# EFT Internals: response processing

## Table Of Contents



Originally written for the development of Haru.

Step-by-step overview of the client processing the response body.

Example path used: **/client/game/start**.

Useful for both Aki devs as reference point for implementing it into the server and modders who want to implement custom payload protection.

## 1 Notes

As of now, the client only supports **aes** as payload encryption type.

Since it's passed as a string, you can override the appropriate method in the client to support additional (custom) encryption types.
To find the method to target, simply look scan for the string **"aes"** inside **Assembly-CSharp.dll**.

## 2 1. Response payload

HTTP header **X-Encryption: aes** is present.

Code

```
0x6B, 0x58, 0xFC, 0x28, 0x6B, 0xFA, 0x1D, 0x74, 0x65, 0xA3, 0xD4, 0x93, 0x1A
0xEF, 0xFF, 0x3D, 0x6E, 0x60, 0x5,  0xA6, 0x1F, 0x99, 0x63, 0x8F, 0xEA, 0xC4,
0x35, 0xF0, 0x10, 0x1A, 0xD5, 0x3C, 0x8B, 0x6B, 0x21, 0x10, 0x29, 0x38, 0xF1,
0xE8, 0x9F, 0x2D, 0x2D, 0x74, 0x34, 0xB,  0x34, 0x8C, 0x97, 0x9E, 0xF3, 0xA9,
0x44, 0x86, 0x7D, 0xA5, 0x58, 0xB2, 0x35, 0x27, 0x91, 0x43, 0x19, 0xD,  0xEA,
0x24, 0xB8, 0x3E, 0xF3, 0x92, 0xF5, 0xA0, 0x7B, 0xD2, 0xE6, 0xFC, 0xB,  0x97,
0x8B, 0x3A, 0x12, 0x7C, 0xE1, 0xA3, 0x75, 0x58, 0xDF, 0x53, 0x9F, 0xB6, 0xAE,
0x24, 0x5E, 0x13, 0xD3, 0xC2
```

# 3 Payload layout

Encryption is **AES**, block cipher mode is **CBC**, with zero-padding.

### 3.1 Key

Format is **AES-192**, data is **UTF-8 bytes**, extracted from the client (0.13.5).

Code

```
0x51, 0x6F, 0x2A, 0x6E, 0x70, 0x37, 0x2A, 0x79, 0x50, 0x48, 0x71, 0x57, 0x58,
0x38, 0x5A, 0x42, 0x33, 0x5A, 0x4F, 0x40, 0x6D, 0x31, 0x6B, 0x34
```

### 3.2 Initialization vector (IV)

First block (16 bytes) of the payload.

Code

```
0x6B, 0x58, 0xFC, 0x28, 0x6B, 0xFA, 0x1D, 0x74, 0x65, 0xA3, 0xD4, 0x93, 0x1A,
0xEF, 0xFF, 0x3D
```

### 3.3 Encrypted data

Remaining bytes after IV block, remaining unused blocks zero-padded by AES.

Code

```
0x6E, 0x60, 0x5,  0xA6, 0x1F, 0x99, 0x63, 0x8F, 0xEA, 0xC4, 0x35, 0xF0, 0x10,
0x1A, 0xD5, 0x3C, 0x8B, 0x6B, 0x21, 0x10, 0x29, 0x38, 0xF1, 0xE8, 0x9F, 0x2D,
0x2D, 0x74, 0x34, 0xB,  0x34, 0x8C, 0x97, 0x9E, 0xF3, 0xA9, 0x44, 0x86, 0x7D,
0xA5, 0x58, 0xB2, 0x35, 0x27, 0x91, 0x43, 0x19, 0xD,  0xEA, 0x24, 0xB8, 0x3E,
0xF3, 0x92, 0xF5, 0xA0, 0x7B, 0xD2, 0xE6, 0xFC, 0xB,  0x97, 0x8B, 0x3A, 0x12,
0x7C, 0xE1, 0xA3, 0x75, 0x58, 0xDF, 0x53, 0x9F, 0xB6, 0xAE, 0x24, 0x5E, 0x13,
0xD3, 0xC2, 0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,
0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,
0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,
0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0
```

## 3.4 2. Decrypted

Result is data compressed with **zlib** (**RFC1950**), level 6 (normal).

Code

```
0x78, 0x9C, 0xAB, 0x56, 0x4A, 0x2D, 0x2A, 0x52, 0xB2, 0x32, 0xD0, 0x1,  0xD1,
0xB9, 0xC5, 0xE9, 0x4A, 0x56, 0x79, 0xA5, 0x39, 0x39, 0x3A, 0x4A, 0x29, 0x89,
0x25, 0x89, 0x4A, 0x56, 0xD5, 0x4A, 0xA5, 0x25, 0xC9, 0xF1, 0x25, 0x99, 0xB9,
0xA9, 0x4A, 0x56, 0x86, 0x66, 0x96, 0x46, 0x46, 0x16, 0xE6, 0x16, 0x46, 0x16,
0x7A, 0x66, 0xC6, 0xA6, 0xE6, 0xB5, 0xB5, 0x0,  0x36, 0xB3, 0x12, 0x11, 0x10,
0x10, 0x10, 0x10, 0x10, 0x10, 0x10, 0x10, 0x10, 0x10, 0x10, 0x10, 0x10, 0x10,
0x10, 0x10, 0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,
0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,
0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,
0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0,  0x0
```

## 3.5 3. Decompressed

Result is UTF-8 bytes.

Code

```
0x7B, 0x22, 0x65, 0x72, 0x72, 0x22, 0x3A, 0x30, 0x2C, 0x22, 0x65, 0x72, 0x72,
0x6D, 0x73, 0x67, 0x22, 0x3A, 0x6E, 0x75, 0x6C, 0x6C, 0x2C, 0x22, 0x64, 0x61,
0x74, 0x61, 0x22, 0x3A, 0x7B, 0x22, 0x75, 0x74, 0x63, 0x5F, 0x74, 0x69, 0x6D,
0x65, 0x22, 0x3A, 0x31, 0x36, 0x39, 0x32, 0x32, 0x38, 0x37, 0x38, 0x32, 0x38,
0x2E, 0x36, 0x33, 0x35, 0x37, 0x7D, 0x7D
```

## 3.6 4. UTF8 text

Code

{"err":0,"errmsg":null,"data":{"utc_time":1692287828.6357}}

Additional information

| | |
|---|---|
| Programming skills required | 1 |
| Technical knowledge requirement | High |