



김우종



2019 해킹캠프 후기

WELCOME TO HACKINGCAMP

20th HackingCamp 후기

- . 자기소개서
- . 괴물들의 발표
- . 팀
- . 해캠CTF Writeup (흔적을 찾아라...)

자기소개서

자기소개서

생년월일: _____

자기소개서를 사실에 입각하여 직접 작성하였습니다.
자기소개서와 관련하여 내용 확인을 요청할 경우 협조할 것입니다.
고의적인 허위사실 기재, 대리 작성, 기타 부적절한 사실이 발견되는 경우
입학전형에서 지원자격을 제한받는
한후 귀교가 시행하는 입학전형에서 지원자격을 제한받는
추천서 및 추천서에 관한 정보의 열람 및 공개를 청구할 권리
및 공개를 청구하지 아니할 것입니다.
관련하여 추천인에게 고의적인 허위정보 제
의되는 경우 불합격, 합격 취소 또는
등의 불이익을 감
2017년

괴물들의 발표

발표는 2가지로 나뉘어짐

실무에서 사용하거나 직접 취약점을
찾았을 때 사용한 기술에 대한 발표

아니면 자신이 어떻게 공부해왔는지에
대한 발표

둘 다 도움이 됨



팀



(팀원들끼리 찍은 사진이 있는데 찾지 못해서 대체;)

CTF Writeup (흔적을 찾아라...)

흔적을 찾아라...

헐... ? 누군가가 장난을 쳐두었어 ! 3가지를 찾아줘 ! 플래그 포맷
HCAMP{삭제된 유저_메모프로그램에 저장된 숫자_부팅 시 조작된 프로세스명}

힌트

- [+] 삭제된 유저는 로그에서 찾을 수 있습니다.
- [+] 메모 프로그램은 *sticky note*입니다.
- [+] 부팅 시 로드 되는 화면은 레지스트리에서 관리합니다.

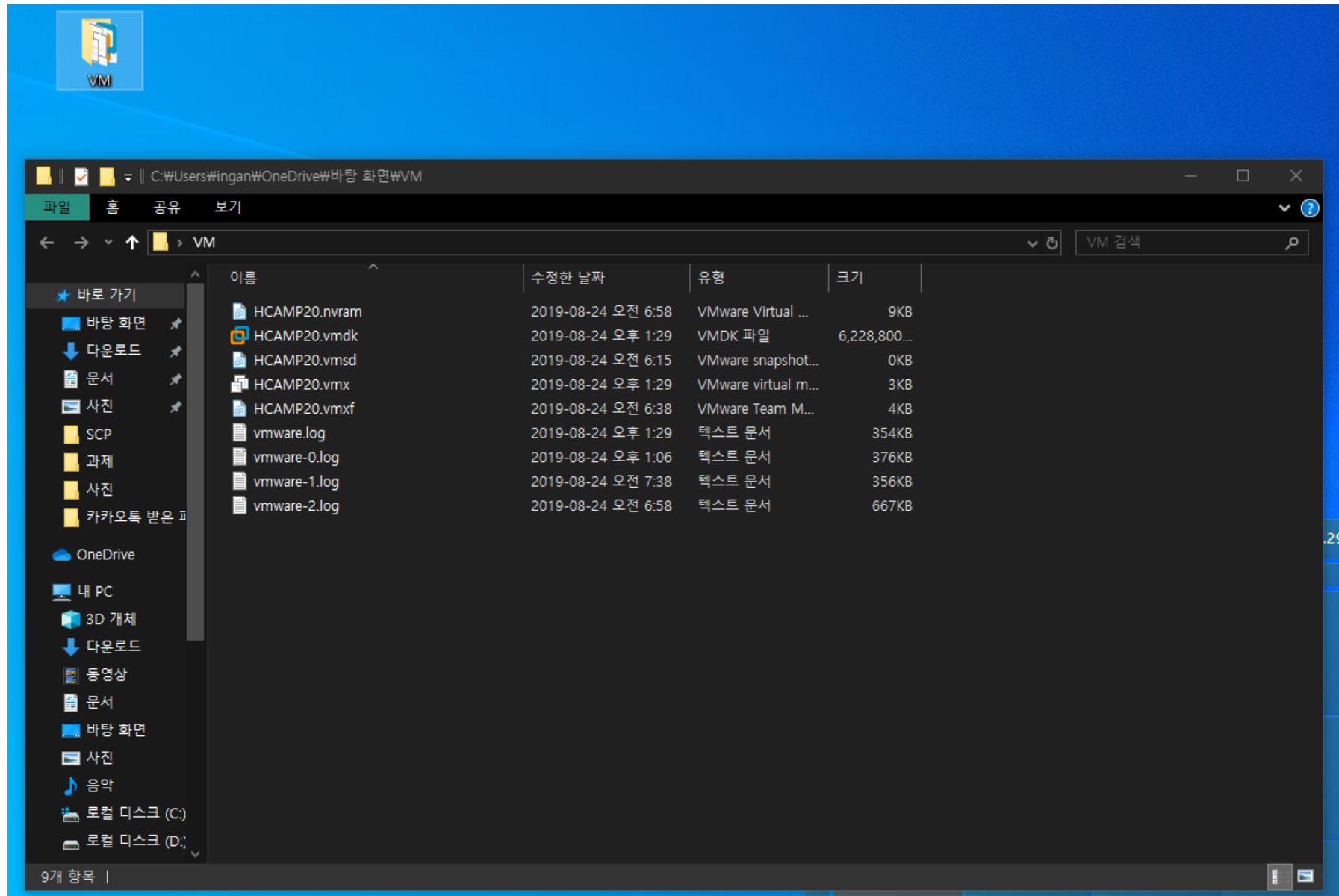
CTF Writeup (흔적을 찾아라...)



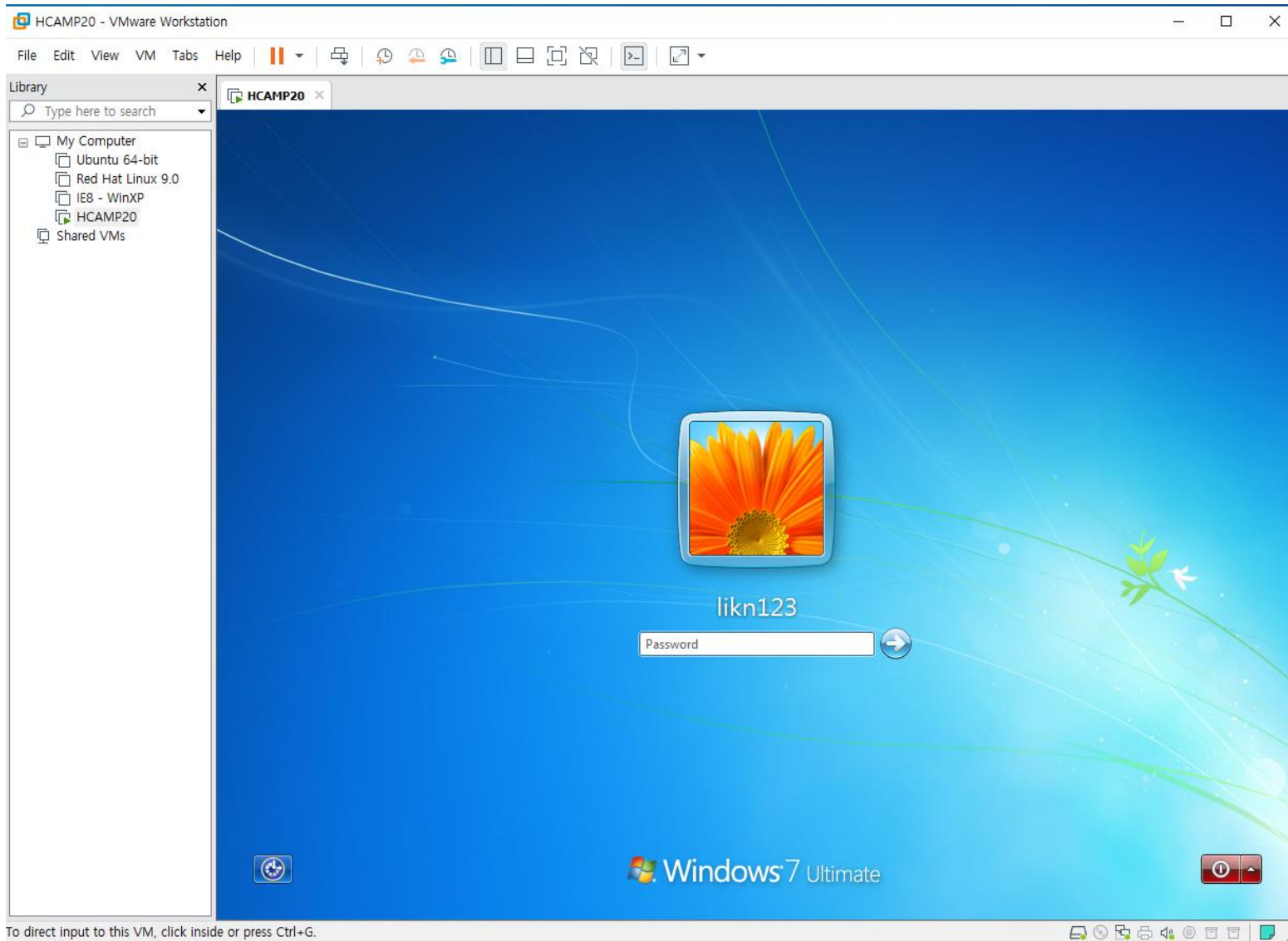
문제파일



압축해제



CTF Writeup (흔적을 찾아라...)

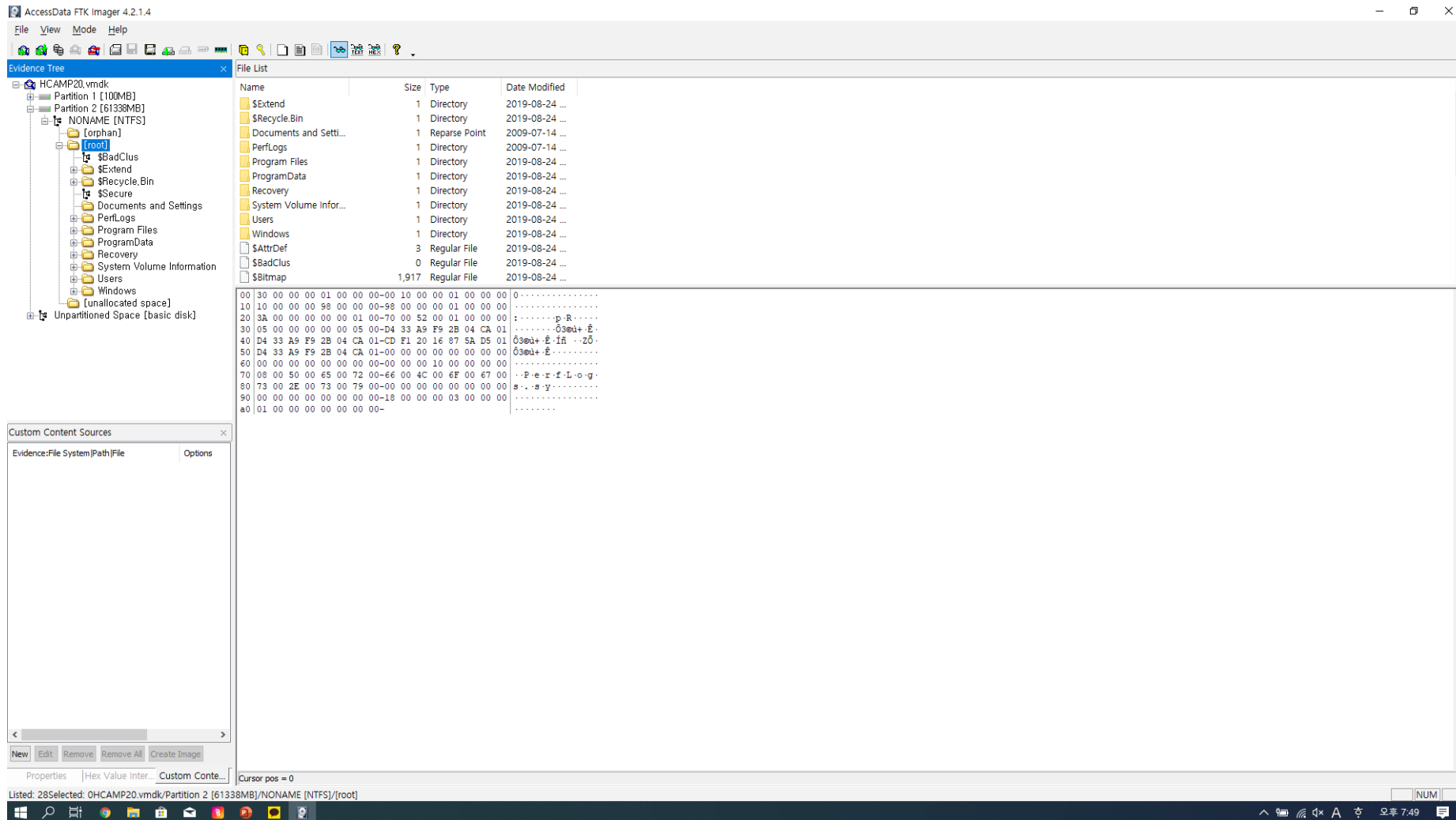


.vmx 파일이 있어서 vmware로 실행

운영체제 : windows 7

비밀번호가 걸려있음

CTF Writeup (흔적을 찾아라...)



Vmware 로 열었을 때
비밀번호가 걸려있어서
FTK Imager로 열어봄
(FTK Imager : 디스크
이미징, 파일시스템 분
석, 삭제파일 복구 등의
기능을 가진 툴)

몇시간 삽질 해봤지만
당시에 나로는 무언가를
찾을 수 없었음...

CTF Writeup (흔적을 찾아라...)

Google

windows 7 비밀번호 취약점

전체 뉴스 이미지 동영상 쇼핑 더보기 설정 도구

검색결과 약 72,700개 (0.45초)

동영상

보안핫점을 이용해 아무것도없이 초간단 비밀번호 해킹!
WINDOW 비밀번호기
7:33 준비물 없음

원도우7 보안핫점을 이용해 아무것도없이 초간단 비밀번호 해킹 ...

freeZINO
YouTube - 2017. 7. 6.

윈도우7 암호풀기
9:58 준비물 X 쉽고 간단하게 해킹
보안핫점이용

원도우7 보안핫점으로 준비물없이, 더 간단하게 쉽게 비밀번호 ...

freeZINO
YouTube - 2018. 1. 3.

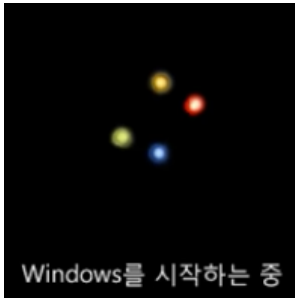
윈도우 7 암호깨지
Windows
비번 잊어버렸을때!!!
5:54

[컴맹탈출] 윈도우7 암호 깨기~ (암호 잊어 버렸을때, 포맷만이 답 ...

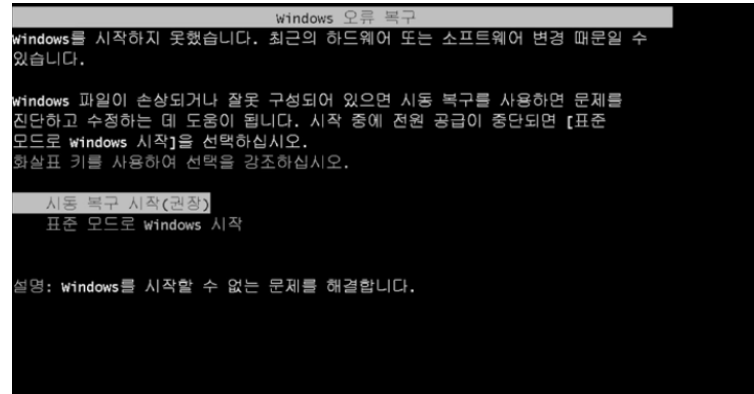
DRONEWORLD드론월드
YouTube - 2016. 4. 16.

CTF Writeup (흔적을 찾아라...)

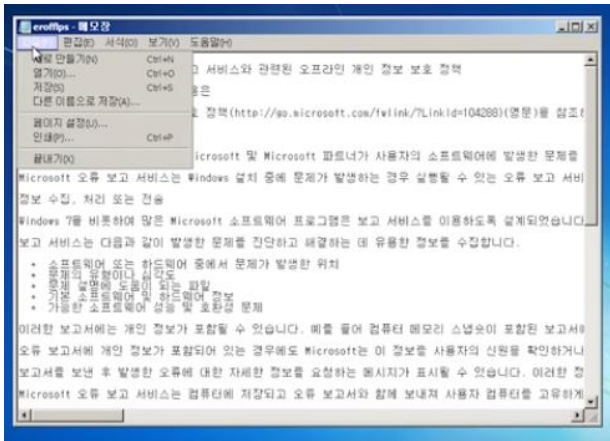
Windows 7 로그인 비밀번호 취약점



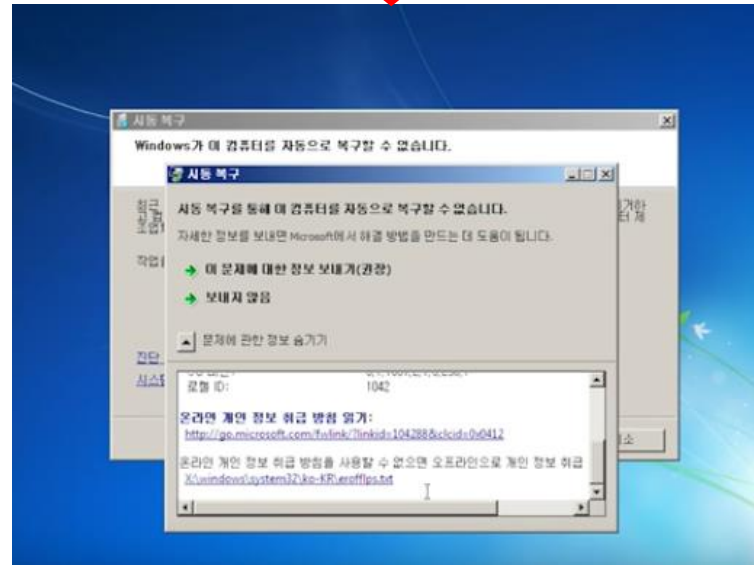
이 그림이 나오면
Windows 강제종료



다시 부팅한 뒤
시동복구 모드로 시작



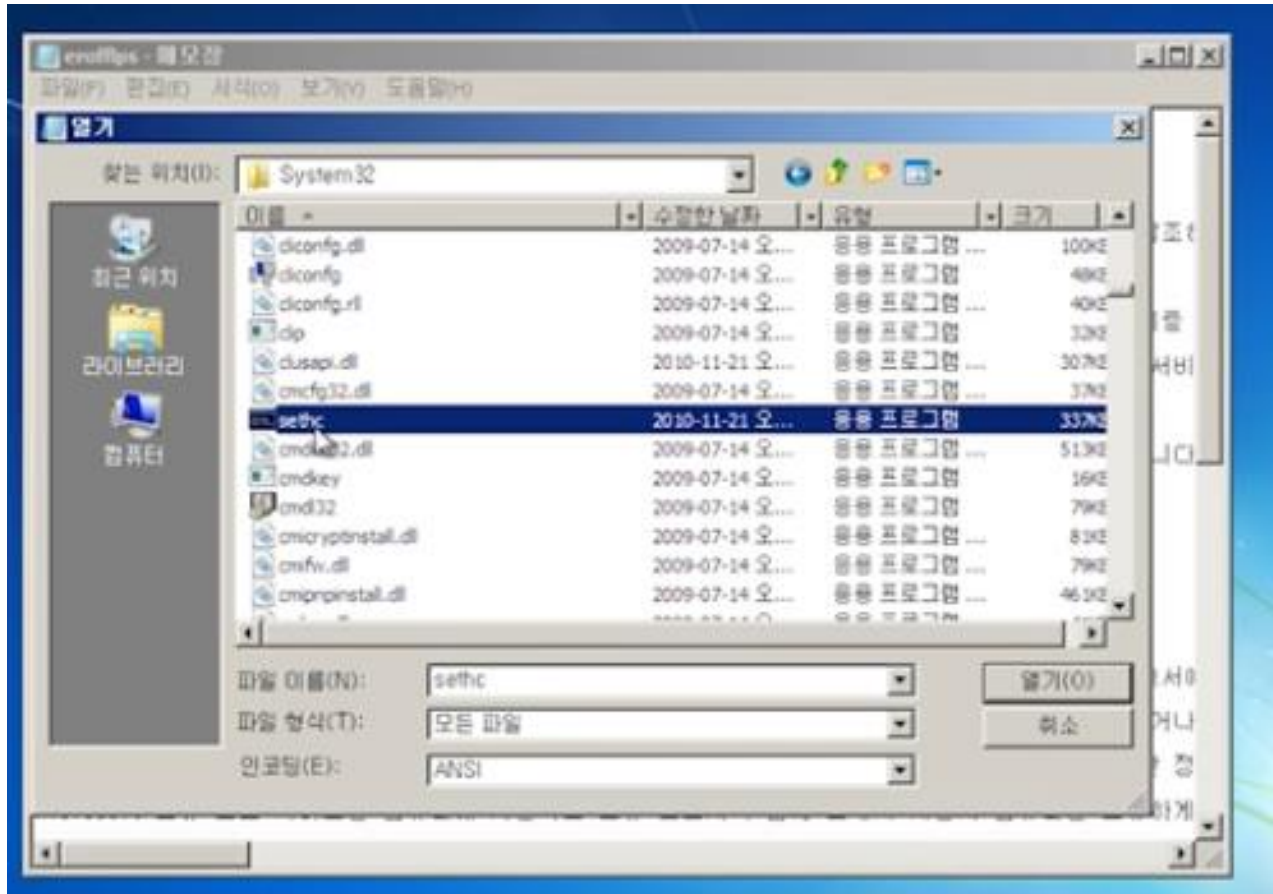
메모장을 다른이름으로
저장을 누르면 파일들을
볼수가 있음



시동 복구가 시작됨

시동복구가 끝나면 문제
에 관한 정보에서 txt파
일을 열 수 있음

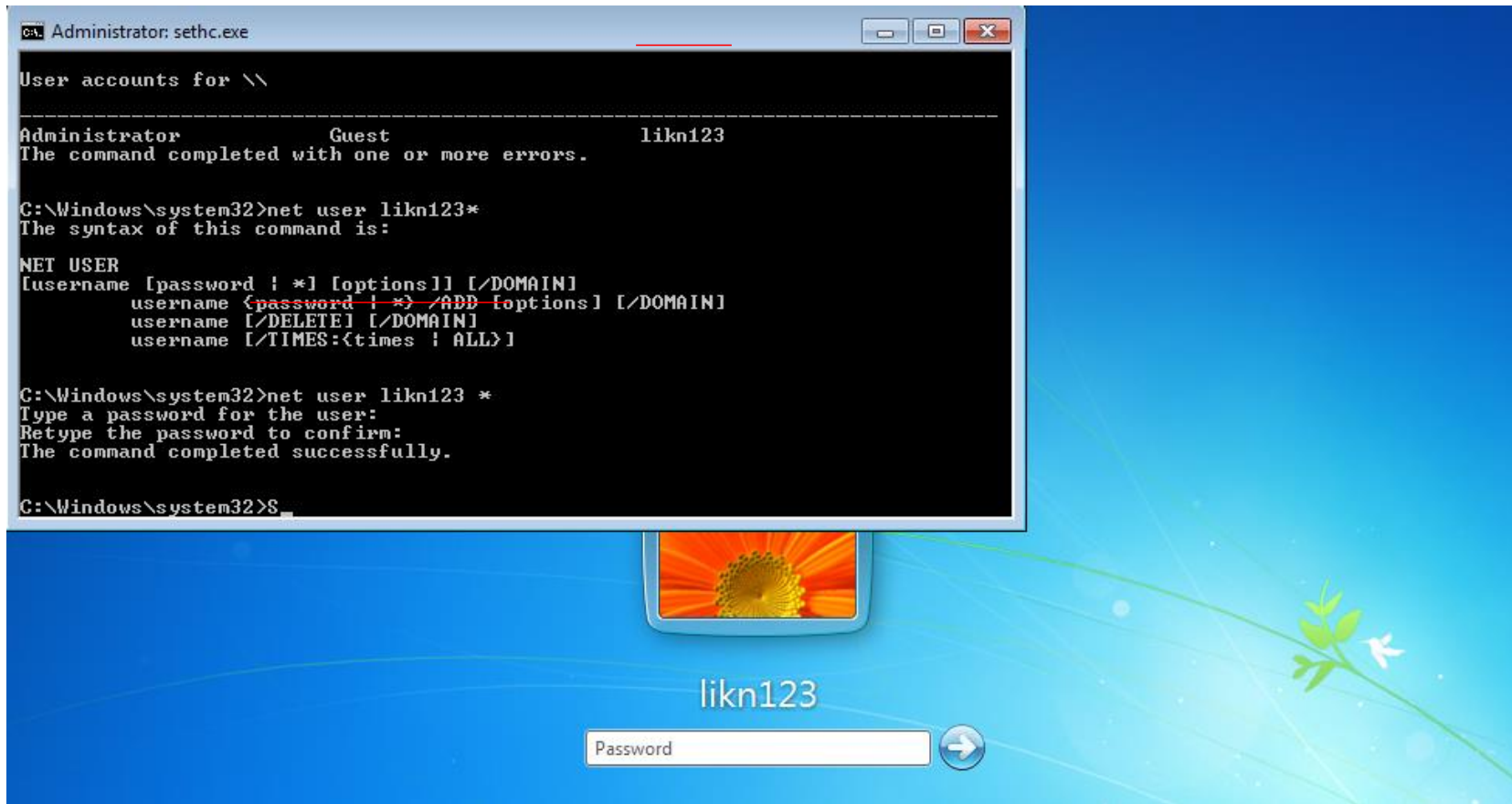
CTF Writeup (흔적을 찾아라...)



System32 파일을 찾아서
cmd를 sethc로 sethc를
sethc1으로 이름을 바꾼다.
(sethc : shift키를 연속으로
누르면 나오는 고정키 설정
(?))

바꾸고 난 뒤 종료

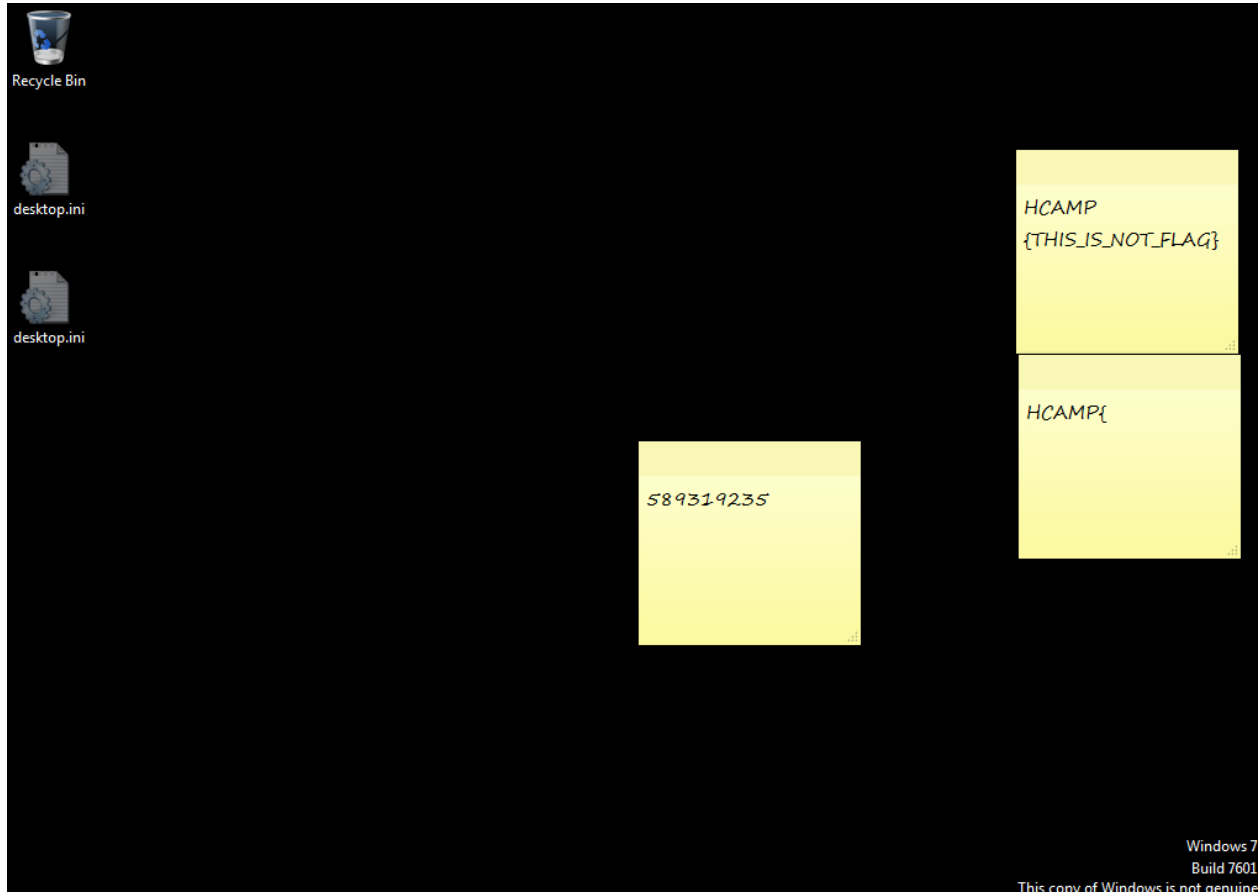
CTF Writeup (흔적을 찾아라...)



1. Shift 연속으로 누르면 고정키 대신 cmd창이 열림

2. net user user명 *로 패스워드를 재설정 할 수 있음

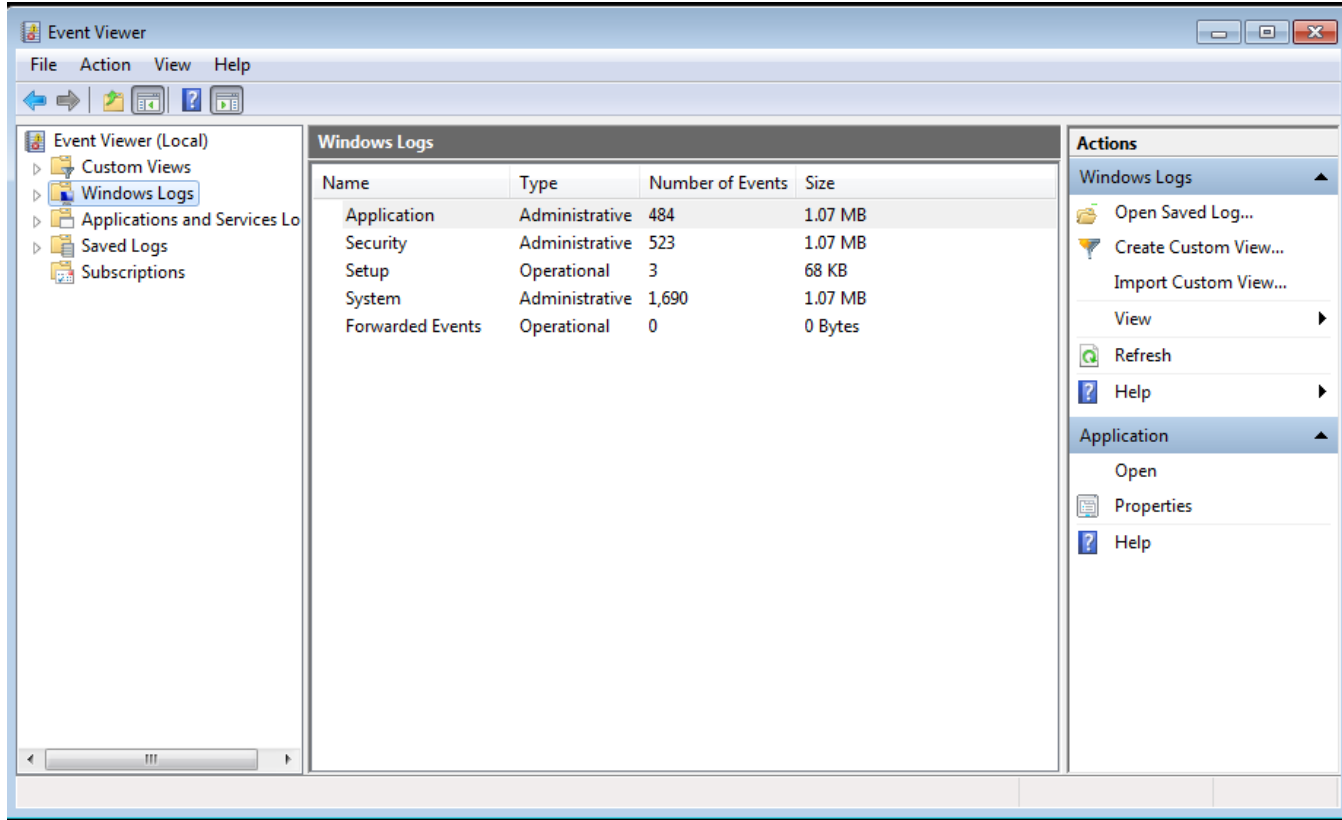
CTF Writeup (흔적을 찾아라...)



Sticky note 에 번호가 있음
Flag 형식에 가운데 값을 찾게 됨

Flag 형식 : HCAMP{삭제된 유저_메모프로그램에 저장된 숫자_부팅 시 조작된 프로세스명}

CTF Writeup (흔적을 찾아라...)

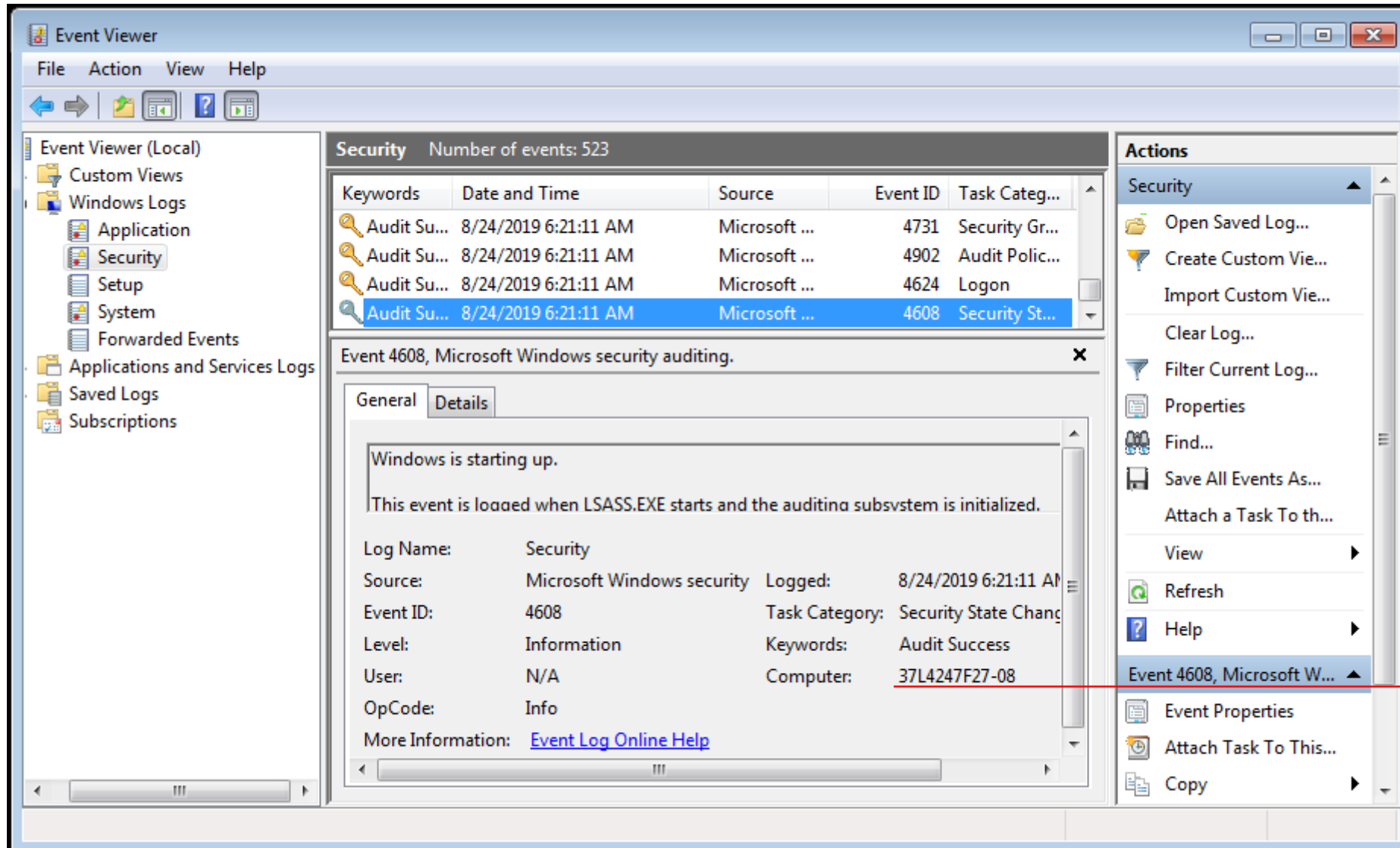


삭제된 유저명 찾는법

1. Windows 로고 + R 키로 실행창 켜기
2. Eventvwr.msc 명령어로 이벤트 뷰어 열기
3. Windows Logs 목록 안 Security 목록에서 삭제된 유저명 찾기

이벤트 뷰어에는 서비스 오류와, 응용 프로그램을 설치 시 발생하는 오류 그리고 하드웨어 장치 및 드라이버에 대한 오류 등을 모두 남깁니다.

CTF Writeup (흔적을 찾아라...)



liken123 과 Administrator
를 제외한 다른 유저명이 있음

CTF Writeup (흔적을 찾아라...)

```
C:\Windows\system32\sethc.exe
C:\Users\likn123>tasklist

Image Name                      PID Session Name        Session#    Mem Usage
=====
System Idle Process             0 Services             0             24 K
System                          4 Services             0             552 K
smss.exe                        272 Services             0             848 K
csrss.exe                       364 Services             0            2,992 K
wininit.exe                     444 Services             0            3,304 K
csrss.exe                       452 Console              1            6,856 K
winlogon.exe                    516 Console              1            4,652 K
services.exe                    524 Services             0            6,816 K
lsass.exe                       560 Services             0            6,440 K
lsass.exe                       568 Services             0            2,996 K
svchost.exe                     680 Services             0            7,180 K
vmacthlp.exe                    740 Services             0            3,456 K
svchost.exe                     784 Services             0            5,876 K
svchost.exe                     856 Services             0           10,816 K
svchost.exe                     916 Services             0            9,256 K
svchost.exe                     948 Services             0           20,228 K
audiodg.exe                    1028 Services             0           13,964 K
svchost.exe                    1096 Services             0            8,176 K
svchost.exe                    1196 Services             0            9,172 K
spoolsv.exe                    1320 Services             0            8,388 K
svchost.exe                    1356 Services             0           10,100 K
svchost.exe                    1524 Services             0            6,756 K
UGAuthService.exe              1612 Services             0            6,876 K
vmtoolsd.exe                   1684 Services             0           12,928 K
taskhost.exe                   1804 Console              1            5,220 K
sppsvc.exe                     212 Services             0            7,056 K
svchost.exe                     564 Services             0            3,540 K
dllhost.exe                    1068 Services             0            8,464 K
dllhost.exe                    1756 Services             0            8,700 K
msdtc.exe                      2064 Services             0            6,244 K
WmiPrvSE.exe                   2180 Services             0            7,048 K
USSVC.exe                      2304 Services             0            5,056 K
userinit.exe                   2384 Console              1            2,676 K
dwm.exe                         2392 Console              1            4,296 K
explorer.exe                   2416 Console              1           26,412 K
vmtoolsd.exe                   2492 Console              1           16,580 K
StikyNot.exe                   2512 Console              1            8,744 K
SearchIndexer.exe              2636 Services             0            8,644 K
SearchProtocolHost.exe         2800 Services             0            6,012 K
SearchFilterHost.exe           2820 Services             0            3,544 K
WmiPrvSE.exe                   3000 Services             0           20,960 K
mobsync.exe                    3036 Console              1            6,092 K
WmiApSrv.exe                   3096 Services             0            4,456 K
sethc.exe                      3132 Console              1            2,476 K
conhost.exe                    3140 Console              1            3,960 K
tasklist.exe                   3160 Console              1            4,420 K

C:\Users\likn123>SS_
```

그리고 다음으로

부팅시 조작된 프로세스를 찾기 위해 tasklist 명령어 사용

이 당시에는 부팅시 조작된 프로세스라고 하여 무작위 대입 공격 식으로 tasklist에 있는 목록 전부 다 씀

-> HCAMP{37L4247F27-08_539319235_tasklist목록}

-> 결과는 모조리 틀림 ㅎㅎ...

CTF Writeup (흔적을 찾아라...)

한참을 헤매다가 힌트를 투척
하셔서 받아먹음

힌트 : [+] 부팅 시 로드 되는
화면은 레지스트리에서 관리
합니다.

그리고 따로 방으로 찾아오서
서 악성코드 형식(?)으로 플
래그를 넣으셨다 했음

-> 부팅시 작동하는
악성코드가 무엇이 있나
구글링

(당시엔 옆 사이트에서 찾지
않았었습니다,
옆 사이트는 특강때 강사님이
알려주신 사이트
: MITRE ATT&ACK)

Registry Run Keys / Startup Folder

Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. ^[1]

These programs will be executed under the context of the user and will have the account's associated permissions level.

The following run keys are created by default on Windows systems:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
```

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

The `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx` is also available but is not created by default on Windows Vista and newer. Registry run key entries can reference programs directly or list them as a dependency. ^[2] For example, it is possible to load a DLL at logon using a "Depend" key with RunOnceEx: `reg add`

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 /d "C:\temp\evil[.]dll" [3]
```

The following Registry keys can be used to set startup folder items for persistence:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
```

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
```

Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use [Masquerading](#) to make the Registry entries look as if they are associated with legitimate programs.




CTF Writeup (흔적을 찾아라...)

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
```

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

Name	Type	Data
 (Default)	REG_SZ	(value not set)
 shell	REG_SZ	h33cxkqi1531
 VMware User Pr...	REG_SZ	"C:\Program Files\VMware\VMware Tools\vmtool...

위 경로 중 한
곳에 shell로
된 플래그가
있었음

CTF Writeup (흔적을 찾아라...)

아래 형식대로 플래그를 입력해 보았지만 정답이 아니었다...

이 때는 이게 플래그가 아닌줄 알았다, 그래서 다른 경로를 열심히 찾아봄

그러다가 모든 수단을 동원해도 플래그를 찾지 못해서 다른 부분을 찾아보기로 했다,
그리고...

Computer: 37L4247F27-08

589319235

ab shell

REG_SZ

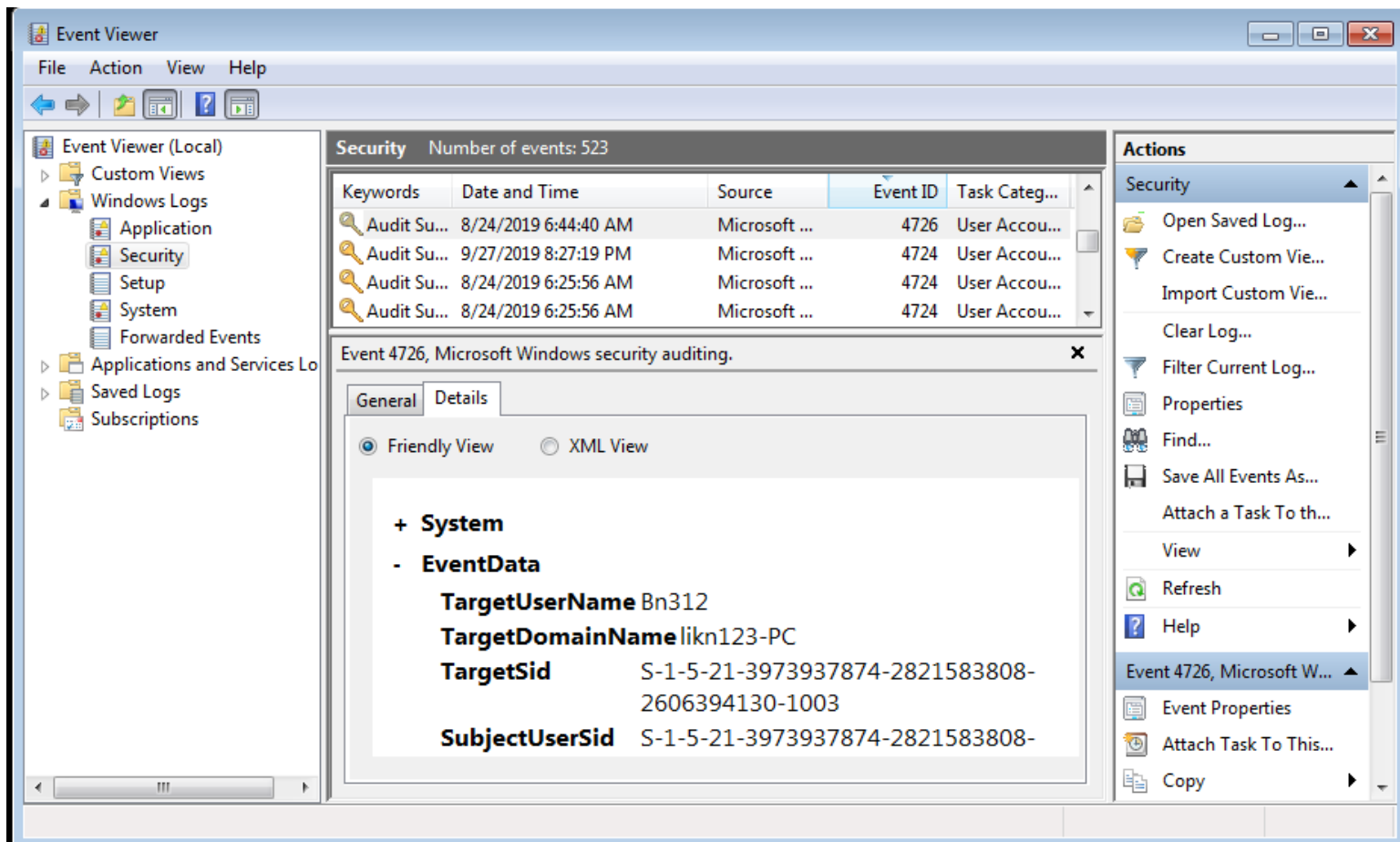
h33cxkqi1531

CTF Writeup (흔적을 찾아라...)

Computer:

37L4247F27-08

이 친구(삭제된 유저 명)가 잘못되어 있었다.....



구글링을 한 결과 유저의 삭제로그
이벤트 ID는 4726

Ctrl + F 를 눌러 4726을 검사하면
옆에 창이 뜬다...

삭제된 유저명은 Bn312였던 것...

CTF Writeup (흔적을 찾아라...)

따라서 플래그는

HCAMP{Bn3 12_5893 19235_n33cxRqi1531}!!!



다음날 출제자가 자신의 의도한 대로 푼 사람이 없다
면서 슬퍼했음...

나중에 와서 출제자가 알려준 의도대로 푼 풀이 방법

삭제된 유저는 로그(이벤트 로그)에서 찾을 수 있음
(root%\Windows\System32\winevt\Logs\Security.evtx)

유저 관련 이벤트 로그는 Security.evtx
FTK Imager로 해당 로그파일을 추출해서 이벤트 뷰어로 봄

Ctrl + F 로 4726 검색

로그 내용에서 '계정 이름: Bn3 12'을 찾을 수 있다.

이벤트 4726, Microsoft Windows security auditing.

일반 자세히

◎ 간단히 보기(N)

○ XML 보기(X)

+ System

- **EventData**

TargetUserName Bn312

TargetDomainNamelikn123-PC

TargetSid S-1-5-21-3973937874-2821583808-2606394130-1003














SubjectUserSid S-1-5-21-3973937874-2821583808-2606394130-1001

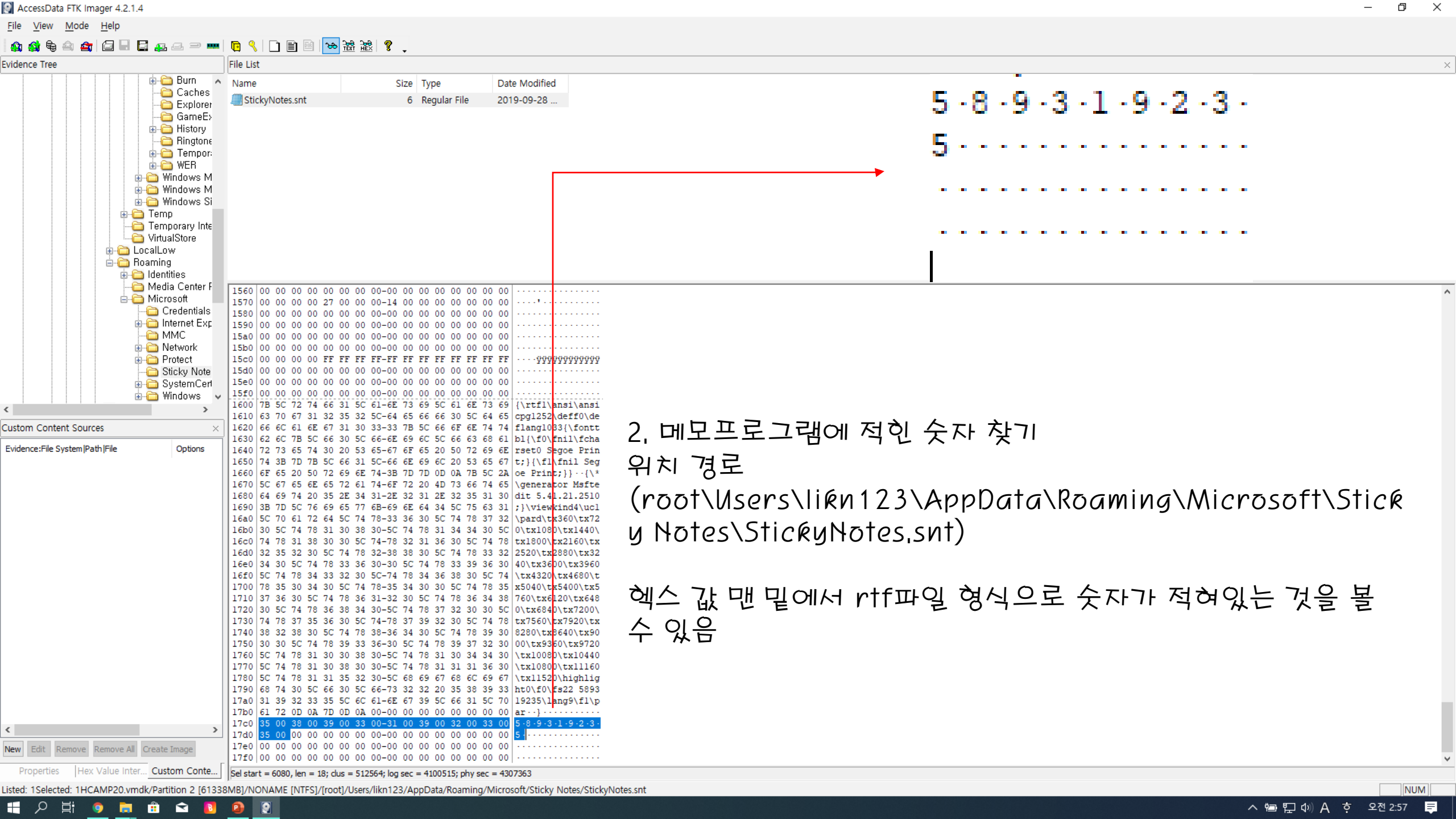
SubjectUserName likn123

SubjectDomainName likn123-PC

SubjectLogonId 0x425e9

PrivilegeList

File List				
Name	Size	Type	Date Modified	
 Microsoft-Windows-...	68	Regular File	2019-09-28 ...	
 Microsoft-Windows-...	68	Regular File	2019-09-28 ...	
 Microsoft-Windows-...	68	Regular File	2019-09-28 ...	
 Microsoft-Windows-...	68	Regular File	2019-09-28 ...	
 Microsoft-Windows-...	68	Regular File	2019-09-28 ...	
 Microsoft-Windows-...	68	Regular File	2019-09-28 ...	
 Microsoft-Windows-...	68	Regular File	2019-09-28 ...	
 Security.evtx	1,092	Regular File	2019-09-28 ...	
 Security.evtx.FileSlack	704	File Slack		
 Setup.evtx	68	Regular File	2019-08-24 ...	
 System.evtx	1,092	Regular File	2019-09-28 ...	
 System.evtx.FileSlack	398	File Slack		
 Windows PowerShell....	68	Regular File	2019-08-24 ...	



2. 메모프로그램에 적힌 숫자 찾기
위치 경로

(root\Users\liken123\AppData\Roaming\Microsoft\Sticky Notes\StickyNotes.snt)

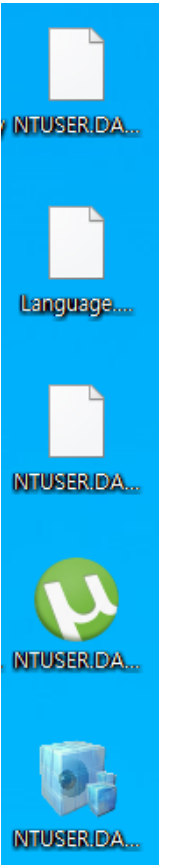
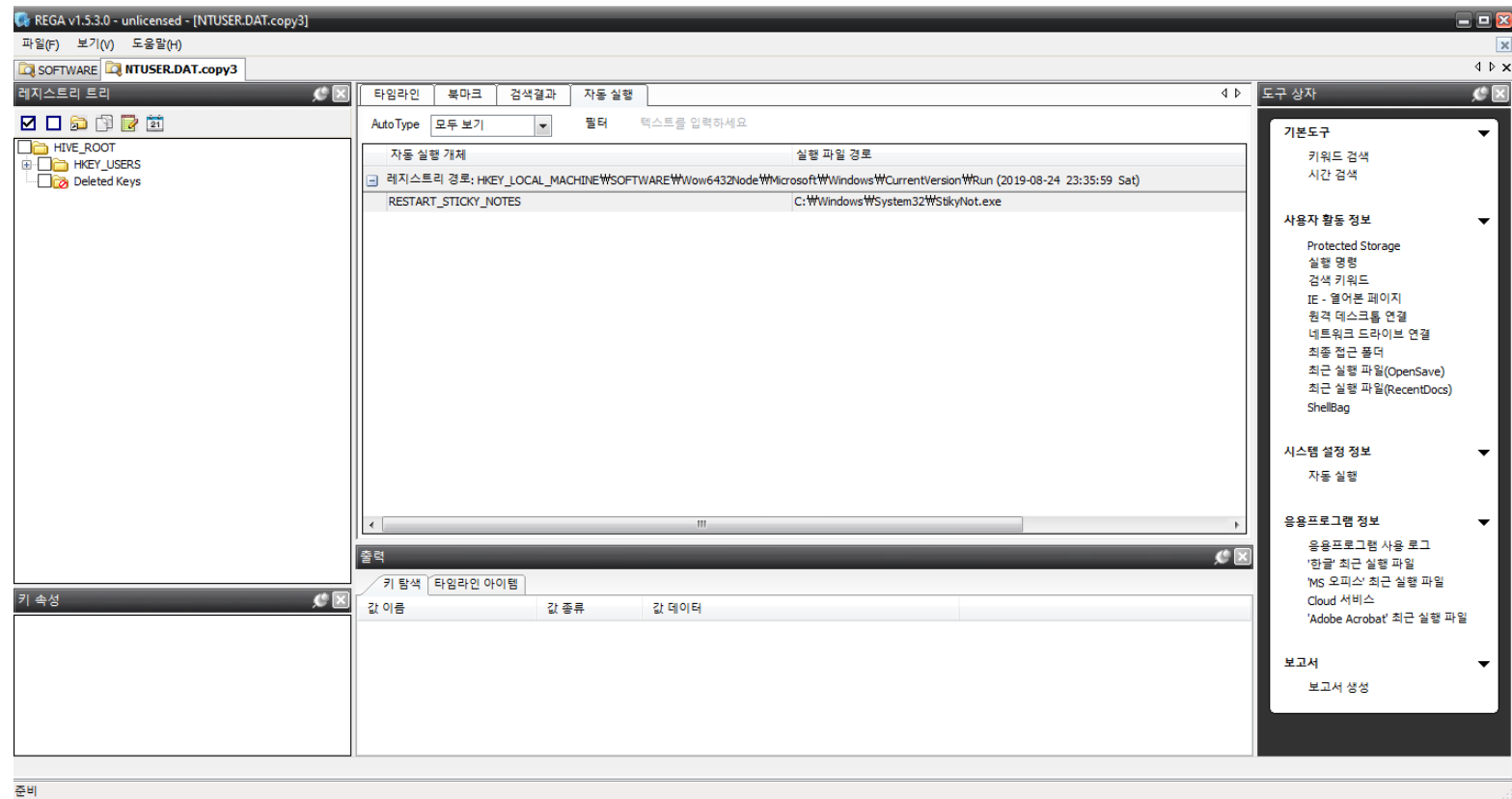
hex 값 맨 밑에서 rtf파일 형식으로 숫자가 적혀있는 것을 볼 수 있음

CTF Writeup (흔적을 찾아라...)

마지막으로 윈도우 실행시 동작된 프로세스만 찾으면 되는데 여기서 삽질 또 삽질 계속 삽질!!!!

1. 처음에는 레지스트리들은 ntuser.dat에서 관리한다고 하여 ntuser.dat을 추출시키고 reg라는 프로그램으로 레지스트리 분석

하지만 아무리 찾아봐도
플래그가 있어야 할 경
로(자동 실행)에는
stickynote 밖에 실행
되지 않음

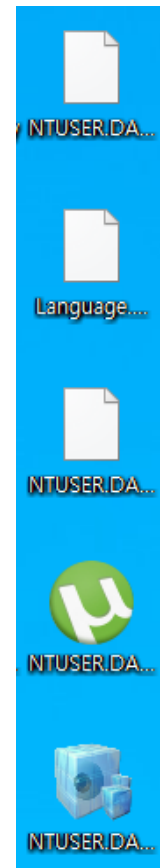
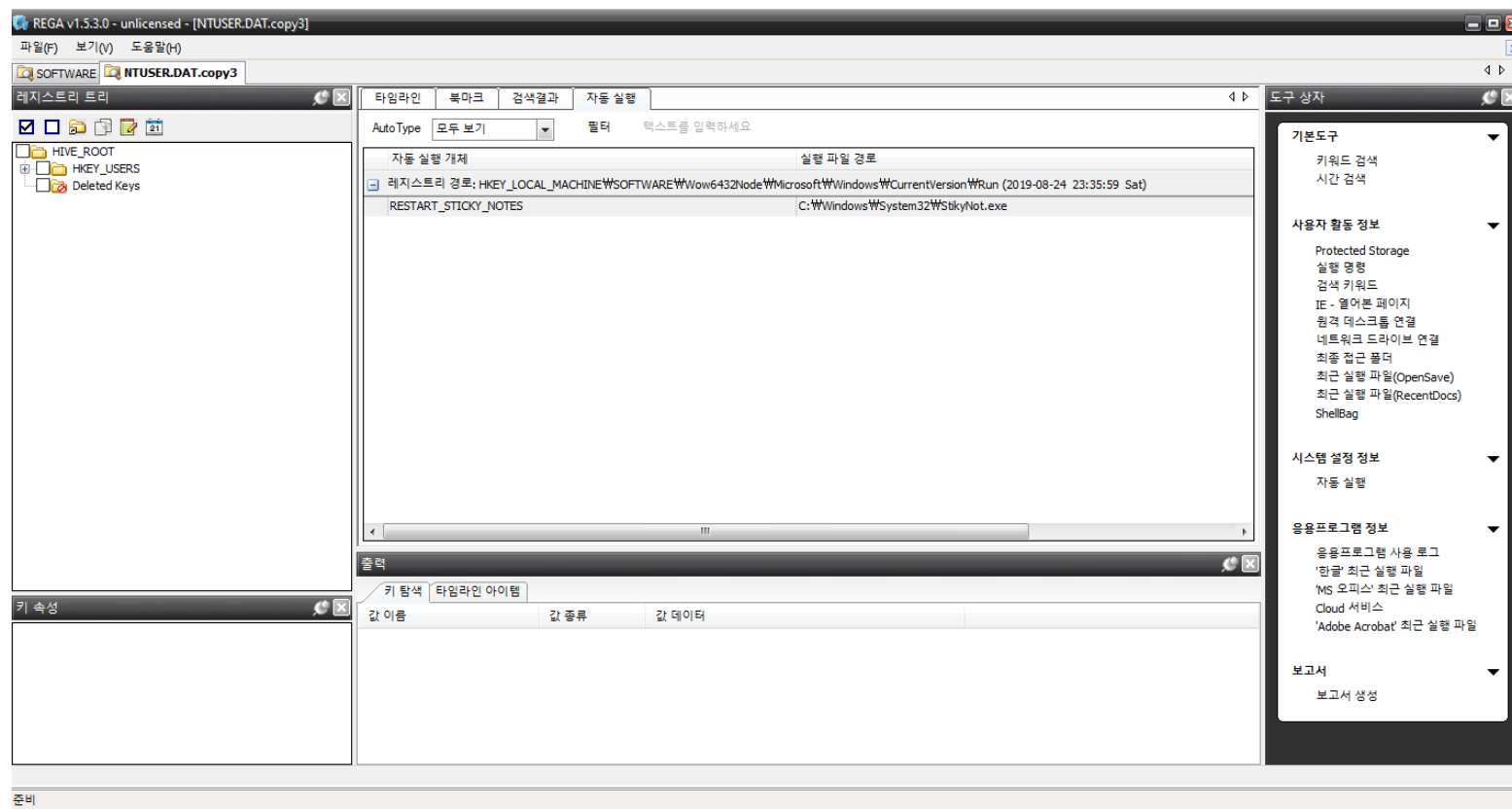


CTF Writeup (흔적을 찾아라...)

마지막으로 윈도우 실행시 동작된 프로세스만 찾으면 되는데 여기서 삽질 또 삽질 계속 삽질!!!!

2. 다음으로는 vmware로 windows를 실행시킨뒤 일시중지로 멈춘뒤 ntuser.dat 파일 추출후 rega로 분석

마찬가지로 아무리 찾아봐도 플래그가 있어야 할 경로(자동 실행)에는 stickynote 밖에 실행되지 않음



CTF Writeup (흔적을 찾아라...)

마지막으로 윈도우 실행시 동작된 프로세스만 찾으면 되는데 여기서 삽질 또 삽질 계속 삽질!!!!

3. 그러다가 이상한 점 발견

내가 찾는 경로는 HKEY_LOCAL_MACHINE 인데 NTUSER.DAT에는 HKEY_USERS 하이브 리스트가 들어 있다는것을 깨달음

4. 그래서 HKEY_LOCAL_MACHINE 경로를 구글링 -

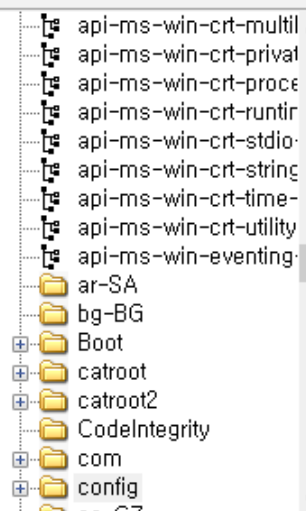
> %root%\Windows\system32\config\SOFTWARE

(SOFTWARE 파일을 추출 해야 HLM이 나오는 걸 알게됨)

5. FTK Imager로 SOFTWARE파일 추출

6. 이렇게 해서 나온 SOFTWARE를 REGA로 분석 -> 자동실행란에 shell을 찾을 수 있음

Evidence Tree



Custom Content Sources

Evidence:File System|Path|File

Options

New Edit Remove Remove All Create Image

Properties Hex Value Inter... Custom Conte...

File List

Name	Size	Type	Date Modified
SECURITY.LOG1		\$I30 INDX Entry	
SECURITY.LOG2	0	Regular File	2009-07-14 ...
SOFTWARE	23,552	Regular File	2019-09-28 ...
SOFTWARE.FileSlack	4	File Slack	
SOFTWARE.LOG	1	Regular File	2010-11-21 ...
SOFTWARE.LOG1	256	Regular File	2019-09-28 ...
SOFTWARE.LOG1.File...	256	File Slack	
SOFTWARE.LOG2	0	Regular File	2009-07-14 ...
SYSTEM	12,544	Regular File	2019-09-28 ...
SYSTEM.FileSlack	200	File Slack	
SYSTEM.LOG	1	Regular File	2010-11-21 ...
SYSTEM.LOG1	256	Regular File	2019-09-28 ...
SYSTEM.LOG1.FileSlack	3,840	File Slack	

5. FTK Imager로 SOFTWARE파일 추출

파일 경로
(%root%\Windows\system32\config\SOFTWARE)

```
00000000 72 65 67 66 1E 02 00 00-1E 02 00 00 EA 63 01 0D regf-----êc--
00000010 EC 75 D5 01 01 00 00 00-05 00 00 00 00 00 00 00 iu0-----
00000020 01 00 00 00 20 00 00 00-00 E0 6F 01 01 00 00 00 ....-...ão....
00000030 65 00 6D 00 52 00 6F 00-6F 00 74 00 5C 00 53 00 e-m-R-o-o-t-\-S-
00000040 79 00 73 00 74 00 65 00-6D 00 33 00 32 00 5C 00 y-s-t-e-m-3-2-\-
00000050 43 00 6F 00 6E 00 66 00-69 00 67 00 5C 00 53 00 C-o-n-f-i-g-\-S-
00000060 4F 00 46 00 54 00 57 00-41 00 52 00 45 00 00 00 O-F-T-W-A-R-E-
00000070 FC D2 CE 6C 01 6E DE 11-8B ED 00 1E 0B CD 18 24 u0il-nP-i-i-i-
00000080 FC D2 CE 6C 01 6E DE 11-8B ED 00 1E 0B CD 18 24 u0il-nP-i-i-i-
00000090 00 00 00 00 FD D2 CE 6C-01 6E DE 11 8B ED 00 1E ...y0il-nP-i-i-
000000a0 0B CD 18 24 72 6D 74 6D-00 00 00 00 00 00 00 00 -i-5rmtm-----
000000b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
000000c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
000000d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
000000e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
000000f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
00001000 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
00001100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
00001200 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
00001300 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
00001400 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
```

Cursor pos = 0; dus = 1396122; log sec = 11168976; phy sec = 11375824



- [-] GPU Pipeline
- [-] HTML Help
- [-] IdentityCRL
- [-] IdentityStore
- [-] IMAPI
- [-] IMEJP
- [-] IMEKR
- [-] IMETC
- [-] Internet Account Manager
- [-] Internet Domains
- [-] Internet Explorer
- [-] IsoBurn
- [-] Jet
- [-] MediaCenterPeripheral
- [-] MediaPlayer
- [-] MessengerService
- [-] MigWiz
- [-] MMC
- [-] Mobile
- [-] MpSigStub
- [-] MSBuild
- [-] MSDE
- [-] MSDTC
- [-] MSF
- [-] MS Licensing
- [-] MSN Apps

[-] 일반	
최종기록시각 (UTC+09:00)	2019-09-28 18:11:44 Sat
[-] 속성	
하위키 개수	132
값 개수	0

자동 실행 개체	실행 파일 경로
[-] 레지스트리 경로: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell (2019-09-28 20:01:12 Sat)	
explorer.exe	explorer.exe
[-] 레지스트리 경로: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit (2019-09-28 20:01:12 Sat)	
C:\Windows\system32\Userinit.exe	C:\Windows\system32\Userinit.exe
[-] 레지스트리 경로: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run (2019-08-25 05:27:27 Sun)	
shell	h33cxkj1531
VMware User Process	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe -n vmusr

6. 이렇게 해서 나온 SOFTWARE를 REGA로 분석 -> 자동실행란
에 shell을 찾을 수 있음

키워드 검색
시간 검색

윈도우 설치 정보

자동 실행

설치된 응용프로그램

보고서 생성



김우종

질문 받아요



WELCOME TO HACKINGCAMP