# 디지털증거의 무결성 입증시 MD5 해시함수 사용에 관한 재고찰

박 재 유[1]

[1]한국과학기술원 소프트웨어대학원

# Re-thinking Old Ways : Proving the Integrity of Digital Evidence Using MD5 Hash Function

Jae-you PARK[1]

[1]Korea Advanced Institute of Science and Technology

cpuu@cs.kaist.ac.kr

요 약

디지털 증거물이 법정에서 인정되기 위해서는 무결성(無缺性, integrity)의 입증이 상당히 중요하다. 대법원의 관련 판례[7]에 따라, 실무적으로는 암호학적 해시 함수를 주로 이용하고 있으며, 대표적으로 MD5 알고리즘이 사실상의 표준으로 여겨진다. 그러나 MD5는 Wang과 Stevens 등에 의해 취약성이 드러났으며, 현재 학계에서는 결코 사용을 권장하지 않는다. 본 논문에서는 관련 연구동향을 살펴보고, 디지털포렌식 분야와 직접적으로 연관되는 문제점을 논하고, 어떠한 대응방안을 마련해야 하는지 방향성을 제시한다.

## Ⅰ. 서 론

정보통신기술은 이미 상당 부분 대중화되었고, 현대인의 일상에서 컴퓨터나 스마트폰의 존재는 결코 무시할 수 없는 큰 비중을 차지하고 있다. 이제는 사이버 관련 범죄가 아닌 일반 사건에서도 전자적인 형태의 문건 파일이나 통신기록 등이 수사의 결정적 역할을 담당하는 사례도 많다. 대표적으로 정보통신망 이용촉진 및 정보보호 등에 관한 법률 위반, 개인정보보호법 위반, 지식재산권 침해, 기업의 정보 감사 또는 기밀 유출 등이 있으며 디지털 증거를 수집하여 법정에 제출하면 그 증거능력의 여부에 따라 사실 입증을 위한 자료로 활용할 수 있다.

여기에서 '진정성'이란 법률적인 의미를 내포하고 있으며 원본 증거의 내용과 법원에 제출된 증거의 내용이 동일하다는 '동일성'과, 법정에 제출되기까지 변경이나 훼손 또는 조작이 없었다는 '무결성' 등의 문제를 포괄한다[1]. 대법원 판례[7]에서는 무결성과 동일성을 입증하기 방법으로 암호학적 해시함수(Cryptographic Hash Function)를 직접적으로 언급하고 있으며, 특히 디지털포렌식 실무에서는 Message-Digest5(이하 MD5) 알고리즘[2]을 통해 해시값을 계산하는 방식을 사실상의 표준(de facto standard)으로 여기는 추세이다[3].

그러나 학문적으로 암호(Cryptography) 분야는 끊임없이 진화하고 있으며[4], 시간이 흐름에 따라 암호해독(Cryptanalysis) 공격이 수행되어 기존 기법의 취약성(Vulnerability)이 밝혀진다면 해당 체계는 사장(死藏)되는 수순을 밟게 되고, 그보다 더 안전한(Secure) 알고리즘을 제안하여 사용도록 권고하는 것이 일반적이다.

본 논문에서는 지금까지 밝혀진 MD5에 대한 공격 동향을 살펴보고, 디지털 포렌식 분야에 직접적으로 적용 가능한 공격 시나리오를 가정해본다. 이를 통해 디지털 증거의 무결성 입증시 사용되어야 할 적합한 해시함수에 관해 고찰하고자 한다.

## Ⅱ. 배경지식

본 단원에서는 논문에서 제기하고자 하는 개념들에 대한 배경지식을 전달한다.

### 1. 디지털 증거의 무결성

디지털 증거는 기본적으로 데이터의 양이 방대하여 특별한 기술과 도구를 사용하지 않으면 추출이 곤란하며, 인간의 오감으로는 직접 정보의 내용을 인지할 수 없는 전자적 정보의 형태로 기록 저장된다는 특징을 가지고 있다. 또한, 간단한 조작만으로 위조 내지 변조가 가능하고 정보 일부의 삭제 또는 변경이 용이하다는 취약성을 특성으로 하므로 진정성의 문제가 항상 수반될 수밖에 없다. 증거의 수집 과정에서 오류가 발생하여 원본의 내용물이 변형될 가능성도 있다. 이런 경우 그 증거는 더 이상 증거로서의 가치를 유지할 수 없게 된다. 따라서 수집된 증거가 원본과 동일하다는 것을 입증할 수 있는 기술적인 조치가 필요하다[1][5].

디지털 자료가 법정에서 증거로 인정받기 위한 요건은 여러 연구자들의 발표나 학회, 표준 정책 기관마다 약간의 차이가 있지만 대체적으로 진정성, 원본동일성, 신뢰성, 정당성, 재현의 원칙, 연계보관성, 무결성 등을 제시하고 있다[6]. 이러한 개념들에 대해 모두 설명하는 것은 본 논문의 범위를 벗어나므로, 여기에서는 무결성(Integrity)이라는 용어에 대부분의 중요한 의미가 내포되어있는 것으로 가정하고 이에 집중하여 내용을 전개하도록 한다.

실제 대법원 판례[7]를 보면, "피압수·수색 당사자가 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체의 해쉬(Hash) 값이 동일하다는 취지로 서명한 확인서면을 교부받아 법원에 제출하는 방법에 의하여 증명하는 것이 원칙이나, 그와 같은 방법에 의한 증명이 불가능하거나 현저히 곤란한 경우에는, 정보저장매체 원본에 대한 압수, 봉인, 봉인해제, '하드카피' 또는 '이미징' 등 일련의 절차에 참여한 수사관이나 전문가 등의 증언에 의해 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이의 해쉬 값이 동일하다거나 정보저장매체 원본이 최초 압수 시부터 밀봉되어 증거 제출 시까지 전혀 변경되지 않았다는 등의 사정을 증명하는 방법 또는 법원이 그 원본에 저장된 자료와 증거로 제출된 출력 문건을 대조하는 방법 등으로도 그와 같은 무결성·동일성을 인정할 수 있다"고 판시하고 있다[1][7]. 이에 따라 수사기관에서는 수집한 디지털 데이터가 위·변조되지 않았음을 나타내는 해시값 검증을 기준으로 무결성과 동일성을 판단하고 있고, 이것이 입증되지 않으면 수집된 디지털 데이터가 범죄에 대한 법적 증거로써 활용될 가치를 잃게 된다는 점에 유의하여, 이와 관련한 다양한 절차 및 제도를 정비하는 등의 연구를 지속 수행하고 있다[8][9].

### 2. 암호학적 해시함수의 성질과 공격법

암호학적 해시(Cryptographic Hash)는 주어진 입력의 크기에 상관없이 고정된 길이의 출력을 계산한 결과이다. 이를 이용하면 데이터의 무결성을 검증할 때 위변조 여부를 파악할 수 있다. 암호학적 정의에 따르면 이상적인 해시함수는 기본적으로 다음 두 성질을 갖는다[10].

· 일방향성(one-way): 주어진 해시 결괏값을 통해 원래의 입력 메시지를 역으로 계산하는 것이 불가능하다.

· 충돌저항성(collision-free): 동일한 해시 결괏값을 갖는 서로 다른 두 메시지 $M_1$과 $M_2$를 찾는 것이 계산상 어렵다.

위의 정의에 따라 구현된 해시함수에 대해, 그 기본 성질에 대한 반례를 제시할 수 있다면 해당 해시함수는 공격되었다고 한다. 또한 일방향성에 대한 공격은 다시 세부적으로 'First - preimage'와 'Second - preimage'로 분류되며, 이를 정리한 내용은 다음과 같다[11]. (단, L은 해시값의 길이)

· 1st-preimage attack: 공격자가 해시값을 알고 있을 때, 해당 입력 메시지 $M$을 $2^L$보다 빨리 찾을 수 있는 경우.

· 2nd-preimage attack: 해시값과 입력 메시지 $M_1$을 알고 있을 때, 해당 해시값과 일치하는 또 다른 입력 $M_2$를 $2^L$보다 빨리 찾을 수 있는 경우. (보통 1st와 같거나, 조금 더 쉬움[49])

· collision attack: 동일한 해시값을 가지는 서로 다른 두 메시지 $M_1$과 $M_2$을 $2^{L/2}$보다 빨리 찾을 수 있는 경우[12].

위의 정리에 따르면 세 가지 공격법 중에 collisoin attack이 가장 쉬운 방법임을 알 수 있다. collisoin attack에 성공했다고 해서 preimage attacks도 항상 성공한다고 일반화할 수는 없으나, 최소한 collision 공격에 성공하면 해당 해시함수는 공격되었다고 결론을 내리게 된다[13][14]. 이 경우 학계에서는 일반적으로 더 이상 해당 해시함수의 사용을 권고하지 않는다[15][16].

## 3. MD5 해시함수와 그 사용실태

암호학적 해시(Cryptographic Hash)는 이상적인 모델이며, 이를 실용적으로 구현한 함수로는 MD4, HAVAL-128, RIPEMD 등이 있었다. 그러나 이 함수들은 충돌쌍 및 제 2 역상을 쉽게 찾을 수 있다는 취약점이 발견되어 새로운 해시함수에 대한 제안이 이루어졌다. 특히 Rivest에 의해 개발된 MD5와[2], 미국 국가안보국(NSA)이 설계한 SHA(Secure Hash Algorithm) 함수[17] 등이 현재 가장 널리 사용되고 있다. 본 논문에서는 Message - Digest 5 (MD5) 알고리즘[2]을 중점적으로 다루므로, 해당 함수의 기술적인 구현을 간단히 요약하여 소개하고, 실무에서의 MD5 사용실태를 확인한다.

MD5는 기존 MD4를 개량한 모델이며, 임의 길이의 메시지를 입력하면, 먼저 적절히 패딩한 후 512 비트 블록 단위로 쪼개는 작업을 수행한다. 이후 초기화 벡터를 설정하고, 압축함수를 적용하는 [그림 1]과 같은 동작을 64회 반복하는 구조로 진행하여 최종적인 수행 결과는 128bits 길이의 값으로 도출된다. 그러나 내용을 사람이 육안으로 구분하기 어려우므로, 가독성을 위해 16진수 형식으로 변환하여 32 길이의 숫자와 문자(A~F) 조합으로 표현하는 형태로 기록하는 것이 일반적이며, 예를 들어 "9e107d9d372bb6826bd81d3542a419d6"의 형식으로 표기한다.

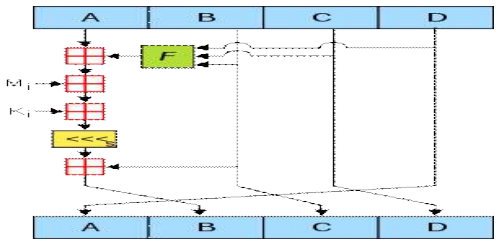


그림 1. MD5의 연산 도식화[18]

이렇게 얻은 문자열은 해당 입력값에 대한 디지털 지문(Fingerprint)으로써 유일하게 구별되며, 이 특성 덕분에 전자적 증거의 무결성을 입증하는데 중요하게 활용되고 있다. 실제로 대검찰청의 관련 규정에 따르면, 증거사본 작성시 MD5 해시값을 분석 보고서에 기입하도록 하고, 이에 참관인의 서명을 확인하는 절차를 진행하도록 하는 서식을 제공하고 있다[19]. 또한, 경찰청의 관련 훈령에서는 '데이터 고유 식별값'이라는 의미로 해시값을 지칭하고 있으며, "디지털 증거의 수집 및 분석 시에는 정확성과 신뢰성이 있는 프로그램을 사용하여야 한다"고 명시하고 있다[20]. 이와 관련한 소프트웨어라 함은, Guidance 社의 Encase와 Access Data 社의 FTK가 대표적이며, 증거사본 생성과 분석 실무에 전 세계적으로 통용되고 있다. 때문에 이들 소프트웨어가 제공하는 결과물을 인용하여 보고서에 삽입하는 경우가 상당한데, [그림 2], [그림 3]과 같이 MD5 함수를 초기설정값(Default)으로 지정하고 있으며, 선택적으로 SHA-1을 지원한다. 때문에 특별한 언급이 없는 한, 포렌식 분야에서는 MD5가 사실상의 표준(de facto standard)으로 여겨지고 있는 실태라고 보아도 과언이 아니다[3].

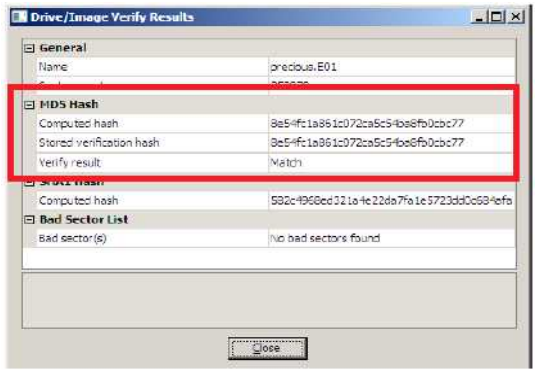


그림 2. Access Data의 FTK

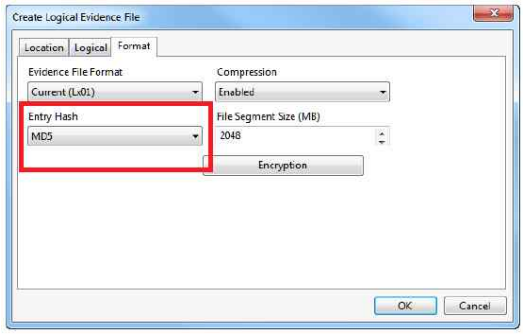


그림 3. Guidance의 Encase

## Ⅲ. MD5 공격의 동향

MD5가 디지털포렌식 분야에서 여전히 활발하게 사용되고 있지만, 암호학계에서는 이미 2004년에 중국 山東대학의 Wang 교수 등에 의해 이론적 취약점이 발견되었고[21], 이후 CRYPTO[1] 2009에서 Marc 등에 의해 MD5의 취약점을 이용한 실용적인 공격방안과 사례가 제시되기도 하였다[22]. 본 단원에서는 현재까지 알려진 해시함수의 대표적인 공격 동향에 대해 살펴본다.

### 1. Brute Force / Birthday Attack

암호학의 가장 고전적인 공격 기법으로는 일명 전수조사(Brute Force)라고 알려진 시행착오식의 방법이 있다. 프로그램을 이용해 입력값을 임의로 생성하여 크랙을 시도하고, 틀리면 다른 값으로 변경하여 재시도하는 방법으로, 가능한 모든 입력의 조합에 대해 반복적으로 조사한다. 이 경우 이론적으로는 정답을 반드시 찾을 수 있으나, 탐색시간이 무한대에 가깝기 때문에 효율적인 방법은 아니다. 다행히도 해시함수의 경우에는 'Dirichlet의 상자원리'에 의해 Collision이 반드시 발생한다는 것이 수학적으로 입증되며, 확률론적 정리를 통해 일명 생일공격(Birthday Attack)으로 알려진 방법으로 전수조사의 범위를 $2^L$에서 $2^{L/2}$로 축소할 수 있다[12]. 따라서 MD5 해시함수의 출력 크기를 대입하여 계산하면 $2^{64}$가 된다. NIST는 현대의 컴퓨팅 자원 성능을 고려하여 계산상 불가능의 기준을 최소 $2^{112}$이상으로 설정하고 있으며[16], MD5는 기준보다 현저히 낮은 복잡도를 가지므로 충분히 공격 가능한 범위에 있다고 볼 수 있다.

### 2. Rainbow Table

레인보우 테이블은 해시의 역상을 미리 계산하여 데이터베이스 테이블에 저장하는 방식으로, Martin Hellman에 의해 1980년 소개되었다[23]. 다수의 평문으로 이루어진 값들에 해시를 적용한 결괏값과 대응시켜 저장해두면 매번 새롭게 계산할 필요 없이 기존의 목록을 탐색하는 것만으로 역상을 쉽게 찾을 수 있다. 그러나 당시에는 레인보우 테이블을 구현하는 것이 매우 복잡하였으며 용량이 방대하여 이를 원활히 활용할 수 없었다. 2000년대 이후 저장매체와 인터넷 기술의 혁신을 힘입어 고용량의 레인보우 테이블을 쉽게 입수할 수 있는 시대가 도래했다. 뿐만 아니라 이미 알려진 해시 값을 원문으로 변환해주는 온라인 서비스(ex : CrackStation.com)마저 성행하고 있다. 이들은 Brute Force 방식에 위키피디아 백과의 낱말 사전 데이터를 혼합 활용하여 계산한 150억 개의 Entry(190GB)에 달하는 테이블을 보유하고 있다[24]. 이를 악용할 경우 Unix 및 Linux 시스템에서 사용자의 패스워드 해시값을 통해 원문을 크래킹 하는 것이 가능하다.

### 3. Xiaoyun Wang의 차분공격

차분 공격(Differential Attack)을 사용하여 MD5를 공격하는 방안은 1992년부터 T. Berson에 의해 시도되었으나[25], 가능성만 제기되었을 뿐 구체적이고 효과적인 해법이 없어 성과가 미미하였다. 한편, 중국의 Wang 교수 등은 알고리즘 내부 논리를 수학적으로 분석하는 방법으로 연구하였으며, 기존의 배타적 논리합(XOR) 방식의 차분공격이 효율적이지 못하다는 것을 발견하고, 부울(Boolean) 함수의 특성을 이용한 새로운 방식을 시도하였다. 이는 각 단계에 연쇄적으로 적용되는 변수에 일정한 조건을 지정하는 방식이며, 이를 사용하여 2004년부터 MD4, MD5, RIPEMD, HAVAL, SHA-0에 대한 구체적인 충돌쌍을 찾았다. 특히 MD5의 경우 IBM P690을 사용했을 때 1시간 이내에 충돌쌍을 찾을 수 있는 매우 강력한 기법임을 밝혀 EUROCRYPT[2] 2005에서 발표하였다[21]. 이후 Wang의 방법보다 개선된 방법도 공개되었으며, 일반 NotebookPC 수준에서도 공격이 가능해졌다[26].

[표 1]은 동일한 MD5가 도출된 사례이다.

1) CRYPTO 2009 was the 29th International Cryptology Conference. It was held at the University of California, Santa Barbara. The academic program covered all aspects of cryptology. Marc Stevens is Winner of the Best Paper Award.

2) The Eurocrypt conference is an international conference on all aspects of cryptology. The Eurocrypt conference has been held every year since 1987, and is held in a different location in Europe every year.

표 1. 두 입력값은 6-bits의 분명한 차이가 있지만, 동일한 MD5 결과값을 도출하여 Collision이 발생한다.

| | |
|---|---|
| $M_1$ | d131dd02c5e6eec4693d9a0698aff95c<br>2fcab58712467eab4004583eb8fb7f89<br>55ad340609f4b30283e4888325**7**1415a<br>085125e8f7cdc99fd91dbd**f**280373c5b |
| | d8823e3156348f5bae6dacd436c919c6<br>dd53e2**b**487da03fd02396306d248cda0<br>e99f33420f577ee8ce54b67080**a**80d1e<br>c69821bcb6a8839396f965**2**b6ff72a70 |
| $M_2$ | d131dd02c5e6eec4693d9a0698aff95c<br>2fcab50712467eab4004583eb8fb7f89<br>55ad340609f4b30283e4888325**f**1415a<br>085125e8f7cdc99fd91dbd**7**280373c5b |
| | d8823e3156348f5bae6dacd436c919c6<br>dd53e23487da03fd02396306d248cda0<br>e99f33420f577ee8ce54b67080**2**80d1e<br>c69821bcb6a8839396f965**a**b6ff72a70 |
| MD5 | 79054025255fb1a26e4bc422aef54eb4 |

Wang의 연구결과는 MD5 알고리즘의 설계적 취약점을 입증하였기에 암호학계에 큰 파장을 일으켰다. 그럼에도 불구하고, 이는 단순히 제한된 환경에서 이론적인 증명에 그쳤기 때문에 실질적인 위협은 되지 않을 것이라는 입장도 있었다. 당시 Bruce Schneier는 "암호학 연구자들에게 있어 굉장한 사건임에 틀림없지만, 실제적으로 디지털 서명 등의 체계가 깨진 것은 아니기 때문에 일반 사용자들에게는 아직 큰 문제가 아니다."라고 논평하였다[27].

## 4. Marc Stevens의 인증서 위조 기법

그러나 예상과는 달리 MD5의 취약점을 이용하여 실제 응용 프로그램 수준에 영향을 미칠만한 공격이 연이어 제시되었다. Wang은 자신의 연구를 확장하여, ITU-T 표준 공개키 기반 X.509 인증을 우회한 사례를 제시하였다. 해당 과정에서는 RSA 공개키 암호화 알고리즘이 적용되고 이를 검증할 때에는 MD5를 사용해 디지털 서명(Signature)을 생성한다. 이때 검증하는 과정에서 해시값만으로 일치 여부를 판별한다는 점을 악용함으로써 상이한 내용의 인증서에 MD5의 Collision이 발생하도록 한다면, 해당 인증서가 조작되었는지 판단할 방안이 없다는 것을 [그림 6]와 같이 입증한 것이다[28].

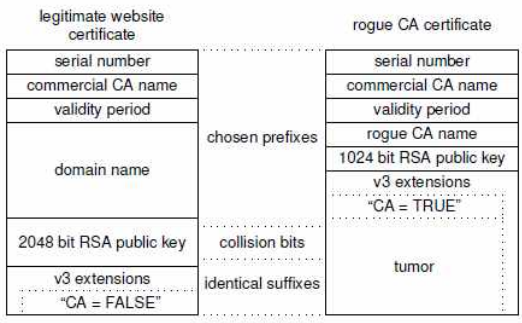


그림 6. 충돌을 야기하도록 조작된 인증서[22]

또한 Wang의 방법에 영감을 얻은 Marc Stevens는 인증 기관(Certification Authority)의 인증서를 위조한다면 SSL 통신임에도 불구하고 중간자 공격(Man-in-the-Middle Attack)을 수행할 수 있음을 보였다. 이는 당시의 대부분의 인터넷 브라우저에 직접적인 영향을 미치는 결과였다. 특히 이들은 Chosen Prefix 방법을 제시함으로써 계산 복잡도를 기존에 비해 $2^{39}$ 수준까지 획기적으로 줄였으며, Identical Prefix의 경우 $2^{16}$임을 밝혔다[22]. 이들은 약 18시간 만에 위조된(Rogue) 인증서 생성을 성공하였는데, Play Station 3 단말기 200여 대를 클러스터 구성한 분산병렬 처리를 통해 성능을 최대화한 것이 비결이었다. 이후 BlackHat USA 2009에서는 GPGPU(General-purpose GPU) 등을 활용한 방법 또한 공개되면서 Marc의 방법보다 더욱 저렴한 비용임에도 9배 이상 속도를 개선시켰음을 보였다[29]. 2016년 현재에는 다양한 클라우드 컴퓨팅 자원과 GPU 성능이 2009년에 비해 더 급진적인 도약을 이루었으므로, 지금의 자원을 사용한다면 공격의 효과는 더욱 강력할 것이다. 이러한 논문들이 발표된 이후 모든 CA 기관은 해시 알고리즘 선택시 기존 MD5에서 SHA-1로의 전환을 의무화하도록 권장되었다.

## Ⅳ. 디지털포렌식 관점에서의 문제점

이러한 암호학계의 연구결과에도 불구하고, 다수의 응용 프로그램에서 여전히 사용 중인 MD5의 존속 여부에 대해서는 논란의 여지가 있었다. 특히, 디지털포렌식 분야에서 국제적으로 유명한 학술저널인 "Digital Investigation"는 Wang의 논문으로 MD5 충돌쌍이 밝혀졌으나 디지털 증거의 무결

성을 입증하는 상황에서는 큰 지장이 없을 것이라는 의견을 다음 세 가지 이유를 들어 설명하였다[30].

·역상(Preimage) 저항성에 관한 공격으로는 여전히 효율적인 방법이 제시되지 않았다.
·Wang의 방법은 특정한 입력 Block에 한정된 결과이므로, 실무의 현장에서 그러한 전제조건이 실현되리라고 가정하기는 어렵다.
·디지털 포렌식에서는 단순히 짧은 문자열이나 메시지 블록에 대해서만 실험하는 것이 아니라, 이미징 된 파일 형태의 입력값을 주로 취급하며 이 경우의 충돌 가능성은 여전히 천문학적으로 희박하다.

이러한 Eric Tompson의 관점은 상당 부분 현재에도 유효하다. 그럼에도 불구하고 최근의 학계 동향에 따르면 이를 반박할 수 있는 근거가 지속적으로 도출되고 있다. 특히, 제 2 역상 저항성은 충돌저항성과 밀접한 관련이 있으며[10], 전수조사보다 빠른 방법으로 탐색할 수 있는 방법이 이미 제시되었다[31]. 또한, 제 1 역상 저항성에 관해서도 $2^{123.4}$으로 탐색한 연구가 공개된 바 있다[32]. 본 단원에서는 지금까지의 연구를 종합하여, 디지털 포렌식 분야에서 MD5를 지속 사용할 경우 직접적으로 유효한 공격 시나리오와 쟁점들을 제시한다.

## 1. 악성코드(Malware) 은닉 실험

MD5의 충돌쌍을 악용한 의미 있는 공격에 관하여는 Narayana이 제시한 "Poisoned Message Attack"이 있다[33][34]. 이는 프로그래밍 언어에서 "if-then-else" 문법 구문의 성질을 이용하여 조건 분기에 사용되는 값을 해시 충돌쌍으로 설정하는 방식을 취한다. 해당 방법은 PDF나 TIFF 등의 파일에도 적용 가능하며, 동일한 해시값을 가지는 서로 다른 두 파일을 생성하게 된다. 따라서 사용자가 모르는 사이 파일이 교체되어도 MD5 해시값을 기반으로 하는 파일 무결성 검사에서는 탐지하지 못하는 취약점이 존재한다. 실제로 해당 공격을 구현한 Peter Selinger의 연구가 발표되었으며[35], 두개의 서로 다른 행위를 수반하는 프로그램이 [그림 5]와 같이 작동하도록 하는 구체적인 코드가 공개되어 있다. 해당 소스코드는 직접 컴파일하여 실행이 가능하며, 컴퓨팅 성능에 따라 30분 내외로 성공한다.

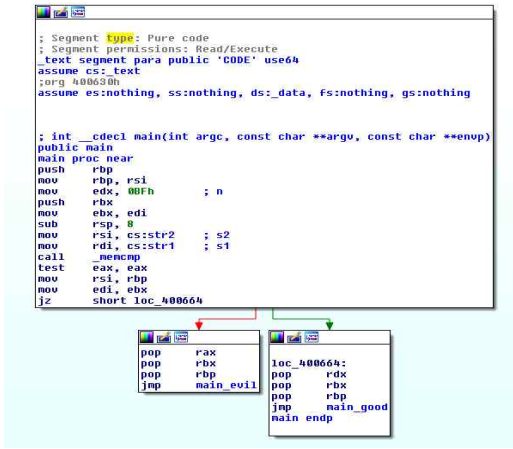


그림 5. Marc Stevens의 공격 프로그램

파일은 "bf262c9ced4ee44cc699e2f36da37f1e"라는 동일한 해시값을 나타내지만, 실행되는 내용은 분명히 다르다. 해당 예제에서는 evil.exe에 단순히 위협적인 메시지를 표출하는 정도에 그쳤지만, 랜섬웨어 등의 악의적인 동작을 하는 프로그램을 삽입하는 것도 가능하다.

## 2. 무결성 보장 불가능

디지털 포렌식 과정에서 디스크 등의 증거를 이미징 하여 *.Ex01 등의 포맷으로 저장하고 해시값을 계산하게 된다. 해당 이미지 파일이 1비트라도 변경된다면 원칙적으로 무결성이 훼손된 것이며 해시값은 기존과 상당한 차이(dramatically changes)를 보여야 한다[30]. 그러나 MD5의 경우 충돌쌍을 찾는 공격 방법이 다른 해시함수에 비해 상당히 공개되었으며, 이를 제 2 역상에 관한 공격으로 일반화하는 것이 이론적으로 가능하다[10][36]. 또한 디스크의 비할당(Unallocated) 영역이나, NTFS의 ADS(Alternate Data Streams)에 충돌을 야기하는 메시지 블록을 은닉하는 등의 시나리오를 재연한다면 무결성이 명백하게 훼손된 경우임에도 해시값이 여전히 일치함을 보임으로써, MD5가 해시함수 본연의 기능을 상실했음을 증명할 수 있다.

## 3. 증거능력에 관한 쟁점

디지털자료 등의 과학적 증거를 법정에서 신뢰할 수 있는지에 대해서는 판례에 의한 몇 가지 중요한

기준들이 있었다. 미국 법원의 경우 1920년대에 Frye test[3]라는 기준을 적용하여 "해당 분야에서 일반적으로 승인된 것"임을 입증하도록 요구하였다. 더 나아가 1993년에는 다우버트 사건[4]에서 과학적 증거의 허용성에 대한 새로운 기준을 다음과 같이 정립하였다[37].

- 검증 가능 여부
- 동료들의 검토를 위한 과학 간행물 게재
- 알려져 있거나 잠재적인 오류율의 정도
- 실험을 통제할 수 있는 표준과 그 적용 여부
- 해당 분야에서 받아들여지는 정도

대한민국의 대법원에서도 거짓말탐지기와 유전자 감식의 경우 위의 다우버트 기준을 적용하고 있다. 즉, 방법이 합리적이며, 기술에 신뢰성과 정확성을 확보할 수 있어야 하며, 관련 전문인이 표준적인 검사기법으로 수행해야 한다고 판시하였다[38][39].

지금까지의 암호학계 연구동향을 종합해보면, Marc Stevens는 컴퓨터 포렌식 분야에서 MD5 존속은 상당히 유해하다는 논문을 발표하였으며[40], 카네기 멜론 대학 소프트웨어공학 연구소에서는 암호학적 해시함수로써의 MD5 사용은 더 이상 부적합하다고 논평하였다. 이에 현재 미국 NIST, NSA 등 기관이 승인한 암호사용 권고안에서는 MD5가 포함되어있지 않다[16]. 이처럼 현대 암호학계에서 MD5사용은 더 이상 승인되기 어렵다는 시각이 보편타당하다. 따라서 법정에서의 과학적 증거 기준을 디지털자료에 대해서도 엄격히 적용한다면, MD5는 더 이상 받아들여지기 어렵다고 본다.

## Ⅴ. 대응방안

지금까지 MD5가 암호학적 해시함수로서의 지위를 상당히 잃었으며, 그 신뢰성이 학계에서 보증되지 않는다는 것을 설명하였다. 따라서 보다 안전한 해시함수로의 전환을 준비해야 할 것이다. 현재 포렌식 유틸리티에서 추가적으로 제공되는 SHA-1 해시함수도 사실상 그 수명이 다하였다. 본 논문에서 자세히 소개하지는 않았지만, Marc Stevens는 SHA-1에 대한 구체적인 취약점 역시 발견하였으며[41][42], 이에 따라 마이크로소프트 인터넷 익스플로러나 구글 크롬 등의 웹 브라우저는 2017년부터 더 이상 SHA-1을 지원하지 않는다.

미국 NIST의 권고안[16]은 암호학적 해시함수에 유효기간을 부여하고 있으며, 현재 SHA-2 사용이 권장된다. 또한, 새로운 표준으로 SHA-3 제정을 추진하였고 최종적으로 Keccak이 선정되었다[43]. 대한민국의 국가보안기술연구소(NSR)에서도 금융, 클라우드, 빅데이터 분야에서 무결성 검증시 사용할 수 있는 고속 해시함수 LSH(Lightweight Secure Hash)을 개발하였다[44]. 때문에 향후에는 안전도 기준을 향상시킨 이러한 새로운 해시 함수들을 사용하는 것이 바람직한 것으로 보인다[45]. 그럼에도 불구하고 SHA-3와 LSH에 공격에 대한 연구 역시 계속해서 진행되고 있으므로[46][47], 이 방법 역시 무한정 보장되는 것은 아닐 것이다.

해시함수 무결성 검증 방식이 갖는 위험성을 방지하기 위해 디지털 증거에 공개키 기반구조를 적용한 공증 방식, 메시지 인증코드 방식 등을 도입해야 한다는 연구도 있었다. 그러나 초기 투자 비용이나 운영의 어려움 등이 발생한다는 단점이 있다[48].

추가적인 비용을 투자하지 않고 즉시 대응할 수 있는 가장 현실적인 방안으로는 현재 대부분의 포렌식 도구가 지원하고 있는 두 가지 해시함수 MD5와 SHA-1을 혼용하여 교차 검증하는 것이며, 이 경우 각각의 취약성을 감안하여도, 두 조건을 동시에 만족시키는 충돌쌍을 발견하는 것은 계산 복잡도가 상당하므로 확률적으로 매우 희박할 것으로 예상된다.

## Ⅵ. 결론

본 논문에서는 디지털포렌식 분야에서 증거의 무결성 검증시 사용되는 해시함수에 대해 소개하고, 취약한 MD5를 중심으로 위협 시나리오를 살펴보았다. 또한, 암호학계의 연구동향을 통해 영원히 안전한 해시함수는 존재할 수 없다는 한계를 직시하였다. 따라서 반드시 2개 이상의 해시 알고리즘을 적용하여 무결성을 입증하도록 관련 법률과 정책, 보고서 양식을 개정하는 것을 권고한다. 장기적인 관점에서는 포렌식 도구에 지원되는 해시함수 수준을 학계의 권고에 따라 주기적으로 상향 조정해야 할 것이다.

3) Frye v. United States, 293 F. 1013 (D.C. Cir. 1923).
4) Daubert v. Merrel Dow Pharmaceuticals, 509 U. S. 579(1993).

## 참 고 문 헌


〔1〕 권양섭. "디지털 증거의 증거능력에 관한 고찰." 법이론실무연구 4.1 (2016): 149-168.

〔2〕 Rivest, Ronald. "The MD5 message-digest algorithm." (1992).

〔3〕 Cameron H. Malin, Eoghan Casey, James M. Aquilina, "Malware Forensics Field Guide for Windows Systems : Digital Forensics Field Guides", pp. 243, 2012.

〔4〕 Itkis, Gene. "Forward security, adaptive cryptography: Time evolution." (2004).

〔5〕 오기두. "형사절차상 컴퓨터관련 증거의 수집 및 이용에 관한 연구." 서울대학교 박사학위논문 (1997).

〔6〕 이준형, 조정원, "디지털 포렌식의 세계(개정판)", pp. 16-17, (2014)

〔7〕 대법원 2013.07.26. 선고 2013도2511 판결

〔8〕 대검찰청, 숭실대학교 "디지털증거의 무결성 유지를 위한 절차와 시설에 관한 연구", (2006)

〔9〕 대검찰청, 고려대학교 산학협력단, "외국판례에 나타난 디지털증거 수집·분석·보존 과정에서의 무결성 논란에 비추어 본 디지털 증거의 활용방안", 2006년 6월.

〔10〕 Rogaway, Phillip, and Thomas Shrimpton. "Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance." International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 2004.

〔11〕 Schneier, Bruce, and Paul Hoffman. "Attacks on cryptographic hashes in internet protocols." (2005).

〔12〕 Bellare, Mihir, and Tadayoshi Kohno. "Hash function balance and its impact on birthday attacks." International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2004.

〔13〕 Stinson, Douglas R. "Some observations on the theory of cryptographic hash functions." Designs, Codes and Cryptography 38.2 (2006): 259-277.

〔14〕 성수학. "해쉬함수에 대한 충돌쌍 탐색 공격의 동향." 정보보호학회지 16.4 (2006): 25-33.

〔15〕 Dang, Quynh. Recommendation for applications using approved hash algorithms. US Department of Commerce, National Institute of Standards and Technology, 2008.

〔16〕 Barker, Elaine, and Allen Roginsky. "Transitions: Recommendation for transitioning the use of cryptographic algorithms and key lengths." NIST Special Publication 800 (2011): 131A.

〔17〕 Eastlake 3rd, D., and Paul Jones. US secure hash algorithm 1 (SHA1). No. RFC 3174. 2001.

〔18〕 MD5. (2016, October 8). In Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=MD5

〔19〕 대검찰청, "디지털포렌식 수사관의 증거 수집 및 분석 규정"〈개정 대검예규 제805호 2015. 7. 16.〉 별지 제3호 서식, 제5호 서식

〔20〕 경찰청(디지털포렌식센터), "디지털 증거 수집 및 처리 등에 관한 규칙"〈경찰청훈령 제766호, 2015. 5. 22.〉 제12조, 제16조

〔21〕 Wang, Xiaoyun, and Hongbo Yu. "How to break MD5 and other hash functions." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2005.

〔22〕 Stevens, Marc, et al. "Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate." Advances in Cryptology-CRYPTO 2009. Springer Berlin Heidelberg, 2009. 55-69.

〔23〕 Hellman, Martin. "A cryptanalytic time-memory trade-off." IEEE transactions on Information Theory 26.4 (1980): 401-406.

〔24〕 https://crackstation.net/

〔25〕 Berson, Thomas A. "Differential cryptanalysis mod 232 with applications to MD5." Workshop on the Theory and Application of of Cryptographic Techniques. Springer Berlin Heidelberg, 1992.

〔26〕 Klima, Vlastimil. "Finding MD5 Collisions on a Notebook PC Using Multi-message

Modifications." IACR Cryptology ePrint Archive 2005 (2005): 102.
〔27〕 Schneier, Bruce. "Cryptanalysis of MD5 and SHA: Time for a New Standard." Computer World,(August, 2004) (2004).
〔28〕 Lenstra, Arjen K., Xiaoyun Wang, and B. M. M. de Weger. Colliding X. 509 certificates. No. EPFL-REPORT- 164541. 2005.
〔29〕 Bevand, Marc. "Md5 chosen-prefix collisions on gpus." Black Hat (2009).
〔30〕 Thompson, Eric. "MD5 collisions and the impact on computer forensics." Digital investigation 2.1 (2005): 36-40.
〔31〕 Kelsey, John, and Bruce Schneier. "Second preimages on n-bit hash functions for much less than 2 n work." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2005.
〔32〕 Sasaki, Yu, and Kazumaro Aoki. "Finding preimages in full MD5 faster than exhaustive search." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2009.
〔33〕 Kashyap, Narayana D. A Meaningful MD5 Hash Collision Attack. Diss. San Jose State University, 2006.
〔34〕 Daum, Magnus, and Stefan Lucks. "Hash Collisions (The Poisoned Message Attack)"The Story of Alice and her Boss"." rump session of Eurocrypt 5 (2005): 253-271.
〔35〕 Selinger, Peter. "MD5 collision demo." (2009).
〔36〕 Gebhardt, Max, Georg Illies, and Werner Schindler. "A Note on the Practical Value of Single Hash Collisions for Special File Formats." Sicherheit. Vol. 77. 2006.
〔37〕 이인영. "뇌영상 증거의 과학적 증거로서의 기능과 한계." 형사법연구 22 (2010): 255-278.
〔38〕 대법원 2005. 5. 26. 선고 2005도130판결.
〔39〕 대법원 2007. 5. 10. 선고 2007도1950판결.
〔40〕 Stevens, Marc, Arjen K. Lenstra, and Benne De Weger. "Chosen-prefix collisions for MD5 and applications." International Journal of Applied Cryptography 2.4 (2012): 322-359.
〔41〕 Karpman, Pierre, Thomas Peyrin, and Marc Stevens. "Practical free-start collision attacks on 76-step SHA-1." Annual Cryptology Conference. Springer Berlin Heidelberg, 2015.
〔42〕 Stevens, Marc, Pierre Karpman, and Thomas Peyrin. "Freestart collision for full SHA-1." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2016.
〔43〕 Chang, Shu-jen, et al. "Third-round report of the SHA-3 cryptographic hash algorithm competition." NIST Interagency Report 7896 (2012).
〔44〕 Kim, Dong-Chan, et al. "Lsh: a new fast secure hash function family." International Conference on Information Security and Cryptology. Springer International Publishing, 2014.
〔45〕 이상진. "디지털 포렌식 개론(개정판)." pp. 286-287, 이룬 출판 (2015).
〔46〕 Dinur, Itai, Orr Dunkelman, and Adi Shamir. "Collision attacks on up to 5 rounds of SHA-3 using generalized internal differentials." International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 2013.
〔47〕 Hao, Yonglin. "Cryptanalysis of the LSH hash functions." Security and Communication Networks 9.16 (2016): 3296-3308.
〔48〕 조상수. "디지털 증거의 법적 지위 향상을 위한 무결성 보장 방안." 형사법의 신동향 27 (2010): 64-109.
〔49〕 Dang, Quynh, Rebecca M. Blank, and Comments From Elaine Barker. "NIST Special Publication 800-107 Revision 1 Recommendation for Applications Using Approved Hash Algorithms." (2012).