[102] – [Stage - 1]

Team Information

Team Name : HSPACE

Team Member : Jinung Lee, Beomjun Park, DoHyeon Kim, Soyoung Cho

Email Address : hspacedigitalforensicslab@gmail.com

Teams must:

- Provide a detailed, step-by-step description of their problem-solving approach to ensure reproducibility by another examiner.
- List all tools used to arrive at their conclusions.

Tools used:

Name:	VMware Workstation Pro	Publisher:	Broadcom
Version:	17.6.3		
URL:	https://www.vmware.com		

Name:	BandiZip	Publisher:	BandiSoft
Version:	7.40		
URL:	https://www.bandisoft.com/bandizip		

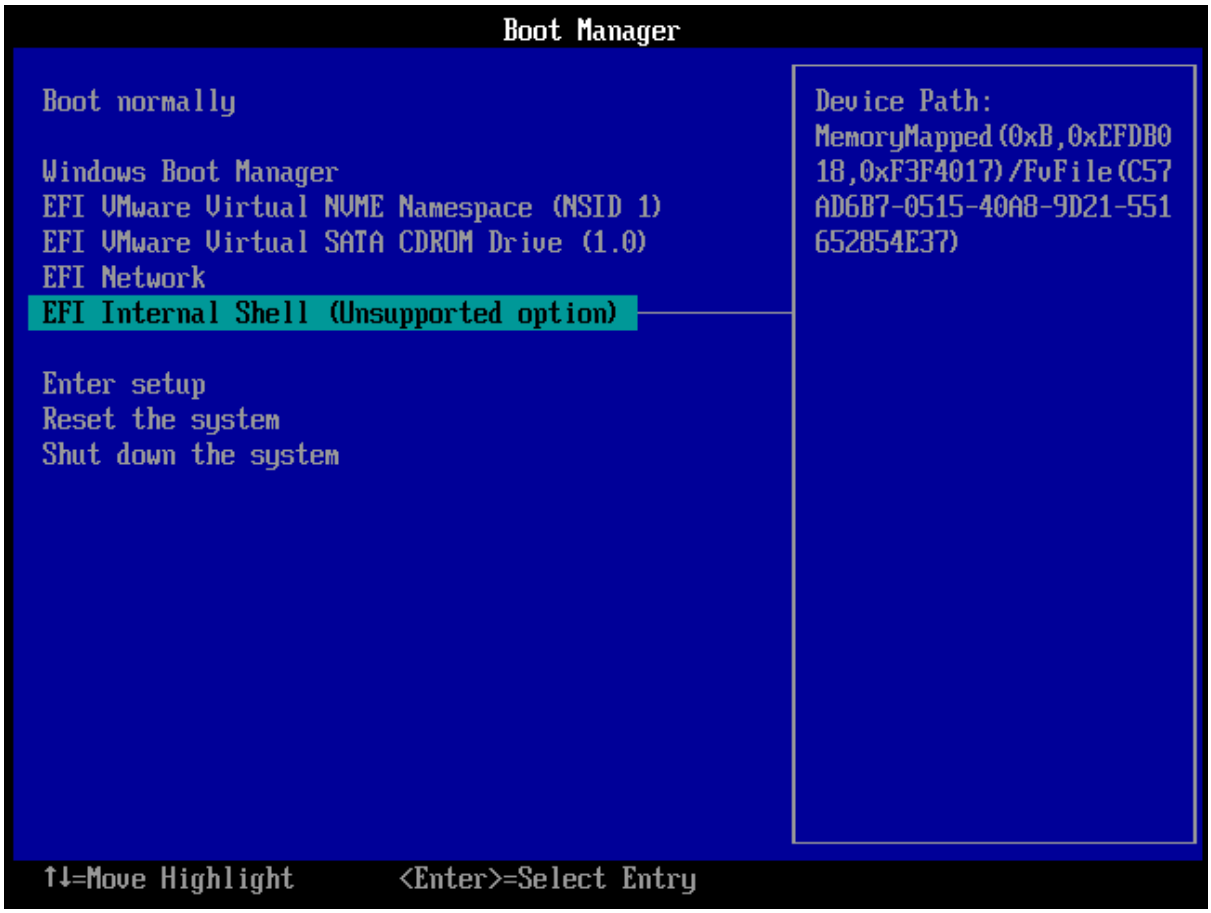
Name:	Python	Publisher:	Python
Version:	3.10		
URL:	https://www.python.org		

문제 풀이

RamdomSeed는 어디에 존재하며 어떻게 획득할 수 있나요?

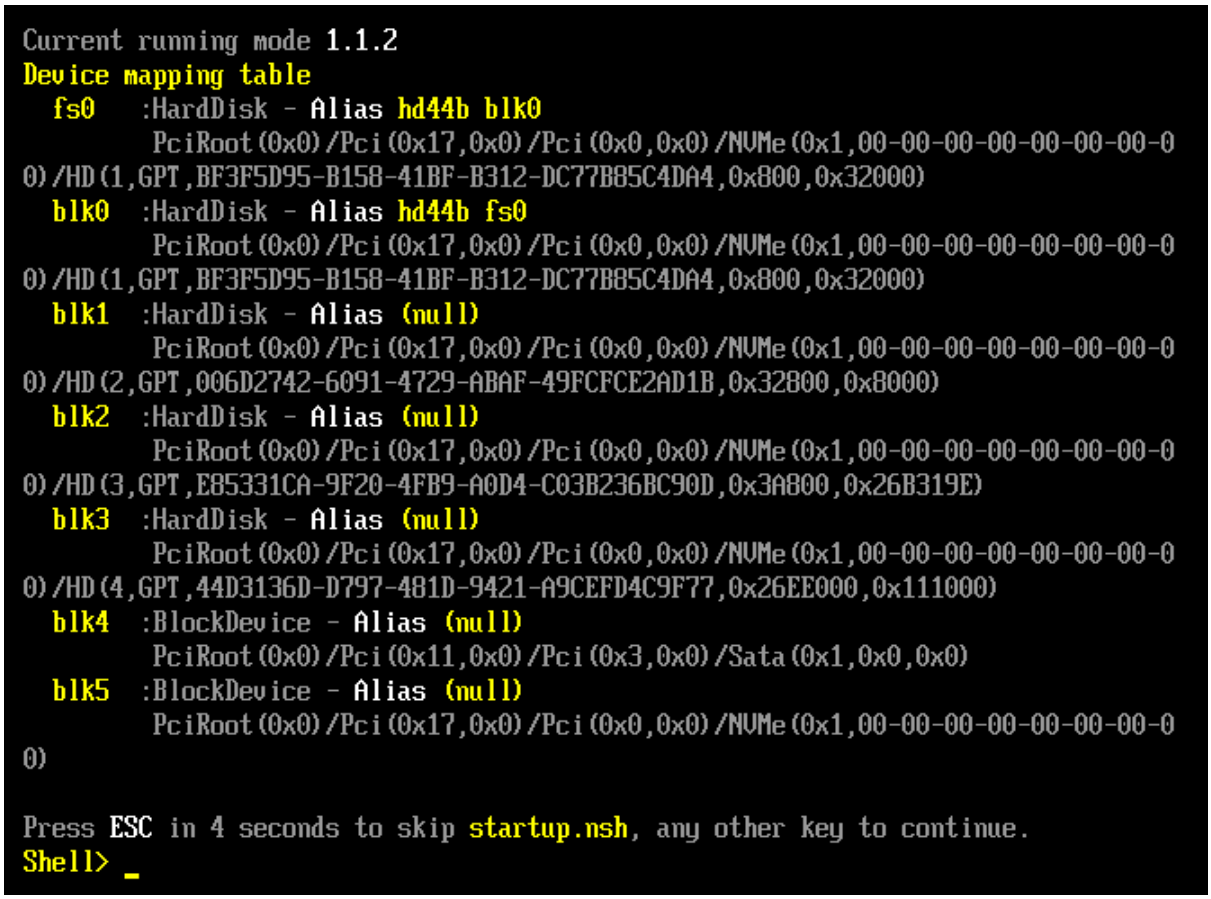
(1) Boot Manager 진입

PC의 전원버튼을 누른 후 특정 키(메인보드 제조사마다 상이)를 트리거 시켜, Boot Manager에 진입하면 EFI (Extensible Firmware Interface) Shell에 접근할 수 있는 메뉴를 확인할 수 있습니다.



(2) EFI Shell 진입

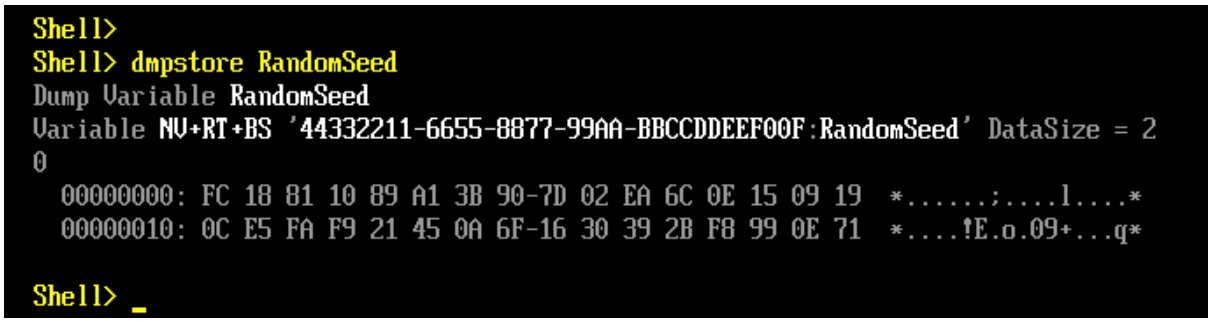
EFI Shell에 진입하게 되면 다음과 같이 명령어를 입력할 수 있는 Shell이 나타나게 됩니다.



(3) EFI Shell 변수 조회

부팅 과정에서 필요한 옵션에 대한 변수 값은 NVRAM(Non-Volatile RAM)에 저장됩니다. EFI Shell에는 NVRAM에 저장되어 있는 변수를 조회하는 "dmpstore"이라는 명령어가 존재합니다.

해당 명령어를 통해 문제 지문에 명시되어 있는 "RandomSeed"를 조회하면, 특정 값이 저장되어 있는 것을 확인할 수 있습니다.



정답	
RandomSeed	FC18811089A13B907D02EA6C0E1509190CE5FAF921450A6F1630392BF8990E71

#FLAG는 무엇인가요?

(1) Base64 URL 인코딩

문제 지문에 따라, 획득한 RandomSeed값을 Base64 URL로 인코딩 합니다.

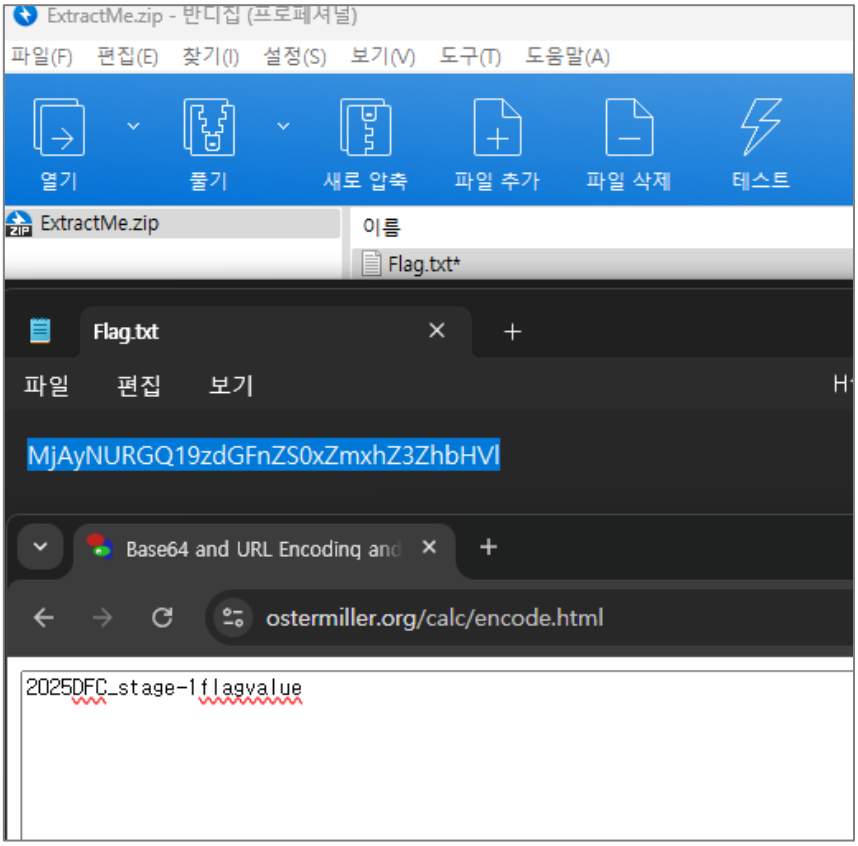
```
solv.py
1  import base64
2  import binascii
3
4  randomseed = b"FC18811089A13B907D02EA6C0E1509190CE5FAF921450A6F1630392BF8990E71".lower()
5  print(base64.urlsafe_b64encode(binascii.unhexlify(randomseed)))

b'_BiBEImhO5B9AupsDhUJGQzl-vkhRQpvFjA5K_iZDnE='
[Finished in 68ms]
```

(2) ZIP 압축 해제

위에서 획득한 값을 ZIP 비밀번호로 적용하여 문제 파일로 주어진 "ExtractMe.zip" 압축 파일의 압축 해제합니다. 이때, 위 Base64 URL 값에서 "=" 패딩을 제외한 값을 비밀번호로 사용합니다.

압축 해제 결과, 다음과 같이 Base64로 추정되는 내용이 포함된 텍스트 파일을 획득할 수 있었습니다. 이어서 Base64 해제 결과, Flag를 획득할 수 있었습니다.



정답	
FLAG	2025DFC_stage-1flagvalue