

string 을 검색하여 시리얼 인증 루틴에 해당하는 함수 시작점을 쉽게 찾을 수 있다.  
 위 그림에서 브레이크포인트 걸린 call 함수가 입력한 name으로 시리얼을 생성한다.  
 이 함수 안으로 진입한다.

진입하면 첫 번째 반복 루틴이 나오는데 분석 해보면 입력한 name을 12자리로 맞춘다.  
 CE2를 입력하면 CE2CE2CE2CE2 이런식으로 맞춘다.

0047F14C	> 75 C6	JNZ SHORT BB574B47.0047F114	
0047F14E	> 8BF3	MOV ESI,EBX	
0047F150	> 85F6	TEST ESI,ESI	
0047F152	> 7E 35	JLE SHORT BB574B47.0047F189	
0047F154	> BB 01000000	MOV EBX,1	
0047F159	> 8B45 F4	MOV EAX,DWORD PTR SS:[EBP-C]	1번 루틴
0047F15C	> 0FB67C18 FF	MOVZX EDI,BYTE PTR DS:[EAX+EBX-1]	
0047F161	> 8B45 F0	MOV EAX,DWORD PTR SS:[EBP-10]	
0047F164	> 0FB64418 FF	MOVZX EAX,BYTE PTR DS:[EAX+EBX-1]	
0047F169	> 03F8	ADD EDI,EAX	
0047F16B	> 8D4D E8	LEA ECX,DWORD PTR SS:[EBP-18]	
0047F16E	> BA 04000000	MOV EDX,4	
0047F173	> 8BC7	MOV EAX,EDI	
0047F175	> E8 0AA9F8FF	CALL BB574B47.00409A84	시리얼 생성
0047F17A	> 8B55 E8	MOV EDX,DWORD PTR SS:[EBP-18]	
0047F17D	> 8D45 EC	LEA EAX,DWORD PTR SS:[EBP-14]	
0047F180	> E8 4F57F8FF	CALL BB574B47.004048D4	
0047F185	> 43	INC EBX	
0047F186	> 4E	DEC ESI	
0047F187	> 75 D0	JNZ SHORT BB574B47.0047F159	
0047F189	> 8D45 F4	LEA EAX,DWORD PTR SS:[EBP-C]	
0047F18C	> 8B55 EC	MOV EDX,DWORD PTR SS:[EBP-14]	
0047F18F	> E8 1055F8FF	CALL BB574B47.004046A4	
0047F194	> 8B45 F4	MOV EAX,DWORD PTR SS:[EBP-C]	
0047F197	> E8 3057F8FF	CALL BB574B47.004048C0	

두 번째 반복 루틴을 보면 12자리 name과 코드에 저장되어진 NH\_KeyGenMe6 와 한 바이트씩 더한후 앞에 00을 붙여 시리얼키를 만든다. 12자리 다 반복한다.

0047F186	> 4E	DEC ESI	
0047F187	> 75 D0	JNZ SHORT BB574B47.0047F159	
0047F189	> 8D45 F4	LEA EAX,DWORD PTR SS:[EBP-C]	
0047F18C	> 8B55 EC	MOV EDX,DWORD PTR SS:[EBP-14]	
0047F18F	> E8 1055F8FF	CALL BB574B47.004046A4	
0047F194	> 8B45 F4	MOV EAX,DWORD PTR SS:[EBP-C]	
0047F197	> E8 3057F8FF	CALL BB574B47.004048C0	
0047F19C	> 8BD8	MOV EBX,EAX	
0047F19E	> 83FB 0C	CMP EBX,0C	
0047F1A1	> 7E 0F	JLE SHORT BB574B47.0047F1B2	
0047F1A3	> 8D45 F4	LEA EAX,DWORD PTR SS:[EBP-C]	
0047F1A6	> 8BCB	MOV ECX,EBX	
0047F1A8	> BA 0D000000	MOV EDX,0D	
0047F1AD	> E8 BA59F8FF	CALL BB574B47.00404B6C	
0047F1B2	> 83FB 0C	CMP EBX,0C	
0047F1B5	> 7D 0B	JGE SHORT BB574B47.0047F1C2	
0047F1B7	> 8D45 F4	LEA EAX,DWORD PTR SS:[EBP-C]	
0047F1BA	> 8B55 F4	MOV EDX,DWORD PTR SS:[EBP-C]	
0047F1BD	> E8 1257F8FF	CALL BB574B47.004048D4	
0047F1C2	> 8B45 F4	MOV EAX,DWORD PTR SS:[EBP-C]	
0047F1C5	> E8 0257F8FF	CALL BB574B47.004048C0	
0047F1CA	> 8BD8	MOV EBX,EAX	
0047F1CC	> 83FB 0C	CMP EBX,0C	
0047F1CF	> 75 CD	JNZ SHORT BB574B47.0047F19E	
0047F1D1	> 8B45 F8	MOV EAX,DWORD PTR SS:[EBP-8]	
0047F1D4	> 8B55 F4	MOV EDX,DWORD PTR SS:[EBP-C]	
0047F1D7	> E8 8454F8FF	CALL BB574B47.00404660	

여기 반복문에서는 위에서 나온 시리얼 키중에 12자리만 가져온다.

후에 입력한 시리얼 뒤에 12자리랑 비교한다.

그림에는 없지만 첫 부분에 입력한 시리얼키 앞부분이 NH6-0- 인지 아닌지 체크부분도 있다.