
Windows 포렌식 – 레지스트리 분석

201812745 김종원

A Table of Contents.


1 Windows 포렌식 및 레지스트리

2 레지스트리 분석 - 실습



Windows 포렌식이란,

사용자가 시스템을 사용하면서 남는 아티팩트를 분석하여,
*파일 유출, 불법 다운, 문서 조작, 저장매체 연결흔적*과 같은
흔적들을 분석하는 과정



Windows 포렌식의 범위

- 레지스트리, \$MFT, 휴지통, 프리패치, 웹 로그, 셸백, 점프리스트, 링크파일, 메모리파일, 스케줄러, ADS,

레지스트리 구성-1

레지스트리 : 시스템에서 사용하는 시스템 구성 정보를 저장한 데이터베이스

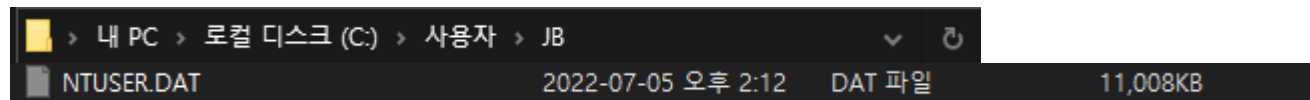
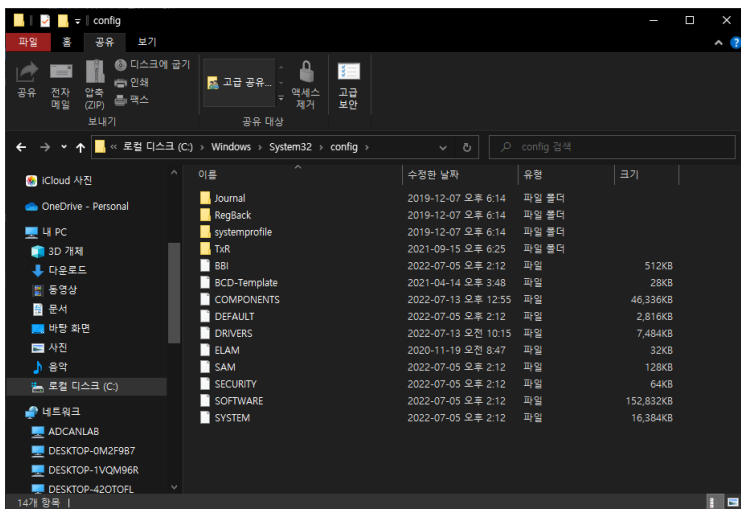


- HKEY_CLASS_ROOT : 파일 연관성과 COM정보
- **HKEY_LOCAL_MACHINE** : 시스템의 하드웨어/소프트웨어 정보
- **HKEY_CURRENT_USER** : 현재 시스템에 로그인 된 사용자 정보
- HKEY_USERS : 모든 사용자 정보
- HKEY_CURRENT_CONFIG : 시스템 시작 시 사용되는 하드웨어 정보

레지스트리 구성-2

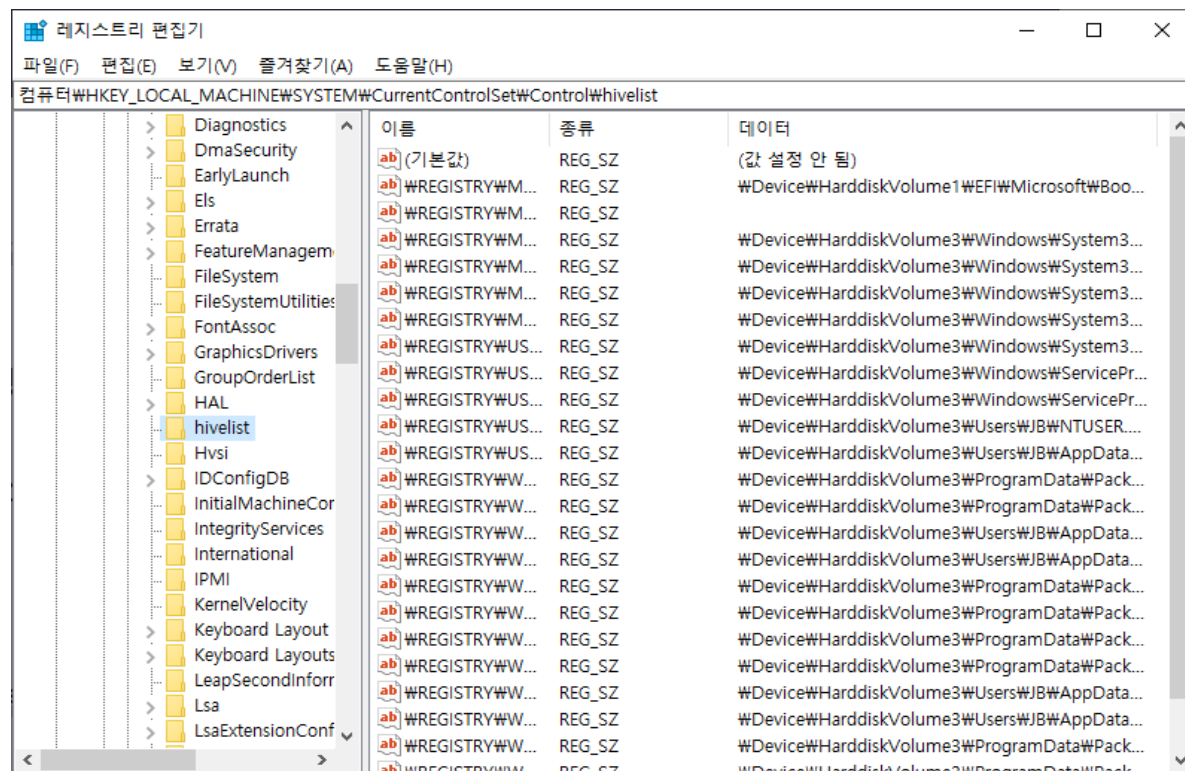
하이브 파일 – 레지스트리의 정보를 가지고 있는 물리적인 파일

- **SAM**: 로컬 계정 정보와 그룹 정보
- **SECURITY** : 시스템 보안 정책과 권한 할당 정보
- **SOFTWARE** : 시스템 부팅에 필요 없는 시스템 전역 구성 정보
- **SYSTEM** : 시스템 부팅에 필요한 전역 구성 정보
- **Ntuser.dat** : 사용자 프로파일 정보



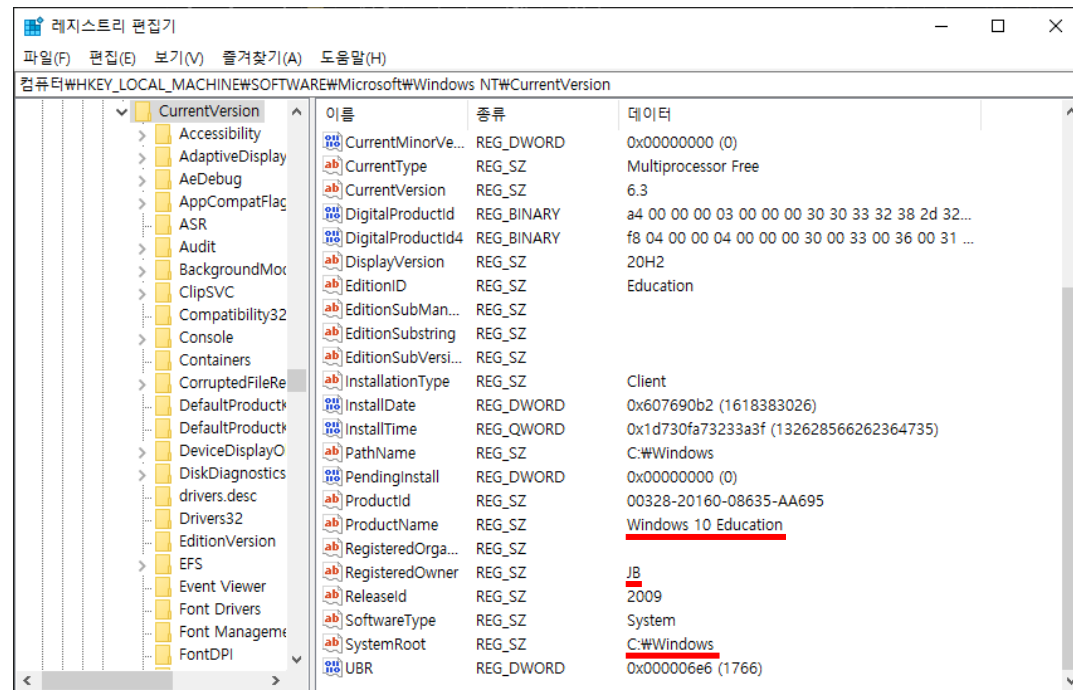
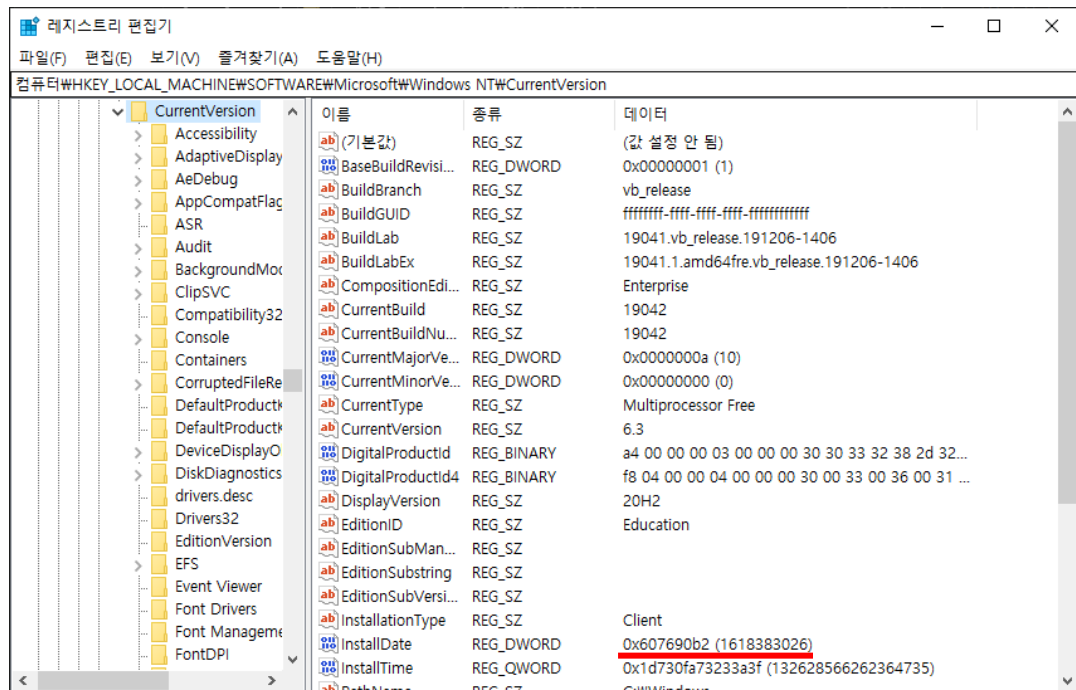
레지스트리 수집

- 해당 경로에서 연결된 하이브 목록 확인 가능
- 일반적으로 레지스트리 파일은 커널에서 열려 있으므로 직접 분석 하거나 이미지에서 채증.



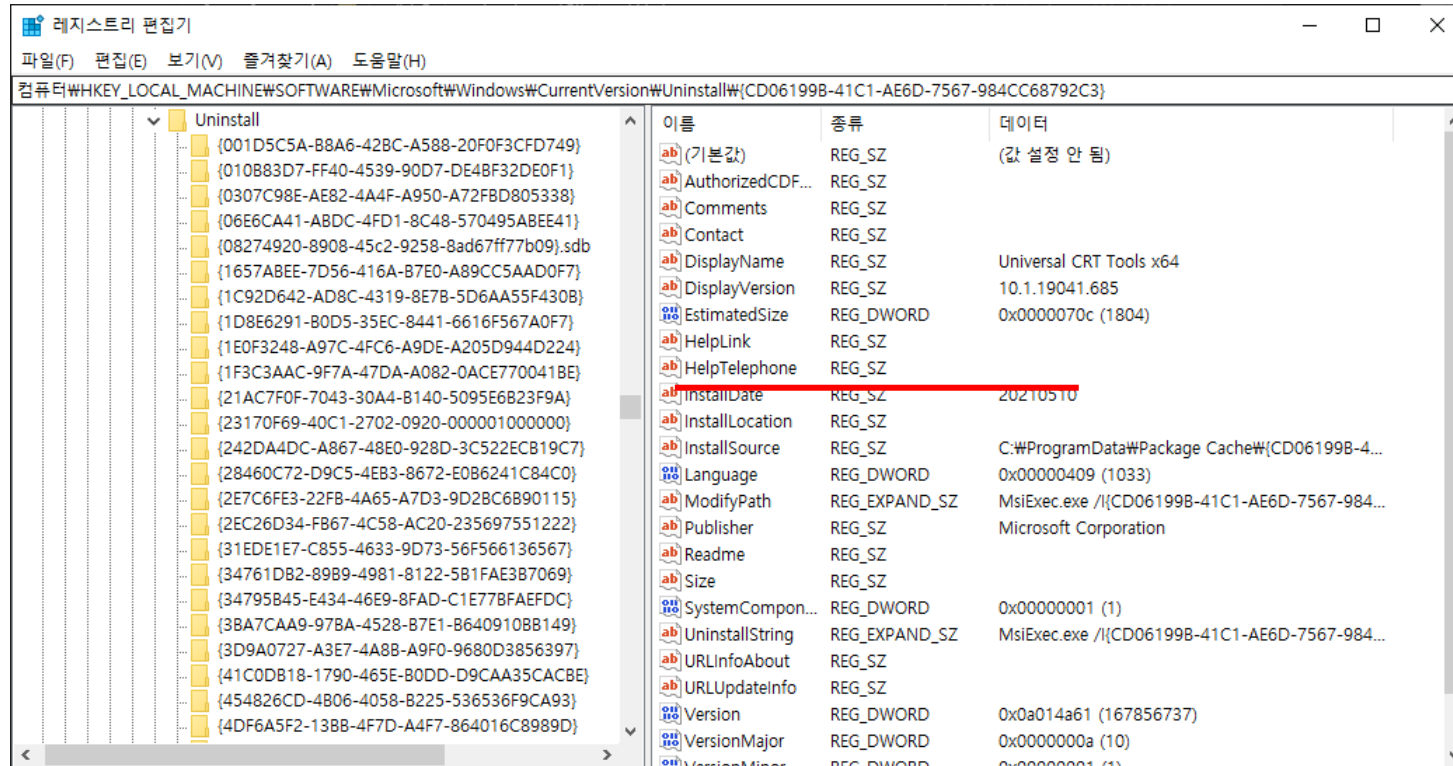
레지스트리 분석

- 시스템 정보 - OS 설치 날짜/시각, OS Version, 컴퓨터이름, 조직이름, 운영체제 설치루트폴더
- 경로 : 컴퓨터\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion



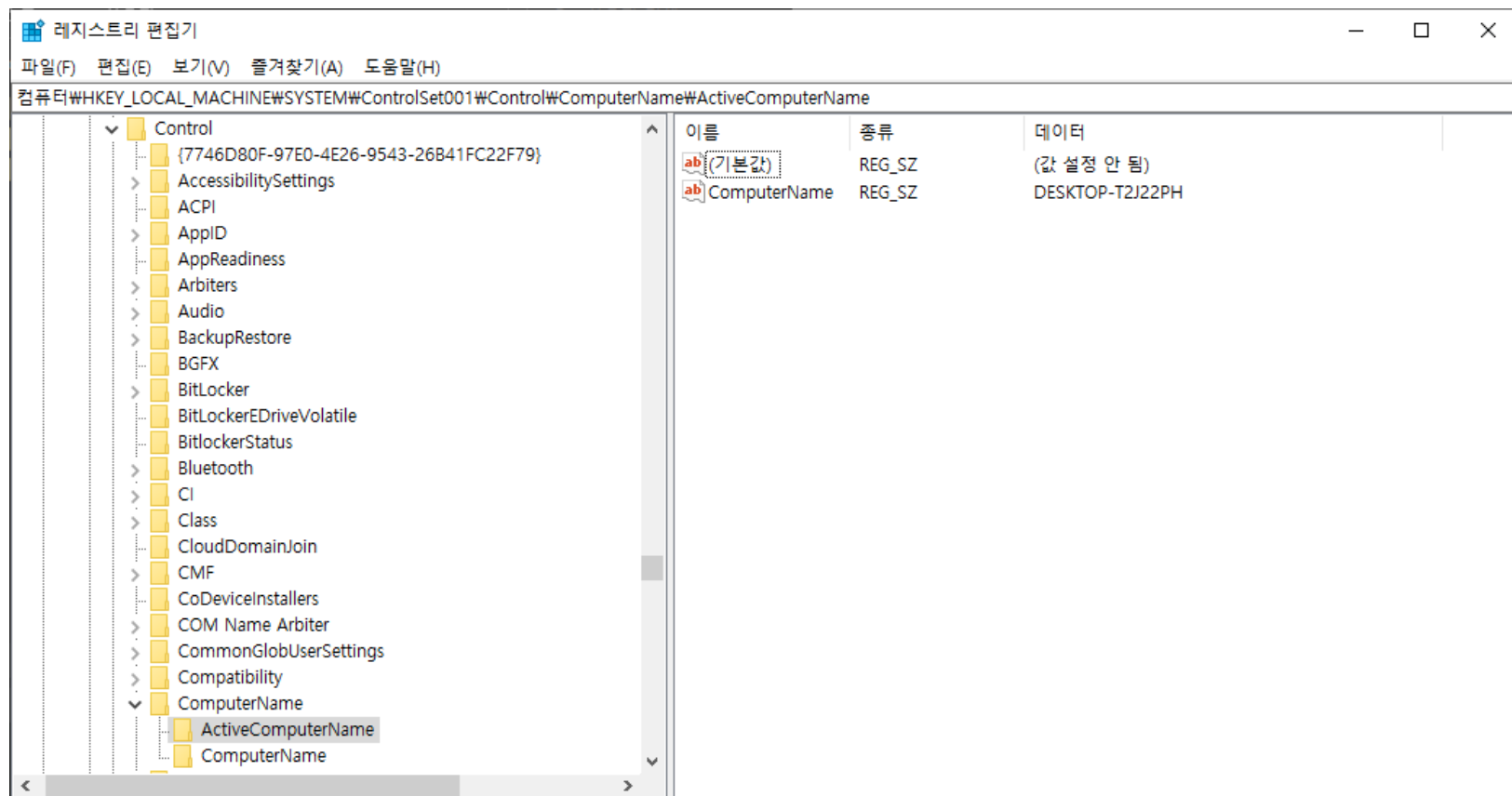
레지스트리 분석

- 설치된 프로그램 목록 – 설치된 프로그램 이름, 버전, 설치시각 및 위치.
제어판에 은닉된 프로그램들도 표시.
- 경로 : 컴퓨터\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall



레지스트리 분석

- 컴퓨터 이름
- 경로 : 컴퓨터\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName

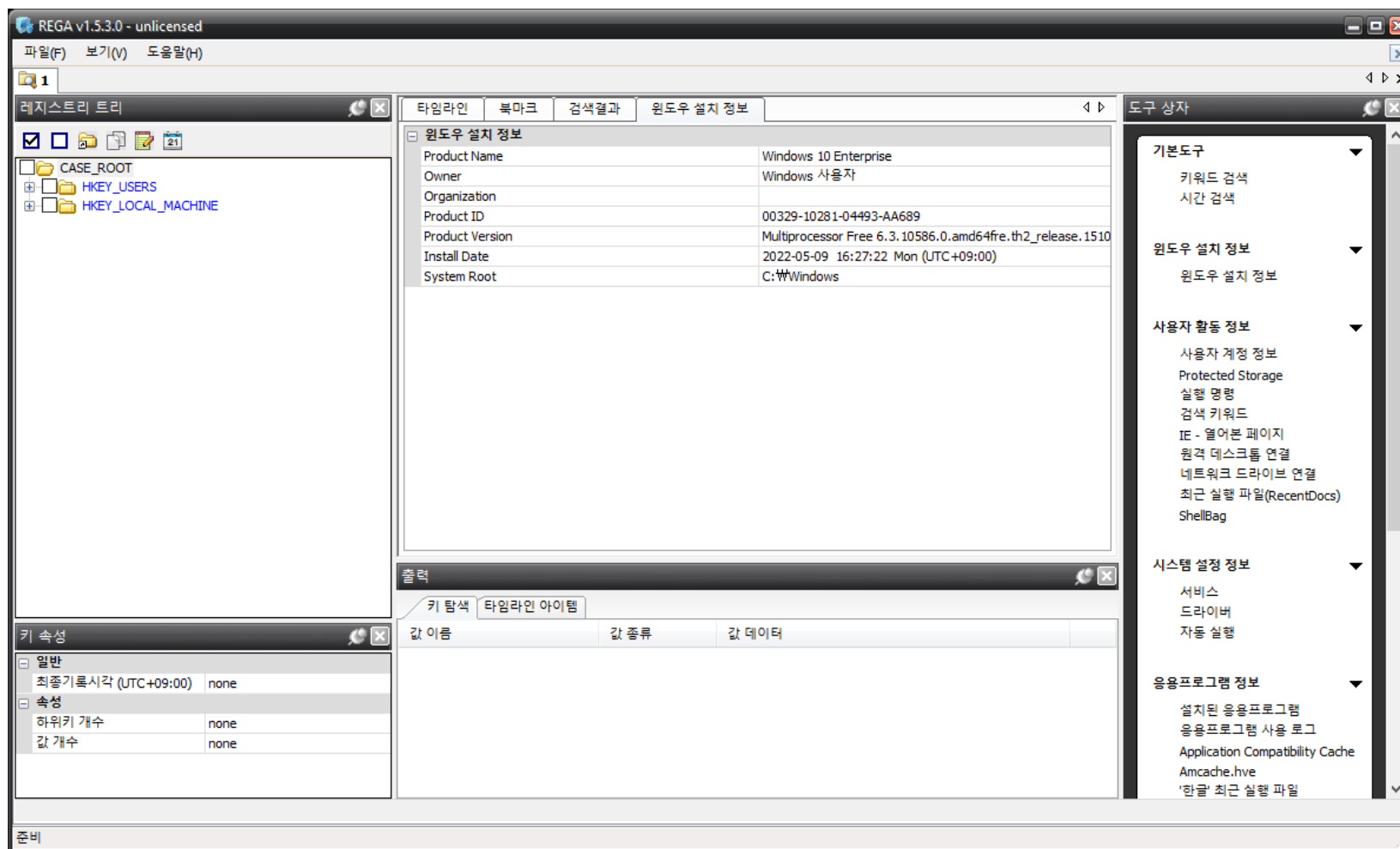


레지스트리 분석

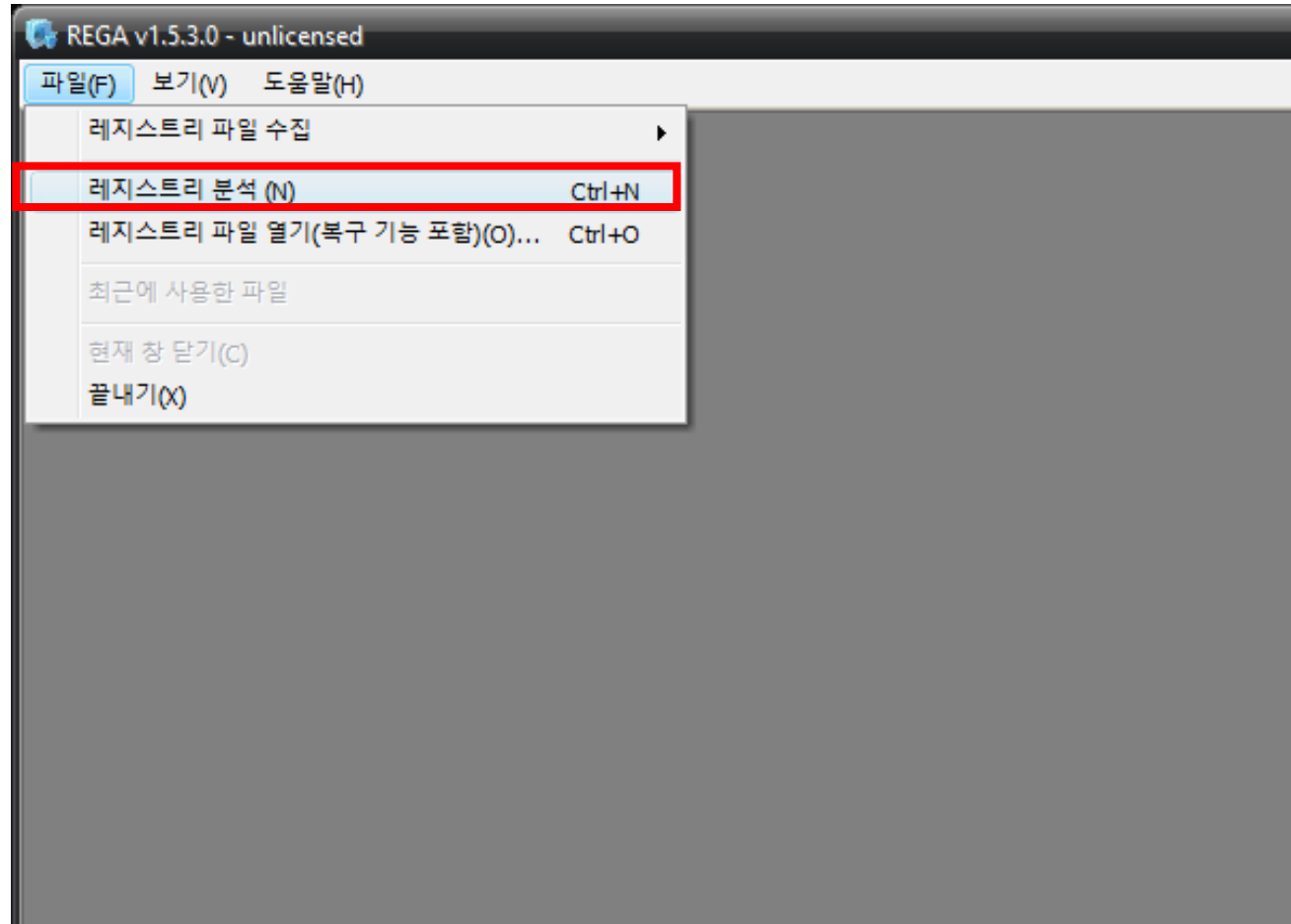
- SID정보
- 사용자 기본 폴더
- 마지막 로그인한 사용자 정보
- 시스템 마지막 종료시간
- 표준 시간대
- 응용 프로그램 사용 흔적
- 그림판, 워드패드에서 열어본 목록
- MS OFFICE, 한글, 곰플레이어, Adobe 사용흔적
- 최근 열어본 파일 흔적
- 최근 실행창 검색 흔적
- 저장매체 연결 흔적

레지스트리 분석 - 도구

- Process Monitor
- RegShot
- RegRipper
- REGA

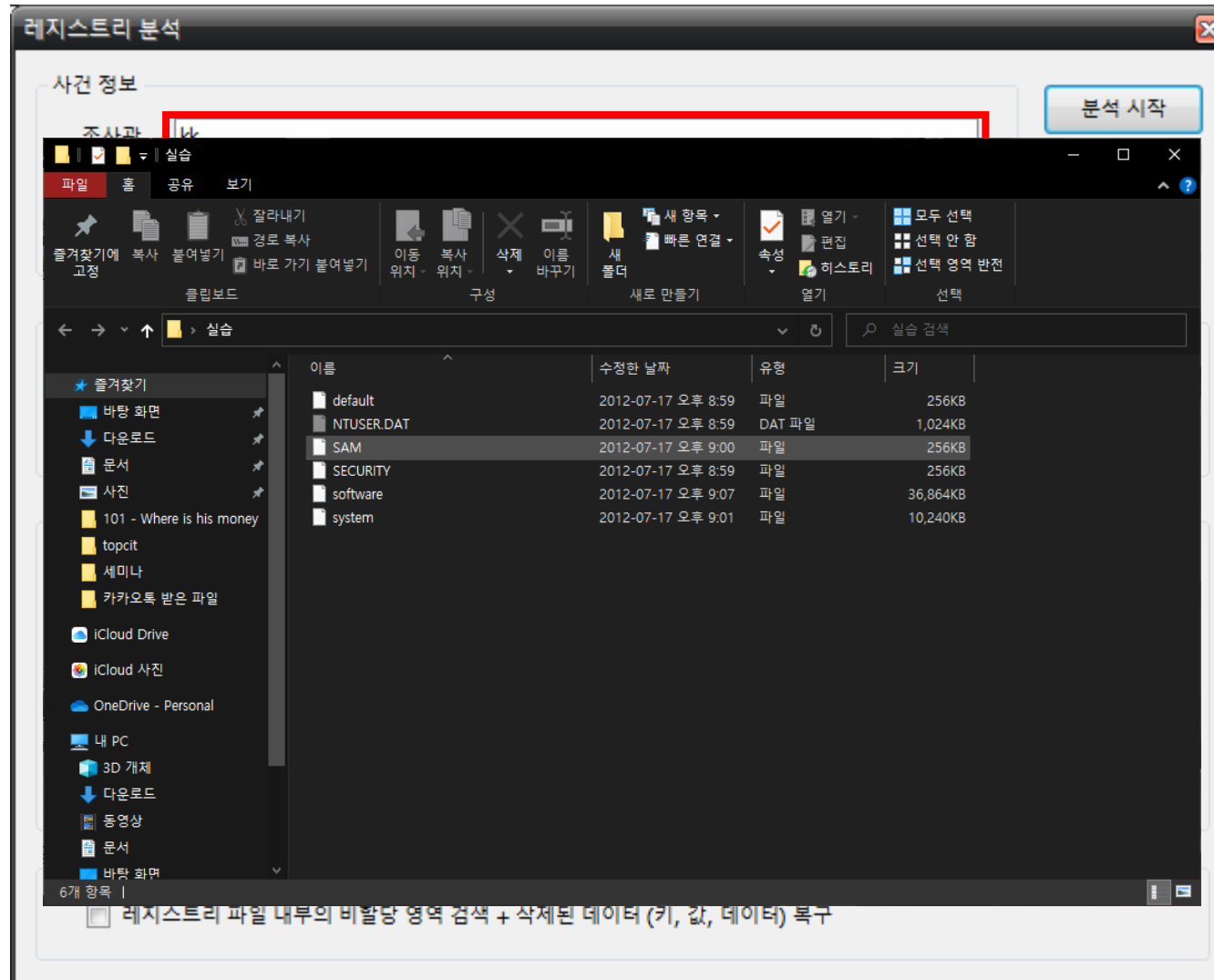


REGA 사용법



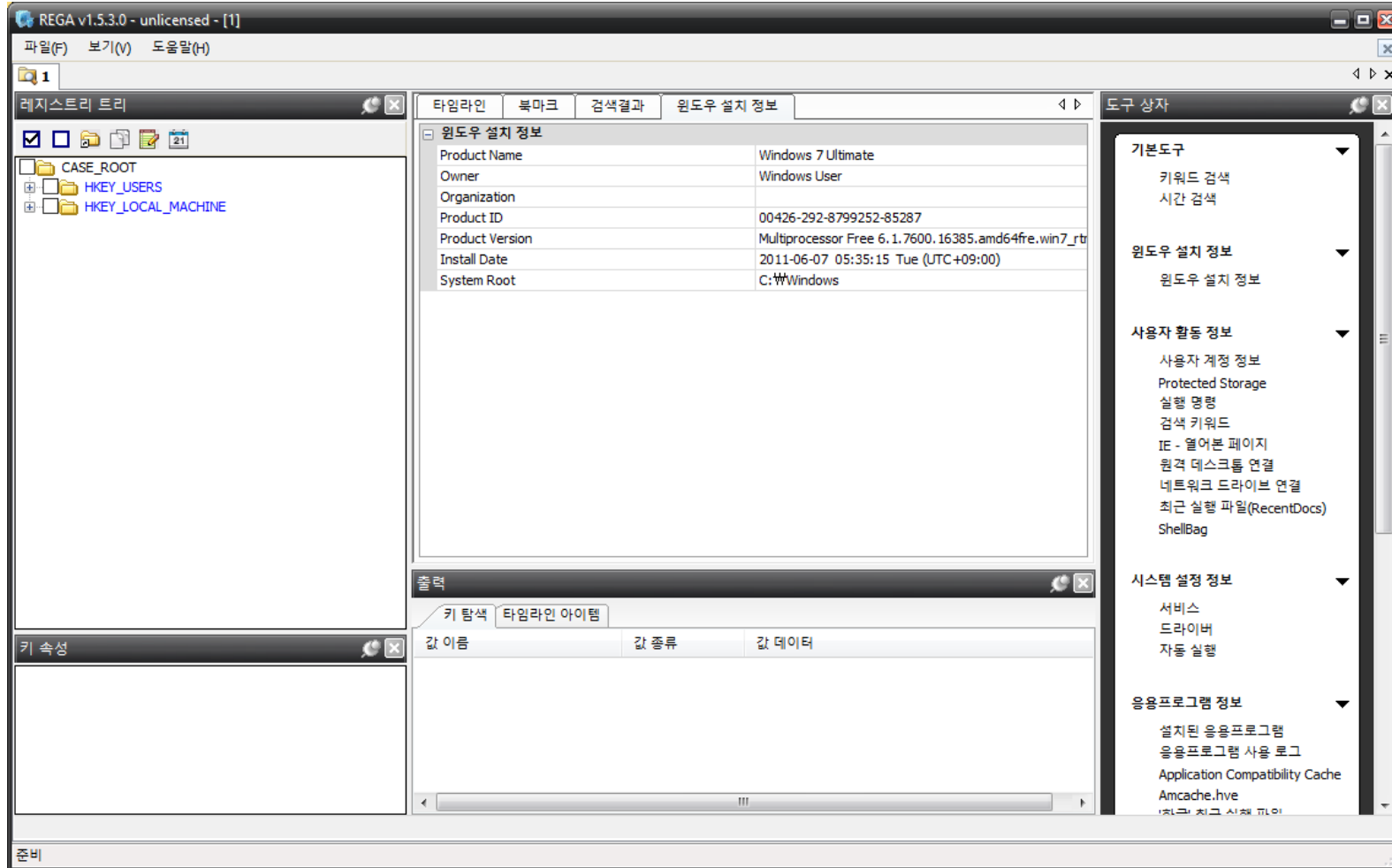
Part 2, 레지스트리 분석 - 실습

REGA 사용법



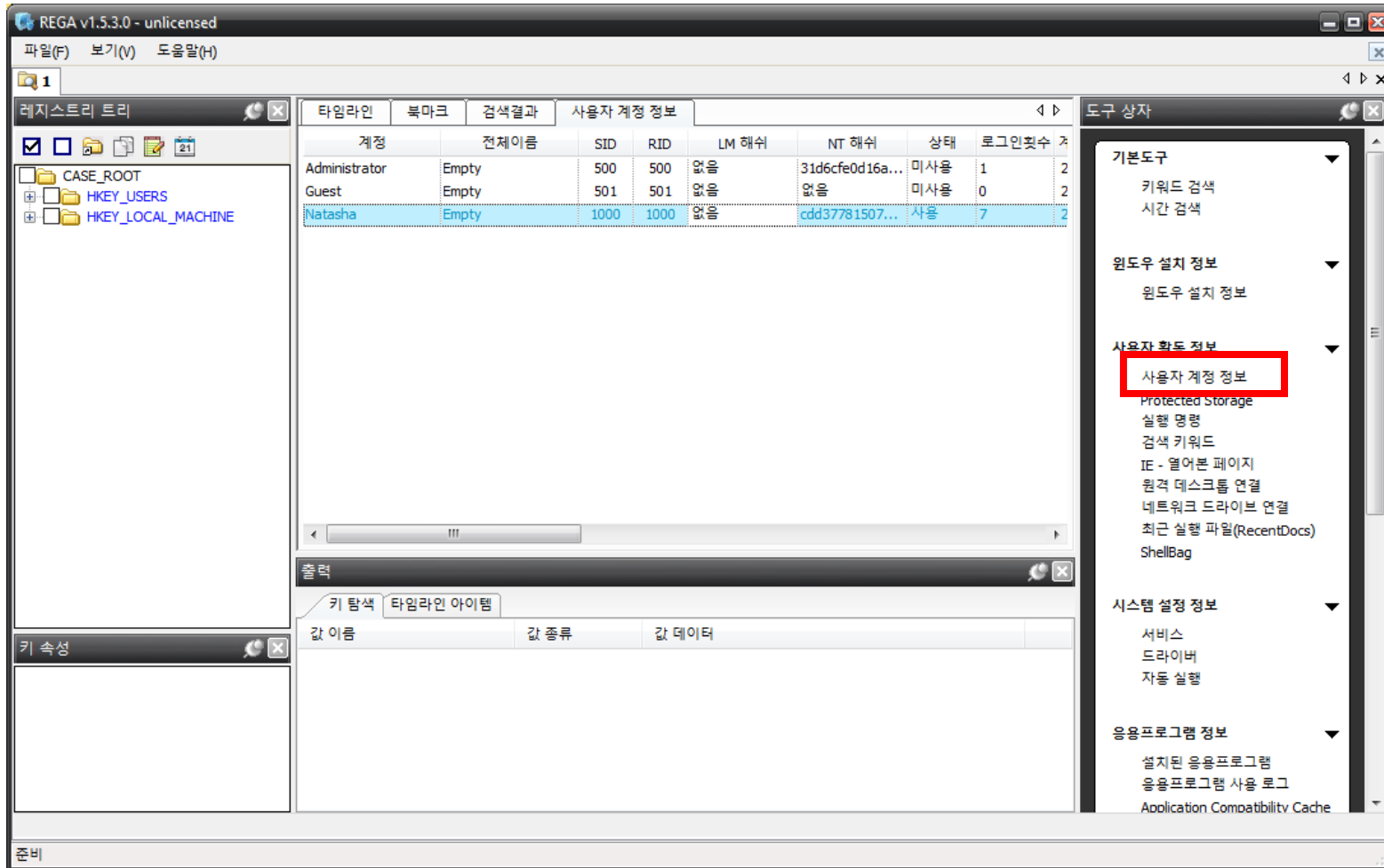
Part 2, 레지스트리 분석 - 실습

REGA 사용법



Part 2, 레지스트리 분석 - 실습

문제 - 시스템의 사용자 이름은 무엇인가요?

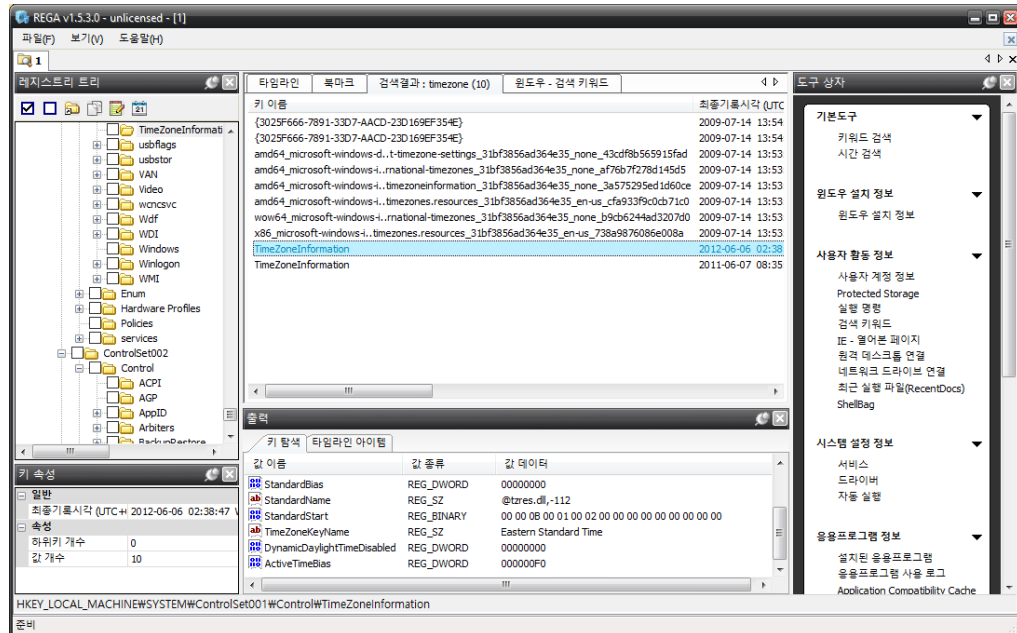
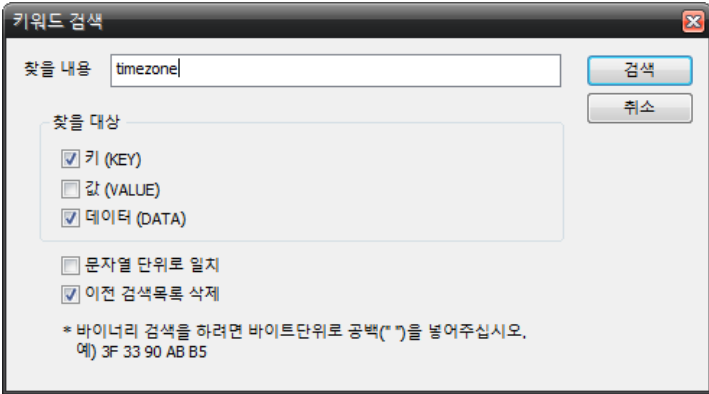








Guest	Empty	501	501	미
Natasha	Empty	1000	1000	미

Answer : **Natasha**

레지스트리 분석 - 실습

문제 - 기본 타임존 포맷은 무엇인가요?

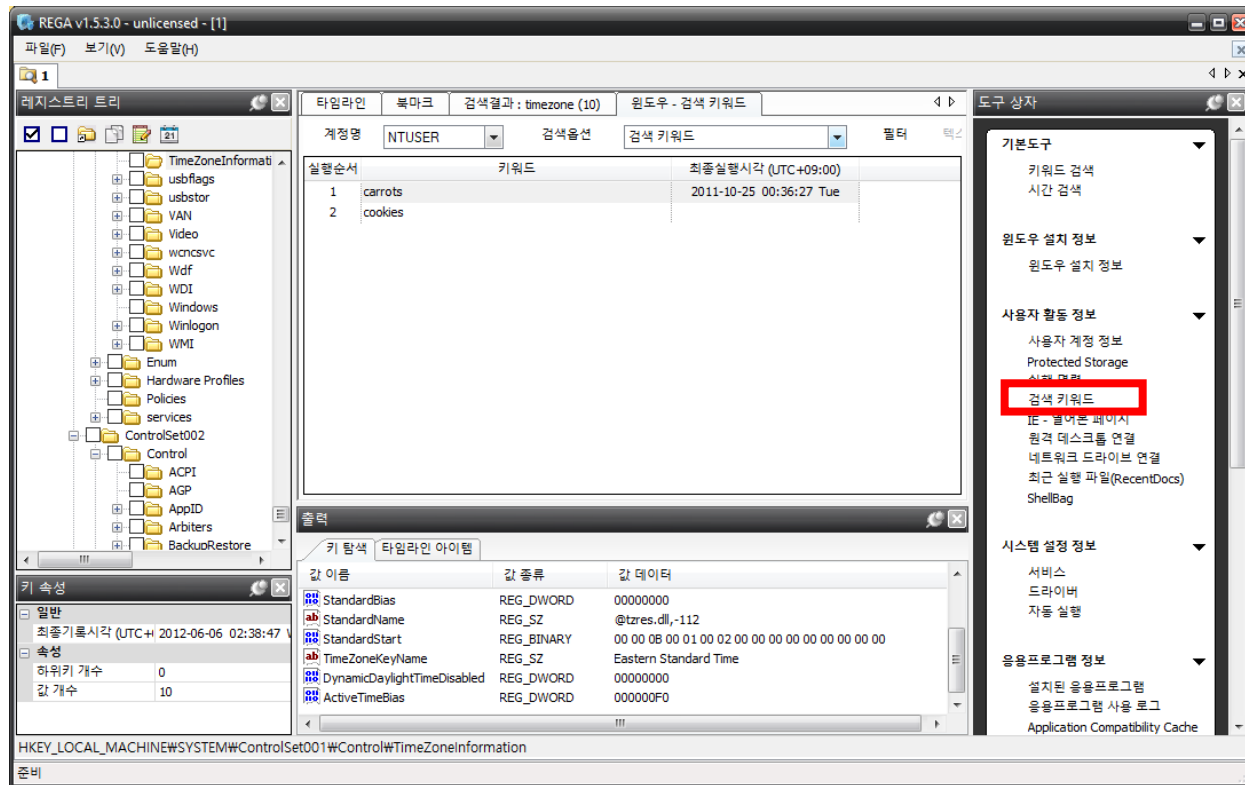


값 이름	값 종류	값 데이터
 StandardBias	REG_DWORD	00000000
 StandardName	REG_SZ	@tzres.dll,-112
 StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00
 TimeZoneKeyName	REG_SZ	Eastern Standard Time
 DynamicDaylightTimeDisabled	REG_DWORD	00000000
 ActiveTimeBias	REG_DWORD	000000F0

Answer : **Eastern Standard Time**

Part 2, 레지스트리 분석 - 실습

문제 – 탐색기에서 검색한 단어는 무엇인가요?

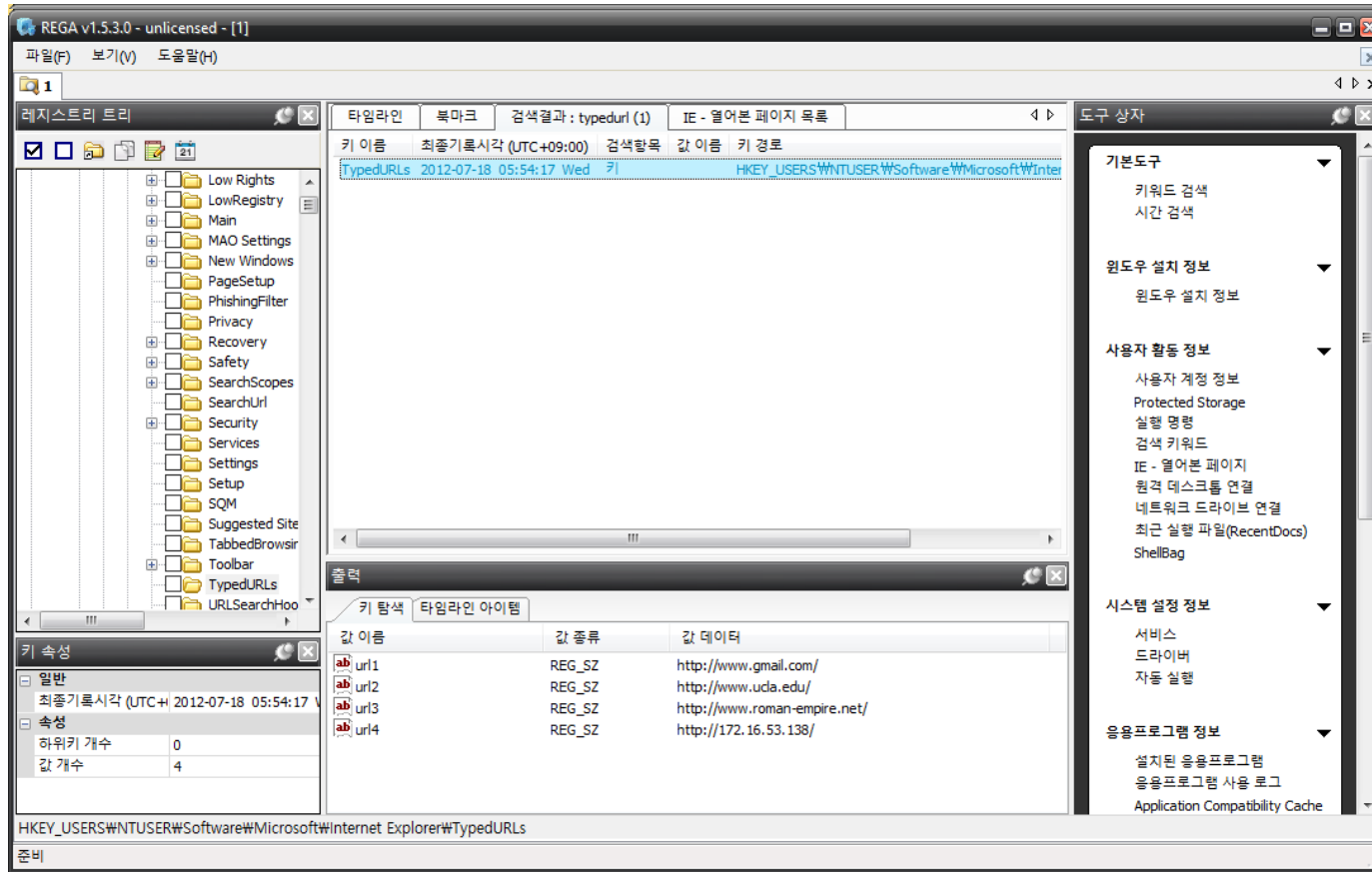


실행순서	키워드
1	carrots
2	cookies

Answer : **carrots, cookies**

Part 2, 레지스트리 분석 - 실습

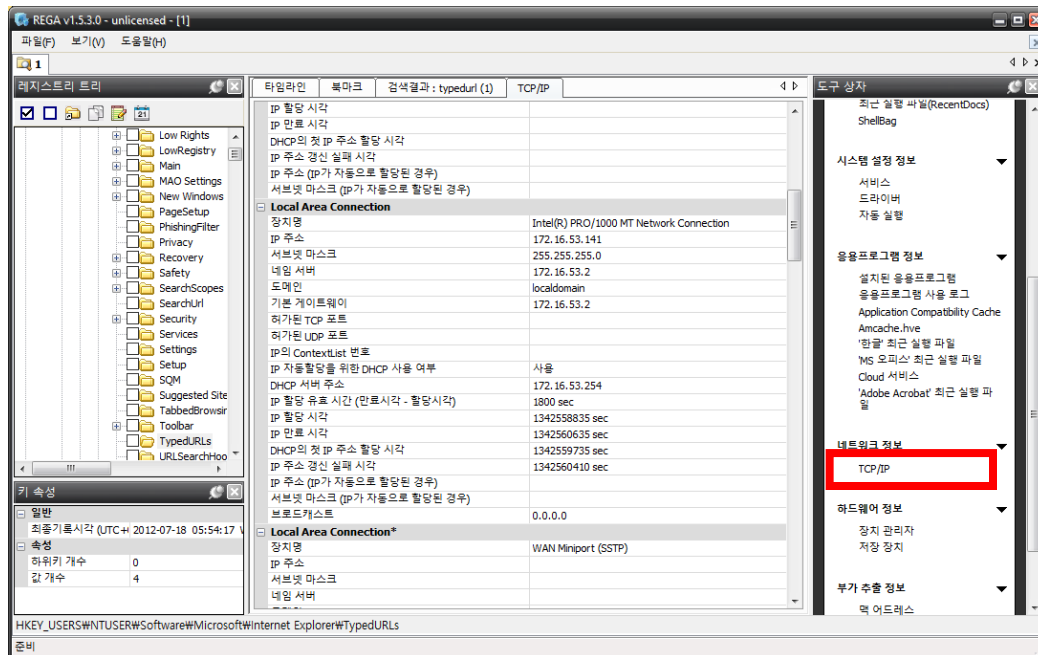
문제 - 나타샤가 IE에 Typing한 URL주소는 무엇인가요?



url1	REG_SZ	http://www.gmail.com/
url2	REG_SZ	http://www.udc.edu/
url3	REG_SZ	http://www.roman-empire.net/
url4	REG_SZ	http://172.16.53.138/

Part 2, 레지스트리 분석 - 실습

문제 - 기본 IP는 무엇인가요?



Local Area Connection	
장치명	Intel(R) PRO/1000 MT Network Connection
IP 주소	172.16.53.141
서브넷 마스크	255.255.255.0
네임 서버	172.16.53.2
도메인	localdomain
기본 게이트웨이	172.16.53.2
허가된 TCP 포트	
허가된 UDP 포트	
IP의 ContextList 번호	
IP 자동할당을 위한 DHCP 사용 여부	사용
DHCP 서버 주소	172.16.53.254
IP 할당 유효 시간 (만료시각 - 할당시각)	1800 sec
IP 할당 시각	1342558835 sec
IP 만료 시각	1342560635 sec
DHCP의 첫 IP 주소 할당 시각	1342559735 sec
IP 주소 갱신 실패 시각	1342560410 sec
IP 주소 (IP가 자동으로 할당된 경우)	
서브넷 마스크 (IP가 자동으로 할당된 경우)	
브로드캐스트	0.0.0.0