INTERNET-DRAFT
<draft-inacio-mile-forensics-01>
Category: Standard

Expires: May 10, 2013

Christopher Inacio
Carnegie Mellon University
Younhee gil
ETRI

November 6, 2012

Digital Forensics Extension for IODEF
draft-inacio-mile-forensics-01

Abstract

This extension to IODEF (RFC 5070) is designed to aid in the sharing and dissemination of digital forensics information. The goal is to allow a tool independent format to share information between organizations focused on digital forensics: drive images, file carving, metadata, and related hashes. As with IODEF and its extensions, it is defined using XML.

Status of this Memo

Copyright and License Notice

Table of Contents

1 Introduction

This extension to IODEF is designed to carry digital forensics information in a way acceptable for chain of evidence handling and general forensics examination. There are various programs that generate forensics information, but few that generate that information in a way that is exchangeable in a universal way.

There have been some efforts to create independent standards, often XML based, to exchange digital forensics information. Indeed, this standard is designed to incorporate features from those efforts, DFXML, DEXF, IOC, and DFRWS. By extending IODEF, however, the goal of this standard is to build upon a widely used IETF standard, take advantage of the other features within the IODEF family of standards.

The main pieces of information this extension seeks to be able to convey are information about file systems and the resulting products from analyzing file systems. This includes information about file carving, system metadata including disk metadata.

1.1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Forensic Extension to IODEF

The Forensics Data is captured within a new class within IODEF's Event Data class, within its Additional Data class. The Forensics Data is not required to be present, and may occur an unlimited number of times as needed.

```
+-------------+
|   Incident  |
+-------------+
|      .      |
|      .      |
|      .      |
| Event Data  |<>-{0..*}-[ Event Data ]
|             |            |<>-{0..*}-[ Additional Data ]
|             |                          |<>-{0..*}-[ Forensics Data]
|             |
+-------------+
```

3. Forensics Data

```
   +----------------+
   | Forensics Data |
   +----------------+
   |                |<>-[Version]
   |                |    |<>-[Major]
   |                |    |<>-[Minor]
   |                |<>-[Site Name]
   |                |<>-[Examiner Name]
   |                |<>-[Evidence ID]
   |                |<>-[Creation Time]
   |                |<>-[Tool Name]
   |                |<>-[Tool Version]
   |                |<>-[Host Operating System]
   |                |
   |                |<>-[Device]
   |                |       |<>-[Device Type]
   |                |       |<>-[Device Model]
   |                |       |<>-[Device Serial]
   |                |       |<>-{0..1}-[Sector Size]
   |                |       |<>-{0..1}-[Device Sectors]
   |                |       |<>-{0..*}-[Hash]
   |                |       |            |<>-[Hash Type]
   |                |       |            |<>-[Hash Size]
   |                |       |            |<>-[Hash Value]
   |                |       |<>-{0..*}-[File Object]
   |                |                   |<>-[Name]
   |                |                   |<>-[ID]
   |                |                   |<>-[Size]
   |                |                   |<>-[Partition]
   |                |                   |<>-[Mode]
   |                |                   |<>-[ACL]
   |                |                   |<>-[mtime]
   |                |                   |<>-[atime]
   |                |                   |<>-[ctime]
   |                |                   |<>-{0..*}-[Byte Run]
   |                |                               |<>-{1..*}-[Hash]
   |                |                                           |<>-[Hash Type]
   |                |                                           |<>-[Hash Size]
   |                |                                           |<>-[Hash
Value]
   |                |<>-[Digital Signature]
   +----------------+
```

3.1 Forensics Type Descriptions

All date-time stamps are compatible with the date-time strings as defined in IODEF [IODEF] which are compatible with RFC 3339 [RFC3339], a restricted subset of ISO 8601:2000 [ISO8601].

3.1.1 Header Information

O Version {Major,Minor} - The version number of the Digital Forensics extension schema definition. These will be defined within the standard schema, available from IANA.

o Site Name - A text string which is a human readable definition of the site that analyzed the contained forensics data.

o Creator Name - The name of the examiner that analyzed or provided the raw data presented within the signed forensics extension.

o Evidence ID - A site specific ID used for tracking the forensics information. For example, a case number for chain of evidence maintenance.

o Creation Time - The time this record was created.

o Device Time - A record of the creation from the forensic data source.

o Tool Name - A string defining the tool used to process the forensics data.

o Tool Version - A version string containing all relevant release information for the generating forensics data tool.

o Host Operating System - The host operating system on which the forensics tool was run; defined in CPE [CPE] format.

3.1.2 Device/Source Information

o Device Type - A string describing the type of device from which data capture was performed. The device types are: hard disk, USB flash, XD card, SSD, CD, DVD, and other.
o Device Model - The model number, provided by the manufacturer, of the device.
o Device Serial - The manufacturer given serial number for the device.
o Sector Size - The size of the sectors on the device, if the device has sector based storage.
o Device Sectors - If the device is sector based, this is the total number of sectors available on the device.

3.1.3 Hash Information

o Hash Type - The hash algorithm used to compute the associated hash. The supported algorithms are MD5, SHA-1, SHA-256.

o Hash Size - The number of octets included in the associated hash value.

o Hash Value - The value of the hash for the related information. The hash value MUST be represented as UTF-8 encoded hexadecimal string value.

3.1.4 Byte Run Information

- Byte Run

3.1.5 File Object Information

- File Object - A collection of values, capturing the relevant file system metadata along with relevant forensic data (byte runs and hashes) for a file of interest.

- Name - The name of the file as captured from the file system metadata.

- ID - A site generated unique number.

- Size - The size of the file, as captured from the file system metadata.

- Partition - The partition that the file system that file came from resides within.

- Mode - File permission mode as captured from the file system.

- ACL - The access control list as captured from the file system.

- mtime - File modification time as captured from the metadata from the filesystem.

- atime - Last file access time as captured from the metadata from the filesystem.

- ctime - Creation time as captured from the metadata from the filesystem.

2. Title

<Document text>

```
Definitions and code {
  line 1
  line 2
}
```

Special characters examples:

The characters , , ,
However, the characters \0, \&, \%, \" are displayed.

.ti 0 is displayed in text instead of used as a directive.
.\" is displayed in document instead of being treated as a comment

C:\dir\subdir\file.ext Shows inclusion of backslash "\".

3 Security Considerations

This standard is an extension to IODEF [IODEF] and as such, the security considerations that apply to IODEF apply to this extension.

In addition, the security provided by the related RID [RID] enhancements apply equally to this extensions as to IODEF [IODEF].

4 IANA Considerations

Registration request for the IODEF Digital Forensics Extension namespace:

URI: urn:ietf:params:xml:ns:iodef-digitalforensics-1.0

Registrant Contact:

Christopher Inacio Carnegie Mellon University 4500 5th Ave
Pittsburgh, PA 15213 USA inacio@cert.org

XML: schema in Appendix N.

5 References

5.1 Normative References

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[IODEF] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident Object Description Exchange Format", RFC 5070, December 2007.

[RID] Moriarty, K., "Real-time Inter-network Defense (RID)", RFC 6045, November 2010.

[RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, July 2002.

5.2 Informative References

[DFXML] Garfinkel, S., "Digital forensics XML and the DFXML toolset", Digital Investigation, 2012.

[DEXF] Gil, Y. H., Hong, D., Rutkowski, A. M., "Revised draft on

Recommendation ITU-T X.def: digital forensics exchange
format", ITU Study Group 17, September 2, 2011.

[NIJ199408] "NIJ Special Report 199408: Forensic Examination of
Digital Evidence: A Guide for Law Enforcement"

[ISO8601]   International Organization for Standardization,
"International   Standard: Data elements and
interchange formats - Information   interchange -
Representation of dates and times", ISO 8601,
Second Edition, December 2000.

Authors' Addresses

Christopher Inacio
4500 5th Ave.
Pittsburgh, PA 15143
USA

EMail: inacio@cert.org

Younhee gil
Electronics and Telecommunications Research Institute

EMail: yhgil@etri.re.kr

Appendix A: Digital Forensics XML Schema

[[preliminary schema here]]

```
   <?xml version="1.0" encoding="UTF-8"?>
   <xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
               xmlns:digitalforensics="urn:ietf:params:xml:ns:iodef-
digitalforensics-1.0"
               targetNamespace="urn:ietf:params:xml:ns:iodef-
digitalforensics-1.0"
               elementFormDefault="qualified"
               attributeFormDefault="unqualified">


       <xsd:element name="digitalforensics" type="digitalforensicsType"/>

       <xsd:element name="digitalforensicsType"/>
       <xsd:complexType name="digitalforensicsType">
           <xsd:attribute name="MajorVersion"type="xsd:integer" use="required"/
>
```

```
           <xsd:attribute name="MinorVersion"type="xsd:integer" use="required"/
>
       </xsd:complexType>
       <!-- HASH type definition -->
       <xsd:simpleType name="hashType">
           <xsd:restriction base="xsd:string">
               <xsd:enumeration value="MD5"/>
               <xsd:enumeration value="SHA-1"/>
               <xsd:enumeration value="SHA-256"/>
           </xsd:restriction>
       </xsd:simpleType>
       <xsd:simpleType name="hashSize" type="xsd:integer"/>
       <xsd:simpleType name="hashValue" type="xsd:string">
           <xsd:restriction>
               <pattern value='[a-fA-F0-9]+'>
           </xsd:restriction>
       </xsd:simpleType>
       <xsd:complexType name="hash">
           <xsd:sequence>
               <xsd:element ref="hashType"/>
               <xsd:element ref="hashSize"/>
               <xsd:element ref="hashValue"/>
           </xsd:sequence>
       </xsd:complexType>

       <!-- byte runs -->
       <xsd:element name="run">
           <xsd:complexType>
               <xsd:attribute name="filesystem_offset"
type="xsd:nonNegativeInteger"/>
               <xsd:attribute name="file_offset" type="xsd:nonNegativeInteger"/
>
               <xsd:attribute name="image_offset"
type="xsd:nonNegativeInteger"/>
               <xsd:attribute name="len" type="xsd:nonNegativeInteger"/>
           </xsd:complexType>
           <xsd:element ref="hash"/>
       </xsd:element>
       <xsd:element name="byte_run">
           <xsd:complexType>
               <xsd:sequence>
                   <xsd:element ref="run" minOccurs="1" maxOccurs="unbounded"/>
               </xsd:sequence>
           </xsd:complexType>
       </xsd:element>

       <!-- File Object Definition -->
       <!-- name, ID, Size, Partition, Mode, ACL, mtime, atime, ctime -->
       <xsd:element name="file_object">
           <xsd:complexType>
               <xsd:sequence>
```

```
                   <!-- <xsd:element name="" type="" minOccurs=""/> -->
                   <xsd:element name="filename" type="xsd:string" minOccurs="0"
maxOccurs="1"/>
                   <xsd:element name="id" type="xsd:string" minOccurs="0"/>
                   <xsd:element name="filesize" type="xsd:positiveInteger"
minOccurs="0"/>
                   <xsd:element name="partition" type="xsd:nonNegativeInteger"
minOccurs="0"/>
                   <xsd:element name="mode" type="xsd:nonNegativeInteger"
minOccurs="0"/>
                   <xsd:element name="acl" type="xsd:string" minOccurs="0"/>
                   <xsd:element name="mtime" type="" minOccurs="0"/>
                   <xsd:element name="atime" type="" minOccurs="0"/>
                   <xsd:element name="ctime" type="" minOccurs="0"/>
                   <xsd:element ref="byte_run" minOccurs="0"/>
                   <xsd:element ref="hash" minOccurs="0"/>
               </xsd:sequence>
           </xsd:complexType>
       </xsd:element>

   </xsd:schema>
```