KIPS Tr. Comp. and Comm. Sys.
Vol.6, No.1 pp.9~16 pISSN: 2287-5891

https://doi.org/10.3745/KTCCS.2017.6.1.9

Screen Capture Authentication System for Web Postings to Used as Digital Evidence

Ju Young Kang† · Sang Jin Lee††

ABSTRACT

In modern society, everyone can easily access the Internet and freely express their opinions or ideas on Web bulletin boards or SNS. At the same time, they are often used as a place of slandering and the spreading of false information about celebrities such as entertainers and politicians. Typically people use the screen capture method to submit web posts as evidence in lawsuits. But it is difficult to get these accepted as evidence in court because screen captured images are easily forged and tempered. Therefore, as described above, using “Proxy Browser”, we propose a screen capture authentication system for web posts that protects forging and tempering to use as digital evidence in court.

Keywords : Digital Evidence, Authentication System, Screen Capture, Authentication for Web Postings

디지털 증거 활용을 위한 웹 게시물 화면캡쳐 인증 시스템

강 주 영† · 이 상 진††

요 약

현대 사회에서는 누구나 쉽게 인터넷에 접근할 수 있으며, 웹 게시판이나 SNS 등에 자신의 의견 또는 사상을 자유롭게 표현한다. 하지만 그에 반해 연예인 또는 정치인 등 유명인사에 대한 비방이나 허위사실을 유포 하는 곳으로 이용되기도 한다. 일반적으로 웹 게시물을 증거로 제출하기 위해 화면캡쳐 방식을 많이 사용하는데 디지털 정보인 화면캡쳐 이미지는 위변조의 용이성, 진정성 등 증거능력 한계로 인해 법정에서 증거로 인정받기 어려움 점이 있다. 따라서 위와 같은 사례를 착안하여 웹 게시물 화면캡쳐 이미지를 법정에서 디지털 증거로 인정받기 위해 위변조가 어려운 Proxy Browser를 사용하여 웹 게시물 화면캡쳐 인증 시스템을 제안하고자 한다.

키워드 : 디지털 증거, 인증 시스템, 화면캡쳐, 웹 게시물 인증

1. 서 론

오늘날 인터넷이 급속하게 보급되어 실생활에서 폭넓게 사용되고 있다. 다양한 연령대가 사용하면서 각 계층에 따라 주로 사용하는 용도가 다양하기 때문에 인터넷에 올라오는 게시글 또는 사진 등이 개인이나 특정 집단의 이익을 위해 사실이 왜곡된 글이나 사진 등이 올라오기도 한다.

인터넷 등 정보통신 수단이 보편화되면서 선거에 있어서도 정당·후보자측이 선거운동의 한 방법으로 사이버공간을 적극 활용하고 있는 추세이다. 특히, 정치인에 대한 허위사실 유포나 비방은 선거기간이라는 상대적으로 짧은 기간 동안에 큰 파급력을 발휘한다.

2011년 12월 29일 헌법재판소는 공직선거법 제93조 1항이 인터넷, UCC, SNS에도 적용되는 것으로 해석하는 것은 위헌이라는 한정위헌(限定違憲) 결정을 내림으로써 SNS를 통한 선거운동을 전면적으로 허용하였다. 선거관리위원회(이하 선관위)는 이 결정의 취지를 반영하여 SNS를 통한 선거운동을 상시 허용한다는 방침을 세워 SNS를 통한 정치적 의사표현과 온라인 선거운동을 보다 활성화시켰다[1].

이 역효과로 특정 집단 또는 일부 네티즌들이 온라인상에서 후보자를 비방·흑색선전하거나 허위사실을 웹 게시물로 유포하는 등 선거법 위반행위가 지속적으로 발생되고 있으며 이는 사회적으로 문제가 되고 있다[2].

하지만 웹 게시물은 디지털 정보의 특성을 가지고 있어 신고자가 단순히 웹 게시물을 화면캡쳐한 자료만을 가지고

† 정 회 원 : 고려대학교 정보보호대학원 정보보호학과 석사과정
†† 종신회원 : 고려대학교 정보보호대학원 교수
Manuscript Received : June 15, 2016
First Revision : August 5, 2016
Second Revision : September 23, 2016
Accepted : November 18, 2016
* Corresponding Author : Sang Jin Lee(sangjin@korea.ac.kr)

법적증거 능력을 갖추기 어렵다. 이에 본 논문에서 웹 게시물을 디지털 증거로 활용하기 위한 시스템을 제안하고 유사 서비스와 차이점을 비교한다.

2. 웹 게시물의 특성과 증거 능력

2.1 증거능력

증거 능력이란 사실 입증 자료가 증거로서 채택되어 법률상의 자격을 가질 수 있는가의 문제로, 제출된 자료가 증거 능력이 있어야만 재판에서 주장을 뒷받침 하는데 사용될 수 있다.

국내법에는 증거와 관련된 개별법이 존재하지 않고, 형사소송법이나 민사소송법의 일부로만 증거 관련 규정을 다루고 있다. 형사소송법에 따르면 법정에서 유효한 증거가 되기 위해 갖추어야 할 조건으로 증거능력과 증명력을 들 수 있다. 증거 능력은 증거조사의 대상이 될 수 있는 일반적인 자격을 의미하며, 증명력은 실제 법정에서 해당 증거가 사실을 판단하는 데에 기여하는 정도를 의미한다. 따라서 증거가 채택되어 법정에서 주장하는 내용을 뒷받침하기 위해서는 증거능력을 가져야 한다. 국내법 하에서는 대부분의 증거에 대한 증거 능력을 인정하고, 위법수집증거배제의 원칙과 전문증거배제 원칙만을 적용한다[3].

2.2 웹 게시물의 특성

웹 게시물은 일반적으로 인터넷 게시판에 올라오는 글을 의미하나, 본 논문에서는 웹 게시물의 범위를 다수가 인터넷을 통해 확인할 수 있는 게시물까지 그 범위를 확대한다. 따라서 카카오톡 등 메신저 앱(App) 대화방 등에 올라오는 대화 및 이미지 등을 포함한다.

또한, 웹 사이트의 운영방식에 따라 웹 게시물의 접근 방식도 크게 3가지 형태로 나눌 수 있다. 첫째 회원 가입과 회원 인증을 거친 후 게시물에 접근하는 방법, 둘째 회원 가입 후 일정 등급 이상의 권한을 부여 받아야 접근 할 수 있는 게시물, 셋째 인증없이 누구나 접근 가능한 게시물 등이 있다.

첫째와 둘째 경우에는 게시물의 접근이 일정부분 제한된다고 볼 수 있으나, 디지털 정보인 웹 게시물 또한 복사가 용이하기 때문에 공개 그룹뿐만 아니라 폐쇄 그룹의 웹 게시물도 해당 그룹의 사용자가 타 사이트로 퍼나르기를 통해 누구나 접근 가능한 공개 게시물로 바뀔 수 있다.

예를 들어 포털사이트의 카페나 페이스북 그룹처럼 특정 인원만 접근 가능한 게시물을 해당 폐쇄 그룹(Closed group)의 멤버가 퍼나르기 등을 통해 공개 사이트로 해당 게시물을 복제하여 원글 작성자가 의도하지 않은 사람들까지 공개되어지는 경우가 생김으로써 큰 파급력을 가진다. 특히, 정치적 이슈나 연예인 사생활 등 악성루머, 허위사실 및 유언비어 유포 등의 매개체로 변질되기도 한다.

이러한 웹 게시물의 특성을 살펴보면 첫 번째 디지털 데이터로서 변조가능성이 있고 두 번째 웹 사이트에 게시되어 다수가 접근이 가능하고 세 번째 작성 후 수정이 가능하여 처음 작성한 내용과 다를 수 있으며 글 작성자 이외에도 해당 사이트의 권한을 가진 자에 의해 수정 및 삭제가 가능하다.

따라서 웹 게시물은 디지털 정보로써 수정 삭제가 용이하며 경우에 따라서 일시적으로 존재하는 휘발성 데이터로 분류할 수 있다. 이러한 디지털 데이터를 증거로 사용하기 위해 게시물이 삭제되기 전 화면캡쳐 및 서버의 데이터 백업을 통해 원본을 보존하는 방법이 가장 효과적이다.

하지만 일반인이 서버의 데이터 백업을 통해 원본을 보존하는 방법은 매우 어렵기 때문에 일반적으로 화면캡쳐 방식을 선호한다.

2.3 웹 게시물이 법적 증거능력을 갖추기 위한 요소

앞서 서술한 내용대로 국내법에는 증거와 관련된 개별법이 존재하지 않고, 형사소송법이나 민사소송법의 일부로만 증거 관련 규정을 다루고 있다. 비교법적 차원에서 미국의 연방증거규칙(Federal Rules of Evidence, 이하 FRE)[4]을 살펴보면 디지털 증거로 논의되고 있는 유형은 이메일이나 문자메시지 등 전자적 통신뿐만 아니라 디지털 사진, 웹사이트 게시물, 컴퓨터를 통해 작성된 데이터 및 저장된 기록 등이 포함된다. 연방증거규칙(FRE)는 디지털 증거의 허용성에 대한 다음 다섯 가지 기준을 제시하였다.

첫째, 디지털 증거의 관련성(FRE 401[5]), 둘째, 디지털 증거의 진정성을 증명하여야 하며, 셋째, 전문법칙에 해당하는 것인지, 넷째 원본제출원칙에 부합하는지, 마지막으로 디지털 증거의 증거적 가치(Probative value)보다 불공정한 편견(FRE 403[6]) 등의 위험이 더 큰지 여부 등이다. 여기서 웹 게시물의 화면캡쳐 이미지와 해당 게시물의 Site URL, ID, IP, 이미지 해쉬값 등(이하 부가정보)을 법정에서 증거능력이 있는 디지털 증거로 활용되려면 무엇보다 진정성과 전문증거배제원칙이 고려되어야 할 것이다.

웹상에서의 특정인에 대한 허위사실, 명예훼손 및 유언비어 유포 등 위법 게시물을 올리는 경우가 많다. 하지만 단순히 화면캡쳐로서 신고자가 캡쳐한 화면을 신뢰할 수 있을까? 또한 신고자가 화면캡쳐 이미지를 위변조 후 신고한 경우도 있을 수 있다. 이처럼 디지털 증거의 특성으로 인하여 상황에 따라 신고자를 신뢰할 수 없는 경우가 발생할 수 있다. 따라서 본 논문에서 제안하고자 하는 시스템은 인터넷상 위법 게시물을 사용자가 간편하게 신고・제보할 수 있게 하고 신뢰할 수 있는 제3의 인증기관이 해당 위법 게시물을 직접 화면캡쳐 하여 해당 시점을 인증・보관 후 수사기관 조사 단계에 자료 제출 및 검증을 제공할 수 있도록 설계하였다.

3. 유사서비스 소개 및 차이점

3.1 전자공증 서비스

전자공증은 전자(화)문서에 대해 전자적 방식으로 공증을 해주는 제도이며 사인(私人) 작성의 전자(화)문서에 대하여 인증을 부여하는 '전자(화)문서인증'과 사인(私人)작성의 전자문서에 대하여 확정일자를 부여하는 '일자정보제공' 등이

있다. 법무부에서 제공하고 있는 전자공증은 정관인증, 사서인증, 의사록인증, 확정일자 등에 대해 촉탁을 할 수 있다. 하지만 본 논문에서 다루는 인터넷상 게시물에 관한 화면캡쳐 디지털 데이터는 국내의 전자공증 시스템이 공증하는 내용의 범위를 넘어선다. 다음으로 전자공증 서비스를 시행하고 있는 미국과 일본의 사례를 알아본다.

1) Digistamp (미국)

1998년에 설립되어 금융・보험・연구 등의 분야에서 전자문서에 대해 e-TimeStamp라는 시점확인토큰(Time-Stamp Token, TST) 서비스를 제공하며 서비스 절차는 다음과 같다[7]. 촉탁인은 시점확인토큰 발급 소트웨어를 이용, 전자문서에 대한 해쉬값을 생성하여 공증인의 역할을 수행하는 시점확인센터에 전송 한다.

시점확인센터는 전송된 전자문서의 해쉬값에 신뢰시각정보를 부여하고, 해당 메시지에 전자서명을 함으로써 시점확인토큰을 생성하고 생성된 시점확인토큰을 촉탁인에게 전달한다.

2) Surety (미국)

Surety는 해쉬체인방식과 시점확인 기술을 이용하여 전자문서에 대한 공증서비스를 제공한다[8]. AbsoluteProof라는 전자공증서비스(시점확인서비스)를 다양한 전자문서에 대해 제공하나 전자문서가 이미 생산되어 PC에 저장되어진 파일에만 적용이 가능하다. 서비스 절차는 다음과 같다.

촉탁인은 시점확인토큰 발급 소프트웨어를 이용, 전자문서에 대한 해쉬값을 생성하여 공증인의 역할을 수행하는 시점확인센터에 전송하고 전송된 전자문서의 해쉬값과 이를 이용하여 센터에서 생성한 시점확인토큰 값, 센터의 새로운 해쉬값 등의 정보를 결합하여 “Surety Integrity Seal”이라는 타임스탬프 토큰을 생성한다.

3) J-Notary (일본)

2000년에 설립되어 dPROVE라는 전자파일 인증서비스를 제공하며, 전자문서의 보관, 공유 서비스도 제공한다[9]. 인증서비스는 공증 종류 중 사서증서 인증에 관한 서비스만 제공하며 서비스 절차는 다음과 같다.

촉탁인이 dPROVE 시스템에 전자문서의 등록을 요청하면, dPROVE 시스템은 촉탁인에게 등록ID를 발급하며 촉탁인은 이해관계인에게 전자문서 및 등록 ID를 전자메일로 전송, 이해관계인은 dPROVE 시스템에 전자문서에 대한 인증을 요청한다. dPROVE 시스템은 이해관계인의 신원 확인 후, 인증서를 송부한다.

4) SecureSeal (일본)

NTT DATA社가 전자문서 등에 대해 10년 이상의 장기 증명서비스를 제공하는 일본 최초의 시점확인서비스로 절차는 다음과 같다[10]. 촉탁인은 전자문서의 해쉬값을 생성하고 이를 시점확인센터로 송부한다. 시점확인센터는 시점확인토큰을 생성하여 이를 촉탁인에게 전달한다.

미국과 일본의 해외 사례에서도 이미 생산된 전자문서 파일을 대상으로 시점 인증서비스를 제공하며 온라인상의 웹 게시물에 대한 화면캡쳐 공증・인증 서비스를 제공하는 기관은 아직 없다.

3.2 시점인증 서비스

1) Archive.org

비영리단체인 “인터넷 아카이브 디지털 라이브러리”에서 서비스하는 사이트로 Wayback Machine이라는 웹크롤러가 인터넷상 웹 사이트를 탐색하여 특정 시점의 웹페이지를 저장하고 있다[11]. 해당 사이트의 특징은 자신의 원하는 사이트의 특정 시점을 사용자가 지정할 수 없으며, 자바스크립트, 깨진 이미지 등 웹표준을 지키지 않은 사이트는 제대로 표현이 안되는 문제점과 크롤링 대상 사이트가 웹봇 환경설정 파일인 robots.txt에서 Wayback Machine을 거부할 경우 수집을 못하는 단점이 있다.

또한, 대상 사이트에 ID와 Password 방식 등의 웹 인증 페이지가 있을 경우 Wayback Machine의 접근자체가 불가능하여 사용자가 원하는 웹 페이지를 보여주지 못하는 경우가 많다.

2) Proof.com

프랑스 회사인 CYBERTOINC에서 운영하는 사이트로 사용자가 원하는 디지털 정보에 대한 시점인증(Time stamping) 서비스를 제공한다. 해당 사이트에서는 사용자가 원하는 디지털 문서나 텍스트 내용 및 화면캡쳐 등과 같은 디지털 정보에 대해 자체 타임스탬프 기능을 이용하여 시점 인증할 수 있는 서비스를 제공한다. 타임스탬프는 SHA256 알고리즘, 타원곡선전자서명 알고리즘(ECDSA) 등을 사용하여 검증한다[12]. 사용자는 원하는 디지털 정보를 해당 사이트에서 시점 인증을 받은 후 발급 받은 해쉬값을 가지고 검증을 요구하는 사용자에게 알려준 뒤, 검증을 요구하는 사용자가 직접 해당 해쉬값을 사이트에 입력하면 특정시점의 디지털 정보가 저장되어 있는 것을 검증 받을 수 있다.

3) ScreenSTAMP

ScreenSTAMP는 사용자가 원하는 특정 웹사이트의 페이지를 ScreenSTAMP의 시스템을 이용하여 화면캡처한 후 타임스탬프를 찍어 시점인증을 해주는 서비스이다. 앞서 살펴본 Proof.com의 서비스와 유사한 서비스 형태로 화면캡쳐 1회당 1달러의 서비스요금을 부과하며 미국에서 서비스를 운영중이다. 하지만 웹 사이트의 인증 페이지가 있는 경우나 클라이언트 IP인증 등의 경우에는 화면캡쳐를 할 수 없는 단점이 존재한다[13].

4) 국립과학수사연구원 DAS

DAS(Digital Authentication System)는 국립과학수사연구원에서 서비스하는 디지털인증시스템이다. 스마트폰을 사용

하여 현장에서 채증 증거물이 해당 시점에 있었다는 것을 증명하기 위해 DAS앱을 통해 사진을 찍으면 디지털 증거물 인증센터에서 사용자ID, 인증ID 및 워터마크 등을 통해 현장에서 찍은 디지털 사진 데이터를 검증하여 해당 시점에 현장에서 찍은 사진임을 확인하는 디지털 파일 인증서를 발급해주는 서비스이다[14].

또한, 현장 채증 이외에도 기 수집된 증거물을 통해 PC에서 디지털 데이터 무결성 인증을 요청할 수 있다. 하지만 화면캡처의 경우 해당 시스템이 제3자의 관점에서 사용자가 원하는 URL등을 직접 접근하지 않기 때문에 사용자가 직접 캡처하여 DAS 시스템을 통해 셀프 인증을 받아야 되는 단점이 존재한다. 이 경우 화면캡처 파일이 이미 조작된 상태에서 인증받을 수 있는 가능성이 존재하므로 향후 법적 증거능력을 의심받을 수 있다.

3.3 제안시스템의 주요 기능

웹 게시물을 디지털 증거화할 수 있는 유사한 서비스를 살펴보았다. 디지털 증거인 웹 게시물이 법적 증거능력을 갖추기 위해 필요한 요건인 진정성, 신뢰성 및 무결성 등을 충족시키는 주요기능을 살펴보면 Table 1과 같다.

먼저 URL access capture 기능을 살펴보면 사용자가 특정 사이트 게시물의 전체 URL를 입력하여 특정 게시물에 직접 접근하여 화면캡처할 수 있는 기능이다. 유사서비스로 소개한 내용중에 URL 단위로 화면캡처를 지원하나 몇몇 서비스는 사용자가 원하는 특정 URL을 직접 입력받아 화면캡처 하는 기능이 없어 사용자가 원하는 특정 페이지를 화면캡처하기 어렵다.

Specific time capture 기능은 사용자가 원하는 시점의 시간에 해당 화면을 캡처하여 디지털 증거화 할 수 있도록 하는 기능이다. 유사서비스로 소개한 특정 서비스는 해당 기능을 제공하지 못하며 특정한 날짜와 시간에 해당하는 기록만 열람할 수 있다.

Closed group capture 기능은 네이버・다음 등 포털사이트의 카페 게시글 또는 페이스북 그룹 게시물 등 로그인이후 권한에 따라 접근 가능한 페이지를 캡처할 수 있는 기능으로 기존서비스는 보통 URL등만 입력받아서 서비스 서버에서 해당URL로 접근하여 화면캡처 기능을 제공하는데 로그인이 필요한 URL에 접근하면 제3의 서버에서는 사용자의 ID/Password를 입력받지 못하기 때문에 로그인이 필요한 페이지를 캡처할 수 없다. 제안하는 서비스는 사용자가 직접 로그인 인증 후에 권한을 부여받아 사용자의 브라우저를 통해 접근하므로 로그인이 필요한 게시물에 접근이 가능하다. 유사 서비스 중에 해당 기능을 완벽히 제공하는 서비스는 제안 서비스가 유일하다.

Table 1. Description of Functions

Functions	Description
URL access capture	사용자가 원하는 URL를 입력하여 화면캡처를 수행할 수 있는 기능
Specific time capture	사용자가 원하는 특정시점에 화면캡처를 수행할 수 있는 기능
Closed group capture	폐쇄 그룹(Closed Group)에 접근하여 화면캡처를 수행 할 수 있는 기능
Protection of image tamper	사용자가 캡처대상 화면(이미지)을 변조하지 못하도록 방지하는 기능

마지막으로 Protection of image tamper 기능으로 사용자가 처음부터 사용자단(Client side)에서 위・변조 후 웹 게시물을 인증 받는 것을 차단하는 기능으로 Proxy Browser를 통해 대상 화면의 URL에 직접 접근하여 온라인 상 현재 시점의 화면을 캡처하여 인증을 받기 때문에 웹 게시물의 위·변조가 어렵다. 위에서 소개한 기능을 기준으로 기존 유사서비스와 차이점을 Table 2에 비교하였다.

4. 웹 게시물 수집・인증 시스템 설계

4.1 웹 게시물 수집・인증 시스템 구성요소

1) 사용자(신고자)

사용자(신고자)는 인터넷상의 위법 게시물에 대한 신고(공증)를 요청하는 사용자이다. 사용자는 인터넷 서핑 중 웹 게시물 또는 허위사실 유포 및 명예훼손 등 위법 게시물을 발견했을 경우 웹브라우저 플러그인(Plug-in) 형태의 소프트웨어를 설치한 후 사용자가 발견한 화면 자체를 보이는 그대로 신고할 수 있다.

Table 2. Comparison of Services

Services	Archive.org	Proof.com	ScreenSTAMP	DAS	Proposed system
URL Access Capture	△	○	○	△	○
Specific time Capture	X	○	○	○	○
Closed Group Capture	X	X	X	△	○
Protection of Image Tamper	○	○	○	X	○

2) Proxy Browser

Proxy Browser는 IE, Chrome, Firefox 등과 같은 일반적으로 사용되는 웹브라우저에 설치되는 플러그인(Plug-in) 형태의 소프트웨어이다. 보통의 위법 게시물의 생성은 폐쇄형 대화방 또는 폐쇄 그룹(Closed group)등에서 최초 생성되어 대중에게 확산되는 경향이 있다. 또한 최근 포털사이트 카페나 토론방 등 대부분의 게시판은 ID/Password 형태의 사용자 인증을 요구하고 있다. 앞서 살펴본 유사 서비스들은 모두 제3의 외부 시스템에서 화면캡쳐를 수행하고 있으며 ID/Password나 사용자의 IP인증 기반 사용자인증 등을 요청하면 제3의 외부 시스템에서 위법 게시물 화면캡쳐를 할 수 없게 된다. 따라서 Proxy Browser를 이용하여 사용자인증 후 웹 게시물 화면을 사용자가 보는 그대로 캡쳐하고 해당 디지털 이미지에 대한 해쉬값을 산출한 후 원본 이미지와 해쉬값, PC정보 등을 패키지 형태로 수집·인증 시스템에 전송하는 역할을 한다. 또한 브라우저에 임베디드 형태로 설치된 Proxy Browser를 사용함으로써 사용자가 화면캡쳐 화면을 임의로 조작할 수 없도록 하여 해당 캡쳐화면의 진정성과 신뢰성을 확보하였다.

3) 수집·인증 시스템(ICEP System)

Proxy Browser는 원본 화면캡쳐 이미지를 수집·인증 시스템에 전송하고, 수집·인증 시스템은 수신한 원본 이미지에 대해 타임스탬프 값을 부여한다. 그러면 현재 단계에서 수집·인증 시스템에 존재하는 파일은 원본 이미지, 해쉬값, 원본 이미지에 대한 타임스탬프 인증서 그리고 최초 전송된 PC의 기본 정보 파일이 있다.

화면캡쳐 이미지의 무결성을 입증하기 위해 수집·인증시스템의 결과물로 위에서 언급된 파일들을 Fig. 1과 같이 하나의 화면캡쳐 증거팩(Image Capture Evidence Pack)인 ICEP 파일로 묶고 데이터베이스화 하여 신뢰할 수 있는 제3의 기관(Third Trusted Party)에 보관한다.

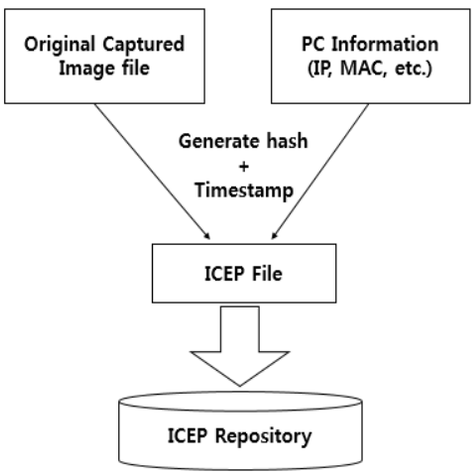


Fig. 1. Concept of ICEP

4) TTP(Trusted Third Party)

앞서 클라이언트단에서 화면캡쳐 이미지가 위·변조 되지 않았다는 것을 담보하기 위해 Proxy Browser와 수집·인증 시스템(ICEP System)의 역할을 알아보았다. 하지만 해당 수집·인증 시스템 또한 누가 어떠한 절차로 구축 운영하는가에 따라 공정성 및 신뢰성에 대한 문제가 제기될 수 있다. 따라서 수집·인증 시스템 구축 및 운영의 신뢰성과 공정성을 담보할 수 있는 기관이 필요하다.

위법 게시물의 디지털 증거를 보관하기 위한 신뢰할 수 있는 제3의 기관은 신뢰성과 진정성 유지를 고려하여 한국인터넷진흥원 등의 공공기관에서 구축 운영하는 방안을 제시한다. 인터넷상 허위사실 유포 및 명예훼손 등에 관한 신고를 받고 이를 ICEP 파일 형태로 보관하고 수사기관의 요청이 있을 시 자료제공 또는 법정 증거로 사용할 수 있도록 한다.

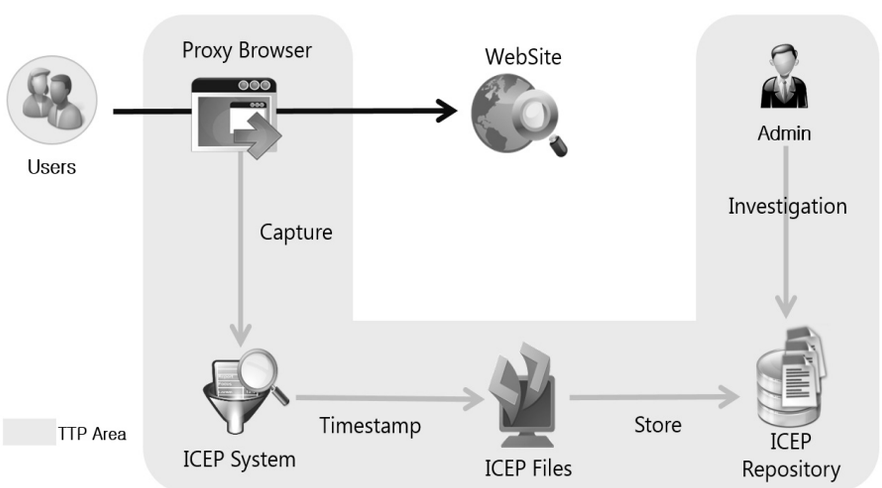


Fig. 2. System Configuration and Flow

4.2 웹 게시물 수집·인증 시스템의 작동 방식

인터넷상 위법 게시물 디지털 증거 수집 시스템의 환경 및 구조는 Fig. 2와 같다. 사용자(클라이언트)단에서 보이는 그대로의 화면을 캡쳐하는 방식이다. 로그인이 필요한 사이트 등 사용자 환경에서 볼 수 있는 화면을 그대로 전송받을 수 있는 점이 주목적이다.

먼저, 사용자는 웹 서핑을 하다가 허위사실 유포 및 명예훼손 등의 위법 게시물을 발견하면 신뢰할 수 있는 제3의 기관이 배포하는 웹 브라우저 부가 기능인 Proxy Browser를 설치하여 사용자가 직접 위법 게시물 화면을 제보·신고할 수 있다. 수집·인증시스템(ICEP System)에서는 Proxy Browser를 통해 전달받은 화면캡쳐 이미지와 사용자 PC정보를 가지고 해쉬값과 시점인증 값을 부여하여 ICEP 파일로 변환하여 ICEP 보관소에 저장한다.

ICEP 보관소에 저장된 파일을 관리자가 확인하여 위법 여부를 판단 후 적절한 조치를 취한다.

4.3 웹 게시물 수집·인증 시스템의 요구 사항

웹 게시물 수집·인증 시스템은 다음의 사항에 대해 무결성과 신뢰성을 가져야 한다.

첫째, 웹 게시물을 캡쳐하여 전송하는 과정에서 원본 웹 게시물이 Proxy Browser에 의해 조작이나 변조가 되지 않아야 하므로 웹 브라우저 및 플러그인(Plug-in) 형태인 Proxy Browser 프로그램이 악성코드나 사용자에 의해 변조되지 않아야 한다.

둘째, Fig. 2의 신뢰할 수 있는 구간(TTP Area)의 구성요소간 통신은 암호화 통신 등 신뢰할 수 있는 프로토콜을 통해 이루어져야 한다. 또한 신뢰할 수 있는 제3의 기관에서 어떠한 위·변조 행위에 대해서 무결성과 신뢰성을 확보해야 한다.

위의 요구사항들을 검증할 수 있는 다양한 체계가 확보되어야 하며 첫 번째 요구사항에 대한 검증방법으로 플러그인 프로그램에 대한 코드사이닝 및 인증서버와의 통신으로 플러그인 업데이트 확인을 통해 변조 유무를 파악할 수 있다.

두 번째 요구사항에 대한 검증방법으로 서버/클라이언트 데이터 전송 구간에 SSL 등 암호화 통신이 구현되어 있는지 확인하고 데이터베이스 서버에 저장되어 있는 웹 게시물 캡쳐 파일을 조작하지 않았다는 것을 해시값 검증 등을 통하여 무결성 및 신뢰성을 확보하여야 할 것이다.

5. Proxy Browser 구현 결과

앞서 설명한 웹 게시물 수집·인증 시스템의 핵심기능인 Proxy Browser를 프로토타입 형태로 개발함으로써, 웹 게시물 수집·인증시스템의 실제 활용 가능성을 확인하였다. 본 Proxy Browser는 구글 크롬(Chorme) 브라우저에서 확장 프로그램(Extension) 형태로 작동되는 플러그인(Plug-in)이며 크롬 브라우저가 설치되는 모든 운영체제에서 사용 가능하다.

5.1 Proxy Browser 구현

웹 게시물 수집·인증 시스템의 중요한 기능 중 하나인 이미지 변조를 막기 위해 구글 크롬(Chrome) 브라우저의 확장 프로그램(Extension) 형태로 Proxy Browser를 구현하였으며 확장 프로그램을 구글 웹 스토어에 정식으로 등록하면 사용자가 Chrome 웹 스토어를 통해 손쉽게 설치할 수 있다.

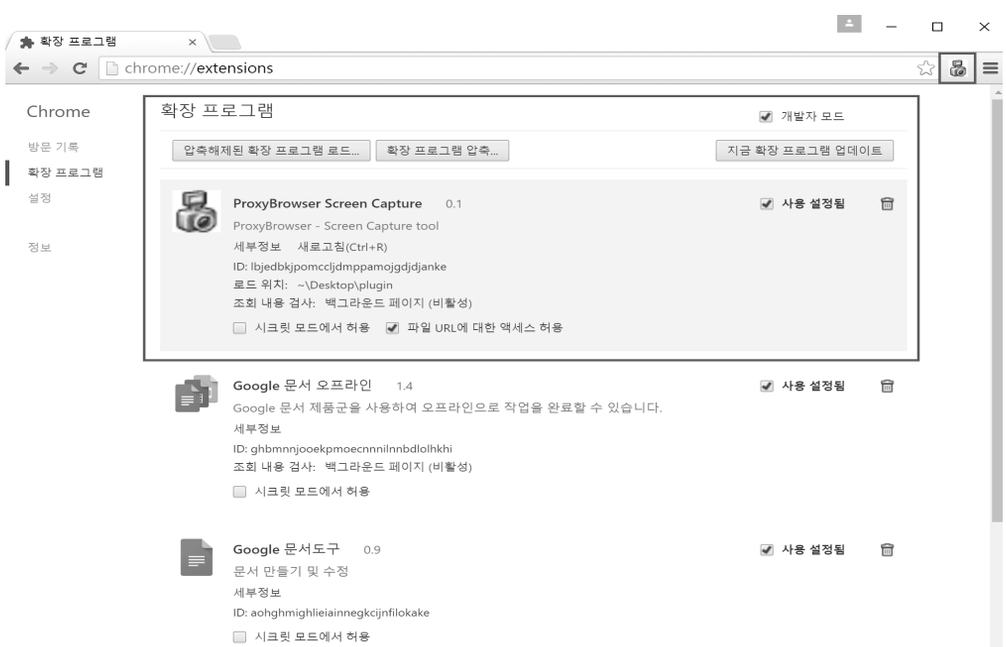


Fig. 3. Proxy Browser of Chrome Extension

Fig. 4. Screen Capture Sends to TTP

사용자가 브라우저를 통해 접속한 화면 그대로를 캡쳐하여 외부의 수집・인증시스템(ICEP System)으로 전송한다. 프로토타입에서는 인증시스템 대신 제3자가 운영 및 서비스하는 이미지 저장소로 캡쳐화면을 전송한다.

프로토타입에서는 앞서 소개한 구성요소 중 핵심기능인 Proxy Browser만 구현하여 실제 사용자 인터넷브라우저 화면에서 캡쳐하여 제3의 저장소로 전송하는 가능함을 확인하였고, 신뢰할 수 있는 제3의기관인 TTP를 선정하여 나머지 구성요소를 구현하여 디지털 증거 활용을 위한 웹 게시물 수집・인증 시스템을 구축할 수 있을 것이다.

6. 결론 및 향후 과제

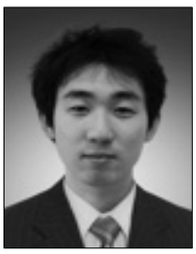
인터넷을 활용한 선거운동이 활발하게 이루어지는 현실에서 인터넷상 위법 게시물에 대한 화면캡쳐 이미지를 증거로 제출하는 사례가 증가하고 있으나, 법정에서 증거능력을 인정받지 못하고 있는 실정이며, 디지털 증거인 화면캡쳐 이미지에 대한 명확한 처리 규정이나 표준이 존재하지 않는 상황에서 화면캡쳐 파일에 대한 무결성, 진정성, 신뢰성 등과 관련된 다양한 논란이 등장할 수 있는 상황이다.

또한, 기존의 화면캡쳐 시점확인 서비스와 웹 크롤러 등의 시스템은 클로즈그룹(페이스북, 포털 카페 등)에 게시된 게시물을 수집하지 못하는 단점이 있다. 이러한 문제를 해결하기 위해 제시한 모델에서 기존의 유사시스템의 단점을 보완하고 화면캡쳐 이미지가 증거능력을 갖추고 사용자가 쉽게 이용할 수 있도록 충분히 진정성, 신뢰성 및 무결성 등을 갖추도록 설계하였다.

향후에는 본 논문에서 제시한 설계 요구사항을 반영한 시스템을 구현하여 실제 적용함으로 사용자 중심의 효율적인 웹 게시물 디지털 증거 수집・인증 시스템으로 활용될 수 있도록 우리나라 환경에 맞는 법과 제도적인 개정에 대한 연구가 필요하다.

References

[1] Public Official Election Act, Article 93, No.1 Limited unconstitutional, (2007heonma1001), 2007.
[2] 5th Simulaneous Local Elections Overview, pp.211-212, 2014.
[3] Ahreum Kim, Yeog Kim, and Sangjin Lee, “A Study on Notary System for Web Postings Digital Evidences,” *Journal of the Korea Institute of Information Security and Cryptology*, Vol.21, No.3, pp.155-165, 2011.
[4] Federal Rules of Evidence 2015 [Internet], http://federalevidence.com/downloads/rules.of.evidence.pdf.
[5] FRE401 [Internet], http://federalevidence.com/rules-of-evidence#Rule401.
[6] FRE403 [Internet], http://federalevidence.com/rules-of-evidence#Rule403.
[7] Digistamp Inc. [Internet], https://www.digistamp.com/about-us/aboutus.
[8] Surety LLC [Internet], http://www.surety.com/solutions.aspx.
[9] J-Notary Ltd [Internet], http://www.jnotary.com/service/summary.html.
[10] SecureSeal Stadnard [Internet], http://www.secureseal.jp/timestamp/about.html.
[11] Archive.org [Internet], http://archive.org/about/.
[12] PROOF.com [Internet], https://www.proof.com/privacy/.
[13] ScreenSTAMP [Internet], http://www.screenstamp.com/services.
[14] NFS DAS [Internet], http://www.mogaha.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000053473&fileSn=1.



강 주 영

e-mail : unfixed@korea.ac.kr
2011년 순천향대학교 정보보호학과(학사)
2013년~현 재 고려대학교 정보보호대학원 정보보호학과 석사과정
관심분야 : Digital Forensic, Information Security

이 상 진

e-mail : sangjin@korea.ac.kr
1987년 고려대학교 수학과(학사)
1989년 고려대학교 수학과(석사)
1994년 고려대학교 수학과(박사)
1989년~1999년 ETRI 선임연구원
1999년~현 재 고려대학교 정보보호대학원 교수
2008년~현 재 고려대학교 디지털포렌식연구센터 센터장
관심분야 : Digital Forensic, Steganography, Hash Function