpuhU1Sa8HyScmXoRixWpJoExBj7MMKwnDzIahaFQGNJYrvFvOnRlBVMfyDSKLdj76UTqKLHcyQjfkGmQXpM6G9TtryGGfptKcO7o69X949gjudpUa7laVS0QeVkTGcoqvG7IMIvvap6vKSc95wLOzotscNJs/jaGaLikbLX/+OfjBq7GCvneDS0HU1g==
guid: f5rT0TD81TeIGtoKn5IJVxcmASUp0EL/2n1Vtfn7xJBUEB9tepa+WKSZc+1boTyu/hWPm1LPJNxhfLm3fNWRPrMvzX6eBqbWdDz01asVjd6cyuqG2F/tT0Yqy+LGD3vabluH891zY194Z9WQ4SNX9LqKuRk2pjvht7zFi9GIkGvEhvU5DhXZVW3NM6ZaTem/Avj0R5ylH2JH3hYLrkTvuSdn1XTnTw4T399MU2nTEAwHTiWr0iHDx5Cz5A0tjSopVrwL5Zm7ESVaj/SVxWejcWYHYzqQ6NmAx8oPSyHOt+Fk2N5gSHNWD5lDW2ZOSpjLit8kjso8PNqAy2PZA3E8YQ==

POST https://data.sms.heytapmobi.com/android/oppo/yellowpage
POST body:
b'{"data":{"index":0,"isWifi":1,"sdk":"3.5.26_deepSleep"},"header":{"p1":"android","p2":"2_5D6B04CC81CE431AB88507C5724CC122d63abc4491c99978...","p3":"3.2.65","p4":30,"p5":"LE2100","p6":"OnePlus","p8":20200100,"p9":["0.0","0.0"],"p10":0,"p11":"2165x1080","p16":"","p17":"20.0.33","p18":"CN","p19":"\xe4\xb8\xad\xe6\x96\x87","p20":"OnePlus","p21":"RKQ1.201105.002","p25":["","CN","CN",null,null,null],"pa0":"1"}}'
Response:
... {"url":"https://tedsyncfs.coloros.com/oppo/yellowpage/20220531_1654000621166/1654000621166_small.edic"} ...


GET https://tedsyncfs.coloros.com/oppo/yellowpage/20220531_1654000621166/1654000621166_small.edic

POST https://icosa.coloros.com/cosa/apk/info
Headers
*colorOSVersion: V11.2*
*trackRegion: *
*otaVersion: LE2100_11.A.05_0050_202104151115*
*romVersion: LE2100_11_A.05*
*androidVersion: 11*
*sign: 3a6b19558a74292de706bc5fcfcaa372118f56...*
*guid: 77283e2f97e308fd02604fd980232117ef1d975e3d109...*
*model: LE2100*
*language: zh-CN*
*operator: *
*uRegion: CN*
*timestamp: 1654037116110*
*Content-Type: application/json; charset=utf-8*
*Accept-Encoding: gzip*
**request body**
["com.unionpay.tsmservice","com.youku.phone","com.nearme.play","com.dianping.v1","com.heytap.health","me.ele","com.heytap.reader","com.baidu.searchbox","com.wuba","com.tencent.qqlive","com.redteamobile.roaming","com.tencent.mtt","com.xunmeng.pinduoduo","com.tencent.weishi","com.ss.android.article.news","com.nearme.gamecenter","com.topjohnwu.magisk","com.ximalaya.ting.android","com.baidu.BaiduMap","com.zhihu.android","com.oneplus.bbs","com.tencent.news","com.heytap.opluscarlink","com.jingdong.app.mall","ctrip.android.view","com.android.email","com.sina.weibo","com.smile.gifmaker","com.taobao.taobao","tv.danmaku.bili","com.eg.android.AlipayGphone","com.heytap.smarthome","com.achievo.vipshop"]

POST https://classify.apps.coloros.com/api/getCategoryInfo
Headers
*content-type: application/x-www-form-urlencoded*
*Accept-Encoding: gzip*
**request body**
sign=5038471c6595238c001664ba224de95e&packageName=com.android.settings,com.coloros.phonemanager,com.finshell.wallet,com.heytap.cloud,com.heytap.vip,com.oneplus.camera,com.coloros.gamespaceui,com.coloros.soundrecorder,com.dianping.v1,com.heytap.reader,com.nearme.play,com.oppo.store,com.tencent.weishi,me.ele,com.android.stk,com.coloros.alarmclock,com.coloros.backuprestore,com.coloros.filemanager,com.heytap.market,com.heytap.music,com.heytap.speechassist,com.heytap.themestore,com.android.email,com.coloros.calculator,com.coloros.compass2,com.coloros.familyguard,com.coloros.note,com.coloros.shortcuts,com.coloros.weather2,com.eg.android.AlipayGphone,com.heytap.health,com.heytap.smarthome,com.nearme.gamecenter,com.oneplus.bbs,com.redteamobile.roaming,com.sina.weibo,com.ss.android.article.news,com.tencent.news,com.topjohnwu.magisk,com.wuba,com.ximalaya.ting.android,com.zhihu.android,ctrip.android.view,tv.danmaku.bili&timestamp=1654038331990

GET https://httpdns.push.heytapmobi.com/getdns/v1?region_code=CN&region_mark=CN&mcs_version=4704&netType=WIFI&brand=&deviceId=e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934c..&vaid=3DF103D64C9B4F6BBDCF93148C33676DEC7D424979CC9C514F..

POST https://stg-data.ads.heytapmobi.com/proxy/strategy/
**request body**
{"head":{"model":"LE2100","osVersion":"LE2100_11_A.05","ptoVer":103,"region":"CN","brand":"ONEPLUS","duId":"3DF103D64C9B4F6BBDCF93148C33676DEC7D42...","ouId":"D601C6CC81A6467C979907FC27664CE6d63abc44..."},"body":{"pkgName":"com.opos.ads","currTime":1639645282}}
```

```


GET http://m.sogo.com/
Set-Cookie: ABTEST=4|1654037122|v1; expires=Thu, 30-Jun-22 22:45:22 GMT; path=/, SNUID=1E025D028E8B6ED9089565378FDAE187; expires=Wed, 31-May-23 22:45:22 GMT; domain=.sogo.com; path=/

GET https://tools.3g.qq.com/wifi/cw.html
Set-Cookie: tgw_l7_route=34844eaa810b839368c498b21d72f453; Expires=Tue, 31-May-2022 23:15:23 GMT; Path=/
```

2.2 Additional connections when making a phone call

```

POST https://sms.ads.heytapmobi.com/api/get_next_config

POST body:
b'{"data":{"index":0,"isWifi":1,"sdk":"3.5.26_deepSleep"},"header":{"p1":"android","p2":"TA8ceffc7322d2ae2e","p3":"5.12.20_06a5641_210301","p4":30,"p5":"LE2100","p6":"OnePlus","p7":"+86131xxxxxxxx","p8":20200100,"p9":["0.0","0.0"],"p10":0,"p11":"2297x1080","p16":"","p17":"21.0.44","p18":"GB","p19":"\xe4\xb8\xad\xe6\x96\x87","p20":"OnePlus","p21":"RKQ1.201105.002","p23":"8986011485103421783 6","p25":["GB",null,"CN",null,null,null],"pa0":"1"}}


POST https://data.sms.heytapmobi.com/dot.php

**request body**
{"header":{"p1":"android","p2":"2_D601C6CC81A6467C979907FC27664CE6d63abc4491c99978426...","p3":"5.12.20_06a5641_210301","p4":30,"p5":"LE2100","p6":"OnePlus","p7":"+86131xxxxxxxx","p8":20200100,"p9":["0.0","0.0"],"p10":0,"p11":"2297x1080","p16":"","p17":"21.0.44","p18":"GB","p19":"","p20":"OnePlus","p21":"RKQ1.201105.002","p23":"8986011485103421783 6","p25":["GB",null,"CN",null,null,null],"pa0":"1"},"data":{"sms_card_patch_ac.index.updater":"030804110003 89{}"}}
```

2.3 Connections when sending or receiving a text

```
POST https://sms.ads.heytapmobi.com/new/v5/phone
Headers
*keyver: 2*
*content-type: text/plain; charset=UTF-8*
*accept-encoding: gzip*
**request body**
{"header":{"p1":"android","p2":"2_D601C6CC81A6467C979907FC27664CE6d63abc4491c..","p3":"5.12.20_06a5641_210301","p4":30,"p5":"LE2100","p6":"OnePlus","p7":"+86131xxxxxxxx","p8":20200100,"p9":["0.0","0.0"],"p10":0,"p11":"2297x1080","p16":"","p17":"21.0.44","p18":"CN","p19":"","p20":"OnePlus","p21":"RKQ1.201105.002","p23":"8986011485103421783 6","p25":["GB",null,"CN",null,null,null],"pa0":"1"},"data":{"phone":"+44751xxxxxxx","dialNumber":"+44751xxxxxxx","dataType":1,"operationType":1,"duration":0,"contact":-1,"recordtime":1641152344516,"city":"","scenetype":2,"contentSign":[],"lasttime":-1}}
```

2.4 Additional Connections When Insert Sim

```

POST http://dm.wo.com.cn:18080/registerv3?ver=3.0&model=LE2100&manuf=OnePlus&sign=XMxQesa6pXoiaOBnUW8xnBc2IMnKbchLUCVXZYdSXTivVO8PaC7fydMIzcdVe5z64oxlGCHOAjEQ%0Aqh6htGoO9bYuUHzci4Ib%2FLcd9HCVruBafllOo7f9dTnpt0Oo2IOt%2Bl0%2FO9fOzaDIQBmRVjtjVftb%0AuJxXcrvS0%2B3McPGt2Oc%3D%0A
Headers
*Content-Type: application/encrypted-json*
*Accept-Encoding: gzip*
**request body**
POST body:
{"Manuf":"OnePlus","Model":"LE2100","HWVersion":"11","SWVersion":"LE2100_11_A.05","OS":"Android","OSVersion":"11","IMEI1":"869046054827160","ICCID1":"","IMSI1":"","MSISDN1":"","MNC1":"","NCLS1":"","CellID1":"","LAC1":"","VolteEnabled1":"","5GEnabled1":"1",
"IMEI2":"869046054827178",
"ICCID2":"9e65fd583a83699d0157af778a7d0202","IMSI2":"b2d5c6783e3fa6eef38ff1fc7dedfb10","MSISDN2":"fb398f2a0e357c02ff3b3934ba4c7593","MNC2":"23415","NCLS2":"LTE","CellID2":"0cd39c5bab62729240cfec53d339392b","LAC2":"2e95ade370c3871fda51e03448bf1b20","VolteEnabled2":"1","5GEnabled2":"","DataSlot":"2","AccType":"WiFi","SubType":{"RAM":"8G","ROM":"256G","FREE":"218G"},"DeviceType":"000005","RegType":"T","SpecVersion":"3.0","RegVersion":"1.2-20210112","Time":"2022-06-19 21:46:00","AppInfo":"","History":[{"Manuf":"OnePlus","Model":"LE2100","HWVersion":"11","SWVersion":"LE2100_11_A.05","OS":"Android","OSVersion":"11","IMEI1":"869046054827160","ICCID1":"","IMSI1":"","MSISDN1":"","MNC1":"","NCLS1":"","CellID1":"","LAC1":"","VolteEnabled1":"","5GEnabled1":"","IMEI2":"869046054827178","ICCID2":"","IMSI2":"","MSISDN2":"","MNC2":"","NCLS2":"","CellID2":"","LAC2":"","VolteEnabled2":"","5GEnabled2":"","DataSlot":"0","AccType":"Disconnected","SubType":{"RAM":"8G","ROM":"256G","FREE":"218G"},"DeviceType":"000005","RegType":"F","SpecVersion":"3.0","RegVersion":"1.2-20210112","Time":"2020-12-31 16:08:09","AppInfo":""}]}

POST https://sms.ads.heytapmobi.com/new/v5/phone
Headers
*keyver: 2*
*content-type: text/plain; charset=UTF-8*
*accept-encoding: gzip*
**request body**
{"header":{"p1":"android","p2":"2_D601C6CC81A6467C979907FC27664CE6d63abc4491c9997842600ab216af9138","p3":"5.12.20_06a5641_210301","p4":30,"p5":"LE2100","p6":"OnePlus","p7":"+86131XXXXXXX","p8":20200100,"p9":["0.0","0.0"],"p10":0,
"p11":"2297x1080","p12":"46001","p14":"460013434948555","p16":"","p17":"21.0.44","p18":"CN","p19":"","p20":"OnePlus","p21":"RKQ1.201105.002","p23":"8986011485103421783 6","p25":["GB",null,"CN",null,null,null],"pa0":"1"},
"data":{"phone":"106551951330490120","dialNumber":"106551951330490120","dataType":1,"operationType":1,"duration":0,"contact":-1,"recordtime":1641112914602,"city":"","scenetype":2,"contentSign":[""],"lasttime":-1}}
```

2.5 Connections with Amap

```
POST http://apsrgeo.amap.com/rgeo/r?q=1&language=cn
Headers
*et: 111*
*Content-Type: application/x-www-form-urlencoded*
*Accept-Encoding: gzip*
POST body:
```

{"data":"<?xml version=\"1.0\" encoding=\"UTF-8\"?><ReverseGeoRQ xmlns=\"http:\/\/rgeo.amap.com\/wps\/2014\" version=\"2.24\" street-address-lookup=\"full\"><authentication version=\"2.2\"><key key=\"eJwVwbkNACAMBLCaYSLlIM-1ScFSiN0RNgb0g1PHge4yLkqUpTR9SSQg1WG16R457wMMKgrm\" username=\"AutoNavi\" \/><\/authentication><point><**latitude**>55.941397<\/latitude><**longitude**>-3.178805<\/longitude><\/point><\/ReverseGeoRQ>","headers":{"restKey":"ee282ec01d1dc9d6eb663f6b19bc5832","imei":"","utdid":"","adiu":"kc8ekchkff668iogofcec93b1da744","sourcePackageName":"com.oppo.nhs","productVersion":"oppo_nlp_42_20130418_5.0.30_a072"}}

POST http://aps.amap.com/APS/r?ver=5.1&q=0&csid=0809b3aa-e9c1-46ec-be1d-721492fb8f93

Headers

gzipped: 1
Accept-Encoding: gzip
et: 111
Content-Type: application/octet-stream

actual post body is not json and does not contain field names, but just values in a compact format. This json below is an intermediate output of the code.

{"curTime":1658011651048,"ver":"5.1","action":1,"respctrl":0,"src":"oppo_nlp_42_20130418","license":"BNPO0B7B4T8OW907232P986CEDE38QW","model":"LE2100","os":"android11","appName":"5.0.30_a072,com.amap.android.location","imei":"","imsi":"","sn":"","smac":"00:00:00:00:00:00","sdkVersion":"nlp_5.0.30_a072","utdid":"","adiu":"","nettype":"","inftype":2,"gtype":0,"fps":{"cellStatus":{"updateTime":4328613,"cellType":5,"mainCell":{"type":1,"mcc":234,"mnc":10,"lac":21929,"cid":60889632,"sid":0,"nid":0,"bid":0,"signalStrength":85,"latitude":0,"longitude":0,"cellAge":0,"lastUpdateTimeMills":0,"registered":true},"cell2":[{"type":4,"mcc":234,"mnc":10,"lac":21929,"cid":60889632,"sid":0,"nid":0,"bid":0,"signalStrength":-120,"latitude":0,"longitude":0,"cellAge":208,"lastUpdateTimeMills":4119726,"registered":false},{"type":4,"mcc":2147483647,"mnc":2147483647,"lac":2147483647,"cid":2147483647,"sid":0,"nid":0,"bid":0,"signalStrength":-120,"latitude":0,"longitude":0,"cellAge":1463,"lastUpdateTimeMills":2865569,"registered":false}]},"wifiStatus":{"updateTime":4326201,"mainWifi":{"mac":"d4:5d:64:db:04:20","ssid":"\"androidprivacy\"","rssi":-26,"frequency":2427,"timestamp":4326493,"type":0},"wifiList":[{"mac":"5c:02:14:89:8d:ef","ssid":"Xiaomi_8DEE","rssi":-27,"frequency":2412,"timestamp":4324537,"type":0},{**"mac"**:"d4:5d:64:db:04:20",**"ssid"**:"androidprivacy","rssi":-27,"frequency":2427,"timestamp":4324788,"type":0},{**"mac"**:"00:08:32:8e:f9:c0",**"ssid"**:"UNITE-Corporate","rssi":-50,"frequency":2462,"timestamp":4325355,"type":0},{"mac":"00:08:32:8e:f9:c6","ssid":"","rssi":-50,"frequency":2462,"timestamp":4325356,"type":0},{"mac":"00:08:32:8e:f9:c1","ssid":"UNITE-Staff","rssi":-51,"frequency":2462,"timestamp":4325355,"type":0},{"mac":"00:08:32:8e:f9:c3","ssid":"uS-Glide","rssi":-51,"frequency":2462,"timestamp":4325355,"type":0},{"mac":"00:08:32:8e:f9:c9","ssid":"","rssi":-56,"frequency":5320,"timestamp":4325393,"type":0},{"mac":"00:08:32:8e:f9:cf","ssid":"U
NITE-Corporate","rssi":-57,"frequency":5320,"timestamp":4325448,"type":0},{"mac":"00:08:32:8e:f9:cc","ssid":"uS-Glide","rssi":-57,"frequency":5320,"timestamp":4325449,"type":0},{"mac":"00:08:32:8e:f9:ce","ssid":"UNITE-Staff","rssi":-58,"frequency":5320,"timestamp":4325448,"type":0},{"mac":"00:08:32:8e:94:00","ssid":"UNITE-Corporate","rssi":-63,"frequency":2437,"timestamp":4324920,"type":0},{"mac":"00:08:32:8e:94:01","ssid":"UNITE-Staff","rssi":-63,"frequency":2437,"timestamp":4324920,"type":0},{"mac":"00:08:32:8e:94:03","ssid":"uS-Glide","rssi":-63,"frequency":2437,"timestamp":4324920,"type":0},{"mac":"00:08:32:8e:94:06","ssid":"","rssi":-64,"frequency":2437,"timestamp":4324921,"type":0},{"mac":"d8:47:32:04:87:ba","ssid":"LuttonPlaceBowlingClub","rssi":-77,"frequency":2422,"timestamp":4324638,"type":0},{"mac":"72:8d:26:ae:81:4f","ssid":"BTWi-fi","rssi":-82,"frequency":2437,"timestamp":4324953,"type":0},{"mac":"00:08:32:8e:dd:af","ssid":"UNITE-Corporate","rssi":-86,"frequency":5200,"timestamp":4324574,"type":0},{"mac":"00:08:32:8e:dd:ae","ssid":"UNITE-Staff","rssi":-86,"frequency":5200,"timestamp":4324574,"type":0},{"mac":"00:08:32:8e:dd:ac","ssid":"uS-Glide","rssi":-86,"frequency":5200,"timestamp":4324575,"type":0},{"mac":"00:08:32:8e:dd:a9","ssid":"","rssi":-87,"frequency":5200,"timestamp":4324558,"type":0}]}},"macsAge":2}

2.6 Connections With China Mobile

POST https://a.fxltsbl.com/accept/sdkService?func=tsdk:postreglog&appkey=A100000357&timestr=1654037702226&imei=869046054827178&version=v2&token=10d5ede314322d195c911d4a57ace907

Headers

Content-Type: application/json; charset=utf-8
Accept-Encoding: gzip
request body

{"sdkVersion":"2.1.11",**"imei1"**:"869046054827178","imei2":"869046054827160",**"deviceId"**:"869046054827178","brand":"OnePlus","model":"LE2100","firmwareVer":"LE2100_11_A.05","systemVer":"11","cpu":"SM8250_AC","rom":"256G","ram":"8.00 GB","type":"1","iccid1":"","iccid2":"","imsi1":"","imsi2":"","mac":"","cellId":"-1","lac":"-1","channel":"18","dataCard":"0","masterStatus":"-1","sendTime":"1654037702188","soltQuantity":"2","dataCard2":"0","soltService1":"1","soltService2":"1","soltNetwork1":"0","soltNetwork2":"0","cellId2":"-1","lac2":"-1","inType":"OPPO LE2100","verify":"imei_unKnown#imsi_unKnown#mac_null#brand_OnePlus#model_LE2100#version_11#totalRam_8GB#SDFreeSpace_223011.46484375#cpu_Qualcomm Technologies, Inc SM8250_AC#screen_1080*2165#SimSerialNumber__unKnown#romSpace_242 GB#battery_100#ROTATION_VECTOR:Y||GYROSCOPE_UNCALIBRATED:Y||GAME_ROTATION_VECTOR:Y||AMBIENT_TEMPERATURE:N||GYROSCOPE:Y||LIGHT:Y||STEP_COUNTER:Y||LINEAR_ACCELERATION:Y||GRAVITY:Y||RELATIVE_HUMIDITY:N||MAGNETIC_FIELD_UNCALIBRATED:Y||GEOMAGNETIC_ROTATION_VECTOR:Y||PRESSURE:N||TEMPERATURE:N||ORIENTATION:Y||ACCELEROMETER:Y||SIGNIFICANT_MOTION:Y||STEP_DETECTOR:Y||PROXIMITY:Y||#","phoneNumber1":"unknown","phoneNumber2":"unknown","status5g1":"0","status5g2

3 REALME

Summary:

(1) Weather app sends OID, VAID, and OAID to oppo server i6.weather.oppomobile.com. Geo-location (latitude and longitude) is transmitted in subsequent requests. Fields lac, and imei exist in the requests but no values are filled in.
(2) The handset sends device details, GUID, OUID, statUId, IMEI and telemetry (event logs and error logs) to dragate.dc.oppomobile.com, in which GUID and IMEI are persistent. GUID the same as what is transmitted to irus.coloros.com.
(3) The handset sends GUID to irus.coloros.com, sends a subset of installed apps to icosa.coloros.com and sends devId to lang.coloros.com. Note that devId would change after factory reset while GUID is persistent.
(4) GUID and sim card status (inserted or not) is posted to esa-reg.myoppo.com periodically.
(5) Same as OnePlus, the handset transmits encrypted contents to log.avlyun.com with the package name com.coloros.wifisecuredetec in the requests. The package would be launched as soon as wifi is enabled and initiates those requests. The time gap between 'enabling wifi' and 'posting requests' is extremely small. By the time frida hooked the functions in this package, the requests are already sent. contents are still unknown.
(6) requests to jits-static-cn.heytapmobi.com contains an id. What is it?
(7) when receiving/sending a text or receiving a phone call, the device sends request to sms.ads.heytapmobi.com which contains both caller's and callee's phone number, device details, duration of the call, OAID and VAID. The handset posts device details (brand, model, screen size, locale) and phone number to sms.ads.heytapmobi.com/api/get_next_config
(8) when the clock app is opened, the handset transmits OUID and AUID to u.bot.heytapmobi.com.

Pre-installed Non-Realme System Apps

(1) **China Mobile SDK** The handset sends multiple requests to a.fxltsbl.com which belongs to a self-registering platform managed by China Mobile. The requests contains IMEI, device details, and all the installed apps. If a sim card is inserted, CellId and lac are also populated.
(2) **Amap** The handset sends encrypted contents to apsrgeo.amap.com, aps.oversea.amap.com, offline.aps.amap.com. The request to apsrgeo.amap.com contains the coordinate of the current location, device details and amap identifiers, including adiu and utdid. Data posted to offline.aps.amap.com contains similar information except for the coordinates. The request to aps.oversea.amap.com incorporate device details, identifiers and also the local Wi-Fi name. adiu and utdid can be reset while restKey are hardcoded in the package.
(3) **sogo** The handset initiate a request to m.sogo.com which routinely set cookies but no subsequent requests observed.
(4) **QQ** sends an empty request to tools.3g.qq.com which returns cookies, but never observe them in other connections.

3.1 Selected Connections During Startup After Factory Reset and When Idle

```
POST https://i6.weather.oppomobile.com/weather/location/v0/sdk?appId=app-weather&authCode=ccf3b4f09c62d6bbd72fa987692510bf50454ca1fb4f..
Headers
*otaVersion: rmx2205_11_a.13*
*romVersion: RMX2205_11_A.13*
*isForeign: 0*
*h: 2400*
*oid: H3I=%IV1%oOzvEZuCgxZ6fNd0N62uIw==%AESK1%Zzp4ByLj1TtnOmHkh22IoQh2FujPC8TLVqqpcBeOaIQ=*
*encryptFlag: 2*
*versionName: 8.2.23*
*pkg: com.coloros.weather.service*
*versionCode: 8002023*
*timeStamp: 1640448232*
*osVersion: V11.1*
*androidVersion: 11*
*w: 1080*
*pkgName: com.coloros.weather.service*
*model: RMX2205*
*authType: 2*
*Content-Type: application/json; charset=utf-8*
*Accept-Encoding: gzip*
**request body**
{'mnc': '-1', 'bssid': '02:00:00:00:00:00', 'latitude': '55.941', 'nid': '0', 'language': 'ZH-CN', 'source': 'Google', 'mcc': '-1', 'ssid': '<unknown ssid>', 'lac': '0', 'sid': '0', 'vaid': '639F1ADD7B6F4CBB8397F82BFAAA988DEC7D42..', 'imei': '-1', 'bid': '0', 'udid': '', 'brand': 'realme', 'oaid': 'FEBF51FCD61E4183BB9113639DDA82F882e82..', 'longitude': '-3.179', 'cid': '0', 'ts': '2021-12-25 16:03:49 GMT'}

POST https://irus.coloros.com/post/Download\_Result
Headers
*user-agent: RMX2205/11/V11.1/3.3.57*
*Content-Type: application/json; charset=utf-8*
*Accept-Encoding: gzip*
**request body**
{"androidVersion":"Android11","colorOSVersion":"ColorOS11.1","imei":"2a3d941aabfc7732b34ceff7820330ebc25b01d3712f8901a..","infos":[{"code":"safe\_floatwindow\_whitelist","newMd5":"0005fe5c4a6c42611bc8e51b87dfae95","oldMd5":"0005fe5c4a6c42611bc8e51b87dfae95"},{"code":"sys\_wms\_intercept\_window","newMd5":"1cb0987b55c0a47eeb3aaaff5fe06cad","oldMd5":"1cb0987b55c0a47eeb3aaaff5fe06cad"},{"code":"safe\_boot\_whitelist","newMd5":"6574ece3847bc128067a6711198ee18f","oldMd5":"6574ece3847bc128067a6711198ee18f"}],"nvCarrier":"10010111","operator":"","otaVersion":"RMX2205\_11.A.13\_0130\_202108051817","productName":"RMX2205","trackRegion":"CN","romVersion":"RMX2205\_11\_A.13","size":"1394","time":1640458731836,"uRegion":"CN","version":"3"}

the IMEI above is actually GUID


POST https://icosa.coloros.com/cosa/apk/info
Headers
*colorOSVersion: V11.1*
*trackRegion: *
*otaVersion: RMX2205\_11.A.13\_0130\_202108051817*
*romVersion: RMX2205\_11\_A.13*
*androidVersion: 11*
*sign: cab36e72495fc026c0248a0d3430a0429b27ecd..*
*guid: 2a3d941aabfc7732b34ceff7820330ebc25b01d3712f89..*
*model: RMX2205*
*language: zh-CN*
*uRegion: CN*
```

request body
["com.unionpay.tsmservice","com.youku.phone","com.nearme.play","me.ele","com.taobao.litetao","com.baidu.searchbox","com.wuba","com.realme.linkcn","com.realmecomm.app","com.redteamobile.roaming","com.tencent.mtt","com.xunmeng.pinduoduo","com.ss.android.article.news","com.nearme.gamecenter","com.topjohnwu.magisk","com.sankuai.youxuan","com.baidu.BaiduMap","com.dragon.read","com.Qunar","com.heytap.opluscarlink","com.jingdong.app.mall","com.android.email","com.sina.weibo","com.smile.gifmaker","com.taobao.taobao","com.heytap.book","com.eg.android.AlipayGphone","com.heytap.smarthome","com.achievo.vipshop"]

POST https://dragate.dc.oppomobile.com/v1/stat/rosdau?appid=21000&logtag=0&nonce=2836&timestamp=1640453885&sign=344a87acbac98f3962930431fe254b03
Headers
Content-Encoding: gzip
Content-Type: text/json; charset=UTF-8
Accept-Encoding: gzip
request body

{"head":{"model":"RMX2205","osVersion":"V11.1","androidVersion":"11","romVersion":"RMX2205_11_A.13","sdkVersion":"5.1.19235","postTime":"1640453885707","carrier":99,"access":"WIFI","channel":"ColorOS","operatorID1":"","operatorID2":"","region":"CN","brand":"realme","**imei**":"865130051443611","**imei2**":"865130051443603","meid":"A00000E503339B","pcba":"00206190192803220000 8338","clientID":"","**duid**":"639F1ADD7B6F4CBB8397F82BFAAA988DEC7D424979CC9...","**ouid**":"FEBF51FCD61E4183BB9113639DDA82F882e82127b7...","**guid**":"2a3d941aabfc7732b34ceff7820330ebc25b0...","os_properties":"otaVersion\u0002RMX2205_11.A.13_0130_202108051817\u0001multi_user_id\u00020\u0001ouid_status\u00021\u0001gaid\u0002dbab177b-211a-47e6-9432-ebc56c040ffb"},"body":[{"clientTime":"2021-12-25 17:38:05","network":"WIFI","resolution":"1080*2293","ramTotal":7.354,"romTotal":107.731,"romReserve":100.26,"ro.boot.vbmeta.device_state":"","**ro.boot.flash.locked**":"0","sim1Carrier":"","sim2Carrier":"","imeis":"865130051443611\u0003865130051443603\u0003\u0003","meids":"A00000E503339B\u0003A00000E503339B\u0003\u0003","iccids":"","imsis":"\u0003","properties":"ota_version\u0002RMX2205_11.A.13_0130_202108051817\u0003user_lang\u0002zh\u0003switchUE\u00020"}]}

POST https://dragate.dc.oppomobile.com/v1/stat/revent?appid=20142&logtag=0&nonce=5873&timestamp=1640446316&sdk_version=54026&sign=b2375cb4e28ef9174ec50ac7e4addca0
Headers
Content-Encoding: gzip
Content-Type: text/json; charset=UTF-8
Accept-Encoding: gzip
User-Agent: 3.12.6
request body

{"head":{"model":"RMX2205","postTime":"1640446316263","osVersion":"V11.1","androidVersion":"11","channel":"2203","region":"CN","romVersion":"RMX2205_11_A.13","access":"WIFI","sdkVersion":54026,"appPackage":"com.nearme.instant.platform","brand":"realme","localId":"G0b7b2a6a16738df3b21122421465","imei":"","multi_user_id":"0","guid":"2a3d941aabfc7732b34ceff7820330ebc25b01d3712f8...","duid":"639F1ADD7B6F4CBB8397F82BFAAA988DE...","ouid":"FEBF51FCD61E4183BB9113639DDA82F882e8...","statUId":"7b825b798e4c2dd74c27d6b27b3f6a0f","carrier":"none","appId":20142,"appVersion":"4.2.1","ssoid":"0","clientTime":"1640446316370"},"body":{"ekv":[{"eventID":"2212","eventTag":"web_app","eventTime":"2021-12-25 15:31:55.933","appId":20142,"appVersion":"4.2.1","duration":0,"access":"WIFI","statSId":"","E_source":"UNDEFINED","E_client_time":"2021-12-25 15:31:55.916","dcsMsgId":"96003668-c1b7-42f4-a1f9-edc6c09eb591","E_launch_type":"UNDEFINED","appCode":"20142","chimera_config_eventid":"8","E_ver_id":"non","E_mainProcess":"1","E_app_id":"non","E_platformVersion":"1081","E_s_package":"UNDEFINED","E_engine_mode":"APP","chimera_config_logmap":"2","E_scene":"UNDEFINED"},{"eventID":"2211","eventTag":"web_app","eventTime":"2021-12-25 15:31:56.243","appId":20142,"appVersion":"4.2.1","duration":0,"access":"WIFI","statSId":"","E_source":"UNDEFINED","E_client_time":"2021-12-25 15:31:55.930","chimera_init_state":"onInitError","dcsMsgId":"2b747e86-6dbd-4b20-8152-add6fc716b7f","E_launch_type":"UNDEFINED","appCode":"20142","E_ver_id":"non","E_mainProcess":"1","E_app_id":"non","E_platformVersion":"1081","E_s_package":"UNDEFINED","E_engine_mode":"APP","chimera_init_fail_code":"2","E_scene":"UNDEFINED"}]}}

POST https://dragate.dc.oppomobile.com/v1/stat/revent?appid=20214&logtag=0&nonce=4705&timestamp=1640647700&sdk_version=54021&sign=fd4cb9a86b45fb3fb24164c94c6b0141
Headers
Content-Encoding: gzip
Content-Type: text/json; charset=UTF-8
Accept-Encoding: gzip
request body
ascci decode exception
matched secretKeyID
{"head":{"model":"RMX2205","postTime":"1640647700022","osVersion":"V11.1","androidVersion":"11","channel":"1","region":"CN","romVersion":"RMX2205_11_A.13","access":"WIFI","sdkVersion":54021,"appPackage":"com.heytap.yoli","brand":"realme","localId":"G006ca8f3c2992922921122759038","imei":"","multi_user_id":"0","guid":"","duid":"639F1ADD7B6F4CBB8397F82BFAAA988...","ouid":"FEBF51FCD61E4183BB9113639DDA82F882e82127b750de77...","statUId":"7b825b798e4c2dd74c27d6b27b3f6a0f","carrier":"none","appId":20214,"appVersion":"40.4.9.5.1","ssoid":"0","clientTime":"1640647700086"},"body":{"ekv":[{"eventID":"10006","eventTag":"10000","eventTime":"2021-12-27 23:28:17.276","appId":20214,"appVersion":"40.4.9.5.1","duration":0,"access":"WIFI","statSId":"","host":"i.youlishipin.com","region":"CN","adg":"49794","aug":"","error_message":"ServerHostResponse is null,error is java.net.SocketTimeoutException: timeout","dcsMsgId":"7aebdd71-5b64-41b6-95fa-83fd444fbae6"},{"eventID":"10006","eventTag":"10000","eventTime":"2021-12-27 23:28:17.277","appId":20214,"appVersion":"40.4.9.5.1","duration":0,"access":"WIFI","statSId":"","host":"i.youlishipin.com","region":"CN","adg":"49794","aug":"","error_message":"ServerHostResponse is null,error is java.net.SocketTimeoutException: timeout","dcsMsgId":"e040cd65-b3cd-4e1f-98d8-896e96423361"},{"eventID":"10006","eventTag":"10000","eventTime":"2021-12-27 23:28:17.278",....

POST https://esa-reg.myoppo.com/api/phoneV3/submit
Headers
Content-Type: application/json; charset=utf-8
Accept-Encoding: gzip
request body

```
{'appId': 'phone_client', 'sign': '
E1F8CFA692376C696D35F0CD3A64B0C7', 'aesIv': '
HVAway51BV0RYCljfHc0XQ==', 'body': '{"SimId":"","
osVersion":"20","submitType":100,"isSimInserted":
false,"key":"
2a3d941aabfc7732b34ceff7820330ebc25b01d3712f..."}\x03\
x03\x03', 'timestamp': 1640448226}
<<< HTTP 200, 64.00B

the key above is GUID. isSimInserted would be set to
true if a sim card is inserted.
```

3.2 Additional connections when making/receiving a phone call

```

POST https://sms.ads.heytapmobi.com/new/v5/phone
Headers
*keyver: 2*
*content-type: text/plain; charset=UTF-8*
*accept-encoding: gzip*
**request body**
{"header":{"p1":"android","p2":"2
_FEBF51FCD61E4183BB9113639DDA82F882e82127b750...","p3
":"5.13.50_4357d47_210611","p4":30,"p5":"RMX2205","p6
":"realme","p7":"+86131xxxxxxxx","p8":20200100,"p9
":["0.0","0.0"],"p10":0,"p11":"2293x1080","p16":"","
p17":"21.0.48","p18":"GB","p19":"","p20":"realme","
p21":"RP1A.200720.011","p25":["GB",null,"CN",null,
null,null],"pa0":"1"},"data":{"phone":"0751xxxxxxx","
dialNumber":"0751xxxxxxx","dataType":5,"operationType
":1,"duration":15,"contact":-1,"recordtime":0,"city
":"","scenetype":10,"ringtime":0,"lasttime":-1}}

POST https://sms.ads.heytapmobi.com/api/sha_info
Headers
*accept-charset: UTF-8*
*x-sdk-version: 21.0.48*
*accept-encoding: gzip*
*content-type: application/json;charset=utf-8*
*tap-gslb: 0,0*
*route-data:
MQE0OTc5NAE1MDEzMDUwAVJNWDIyMDUBcmVhbG1lAUNOAQ==*
**request body**
{"header":{"imei":"TA80a616d5d2ef6286","model":"
RMX2205","osVersion":"V11.1","romVersion":"
RMX2205_11_A.13","androidVersion":"11","apiVersion
":30,"versionName":"REL","versionCode":"5013050","
clientTime":1640612885002,"oaId":"
FEBF51FCD61E4183BB9113639DDA82F882e82...","
vaId":"7443923
F7CC14581B8DD4034243251C927717f5c9c6d559c71d438251cf64300
"},"data":{"lastTime":0,"page":1,"pageCount":50,"
version":1}}
```

3.3 Connections When a sim card inserted

```
POST https://c
Headers
*Content-Type: application/json;charset=UTF-8*
*Accept-Encoding: gzip*
**request body**
ascci decode exception
**pb decode failed**
Decoding message of length 123 (1,394)
Trying protobuf again with pb_start= -1
POST body:
`b'{"data":{"index":0,"isWifi":1,"sdk":"3.5.27
_deepSleep"},"header":{"p1":"android","p2":"
TA80a616d5d2ef6286","p3":"5.13.50_4357d47_210611","p4
":30,"p5":"RMX2205","p6":"realme","p7":"
+86131xxxxxxxx","p8":20200100,"p9":["0.0","0.0"],"p10
":0,"p11":"2293x1080","p16":"","p17":"21.0.48","p18
":"GB","p19":"\xe4\xb8\xad\xe6\x96\x87","p20":"realme
","p21":"RP1A.200720.011","p25":["GB",null,"CN",null,
null,null],"pa0":"1"}}'`
```

3.4 Connections with Amap

```
POST http://apsrgeo.amap.com/rgeo/r?q=1&type=0&csid=&
language=zh&productId=2&commonparmeter=gdgmS6uc1K%2
Fjl1CFXJ%2F%2FFxGokM1c00U37FS5Y6PXLl58DbluR%2
BjM44h14eyXjtxsYU%2
FEp5dR5giBJqKv5ftVwZlIM09pNblCDilhP%2BD%2
BVAcjOQdHDluXUoDu8gWv0FbJtImVYpzj%2
Bkl6InGr7KYJzbNb35rAEJP6fUTOM%2BKXB7PwXZD47%2BKHz%2
FPviEQEOsPXB%2BYYlPMivlxQ5W8Z8fge%2
ByvaqDKRfacVWpp12lpNoJJosNWu2uNCsFcITs%...
Headers
*et: 111*
*Content-Type: application/x-www-form-urlencoded*
*Accept-Encoding: gzip*

{"data":"<?xml version=\"1.0\" encoding=\"UTF-8\"?><
ReverseGeoRQ xmlns=\"http:\/\/rgeo.amap.com\/wps
\/2014\" version=\"2.24\" street-address-lookup=\"
full\"><authentication version=\"2.2\"><key key=\"
eJwVwbkNACAMBLCaYSLlIM-1
ScFSiN0RNgb0g1PHge4yLkqUpTR9SSQg1WG16R457wMMKgrm\"
username=\"AutoNavi\" \/><\/authentication><point><
latitude>55.941098<\/latitude><longitude>-3.178640<\/
longitude><\/point><\/ReverseGeoRQ>","headers":{"
restKey":"ee282ec01d1dc9d6eb663f6b19bc5832","imei
":"","utdid":"","adiu":"
kjfsfpoqlfdd267baf1c23cd045a12","sourcePackageName":"
com.oppo.nhs","productVersion":"
oppo_nlp_42_20130418_6.0.07_a072"}}

the text following `commonparmeter=` in the url is
decoded as:
model=RMX2205&brand=realme&osinfo=android11&osVer=30&
appName=com.amap.android.location&packageName=com.
amap.android.location&diu=&imsi=&productVerion=6.0.07
_a072&colVer=v75&utdid=YtsNyTnjj8cDAMYoZwfZDB11&adiu=
kjfsfpoqlfdd267baf1c23cd045a12&sn=&oaid=&
networkOperator=&src=nlp&license=
BNPO0B7B4T8OW907232P986CEDE38QW&productId=2&mapkey=
ee282ec01d1dc9d6eb663f6b19bc5832

POST https://offline.aps.amap.com/LoadOfflineData/
repeatData?&commonparmeter=8LhgcMdKQJM%3D
Headers
*aps_c_key:
Ni4wLjA3X2EwNzIqY29tLmFtYXAuYW5kcm9pZC5sb2NhdGlvbg==*
*v: 1.5*
*aps_c_src: bGNfMg==*
*gzipped: 1*
*Accept-Encoding: gzip*
*Content-Type: application/octet-stream*
*et: 110*

partial post body:
1
1.5
2
com.amap.android.location (package name)
6.0.07_a072 (productVersion)
30 (osVer)
YtsNyTnjj8cDAMYoZwfZDB11 (utdid)
kjfsfpoqlfdd267baf1c23cd045a12 (adiu)
0
realme (brand)
RMX2205 (model)
BNPO0B7B4T8OW907232P986CEDE38QW (license)
```

```
ee282ec01d1dc9d6eb663f6b19bc5832 (mapkey)


POST http://aps.oversea.amap.com/APS/r?&q=0&ver=5.3&commonparmeter=8LhgcMdKQJM%3D&csid=d7810d9a-fc3c-4b0b-b8ff-872fb3e06c86
Headers
*aps_c_key: Ni4wLjA3X2EwNzIqY29tLmFtYXAuYW5kcm9pZC5sb2NhdGlvbg==*
*aps_c_src: bGNfMg==*
*gzipped: 1*
*Accept-Encoding: gzip*
*et: 111*
*Content-Type: application/octet-stream*

partial post body:

00:00:00:00:00:00 (empty mac address)
6gAKAKlVB4ahA2MAAA== (unknown)
AgTqAAoAqVUHhqEDtAAANQGTCwAA//// fwTqAAoAqVUHhqEDrwAANQGTCwAA////fw== (unknown)
1F1k2wQgECJhbmRyb2lkcHJpdmFjeSLelwI= (decoded as "androidprivacy" -- WiFi name)
AAA= (unknown)
AgAjMA== (unknown)
AgGpVQeGoQPbBAGpVSAaoQOaAw== (unknown)
nlp_6.0.07_a072 (productVersion)
YtsNyTnjj8cDAMYoZwfZDB11 (utdid)
kjfsfpoq1fdd267baf1c23cd045a12 (adiu)
```

3.5 Connections With China Mobile

```
POST https://a.fxltsbl.com/accept/sdkService?func=tsdk:postreglog&appkey=A100007874&timestr=1640546890684&imei=865130051443611&version=v2&token=94eb2c89e43e6f2679d06bb0ca6fa5e1
Headers
*Content-Type: application/json; charset=utf-8*
*Accept-Encoding: gzip*
**request body**
{"sdkVersion":"3.0.0","imei1":"865130051443611","imei2":"865130051443603","brand":"realme","model":"RMX2205","firmwareVer":"RMX2205_11_A.13","systemVer":"11","cpu":"MT6891Z","rom":"128G","ram":"8.00 GB","type":"1","iccid2":"","imsi1":"","imsi2":"","mac":"","cellId":"60937377","lac":"850","channel":"18","dataCard":"0","masterStatus":"0","sendTime":"1640546890605","soltQuantity":"2","dataCard2":"0","soltService1":"2","soltService2":"1","soltNetwork1":"0","soltNetwork2":"0","cellId2":"-1","lac2":"-1","inType":"RMX2205","verify":"imei_unKnown#imsi_unKnown#mac_null#brand_realme#model_RMX2205#version_11#totalRam_8GB#SDFreeSpace_102583.7890625#cpu_MT6891Z\/CZA#screen_1080*2293#SimSerialNumber__unKnown#romSpace_116 GB#battery_90#ROTATION_VECTOR:Y||GYROSCOPE_UNCALIBRATED:Y||GAME_ROTATION_VECTOR:Y||AMBIENT_TEMPERATURE:N||GYROSCOPE:Y||LIGHT:Y||STEP_COUNTER:Y||LINEAR_ACCELERATION:Y||GRAVITY:Y||RELATIVE_HUMIDITY:N||MAGNETIC_FIELD_UNCALIBRATED:Y||GEOMAGNETIC_ROTATION_VECTOR:Y||PRESSURE:N||TEMPERATURE:N||ORIENTATION:Y||ACCELEROMETER:Y||SIGNIFICANT_MOTION:Y||STEP_DETECTOR:Y||PROXIMITY:Y||#","phoneNumber1":"unknown","phoneNumber2":"unknown","status5g1":"0","status5g2":"-1","currentRam":"2.27 GB","currentRom":"7.55 GB"}

POST https://a.fxltsbl.com/accept/preInstalledApp?appkey=A100007874&timestr=1640446177925&imei=865130051443611&version=v2&token=303c70980740ab6ec657506c889ac99b
Headers
*Content-Type: application/json; charset=utf-8*
*Accept-Encoding: gzip*
**request body**
{"sdkVersion":"3.0.0","imei1":"865130051443611","imei2":"865130051443603","appArray":[{"appName":"com.coloros.foundation.BackupRestoreApplication","pkgName":"com.coloros.backuprestore","appVersion":"5.75.3","installTime":"1627110625000","signatureInfo":"D5F2D71470028A27F040234DBE7B62B0"},{"pkgName":"com.google.android.networkstack.tethering","appVersion":"11-7069081","installTime":"0","signatureInfo":"551004F246C7623F557504C86B824393"},{"appName":"com.mediatek.gba.GbaApp","pkgName":"com.mediatek.gba","appVersion":"11","installTime":"1230768000000","signatureInfo":"5763862465386D42DA5B339E7331D76B"},{"appName":"com.mediatek.ims.ImsApp","pkgName":"com.mediatek.ims","appVersion":"11","installTime":"1230768000000","signatureInfo":"5763862465386D42DA5B339E7331D76B"},{"pkgName":"com.android.cts.priv.ctsshim","appVersion":"11-6508977","installTime":"0","signatureInfo":"E89B158E4BCF988EBD09EB83F5378E87"},{"appName":"com.coloros.apprecover.AppRecoverApplication","pkgName":"com.coloros.apprecover","appVersion":"1.1.54","installTime":"1627110625000","signatureInfo":"D5F2D71470028A27F040234DBE7B62B0"},{"appName":"com.oppo.ctautoregist.RegisterApplication","pkgName":"com.oppo.ctautoregist","appVersion":"8.1.25","installTime":"1627309389000","signatureInfo":"D5F2D71470028A27F040234DBE7B62B0"},{"pkgName":"com.google.android.ext.services","appVersion":"r_aml_301500700","installTime":"0","signatureInfo":"19F24A7DF7F27B58374AD3A1D082A356"},{"appName":"com.oplus.onekeylockscreen.LockScreenApplication","pkgName":"com.coloros.onekeylockscreen","appVersion":"8.0.12","installTime":"1640290182000","signatureInfo":"D5F2D71470028A27F040234DBE7B62B0"},...
```

3.6 Connections When Starting Clock

```
POST https://u.bot.heytapmobi.com/user/ask
Headers
*Content-Type: application/json; charset=utf-8*
*Accept-Encoding: gzip*
**request body**
{"apId":"","appVersion":"1.0.0","auId":"F0F1040866EF46B78A91DC5DD274B4D...","duId":"","guId":"","imei":"","ouId":"FEBF51FCD61E4183BB9113639DDA82F882e..."}
```