

赛题名称：MISE01

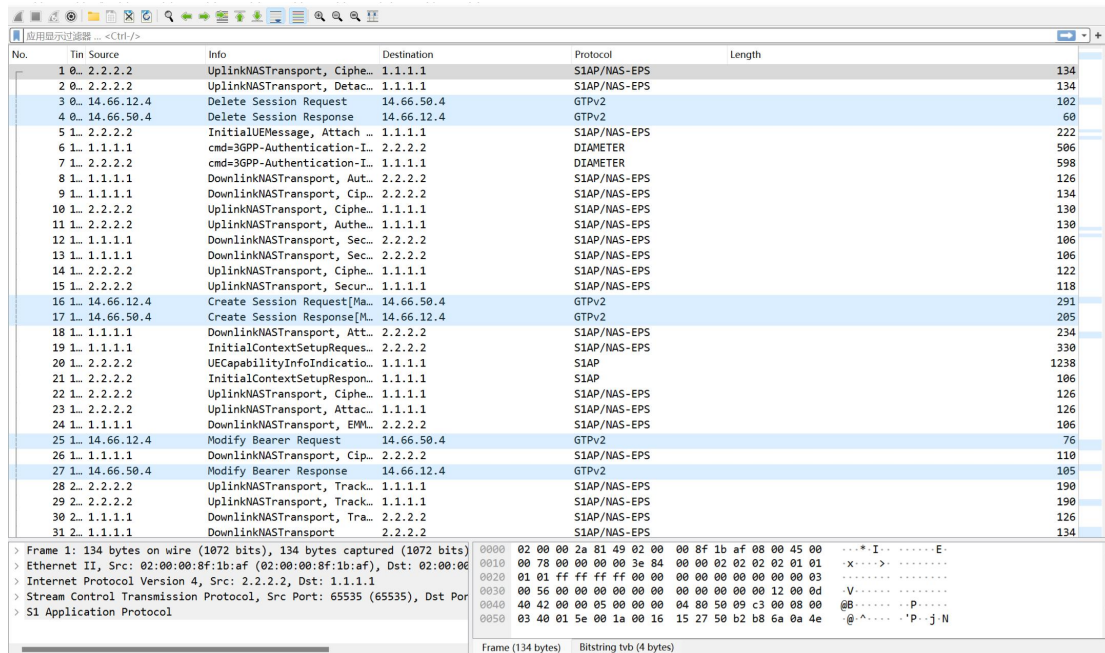
解题步骤（WriteUp）

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：wireshark 打开数据包



No.	Time	Source	Info	Destination	Protocol	Length
1	0.000000	2.2.2.2	UplinkNASTransport, Ciph...	1.1.1.1	SIAP/NAS-EPS	134
2	0.000000	2.2.2.2	UplinkNASTransport, Detac...	1.1.1.1	SIAP/NAS-EPS	134
3	0.000000	14.66.12.4	Delete Session Request	14.66.50.4	GTPV2	102
4	0.000000	14.66.50.4	Delete Session Response	14.66.12.4	GTPV2	60
5	1.000000	2.2.2.2	InitialUEMessage, Attach ...	1.1.1.1	SIAP/NAS-EPS	222
6	1.000000	1.1.1.1	cmd=3GPP-Authentication-I...	2.2.2.2	DIAMETER	506
7	1.000000	2.2.2.2	cmd=3GPP-Authentication-I...	1.1.1.1	DIAMETER	598
8	1.000000	1.1.1.1	DownlinkNASTransport, Aut...	2.2.2.2	SIAP/NAS-EPS	126
9	1.000000	1.1.1.1	DownlinkNASTransport, Cip...	2.2.2.2	SIAP/NAS-EPS	134
10	1.000000	2.2.2.2	UplinkNASTransport, Ciph...	1.1.1.1	SIAP/NAS-EPS	130
11	1.000000	2.2.2.2	UplinkNASTransport, Authe...	1.1.1.1	SIAP/NAS-EPS	130
12	1.000000	1.1.1.1	DownlinkNASTransport, Sec...	2.2.2.2	SIAP/NAS-EPS	106
13	1.000000	1.1.1.1	DownlinkNASTransport, Sec...	2.2.2.2	SIAP/NAS-EPS	106
14	1.000000	2.2.2.2	UplinkNASTransport, Ciph...	1.1.1.1	SIAP/NAS-EPS	122
15	1.000000	2.2.2.2	UplinkNASTransport, Secur...	1.1.1.1	SIAP/NAS-EPS	118
16	1.000000	14.66.12.4	Create Session Request[Ma...	14.66.50.4	GTPV2	291
17	1.000000	14.66.50.4	Create Session Response[M...	14.66.12.4	GTPV2	205
18	1.000000	1.1.1.1	DownlinkNASTransport, Att...	2.2.2.2	SIAP/NAS-EPS	234
19	1.000000	1.1.1.1	InitialContextSetupReques...	2.2.2.2	SIAP/NAS-EPS	330
20	1.000000	2.2.2.2	UECapabilityInfoIndicatio...	1.1.1.1	SIAP	1238
21	1.000000	2.2.2.2	InitialContextSetupRespon...	1.1.1.1	SIAP	106
22	1.000000	2.2.2.2	UplinkNASTransport, Ciph...	1.1.1.1	SIAP/NAS-EPS	126
23	1.000000	2.2.2.2	UplinkNASTransport, Attac...	1.1.1.1	SIAP/NAS-EPS	126
24	1.000000	1.1.1.1	DownlinkNASTransport, EMM...	2.2.2.2	SIAP/NAS-EPS	106
25	1.000000	14.66.12.4	Modify Bearer Request	14.66.50.4	GTPV2	76
26	1.000000	1.1.1.1	DownlinkNASTransport, Cip...	2.2.2.2	SIAP/NAS-EPS	110
27	1.000000	14.66.50.4	Modify Bearer Response	14.66.12.4	GTPV2	105
28	2.000000	2.2.2.2	UplinkNASTransport, Track...	1.1.1.1	SIAP/NAS-EPS	190
29	2.000000	2.2.2.2	UplinkNASTransport, Track...	1.1.1.1	SIAP/NAS-EPS	190
30	2.000000	1.1.1.1	DownlinkNASTransport, Tra...	2.2.2.2	SIAP/NAS-EPS	126
31	2.000000	1.1.1.1	DownlinkNASTransport	2.2.2.2	SIAP/NAS-EPS	134

> Frame 1: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
> Ethernet II, Src: 02:00:00:8f:1b:af (02:00:00:8f:1b:af), Dst: 02:00:00:00:00:00
> Internet Protocol Version 4, Src: 2.2.2.2, Dst: 1.1.1.1
> Stream Control Transmission Protocol, Src Port: 65535 (65535), Dst Port: 65535
> SI Application Protocol

0000 02 00 00 2a 81 49 02 00 00 8f 1b af 08 00 45 00 ...* I- - - - - E-
0010 00 78 00 00 00 00 3e 84 00 00 02 02 02 01 01 -X- - - - -
0020 01 01 ff ff ff ff 00 00 00 00 00 00 00 00 03 -V- - - - -
0030 00 56 00 00 00 00 00 00 00 00 00 00 12 00 0d -V- - - - -
0040 40 42 00 00 05 00 00 00 04 80 50 09 c3 00 08 00 @B- - - - -
0050 03 40 01 5e 00 1a 00 16 15 27 50 b2 b8 6a 0a 4e @-^ - - - - 'P- - - - j- N

Frame (134 bytes) Bitstring tvb (4 bytes)

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。

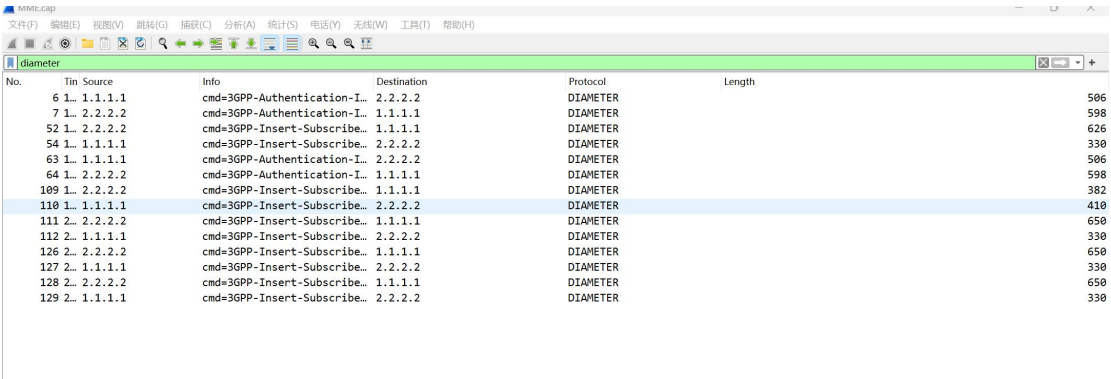
四、GTPv2 (GPRS Tunneling Protocol version 2, GPRS 隧道协议版本 2)

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



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：

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
Supported-Features: 0000010a4000000c000028af0000027580000018000028af000000010000027680000100c						
AVP: Vendor-ID(266) l=12 fa=M- val=10415						
AVP: Feature-List-ID(629) l=16 fv=- vnd=TGPP val=1						
AVP Code: 629 Feature-List-ID						
> AVP Flags: 0x80, Vendor-Specific: Set						
AVP Length: 16						
AVP Vendor Id: 3GPP (10415)						
Feature-List-ID: 1						
> AVP: Feature-List(630) l=16 fv=- vnd=TGPP val=402654720						
AVP: Result-Code(268) l=12 fa=M- val=DIAMETER_SUCCESS (2001)						
AVP: Origin-Host(264) l=62 fa=M- val=mmeC60.mmegi0361.mme.epc.mnc008.mcc460.3gppnetwork.org						
AVP: Origin-REALM(296) l=41 fa=M- val=epc.mnc008.mcc460.3gppnetwork.org						
AVP: RAT-Type(1032) l=16 fv=- vnd=TGPP val=EUTRAN (1004)						
AVP Code: 1032 RAT-Type						
> AVP Flags: 0x80, Vendor-Specific: Set						
1... .. = Vendor-Specific: Set						
.0... .. = Mandatory: Not set						
.0... .. = Protected: Not set						
.0... .. = Reserved: Not set						
....0... = Reserved: Not set						
....0... = Reserved: Not set						
....0... = Reserved: Not set						
AVP Length: 16						
AVP Vendor Id: 3GPP (10415)						
RAT-Type: EUTRAN (1004)						
> AVP: Auth-Session-State(277) l=12 fa=M- val=NO_STATE_MAINTAINED (1)						

```

0000 02 00 00 f9 e7 53 02 00 00 d8 ba b9 08 00 45 00 .....S...
0010 01 3c 00 00 00 3e 84 00 00 01 01 01 01 02 02 ...<-.-.-.-
0020 02 02 ff ff ff ff 00 00 00 00 00 00 00 00 03 .....
0030 01 1c 00 00 00 00 00 00 00 00 00 00 2e 01 ....@.....
0040 01 ac 40 00 01 3f 01 00 00 23 07 f8 89 a2 07 f8 @.....?
0050 89 c2 00 00 01 87 00 00 00 09 31 00 00 00 00 .....@...
0060 01 04 00 00 00 20 00 00 01 0a 40 00 00 0c 00 .....@...
0070 28 af 00 00 01 02 40 00 00 0c 01 00 00 23 00 .....@...
0080 02 74 80 00 00 00 00 28 af 00 00 01 0a 40 00 t.....8...
0090 00 0c 00 00 28 af 00 02 75 80 00 00 10 00 00 .....(-....
00a0 28 af 00 00 00 01 00 00 02 76 80 00 00 10 00 .....(-....
00b0 28 af 18 00 06 00 00 00 01 0c 40 00 00 0c 00 .....(-....
00c0 07 d1 00 00 01 08 40 00 00 3e 6d 6d 65 63 30 .....@.....
00d0 2e 6d 6d 65 67 69 30 33 3e 31 2e 6d 6d 65 2e 65 .mmeigi03
00e0 70 63 2e 6d 6e 63 30 38 36 6d 63 63 34 36 30 pc.mnc00
00f0 2e 33 67 70 70 6e 65 74 77 6f 72 6b 2e 6f 72 67 .3gppnetw
0100 00 00 00 00 01 28 40 00 00 29 65 70 63 2e 6d 6e .....
0110 63 30 38 2e 6d 63 63 34 36 30 2e 33
```

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

diameter					
No.	Tin Source	Info	Destination	Protocol	Length
52	1. 2.2.2.2	cmd=3GPP-Insert-Subscribe...	1.1.1.1	DIAMETER	
54	1. 1.1.1.1	cmd=3GPP-Insert-Subscribe...	2.2.2.2	DIAMETER	
63	1. 1.1.1.1	cmd=3GPP-Authentication-I...	2.2.2.2	DIAMETER	
64	1. 2.2.2.2	cmd=3GPP-Authentication-I...	1.1.1.1	DIAMETER	
109	1. 2.2.2.2	cmd=3GPP-Insert-Subscribe...	1.1.1.1	DIAMETER	
110	1. 1.1.1.1	cmd=3GPP-Insert-Subscribe...	2.2.2.2	DIAMETER	
111	2. 2.2.2.2	cmd=3GPP-Insert-Subscribe...	1.1.1.1	DIAMETER	
112	2. 1.1.1.1	cmd=3GPP-Insert-Subscribe...	2.2.2.2	DIAMETER	
126	2. 2.2.2.2	cmd=3GPP-Insert-Subscribe...	1.1.1.1	DIAMETER	
127	2. 1.1.1.1	cmd=3GPP-Insert-Subscribe...	2.2.2.2	DIAMETER	
128	2. 2.2.2.2	cmd=3GPP-Insert-Subscribe...	1.1.1.1	DIAMETER	
129	2. 1.1.1.1	cmd=3GPP-Insert-Subscribe...	2.2.2.2	DIAMETER	

AVP Code: 1490 IDR-Flags	00c0 6f 72 67 00 00 00 00 01 0a 40 00 00 0c 00 01
AVP Flags: 0xc0, Vendor-Specific: Set, Mandatory: Set	00d0 07 db 00 00 01 25 40 00 00 3e 6d 65 63 36 30
1... = Vendor-Specific: Set	00e0 2e 6d 6d 65 67 69 30 33 36 31 2e 6d 65 2e 6f
..1... = Mandatory: Set	00f0 70 63 2e 6d 6e 63 30 38 2e 6d 63 63 34 36 31
...0... = Protected: Not set	0100 2e 33 67 70 70 6e 65 74 77 6f 72 6b 2e 6f 72 6f
...0... = Reserved: Not set	0110 00 00 00 00 01 1b 40 00 00 29 65 70 63 2e 6d 6f
...0... = Reserved: Not set	0120 63 30 38 2e 6d 63 63 34 36 30 2e 33 67 70 71
...0... = Reserved: Not set	0130 6e 65 74 77 6f 72 6b 2e 6f 72 67 00 00 00 00
...0... = Reserved: Not set	0140 01 15 40 00 00 0c 00 00 00 00 00 00 01 40 01
...0... = Reserved: Not set	0150 00 17 34 36 30 38 31 41 34 33 44 43 38 39 41
...0... = Reserved: Not set	0160 41 00 00 00 05 d2 c0 00 00 10 00 00 28 af 00 01
AVP Length: 16	0170 00 00 00 00 05 78 c0 00 01 18 00 00 28 af 00 01
AVP Vendor Id: 3GPP (10415)	0180 05 95 c0 00 01 0c 00 00 28 af 00 00 05 8f c0 01
IDR Flags: 0x00000000	0190 00 10 00 00 28 af 00 00 01 00 00 05 94 c0 01
0000 0000 0000 0000 0000 0000 = Spare: 0x00000000	01a0 00 10 00 00 28 af 00 00 00 00 00 05 96 c0 01
...0... = P-CSCF Restoration Request: Not set	01b0 00 e0 00 00 28 af 00 00 05 8f c0 00 10 00 01
...0... = RAT-Type Requested: Not set	01c0 28 af 00 00 00 01 00 00 03 50 c0 00 05 8f c0 01
...0... = Remove SMS Registration: Not set	01d0 28 af 00 01 0f 01 4f b0 00 00 00 00 05 b0 c0 01
...0... = Local Time Zone Request: Not set	01e0 00 10 00 00 28 af 00 00 00 00 00 01 ed 40 01
...0... = Current Location Request: Not set	01f0 00 12 61 62 63 31 32 33 2e 63 6f 6d 00 00 00
...0... = EPS Location Information Request: Not set	0200 05 97 c0 00 00 38 00 00 28 af 00 00 04 04 c0 01
...0... = EPS User State Request: Not set	0210 00 10 00 00 28 af 00 00 00 05 00 00 04 04 c0 01
...0... = T-ADS Data Request: Not set	0220 00 1c 00 00 28 af 00 00 04 16 c0 00 10 00 01
...0... = UE Reachability Request: Not set	0230 28 af 00 00 00 01 00 00 05 9e c0 00 10 00 01
AVP: Subscription-Data(1400) l=280 f=VM- vnd=TGPP	0240 28 af 00 00 00 00 00 01 e6 40 00 00 18 00 01
	0250 01 4e 40 00 00 0e 00 01 0d fe f1 96 00 00 00
	0260 05 9b c0 00 00 2c 00 00 28 af 00 00 02 04 c0 01

要么就是 idrflags 要么就是
没有别的。

diameter					
No.	Tin Source	Info	Destination	Protocol	Length
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

AVP Length: 16	0000 02 00 00 a2 53 74 02 00 00 58 d6 89 08 00 45 00
AVP Vendor Id: 3GPP (10415)	0010 01 8c 00 00 00 00 3e 84 00 00 01 01 01 02 02
RAT-Type: EUTRAN (1004)	0020 02 02 ff ff ff ff 00 00 00 00 00 00 00 03
AVP: EPS-Location-Information(1496) l=80 f=V- vnd=TGPP	0030 01 6c 00 00 00 00 00 00 00 00 00 02 e1 00 00
AVP Code: 1496 EPS-Location-Information	0040 01 5c 40 00 01 3f 01 00 00 23 9b c1 10 f8 9b c1
AVP Flags: 0x80, Vendor-Specific: Set	0050 10 f8 00 00 01 07 40 00 00 09 31 00 00 00 00
1... = Vendor-Specific: Set	0060 01 04 40 00 00 20 00 00 01 0a 40 00 0c 00 00
..1... = Mandatory: Not set	0070 28 af 00 00 01 02 40 00 00 0c 01 00 00 23 00 00
...0... = Protected: Not set	0080 02 74 80 00 00 38 00 00 28 af 00 00 01 0a 40 00
...0... = Reserved: Not set	0090 00 0c 00 00 28 af 00 00 02 75 80 00 00 10 00 00
...0... = Reserved: Not set	00a0 28 af 00 00 00 01 00 00 02 76 80 00 00 10 00 00
...0... = Reserved: Not set	00b0 28 af 18 00 06 00 00 00 01 0c 40 00 00 0c 00 00
...0... = Reserved: Not set	00c0 07 d1 00 00 01 08 40 00 00 3e 6d 6d 65 63 36 30
...0... = Reserved: Not set	00d0 2e 6d 6d 65 67 69 30 33 36 31 2e 6d 6d 65 2e 65
AVP Length: 80	00e0 70 63 2e 6d 6e 63 30 38 2e 6d 63 63 34 36 30
AVP Vendor Id: 3GPP (10415)	00f0 2e 33 67 70 70 6e 65 74 77 6f 72 6b 2e 6f 72 6f
EPS-Location-Information: 00000640000044000028af0000064280000013000028af46c111738937e60000	0100 00 00 00 00 01 28 40 00 00 29 65 70 63 2e 6d 6e
AVP: Auth-Session-State(277) l=12 f=M- val=NO_STATE_MAINTAINED (1)	0110 63 30 38 2e 6d 63 63 34 36 30 2e 33 67 70 70
	0120 6e 65 74 77 6f 72 6b 2e 6f 72 67 00 00 00 00
	0130 04 08 80 00 00 10 00 00 28 af 00 00 03 ec 00 00
	0140 05 d8 80 00 00 50 00 00 28 af 00 00 06 40 80 00
	0150 00 44 00 00 28 af 00 00 06 42 80 00 00 13 00 00
	0160 28 af 46 c1 11 73 89 37 e6 00 00 00 06 43 80 00
	0170 00 11 00 00 28 af 64 f0 80 99 f4 00 00 00 00
	0180 06 4b 80 00 00 10 00 00 28 af 00 00 00 01 00 00
	0190 01 15 40 00 00 0c 00 00 01

终于翻到一些不一样的地方，location

.....

