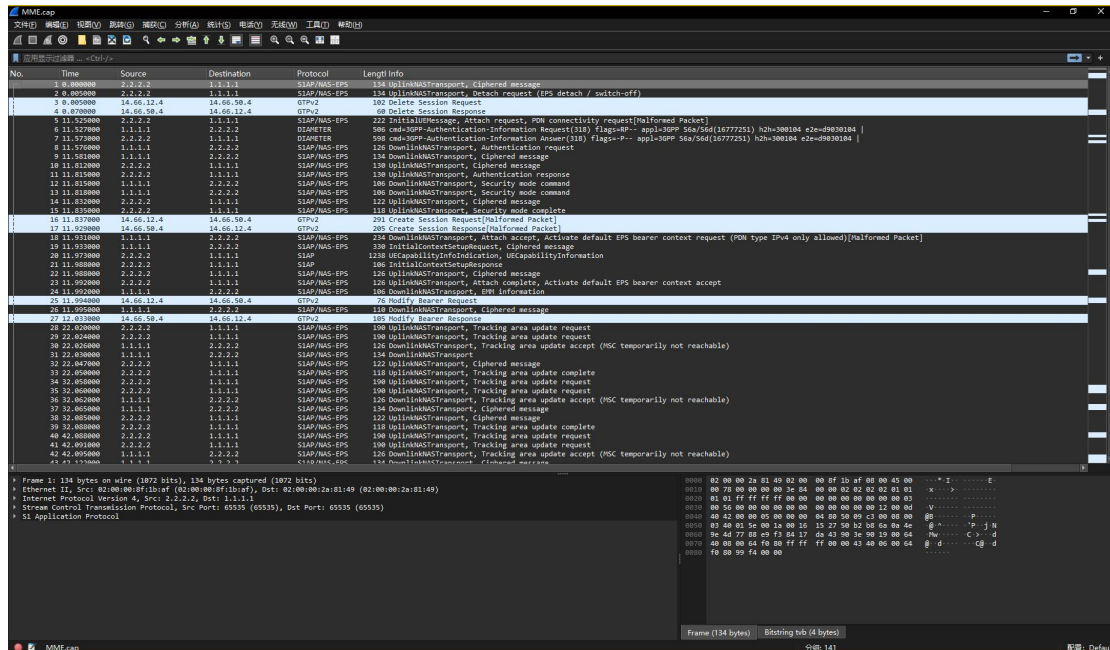


赛题名称: Misc1

解题步骤 (WriteUp)

第一步：要求寻找定位信息，查看流量包，基本都是和基站通信的数据包



第二步： LTE 通信流量包中有一个被称作 ECGI 的值，可以包含一定的位置信息

在基站通信中，ECGI (E-UTRAN Cell Global Identifier) 是一个用于唯一标识 LTE (长期演进) 网络中每个小区的标识符。ECGI 由两个主要部分组成：

1. ****PLMN ID (Public Land Mobile Network Identifier)****: 这是一个标识公共陆地移动网络的代码，通常由一个移动国家码（MCC）和一个移动网络码（MNC）组成。
2. ****Cell ID****: 这是一个在特定 PLMN 下唯一标识小区的编号。

ECGI 的格式通常是: ` $\langle \text{PLMN ID} \rangle + \langle \text{Cell ID} \rangle`。通过 ECGI, 网络能够识别和区分不同的基站小区, 这对于移动设备在网络中的定位、切换和资源管理等功
能至关重要。$

在实际应用中，ECGI 被用于各种网络操作，例如小区选择、切换、以及在网络管理和优化中进行小区的监控和分析。

可以认为就是 ECGI 值泄露了用户的位置信息

第三步：查询流量包，大部分包都是加密后的包，无法解密，考虑其中的
cmd=3GPP-Insert-Subscriber-Data Answer(319) flags=-P-- appl=3GPP
S6a/S6d(16777251) h2h=9bc110f8 e2e=9bc110f8 | 包，这种包属于基站给用
户的回答包，其中会包含基站信息

```
122 UplinkNASTransport, Ciphred message
382 cmd=3GPP-Insert-Subscriber-Data Request(319) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h=9bc110f8 e2e=9bc110f8 |
410 cmd=3GPP-Insert-Subscriber-Data Answer(319) flags=-P-- appl=3GPP S6a/S6d(16777251) h2h=9bc110f8 e2e=9bc110f8 |
650 cmd=3GPP-Insert-Subscriber-Data Request(319) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h=7f889a2 e2e=7f889a2 |
830 cmd=3GPP-Insert-Subscriber-Data Answer(319) flags=-P-- appl=3GPP S6a/S6d(16777251) h2h=7f889a2 e2e=7f889a2 |
90 UEContextReleaseRequest [RadioNetwork-cause=user-inactivity]
60 Release Access Bearers Request
```

.....

第四步：在第 110 包查看到 location 关键字，定位到 ECGI 值

```
AVP: RAT-Type(1052) l=16 f=V-- vnd=3GPP val=EUTRAN (1004)
AVP: EPS-Location-Information(1496) l=80 f=V-- vnd=3GPP
  AVP Code: 1496 EPS-Location-Information
  AVP Flags: 0x80, Vendor-Specific: Set
  AVP Length: 80
  AVP Vendor Id: 3GPP (10415)
  EPS-Location-Information: 0000064080000044000028af0000064280000013000028af4e378a561e44ce00000006438000001100
    AVP: MME-Location-Information(1600) l=68 f=V-- vnd=3GPP
      AVP Code: 1600 MME-Location-Information
      AVP Flags: 0x80, Vendor-Specific: Set
      AVP Length: 68
      AVP Vendor Id: 3GPP (10415)
      MME-Location-Information: 0000064280000013000028af4e378a561e44ce000000064380000011000028af64f08099f400
        AVP: E-UTRAN-Cell-Global-Identity(1602) l=19 f=V-- vnd=3GPP val=4e378a561e44ce
          AVP Code: 1602 E-UTRAN-Cell-Global-Identity
          AVP Flags: 0x80, Vendor-Specific: Set
          AVP Length: 19
          AVP Vendor Id: 3GPP (10415)
          E-UTRAN-Cell-Global-Identity: 4e378a561e44ce
          Padding: 00
        AVP: Tracking-Area-Identity(1603) l=17 f=V-- vnd=3GPP val=64f08099f4
```

4e378a561e44ce

Md5 后得到 192d9cbb319a53d18059a30f50db7e7b，即为 flag