

## 102 – Stage-1

### Team Information

Team Name : HUNTR/X

Team Member : Hyeonseo Shin, Seungyeon Lim, Sugyung Lee

Email Address : huntrix@googlegroups.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:	UEFITool NE	Publisher:	CodeRush
Version:	Alpha 72		
URL:	<a href="https://github.com/LongSoft/UEFITool">https://github.com/LongSoft/UEFITool</a>		

Name:	HxD Hex Editor	Publisher:	Maël Hörz
Version:	2.5.0		
URL:	<a href="https://mh-nexus.de/en/hxd/">https://mh-nexus.de/en/hxd/</a>		

### Step-by-step methodology:

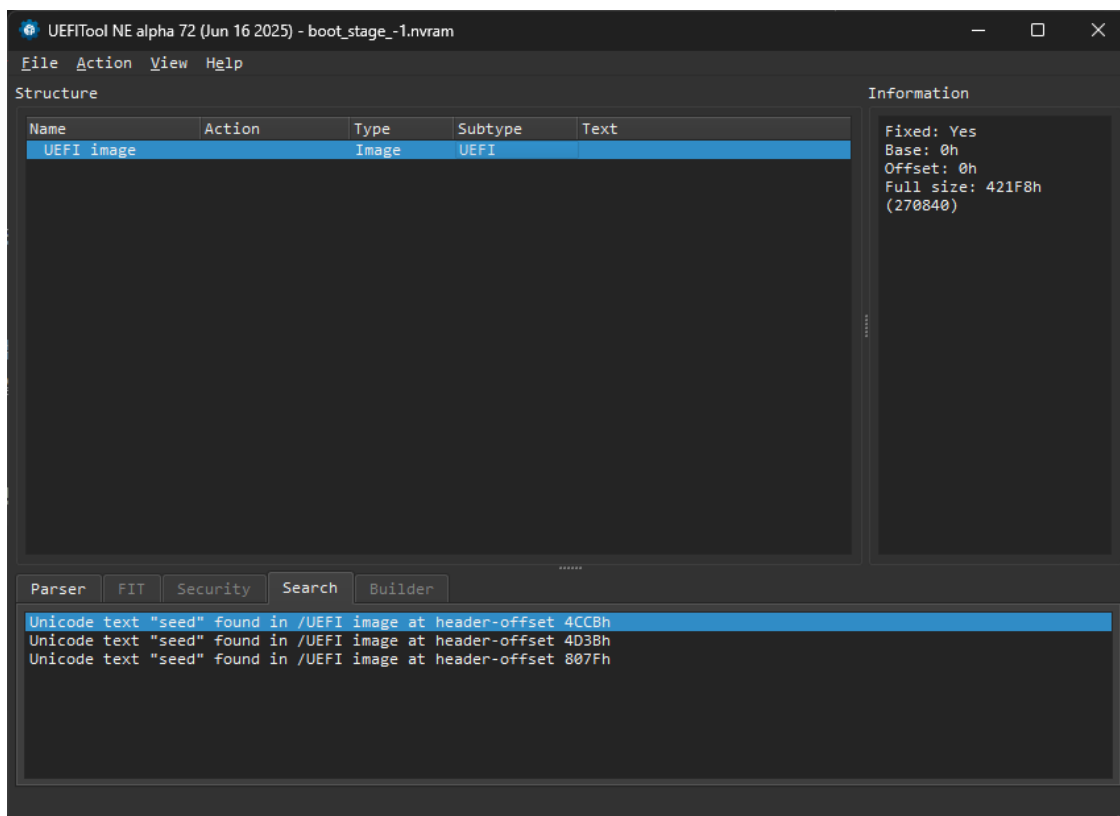
#### 1) VM 분석 환경 준비

이름	유형	압축된 크기	암호 사용	크기	비율
 boot_stage_-1	VMware Virtual Machine nonvolatile RAM	18KB	아니요	265KB	94%
 boot_stage_-1	VMware snapshot metadata	0KB	아니요	0KB	0%
 boot_stage_-1	VMware virtual machine configuration	2KB	아니요	4KB	67%
 boot_stage_-1	VMware Team Member	1KB	아니요	1KB	31%
 boot_stage_-1.vmdk	VMware.VirtualDisk	5,208,934KB	아니요	10,724,416KB	52%

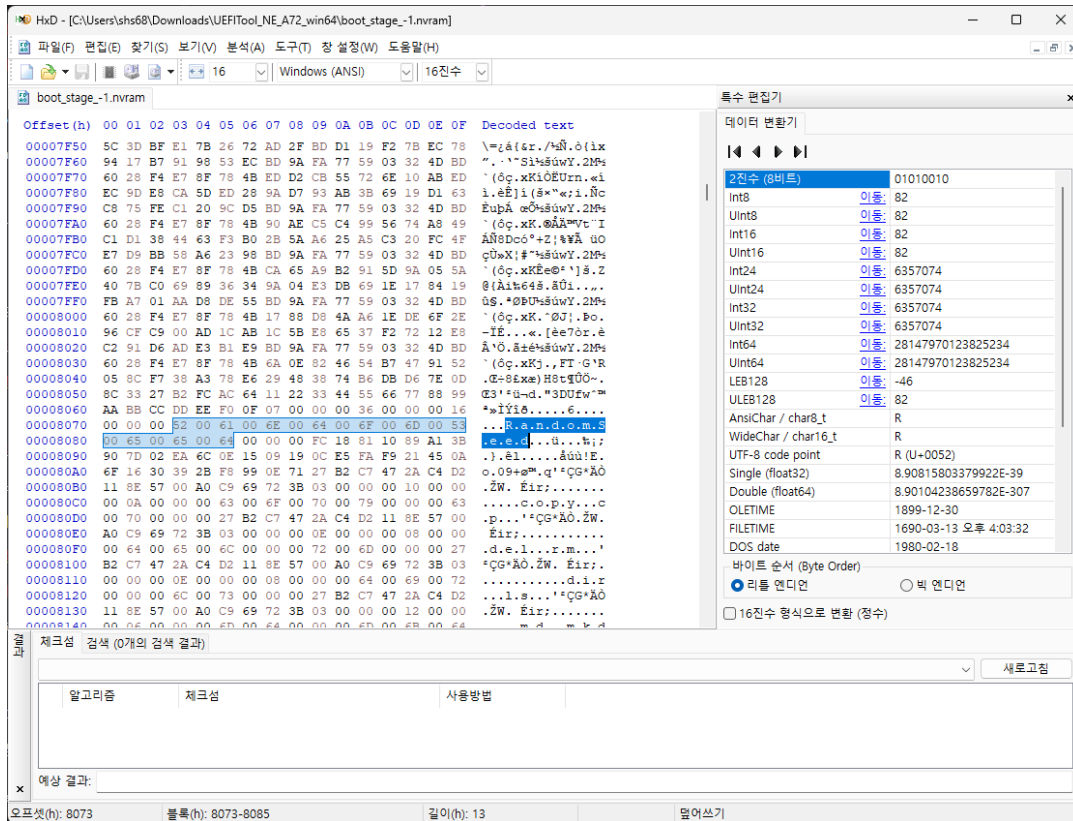
다운로드 받은 VM 아카이브 내에서 **.nvram 파일**(boot\_stage\_-1)을 확인하였다.  
이 파일은 VMware VM의 UEFI NVRAM 내용을 저장하는 영역으로, 물리 PC의 펌웨어 저장소와 동일한 역할을 한다.

## 2) RandomSeed 위치 탐색

UEFITool NE에서 .nvram 파일을 열고, 검색 기능으로 "seed" 문자열을 탐색하였다.  
그 결과 "RandomSeed" 변수명을 확인할 수 있었다.



## 3) Raw 데이터 추출



HxD로 .nvram 파일을 열어 "RandomSeed" (UTF-16 문자열) 바로 뒤의 구조를 확인하였다.

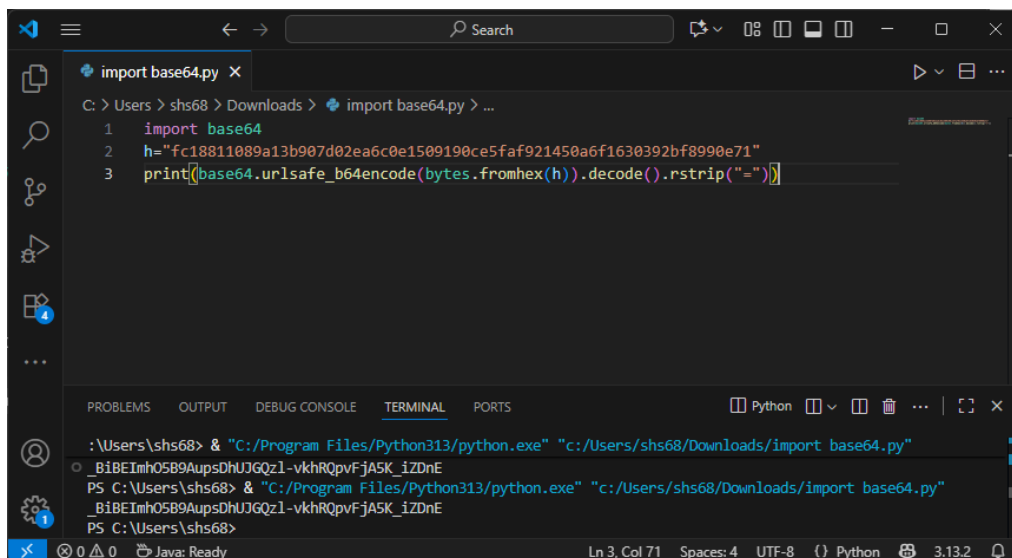
이름 이후 나타나는 32바이트 데이터가 실제 RandomSeed 값이었다.

- 추출된 RandomSeed (hex):

fc18811089a13b907d02ea6c0e1509190ce5faf921450a6f1630392bf8990e71

#### 4) Base64 URL-safe 인코딩

Python을 이용하여 추출된 RandomSeed 값을 Base64 URL-safe로 인코딩하였다.



The image shows a Visual Studio Code editor window with a Python file named 'import base64.py'. The script contains the following code:

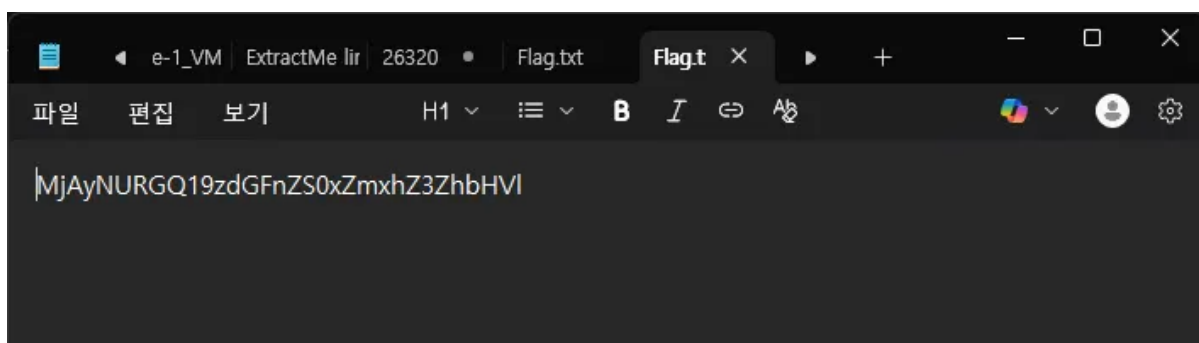
```
1 import base64
2 h="fc18811089a13b907d02ea6c0e1509190ce5faf921450a6f1630392bf8990e71"
3 print([base64.urlsafe_b64encode(bytes.fromhex(h)).decode().rstrip("=")])
```

The terminal at the bottom shows the command to run the script and its output:

```
:Users\shs68> & "C:/Program Files/Python313/python.exe" "c:/Users/shs68/Downloads/import base64.py"
_BiBEImhO5B9AupsDhUJGQzl-vkhRQpvFjA5K_iZDnE
PS C:\Users\shs68> & "C:/Program Files/Python313/python.exe" "c:/Users/shs68/Downloads/import base64.py"
_BiBEImhO5B9AupsDhUJGQzl-vkhRQpvFjA5K_iZDnE
PS C:\Users\shs68>
```

- 결과 비밀번호: `_BiBEImhO5B9AupsDhUJGQzl-vkhRQpvFjA5K_iZDnE`  
URL-safe 규칙: `+` → `-`, `/` → `_` 패딩 = 제거.

## 5) ZIP 파일 해제 및 FLAG 획득



7-Zip을 이용하여 해당 비밀번호를 입력해 Encrypted Zip File을 해제하였다.  
압축 해제 후 FLAG.txt를 열어 정답을 확인할 수 있었다.

- **FLAG** : `MjAyNURGQ19zdGFnZS0xZmxhZ3ZhbHVI`