情 報 保 護 學 會 誌
第19卷 第5號, 2009. 10

고속 디지털 포렌식 기술

김 건 우*, 홍 도 원**

요 약

개인용 컴퓨터의 디스크 용량 증가와 저장, 분석되어야 하는 방대한 양의 데이터는 포렌식 수집과 분석 시간을 점점 더 요구하고 있다. 이에 ETRI는 대용량 데이터에 대한 고속 수집 및 검색, 분석을 가능하게 하는 고속 포렌식 시스템을 개발하였다. 포렌식 분석은 질의어에 대한 검색의 연속된 과정이라고도 할 수 있어 고속 포렌식 시스템은 하드웨어 가속기를 이용하거나 인덱스를 구축하여 고속으로 데이터를 검색하는 기술을 제공한다. 또한, 안티포렌식 기법중 하나인 파일 암호화는 문서 열람을 불가능하게 해 증거 발견을 어렵게 한다. 이에 고속 포렌식 시스템은 제한된 수사 시간을 고려하여 고속으로 패스워드를 해독하는 기능을 제공한다.

Ⅰ. 서 론

디지털 포렌식(Digital Forensics)이란 사이버 범죄, 정보 유출 등과 관련된 디지털 증거가 법적 증거력을 갖게 하기 위해 디지털 데이터를 수집, 보관, 분석, 보고하는 과학적이고 논리적인 절차와 방법을 의미한다. 포렌식 기술은 컴퓨터 관련 범죄수사를 위한 국가기관 뿐만 아니라, 회계 부정 방지, 기업 내부 기밀유출 방지 등 기업에서의 내부 보안 강화를 위해 활용될 수 있다. 아직까지 우리나라에서는 포렌식 기술에 의한 디지털 증거의 법적 채택보다는 수사시 증거 발견을 위한 도구나 기업에서 개인정보 유출 탐지 등의 도구로 주로 이용되고 있다.

대부분의 디지털 포렌식 도구는 저장장치로부터 데이터를 수집해서 이미징하고 무결성을 제공한다. 또한, 수집된 데이터로부터 디스크 browsing 및 viewing, 웹 히스토리 분석, 파일 시그니쳐 분석, 타임라인 분석, 삭제 이메일 검색 등 디지털 증거 분석 기능을 제공한다. 하지만, 한글 등 국산 소프트웨어 지원, 스토리지 대용량화에 따른 데이터의 고속 검색 및 분석, 암호데이터 복구 등에서 만족할 만한 성능을 보이지 못하고 있다.

그래서, ETRI는 2007년 3월부터 "정보투명성 보장형 디지털 포렌식 시스템 개발" 과제를 수행하여, 연구 내용중 하나인 고속 포렌식 시스템(High-Speed Forensic System, 이하 HSFS)을 개발하고 있다. HSFS는 고속 수집 및 검색/분석에 초점을 둔 포렌식 시스템으로 대용량 저장매체를 지원하는 독자적인 이미징 포맷을 가지고 이미징 속도를 향상시킨다. 또한, 삭제 및 유실 데이터의 복구 기능을 제공한다.

본 고에서는 ETRI HSFS 시스템에 대해서 간단히 소개한다. 특히, HSFS의 주요 고속화 기술인 포렌식 검색 기술과 패스워드 고속 해독 기술에 관하여 기술한다.

한글 분석 능력이 강화된 고속 인덱스 생성과 하드웨어 가속을 통한 검색 기술은 포렌식 수사뿐 아니라 정보검색 시스템 분야에도 적용될 수 있다.

또한, 암호파일의 패스워드 복구, 특히, 그래픽 프로세서를 사용한 성능 가속화는 패스워드 해독 전용 하드웨어 장비에 비해 추가되는 비용도 크지 않다.

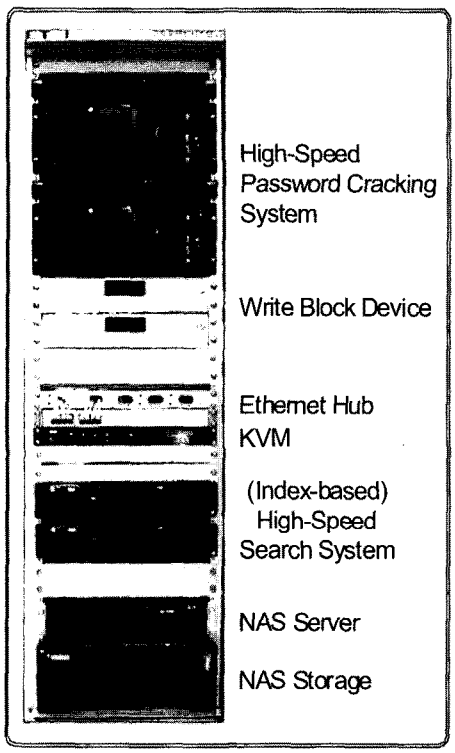
본 연구는 지식경제부 및 정보통신연구진흥원의 IT 신성장동력 핵심기술개발 사업의 일환으로 수행하였음 [2007-S019-03, 정보투명성 보장형 디지털 포렌식 시스템 개발]

* 한국전자통신연구원 암호기술연구팀 (wootopian@etri.re.kr)
** 한국전자통신연구원 암호기술연구팀 (dwhong@etri.re.kr)

Ⅱ. 고속 디지털 포렌식 시스템

2.1 HSFS 형상

HSFS는 대용량 저장장치와 고속화 하드웨어를 가진 서버와 사용자 인터페이스를 가진 GUI 콘솔로 구성된다.



〔그림 1〕 ETRI HSFS

서버는 대용량 스토리지 뿐 아니라 고속 처리를 위해 암호가속 하드웨어, 압축가속기 및 고속 검색을 위한 패턴 매칭 보드를 포함한다. 그래서, 고속 검색 서브시스템과 멀티 GPU를 활용한 패스워드 고속 해독 서브시스템을 가진다.

이미지 암복호 고속화를 위한 암호 가속 보드는 HIFN 7956HXL를 사용하고, 압축과 검색 가속 보드로는 Tarari GPX-3113를 사용했다. 검색 가속 보드 설치를 위해 PCI-X 슬롯, 10MB 디스크 용량, 최소 1GB RAM이 필요하고, 보드는 2.4.x 리눅스 커널에서 동작한다.

패스워드 고속 해독을 위해 2개의 Tesla S870 시스템이 사용되고, S870은 C870 4개로 구성된다. 패스워드 해독은 PC에 장착된 Geforce 9800GTX 같은 개별 GPU에서도 동작가능하다. 고성능 GPU를 장착하여 활용할 때는 큰 전원 공급이 필요하므로 용량이 충분한 파워 서플라이를 사용할 필요가 있다.

각 블록이 기능을 수행할 때 필요한 파일 형태의 데이터 저장을 위해 500GB 용량의 디스크 12개를 사용하였다. 이들 중 한개의 디스크 용량은 RAID 5 구성에서 parity를 저장하는데 사용하고, 한개의 디스크는 다른 디스크의 장애시 교체분으로 지정하여 실제 저장요량은 10개의 디스크 용량인 5TB 이다.

GUI 콘솔은 사용자 인터페이스를 관장하며, 사용자의 요구가 발생할 경우 서버내의 개별 블록 및 각 서브시스템에 해당 명령을 전송하면, 블록 및 서브시스템은 자신이 맡은 기능을 수행하여 그 결과를 GUI 콘솔에 통보하여 사용자에게 전달한다. 고속화 장비를 이용하지 않는 디지털 포렌식의 기본기능은 GUI 콘솔과 연결된 윈도우즈 PC에서 구현하였다.

2.2 HSFS 기능

HSFS는 컴퓨터의 하드디스크를 주 대상으로 디스크의 내용을 모두 읽어 조사할 수 있는 형태의 파일로 작성한 다음, 이 파일을 대상으로 특정 키워드 검색이나, 시계열분석과 같은 작업을 통하여 증거자료를 찾아낸 후 보고서를 작성하는 기능을 가진다. 또한 대용량의 하드디스크를 처리할 수 있고, 컴퓨터를 압수하지 못하는 경우와 동작중인 컴퓨터에서의 메모리나 통신포트 등의 정보를 획득하여 분석할 수 있는 기능이 있다.

HSFS는 고속처리를 위하여 다음과 같은 기능을 가진다.

- 쓰기금지(Write-Block) 처리된 장치를 통해 디스크의 모든 정보를 bit-by-bit 방식으로 읽어와 image 파일을 생성하여 파일 스트림 방식으로 저장한다. 하드웨어 가속기는 이미지 파일의 복호화와 압축해제를 지원한다.
- 아래아 한글, PDF 등의 파일에 대해서는 기본적으로는 검색이 불가능하기 때문에, 이에 대한 검색이 가능하도록 구조를 해체하여 plain text 형태로 데이터를 변경한다. 또한, 그림파일이나 plain text가 아닌 파일을 GUI에서 볼 수 있는 형태로 변환한다.

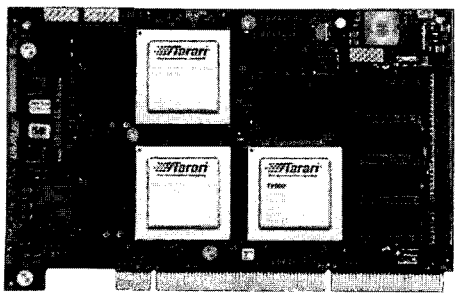
- 이미징 및 검색에서 사용하는 공통 라이브러리를 제공한다. 암호가속보드와 압축가속보드를 통해 고속화가 가능하다.
- 이미지 및 파일에서 패턴매칭 보드를 통해 키워드 및 regular expression를 고속 검색한다. HWP나 PDF 파일은 이미지에서 바로 검색이 불가능하므로 변환된 파일을 읽어서 검색한다.
- on/off line 데이터에 대한 인덱스 검색 기능을 가진다. 즉,이미지에서 인덱스 대상 명사를 분석하고 인덱스 DB를 생성하며, 이를 대상으로 검색을 수행한다.
- 각종 어플리케이션에 대해 설정된 패스워드를 찾아낸다. 이를 위해 패스워드 사전 생성 기능, 사전을 이용한 패스워드 검색, 전수조사를 통한 패스워드 검색을 수행한다.

Ⅲ. 고속 포렌식 검색 기술

디지털 포렌식 검색 기술은 대용량 디스크 데이터로부터 사용자의 질의에 대해 빠짐없이 매칭되는 모든 결과를 정확하게 최대한 빠른 시간내에 찾는것이 핵심이다. 포렌식 검색은 일반 검색과는 달리 물리적 레벨에서 비트와이즈 연산을 바탕으로 검색을 수행해야 하기 때문에 많은 시간이 소요된다. 이에 ETRI는 하드웨어 기반의 포렌식 고속 검색 시스템과 인덱스 기반의 고속 검색 시스템을 개발하였다.

3.1 하드웨어 기반 고속 검색 기술

패턴매칭보드를 사용한 고색 검색은 MS-Office, HWP, PDF와 같은 다양한 방식의 파일, 문자열, 표현식 검색이 가능하고 삭제/유실된 파일 및 슬랙/미할당영역에 포함된 문자열 검색 기능도 포함한다. 특히, 훈글 등 국산 소프트웨어 지원과 문서내의 영어와 한글도 지원하는 것을 특징으로 한다. Tarari 보드를 이용하면 컨텐츠 필터링, 안티 스팸, 실시간 메시지 라우팅과 같은 응용 개발이 가능한데, 최대 1Gb/s 속도로 데이터 스트림의 고정 또는 가변 패턴 분석이 가능하다.



〔그림 2〕 Tarari GPX-3113

HSFS의 GUI 콘솔로부터 질의를 받은 고속 검색 시스템은 리눅스 환경에서 Tarari Grand Prix 3113 보드를 사용한 검색엔진을 통해서 결과를 다시 GUI 콘솔로 보낸다.

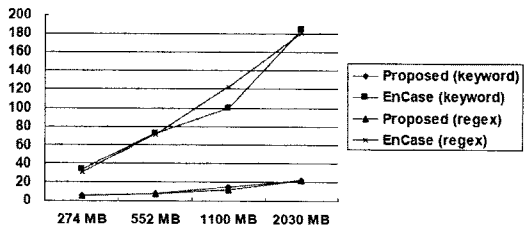
증거 이미지에 포함된 검색어의 패턴을 수행하는 방법을 사용하는 HSFS 고속 검색 시스템은 가장 많이사용하는 포렌식 툴인 EnCase[1]와 비교해 약 5배 이상 빠른 검색 결과를 보여주었다.

키워드 서칭에 대한 검색 시간을 측정하기 위해 1GB dd 이미지를 대상으로 하였고, 단일키워드, 복수키워드, regular expression에 대한 성능을 측정하였다[2].

〔표 1〕 검색 속도 및 건수, MB/s(건수)

	단일키워드	복수키워드	정규표현식
EnCase	20.14 (18)	17.41 (711)	17.12 (0)
ETRI HSFS	100.84 (18)	97.03 (823)	102.58 (70)

또한, 포렌식 이미지 크기 증가에 대한 검색 속도를 측정하기 위하여 서로 다른 크기의 이미지 4개를 생성하여 단일키워드와 정규표현식에 대한 성능을 확인할수 있었다. 2030MB 이미지에 대한 단일키워드 검색시 Encase는 184초가 걸렸으나 HSFS를 이용하면 22초가 소요되었다[2].



〔그림 3〕 이미지 크기에 대한 검색 시간

3.2 인덱스 기반 고속 검색 기술

다수개의 질의어에 대한 동시 검색이나 대용량 데이터로부터 즉시 응답을 요구하는 환경에서는 하드웨어 기반 검색법이라도 실시간으로 검색 결과를 얻을수는 없다. 그래서, ETRI는 포렌식 이미지에 대해 인덱스를 고속으로 생성하고 검색 시 인덱스를 참조하여 실시간으로 검색 결과를 제시하는 인덱스 기반 고속 검색 기술을 개발하였다.

인덱싱은 포렌식 이미지 또는 온라인 데이터로부터 plain text가 아닌 일정 형식의 구조를 갖는 파일의 구조를 해제하고, 해제된 파일을 대상으로 형태소 기반 분석과 바이그램 분석 등을 수행 후, 인덱스를 생성해 DB에 저장하는 일련의 과정이다. 인덱스 검색은 이미지 및 온라인 데이터를 대상으로 생성된 인덱스 DB에서 검색어를 찾는 작업이다. HSFS는 기존의 포렌식 도구와는 달리 한글 인덱스어 추출 및 국산 소프트웨어 생성 파일에 대한 처리를 지원하는 등 다음과 같은 기능을 가진다.

3.2.1 한글 분석 능력이 강화된 인덱스 생성

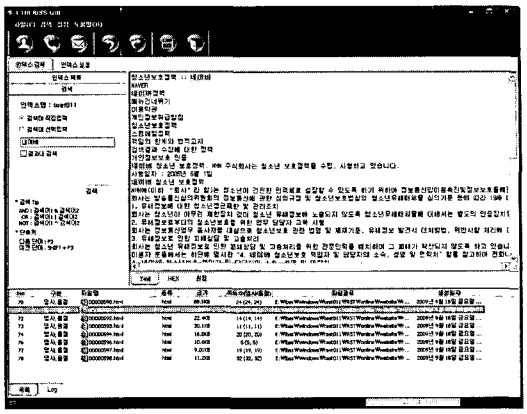
- 한글 명사 분석을 통한 인덱스어 추출
- Bigram을 이용한 인덱스어 추출
- 전화번호/Email/주민번호 등 패턴에 대한 인덱스 생성
- 색인/역색인 DB 구축
- 삭제파일에 대한 인덱스 생성
- 사용자 사전 편집 기능

3.2.2 인덱스 기반 디지털 증거 검색

- 인덱스 기반 명사단위 및 음절단위 검색 (검색어에 대한 정확도 및 재현율 높음)
- 체인 키워드 검색
- 전화번호/Email/주민번호 등 패턴에 대한 검색

3.2.3 온라인 지원 인덱스 생성

- 일반 웹사이트 데이터 수집 및 인덱스 생성
- 온라인 데이터 인덱스 검색(키워드 및 패턴 검색)



〔그림 4〕 온라인 데이터 인덱스 검색 도구

Ⅳ. 패스워드 고속 해독 기술

오피스 파일, PDF 파일, 압축파일 등의 암호화는 사용자가 입력한 패스워드와 어플리케이션별 암호 알고리즘을 사용하여 이루어진다. 패스워드 해독은 사용자 패스워드 후보로부터 암호화 키 유도가 이루어지고 이 키를 이용해 어플리케이션별 패스워드 비교를 통해 이루어진다. 이러한 패스워드 공격에는 전수 조사, 사전을 이용한 공격법이 존재한다.

사전 공격법은 사전의 효율적인 구축에 의존한다. 패스워드가 주민번호, 이름, 또는 특정단어의 조합 등 개인정보에 의거하거나 일반적으로 많이 사용하는 단어라면 사전 공격법은 효율적일 수 있다.

하지만 사용자 패스워드가 난수로 설정되었거나 사전에 포함되지 않는다면 전수조사에 의해 사용가능한 모든 문자열과 모든 키 스페이스를 검색할 수 있는 방법이 요구된다. 이는 입력 패스워드의 가용 공간 전체를 조사해야 하므로 엄청난 시간을 필요로 한다. 그래서, ETRI는 그래픽 프로세서를 활용하여 다수의 패스워드 후보에 대한 패스워드 검증 연산을 병렬처리하여, 범용 연산을 이용할때보다 고속으로 패스워드를 해독하는 시스템을 개발하였다. 물론 사전공격과 이를 위한 개인용/범용 사전 생성 기능도 제공한다.

4.1 패스워드 검색 시스템

ETRI 패스워드 검색 시스템은 소프트웨어 기반의 패스워드 탐색 기능, 사전생성, 파일 정보 추출 기능 및

사용자 인터페이스를 가진 윈도우즈 GUI와 GPU를 활용한 패스워드 고속 검색을 위한 리눅스 머신으로 구성된다. 그 특징은 다음과 같다.

4.1.1 GPU를 이용한 패스워드 고속 해독 기능

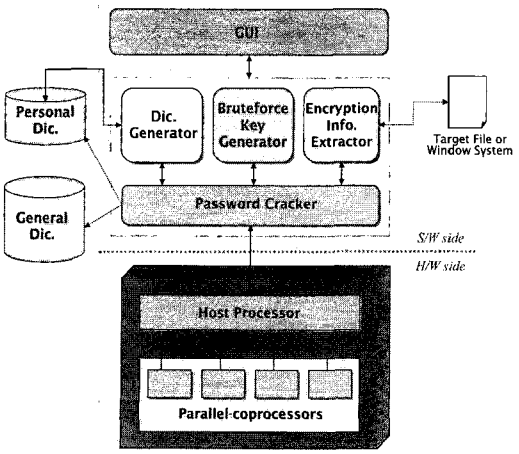
- 대상 어플리케이션에 따라 최적화된 멀티 GPU, 멀티노드 병렬처리 처리 코드 사용
- MS-Word, Excel, PowerPoint, PDF 등 다양한 어플리케이션에 대응
- 사용자 지정에 따른 조사 문자열 선택 기능

4.1.2 범용연산/사전을 활용한 패스워드 해독 기능

- 전수조사 및 기생성된 사전에 기재된 단어들을 이용한 패스워드 해독
- 2개의 사전파일을 동시에 이용할 수 있음

4.1.3 사전 생성 기능

- 이름, 주민번호, 전화번호, 사용자정의 문자 등 용의자의 개인정보들로부터 생성된 패스워드 후보 단어들의 목록 생성
- 기존의 휴리스틱한 알고리즘의 사용을 벗어나 통계적으로 조사된 한국인들의 단어생성 패턴에 기반한 사전 생성 알고리즘 사용
- 한/영 변환을 고려한 패스워드 분포 패턴 생성



〔그림 5〕 ETRI 패스워드 해독 시스템 구조

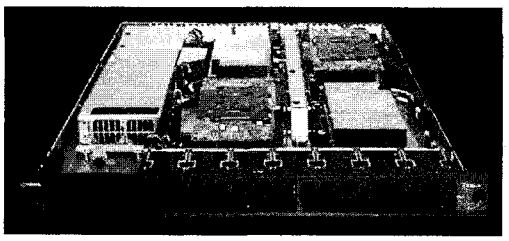
패스워드 검색 고속화를 위해 bit-wising을 통해 루프문으로 인한 속도 저하를 개선하고 GPU를 활용한 멀티쓰레딩 기법을 적용하였다.

4.2 GPU를 사용한 패스워드 고속 탐색

패스워드 탐색에 이용할수 있는 GPU 그래픽 카드는 대부분의 PC에서 이미 장착되어 있어 추가로 비용이 소요되지 않는 장점이 있다. 그래서, NVIDIA사의 Geforce, Tesla, Quadro 시리즈를 사용하여 패스워드 해독에 활용하였다. 또한, 그래픽 칩셋에 대한 어플리케이션 개발환경인 CUDA[3]를 이용하면 그래픽 API에 대한 지식없이 기존의 C/C++을 이용한 어플리케이션 개발이 가능하다.

예를들어, Geforce 9800GTX[4] GPU는 16개의 멀티프로세서로 구성되고, 각 멀티프로세서는 8개의 스트림 프로세서로 이루어져 있어 총 128개의 프로세서 코어를 가진다. 각각의 멀티프로세서는 8192개의 레지스터를 가지고 있고 고속의 데이터 읽기/쓰기가 가능한 16KB on-chip shared memory를 스트림 프로세서가 공유한다. 패스워드 고속 탐색은 shared memory의 데이터 캐쉬 기능을 이용하여 칩 외부와의 통신을 최소화하고, 멀티 쓰레드의 효율적인 블록화를 통해 동일 업무의 병렬처리 속도를 향상시킬수 있다.

[그림 6]은 표준 19" 1U 랙 장착 섀시에 4개의 C870이 장착된 S870[4] 시스템이다. HSFS에는 2U가 장착되어 총 8개의 GPU를 동시에 구동한다. 각각의 노드는 4개의 GPU를 가지므로 패스워드 후보를 8개의 GPU에 중복되지 않고 서로 다르게 할당하여 운영하는 것이 중요하다.



〔그림 6〕 Tesla S870

[표 2]는 ETRI 패스워드 해독 시스템을 이용하여 사용자 패스워드 설정이 많이 되어있는 두 개의 어플리케

이션에 대해 패스워드 해독을 시도하여 초당 검색한 패스워드 후보 개수를 나타낸 것이다. 전수조사를 위해 26개의 영어소문자, 26개의 영어대문자 10개 숫자, 33개의 특수문자를 포함한 95개 문자 집합을 사용하여 각 패스워드 후보를 생성하였다. 소프트웨어를 이용한 해독은 Intel Core2 Quad CPU(2.66GHz)와 3GB 메모리를 장착한 GUI PC에서 실행되었다. 그리고, GPU 가속을 위해 9800GTX 그래픽카드가 탑재된 리눅스 머신과 C870/S870이 탑재된 HSFS에서 각각 테스트 하였다.

MS-word의 문서 암호화 종류는 디폴트로 설정된 Office 97/2003 호환 가능 버전으로 하였고, Adobe PDF는 128비트 RC4 암호화 레벨을 적용한 파일을 대상으로 하였다. MS-word의 경우 60개의 쓰레드로 구성된 256개의 블록을 선언하여 15,360개의 쓰레드를 사용하였을때 최고의 GPU 성능을 보여주었다.

〔표 2〕 패스워드 해독 성능

	MS-Word	Adobe PDF
S/W	285,000	30,000
9800GTX	3,100,000	270,000
C870	2,200,000	230,000
S870	8,600,000	1,000,000
2*S870	17,000,000	2,100,000

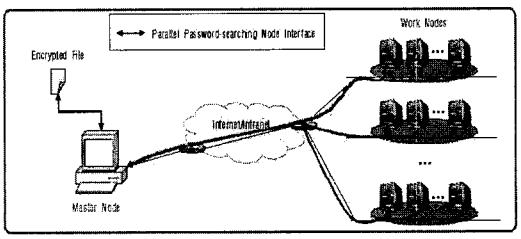
C870는 240개의 프로세서 코어를 가지나 프로세서 클럭과, 메모리 속도가 9800GTX 보다 좋지않아 패스워드 해독 성능은 9800GTX 보다 어플리케이션에 따라 15%~30% 정도 떨어진다. 하지만, 2개의 S870을 사용하면 9800GTX 보다 6배 이상의 성능향상을 보여주고, 소프트웨어를 이용한 해독과 비교해서는 60~70배의 속도 향상을 이루었다. 6자의 PDF 패스워드를 소프트웨어만 이용하여 해독하면 최대 32일이 걸리지만 HSFS를 사용하면 10시간 이내에 패스워드를 발견할수 있다. 7자 MS-word인 경우 각각 최대 7.7년과 40일이 소요된다[5].

해독 대상이 되는 어플리케이션마다 적용된 암호 알고리즘 종류와 반복되는 암호 연산 회수가 다르기 때문에 해독 성능은 어플리케이션에 따라 차이가 나지만 GPU 가속을 이용할때의 성능향상은 거의 동일한 결과를 보여주었다.

4.3 멀티 노드를 사용한 패스워드 해독 고속화

GPU 칩 내부의 다중 코어를 활용한 병렬처리 패스워드 검색 속도의 향상 기술을 다중 시스템 노드로 확장하기 위해, 국내 최대 규모의 GPU 클러스터인 KISTI Picasso 시스템을 활용하였다. 100여개의 노드가 있고 노드당 2개의 CPU와 1개의 Quadro FX-5600 GPU가 장착되어 있다.

[그림 7]과 같이 마스터노드는 암호파일 선택 등 사용자 인터페이스만 제공하고 실제 패스워드 탐색은 멀티 워크노드에서 진행된다.



〔그림 7〕 패스워드 해독을 위한 멀티 노드 활용

FX-5600 GPU 하나만 이용할 경우는 C870과 비슷한 결과를 보여준다. ETRI는 20개의 노드를 사용하여 테스트한 결과 노드수 증가에 대한 패스워드 해독 성능의 선형적인 증가를 확인하였다. 그리고, 소프트웨어를 사용한 것과 비교해서 약 160배의 가속 향상 성능을 보여주었다.

〔표 3〕 멀티노드를 사용한 패스워드 해독 성능

	MS-Word	Adobe PDF
FX-5600	2,300,000	220,000
20*FX-5600	45,000,000	4,500,000
Speed-Up	20배	20배
Spped-Up (SW/20 노드)	160배	150배

향후 모든 가용 노드를 사용하여 CPU와 GPU 자원을 패스워드 해독만을 위해 점유하여 소프트웨어 대비 1,000배 이상의 성능향상을 목표로 한다.

V. 결 론

대용량 데이터를 대상으로 신속한 포렌식 분석을 위해서 처리 속도가 중요하여 하드웨어 가속과 병렬처리 기법을 적용하는 것이 적합하다. 최근의 디지털 포렌식 관련 연구 주제들도 데이터의 고속 검색/분석, 파일카빙 및 패스워드 해독을 위한 고성능 시스템 사용과 연산의 병렬화 사용에 초점을 맞추고 있다.

ETRI HSFS는 국산 소프트웨어 지원을 포함하여 고속 검색 기술과, 암호화 파일 고속 해독 기능 등 대용량 데이터에 대한 고속 포렌식 분석에 적합한 시스템이다.

향후 디지털 포렌식은 e-Discovery 도입과 함께 더욱 큰 시장을 형성할 것으로 예상된다. 공공기관으로부터 민간으로의 포렌식이 확대 적용되면 기업은 소송 발생 시 요구되는 자료를 대규모 데이터에서 제한된시간내에 찾아 법정에 제출하여야 한다. 또한, 기업 기밀보호나 범죄사실 은폐를 위한 파일 암호화는 불법행위 발생시 포렌식 수사를 방해하는 안티포렌식이 되므로 ETRI HSFS 패스워드 고속 해독은 이를 해결하는 좋은 대안이 될 수 있다.

참고문헌

[1] http://www.guidancesoftware.com/.

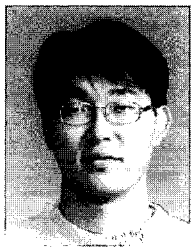
[2] Lee J et al., High-speed search using Tarari content processor in digital forensics, Digital Investigation (2008), doi:10.1016/j.diin. 2008. 05. 006.

[3] "NVIDIA CUDA Compute Unified Device Architecture Programming Guide", Ver. 2.0, 2008. http://www.nvidia.com.

[4] http://kr.nvidia.com/object/cuda_learn_products_kr.html.

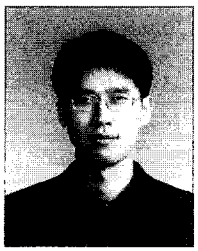
[5] 김건우, 이상수, 홍도원, "GPU 기반의 PDF 파일 패스워드 발견", 디지털 포렌식 기술 워크샵, 2008.

〈著者紹介〉



김 건 우 (Keonwoo Kim)
정회원

1999년 2월: 경북대학교 전자공학과 졸업
2001년 2월: 경북대학교 전자공학과 석사
2001년 1월~현재: 한국전자통신연구원 선임연구원
<관심분야> 디지털 포렌식, 모바일 보안, 암호 프로토콜



홍 도 원 (Dowon Hong)
정회원

1994년 2월: 고려대학교 수학과 학사 졸업
1996년 2월: 고려대학교 수학과 석사 졸업
2000년 2월: 고려대학교 수학과 박사 졸업
2000년 4월~현재: 한국전자통신연구원 암호기술연구팀 팀장
<관심분야> 암호프로토콜, 암호이론, 프라이버시 보호기술, 디지털 포렌식