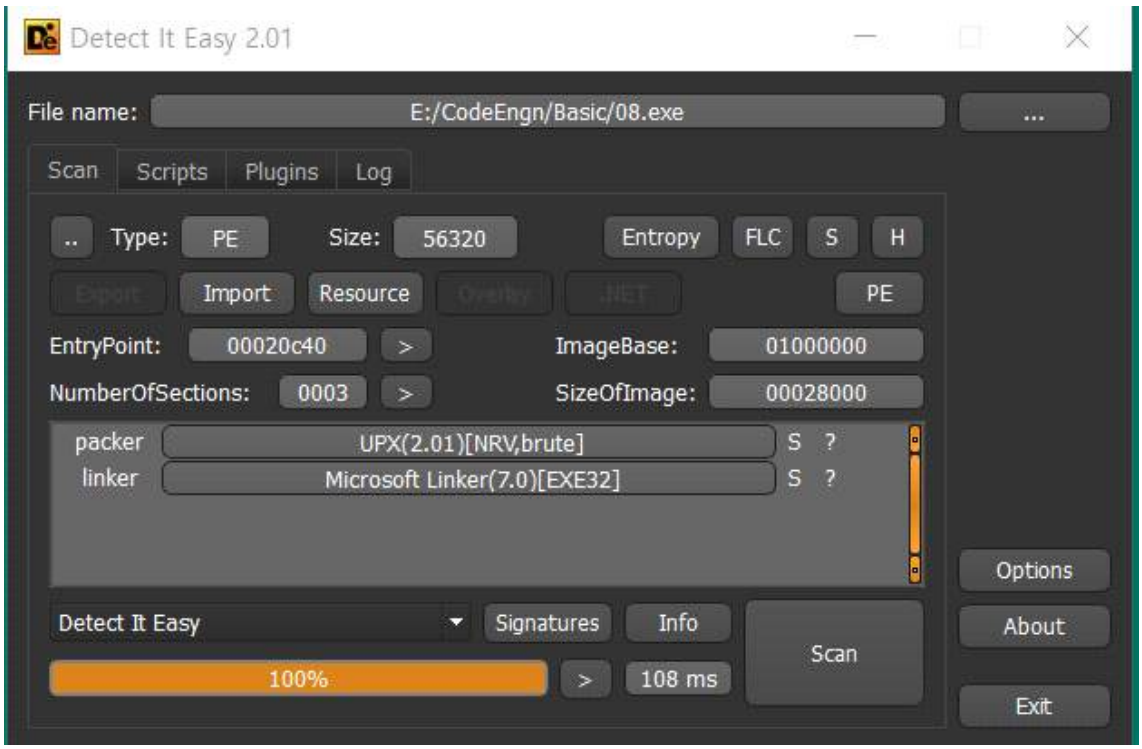
2019.02.14. CodeEngn RCE L08
Tree to Tree

OEP구하는 문제
OEP는 리얼 EP(EntryPoint)라고 할 수 있다.

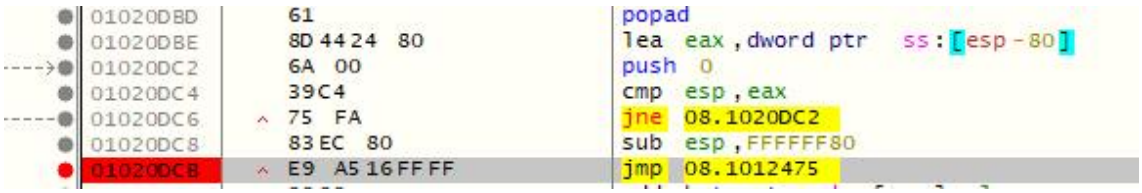


또 UPX! 버전은 다르다 2.01버전! UPX는 모든버전 언팩하는게 똑같다.

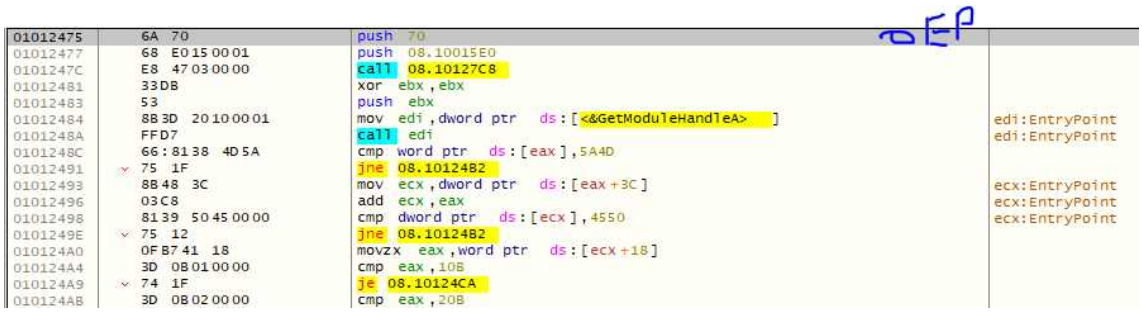
pushad에 breakpoint를 걸고

주소	Module/Label/Exception	상태	디스어셈블리	Hits	Summary
01020C40	<08.exe.EntryPoint>	One-time	pushad	0	진입점 중단점

popad를 찾으로 밑으로 쭈욱 내리면
popad아래부분에 jmp 명령어에 breakpoint걸고



실행 후 점프 하면 OPE를 찾을 수 있다.



OEP 01012475