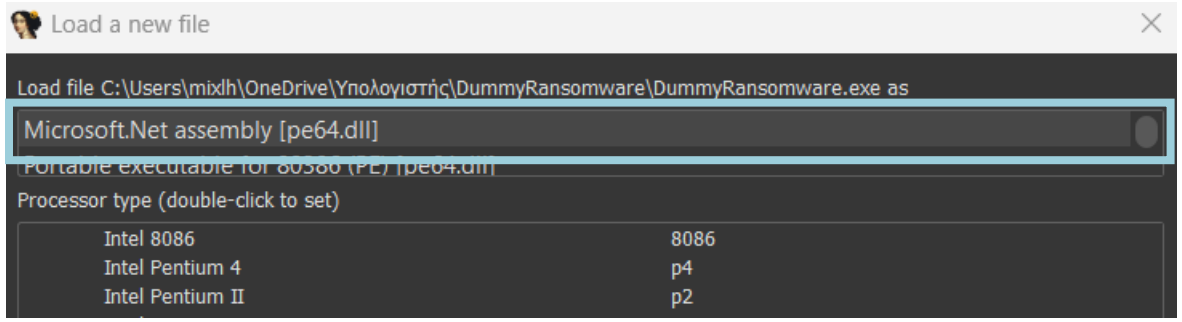
DNSPY

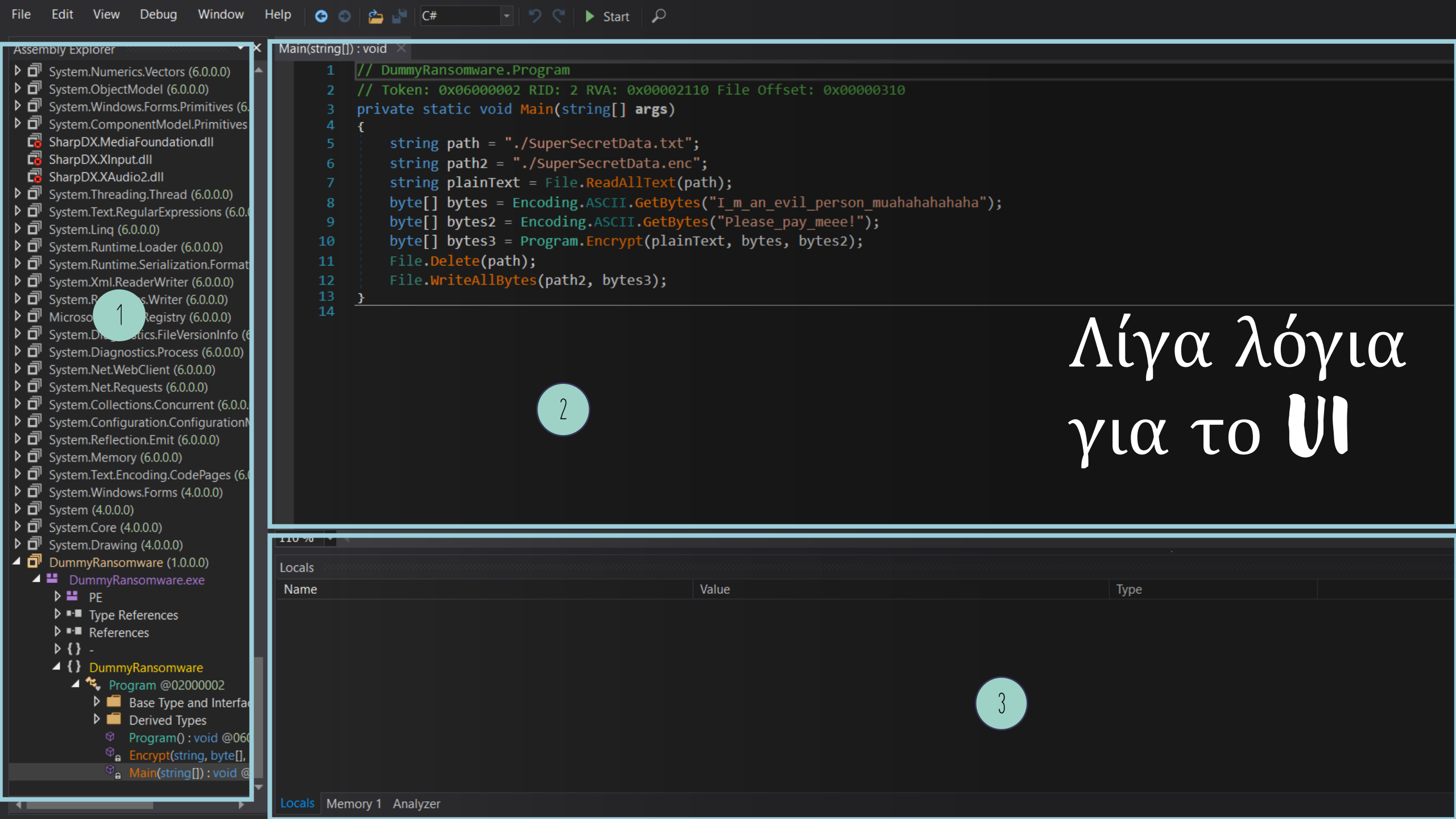
I mean, couldn't they make a better logo?

Τι είναι το DnSpy;

- Άλλος ένας decompiler/debugger
- Αλλά χρησιμοποιείται για C# executables (.NET Assemblies)
- Πώς καταλαβαίνω ένα .NET Assembly?

- Απλά ρώτα την IDA




File Edit View Debug Window Help
C#
Start
Assembly Explorer
System.Numerics.Vectors (6.0.0.0)
System.ObjectModel (6.0.0.0)
System.Windows.Forms.Primitives (6.
System.ComponentModel.Primitives
SharpDX.MediaFoundation.dll
SharpDX.XInput.dll
SharpDX.XAudio2.dll
System.Threading.Thread (6.0.0.0)
System.Text.RegularExpressions (6.0.
System.Linq (6.0.0.0)
System.Runtime.Loader (6.0.0.0)
System.Runtime.Serialization.Format
System.Xml.ReaderWriter (6.0.0.0)
System.R s.Writer (6.0.0.0)
Microso Registry (6.0.0.0)
System.Di tics.FileVersionInfo (
System.Diagnostics.Process (6.0.0.0)
System.Net.WebClient (6.0.0.0)
System.Net.Requests (6.0.0.0)
System.Collections.Concurrent (6.0.0.
System.Configuration.ConfigurationM
System.Reflection.Emit (6.0.0.0)
System.Memory (6.0.0.0)
System.Text.Encoding.CodePages (6.
System.Windows.Forms (4.0.0.0)
System (4.0.0.0)
System.Core (4.0.0.0)
System.Drawing (4.0.0.0)
DummyRansomware (1.0.0.0)
DummyRansomware.exe
PE
Type References
References
-
DummyRansomware
Program @02000002
Base Type and Interfa
Derived Types
Program() : void @060
Encrypt(string, byte[],
Main(string[]) : void @
1
Main(string[]) : void
1 // DummyRansomware.Program
2 // Token: 0x06000002 RID: 2 RVA: 0x00002110 File Offset: 0x00000310
3 private static void Main(string[] args)
4 {
5 string path = "./SuperSecretData.txt";
6 string path2 = "./SuperSecretData.enc";
7 string plainText = File.ReadAllText(path);
8 byte[] bytes = Encoding.ASCII.GetBytes("I_m_an_evil_person_muahahahahaha");
9 byte[] bytes2 = Encoding.ASCII.GetBytes("Please_pay_meee!");
10 byte[] bytes3 = Program.Encrypt(plainText, bytes, bytes2);
11 File.Delete(path);
12 File.WriteAllBytes(path2, bytes3);
13 }
14
2
Λίγα λόγια για το UI
110 %
Locals
Name
Value
Type
3
Locals
Memory 1
Analyzer

Λίγα λόγια για το UI

1. **Assembly Explorer** → Η λίστα με τα εκτελέσιμα (assemblies) που έχουν φορτωθεί στο DnSpy.

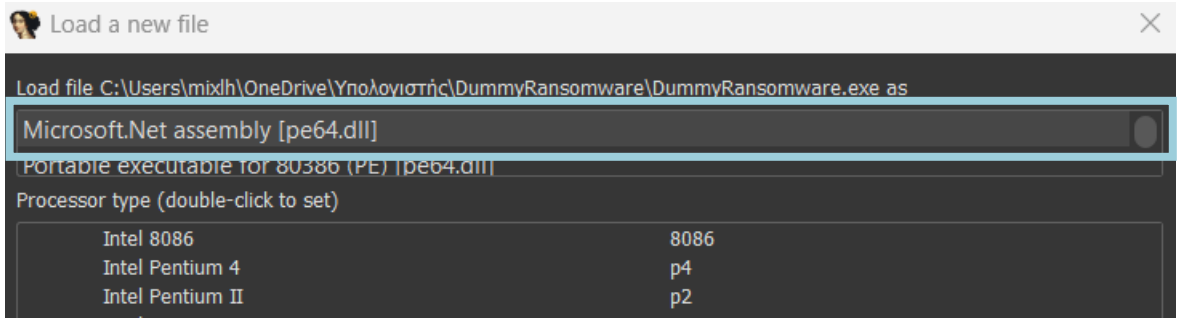
2. **Decompilation View** → Σε αυτό το παράθυρο εμφανίζεται ο decompiled κώδικας των μεθόδων των κλάσεων του προγράμματος, καθώς και πληροφορίες metadata του .NET Assembly.

3. **Debugging View** → Εδώ εμφανίζονται πληροφορίες σχετικά με τις τιμές των local variables, της μνήμης του προγράμματος κ.α. όταν το εκτελούμε δυναμικά μέσω του DnSpy (Το debugging δε θα μας απασχολήσει σε αυτές τις διαφάνειες).

Παράδειγμα ανάλυσης C# Assembly μέσω DnSpy

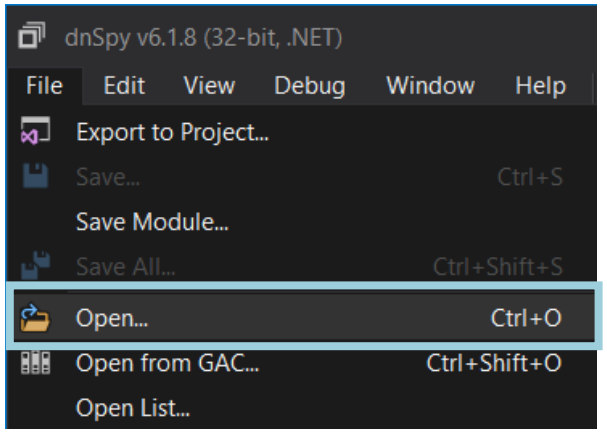
- Θα αναλύσουμε την περίπτωση ενός mini ransomware

Έχουμε 2 αρχεία. Ένα executable κι ένα encrypted file με «σημαντικά» δεδομένα.
Η IDA μας λέει για το executable:

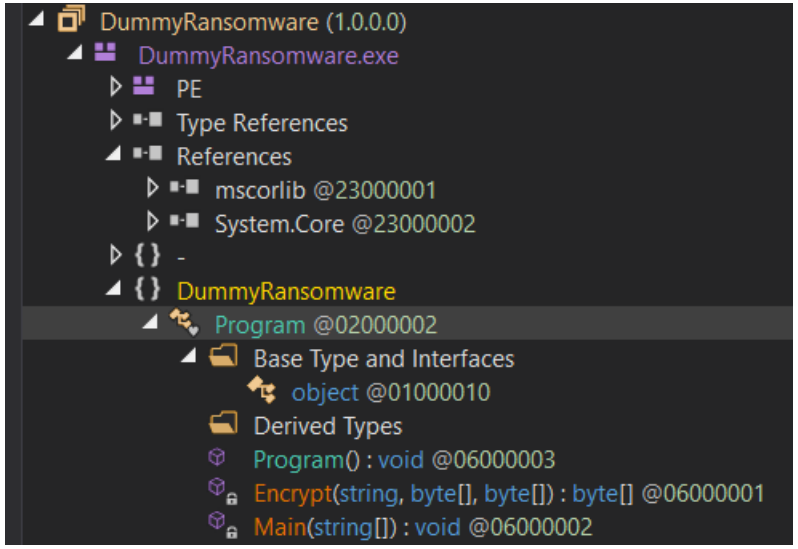


Η IDA Pro υποστηρίζει .NET disassembly/decompilation. Ωστόσο διαθέτουμε τη free έκδοση ☹
Άρα θα χρησιμοποιήσουμε το εξίσου ισχυρό DnSpy!

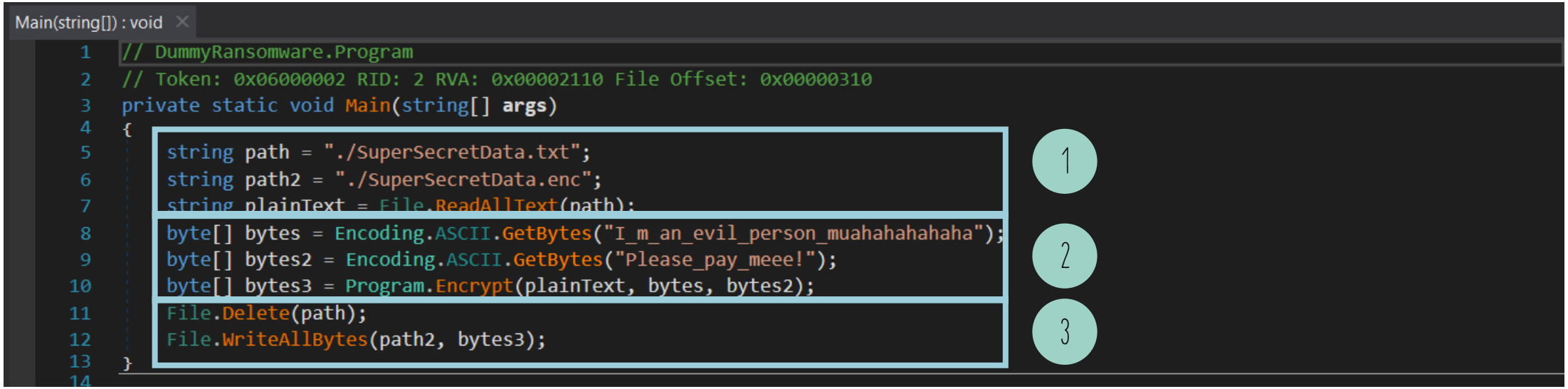
- Η φόρτωση του αρχείου στο DnSpy μπορεί να γίνει από το μενού File → Open…



- Αφού φορτώσουμε το αρχείο, μπορούμε να δούμε τη δομή του στον Assembly Explorer:



- Επιλέγουμε προς προβολή τη μέθοδο Main



- Διαπιστώνουμε τα εξής:

1. Αρχικά στις μεταβλητές **path** και **path2** αποθηκεύονται οι διαδρομές 2 αρχείων.
Αργότερα, βλέπουμε ότι τα περιεχόμενα του 'SuperSecretData.txt' διαβάζονται στη μεταβλητή **plainText**, οπότε υποθέτουμε ότι το **path** αντιστοιχεί στο αρχείο μας πριν το encryption.

2. Καλείται η συνάρτηση Encrypt με ορίσματα το plainText και δύο άλλες μεταβλητές, η κάθε μία από τις οποίες περιέχει μια συμβολοσειρά (που έχει μετατραπεί σε bytes). Οι δύο συμβολοσειρές είναι οι 'I_m_an_evil_person_muahahahahaha' και 'Please_pay_meee!'. Το αποτέλεσμα του encryption αποθηκεύεται στη μεταβλητή **bytes3**.

3. Τέλος, το αρχικό μας αρχείο 'SuperSecretData.txt' διαγράφεται και τη θέση του παίρνει το 'SuperSecretData.enc', το οποίο περιέχει τα encrypted δεδομένα. Άρα τελικά η μεταβλητή **path2** αντιστοιχεί τελικά στο όνομα που θα λάβει το encrypted αρχείο.

- Επιλέγουμε προς προβολή τη μέθοδο Encrypt

```
1  // DummyRansomware.Program
2  // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
3  private static byte[] Encrypt(string plainText, byte[] Key, byte[] IV)
4  {
5      byte[] result;
6      using (AesManaged aesManaged = new AesManaged())
7      {
8          ICryptoTransform transform = aesManaged.CreateEncryptor(Key, IV);
9          using (MemoryStream memoryStream = new MemoryStream())
10         {
11             using (CryptoStream cryptoStream = new CryptoStream(memoryStream, transform, CryptoStreamMode.Write))
12             {
13                 using (StreamWriter streamWriter = new StreamWriter(cryptoStream))
14                 {
15                     streamWriter.Write(plainText);
16                 }
17                 result = memoryStream.ToArray();
18             }
19         }
20     }
21     return result;
22 }
23
```

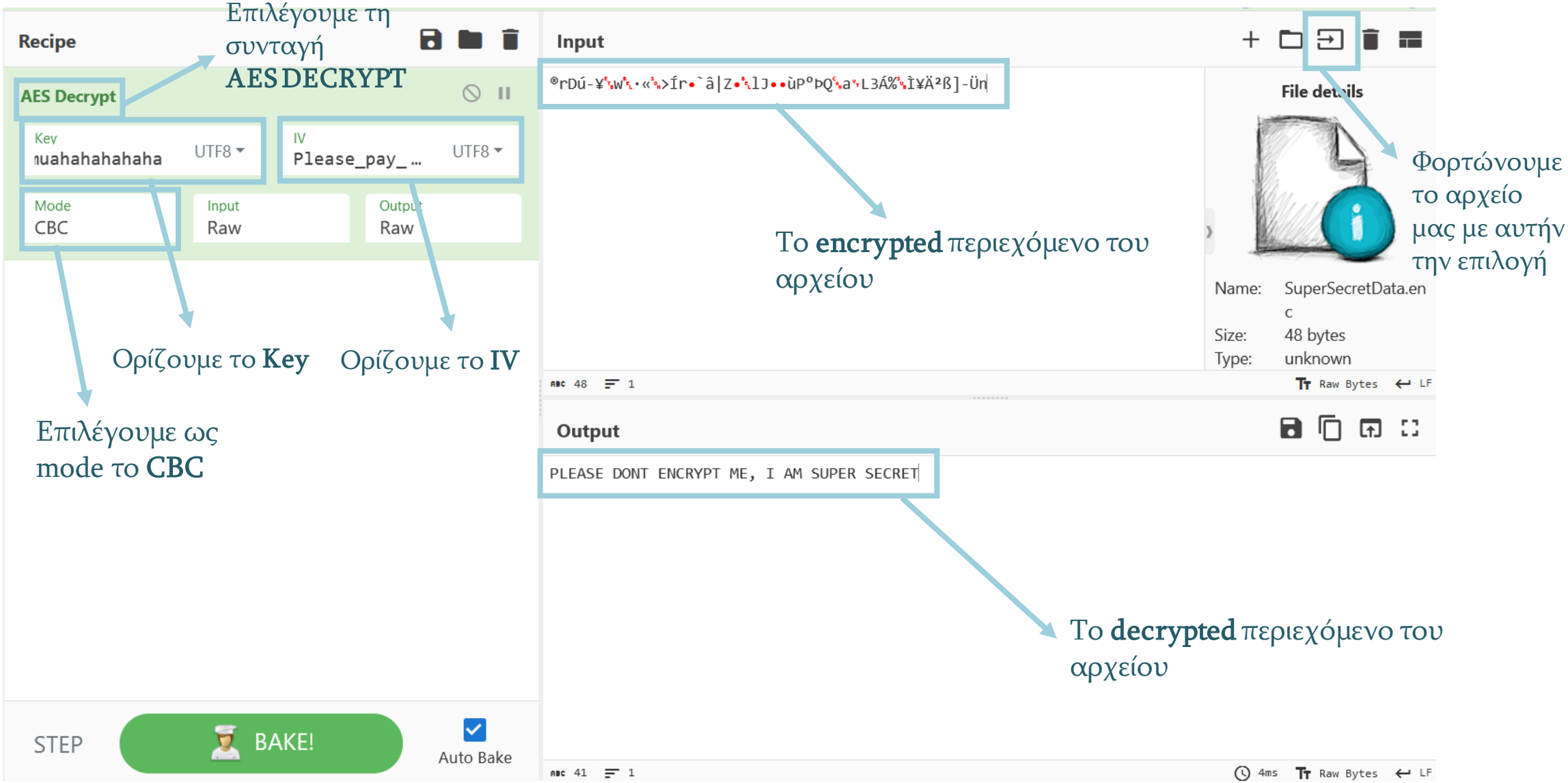
Παραθέτουμε επίσης το τμήμα κώδικα της Main που την καλεί:

```
byte[] bytes = Encoding.ASCII.GetBytes("I_m_an_evil_person_muahahahahaha");
byte[] bytes2 = Encoding.ASCII.GetBytes("Please_pay_meee!");
byte[] bytes3 = Program.Encrypt(plainText, bytes, bytes2);
```

Με βάση τα παραπάνω, μπορούμε να διαπιστώσουμε ότι το Encryption method που χρησιμοποιήθηκε ήταν ο αλγόριθμος AES-CBC, με **key** το 'I_m_an_evil_person_muahahahahaha' και **IV** το 'Please_pay_meee!'. Ο λόγος που οι συμβολοσειρές για το key και το iv μετατράπηκαν σε bytes είναι ότι σε αυτήν τη μορφή τις ζητά ο αλγόριθμος.

Συνεπώς μπορούμε πλέον να προχωρήσουμε στο decryption.

- Υπάρχουν πολλοί τρόποι για να κάνει κανείς AES Decryption. Για λόγους απλούστευσης θα χρησιμοποιήσουμε πάλι το εργαλείο CyberChef!!



References and addressing the elephant

References

- Για την υλοποίηση του AES χρησιμοποίησα αυτόν τον κώδικα:

AES Template

- Το github του DnSpy: DnSpy – Repo

Επιπλέον υλικό

- Σε αυτό το σημείο πρέπει να αναφέρω ότι το DnSpy έχει και άλλες λειτουργίες πέρα από decompiler. Μπορεί να χρησιμοποιηθεί ως disassembler, debugger και ακόμα και για patching .NET Assemblies. Για περισσότερο υλικό μπορείτε να δείτε τα παρακάτω:

DnSpy Game Modding

Advanced DnSpy Tricks

Ok, so that was short, hope that it was also sweet!!