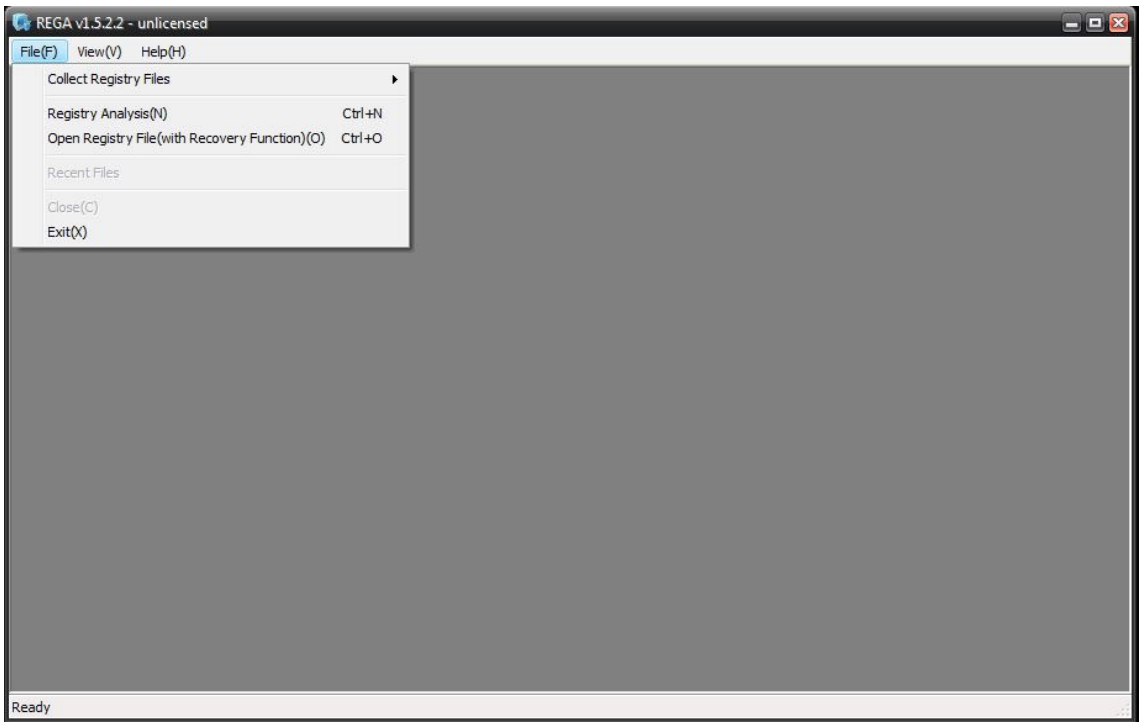
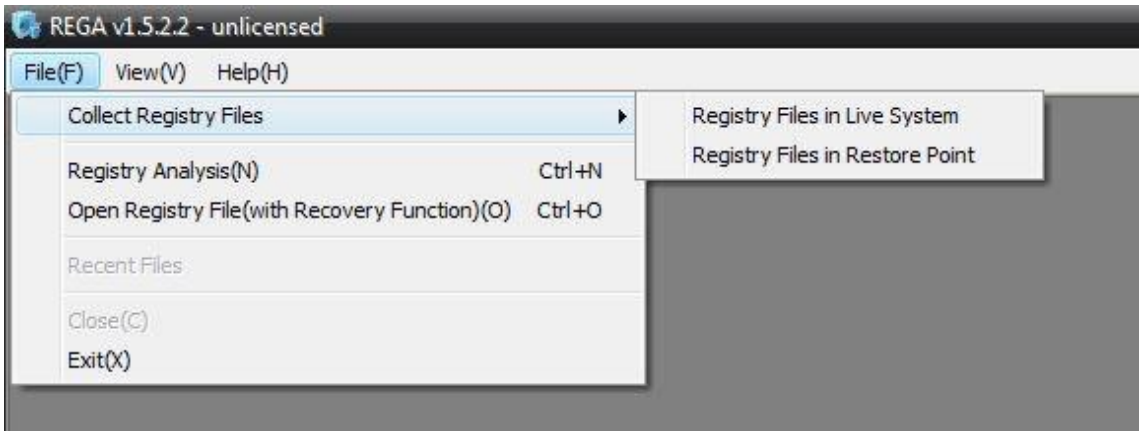
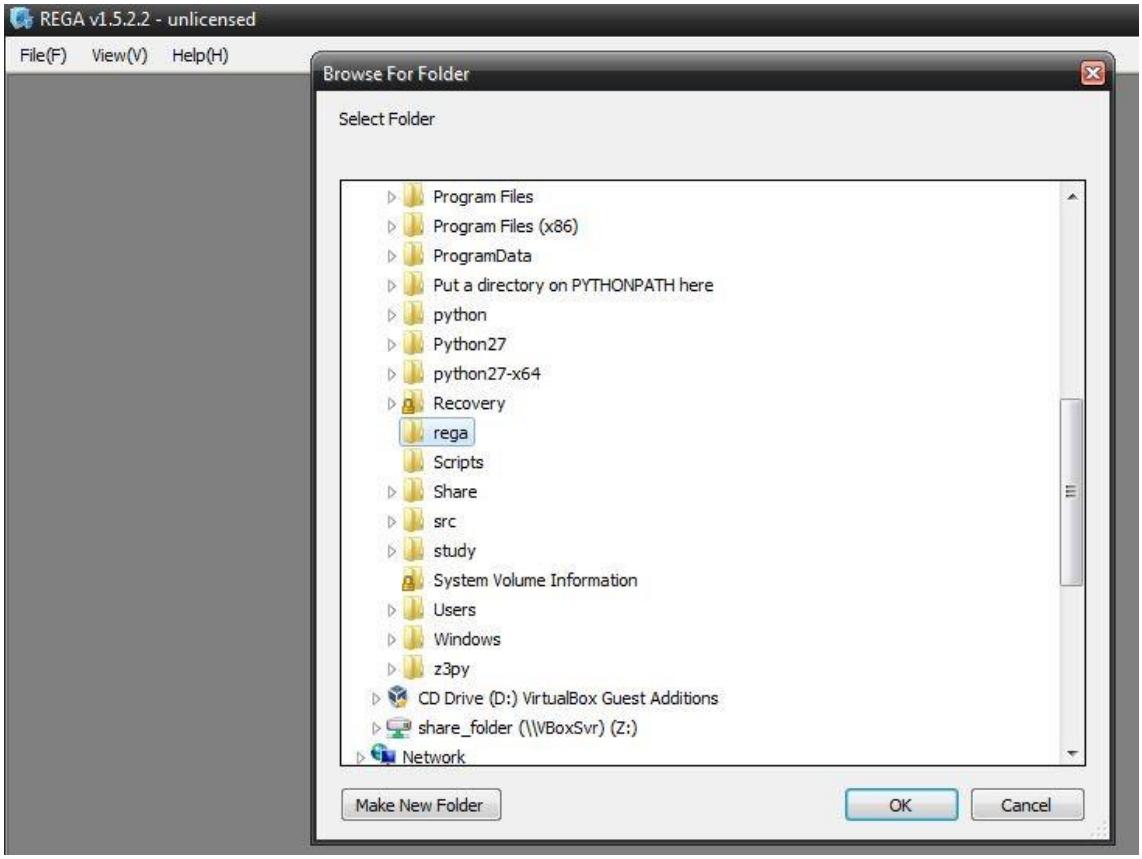
1. rega 를 구동시키면 다음과 같은 화면을 볼 수 있다.



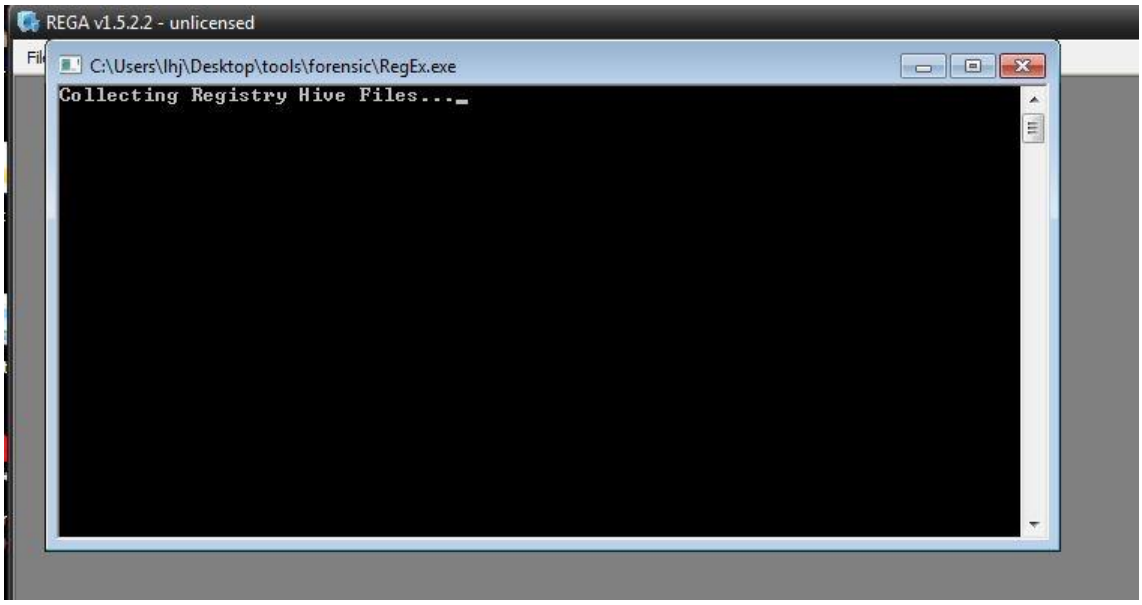

2. File - Collect Registry Files - Registry Files in Live System 을 누르면



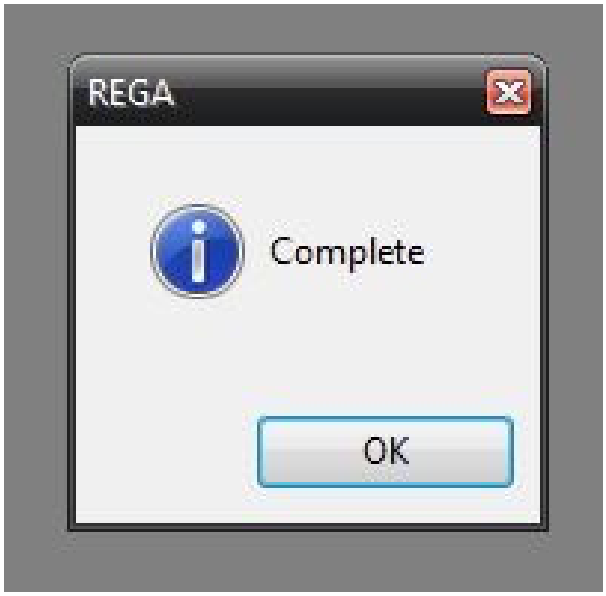

3. 레지스트리 내용을 추출한 결과를 저장할 위치를 정해준다.



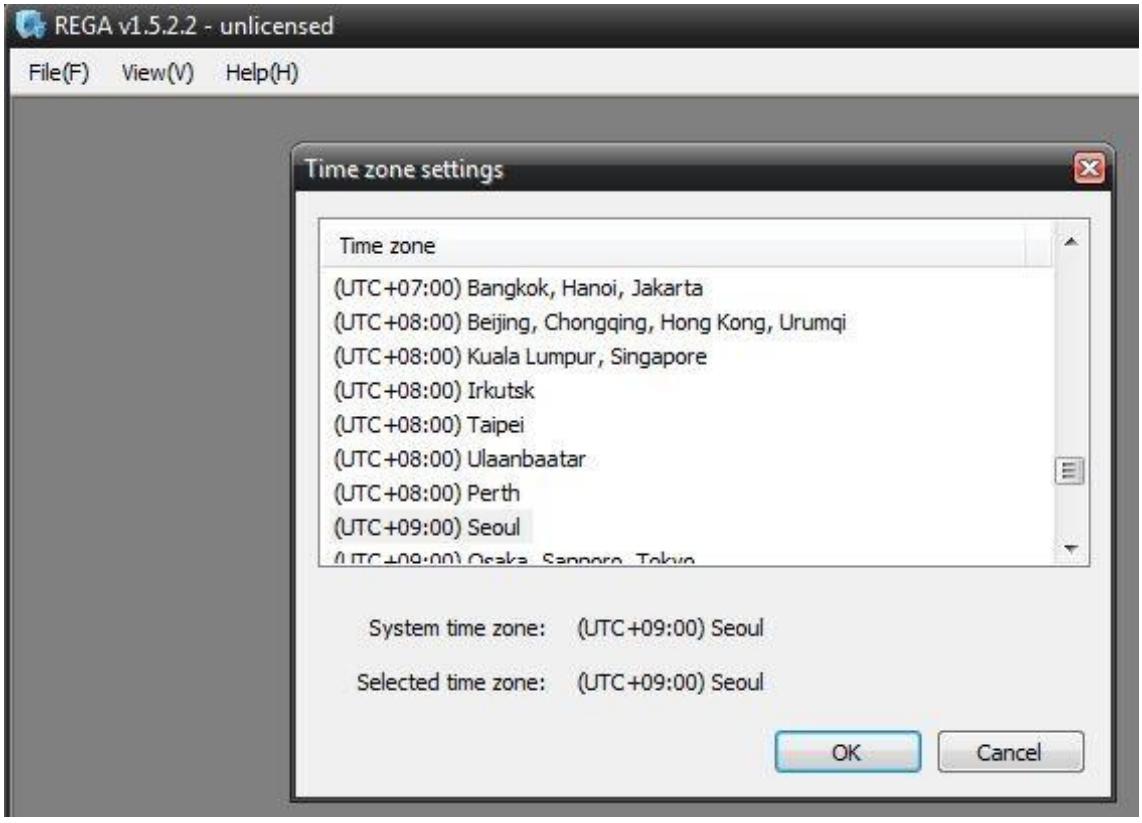

4. 레지스트리 하이브 파일들을 모은다.



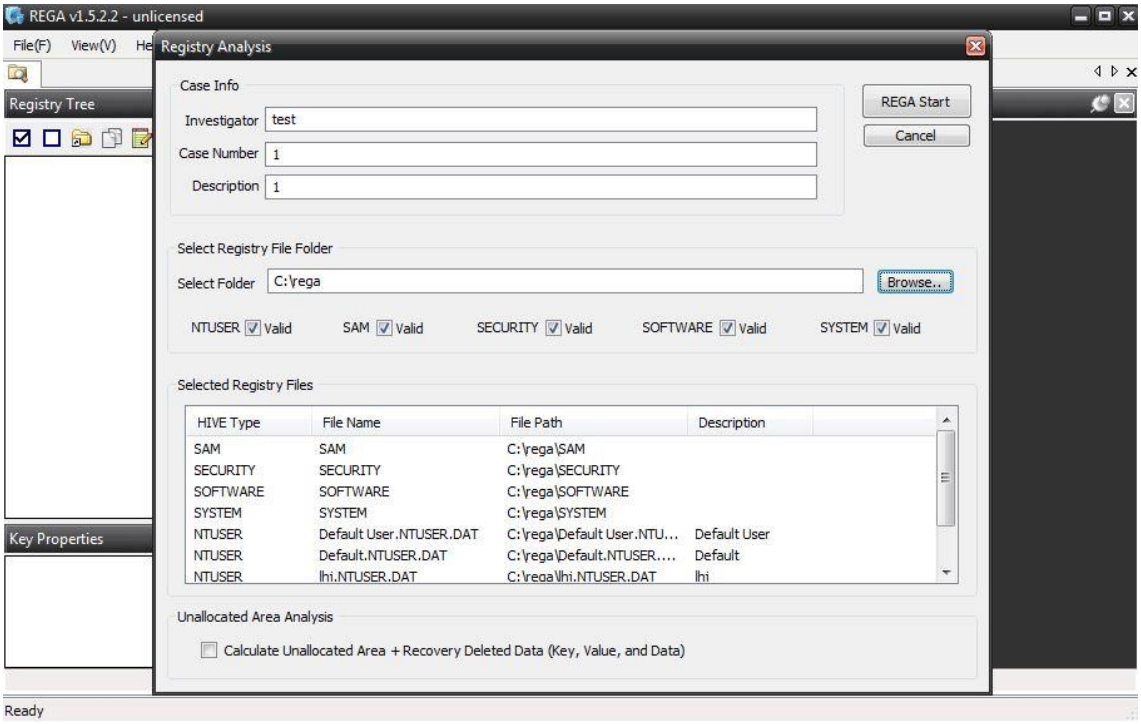

5. 다 모으고 나면 complete 를 볼 수 있다.



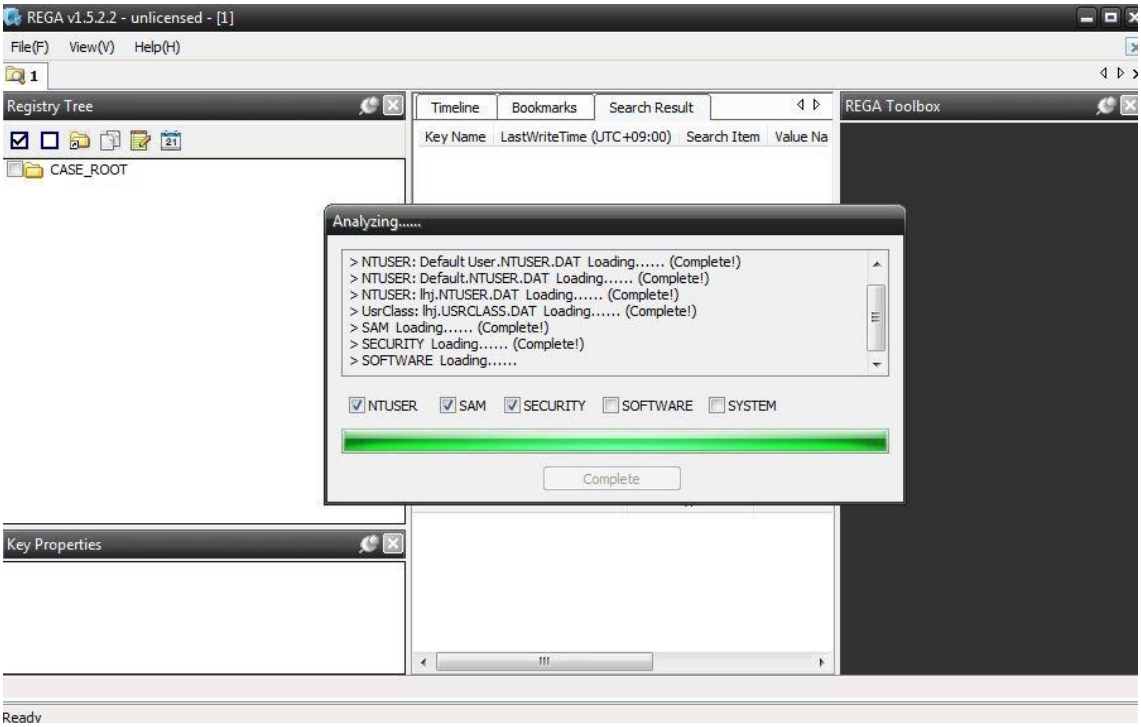

6. 그리고 Time zone settings 가 나오는데 Seoul 을 선택해준다.



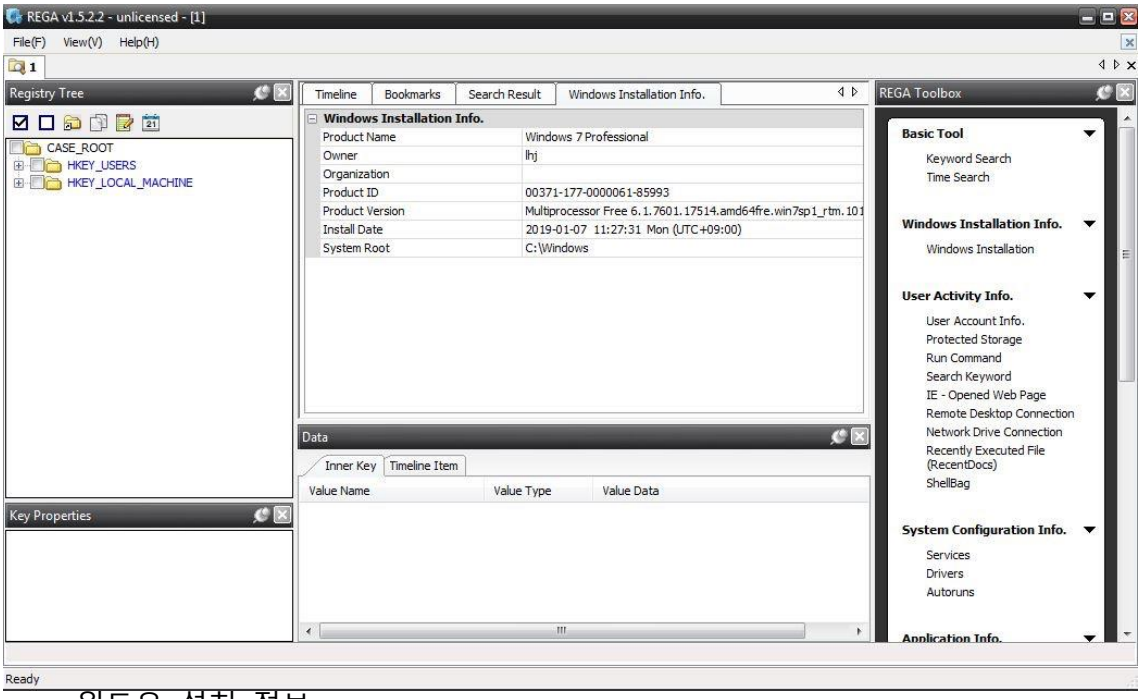

7. 저장될 정보를 설정해주고, Select Folder 에 레지스트리 하이브를 모은 폴더를 지정해준다.



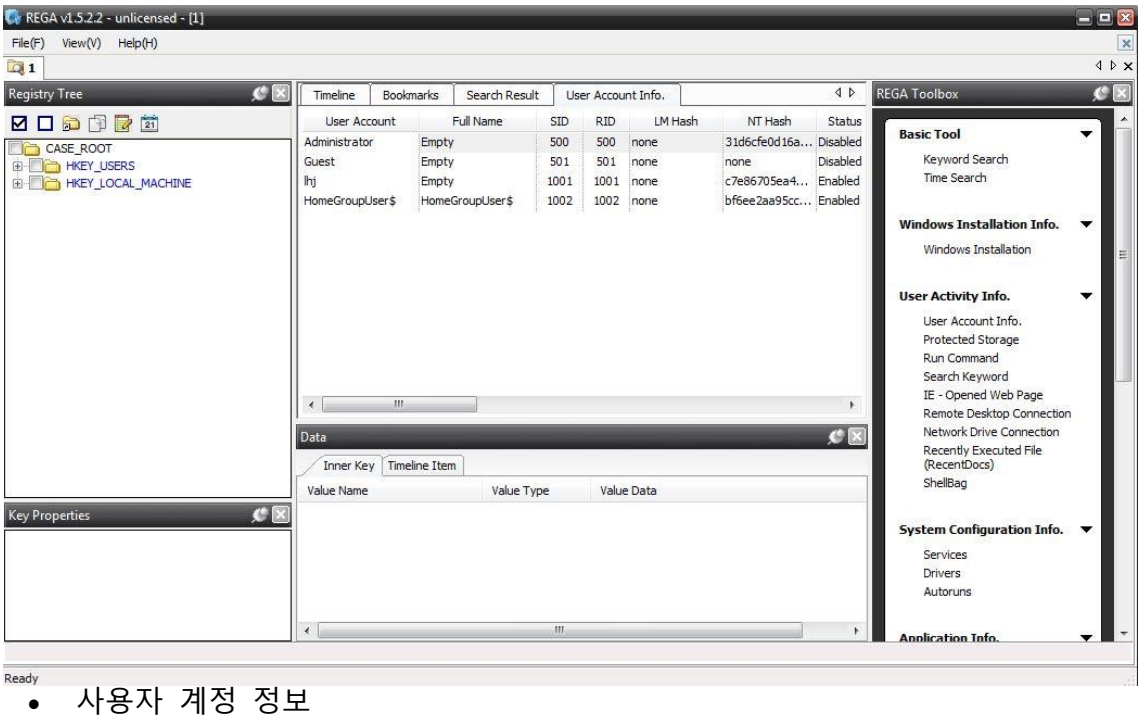

8. REGA Start 를 누르면, 다음과 같이 분석을 시작한다.



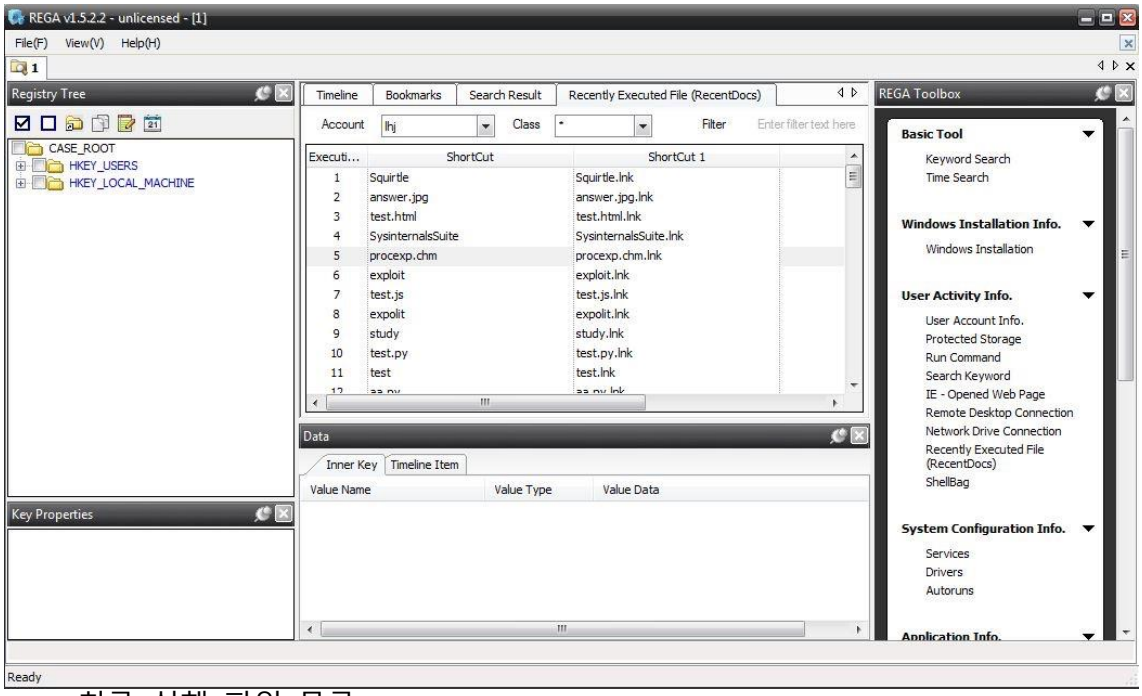

9. 분석 결과로 다음과 같은 정보들을 얻을 수 있다.



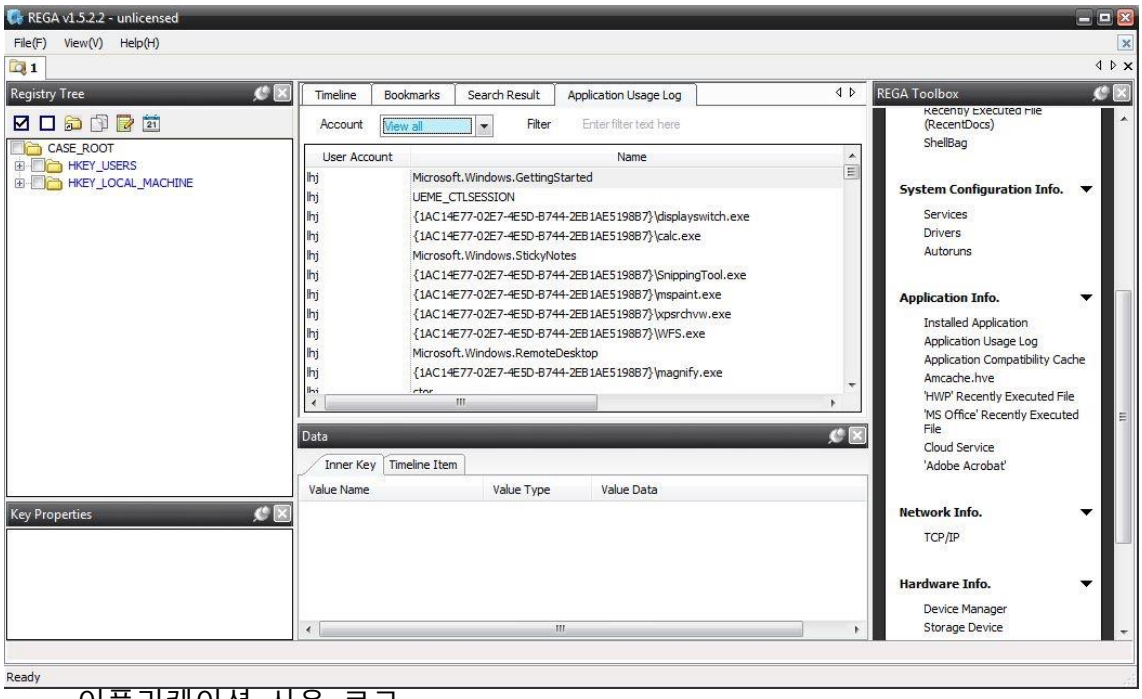

- 윈도우 설치 정보




- 사용자 계정 정보




- 최근 실행 파일 목록




- 어플리케이션 사용 로그