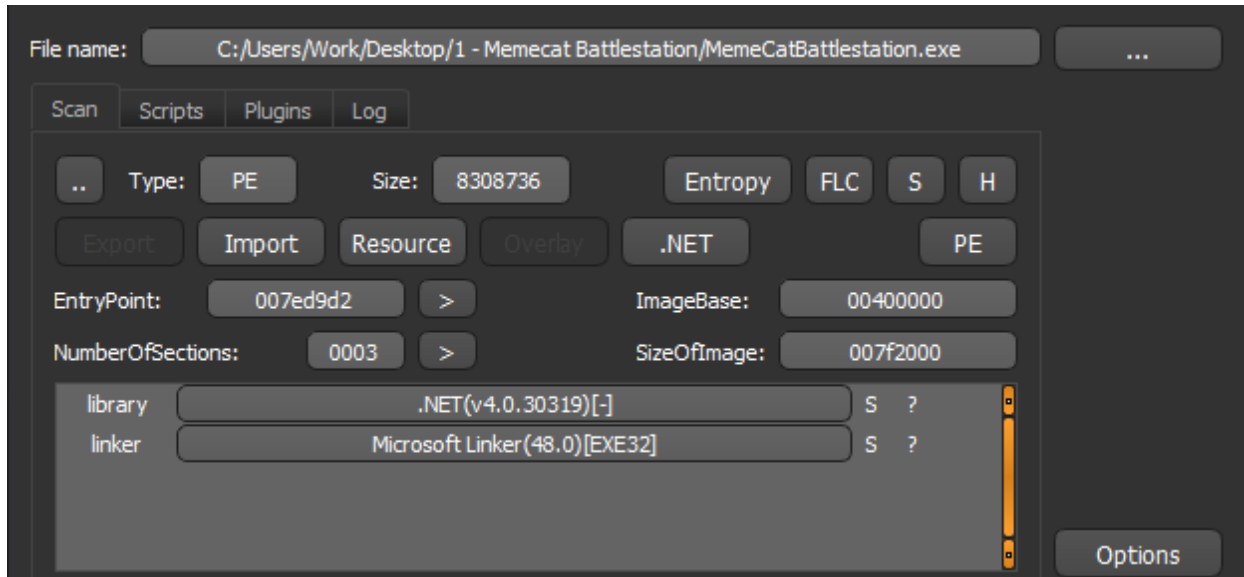


Memecat Battlestation

Đầu tiên ta kiểm tra xem chương trình viết bằng ngôn ngữ gì

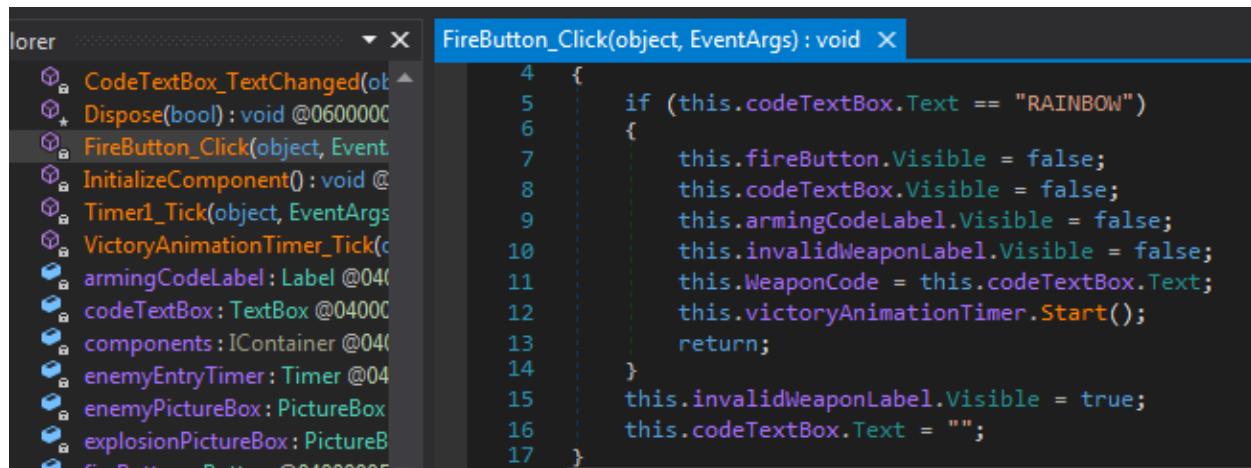


Như hình, chương trình được viết bằng .NET, cho nên tiếp theo là debug chương trình bằng dnSpy

```
Application.Run(stage1Form);
if (stage1Form.WeaponCode == null)
{
    return;
}
Stage2Form stage2Form = new Stage2Form();
stage2Form.Location = stage1Form.Location;
Application.Run(stage2Form);
if (stage2Form.WeaponCode == null)
{
    return;
}
Application.Run(new VictoryForm
{
    Arsenal = string.Join(",", new string[]
    {
        stage2Form.WeaponCode,
        stage1Form.WeaponCode
    }),
    Location = stage2Form.Location
});
```

Nhìn vào hàm main ta thấy có 2 form nhập mã và 1 form hiển thị flag

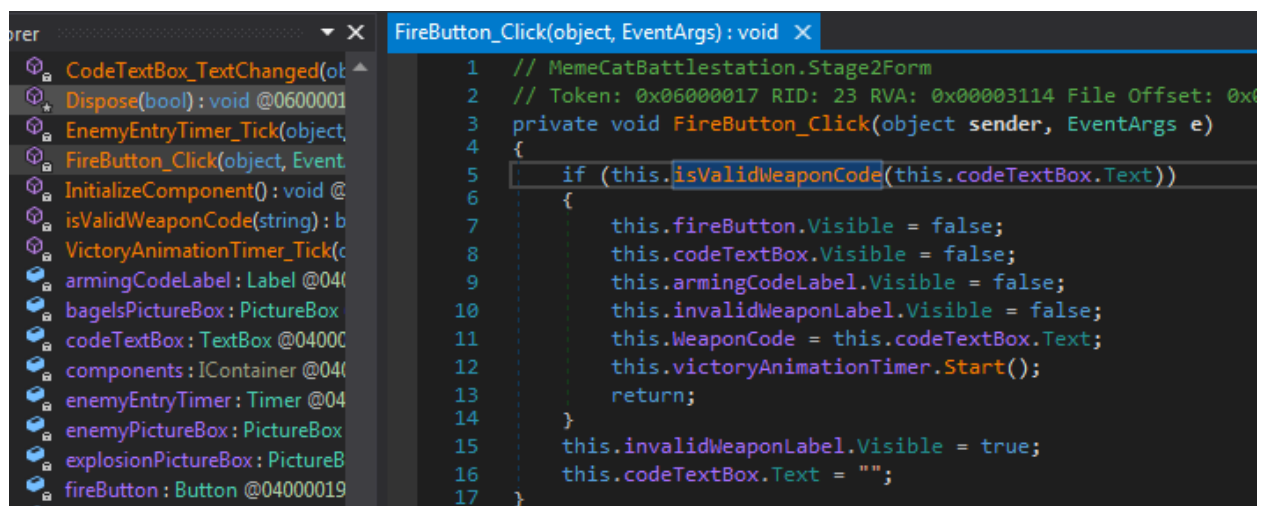
Kiểm tra stage1Form ta thấy có FireButton_Click bên trong có đoạn code:



```
FireButton_Click(object, EventArgs) : void X
4 {
5     if (this.codeTextBox.Text == "RAINBOW")
6     {
7         this.fireButton.Visible = false;
8         this.codeTextBox.Visible = false;
9         this.armingCodeLabel.Visible = false;
10        this.invalidWeaponLabel.Visible = false;
11        this.WeaponCode = this.codeTextBox.Text;
12        this.victoryAnimationTimer.Start();
13        return;
14    }
15    this.invalidWeaponLabel.Visible = true;
16    this.codeTextBox.Text = "";
17 }
```

Theo như đoạn code trên, mã cho stage1Form là “RAINBOW”

Tương tự ta kiểm tra stage2Form:



```
FireButton_Click(object, EventArgs) : void X
1 // MemeCatBattlestation.Stage2Form
2 // Token: 0x06000017 RID: 23 RVA: 0x00003114 File Offset: 0x00003114
3 private void FireButton_Click(object sender, EventArgs e)
4 {
5     if (this.isValidWeaponCode(this.codeTextBox.Text))
6     {
7         this.fireButton.Visible = false;
8         this.codeTextBox.Visible = false;
9         this.armingCodeLabel.Visible = false;
10        this.invalidWeaponLabel.Visible = false;
11        this.WeaponCode = this.codeTextBox.Text;
12        this.victoryAnimationTimer.Start();
13        return;
14    }
15    this.invalidWeaponLabel.Visible = true;
16    this.codeTextBox.Text = "";
17 }
```

Lúc này fire button sẽ gọi hàm isValidWeaponCode để check input của Textbox

```
private bool isValidWeaponCode(string s)
{
    char[] array = s.ToCharArray();
    int length = s.Length;
    for (int i = 0; i < length; i++)
    {
        char[] array2 = array;
        int num = i;
        array2[num] ^= 'A';
    }
    return array.SequenceEqual(new char[]
    {
        '\u0003',
        ',',
        '&',
        '$',
        '-',
        '\u001e',
        '\u0002',
        ',',
        '/',
        '/',
        '.',
        '/'
    });
}
```

Theo đoạn code trên ta chỉ cần lấy từng giá trị trong array XOR với giá trị của ký tự 'A' là 0x41 là sẽ có được mã của stage2Form, đoạn mã này là Bagel_Cannon

Và ta có Flag là:

Kitteh_save_galixy@flare-on.com