赛题名称：MISE01

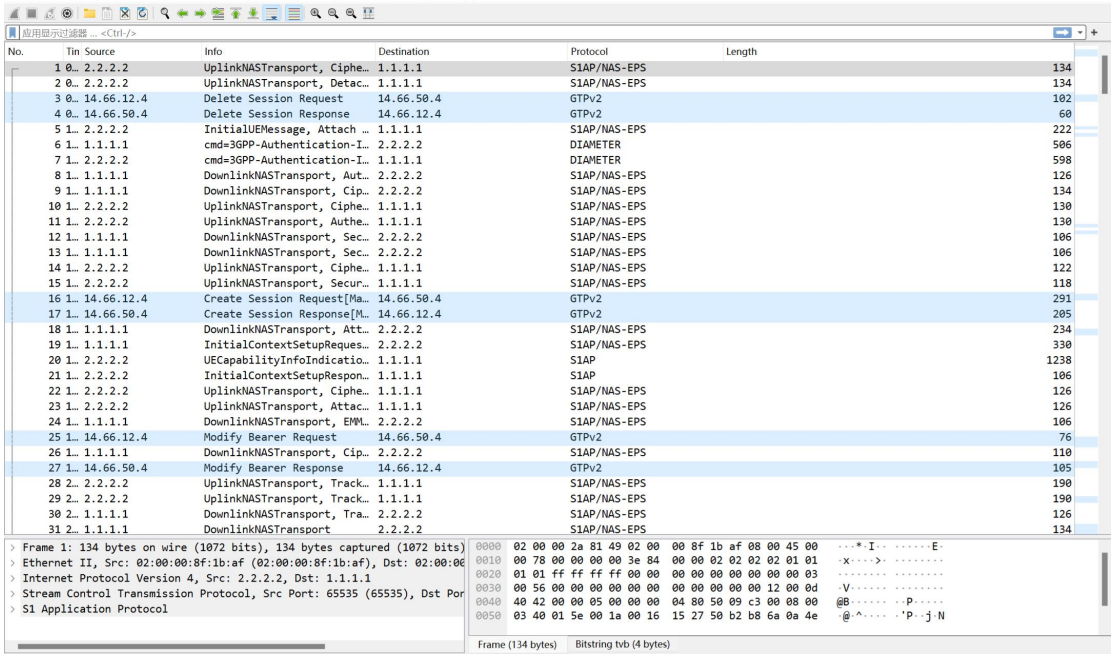
解题步骤（WriteUp）

第一步：打开附件发现是一个流量包，同时查看题目描述。

某单位网络遭到非法的攻击，安全人员对流量调查取证之后保存了关键证据，发现人员的定位信息存在泄露
请对其进行分析。flag 为用户位置信息进行 32 位 md5 哈希值

发现其实就是个常规的流量分析，同时找到对应的攻击行为同时根据题目描述，我们是要找到对应的用户位置。

第二步：wirshark 打开数据包



对于这个流量 gpt 查询一下协议

一、S1AP（S1 Application Protocol，S1 应用协议）

S1AP 是 LTE（Long Term Evolution，长期演进）网络中 eNodeB（Evolved Node B，演进型基站）和核心网（MME，Mobility Management Entity，移动性管理实体）之间的接口协议。

主要功能包括：

1. 建立、修改和释放 S1 接口承载。
2. 为 UE（User Equipment，用户设备）在 LTE 网络中的移动性管理提供支持，例如切换过程中的信令交互。
3. 传递 UE 的上下文信息和 NAS（Non-Access Stratum，非接入层）信令消息。

二、NAS-EPS（Non-Access Stratum for Evolved Packet System，演进分组系统非接入层）

NAS 是 UE 和核心网之间的控制面协议，在 EPS（Evolved Packet System，演进分组系统）中，NAS 协议主要用于处理与移动性管理、会话管理和用户数据传输相关的信令。

主要功能包括：

1. 移动性管理，如附着、分离、跟踪区更新等。
2. 会话管理，如建立、修改和释放 EPS 承载。
3. 传递用户数据和控制信息。

三、DIAMETER

DIAMETER 是一种用于认证、授权和计费（AAA，Authentication、Authorization and Accounting）的通信协议。

主要应用场景包括：

1. 在移动通信网络中，用于移动数据业务的认证和授权，确保用户能够合法地访问网络资源。
2. 实现网络中的计费功能，记录用户的使用情况并生成计费信息。
3. 支持不同网络实体之间的通信，如 AAA 服务器、策略服务器等。

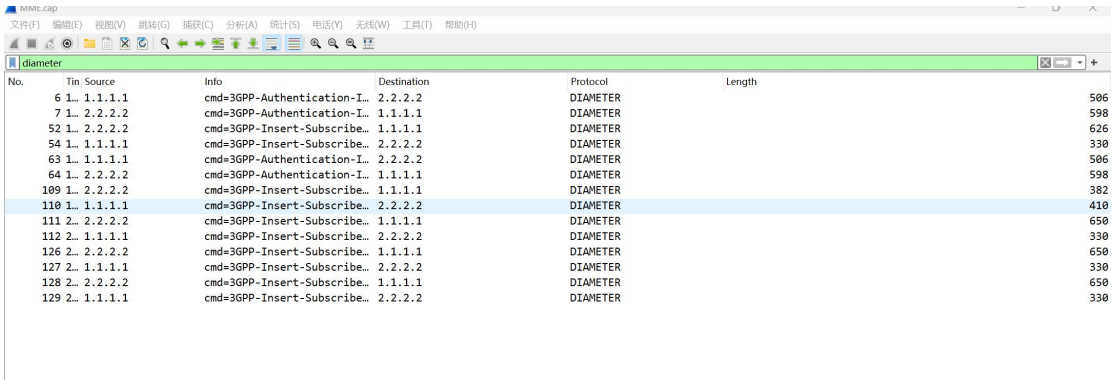
四、GTPv2（GPRS Tunneling Protocol version 2，GPRS 隧道协议版本 2）

GTPv2 主要用于在 LTE 网络中传输用户数据和信令消息。

主要功能包括：

1. 在核心网中建立和管理用户平面隧道，实现用户数据的传输。
2. 支持移动性管理，如切换过程中的数据转发。
3. 传递控制面信令，如创建、修改和删除承载的请求和响应。

其实这个时候的思路其实是很好想的，首先我们要找 用户泄露的位置信息。这又是一个移动通信的一些协议。同时我翻看了很多数据包只有 DIAMETER 是最长的感觉最能出货，其他的看了十六进制都很短。同时可以看到 DIAMETER 这个协议跟用户有关，他是作为一个用户认证授权计费的协议。所以过滤 DIAMETER



No.	Tin	Source	Info	Destination	Protocol	Length
6	1…	1.1.1.1	cmd=3GPP-Authentication-I…	2.2.2.2	DIAMETER	506
7	1…	2.2.2.2	cmd=3GPP-Authentication-I…	1.1.1.1	DIAMETER	598
52	1…	2.2.2.2	cmd=3GPP-Insert-Subscribe…	1.1.1.1	DIAMETER	626
54	1…	1.1.1.1	cmd=3GPP-Insert-Subscribe…	2.2.2.2	DIAMETER	330
63	1…	1.1.1.1	cmd=3GPP-Authentication-I…	2.2.2.2	DIAMETER	506
64	1…	2.2.2.2	cmd=3GPP-Authentication-I…	1.1.1.1	DIAMETER	598
109	1…	2.2.2.2	cmd=3GPP-Insert-Subscribe…	1.1.1.1	DIAMETER	382
110	1…	1.1.1.1	cmd=3GPP-Insert-Subscribe…	2.2.2.2	DIAMETER	410
111	2…	2.2.2.2	cmd=3GPP-Insert-Subscribe…	1.1.1.1	DIAMETER	650
112	2…	1.1.1.1	cmd=3GPP-Insert-Subscribe…	2.2.2.2	DIAMETER	330
126	2…	2.2.2.2	cmd=3GPP-Insert-Subscribe…	1.1.1.1	DIAMETER	650
127	2…	1.1.1.1	cmd=3GPP-Insert-Subscribe…	2.2.2.2	DIAMETER	330
128	2…	2.2.2.2	cmd=3GPP-Insert-Subscribe…	1.1.1.1	DIAMETER	650
129	2…	1.1.1.1	cmd=3GPP-Insert-Subscribe…	2.2.2.2	DIAMETER	330

一个一个翻找想找到一些位置信息但是一直找不到。继续问 gpt

3. 传递控制面信令，如创建、修改和删除承载的请求和响应。

DIAMETER 跟用户有关，那么她有没有可能泄露用户的一些信息比如位置

DIAMETER 协议本身一般不会直接泄露用户的位置信息等敏感内容。

DIAMETER 主要用于认证、授权和计费等功能，在通信过程中会对信息进行一定程度的加密和保护。然而，如果网络存在安全漏洞或者遭受恶意攻击，那么理论上可能会导致包括与用户相关的信息被泄露，但这并不是 DIAMETER 协议正常运行情况下会发生的情况。

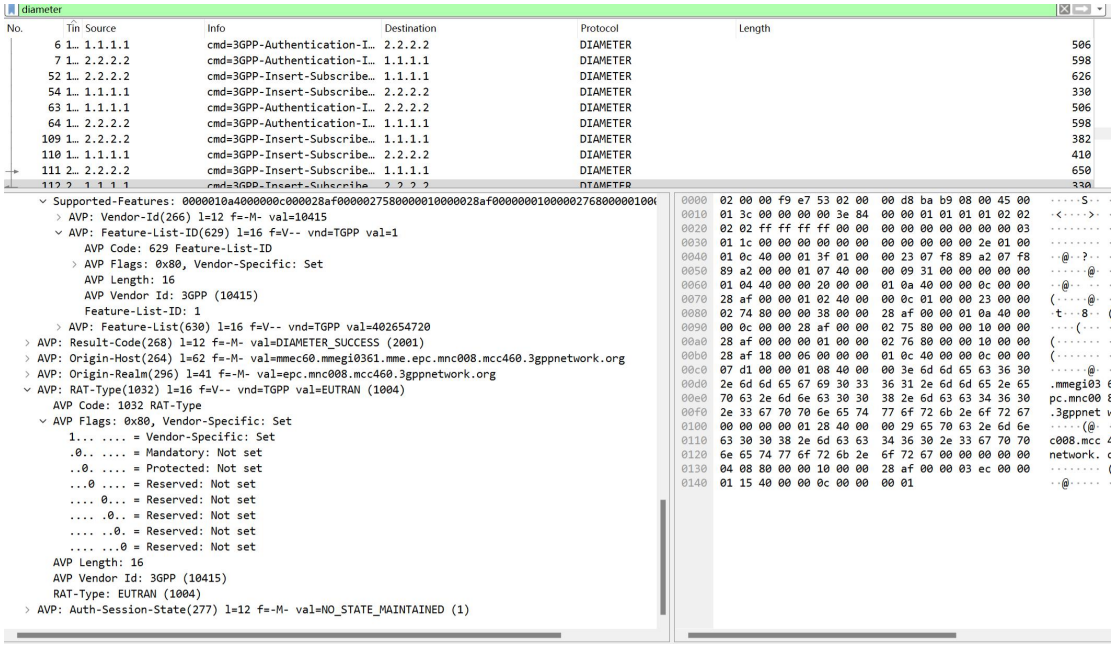
此外，现代通信网络通常会采取多重安全措施来保护用户信息的安全，包括加密、访问控制、安全审计等，以降低信息泄露的风险。

难道网络通信的时候用户个人位置网络信息无法找到吗

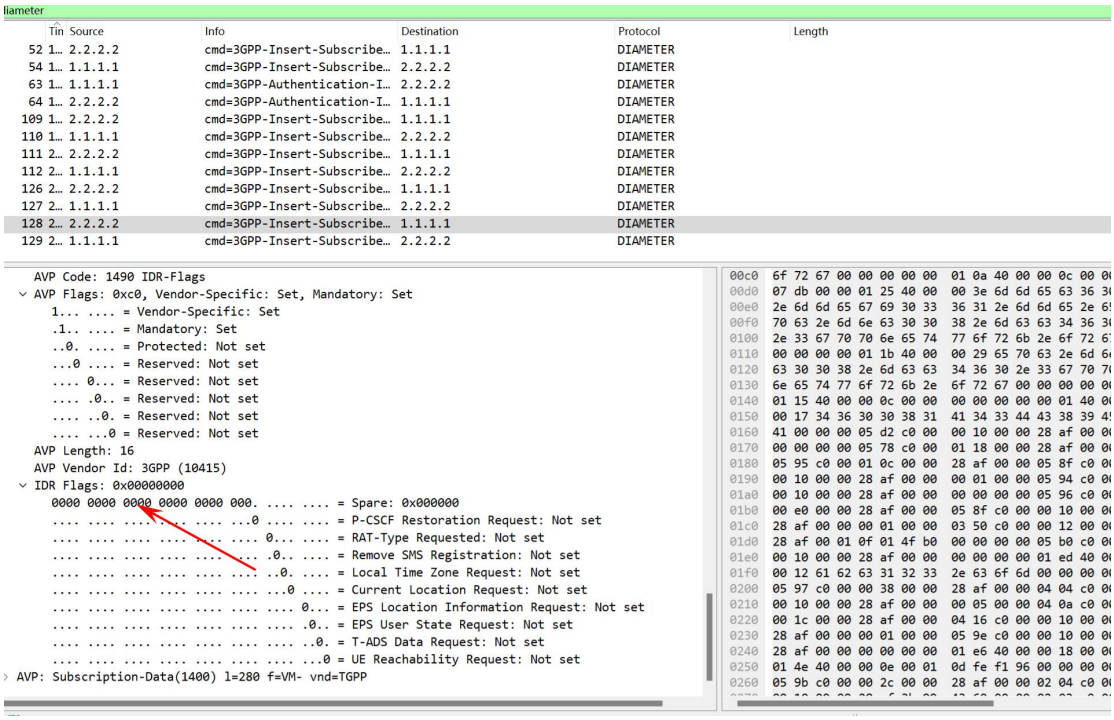
在网络通信中，要确切找到用户个人位置信息并不是一件容易的事，且通常不能随意获取。

一方面，从技术 ●

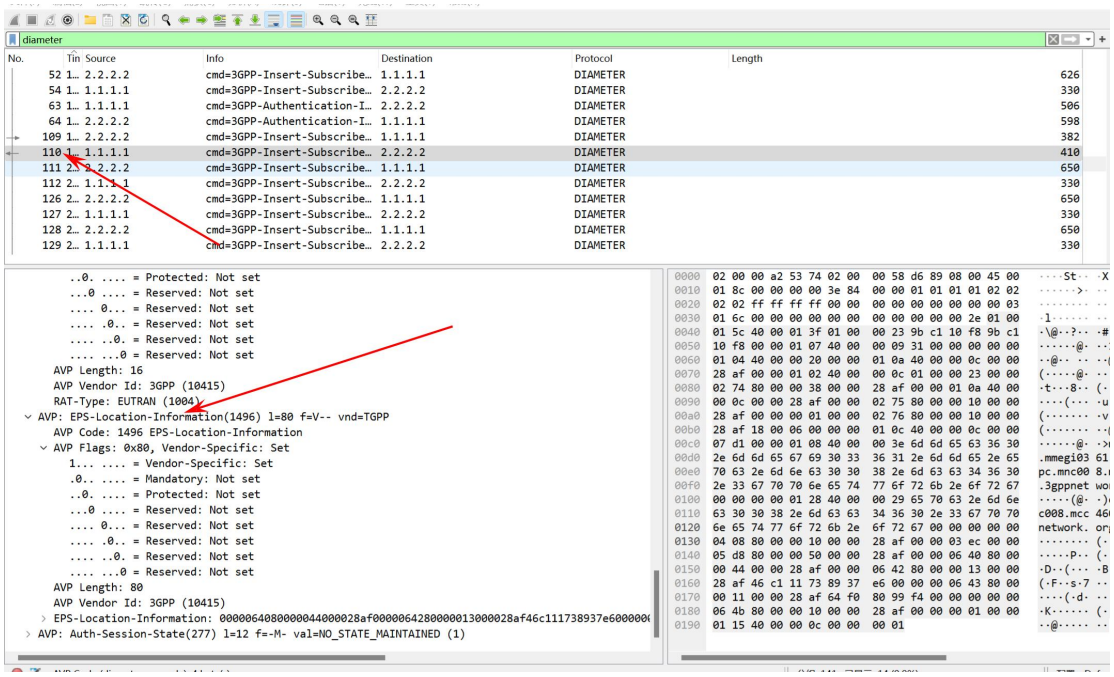
第三步：



数据不多，我一个一个翻的数据包，大多数都没有什么位置的数据头

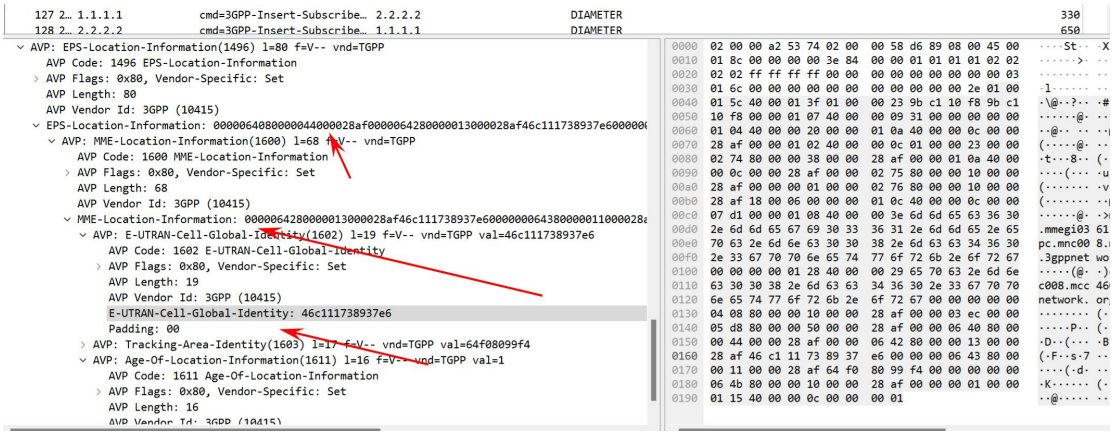


要么就是 idrflags 要么就是
没有别的。



终于翻到一些不一样的地方，location
……

第 4 步：



把所有的可能位置信息都 md5 加密，试出来是第三个。

这个 E-UTRAN-Cell-Global-Identity（E-UTRAN 小区全局标识）是一个由特定编码组成的字符串，用于唯一标识 LTE（Long Term Evolution，长期演进）网络中的一个小区。

它通常由移动国家码（MCC）、移动网络码（MNC）和小区标识（Cell ID）组成。不过仅从这个具体的字符串很难直接解读出对应的国家、网络运营商以及小区的具体位置等详细信息。