# Reverse2 L08 Report by vivaman

1. Level8

- **Borland Delphi 6.0 - 7.0**
- **Dede 를 이용하여 불러 들인 후, Button1Click 으로 들어 갑니다.**

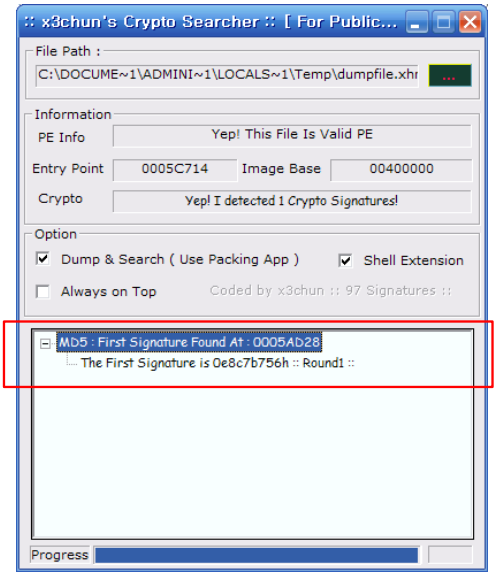
- **Dede Button1Click** ...쭈욱~ 내려가면...

```
0045BB9B   E8B0FCFFFF          call    0045B850
0045BBA0   8B55EC              mov     edx, [ebp-$14]
0045BBA3   58                  pop     eax
0045BBA4   E89390FAFF          call    00404C3C
0045BBA9   751A                jnz     0045BBC5
0045BBAB   6A40                push    $40
* Possible String Reference to: 'Good Boy!!!'
0045BBAD   B964BC4500          mov     ecx, $0045BC64
* Possible String Reference to: 'Well done!'
```

- **0045B850 에서...조금 내려 가면 Serial을 만들기 시작합니다.**

```
0045B898   B901000000          mov     ecx, $00000001
0045B89D   8B5DFC              mov     ebx, [ebp-$04]
0045B8A0   0FB6740BFF          movzx   esi, byte ptr [ebx+ecx-$01]
0045B8A5   03F2                add     esi, edx
0045B8A7   69F672070000        imul    esi, esi, $00000772
0045B8AD   8BD6                mov     edx, esi
0045B8AF   0FAFD6              imul    edx, esi
0045B8B2   03F2                add     esi, edx
0045B8B4   0BF6                or      esi, esi
0045B8B6   69F674040000        imul    esi, esi, $00000474
0045B8BC   03F6                add     esi, esi
0045B8BE   8BD6                mov     edx, esi
0045B8C0   41                  inc     ecx
0045B8C1   48                  dec     eax
0045B8C2   75D9                jnz     0045B89D
```

```
0045B8D5   8B55FC              mov     edx, [ebp-$04]
0045B8D8   0FB65402FF          movzx   edx, byte ptr [edx+eax-$01]
0045B8DD   83C211              add     edx, +$11
0045B8E0   83EA05              sub     edx, +$05
0045B8E3   69D292000000        imul    edx, edx, $00000092
0045B8E9   03D2                add     edx, edx
0045B8EB   69D219080000        imul    edx, edx, $00000819
0045B8F1   0155F0              add     [ebp-$10], edx
0045B8F4   48                  dec     eax
0045B8F5   85C0                test    eax, eax
0045B8F7   75DC                jnz     0045B8D5
```

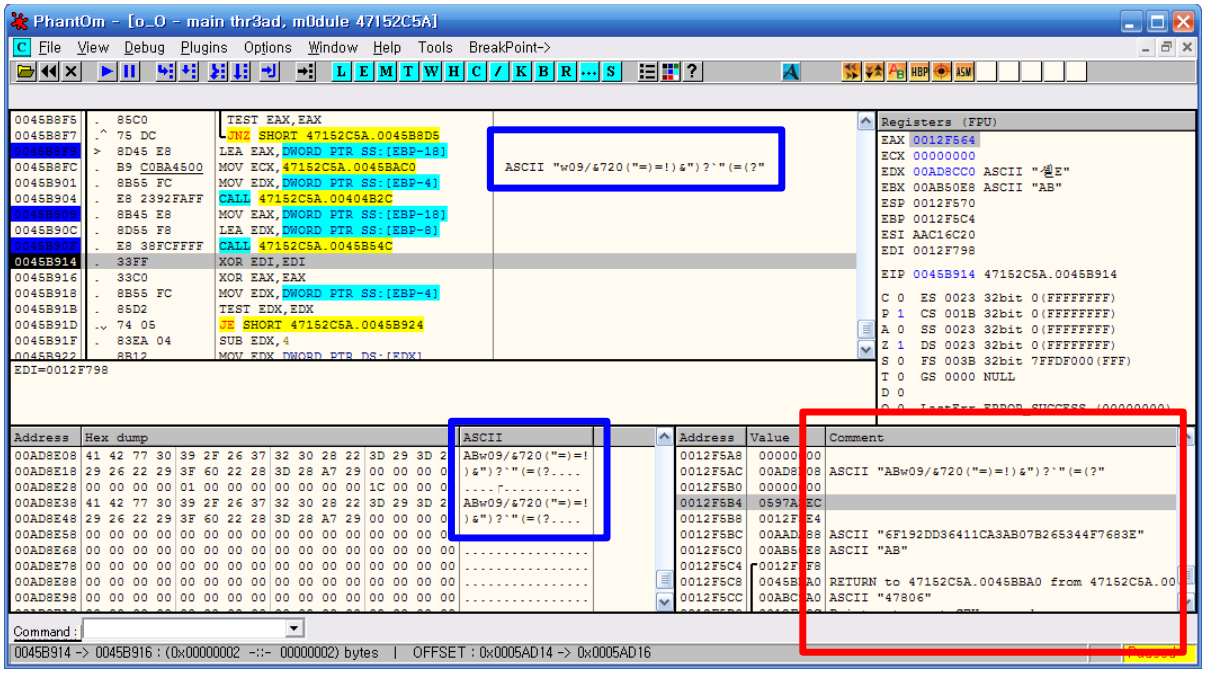



1번째

```
for (int i = 0; i < text.Length; i++)
{
    num2 = Convert.ToInt32(text[i]) + num;
    num2 *= 0x772;
    num3 = num2 * num2;
    num2 = num3 + num2;
    num2 *= 0x474;
    num2 += num2;
    num = num2;
}
```

2번째

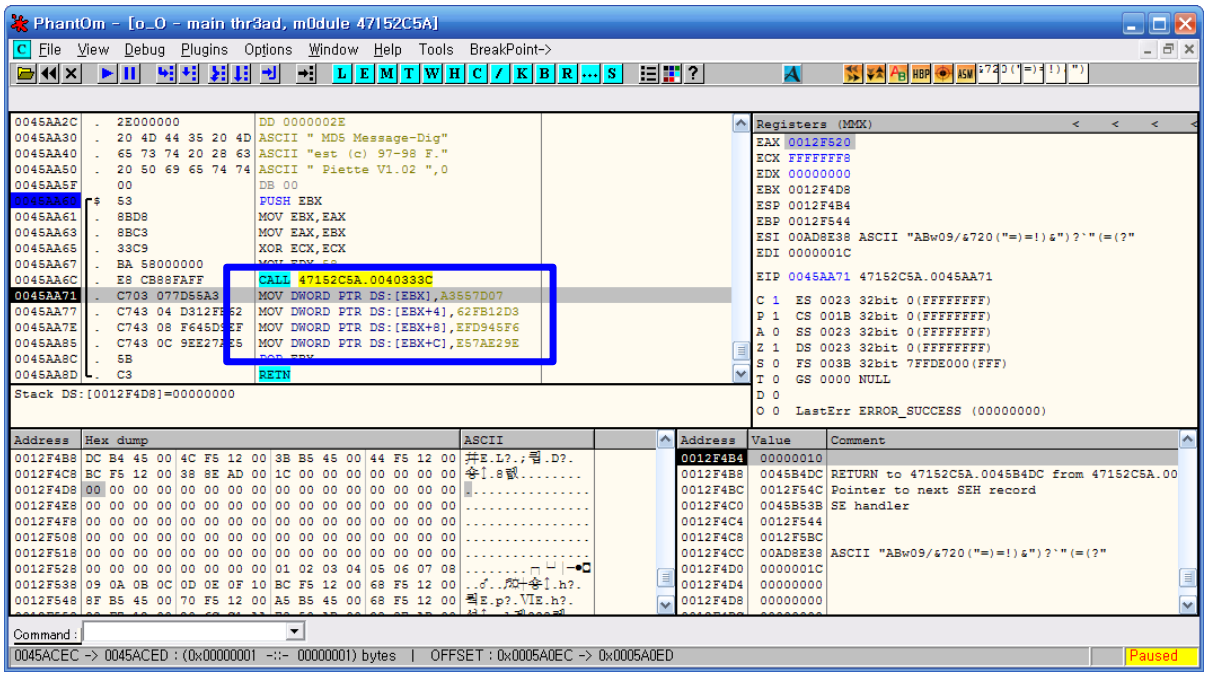
```
for (int j = text.Length - 1; j >= 0; j--)
{
    num2 = Convert.ToInt32(text[j]) + 0x11;
    num2 -= 5;
    num2 *= 0x92;
    num2 += num2;
    num2 *= 0x819;
    num += num2;
}
```




- AB 를 입력 했을 때, 만들어지는 MD5 는 "9E0E9E545EF63D41DFB653DAECF8EBC7"
- ABw09/&720("=)=!)&")?`"(=(?. 를 입력 했을 때, 만들어지는 MD5 는 "BEE310DE161CD8C8AA4E9FED5397EF22"
- 입력한 이름에 w09/&720("=)=!)&")?`"(=(?. 문자열을 더해서 MD5로 가는 것 같다...
- 그런데.... "6F192DD36411CA3AB07B265344F7683E"이 나온다.

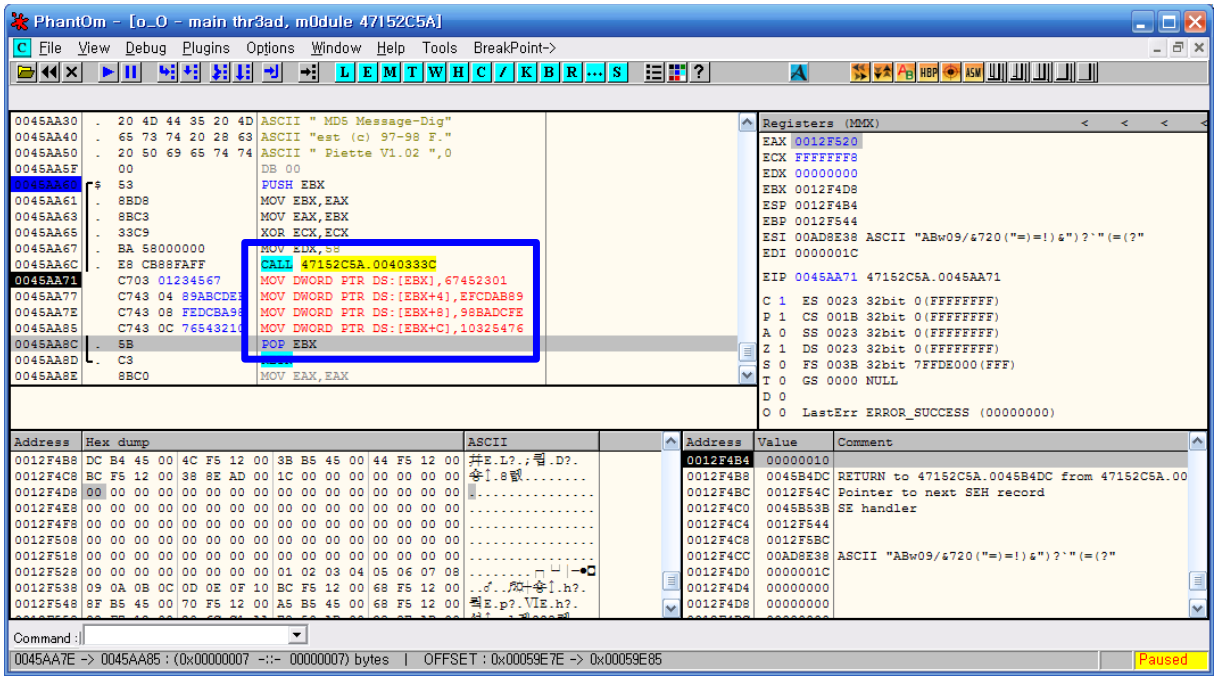
- MD5 계산에 문제가 있는거 같아서 ... 추적 시작..
- 0045B90F |. E8 38FCFFFF CALL 47152C5A.0045B54C
- 0045B58A |. E8 11FFFFFF CALL 47152C5A.0045B4A0
- 0045B4D7 |. E8 84F5FFFF CALL 47152C5A.0045AA60

- 이런, "Initialize()"값이 다른 것 같다.

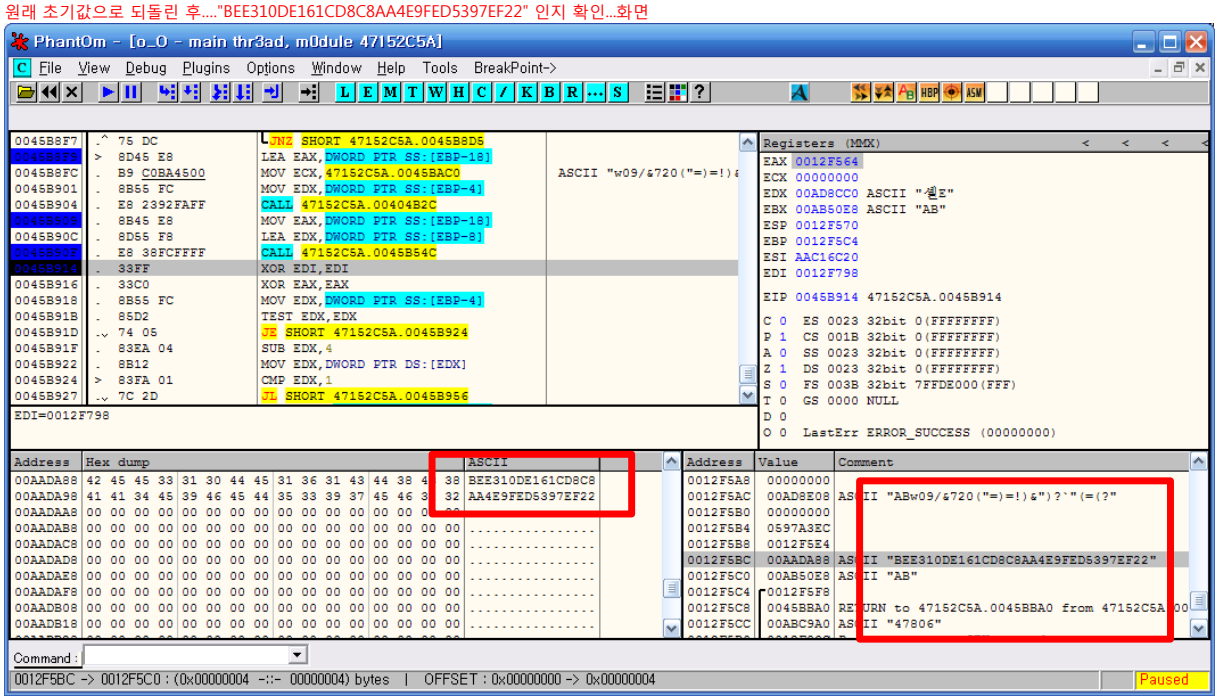



- 그래서, 원래 값으로 바꿔 보고,,,
- ABw09/&720("=)=!)&")?`"(=(?. 를 입력 했을 때, 만들어지는 MD5 는 "BEE310DE161CD8C8AA4E9FED5397EF22"인지 확인해보자 .

```
state[0] = 0xA3557D07; // 원래값: 0x67452301
state[1] = 0x62FB12D3; // 원래값: 0xefcdab89
state[2] = 0xEFD945F6; // 원래값: 0x98badcfe
state[3] = 0xE57AE29E; // 원래값: 0x10325476
```




- 원래 초기값으로 되돌린 후...."BEE310DE161CD8C8AA4E9FED5397EF22" 인지 확인...화면




- ABw09/&720("=)=!)&")?`"(=(?. 를 입력 했을 때, 만들어지는 MD5 는 "BEE310DE161CD8C8AA4E9FED5397EF22"
- **맞네요... Bingo~~~**

- 이제, 문제는 ABw09/&720("=)=!)&")?`"(=(?. 를 어떻게 입력하느냐가 문제인데...
- 이상한 문자가 섞여 있어서 쉽게 입력되질 않으니..
- Brute Force 로 만들어진 문자열에 w09/&720("=)=!)&")?`"(=(?. 를 간단히 byte[] 배열로 만들어서 입력하면 되겠습니다.

- 또, 문제가 되는 건, MD5에서 문자열로만 했었기 때문에...
- byte[] 배열을 사용할 수 있게 함수를 하나 이용하겠습니다.

```
public static string Md5Initarray(byte[] buffer)
{
    MD5 md = new MD5CryptoServiceProvider();
    byte[]  hash = md.ComputeHash(buffer);
    StringBuilder builder = new StringBuilder();
    foreach (byte num in hash)
    {
        builder.Append(num.ToString("x2"));
    }
    return builder.ToString();
}
```

**3번째**

```
byte[] buffer = new byte[]
{
0x77, 0x30, 0x39, 0x2f, 0x26, 0x37, 50, 0x30, 40, 0x22, 0x3d, 0x29, 0x3d,
0x21, 0x29, 0x26, 0x22, 0x29, 0x3f, 0x60, 0x22, 40, 0x3d, 40, 0xa7, 0x29
};
```

- 테스트 결과....잘 돌아 갑니다..

```
0045B929   8B4DFC              mov     ecx, [ebp-$04]
0045B92C   0FB64C11FF          movzx   ecx, byte ptr [ecx+edx-$01]
0045B931   03F9                add     edi, ecx
0045B933   81C729090000        add     edi, $00000929
0045B939   81C767070000        add     edi, $00000767
0045B93F   03F8                add     edi, eax
0045B941   69FF92830000        imul    edi, edi, $00008392
0045B947   8BC7                mov     eax, edi
0045B949   83E833              sub     eax, +$33
0045B94C   0FAFC7              imul    eax, edi
0045B94F   03C7                add     eax, edi
0045B951   4A                  dec     edx
0045B952   85D2                test    edx, edx
0045B954   75D3                jnz     0045B929
```

4번째

```
for (int k = text.Length - 1; k >= 0; k--)
                {
                    num2 = Convert.ToInt32(text[k]);
                    num += num2;
                    num += 0x929;
                    num += 0x767;
                    num += num3;
                    num *= 0x8392;
                    num3 = num;
                    num3 -= 0x33;
                    num3 *= num;
                    num3 += num;
                }
```

```
0045B966   7E48                jle     0045B9B0
0045B968   C745EC01000000      mov     dword ptr [ebp-$14], $00000001
0045B96F   8B55FC              mov     edx, [ebp-$04]
0045B972   8B4DEC              mov     ecx, [ebp-$14]
0045B975   0FB6540AFF          movzx   edx, byte ptr [edx+ecx-$01]
0045B97A   03DA                add     ebx, edx
0045B97C   03DB                add     ebx, ebx
0045B97E   8BD3                mov     edx, ebx
0045B980   0FAFD3              imul    edx, ebx
0045B983   0FAFDA              imul    ebx, edx
0045B986   83F310              xor     ebx, +$10
0045B989   83CB44              or      ebx, +$44
0045B98C   69D373030000        imul    edx, ebx, $00000373
0045B992   81C243040000        add     edx, $00000443
0045B998   8BDA                mov     ebx, edx
0045B99A   8B55FC              mov     edx, [ebp-$04]
0045B99D   8B4DEC              mov     ecx, [ebp-$14]
0045B9A0   0FB6540AFF          movzx   edx, byte ptr [edx+ecx-$01]
0045B9A5   03DA                add     ebx, edx
0045B9A7   0FAFDB              imul    ebx, ebx
0045B9AA   FF45EC              inc     dword ptr [ebp-$14]
0045B9AD   48                  dec     eax
0045B9AE   75BF                jnz     0045B96F
0045B9B0   8D45E4              lea     eax, [ebp-$1C]
```

5번째

```
for (int m = 0; m < text.Length; m++)
                {
                    num4 = Convert.ToInt32(text[m]);
                    num5 += num4;
                    num5 += num5;
                    num4 = num5;
                    num4 *= num5;
                    num5 *= num4;
                    num5 ^= 0x10;
                    num5 |= 0x44;
                    num4 = num5 * 0x373;
                    num4 += 0x443;
                    num5 = num4;
                    num4 = Convert.ToInt32(text[m]);
                    num5 += num4;
                    num5 *= num5;
                }
```

- **Brute Force 용 배열..**

```
string[] ch = new string[]
            {
            "A","B","C","D","E","F","G","H","I","J","K","L","M","N","O","P","Q","R","S","T","U","V","W","X","Y","Z",
            "0","1","2","3","4","5","6","7","8","9" ,
            "a", "b", "c", "d", "e", "f", "g", "h", "i", "j", "k", "l", "m", "n", "o", "p", "q", "r", "s","t","u","v","w","x","y","z"
            };
```

➢ **후기:**

➢ AB 를 입력했을 경우, 처음 나오는 시리얼이 AAC16C20 ,즉, 8자리 수이고 , 5D88 과는 비교할 수 없다.

- 역함수로는 불가능 하므로, 결국 Brute Force 로 해결 가능하다.
- C# 에서 MD5가 기본적으로 제공되므로...

```
state[0] = 0xA3557D07; // 원래값: 0x67452301
state[1] = 0x62FB12D3; // 원래값: 0xefcdab89
state[2] = 0xEFD945F6; // 원래값: 0x98badcfe
state[3] = 0xE57AE29E; // 원래값: 0x10325476
```

- 초기값 변환을 위한, C#용 MD5 소스를 구해야 했고..(C++,VB6 는 있는데..역시 구글링..)

- 입력한 이름 뒤에 더해지는 w09/&720("=)=!)&")?`"(=(?. 때문에,

```
public static string Md5Initarray(byte[] buffer)
{
    MD5 md = new MD5CryptoServiceProvider();
    byte[]  hash = md.ComputeHash(buffer);
    StringBuilder builder = new StringBuilder();
    foreach (byte num in hash)
```

```
            {
                builder.Append(num.ToString("x2"));
            }
            return builder.ToString();
        }
```

..가 필요했다...

-끝-