TTA Standard

정보통신단체표준
TTAS.KO-12.0057

제정일: 2007 년 12 월 26 일

컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항

(Digital Data Acquisition Tool Requirements for Computer Forensics)

TTA 한국정보통신기술협회
Telecommunications Technology Association

정보통신단체표준 제정일 : 2007 년 12 월 26 일
TTAS.KO-12.0057

컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항

(Digital Data Acquisition Tool Requirements for Computer Forensics)

TTA 한국정보통신기술협회
Telecommunications Technology Association

서 문

1. 표준의 목적

본 표준은 컴퓨터 포렌식을 위한 디지털 데이터 수집도구 제조업자에게 기 개발된 도구의 개선 및 향후 개발 예정인 도구의 설계에 대한 가이드라인을 제시한다. 또한, 디지털 데이터 수집도구 사용자에게 도구를 선택하고 사용하는데 있어 필요한 정보를 제공하며, 관련 당사자들이 데이터 수집도구의 능력을 이해하는데 필요한 정보를 제공함에 그 목적이 있다.

2. 주요 내용 요약

본 표준은 디지털 데이터 원본 저장소로부터 데이터를 획득하여 디지털 데이터 복사 원본을 생성하는 디지털 데이터 수집도구가 법정에서 효력을 발휘할 수 있도록 디지털 증거를 확보하는 컴퓨터 포렌식 도구로 활용되기 위해 만족해야 하는 기능적 명세를 제공한다. 데이터 수집도구는 디지털 데이터 원본의 완전하고 정확한 수집을 보장해야 하며, 오류 기록, 오류 발생 시 대체 및 수집 과정에서의 무결성 확인 기능을 제공해야 한다. 선택적으로 제공되는 기능에는 보관 과정에서의 무결성 확인, 이미지 파일 포맷 변경, 이미지 파일 분할 기능 등이 있으며, 수집 과정에 대한 정보 기록 등의 추가 기능도 존재한다.

3. 표준 적용 산업 분야 및 산업에 미치는 영향

현재 개발 중이거나 개발 예정인 컴퓨터 포렌식을 위한 디지털 데이터 수집도구들의 성능 개선을 기대할 수 있으며, 사용자가 신뢰성 있는 포렌식 도구를 선택할 수 있도록 가이드라인을 제시한다.

4. 참조 표준(권고)

4.1 국외표준(권고)

없음

4.2 국내표준

없음

5. 참조표준(권고)과의 비교

5.1 참조표준(권고)과의 관련성

해당사항 없음

5.2 참조한 표준(권고)과 본 표준의 비교표

해당사항 없음

6. 지적재산권 관련사항

2007 년 12 월 현재까지 본 표준과 관련된 지적재산권은 없음

7. 적합인증 관련사항

7.1 적합인증 대상 여부

해당사항 없음

7.2 시험표준제정여부(해당 시험표준번호)

해당사항 없음

8. 표준의 이력

판수	제/개정일	제.개정내역
제 1 판	2007. 12. 26	제정

Preface

1. The Purpose of Standard

This standard aims to provide guideline for improvement and design of the digital data acquisition tool for computer forensics. Also, it offers users some information so that they can choose and use the tool properly. And using that information, the person who works in the area of computer forensics can understand the ability of digital data acquisition tool well,

2. The summary of contents

This standard offers functional requirements for digital data acquisition tools using in digital forensics which acquire data from digital source and create disk image or clone of it. In order to use the digital data acquisition tools in the field of digital forensics, reliability of the tools is required to be ensured. Completeness and accuracy are important factors in data acquisition. The tool shall completely and accurately acquire all data from the digital source. Error reporting, error substitution, and integrity checking during acquisition are mandatory requirements also. In addition, there are some optional requirements such as integrity checking after acquisition, logging, conversion of an image file, etc.

3. Applicable fields of industry and its effect

This standard is to mitigate user's discredit on digital data acquisition tool for computer forensics and expand digital forensic tool market by supplying tool specification.

4. Reference Standards (Recommendations)

4.1 International Standards (Recommendations)

None

4.2 Domestic Standards

None

5. Relationship to Reference Standards(Recommendations)

5.1 The relationship of Reference Standards

Not applicable

5.2 Differences between Reference Standard(recommendation) and this standard

Not applicable

6. The Statement of Intellectual Property Rights

As of December 2007, any IPRs related to this standard cannot be found

7. The Statement of Conformance Testing and Certification

Not applicable

8. The History of Standard

Edition	Issued date	Contents
The 1st edition	2007. 12. 26	Established

목 차

1. 개요 1

2. 표준의 구성 및 범위 3

3. 정의 3

3.1. 용어 정의 3

3.2. 약어 4

4. 디지털 데이터 수집도구의 필수적인 요구사항 5

4.1. 일반적 요구사항 5

4.2. 디스크 이미지 작성시 요구사항 6

4.3. 쓰기방지 장치가 없는 환경에서의 요구사항 6

4.4. 디스크 이미지와 복제 디스크 생성 기능 동시 제공 시 요구사항 7

5. 디지털 데이터 수집도구의 선택적 기능 및 각 기능 별 요구사항 8

5.1. 디지털 데이터 수집도구의 선택적 기능 8

5.2. 디스크 이미지 파일 작성과 관련된 선택적 기능 8

5.3. 복제 디스크 생성과 관련된 선택적 기능 9

Contents

1. Introduction 1

2. Constitution and Scope 3

3. Terms and Definitions 3

3.1.Terms 3

3.2. Abbreviation 4

4. Mandatory Requirements of Digital Data Acquisition Tools 5

4.1. General requirements 5

4.2. Requirements for disk imaging 6

4.3. Requirements for unprotected acquisitions 6

4.4. Requirements for the tools imaging and creating of clone 7

5. Optional Functions and Requirements related to the Functions 8

5.1. Optional Functions 8

5.2. Optional Functions for disk imaging 8

5.3. Optional Functions for creating of clone 9

컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항

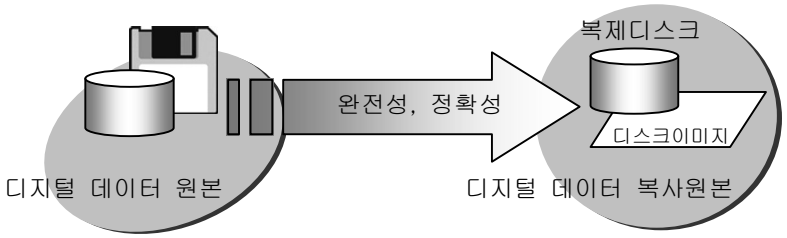
Digital Data Acquisition Tool Requirements for Computer Forensics

1. 개요

디지털 데이터는 그 특성상 복제가 쉬울 뿐만 아니라 원본과 사본의 구분이 어렵고, 데이터의 조작, 변경, 삭제 등이 매우 용이하다. 그러므로 디지털 데이터로부터 확보한 디지털 증거가 법적 효력을 가지기 위해서는 증거 데이터의 진정성, 무결성, 신뢰성, 원본성이 확보되어야 하고, 이를 위해 규격화되고 표준화된 디지털 포렌식 도구가 요구된다. 증거 데이터의 진정성이란 저장, 수집 과정에서 오류가 없으며, 의도된 결과가 정확히 획득되었고, 그로 인해 생성된 자료인 것임이 인정되어야 한다는 것이다. 무결성이란 증거 데이터가 저장된 매체에서 법정에 제출되기까지 변경이나 훼손 없이 보호되었다는 것을 말하며, 신뢰성이란 증거 데이터의 분석 등 처리에 사용된 장비 및 프로그램의 신뢰성이 입증되어야 한다는 것을 뜻한다. 디지털 증거 자체는 가시성과 가독성이 없으며 매체독립적인 정보이기 때문에 법정에 제출할 때 가시성, 가독성 있는 형태로 변환하여 제출하게 된다. 원본성이란 이러한 경우 제출되는 증거 데이터가 원 매체에 있는 증거와 동일해야 함을 의미한다.

디지털 증거 획득을 위한 데이터 처리는 평가(assessment), 수집(acquisition), 조사(examination) 및 문서화와 보고(documenting and reporting)의 4단계로 이루어진다. 이는 범죄 현장에서 범죄에 사용되었거나 연관된 디지털 증거를 포함하고 있는 시스템을 가려낸 후 해당 시스템으로부터 디지털 데이터를 수집하고, 수집된 데이터를 이용해 디지털 증거를 추출하는 조사과정을 거친 후 디지털 증거 및 조사과정을 문서화하여 보고하는 일련의 과정을 포함한다. 디지털 포렌식 도구는 독립된 각 단계별 기능을 제공할 수도 있고, 전체 과정을 포함하는 하나의 통합 시스템 형태로 존재할 수도 있다.

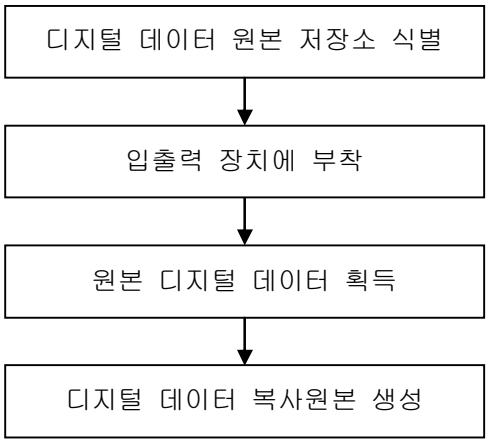
이 중 디지털 데이터 수집도구는 아래 (그림 1-1)에 나타낸 바와 같이 디지털 데이터 원본 저장소로부터 데이터를 읽어 디지털 데이터 원본과 동일한 데이터를 포함한 사본을 생성하는 것을 목표로 한다. 컴퓨터 포렌식 영역에서 분석을 위해 획득한 최초의 사본을 복사 원본이라 정의한다. 컴퓨터 포렌식에서 디지털 데이터 원본을 저장하는 디지털 데이터 복사 원본에는 하나 이상의 디스크 이미지, 또는 디지털 원본과 동일한 저장소 형태의 복제 디스크가 있다. 디스크 이미지는 디스크 이미지 탐색 기능을 갖는 특정 도구를 이용해 액세스되는데 반해 복제 디스크는 컴퓨터의 정상적인 파일 시스템을 통해 액세스된다.



(그림 1-1) 성공적인 디지털 데이터 수집

디지털 데이터 수집의 이상적인 목적은 완전성과 정확성이다. 완전한 수집이란 디지털 데이터 복사 원본이 비트 단위로 디지털 데이터 원본과 동일한 것을 말하며, 정확한 수집이란 디지털 데이터 복사 원본이 오류 없이 정확하게 생성되는 것을 의미한다.

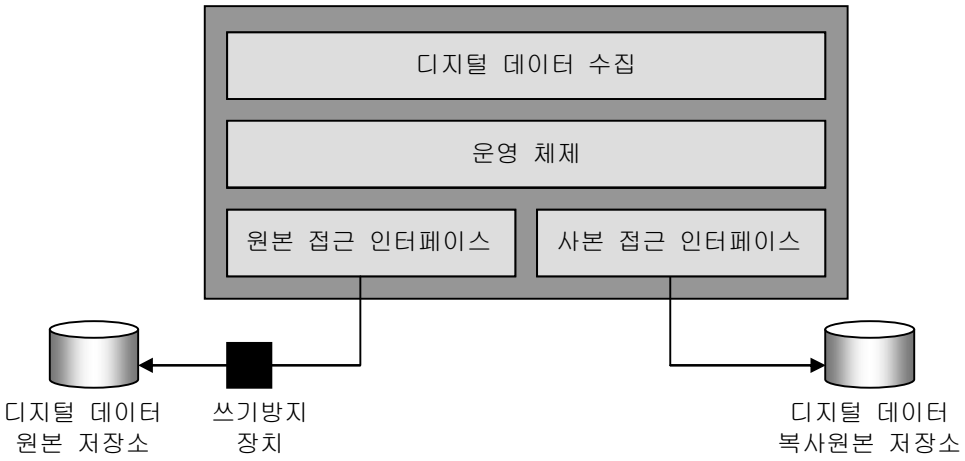
(그림 1-2)는 디지털 데이터 수집 과정을 나타낸 것이다. 디지털 데이터 수집 과정은 디지털 데이터 원본 저장소를 식별하고 입출력 장치에 부착 후 접근 인터페이스를 통해 디지털 데이터 원본을 획득 한 후 디지털 데이터 복사 원본 저장소에 복사 원본을 생성하는 과정으로 구성된다.



(그림 1-2) 디지털 데이터 수집 과정

획득 과정에서 사용되는 디지털 데이터 원본 저장소는 컴퓨터의 하드 디스크 드라이브, 카메라의 메모리 카드, 플래쉬 메모리 장치, 또는 분리 가능한 형태로 디지털 데이터 저장이 가능한 다른 다양한 디지털 매체와 같은 물리적 장치일 것이다. 다른 경우로 디지털 소스는 물리적 장치의 논리적인 드라이브일 수도 있다.

아래 (그림 1-3)은 디지털 데이터 수집 시스템의 구성을 나타낸 것이다. 획득을 위해 식별된 디지털 데이터 저장소를 컴퓨터 입출력 장치에 부착함에 있어 몇몇 데이터 수집 도구들은 시작과 종료 과정 동안 원본 데이터를 변경하기도 하므로 이를 막기 위해 쓰기방지 장치의 사용이 권장된다.



(그림 1-3) 디지털 데이터 수집 시스템 구성

2. 표준의 구성 및 범위

본 표준은 컴퓨터 포렌식 도구 중 컴퓨터의 접근 인터페이스로 접근 가능한 디지털 데이터 저장소로부터 데이터를 수집하는 도구가 가져야 할 요구 사항을 정의한다. 이동전화 단말, 호출기, PDA 등과 같은 다른 디지털 장치로부터 데이터를 획득하는 도구들은 포함하지 않는다. 데이터 획득도구의 적절하거나 부적절한 사용은 본 표준의 범위에 속하지 아니한다.

본 표준의 3장에서는 본 문서에서 사용되는 용어 및 약어를 나열하였다. 4장에서는 모든 디지털 데이터 수집도구가 만족해야 할 필수적인 요구 사항을 정의하고, 5장에서는 디지털 데이터 수집도구가 선택적으로 제공할 수 있는 기능 및 각 기능들이 제공된다는 조건하에서 디지털 데이터 수집도구가 만족해야 하는 요구 사항들을 명시한다.

3. 정의

3.1. 용어 정의

가. 디스크 이미지
: 디지털 데이터 원본의 비트 단위 데이터를 모두 포함하고 있는 파일

나. 디지털 데이터 복사 원본
: 디지털 데이터 원본으로부터 분석을 위해 획득한 최초의 사본

다. 디지털 데이터 수집
: 디지털 데이터 원본 저장소로부터 데이터를 획득하여 디지털 데이터 복사 원본을 생성하는 과정

라. 디지털 데이터 수집도구
: 디지털 데이터 수집 기능을 제공하는 하드웨어, 또는 소프트웨어적 도구

마. 디지털 데이터 원본
: 수집 대상이 되는 외부에서 접근 가능한 디지털 데이터

바. 디지털 데이터 원본 저장소
: 디지털 데이터 원본을 저장하고 있는 공간. 물리적 드라이브뿐만 아니라 파티션과 같은 논리적 드라이브, 연속적인 섹터들의 블록, 분리 가능한 디지털 매체 등을 포함함

사. 디지털 데이터 획득
: 디지털 데이터 원본 저장소로부터 디지털 데이터를 읽어 들이는 행위

아. 디지털 증거
: 디지털 형태로 저장되거나 전송되는 증거가치가 있는 정보

자. 디지털 포렌식
: 컴퓨터, 또는 기타 디지털 저장 매체에 남아 있는 디지털 증거를 법적 증거력을 갖도록 논리적이며 표준화된 절차와 방법을 통해 수집, 보관, 분석 및 보고하는 과정

차. 복제 디스크
: 디지털 소스와 비트 단위로 동일한 데이터를 포함하고 있는 디스크

카. 완전한 수집
: 디지털 데이터 복사 원본을 생성함에 있어 디지털 데이터 원본과 비트 단위로 동일하게 생성하는 것

타. 접근 인터페이스
: 디지털 데이터 저장장치에 접근하기 위해 사용되는 물리적 인터페이스와 접근 방법의 결합

파. 정확한 수집
: 디지털 데이터 복사 원본을 생성함에 있어 오류 없이 정확하게 생성하는 것

하. 컴퓨터 포렌식
: 컴퓨터의 접근 인터페이스를 통해 접근 가능한 디지털 데이터 원본 저장소로부터 법적 증거력을 갖도록 디지털 증거를 논리적이며 표준화된 절차와 방법을 통해 수집, 보관, 분석 및 보고하는 과정

3.2. 약어

PDA	Personal Digital Assistant

4. 디지털 데이터 수집도구의 필수적인 요구사항

본 절에서는 디지털 데이터 수집도구가 만족해야 할 필수적인 요구 사항을 열거한다. 본 절은 수집 도구의 일반적인 요구사항과 디스크 이미지 생성 기능을 갖는 수집도구의 요구사항 및 쓰기방지 장치가 없는 환경에서의 요구사항으로 구성된다.

4.1. 일반적 요구사항

모든 디지털 데이터 수집도구는 아래의 요구 사항을 만족해야 한다.

<표 4-1> 디지털 데이터 수집도구 요구사항

구분	요구사항
DA_MG_01	디지털 데이터 수집도구는 획득한 디지털 데이터 원본의 디스크 이미지나 복제 디스크를 생성할 수 있어야 한다.
DA_MG_02	디지털 데이터 수집도구는 디지털 데이터 원본 저장소의 전체 데이터를 수집할 수 있어야 한다.
DA_MG_03	디지털 데이터 수집도구는 디지털 데이터 원본 저장소의 일정 부분 데이터를 수집할 수 있어야 한다.
DA_MG_04	디지털 데이터 수집도구는 디지털 데이터 원본 저장소의 데이터를 완전하게 수집해야 한다.
DA_MG_05	디지털 데이터 수집도구는 디지털 데이터 원본 저장소의 데이터를 정확하게 수집해야 한다.
DA_MG_06	디지털 데이터 수집도구는 디지털 데이터 획득 과정에서 오류가 발생한다면 오류의 유형과 위치를 사용자에게 알려야 한다.
DA_MG_07	디지털 데이터 수집도구는 디지털 데이터 획득 과정에서 해결할 수 없는 오류가 발생한다면 복사 원본 저장소의 해당 위치에 분석 결과에 영향을 주지 않는 값으로 대체해야 한다.
DA_MG_08	디지털 데이터 수집도구는 디지털 데이터 복사 원본 작성시 저장소의 공간 부족을 포함한 기타 오류가 발생한다면 이를 사용자에게 알려야 한다.

* DA 는 data acquisition 을 의미한다.

* M 은 mandatory 를 의미한다.

* G 는 general 을 의미한다.

디지털 데이터 수집도구는 디지털 데이터 원본으로부터 복사 원본을 생성하는 도구로써 복사 원본의 형태로 디스크 이미지나 복제 디스크 둘 중 하나를 생성할 수 있어야 한다. 또한, 디스크 이미지와 복제 디스크 생성 기능을 동시에 가질 수 있으며, 이러한 경우의 요구사항은 4.3절을 따른다.

디지털 데이터 수집도구는 디지털 데이터 원본 저장소에 포함된 데이터 전체를 수집할 수 있는 기능을 제공해야 하며, 경우에 따라 사용자가 선택한 일정 부분의 데이터를 수집할 수 있는 기능을 제공해야 한다.

디지털 데이터 수집도구는 디지털 데이터 원본 저장소로부터 데이터를 획득해 복사 원

본을 생성함에 있어 원본 저장소의 배트섹터를 제외한 모든 디지털 데이터 원본과 비트 단위로 동일하게, 즉, 완전하게 생성해야 하며, 오류 없이 정확하게 생성해야 한다.

만일 디지털 데이터 원본 저장소로부터 데이터 획득 과정에서 오류가 발생한다면, 오류의 유형과 위치를 사용자에게 알려야 한다. 특히 획득 과정에서 해결할 수 없는 오류가 발생한다면 복사 원본 저장소의 해당 위치에 추후 분석 과정에 영향을 미치지 않도록 약속된 어떤 값을 대체하여야 한다. 만일 해당 비트를 임의로 '0'이나 '1'로 채운다면 이를 알지 못하는 분석 시스템에서는 이 값 또한 획득된 값이라 여기고 분석 및 검색에 사용할 것이다. 그러므로, 분석 시스템에서 오류라고 인지할 수 있는 다른 값으로 대체해야 한다.

디지털 데이터 원본으로부터 복사 원본을 생성하는 과정은 디지털 데이터 원본을 읽어 들여 지정된 저장소에 읽어 들인 데이터를 기록하는 것으로 이해할 수 있다. 이때 지정된 저장소에 기록하는 과정에서의 오류가 발생한다면 더 이상 작업을 진행할 수 없으므로 이에 대한 정확한 정보를 사용자에게 알리는 기능을 제공해야 한다.

4.2. 디스크 이미지 작성시 요구사항

디지털 데이터 수집도구가 디스크 이미지 생성 기능을 제공한다면, 디스크 이미지 생성과 관련해 아래의 요구 사항을 만족해야 한다.

<표 4-2> 디스크 이미지 생성 기능에 대한 요구사항

구분	요구사항
DA_MI_01	디지털 데이터 수집도구가 디스크 이미지 생성 기능을 갖는다면, 하나 이상의 디스크 이미지 포맷을 지원해야 한다.
DA_MI_02	디지털 데이터 수집도구가 디스크 이미지 생성 기능을 갖는다면, 디스크 이미지로부터 컴퓨터 파일 시스템으로 접근 가능한 디지털 데이터 원본 저장소와 동일한 형태의 디스크를 복원하는 수단을 제공해야 한다.

* I 는 imaging 을 의미한다.

디스크 이미지 생성 기능을 제공하는 디지털 데이터 수집도구는 하나 이상의 디스크 이미지 포맷을 제공해야 하며, 제공되는 디스크 이미지 포맷은 자체적으로 정의 가능하다. 단, 디스크 이미지로부터 컴퓨터 파일 시스템으로 접근 가능한 형태의 디스크를 복원하는 기능을 제공해야 한다..

4.3. 쓰기방지 장치가 없는 환경에서의 요구사항

(그림 1-3)에서 설명한 바와 같이 데이터 수집 과정에서 원본 데이터의 변경을 막기 위해 쓰기방지 장치의 사용이 권장되나, 유닉스의 쓰기권한을 해제한 마운팅이나 DOS 환경에서는 원본 데이터의 임의적 변경을 야기하지 않으므로 쓰기방지 장치의 사용이 강요되지는 않는다. 그러나 이러한 경우라도 사용자의 실수 등으로 인한 원본 데이터의 변경이 발생할 수 있으므로 쓰기방지 장치가 없는 환경에서 동작하는 디지털 데이터 수집도구는 아래의 요구사항을 만족해야 한다.

<표 4-3> 쓰기방지 장치가 없는 환경에서의 요구사항

구분	요구사항
DA_MW_01	디지털 데이터 수집도구가 쓰기방지 장치 없이 동작한다면, 데이터 수집 과정에서 데지털 데이터 원본의 변경이 발생했는지 확인하는 수단을 제공해야 한다.

*W 는 write blocker 를 의미한다.

4.4. 디스크 이미지와 복제 디스크 생성 기능 동시 제공 시 요구사항

디지털 데이터 수집도구가 디스크 이미지 파일 작성과 복제 디스크 생성 기능을 동시에 제공한다면 아래 요구사항을 만족해야 한다.

<표 4-4> 디스크 이미지와 복제 디스크 생성 기능 동시 제공 시 요구사항

구분	요구사항
DA_MG_01_01	디지털 데이터 수집도구가 디스크 이미지와 복제 디스크 둘다 생성하는 기능을 제공한다면, 사용자가 디스크 이미지와 복제 디스크 중 선택하여 생성할 수 있는 기능을 제공해야 한다.

5. 디지털 데이터 수집도구의 선택적 기능 및 각 기능 별 요구사항

본 절에서는 디지털 데이터 수집도구가 선택적으로 제공할 수 있는 기능 및 각 기능들이 제공된다는 조건하에서 디지털 데이터 수집도구가 만족해야 하는 요구 사항들을 명시한다.

5.1. 디지털 데이터 수집도구의 선택적 기능

디지털 데이터 수집도구는 아래 기능을 선택적으로 제공할 수 있다.

<표 5-1> 디지털 데이터 수집도구의 선택적 기능

구분	선택적 기능
DA_OG_01	디지털 데이터 복사 원본의 보관 과정에서 데이터 변동이 발생했는지 확인하는 기능
DA_OG_02	디지털 데이터 복사 원본의 보관 과정에서 데이터 변동이 발생했을 때 해당 위치를 알리는 기능
DA_OG_03	전체 디지털 데이터 수집 과정을 기록하는 기능

*O 는 optional 을 의미한다.

디지털 데이터 수집도구가 데이터 수집과정 기록 기능을 제공한다면, 아래와 같은 내용을 포함해야 한다.

1. 데이터 수집 도구에 대한 정보
2. 데이터 획득과 관련해 획득 일자, 획득 시간
3. 데이터 획득과 관련해 디스크 크기, 제조업자, 모델 번호, 시리얼 번호, 파티션 테이블 등 대상 장치의 정보
4. 데이터 획득과 관련해 획득된 데이터의 용량, 획득 결과
5. 획득자의 정보 및 사용자 의견

5.2. 디스크 이미지 파일 작성과 관련된 선택적 기능

디지털 데이터 수집도구가 디스크 이미지 생성 기능을 제공한다면, 디스크 이미지 생성과 관련해 아래 기능을 선택적으로 제공할 수 있다.

<표 5-2> 디스크 이미지 생성과 관련된 선택적 기능

구분	선택적 기능
DA_OI_01	디스크 이미지 생성시 디스크 이미지를 분할하여 생성할 수 있는 기능
DA_OI_02	디스크 이미지 저장소의 공간이 부족할 때 저장소를 전환하여 추가적인 디스크 이미지를 생성하는 기능
DA_OI_03	특정 포맷의 디스크 이미지를 다른 포맷의 디스크 이미지로 변환하는 기능
DA_OI_04	디스크 이미지의 일부에 대한 복제 디스크를 생성하는 기능
DA_OI_05	디스크 이미지 생성시 생성된 디스크 이미지를 압축하는 기능

DA_OI_06	디스크 이미지 생성시 생성된 디스크 이미지를 암호화하는 기능

모든 디지털 데이터 수집도구가 위에서 언급한 기능들을 제공해야 하는 것은 아니다. 즉, 디스크 이미지 생성시 디스크 이미지를 분할하여 생성할 수 있는 기능은 도구에 따라 제공할 수도 있고, 제공하지 않을 수도 있다. 그러나 만일 이 기능을 제공한다면 이와 연관되어 아래의 요구사항은 필수적으로 만족해야 한다.

<표 5-3> 디스크 이미지 분할 기능과 관련된 요구사항

구분	요구사항
DA_CI_01	디지털 데이터 수집도구가 디스크 이미지 분할 기능을 제공한다면, 전체 분할 디스크 이미지 내에 존재하는 데이터는 원본 데이터와 동일하여야 한다.
DA_CI_02	디지털 데이터 수집도구가 디스크 이미지 분할 기능을 제공한다면, 각 분할 디스크 이미지를 서로 다른 저장소에 저장할 수 있는 기능을 제공해야 한다.
DA_CI_03	디지털 데이터 수집도구가 디스크 이미지 분할 기능을 제공한다면, 사용자가 분할 디스크 이미지의 크기를 선택할 수 있는 기능을 제공해야 한다.

*C 는 conditional 을 의미한다.

마찬가지로 디스크 이미지 저장소 전환 기능도 필수적으로 제공해야 하는 것은 아니나, 디지털 데이터 수집도구가 디스크 이미지 저장소 전환 기능을 제공한다면 아래 요구사항을 만족해야 한다.

<표 5-4> 디스크 이미지 저장소 전환 기능과 관련된 요구사항

구분	요구사항
DA_CI_04	디지털 데이터 수집도구가 디스크 이미지 저장소 전환 기능을 제공한다면, 전체 분할 디스크 이미지 내에 존재하는 데이터는 획득된 원본 데이터와 동일하여야 한다.

디지털 데이터 수집도구가 디스크 이미지 포맷 변환 기능을 제공한다면 아래 요구사항을 만족해야 한다.

<표 5-5> 디스크 이미지 포맷 변환 기능과 관련된 요구사항

구분	요구사항
DA_CI_05	디지털 데이터 수집도구가 디스크 이미지 포맷 변환 기능을 제공한다면, 변환된 디스크 이미지와 원본 디스크 이미지내에 포함된 모든 데이터는 비트 단위로 동일해야 한다.

5.3. 복제 디스크 생성과 관련된 선택적 기능

디지털 데이터 수집도구가 복제 디스크 생성 기능을 제공한다면, 복제 디스크 생성과 관련해 아래 기능을 선택적으로 제공할 수 있다.

<표 5-6> 복제 디스크 생성과 관련된 선택적 기능

구분	선택적 기능
DA_OC_01	복제 디스크 저장소의 공간이 부족할 때 가능한 용량만큼 복제 디스크를 생성하는 기능

*C 는 clone 을 의미한다.

디지털 데이터 수집도구가 디지털 데이터 원본 저장소와 동일한 복제 디스크를 생성함에 있어 일반적으로 복제 디스크를 위한 저장소의 용량은 원본 저장소의 용량과 동일하거나 더 크도록 요구되지만 간혹 그렇지 못한 경우도 있을 수 있다. 일반적으로 이러한 경우, 쓰기오류 등이 발생하며 디지털 데이터 수집도구는 이를 인지하고 사용자에게 알리는 기능을 제공해야 한다. 그러나 선택적으로 부족하나마 준비된 저장소의 용량만큼이라도 복제 디스크를 생성할 수 있는 기능을 제공함으로써 주어진 상황에서 최선의 데이터 수집이 이루어지도록 할 수 있다.

표준작성 공헌자

표준 번호 : TTAS.KO-12.0057

이 표준의 제.개정 및 발간을 위해 아래와 같이 여러분들이 공헌하였습니다.

구분	성명	위원회 및 직위	연락처	소속사
과제 제안	길연희	PG102 위원	042-860-1031 yhgil@etri.re.kr	ETRI
표준 초안 제출	길연희	PG102 위원	042-860-1031 yhgil@etri.re.kr	ETRI
표준 초안 검토 및 작성	길연희	PG102 위원	042-860-1031 yhgil@etri.re.kr	ETRI
	은성경	PG102 부의장	042-860-5741 skun@etri.re.kr	ETRI
	홍도원	PG102 위원	042-860-6147 dwhong@etri.re.kr	ETRI
	인재형	PG102 참관자	02-3438-6600 injazz@finaldata.com	파이널데이터
	원유재	PG102 의장	02-405-5360 yjwon@kisa.or.kr	KISA
		외 PG102 위원		
표준안 심의	정교일	공통기반 기술위원회 의장	kyoil@etri.re.kr	ETRI
	김응배	공통기반 기술위원회 부의장	ebkim@etri.re.kr	ETRI
	원유재	공통기반 기술위원회 부의장	02-405-5360 yjwon@kisa.or.kr	KISA
	이필중	공통기반 기술위원회 부의장	054-279-2232 pjl@postech.ac.kr	포항공대
		외 공통기반 기술위원회 의장		
사무국 담당	김 선	팀 장	031-724-0080 skim@tta.or.kr	TTA
	오흥룡	과 장	031-724-0083 hroh@tta.or.kr	TTA

정보통신단체표준

컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항
(Digital Data Acquisition Tool Requirements for Computer Forensics)

발행인 : 김원식
발행처 : 한국정보통신기술협회
463-824, 경기도 성남시 분당구 서현동 267-2
Tel : 031-724-0114, Fax : 031-724-0119
발행일 : 2007.12