# 인터넷 웹브라우저에서 화면캡쳐한 파일의 무결성에 관한 연구

이종구
고려대학교 컴퓨터정보통신대학원 컴퓨터・정보통신학과
e-mail: ettlab@korea.ac.kr

# A Study on Integrity of screenshot-file on Internet Web Browser

Jong-Koo Lee
Dept of Computer & Information Technology,
Graduate School of Computer & Information Technology, Korea University

요 약

일반적인 사이버 범죄 중에서 포탈사이트 게시판에 명예를 훼손할 목적으로 글을 올린 경우를 생각해보자. 인터넷 웹브라우저 내용을 출력하거나 화면캡쳐 도구를 이용하여 생성한 파일은 웹브라우저 내용을 클라이언트가 임의로 수정하여 출력하거나 화면캡쳐 파일을 수정할 가능성이 존재하고 무결성 보장이 힘들다. 본 논문에서는 실제 내컴퓨터의 모니터에서 보이는 화면은 얼마든지 조작이 가능함을 예를 들어 보일 것이며 화면캡쳐 파일의 무결성 보장을 위한 시스템을 제시하려고 한다.

## 1. 서론

일반적인 사이버 범죄 중에서 포탈사이트의 자유게시판에 누군가의 명예를 훼손할 목적으로 글을 올린 경우를 생각해보자. 명예훼손을 당한 사람이 해당 포탈사이트에서 우연히 자신을 비난하는 내용을 쓴 게시글을 확인하고 비난하는 사람을 상대로 명예훼손죄로 고발하는 일이 있다고 하자. 고발하기 전에 해야 할 일 중에는 해당 포탈사이트의 게시글을 컴퓨터 프린터를 이용해서 게시물 내용을 출력하던지, 컴퓨터 모니터 화면을 카메라를 이용해서 찍던지, 컴퓨터에서 지원하는 화면캡쳐 프로그램을 이용해서 저장을 해야만 할 것이다. 또한 포탈사이트 운영자에게 게시판 글의 내용을 보존해 줄 것을 요청할 수 도 있다.

명예훼손을 한 사람이 포탈게시판에서 자신이 쓴 글을 지우고 고소자(명예훼손을 당한 사람)가 제시하는 증거가 조작된 것이라고 주장한다면 해당 게시물의 인쇄물, 화면캡쳐 파일, 카메라로 찍은 사진 등이 증거로써의 가치가 있겠는가? 설상가상으로 해당 포탈사이트에서 게시글의 내용을 지운상태이며 포탈사이트에서 게시글의 복구가 힘든 경우라면 증거 자료로 사용될 수 있겠는가?

본 논문에서는 실제 몇 가지 기술을 이용하면 내컴퓨터의 모니터에서 보이는 화면은 얼마든지 조작이 가능하다는 것을 제시할 것이며 화면캡쳐한 파일의 무결성 보장을 위한 방법을 제시하려고 한다.

## 2. 관련연구 및 문제점

### 2.1 데이터의 무결성을 보장하는 방법

무결성이란 비인가된 주체에 의하여 정보가 추가, 수정, 삭제되지 않음을 의미하며 무결성 보장이란 변경되지 않음을 보장하는 것으로, 정보의 정확성 및 완전성을 보호하는 것을 의미한다. 본 논문에서는 해쉬알고리즘을 이용한 파일의 무결성 보장에 대해서만 논하기로 하겠다.

### 2.2 전자서명

전자서명의 검증은 공개키를 이용하여 서명값을 푼 값과 문서에 대한 해쉬 값이 같은지를 비교하는 방법을 사용한다. 전자서명은 서명자가 누구인지를 알 수 있는 것 외에 여러 가지 효력을 갖지만 효력을 갖추기 위한 5가지 조건들(위조불가, 서명자 인증, 부인불가, 변경불가, 재상용 불가
)을 만족할 때에만 전자서명으로써의 효력을 가진다.[1] 전자서명의 조건들 중 위조불가, 변경불가의 조건들에 적용하는 해시값 비교 방법을 본 논문의 무결성 검증 방법으로 이용할 것이다.

### 2.3 공인인증기관과 공인인증 과정

공인인증기관은 사용자의 전자서명 검증키에 대한 무결성 보장과 신분정보의 표시를 위한 인증서발급

서비스를 제공한다.[2]

본 논문에서 제시하는 웹화면캡쳐 파일의 무결성 검증을 위한 인증서버는 공인인증기관이 갖춰야 할 여러 가지 법적인 규정을 만족하지 않으며 화면캡쳐 파일의 무결성 검증을 위한 검증서버로의 역할만 한다.

### 2.4 YBM시사닷컴 사이트의 토익점수 확인과정

YBM시사닷컴 사이트에서 토익점수 확인 방법은 온라인발급 원본 대조 방법과 원본 대조 프로그램을 통한 검증 방법의 두 가지가 있다. 온라인발급원본 대조 방법은 수험번호와 발급번호를 입력하여 원본 대조를 통해서 위·변조 여부를 육안으로 확인하는 것이다. 원본대조 프로그램을 통한 검증 방법은 발급문서의 스캔 및 원본문서 복원을 통한 위·변조 검증 방법이며 문서의 위·변조 내용을 육안확인하고 행정전자서명으로 검증한다.

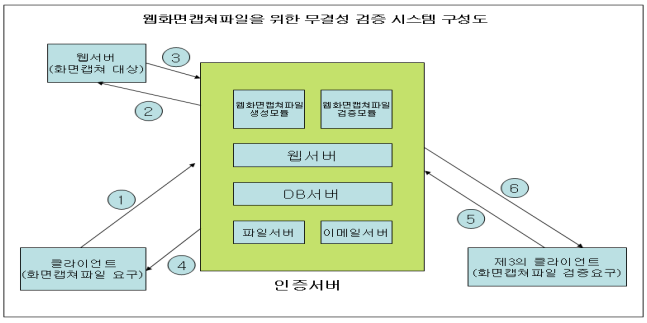
본 논문에서는 온라인발급원본 대조 방법을 이용하여 웹브라우저를 통한 화면캡쳐 파일의 무결성을 검증하는 방법으로 이용할 것이다.

### 2.5 SHA-2

현재 SHA-1(Secure Hash Algorithm)이 많은 보안 프로토콜과 프로그램에 사용되고 있다. 하지만 2004년 SHA-1의 취약점 가능성이 제기되었으며[3] 2005년 2월 실제로 SHA-1의 취약점이 공개되었다.[4] 미국 NIST 에서는 SHA-2를 사용하기를 권장하고 있으며 새로운 해시함수인 SHA-3을 개발 중이다.[5] 본 논문에서는 SHA-2 해시함수를 이용하여 화면캡쳐 파일의 무결성을 검증하려 한다.

## 3. 본론

### 3.1 웹화면캡쳐파일을 위한 무결성 검증 시스템 구성도




### 3.2 웹화면캡쳐파일의 무결성 검증 시나리오

1. 클라이언트가 인증서버에 로그인 한 후 화면캡쳐를 원하는 웹사이트 주소를 입력하고 화면캡쳐를 요청한다.
2. 사이트 주소를 입력받은 인증서버가 클라이어트가 화면캡쳐하기를 원하는 웹서버에 화면캡쳐 모듈을 통해서 접속한다.
3. 클라이언트에 의해서 요청받은 화면캡쳐대상사이트에 인증서버가 화면캡쳐파일 생성모듈을 이용하여 화면캡쳐하여 파일을 생성하고 인증서버의 DB에 필요한 데이터를 저장한다. 이때 생성된 화면캡쳐파일의 SHA-2 해쉬값이 인증서버의 DB에 저장되어 나중에 파일의 검증에 이용된다.
4. 화면캡쳐파일생성과 DB서버에 데이터 저장이 완료된 후 클라이언트에서 이메일 주소로 해당 화면캡쳐 파일을 첨부하고 검증에 필요한 데이터를 같이 전송해 준다. 4단계까지 클라이언트가 요구한 화면캡쳐파일의 생성과 검증에 필요한 데이터가 DB서버에 저장이 된다.
5. 제3의 클라이언트가 이전에 제시한 클라이언트의 화면캡쳐 파일에 대한 무결성 검증을 원할 경우 인증서버에 접속하여 로그인 한 후 무결성 확인을 위한 인터넷사이트 주소와 검증키 값을 인증서버에 입력한다.
6. 인증서버는 제3의 클라이언트가 입력한 인터넷사이트주소와 검증키 값이 일치하는 경우 해당 클라이언트에게 기존화면캡쳐파일의 원본과 해당 해쉬값을 제공해 준다. 클라이언트는 제공받은 파일과 해쉬값을 기존 화면캡쳐파일의 내용과 해쉬값을 비교해서 무결성을 검증할 수 있다.

## 4. 결론

컴퓨터 모니터에서 인터넷 웹브라우저의 내용을 증거로 남기는 방법은 해당 사용자의 컴퓨터의 모니터에 보이는 화면이 아닌 객관적으로 인증 받을 수 있는 인증서버를 통해 해당 게시물을 화면캡쳐하여 저장하는 것이다.

즉 공인인증센터의 인증기관과 같은 개념의 공인된 인증서버을 통해서 화면캡쳐를 함으로써 개인 컴퓨터에서 화면캡쳐 도구를 이용하거나 모니터를 카메라로 찍던지 출력하는 방법의 한계를 극복할 수 있다.

## 참고문헌

[1] 김현철, “전자서명과 인증”, 전자공학회지, 제30권 제6호, P595, 2003.6.

[2] KISA의 “전자서명 홍보용 교재 알기쉬운 전자서명” p16, http://www.kisa.or.kr/kisa/kcac/down/banner_01/easycert_1.pdf

[3] Xiaoyun Wang,“Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD”, August 17, 2004, http://eprint.iacr.org/2004/199

[4] Xiaoyun Wang, “Collision Search Attacks on SHA1”, February 13, 2005, http://theory.csail.mit.edu/~yiqun/shanote.pdf

[5] http://csrc.nist.gov/groups/ST/hash/timeline.html