跨性别安全指南

// TODO：对本文内容的简单介绍
// TODO：关于经济独立

关于你的手机

1. 大原则

首先请从抵制国产软件开始。因为家长一旦求助于公权力，可以很容易地从国内的互联网公司那里调取数据。原则上来说：国产软件能不用就不用。

聊天使用官方Telegram并且不要交换联系人。

注意密码安全。至少使用不重复且字母数字混合的密码。

2. 准备匿名手机卡

准备一张匿名手机卡（最好寻求灰色产业链购买国内已实名的手机卡，也可以用别人的淘宝购买香港卡，或者美国朋友代购Project Fi），设置8位数PIN码。在紧急情况下插入能修改IMEI的或者没有插过自己的手机卡的手机使用。

注意：Project Fi 的默认 PIN 码不是 1234，无法修改。切勿多次尝试导致锁卡。

学会修改手机的 IMEI。

> *高通方案的手机使用 QPST 修改 NV 550。操作过程很麻烦且不一定成功，以后细说。*
>
> *MTK 方案的手机在工程模式里使用 AT 指令修改。*
> *卡1：AT+EGMR=1,7,"IMEI Number"*
> *卡2：AT+EGMR=1,10,"IMEI Number"*
> *对于某些锁定不让发AT+EGMR指令的手机，例如小米的部分机型，可以试着改变大小写和添加空格。例如 at+ egmr = 1,7,"IMEI Number" 。再不行的话去 /dev 下面找基带的 tty 设备，然后 echo -e 'AT+EGMR=1,7,"IMEI Number"\r' > /dev/ttyXXX0*

3. 如果你正在使用Android系统

千万不要用国产rom。最好刷成官方LineageOS并加密。

LineageOS 可以快速禁用指纹和人脸识别。

必须要用的国产软件，请使用XPrivacyLua+Island控制权限。

Island 用于防止 app 读取手机存储里的内容。

4. 如果你正在使用iOS系统

使用非国区的 iCloud 帐号。

手机彻底关闭Siri，因为Siri 会一直听你说话，并将数据分享给国内公司。

关闭国产app的所有权限和后台应用刷新。

注意随时清空剪贴板。

及时升级到最新的iOS。旧版的iOS有很多漏洞。

在IOS11及以上版本中，按5下电源键可以禁用指纹或人脸解锁。同时也会触发紧急模式。

5. 关于你的个人电脑

电脑上使用国产软件的话都放在虚拟机里运行，视情况决定是否要使用 tor。

// 浏览器插件：uBlock Origin、WebRTC Block

使用强密码加密硬盘。（Windows：BitLocker，Linux：dm-crypt，Mac：FileVault）
如果使用 TPM 认证的话，请确保你的登录密码无懈可击。

如果之前电脑直接安装过国产软件，请重装系统。

6. 最后提醒

万万不可怕麻烦。安全和便利是鱼和熊掌不可兼得的。

当你面对家长的时候

请开始学会评估和分析家长的心理模型，注意根据他们的个人性格和态度研究他们有没有做出过激的事情的可能。

家长是否有主见也是一个很重要的因素。不然有可能被亲戚蛊惑。

学会识破家里人的亲情牌和糖衣炮弹，例如拉儿时家常，邀请回家过年，甚至谎称家里有人去世等。请仔细思考他们是不是只是借此来骗你回去。

特别提醒在海外留学的MtF们， 如果家长的态度不是一开始就接受LGBT群体，就不要轻易回国。鉴于身处海外的特殊性，家长更有可能对你使用柔情的手法来骗你回国。

对此请不要心软。不然很可能死无葬身之地。

警告：如果被过激的家长控制，你很可能会被送进某些限制人身自由的机构如戒网瘾学校，强制性精神病院等。

拘束带和镇静剂是常见的束缚手段。

寻求安全援助

1. 在相对稳定的时期也要做好防范

保管好自己的各种证件。背下来关键联系人的手机号码，自己的身份证、银行卡号码。

请使用可靠的安全途径建立与可靠的朋友的联系。

// 学会使用查找手机的功能
// 善用各运营商的小号功能，注意请不要使用阿里小号。
// 不要泄露手机号，网上有成吨的泄露的 API 接口可以直接拿到你的真实姓名。

此外，你也可以以攻为守，考虑监控家长。

针对移动用户：和平时期可以考虑使用亲情通监控家人行踪，目前已知广东，北京，河北可用，请自行联系当地运营商确认。

> *亲情通是中国移动公司推出的一项位置类自有业务，您在对方同意的情况下将其加入自己的关爱名单之后，即可通过短信、WAP或WEB方式查询到与该客户位置相关的信息。*
> *定位基于GPS和CELL-ID基站。*

如果家长使用 Android 手机，而且你又有能力的话，也可以自己写一个 native 后门。
至于为什么要 native，是因为如果家里人用的是国产手机和国产ROM的话，常驻后台的并且获取各种权限的 app 很容易被系统自带的“权限管理”揪出来。
以下是一些参考：

> *用 `inotify(7)` 监视 Telephony Provider 的数据库和 `/sdcard` 里的特定文件夹，发现更改后加密上传至自己的服务器。*
>
> *把编译器的优化开到顶（`-Ofast`，以及为手机 CPU 架构优化的选项），并且 strip 掉符号，以（略微）增加被逆向的难度。*

可以 hook 掉 `/system/bin/debuggerd` 来实现开机自启。
提前排查由 SELinux Context 导致的权限问题。

如果家长使用苹果手机，你可以考虑利用iCloud同步和查找。

如果家长有使用自有车辆的可能，你可以自行购买车用GPS监控仪实时定位车辆位置。

但也务必考虑这么做的法律风险，如果你家长具有一定法律意识且与你面对强烈对抗的话。

2. 在与家长的强烈对抗有发生预兆时请及时寻求援助

请立刻通过安全途径向靠得住的朋友扩散有效信息。

联系NGO组织，例如北京同志中心、广州跨性别中心。

3. 跑路时也请注意

尽量一次性在某地点取现并在之后主要或完全使用现金。

坐火车逃跑的话可以考虑买一张更远目的地的票，然后提前下车。为了进一步增大搜索难度，建议在小站下车，小站往往缺少出站自动化验票设备。

不要住宾馆。警察可以很轻易地查到开房记录。

MTF 考虑女装化妆出门，FTM 考虑男装短发，避免被路上的天网系统人脸识别。

使用电信2/3G和移动联通的2G网络可以降低被网络定位的精确度。因为是低频，覆盖广。这只是一种在没有匿名手机卡的情况下可以使用的辅助手段。

关于移动网络的一些技术细节：
GSM 网络有被窃听和中间人攻击的风险。
移动和电信的 4G 网络都是不加密的。
联通的 3G 使用的是 GEA1 弱加密。也有时不加密。
电信的 2G 没有启用 CAVE 加密，但是由于扩频通讯的特点，较难被攻击。

4. 在基本确定住所，准备长期生存的时候

请把自己租的房子变成一座堡垒。

在选择住宿地点时你应该优先考虑的事

如果要租房并且经济条件允许的话，优先考虑万科的房子，安保相当严格。

> *具体来说，每个出入口都有闸机和保安把守；送外卖的没有业主确认都进不来；家中每个房间都有呼叫保安的按钮。*

就算在经济条件不允许的情况下也一定要优先考虑小区安保条件。优秀的安保环境是你的第一道防线，至少能使你及时知晓不速之客的到来，为你拖延时间。

在选好小区之后

更换成难以被撬开的门锁。

给关键网络设施加装后备电源和备用的移动网络接入。

// 电源板、锂电池的购买链接
// UPS选购指南
// OpenWrt mwan3 howto

在门上安装震动报警传感器。

丢弃快递包装前，销毁上面的所有个人信息。

备好防狼喷雾、榔头、扳手之类的武器。

安装监控。

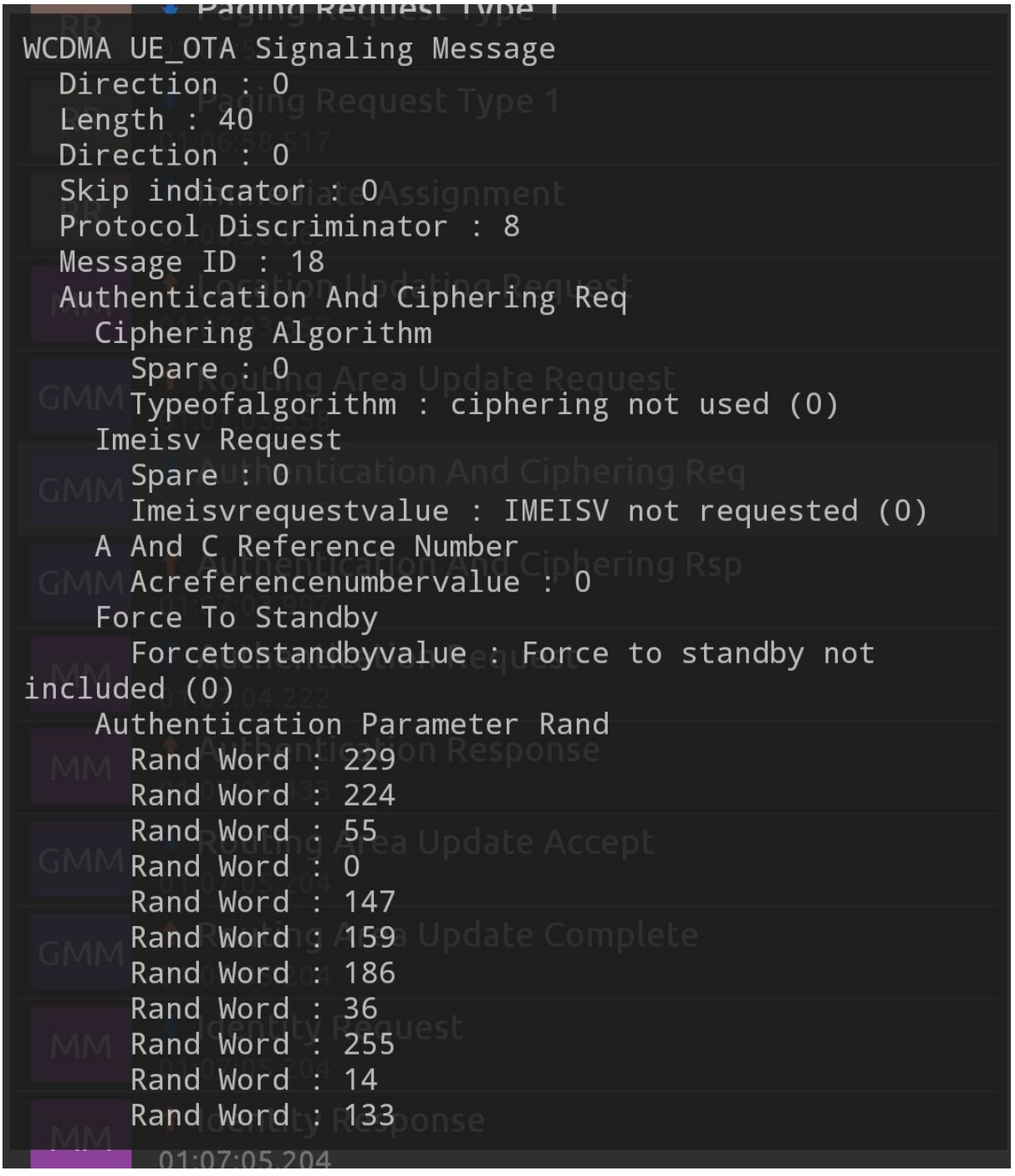
海康的摄像头值得优先考虑，使用的是标准的 RTSP 协议。注意单独隔离摄像头内网。监控录像实时上传到境外VPS，同时将移动物体画面使用Telegram Bot推送到手机上。

你可以使用 ffmpeg 把视频流使用 MKV 格式保存到本地，再持续 rsync 到国外 VPS。

> *关于移动物体画面推送：*
> *1、本地搭一个 FTP 服务器，记得 chroot*
> *2、让海康的摄像头在检测到移动物体后，拍照，并且上传到 FTP*
> *3、使用 `inotifywait(1)` 和 `curl(1)` 自动把新上传的照片发到 Telegram Bot 上*

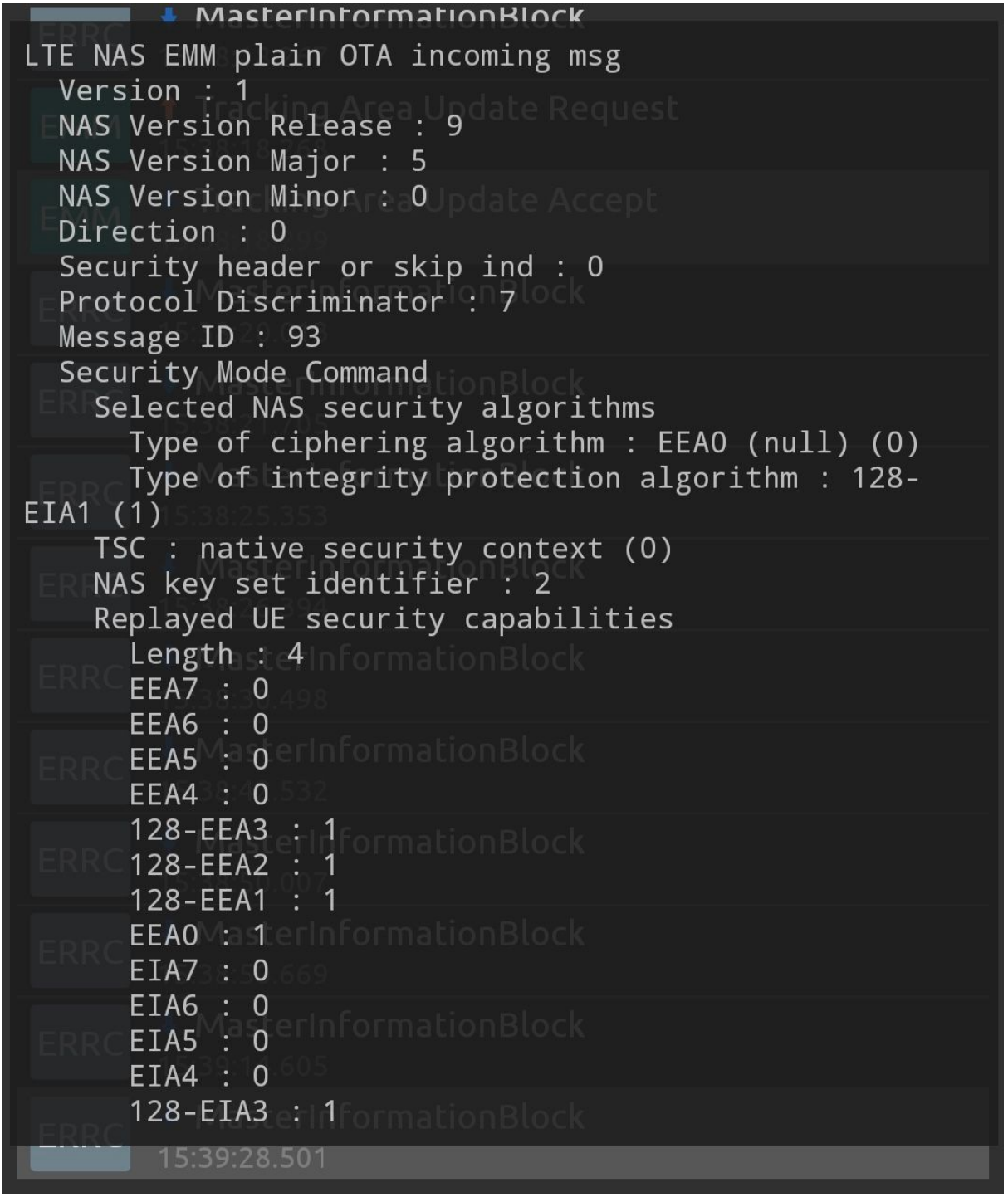
附录和参考

未加密的联通3G。

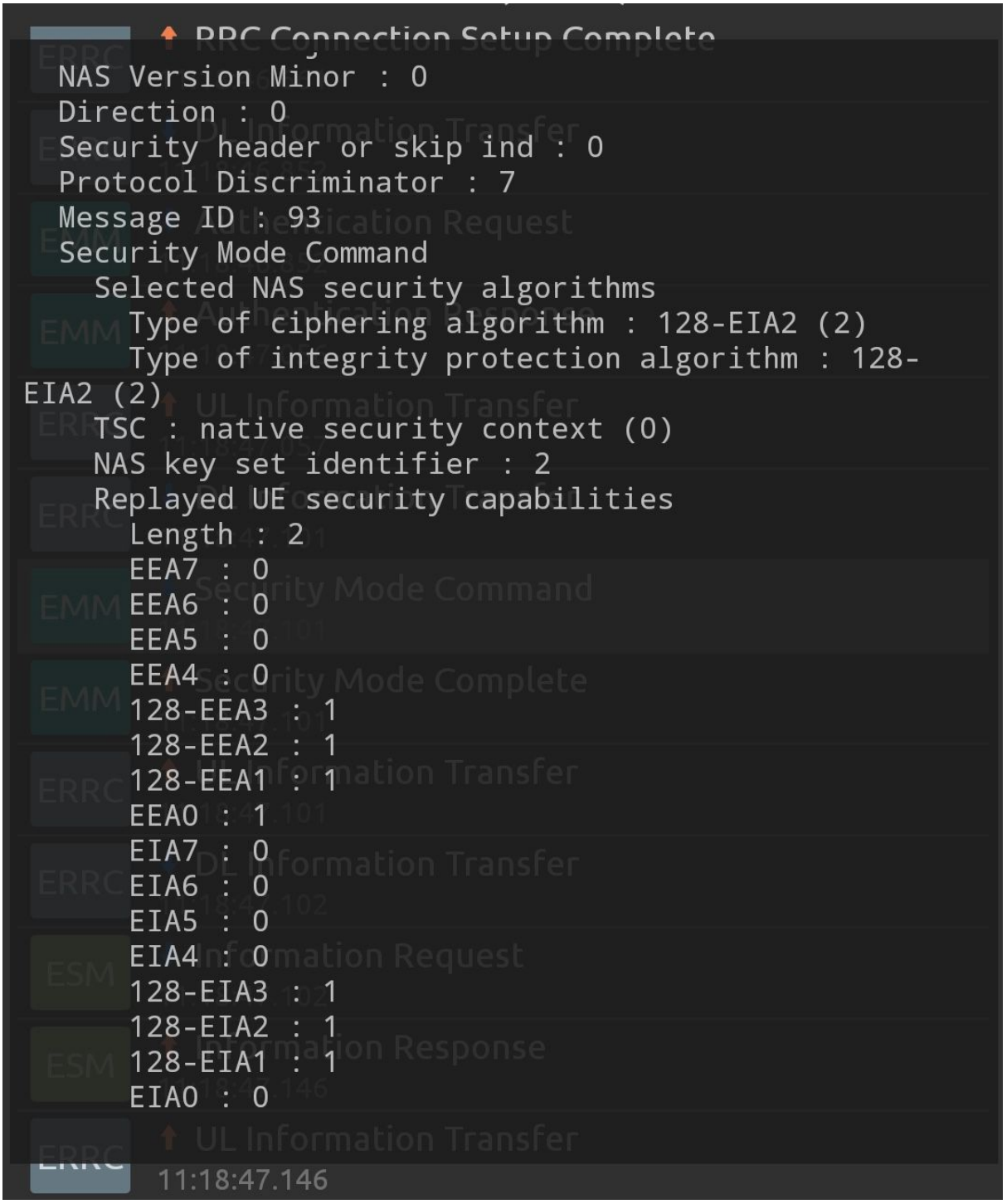


```
WCDMA UE_OTA Signaling Message
  Direction : 0
  Length : 40
  Direction : 0
  Skip indicator : 0
  Protocol Discriminator : 8
  Message ID : 18
  Authentication And Ciphering Req
    Ciphering Algorithm
      Spare : 0
      Typeofalgorithm : ciphering not used (0)
    Imeisv Request
      Spare : 0
      Imeisvrequestvalue : IMEISV not requested (0)
    A And C Reference Number
      Acreferencenumbervalue : 0
    Force To Standby
      Forcetostandbyvalue : Force to standby not
included (0)
    Authentication Parameter Rand
      Rand Word : 229
      Rand Word : 224
      Rand Word : 55
      Rand Word : 0
      Rand Word : 147
      Rand Word : 159
      Rand Word : 186
      Rand Word : 36
      Rand Word : 255
      Rand Word : 14
      Rand Word : 133
```

未加密的电信4G


LTE NAS EMM plain OTA incoming msg
Version : 1
NAS Version Release : 9
NAS Version Major : 5
NAS Version Minor : 0
Direction : 0
Security header or skip ind : 0
Protocol Discriminator : 7
Message ID : 93
Security Mode Command
Selected NAS security algorithms
Type of ciphering algorithm : EEA0 (null) (0)
Type of integrity protection algorithm : 128-EIA1 (1)
TSC : native security context (0)
NAS key set identifier : 2
Replayed UE security capabilities
Length : 4
EEA7 : 0
EEA6 : 0
EEA5 : 0
EEA4 : 0
128-EEA3 : 1
128-EEA2 : 1
128-EEA1 : 1
EEA0 : 1
EIA7 : 0
EIA6 : 0
EIA5 : 0
EIA4 : 0
128-EIA3 : 1

联通4G是加密的


RRC Connection Setup Complete
NAS Version Minor : 0
Direction : 0
Security header or skip ind : 0
Protocol Discriminator : 7
Message ID : 93
Security Mode Command
Selected NAS security algorithms
Type of ciphering algorithm : 128-EIA2 (2)
Type of integrity protection algorithm : 128-
EIA2 (2)
TSC : native security context (0)
NAS key set identifier : 2
Replayed UE security capabilities
Length : 2
EEA7 : 0
EEA6 : 0
EEA5 : 0
EEA4 : 0
128-EEA3 : 1
128-EEA2 : 1
128-EEA1 : 1
EEA0 : 1
EIA7 : 0
EIA6 : 0
EIA5 : 0
EIA4 : 0
128-EIA3 : 1
128-EIA2 : 1
128-EIA1 : 1
EIA0 : 0
UL Information Transfer
11:18:47.146

电信2G不加密


Channel
PN
RSSI
Ec/Io
283
-52.6 dBm
-4.7 dB
PLMN
Band
BID
SID/NID
460 / 03
800M
信令 (筛选)
Channel : 8
MSG_LENGTH : 19
MSG_TYPE : 7
In-Traffic System Parameters
FDSCH_LAYER2_BEG_FIELDS
ACK_SEQ : 0
MSG_SEQ : 0
ACK_REQ : 0
ENCRYPTION : 0
SID :
NID : 1
SRCH_WIN_A : 28 (6)
SRCH_WIN_N : 60 (8)
SRCH_WIN_R : 80 (9)
T_ADD : -14
T_DROP : -16
T_COMP : 2.5
T_TDROP : 4 (3)
NGHBR_MAX_AGE : 0
P_REV : IS-2000 Release 0 (6)
SOFT_SLOPE : 0
ADD_INTERCEPT : 4
DROP_INTERCEPT : 0
PACKET_ZONE_ID :
EXTENSION : 0
T_SLOTTED_INCL : 0
IS2000_L2_PDU_PADDING
CRC : 1829