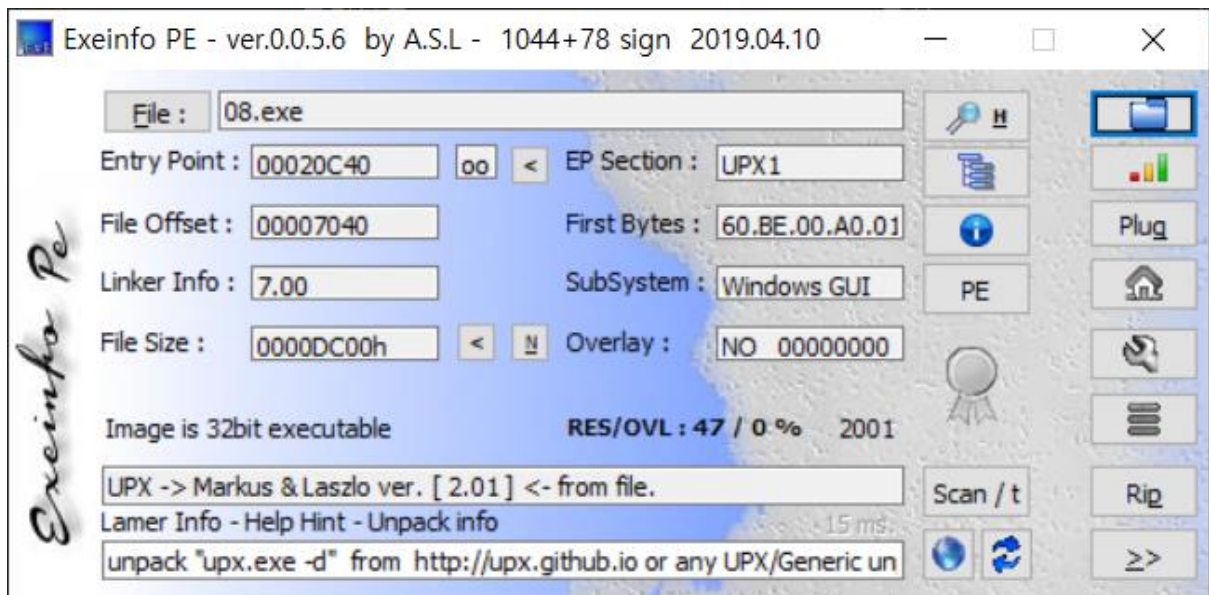


07.exe - OEP를 구하시오 Ex) 00400000

OEP 코드를 알기 위해 PE 분석을 해본다.



현재 UPX로 Packing이 되어있어 정상적인 OEP를 알 수가 없다. OEP를 알기 위해 UPX로 Unpacking를 해준다.

```
PS D:\OneDrive - JaeSeo\KShield Jr\tools\Reversing\upx-3.95-win64> .\upx.exe -d "C:\Users\kimja\Documents\UPX_unpacking\08-upxUnPacked.exe"
```

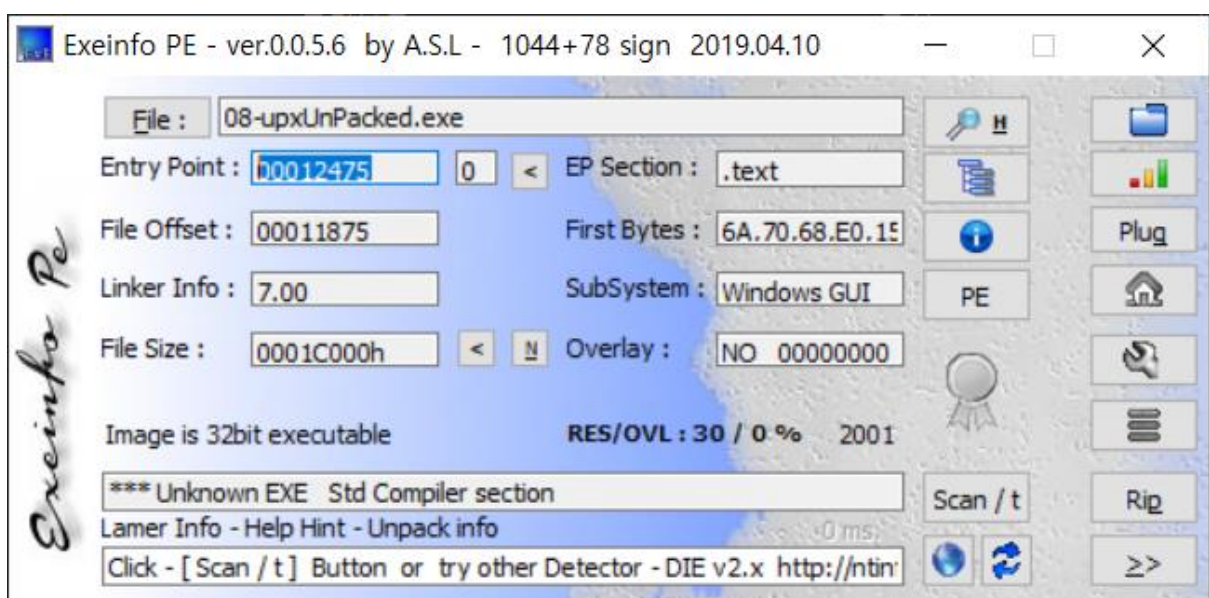
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2018
UPX 3.95w Markus Oberhumer, Laszlo Molnar & John Reiser Aug 26th 2018

File size	Ratio	Format	Name
114688 <-	56320	49.11%	win32/pe
			08-upxUnPacked.exe

Unpacked 1 file.

```
PS D:\OneDrive - JaeSeo\KShield Jr\tools\Reversing\upx-3.95-win64>
```

그리고 ExeinfoPE를 통해 다시한번 분석해본다.




EP는 00012475 라는 것을 알게 되었다.

Header info : [08-upxUnPacked.exe] - Size of Code : 012800h - decimal : 74 KB

Directory Info :		RVA	SIZE		
Export :	00000000	00000000	Not used	[1970-01-01]	
Import :	00012B80	0000008C	(01) .text	[1970-01-01]	
	00016000	0000897C	30 % of exe	Nr of ID : 8	
	00000000	00000000		[1970-01-01]	
Security :	00000000	00000000	not Signed		
Base Reloc :	00000000	00000000			
Debug :	00000000	00000000			
Architecture :	00000000	00000000		[1970-01-01]	
Global PTR :	00000000	00000000			
TLS Table :	00000000	00000000	Not used		
Load Config :	00000000	00000000			
Bound Import :	00000000	00000000	Not used		
Imp.Table IAT :	00000000	00000000	Not used		
Delay Import :	00000000	00000000			
Com Descriptor :	00000000	00000000	>> .NET Meta Directory		
reserved :	00000000	00000000			

From header :		Very often :
Size of headers :	00001000	400 or 1000
Size of optional header :	00E0	00E0
Number of Dirs :	0010	0010h
Base of Code :	00001000	00001000
Image Base :	01000000	00400000
Magic optional header :	010B	010B 32bit
Debugger Info - size :	No	
File offset to PE :	00F0	click me
Checksum CRC :	00000000	00000000
Machine type :	0x14C Intel I386 (same ID used for 4	
OS version :	5.1 5.1 Win NT 5.1 XP	
From file		4.0
Image version :	5.01	
File / sec-n alignment :	0200 / 1000	
Entry Point to End of File bytes :	42891 = 41.89 KB	

File icon : 

Close

또한 Image Base는 01000000인 것을 알 수 있다.

OEP는 Image Base + EP 하여 구한다.

정답: 01012475