TTA Standard

정보통신단체표준(국문표준)

TTAS.KO-12.00XX

제정일: 2019년 12월 XX일

디지털 포렌식 조사를 위한 통합 정보 처리 규격 - 제 2부 : 데이터 종류별 규격 정의 -

Data Expression Standard for Digital Forensic Investigation: Part 2. Data Types and Definition

한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 사이버보안 프로젝트그룹(PG503)

표준안 심의 위원회　정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	이상진	고려대학교	교수	사이버보안프로젝트그룹 특별위원	
	한재혁	고려대학교	연구원		
표준 초안 작성자	이상진	고려대학교	교수	사이버보안프로젝트그룹 특별위원	
	손태식	아주대학교	교수		
	이성주	㈜인정보	이사		
	박경해	㈜클루드인	이사		
	한재혁	고려대학교	연구원		
	윤우성	고려대학교	연구원		
	김지언	고려대학교	연구원		
사무국 담당	황예지	TTA			

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2019.12

서 문

1 표준의 목적

디지털포렌식 조사는 디지털 데이터로부터 사건의 단서나 증거와 같은 정보를 도출하기 위해 정보저장매체로부터 데이터를 수집하고 분석한다. 이러한 조사 과정에서 처리되는 데이터는 그 데이터를 생성한 응용프로그램이나 저장되는 환경에 따라 매번 다르게 표현되기 때문에 효율적인 분석이 어려우며, 일관된 분석을 위해서는 정형화된 형태로 가공해야 한다.

이 표준은 디지털 포렌식 조사에서 동일한 성격의 데이터를 일관된 형태로 분석하기 위해 분석용 데이터의 저장 규격을 정의하는 것이 목적이다. 총 3부로 구성되어 있으며, 1부에서는 데이터 처리 규격을 정의하기에 앞서 개요와 요구사항을 정의하며, 2부에서는 데이터 종류별로 처리 규격을 정의하고, 3부에서는 기존 환경(레거시)을 고려하여 상호 호환성을 위한 사용방법을 정의한다.

2 주요 내용 요약

이 표준은 디지털 포렌식 조사에서 데이터를 처리하기 위한 규격을 구성하는 최소 단위인 객체의 속성을 데이터 종류별로 정의한다. 데이터 종류는 디지털 포렌식 조사에서 자주 사용되는 데이터를 대상으로 선정하였으며, 파일, 위치, 사람, 문자열 등 총 15가지를 대상으로 하였다. 특히, 파일 속성은 압축파일, 문서파일, 실행파일, 미디어파일(사진, 동영상) 등 구체적인 표현이 가능하도록 세분화하여 정의하였다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

- 해당 사항 없음

3.2 인용 표준과 본 표준의 비교표

- 해당 사항 없음

Preface

1 Purpose

On the digital forensic investigation, it's need to collect and analyze digital data, which is usually recorded on the storage media, to derive information from digital evidence. In this process, data is expressed fairly differently depending on the analysis environment by applications, methods, or investigators. The reason why it is difficult to analyze efficiently, therefore it should be processed in a regular form.

The purpose of this standard is to define the specification of the data expression in order to analyze digital data of the same categorization in a digital forensic investigation. This standard consists of three parts. Part 1 describes the framework and defines requirements, Part 2 defines the data types and specification for each data type, and Parr 3 describes the usage method for interoperability considering the existing environment (i.e. legacy)

2 Summary

This standard defines specifications of data expression for digital forensic investigation and suggests how to use it. This standard defines the properties of objects, which are the smallest unit that constitutes the specification for processing data. Data types were selected from the data which are frequently used in the digital forensic investigation, and 15 data types such as a file, location, person, and text were included. In particular, file attributes are defined by file type such as compression file, document file, execution file, and media file (photo, video).

3 Relationship to Reference Standards

3.1 Relationship to Reference Standards

- None

3.2 Comparison between This Standard and Reference Standards

- None

목 차

디지털포렌식 조사를 위한 데이터 처리 규격
- 제2부 : 데이터 종류별 규격 정의 -
(Data Expression Standard for Digital Forensic Investigation: Part 2. Data Types and Definition)

1 적용 범위

수사 과정에서 발견된 디지털 기기에는 많은 양의 데이터가 저장되어 있다. 디지털 포렌식 조사를 위해서는 디지털 기기 내에 있는 데이터를 수집해야 한다. 그리고 수집한 데이터를 여러 도구를 통해 분석하게 되는데, 이 과정에서 각 도구가 산출하는 분석 결과가 서로 상이한 경우가 많다. 따라서 분석 결과를 종합하여 공유하는데 상당한 시간이 소요된다. 이러한 문제점을 해결하기 위해 수집된 디지털 데이터를 추출하여 정규화하여 저장되도록 함으로써 일관된 형태로 분석할 필요가 있다. 이를 위해 데이터 종류별로 규격을 정의한다.

본 규격은 육하원칙을 기본으로 사용자 행위와 대상 파일의 생성 과정에 초점을 두고 정의하였으며, 육하원칙 적용이 어려운 정보의 경우 적용되는 일부의 필드에서만 정의하였다.

2 인용 표준

해당 사항 없음

3 용어 정의

3.1 메타데이터 (metadata)

일련의 데이터를 정의하고 설명해 주는 데이터. 컴퓨터에서는 데이터 사전의 내용, 스키마 등을 의미하고, 하이퍼텍스트 마크업 언어(HTML) 문서에서는 메타 태그 내의 내용이 메타데이터이다. 메타데이터는 여러 용도로 사용되나 주로 빠른 검색과 내용을 간략하고 체계적으로 기록하기 위해 많이 사용된다. [출처: TTA 정보통신용어사전]

3.2 레거시 (legacy)

과거에 개발되어 현재에도 사용 중인 낡은 하드웨어나 소프트웨어 [출처: TTA 정보통신용어사전]

3.3 오프셋 (offset)

컴퓨터 기억 장치에서 임의 주소에서 간격을 두고 떨어진 주소와의 거리 [출처: TTA 정보통신용어사전]

3.4 패킹 (packing)

실행파일(PE파일구조 등)에서 파일의 용량을 압축하고 역공학 등의 방법으로 실행되는 과정이 노출되는 것을 보호하기 위한 기법

3.5 포스트스크립트 (postscript)

미국 어도비사에서 개발한 페이지 기술 언어(PDL). 매끄럽고 섬세한 고품질 글자체(font)와 도형의 이미지를 프린터에 인쇄하거나 화면에 표시할 수 있게 한다. [출처: TTA 정보통신용어사전]

4 약어

EAT	Export Address Table
GPS	Global Positioning System
IAT	Import Address Table
JSON	Java Script Object Notation
PDL	Page Description Language
PE	Portable Executable
RFC	Request for Comment
SHA	Secure Hash Algorithm
SNS	Social Network Service
UTF	Unicode Transformation Format
TLS	Transport Layer Security

5 데이터 규격(속성) 정의

5.1 파일(file)

<표 5-1> 파일 객체의 속성

키 이름	자료형	반복수	설명
IsEncrypted	boolean	0..1	파일의 암호와 여부
IsDeleted	boolean	0..1	파일의 삭제 여부
FileName	String	0..1	파일 이름
FilePath	String	1..1	파일 저장경로
FileExtension	String	0..1	파일 확장자
FileSize	integer	0..1	파일 크기
MagicNumber	String	0..1	파일 시그니처
HashValue	String	0..1	해시값
HashType	String	0..1	해시함수의 종류
CreatedTime	datetime	0..1	파일이나 디렉터리가 생성된 시각
ModifiedTime	datetime	0..1	파일이나 디렉터리가 수정된 시각
MFTChangedTime	datetime	0..1	MFT 속성이 수정된 시각
AccessdTime	datetime	0..1	파일이나 디렉터리로 접근한 시각
DeteledTime	datetime	0..1	파일이나 디렉터리가 삭제된 시각
FileAttribute	list	0..1	파일 속성
Permission	list	0..1	파일 접근 권한
UserOwner	String	0..1	파일이나 디렉터리의 소유자
GroupOwner	String	0..1	파일이나 디렉터리의 그룹
ByteRuns	list	1..1	파일의 논리적인 위치
FilePassword	String	0..1	암호화된 파일의 비밀번호
Source	object	1..*	파일의 출처

5.1.1 압축파일(archive)

<표 5-2> 압축파일 객체 내용

키 이름	자료형	반복수	설명
Owner	string	0..1	생성자 정보
LastModifiedTime	datetime	0..*	마지막으로 수정한 시각
FileCount	integer	1..1	압축파일 내 포함된 파일의 수
ArchivedData	object	1..*	압축되어 있는 파일
Flags	string	0..1	파일에 적용된 설정 값
CompressionMethod	string	0..1	압축에 사용한 프로그램
Checksum	string	0..1	체크섬
Comment	string	0..1	파일에 대한 설명

5.1.2 실행파일(executable)

<표 5-3> 실행파일 객체 내용

키 이름	자료형	반복수	설명
IsPacked	boolean	0..1	파일의 패킹 여부
PackedMethod	string	0..*	파일에 적용된 패킹 방법
EntryPoint	integer	0..1	실행 진입 위치
ImportTableFunction	string	0..*	IAT 정의된 함수
ExportTableFunction	string	0..*	EAT 정의된 함수

5.1.3 문서파일(document)

<표 5-4> 문서파일 객체 내용

키 이름	자료형	반복수	설명
Author	string	1..*	작성자 정보
LastSavedBy	string	1..1	마지막으로 저장한 사용자 정보
CreatedTime	datetime	1..1	파일이 생성된 시간
LastSavedTime	datetime	1..1	마지막으로 저장된 시간
LastPrintedTime	datetime	1..1	마지막으로 출력된 시간
Templete	string	0..1	서식 파일
Company	string	0..1	사용자가 입력한 회사 정보
Subject	string	0..1	파일 주제
Tags	string	0..*	파일 태그 정보
RevisionNumber	string	0..1	수정 횟수
TotalTime	string	0..1	총 편집 시간
ProgramName	string	0..1	작성한 프로그램 이름
CodePage	string	0..1	사용한 코드 페이지
PageCount	integer	0..1	페이지 수
WordCount	integer	0..1	단어 수
LineCount	integer	0..1	줄 수
Comment	string	0..1	파일에 대한 설명
Attribute	string	0..1	파일 속성 (암호화, 읽기전용 등)

5.1.4 글꼴파일(font)

<표 5-5> 글꼴파일 객체 내용

키 이름	자료형	반복수	설명
FontFamilyName	string	1..1	글꼴의 대분류 이름
UniqueFontIdentifier	string	1..1	글꼴의 고유 식별자
FullFontName	string	1..1	글꼴의 이름
FontVersion	string	1..1	글꼴의 버전
PostscriptName	string	0..1	글꼴의 포스트스크립트 이름
FontDescription	string	0..1	글꼴 설명
FontURLVendor	string	1..1	글꼴이 제공되는 URL 정보

5.1.5 미디어파일(media)

<표 5-6> 미디어 객체 내용

키 이름	자료형	반복수	설명
Manufacturer	object	1..*	제조사 정보
Model	string	1..*	촬영 기기 정보
Editor	object	0..*	편집자 정보
DigitizedTime	datetime	1..*	디지털화 시각
LastModifiedTime	datetime	0..*	마지막으로 수정된 시각
Location	object	0..*	위치 정보
Resolution	string	0..*	해상도
Orientation	string	0..*	이미지 파일 기준 (가로, 세로)
Compression_method	string	0..*	압축 방법
Text	string	0..*	문자열 정보
MediaVersion	float	0..*	버전

5.1.6 메모리파일(memory)

<표 5-7> 메모리 객체 내용

키 이름	자료형	반복수	설명
IsInjected	bool	1..1	데이터 삽입 발생 여부
IsMapped	bool	1..1	메모리 할당 여부
IsProtected	bool	1..1	메모리 보호 기법 적용 여부
IsVolatile	bool	1..1	휘발성 여부
MemoryOSName	string	0..1	메모리가 사용된 운영체제 이름
RegionSize	integer	0..1	메모리 영역의 크기
BlockType	string	0..1	메모리의 블록 유형
RegionStartAddres	integer	0..1	메모리 영역의 시작 주소
RegionEndAddress	integer	0..1	메모리 영역의 끝 주소
ExtractedFeatures	string	0..1	추출된 특징들

5.2 위치(location)

<표 5-8> 위치기록 객체 내용

키 이름	자료형	반복수	설명
Duration	integer	0..*	이동 시간
StartPoint	string	1..1	시작지점
EndPoint	string	0..1	종료지점
StopPoint	string	0..*	경유지점
Address	string	0..1	특정 위치의 주소
Postcode	string	0..1	특정 위치의 우편번호
TelephoneNumber	string	0..*	특정 위치의 전화번호
Latitude	string	0..*	위도 표현
Longitude	string	0..*	경도 표현
LocationName	string	0..*	특정 지점, 경유지
Source	object	1..*	객체 내용의 출처

5.3 문자열(string)

<표 5-9> 문자열 객체 내용

키 이름	자료형	반복수	설명
StringContent	string	1..*	문자열 내용
CodePage	string	0..1	인코딩 종류
Grammar	object	0..1	문자열에 적용된 문법
Source	object	1..*	객체 내용의 출처

5.4 사람(people)

<표 5-10> 사람 객체 내용

키 이름	자료형	반복수	설명
Owner	object	1..1	사용자 계정 정보
Company	string	0..1	직장
LastName	string	1..1	성
FirstName	string	1..1	이름
PhoneNumber	string	1..*	전화번호
PhoneType	string	1..*	전화번호 속성 (개인, 직장 등)
Email	string	1..*	전자우편 주소
URL	string	1..*	블로그, 개인 홈페이지 주소
Address	string	1..*	주소
BankAccount	string	0..*	은행 계좌정보
Birthday	integer	0..1	생일
Memo	string	0..*	메모
Picture	string	0..*	사진
Application	string	0..*	사용 어플리케이션 정보
Source	object	1..*	객체 내용의 출처

5.5 일정(calender)

<표 5-11> 일정 객체 내용

키 이름	자료형	반복수	설명
AccountName	object	1..1	사용자 계정 정보
Attendants	object	0..*	참석자 정보
StartTime	datetime	0..1	일정 시작 시각
EndTime	datetime	0..1	일정 종료 시각
Repeat	integer	0..1	반복 여부, 횟수
Period	string	0..1	반복 주기
CreatedTime	datetime	1..1	일정 생성 시각
RemindTime	datetime	0..1	일정 알림 시각
Location	object	0..1	장소 정보
Title	string	1..1	일정 제목
Description	string	0..*	설명
Source	object	1..*	객체 내용의 출처

5.6 통화(call)

<표 5-12> 통화 객체 내용

키 이름	자료형	반복수	설명
From	object	1..1	발신자 정보
To	object	1..1	수신자 정보
StartTime	datetime	1..1	통화 시작 시각
EndTime	datetime	1..1	통화 종료 시각
Location	object	0..1	위치 정보
CallRecord	object	0..*	통화 녹음 파일
Application	string	0..1	사용 어플리케이션 정보
CallType	string	1..1	수신, 발신, 취소, 부재중 등
Source	object	1..*	객체 내용의 출처

5.7 클라우드(cloud)

<표 5-13> 클라우드 객체 내용

키 이름	자료형	반복수	설명
AccountName	object	1..1	사용자 계정 정보
Shared	string	0..*	공유 계정
CreatedTime	datetime	1..1	생성 시각
LastModifiedTime	datetime	1..1	마지막 수정 시각
IPAddress	string	0..1	IP 주소
FileName	string	0..*	파일명
Upload	bool	·0..1	업로드 여부
Download	bool	0..1	다운로드 여부
Source	object	1..*	객체 내용의 출처

5.8 연결(connection)

<표 5-14> 연결 객체 내용

키 이름	자료형	반복수	설명
From	object	1..1	발신자 정보
To	object	1..1	수신자 정보
StartTime	datetime	1..1	연결 시작 시각
EndTime	datetime	1..1	연결 종료 시각
Location	object	0..1	위치 정보
DomainName	string	0..1	도메인 이름
DeviceName	string	0..1	기기 이름
ConnectionType	string	0..1	연결 타입
Source	object	1..*	객체 내용의 출처

5.9 전자우편(email)

<표 5-15> 전자우편 객체 내용

키 이름	자료형	반복수	설명
From	object	1..1	전자우편 계정 정보
To	object	1..1	전자우편 계정 정보
CC	string	0..*	참조
BCC	string	0..*	숨은 참조
SendTime	datetime	1..1	보낸 시각
ReceiveTime	datetime	1..1	받은 시각
IPaddress	string	1..1	IP 주소
DomainName	string	0..1	도메인명
SMTPServer	string	0..1	경유지
Subject	string	0..1	메일 제목
Attachment	object	0..*	첨부 파일
Content	string	0..1	내용
Result	string	1..1	수신/발신 결과
Signature	string	0..1	서명
Source	object	1..*	객체 내용의 출처

5.10 거래(exchange)

<표 5-16> 거래기록 객체 내용

키 이름	자료형	반복수	설명
From	object	1..1	송신자 정보
To	object	1..1	수신자 정보
EventTime	datetime	1..1	거래가 발생한 시각
Location	object	0..1	장소 정보
TotalAmount	integer	1..1	거래 규모
Unit	list	0..1	거래 단위 (원, 달러, 박스 등)
Description	string	0..1	거래 내역
Method	string	0..1	송금 방법
Source	object	1..*	객체 내용의 출처

5.11 메시지(message)

<표 5-17> 메시지 객체 내용

키 이름	자료형	반복수	설명
From	object	1..1	발신자 정보
To	object	1..1	수신자 정보
SendTime	datetime	1..1	메시지 발신 시각
ReceiveTime	datetime	1..1	메시지 수신 시각
Location	object	0..1	위치 정보
Message	string	1..1	메시지 내용
Attachments	object	0..*	첨부 파일
Application	string	0..1	사용 어플리케이션 정보
ChatType	string	1..1	수신, 발신
Source	object	1..*	객체 내용의 출처

5.12 소셜 네트워크 서비스(social)

<표 5-18> 소셜 네트워크 서비스 객체 내용

키 이름	자료형	반복수	설명
AccountName	object	1..1	사용자 계정 정보
UploadTime	datetime	0..1	업로드 시각
Browser	string	0..1	브라우저 정보
Contents	object	1..1	게시한 내용
UploadType	string	0..1	업로드 방법
Source	object	1..*	객체 내용의 출처

5.13 웹 기록(web)

<표 5-19> 웹 기록 객체 내용

키 이름	자료형	반복수	설명
UserName	object	1..1	사용자 계정 정보
VisitedTime	datetime	1..1	방문 시각
LastAccessedTime	datetime	1..1	마지막으로 접근한 시각
ExpiredTime	datetime	1..1	파기 시각
DownloadTime	datetime	1..1	다운로드 시각
Browser	string	1..1	브라우저 정보
Path (file, save)	string	1..*	파일 경로(다운로드 시)
Host	string	1..1	호스트 PC
URLAddress	string	1..*	URL 주소
URLType	string	1..*	URL 종류(방문기록, 쿠키 등)
Description	string	0..*	설명
DownloadResult	boolean	1..*	다운로드 결과(T/F)
Title	string	1..*	해당 사이트 이름
Type	string	0..1	타입
VisitCount	integer	1..1	방문 횟수
Attribute	string	0..*	속성(즐겨찾기 등)
Source	object	1..*	객체 내용의 출처

5.14 시스템 로그(systemlog)

<표 5-20> 시스템 로그 객체 내용

키 이름	자료형	반복수	설명
ArtifactType	string	1..1	아티팩트 종류
AccountName	string	0..*	사용자 계정 이름
UserName	string	0..*	사용자 이름
ComputerName	string	0..1	컴퓨터 이름
DriveType	string	0..1	연결된 장치 종류
VolumeName	string	0..1	볼륨 이름
SerialNumber	string	0..1	장치고유번호
VendorName	string	0..1	제조사 이름
CreatedTime	datetime	1..1	파일 또는 디렉터리 생성된 시각
LastModifiedTime	datetime	1..1	마지막으로 수정된 시각
MFTModifiedTime	datetime	0..1	MFT 속성이 수정된 시각
LastAccessTime	datetime	1..1	마지막으로 접근한 시각
DeteledTime	datetime	0..1	삭제된 시각
EventOccuredTime	datetime	0..1	로그가 발생한 시각
LoggedInTime	datetime	0..1	로그인 시각
LoggedOutTime	datetime	0..1	로그아웃 시각
FullPath	string	1..1	파일 경로
FileName	string	1..1	파일 이름
FileSize	integer	1..1	파일 크기
FileAttribute	string	0..*	파일 속성(숨김, 암호화 등)
ExecutionCommand	string	0..*	실행창을 이용한 명령어
SearchKeyword	string	0..*	검색한 키워드
RemoteDesktopConnection	string	0..*	원격 데스크톱 연결 기록
NetworkDriveConnection	string	0..*	네트워크 드라이브 연결 기록
RecentFiles	string	0..*	최근 실행/열람된 파일
ExecutionAutoRun	string	0..*	자동으로 실행되는 프로세스
InstalledApplication	string	0..*	설치한 응용 프로그램 목록
ConnectedDevices	string	0..*	시스템에 연결된 매체

키 이름	자료형	반복수	설명
MacAddress	string	0..*	시스템의 MAC 주소
ProcessPath	string	0..*	프로세스 실행경로
ExecutionCount	string	0..*	응용 프로그램의 실행 횟수
LastExecutionTime	string	0..*	마지막 실행 시각
RunCounter	int	0..*	프로세스 실행 횟수
LinkedFilePath	string	0..*	연결된 파일 경로
ReferenceFile	string	0..*	참조하는 파일
ProviderName	string	0..1	이벤트로그 제공 이름
EventID	string	1..1	이벤트ID 번호
TaskCategory	string	0..1	작업 범주
TargetCreatiedTime	datetime	0..1	대상 파일의 생성시각
TargetModifiedTime	datetime	0..1	대상 파일의 수정시각
TargetAccessTime	datetime	0..1	대상 파일의 접근시각
Description	string	0..1	상세 설명
Source	object	1..*	객체 내용의 출처

5.15 네트워크 로그(network)

<표 5-21> 네트워크 로그 객체 내용

키 이름	자료형	반복수	설명
UserIP	object	1..1	사용자 계정 정보
StartTime	datetime	1..1	네트워크 연결 시작 시각
EndTime	datetime	1..1	네트워크 연결 완료 시각
SourceAddress	string	1..1	네트워크 출발지 소켓 주소
DestinationAddress	string	1..1	네트워크 목적지 소켓 주소
NetworkAdapter	string	0..1	네트워크 어댑터
State	string	1..*	네트워크 상태
TLSUsed	bool	0..1	TLS 사용 여부
Source	object	1..*	객체 내용의 출처

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

Ⅰ-1.1 지식재산권 확약서

해당 사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

Ⅰ-2.1 시험인증 대상 여부

해당 사항 없음

Ⅰ-2.2 시험표준 제정 현황

해당 사항 없음

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

Ⅰ-3.1 디지털 포렌식 조사를 위한 통합 정보 처리 규격 - 제1부 : 개요 및 요구사항

핵심 개념을 정의하는 문서로 표준에서 다루는 표현 범위와 기본적인 개념, 참고표준과 비교를 통해 차별되는 특징에 대한 설명을 제공

Ⅰ-3.2 디지털 포렌식 조사를 위한 통합 정보 처리 규격 - 제3부 : 데이터 처리 상호 호환을 위한 참조 모델

규격의 활용을 유스케이스로 제시하고 레거시와 상호 호환을 위한 참조 모델을 제공

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] TTAK.KO-12.0080, "디지털 증거 파일 교환포맷", 2008.12.19.

[2] TTAE.OT-12.0019, "구조화된 위협 정보 표현 규격(STIX) 버전 2.0", 2018.12.19.

[3] KS X 1220, "디지털 증거 데이터 패키지", 2014.11.28.

[4] TTAS.KO-12.0058/R1, "디지털 증거 수집 보존 가이드라인", 2017.12.13.

[5] OASIS Cyber Threat Intelligence (CTI) TC, STIX(Structured Threat Information Expression) 2.0, 2018.05.10.

[6] Mirtre, Cyber Observable eXpression(CybOX) 2.1, 2014.01.23.

[7] Rutkowski A, Kadobayashi Y, Furey I, Rajnovic D, Martin R, Takahashi T, Schultz C, Reid G, Schudel G, Hird M, Adegbite S., "CYBEX – The Cybersecurity Information Exchange Framework (X.1500)", ACM SIGCOMM Computer Communication Review. 40(5), pp. 59-64. 2010.10.22.

[8] Casey E, Barnum S, Griffith R, Snyder J, van Beek H, Nelson A., "Advancing coordinated cyber-investigations and tool interoperability using a community developed specification language", Digital Investigation. 22, pp. 14-45. 2017.09.01.

[9] Biasiotti, M.A., Mifsud Bonnici, J.P., Cannataci, J., Turchi, F. "Handling and Exchanging Electronic Evidence Across Europe", Vol. 39. Springer, 2018.

[10] Casey E, Back G, Barnum S., "Leveraging CybOX™ to standardize representation and exchange of digital forensic information", Digital Investigation. 12, pp. S102-110. 2015.05.01.

[11] Garfinkel, S., "Digital forensics XML and the DFXML toolset", Digital Investigation, 8(3-4), pp.161-174. 2012.

[12] TTAE.IF-RFC3339, “날짜와 시간 표현 형식에 관한 프로파일”, 2004.12.23.

※ 상기 기재된 참고 문헌의 발간일이 기재된 경우, 해당 표준(문서)의 해당 버전에 대해서만 유효하며, 연도를 표시하지 않은 경우에는 해당 표준(권고)의 최신 버전을 따름

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2019.12.XX	제정 TTAK.KO-12.00xx	-	사이버보안 프로젝트그룹 (PG503)