HGAME 2021 Week 2 Writeup

MISC

A R K

首先打开流量包分析，主要内容是 TLS 协议文件和 FTP 文件。FTP-Data 文件名为 ssl.log 因此猜测使用 log 文件来解码 TLS 文件。

21	1.072739357	192.168.2.128	172.67.148.67	HTTP	340	POST /account/login HTTP/1.1 (application/json)
54	5.998957709	172.67.148.67	192.168.2.128	HTTP	1143	HTTP/1.1 200 OK (application/json)
85	6.702476657	192.168.2.128	172.67.148.67	HTTP	263	GET /announce/Bilibili/announcement.meta.json HTTP/1.1
91	7.396729074	172.67.148.67	192.168.2.128	TLSv1.3	700	[TLS segment of a reassembled PDU]HTTP/1.1 200 OK (application/json)
118	8.047077299	192.168.2.128	172.67.148.67	HTTP	78	POST /user/checkIn HTTP/1.1 (application/json)
122	8.766021083	172.67.148.67	192.168.2.128	TLSv1.3	121	[TLS segment of a reassembled PDU]HTTP/1.1 200 OK (application/json)
144	9.349342062	192.168.2.128	172.67.148.67	HTTP	88	POST /activity/getChainLogInReward HTTP/1.1 (application/json)
150	10.024685671	172.67.148.67	192.168.2.128	TLSv1.3	144	[TLS segment of a reassembled PDU]HTTP/1.1 200 OK (application/json)
173	10.700652358	192.168.2.128	172.67.148.67	HTTP	103	POST /activity/loginOnly/getReward HTTP/1.1 (application/json)
177	11.571132572	172.67.148.67	192.168.2.128	TLSv1.3	148	[TLS segment of a reassembled PDU]HTTP/1.1 200 OK (application/json)
200	12.171487416	192.168.2.128	172.67.148.67	HTTP	156	POST /gacha/tenAdvancedGacha HTTP/1.1 (application/json)
204	13.208272983	172.67.148.67	192.168.2.128	TLSv1.3	881	[TLS segment of a reassembled PDU]HTTP/1.1 200 OK (application/json)
227	13.919163412	192.168.2.128	172.67.148.67	HTTP	101	POST /quest/getBattleReplay HTTP/1.1 (application/json)
239	14.969659128	172.67.148.67	192.168.2.128	TLSv1.3	1328	HTTP/1.1 200 OK (application/json)
262	15.395275881	192.168.2.128	172.67.148.67	HTTP	273	POST /quest/battleStart HTTP/1.1 (application/json)
266	16.123297908	172.67.148.67	192.168.2.128	TLSv1.3	245	[TLS segment of a reassembled PDU]HTTP/1.1 200 OK (application/json)
288	16.798988072	192.168.2.128	172.67.148.67	HTTP	4040	POST /quest/battleFinish HTTP/1.1 (application/json)
294	17.775456864	172.67.148.67	192.168.2.128	TLSv1.3	139	HTTP/1.1 200 OK (application/json)

根据文件名和题目可以推测这是明日方舟游戏中产生的数据包。数据类型全是 json 类型，加上题目提示说用可部署单位画了个东西，推测可能在 json 数据包中有和坐标相关的信息。

根据 hint 自律猜测数据在 getBattleReplay 请求的返回数据中。

{"battleReplay":"UEsFBhQAAAAIALdiS1Ki22GCdCgAABi+BQANAAAAZGVmYXVsdF9lbnRyecSdTavTQBRA/0vcRp25dzIf7lRciIIi4klRCTZqNE21SZ+K+N+d5tYvdH/ARV+/zmttpjfnMLxvzet+/7Ef3
U9QwORT2DQ1HP4FDUMzgU9QwORT2DQ1HP4FDUMzgU9QwORT1twainZNRTMuopGfWUjHpKRj0lo56SUU/JqKdk1FMy6ikZ9ZSMekpGPSWjnpJRT8mop2TUUzLqKRn1llx6SkY9JaOekIFPyain
UYYVUYYVUYYVUYYVUYYVUYYVUYYVUYYVUYYVUYYVQVUYeIMjqiwn3BEhf2ElyrsJxxRYRc4o8lucEaFXeCMCrvAGRVW4ZwKEweqMHGgChMHqjBxoAoTB6owcaAKEweqMHGgChMHqjBxoAoTB6owcaAKEweqMH
M5IMbA1lwZCALjgxk/EADGdJAhjSQIQ1kSAMZ0kCGNJAhDWRIAxnSQIY0kCENZEgDGdJAhjSQIQ1kSAMZ0kCGNJAhDWRIAxnSQIY0kCENZEgDGdJAhjSQIQ1kSAMZ0kCGNJD5gSMDWXBkIAuC
UKzgq9QqOSr2Co1Kv/8BSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSr8tSb3zgqNQrOCr1Co5KvYKjUq/gqNQrOCr
jCH47juD3jRv4feMGft+4gd83buD3jRv4feMGft+4gd+Ol/jtOILfjiP47TiC3/pA+C0JvyXhtyT8loTfkvBbEn5Lwm9J+C0JvyXhtyT8loTfkvBbEn5Lwm9J+C0JvyXhtyT8loTfkvBbEn5Lwm9J+C0JvyXhtyT8
+O47g940b+O04gt+Ol/jtOILfjiP4jQ+E35DwGxJ+Q8JvSPgNCb8h4Tck/IaE35DwGxJ+Q8JvSPgNCb8h4Tck/IaE35DwGxJ+Q8JvSPgNCb8h4Tck/IaE35DwGxJ+Q8JvSPgNCb8h4fd541P8WH5x8WP
0kFcayCsN5JUG8koDeaWBvNJAXmggu37DjYH8wo2B/MKNgfzCjYH8wo2B/MKNgfzCjYH8wo2B/MKNgfzCjYH8wo2B/AV3BrILGsguaCC7oIHsggayCxrILmggu6CB7IIGsgsayC5oILuggeyCBrILGs
qUuCoLgWO6tIjM8cjM8cjM8cjM8cjM8cjM8cjM8cjM8cjM8cjffsjffsjffsjffsjffsjffsjffsjffsjfftfuPxW+8hPuI/8hCO+/ZG+/ZG+vX/DkfgNHInfwJH4DRyJ38CR+A0cid/AkfgNHInfwJH4DRyJ38CR+A0cid/
hQlzYmIIXNqbghY0peGFjCl7YmIIXNn4Sd0e3dQMxFEQb8seSkpar/htL4PvyUsKpYGAYlskZiNoLXtjYC17Y2Ate2NgLRr29YNTbC0a9veCFjb3ghY294IWNvWBL3Qu21L1kS61fOGqpgaOWGjhqqYGj
g6MJG4OjCRuDowkbg6MJG4OjCRuDowkbg6MJG4OjCxpbid0vxu6X4DRzdHAgc3RwIHN0c2FL8bil+txS/W94c2PLmwJY3B7b07Vv69i19+5ZvYW/5FvaWb2FvmTm2zBxbZo4tX5Dc8gXJLV+QnF
ayJYGsqWBbGkgv3D5eN3yCbfIE068/D4NX36fhi+//4fLJ9zlJ9zlJxzJHC0zR8vM0TJztMwcLTNHy8zRMnO0zBwtfXtL397St1+/cOTbA0e+PXDk2wNHvj1w5NsDR749cOTbA0e+PXDk2wNHvj1w5Nv
L73BfXL7ViMmUNJmSJvM//sj/80d+5o/8zAmFlaSwkhRWksJKUlhJCitpMiVNpqTJILxPpuR9MiXvk7lvHJlMx5HJdByZTMeRyXQcmcz9QZO50mSuNJkrTeZKk7nSZK40mStN5kqTudJkrjSZK03mSpC
pR72Uo17KUS/lqJdy1Eu5LqVcl1KuSynXpZTrUsp16X/80Lh8pZZ8pZKZI+XMkXLmeN44mjk6jmaOjqOZo+No5uq4mjk6jmaOjqOZo+No5uq4mjk6jmaOjqOZo+No5uq

得到一串以==结尾的字符，推测是 Base64，使用文本解密失败，想起上周没做出来的那道 msic 题，猜测是二进制文件，使用上周官方 Writeup 中的脚本。

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
	50	4B	05	06	14	00	00	00	08	00	B7	62	4B	52	A2	DB	PK ·bKR¢Û
	61	82	74	28	00	00	18	BE	05	00	0D	00	00	00	64	65	a,t(¾ de
	66	61	75	6C	74	5F	65	6E	74	72	79	C4	9D	4D	AB	D3	fault_entryÄ M«Ó
	40	14	40	FF	4B	DC	46	9D	B9	77	32	1F	EE	54	5C	88	@ @ÿKÜF ¹w2 îT\ˆ
	82	22	E2	42	11	09	36	6A	34	4D	B5	49	9F	8A	F8	DF	,"âB 6j4MµIŸŠøß
	9D	E6	D6	2F	74	7F	C0	45	5F	BF	CE	6B	6D	A6	37	E7	æÖ/t ÀE_¿Îkm¦7ç
	30	BC	6F	CD	EB	7E	FF	B1	1F	DF	CE	8F	E6	E9	EB	B3	0¼oÍë~ÿ± ßÎ æéë³
	E1	B8	8C	87	B9	B9	E5	DB	66	1D	F7	C3	B2	D6	1B	9B	á¸Œ‡¹¹åÛf ÷Ã²Ö ›

发现文件头是 50 4B 05 06，修改为 50 4B 03 04，后解压得到 json 文件。

{"campaignOnlyVersion":1,"timestamp":"1612849000","journal":{"metadata":
{"standardPlayTime":272.999725,"gameResult":1,"saveTime":"2021-02-09T13:36:36.552186Z","remainingCost":99,"remainingLifePoint":3,"killedEnemiesCnt":57,"missedEnemiesCnt":0,"levelId":"Ac
vities/act16d5/level_act16d5_10","stageId":"act16d5_10","validKilledEnemiesCnt":57},"squad":
[{"charInstId":8,"skinId":"char_2015_dusk#1","tmplId":null,"skillId":"skchr_dusk_1","skillIndex":0,"skillLvl":1,"level":1,"phase":0,"potentialRank":0,"favorBattlePhase":38,"isAssistChar
true}],"logs":[{"timestamp":0,"signiture":{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":12}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":13}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":14}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":15}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":16}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":17}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":18}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":19}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":20}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":21}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":22}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":23}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":24}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":25}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":26}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":27}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":28}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":29}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":30}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":31}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":32}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":36}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":37}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":38}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":39}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":40}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":41}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":42}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":43}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":44}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":54}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":55}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":56}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":60}},{"timestamp":0,"signiture":

发现 pos 。使用正则表达式过滤后得到坐标，使用 EasyX 画图绘制图形。

```c
#include <stdio.h>
#include <graphics.h>
#include <time.h>

int main()
{
    int x, y,i;
    int a[10000] = {12,12,12,13,12,14,12,15,12,16,12,17,1
    initgraph(256, 256);
    setbkcolor(WHITE);
    cleardevice();
    for(int i=0;i<=10000;i+=2)
    {
        x = a[i];
        y = a[i + 1];
        putpixel(x,y,RED);
    }
    while (1);
    return 0;
}
```

由于直接使用 scanf 会卡死，故而直接写死，运行得到二维码。

扫描二维码，得到最终 flag。