2021 가을학기 성신여자대학교

디지털포렌식실습 (LB002800)

디지털포렌식실습 과제 (Assignment #1)

성명: 이혜린

학번: 20190937

문제를 잘 읽고, 문제에서 요구하는 질문에 대한 답변을 작성하여 제출하세요.

문제 관련 질문이 있을 경우, 이메일을 통해 질문을 작성하시면 됩니다.

(이 페이지는 채점 시 활용할 것이며 별도 추가하여 제출하시지 않으셔도 됩니다. 답안 작성시 문제 내용은 모두 제거하고 답에 해당 하는 부분만 쓰셔도 됩니다.)

답변의 경우, 표지와 문제 내용을 제외하고 최대 10페이지 이내로 작성하시길 바랍니다 (초과 시 초과 page 당 감점 있을 예정).

Total / 30

Name: 이혜린 Student ID: 20190937

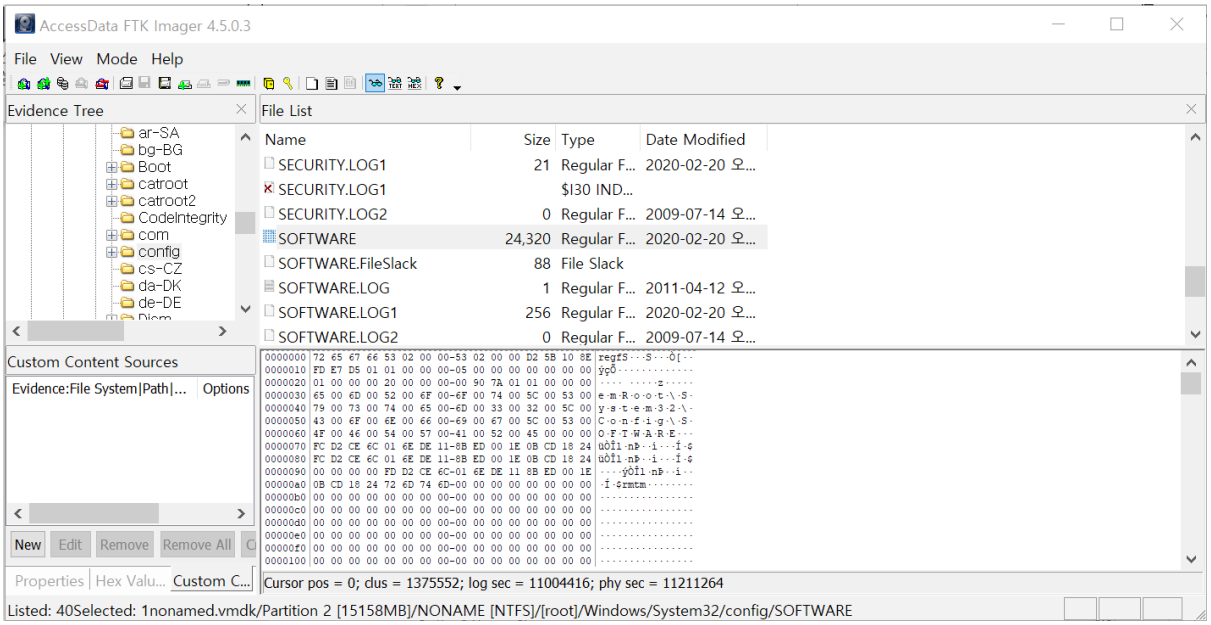
(15 points) 한 회사에서 내부 자료가 유출되는 사건이 발생하였다. 유출된 자료가 판매되고 있다는 제보를 받고, 경찰에서 판매자와 구매자를 모두 잡는다. 다만, 구매자가 자료를 구매했다는 증거가 부족한 상황이다. 그래서 구매자의 PC를 이미지를 따서 우리 회사에 분석을 의뢰했다. 구매자의 집에서 수상한 USB들이 다수 발견되었다고 한다. 구매자의 PC에서 사용된 USB를 찾기 위해, 문제와 함께 첨부된 파일을 구글 드라이브로부터 다운로드 하여 연결된 모든 USB 대용량 장치의 브랜드를 찾는 분석을 진행하자. **(풀이과정 스크린샷 첨부 필수)**

HINT 1) 진행을 위해, 제공된 VMDK 이미지 파일을 FTK Imager로 실행한 후 레지스트리 파일을 Export하여 분석

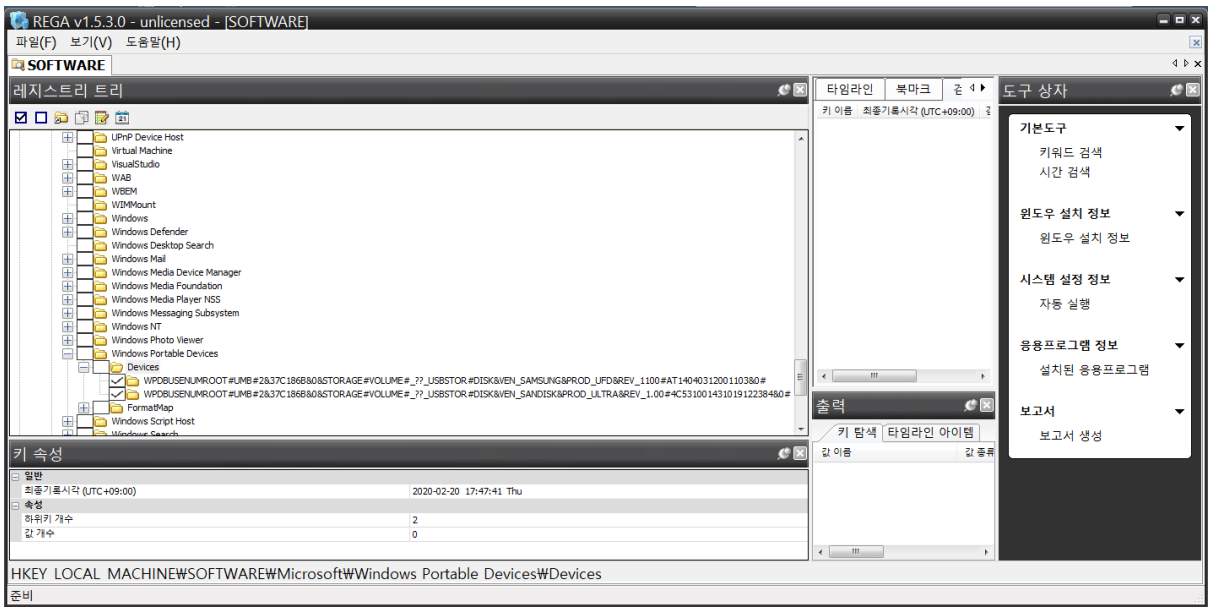
레지스트리 경로	하이브 파일 경로
HKEY_LOCAL_MACHINE\BCD00000000	{Boot Partition}\Boot\BCD
HEKY_LOCAL_MACHINE\COMPONENTS	%SystemRoot%\System32\Config\COMPONENTS
HEKY_LOCAL_MACHINE\SYSTEM	%SystemRoot%\System32\Config\SYSTEM
HEKY_LOCAL_MACHINE\SAM	%SystemRoot%\System32\Config\SAM
HEKY_LOCAL_MACHINE\SECURITY	%SystemRoot%\System32\Config\SECURITY
HEKY_LOCAL_MACHINE\SOFTWARE	%SystemRoot%\System32\Config\SOFTWARE
HEKY_LOCAL_MACHINE\HARDWARE	Volatile
HKEY_USERS\<SID of local service account>	%SystemRoot%\ServiceProfiles\LocalService\NTUSER.DAT
HKEY_USERS\<SID of network service account>	%SystemRoot%\ServiceProfiles\NetworkService\NTUSER.DAT
HKEY_USERS\<SID of username>	%UserProfile%\NTUSER.DAT
HKEY_USERS\<SID of username>_Classes	%UserProfile%\AppData\Local\Microsoft\Windows\Usrclass.dat
HKEY_USERS\.DEFAULT	%SystemRoot%\System32\Config\DEFAULT 23

hint3 에 따르면, HKLM\Software\Microsoft\Windows Portable Devices\Devices 레지스트리의 하위 키에서 USB 장치의 브랜드 정보가 확인 가능하다.
따라서, 우리는 HKEY_LOCAL_MACHINE\SOFTWARE 의 하이브 파일 경로가 필요하고 그것은 %SystemRoot%\System32\Config\SOFTWARE임을 알 수 있다. 해당 경로로 가서 하이브 파일을 추출해준다.

Name: 이혜린 Student ID: 20190937



HINT 2) Export한 레지스트리 파일을 분석하기 위해 REGA 프로그램을 사용. (다운로드 링크: forensic.korea.ac.kr/tools.html) 다운로드 한 뒤 [파일] -> [레지스트리 파일 열기] 선택한 뒤 시간을 서울로 설정하고, Export한 레지스트리 파일을 선택하면 레지스트리 편집기와 같은 창을 확인 가능



HINT 3) HKLM\Software\Microsoft\Windows Portable Devices\Devices 레지스트리의 하위 키에서 USB 장치의 브랜드 정보를 확인 가능

Name: 이혜린 Student ID: 20190937

HKLM\Software\Microsoft\Windows Portable Devices\Devices 레지스트리의 하위 키들은 다음과 같다.

WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_SAMSUNG&PROD_UFD&REV_1100#AT14040312001103&0#

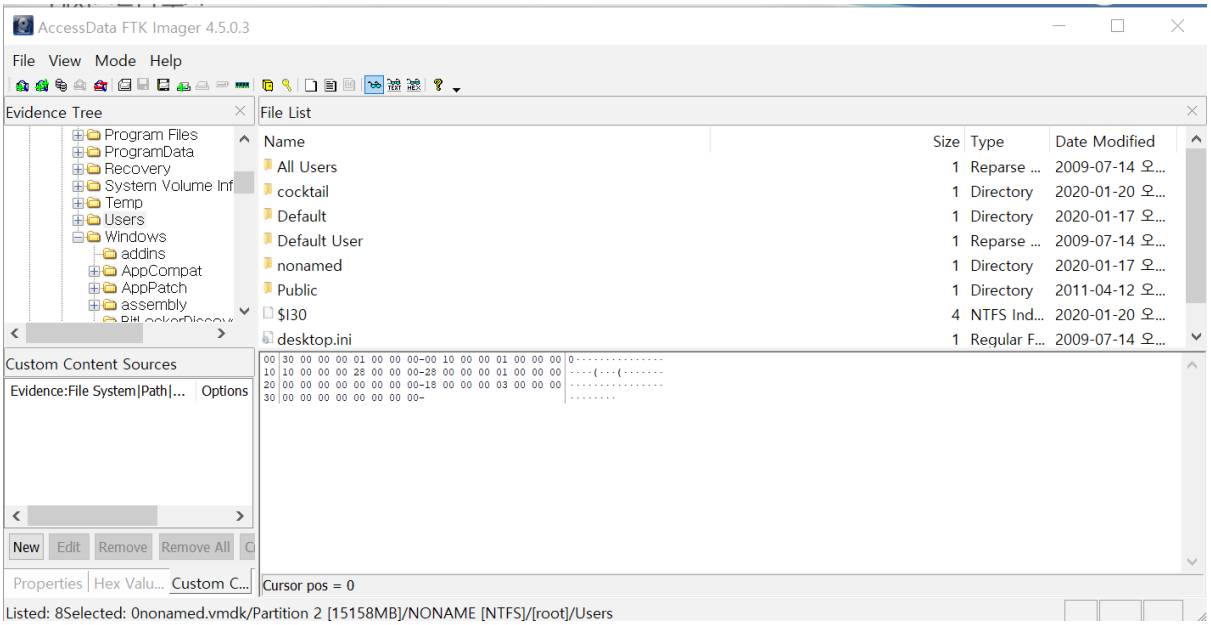
WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_SANDISK&PROD_ULTRA&REV_1.00#4C531001431019122384&0#

USB 장치의 브랜드 정보: Samsung, Sandisk 임을 확인할 수 있음.

(15 points) (동일한 파일로 문제 풀이 계속 진행) 포렌식 분석을 통해 구매자의 계정이 nonamed임을 파악하였는데, 조사 과정에서 구매자의 집에 PC를 함께 사용하는 동거자가 있었던 것으로 추정된다. 동거자가 사용한 계정의 이름을 알아내고, 해당 계정이 삭제된 시간을 파악하여 YYYY/MM/DD:HH:MM:SS 형식으로 나타내라. **(풀이과정 스크린샷 첨부 필수)**

HINT 1) 진행을 위해, 제공된 VMDK을 FTK Imager로 실행한 후 분석을 통해 사용자 계정 파악

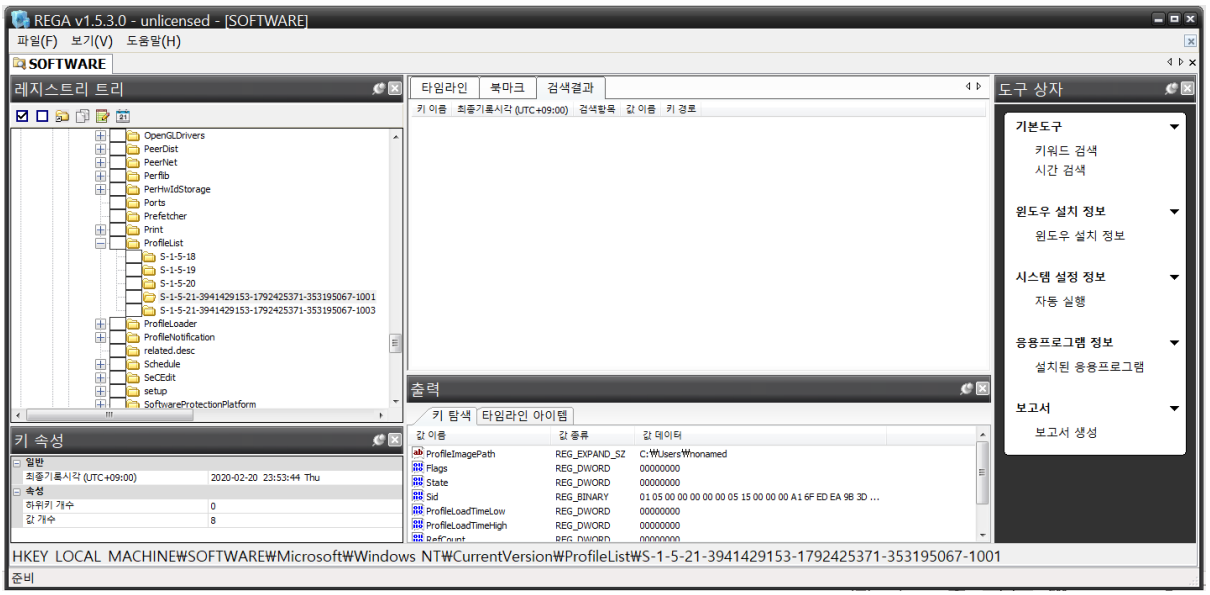
Name: 이혜린 Student ID: 20190937



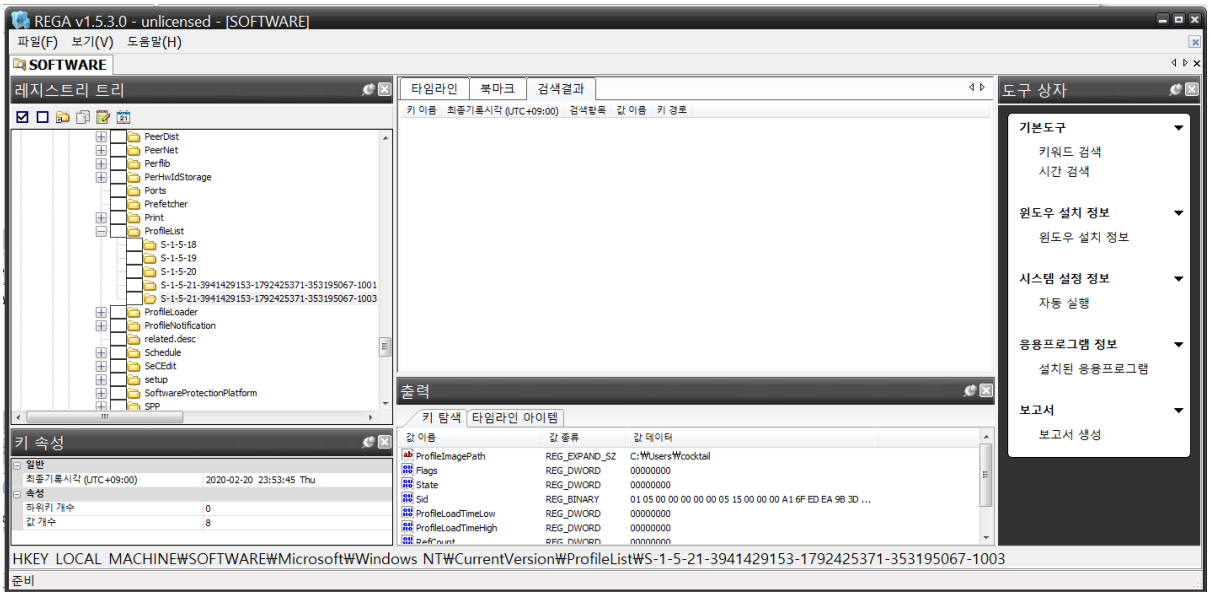
Partition2/NONAME [NTFS]/[root]/Users 에 보면, cocktail, nonamed 등의 계정이 있음을 확인할 수 있다.

사용자 계정은, FTK Imager에서 %SystemRoot%\System32\Config\SOFTWARE 을 export해서,

Rega 에서 HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion \ProfileList을 분석해봐도 확인해 볼 수 있다.



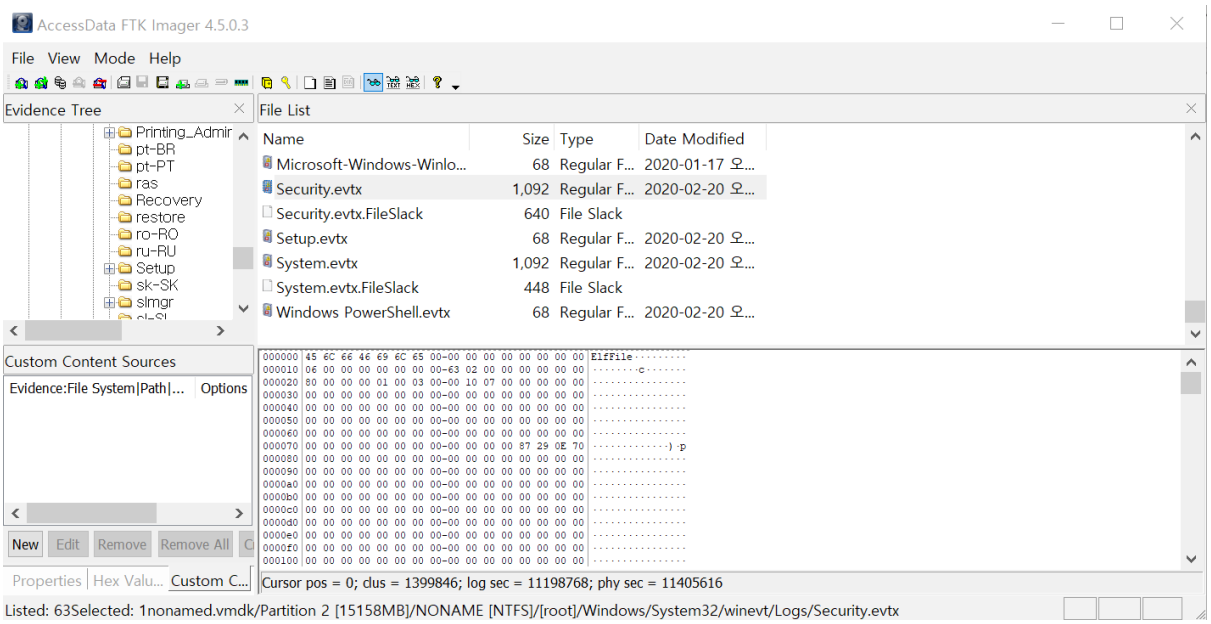
Name: 이혜린 Student ID: 20190937



HINT 2) FTK Imager에서 보안 이벤트 로그를 저장하는 파일을 Export하여 확인

어떤 사용자 계정이 사용되었는지, 어떤 컴퓨터에 접근했는지 알고싶으면 시스템 로그온, 계정 생성, 권한 사용 등에 따른 이벤트와 보안과 관련된 항목들이 저장된 security.evtx를 보면 된다.

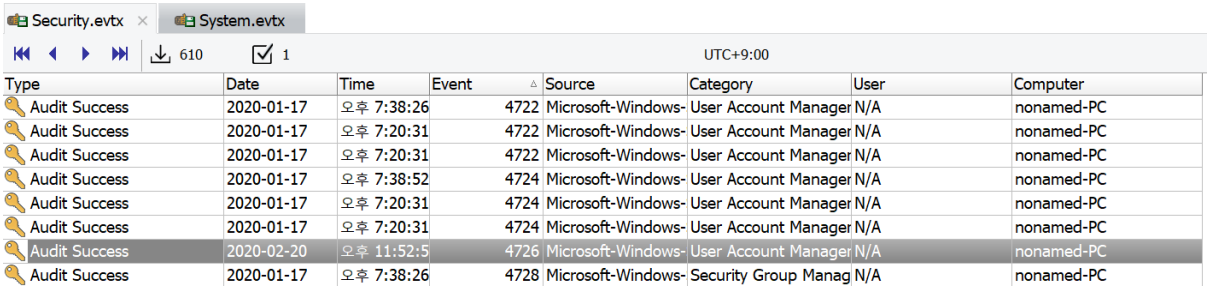
security.evtx의 경로는 '%SystemRoot%\System32\Winevt\Logs\Security.evtx이므로 해당 경로로 가서 파일을 export해준다.



HINT 3) 보안 이벤트 로그 중 이벤트 ID "4726:삭제된 사용자 계정"를 활용

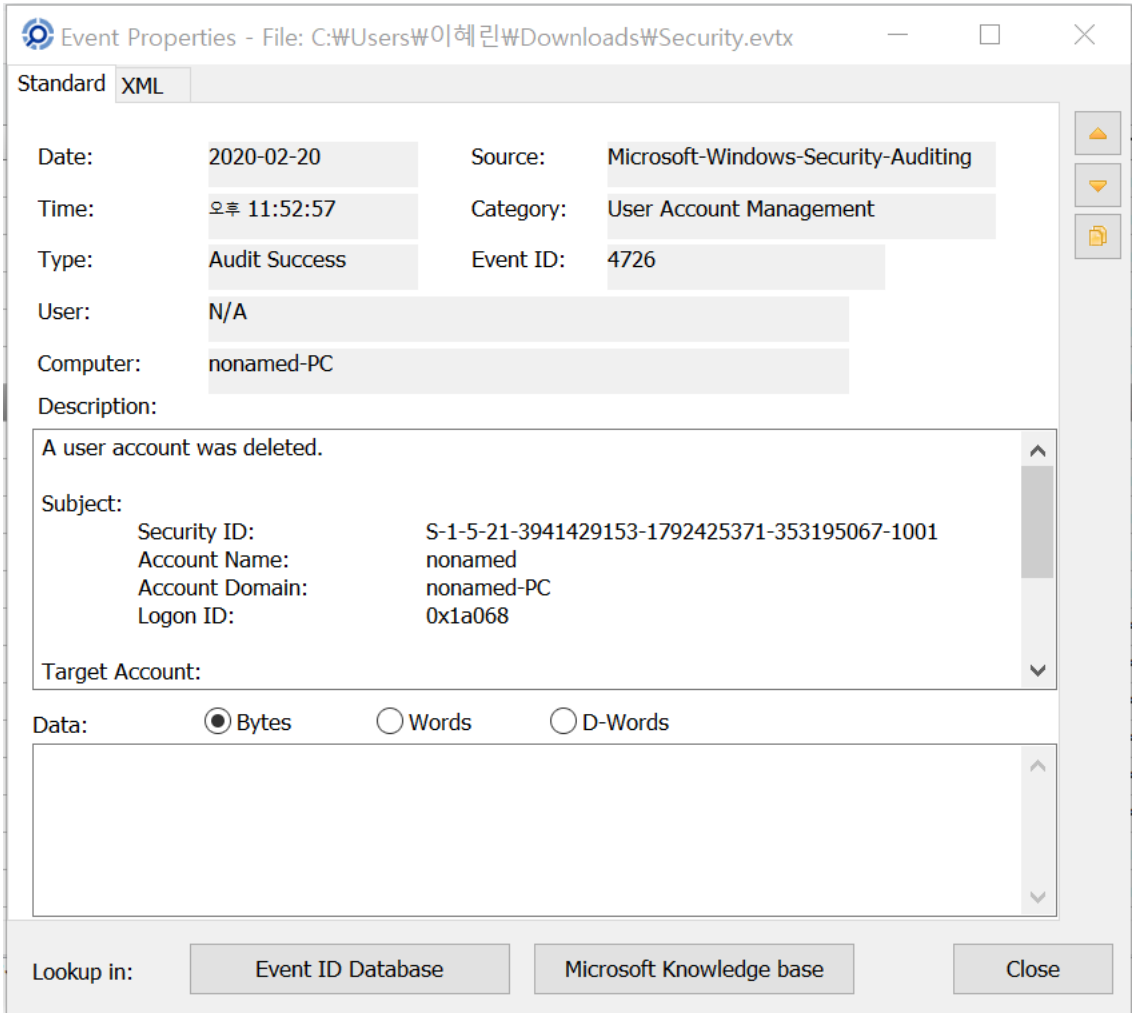
Name: 이혜린 Student ID: 20190937

Event Log Explorer 을 관리자 권한으로 실행하여 security.evtx를 분석한다.

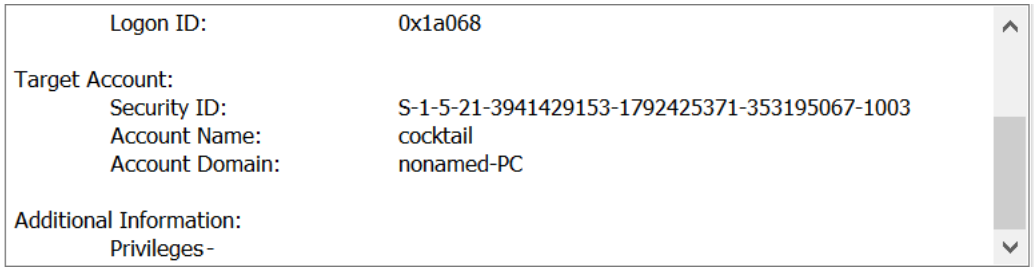


Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	2020-01-17	오후 7:38:26	4722	Microsoft-Windows-	User Account Manager	N/A	nonamed-PC
Audit Success	2020-01-17	오후 7:20:31	4722	Microsoft-Windows-	User Account Manager	N/A	nonamed-PC
Audit Success	2020-01-17	오후 7:20:31	4722	Microsoft-Windows-	User Account Manager	N/A	nonamed-PC
Audit Success	2020-01-17	오후 7:38:52	4724	Microsoft-Windows-	User Account Manager	N/A	nonamed-PC
Audit Success	2020-01-17	오후 7:20:31	4724	Microsoft-Windows-	User Account Manager	N/A	nonamed-PC
Audit Success	2020-01-17	오후 7:20:31	4724	Microsoft-Windows-	User Account Manager	N/A	nonamed-PC
Audit Success	2020-02-20	오후 11:52:5	4726	Microsoft-Windows-	User Account Manager	N/A	nonamed-PC
Audit Success	2020-01-17	오후 7:38:26	4728	Microsoft-Windows-	Security Group Manag	N/A	nonamed-PC

이벤트 ID 4726인 이벤트 로그를 더블 클릭하면,



2020/02/20:23:52:57에 nonamed-PC에서 누군가가 nonamed 계정을 이용하여 한 사용자 계정을 삭제했다는 것을 알 수 있다. 그리고 삭제된 계정의 이름은



cocktail이다.

계정 삭제된 시간: 2020/02/20:23:52:57, 삭제된 계정 이름: cocktail