



STIX™ Version 2.0. Part 4: Cyber Observable Objects

Committee Specification Draft ~~01~~02 /
Public Review Draft ~~01~~02

~~24 February~~03 May 2017

Specification URIs

This version:

<http://docs.oasis-open.org/cti/stix/v2.0/csprd02/part4-cyber-observable-objects/stix-v2.0-csprd02-part4-cyber-observable-objects.docx> (Authoritative)
<http://docs.oasis-open.org/cti/stix/v2.0/csprd02/part4-cyber-observable-objects/stix-v2.0-csprd02-part4-cyber-observable-objects.html>
<http://docs.oasis-open.org/cti/stix/v2.0/csprd02/part4-cyber-observable-objects/stix-v2.0-csprd02-part4-cyber-observable-objects.pdf>

Previous version:

<http://docs.oasis-open.org/cti/stix/v2.0/csprd01/part4-cyber-observable-objects/stix-v2.0-csprd01-part4-cyber-observable-objects.docx> (Authoritative)
<http://docs.oasis-open.org/cti/stix/v2.0/csprd01/part4-cyber-observable-objects/stix-v2.0-csprd01-part4-cyber-observable-objects.html>
<http://docs.oasis-open.org/cti/stix/v2.0/csprd01/part4-cyber-observable-objects/stix-v2.0-csprd01-part4-cyber-observable-objects.pdf>

Previous version:

N/A

Latest version:

<http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part4-cyber-observable-objects.docx>
(Authoritative)
<http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part4-cyber-observable-objects.html>
<http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part4-cyber-observable-objects.pdf>

Technical Committee:

OASIS Cyber Threat Intelligence (CTI) TC

Chair:

Richard Struse (Richard.Struse@HQ.DHS.GOV), DHS Office of Cybersecurity and Communications (CS&C)

Editors:

~~Ivan Kirillov (ikirillov@mitre.org), MITRE Corporation~~
Trey Darley (trey@kingfisherops.com), Kingfisher Operations, sprl
~~Ivan Kirillov (ikirillov@mitre.org), MITRE Corporation~~

Additional artifacts:

This prose specification is one component of a Work Product that also includes:

- STIX™ Version 2.0. Part 1: STIX Core Concepts. <http://docs.oasis-open.org/cti/stix/v2.0/csprd042/part1-stix-core/stix-v2.0-csprd042-part1-stix-core.html>.
- STIX™ Version 2.0. Part 2: STIX Objects. <http://docs.oasis-open.org/cti/stix/v2.0/csprd02/part2-stix-objects/stix-v2.0-csprd02-part2-stix-objects.html>.

- *STIX™ Version 2.0. Part 3: Cyber Observable Core Concepts*. <http://docs.oasis-open.org/cti/stix/v2.0/csprd02/part3-cyber-observable-core/stix-v2.0-csprd02-part3-cyber-observable-core.html>.
- (this document) *STIX™ Version 2.0. Part 4: Cyber Observable Objects*. <http://docs.oasis-open.org/cti/stix/v2.0/csprd04/part4-cyber-observable-objects/stix-v2.0-csprd04-part4-cyber-observable-objects.html>.
- *STIX™ Version 2.0. Part 5: STIX Patterning*. <http://docs.oasis-open.org/cti/stix/v2.0/csprd02/part5-stix-patterning/stix-v2.0-csprd02-part5-stix-patterning.html>.

Related work:

This specification replaces or supersedes:

- *STIX™ Version 1.2.1. Part 1: Overview*. Edited by Sean Barnum, Desiree Beck, Aharon Chernin, and Rich Piazza. Latest version: <http://docs.oasis-open.org/cti/stix/v1.2.1/stix-v1.2.1-part1-overview.html>.
- *Cybox™ Version 2.1.1. Part 01: Overview*. Edited by Trey Darley, Ivan Kirillov, Rich Piazza, and Desiree Beck. Latest version: <http://docs.oasis-open.org/cti/cybox/v2.1.1/cybox-v2.1.1-part01-overview.html>.

This specification is related to:

- *TAXII™ Version 2.0*. Edited by ~~Bret Jordan and John Wunder~~, Mark Davidson, and ~~Bret Jordan~~. Latest version: <http://docs.oasis-open.org/cti/taxii/v2.0/taxii-v2.0.html>. ~~Work in progress.~~

Abstract:

Structured Threat Information Expression (STIX™) is a language for expressing cyber threat and observable information. This document defines a set of cyber observable objects that can be used in STIX and elsewhere.

Status:

This document was last revised or approved by the OASIS Cyber Threat Intelligence (CTI) TC on the above date. The level of approval is also listed above. Check the “Latest version” location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti#technical.

TC members should send comments on this specification to the TC’s email list. Others should send comments to the TC’s public comment list, after subscribing to it by following the instructions at the “[Send A Comment](#)” button on the TC’s web page at <https://www.oasis-open.org/committees/cti/>.

This Committee Specification Public Review Draft is provided under the Non-Assertion Mode of the OASIS IPR Policy, the mode chosen when the Technical Committee was established. For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC’s web page (<https://www.oasis-open.org/committees/cti/ipr.php>).

Note that any machine-readable content ([Computer Language Definitions](#)) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any such plain text file and display content in the Work Product’s prose narrative document(s), the content in the separate plain text file prevails.

Citation format:

When referencing this specification the following citation format should be used:

[STIX-v2.0-Pt4-Cyb-Objects]

STIX™ Version 2.0. Part 4: Cyber Observable Objects. Edited by ~~Trey Darley and Ivan Kirillov and Trey Darley~~, ~~24 February~~, 03 May 2017. OASIS Committee Specification Draft ~~0402~~ / Public Review Draft 0402. <http://docs.oasis-open.org/cti/stix/v2.0/csprd02/part4-cyber-observable-objects/stix-v2.0-csprd02-part4-cyber-observable-objects.html>. Latest version: <http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part4-cyber-observable-objects.html>.

Notices

Copyright © OASIS Open 2017. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full [Policy](#) may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of [OASIS](#), the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <https://www.oasis-open.org/policies-guidelines/trademark> for above guidance.

Portions copyright © United States Government 2012-2016~~7~~^Z. All Rights Reserved.

STIX™, CYBOX™, AND TAXII™ (STANDARD OR STANDARDS) AND THEIR COMPONENT PARTS ARE PROVIDED "AS IS" WITHOUT ANY WARRANTY OF ANY KIND, EITHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY THAT THESE STANDARDS OR ANY OF THEIR COMPONENT PARTS WILL CONFORM TO SPECIFICATIONS, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR FREEDOM FROM INFRINGEMENT, ANY WARRANTY THAT THE STANDARDS OR THEIR COMPONENT PARTS

WILL BE ERROR FREE, OR ANY WARRANTY THAT THE DOCUMENTATION, IF PROVIDED, WILL CONFORM TO THE STANDARDS OR THEIR COMPONENT PARTS. IN NO EVENT SHALL THE UNITED STATES GOVERNMENT OR ITS CONTRACTORS OR SUBCONTRACTORS BE LIABLE FOR ANY DAMAGES, INCLUDING, BUT NOT LIMITED TO, DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, ARISING OUT OF, RESULTING FROM, OR IN ANY WAY CONNECTED WITH THESE STANDARDS OR THEIR COMPONENT PARTS OR ANY PROVIDED DOCUMENTATION, WHETHER OR NOT BASED UPON WARRANTY, CONTRACT, TORT, OR OTHERWISE, WHETHER OR NOT INJURY WAS SUSTAINED BY PERSONS OR PROPERTY OR OTHERWISE, AND WHETHER OR NOT LOSS WAS SUSTAINED FROM, OR AROSE OUT OF THE RESULTS OF, OR USE OF, THE STANDARDS, THEIR COMPONENT PARTS, AND ANY PROVIDED DOCUMENTATION. THE UNITED STATES GOVERNMENT DISCLAIMS ALL WARRANTIES AND LIABILITIES REGARDING THE STANDARDS OR THEIR COMPONENT PARTS ATTRIBUTABLE TO ANY THIRD PARTY, IF PRESENT IN THE STANDARDS OR THEIR COMPONENT PARTS AND DISTRIBUTES IT OR THEM "AS IS."

Table of Contents

1	Introduction	8
1.0.1	IPR Policy	8
1.1	Terminology	8
1.2	Normative References	8
1.3	Naming Requirements	10
1.3.1	Property Names and String Literals	10
1.3.2	Reserved Names	10
1.4	Document Conventions	10
1.4.1	Naming Conventions	10
1.4.2	Font Colors and Style	10
2	Defined Object Data Models	12
2.1	Artifact Object	12
2.1.1	Properties	12
2.2	AS Object	13
2.2.1	Properties	13
2.3	Directory Object	14
2.3.1	Properties	14
2.4	Domain Name Object	15
2.4.1	Properties	15
2.5	Email Address Object	16
2.5.1	Properties	16
2.6	Email Message Object	17
2.6.1	Properties	17
2.6.2	Email MIME Component Type	19
2.6.2.1	2.6.2.1 Properties	20
2.7	File Object	23
2.7.1	Properties	23
2.7.2	Archive File Extension	27
2.7.2.1	Properties	27
2.7.3	NTFS File Extension	28
2.7.3.1	Properties	29
2.7.3.2	Alternate Data Stream Type	29
2.7.3.2.1	Properties	29
2.7.4	PDF File Extension	30
2.7.4.1	Properties	30
2.7.5	Raster Image File Extension	31
2.7.5.1	Properties	31
2.7.6	Windows™ PE Binary File Extension	32
2.7.6.1	Properties	32
2.7.6.2	Windows™ PE Binary Vocabulary	33
2.7.6.3	PE Optional Header Type	34
2.7.6.3.1	Properties	34
2.7.6.4	Windows™ PE Section Type	36

2.7.6.4.1 Properties	36
2.8 IPv4 Address Object	38
2.8.1 Properties	39
2.9 IPv6 Address Object	40
2.9.1 Properties	40
2.10 MAC Address Object	41
2.10.1 Properties	41
2.11 Mutex Object.....	42
2.11.1 Properties	42
2.12 Network Traffic.....	42
2.12.1 Properties	43
2.12.2 HTTP Request Extension	49
2.12.2.1 2.12.2.1 Properties.....	49
2.12.3 ICMP Extension.....	50
2.12.3.1 Properties	51
2.12.4 Network Socket Extension	51
2.12.4.1 Properties	52
2.12.4.2 Network Socket Address Family Enumeration	52
2.12.4.3 Network Socket Protocol Family Enumeration	53
2.12.4.4 Network Socket Type Enumeration	54
2.12.5 TCP Extension	55
2.12.5.1 Properties	56
2.13 Process Object	57
2.13.1 Properties	57
2.13.2 Windows™ Process Extension	59
2.13.2.1 Properties.....	59
2.13.3 Windows™ Service Extension	60
2.13.3.1 Properties.....	61
2.13.3.2 Windows™ Service Start Type Enumeration.....	61
2.13.3.3 Windows™ Service Type Enumeration	62
2.13.3.4 Windows™ Service Status Enumeration	62
2.14 Software Object	63
2.14.1 Properties	64
2.15 URL Object	65
2.15.1 Properties	65
2.16 User Account Object.....	65
2.16.1 Properties	65
2.16.2 Account Type Vocabulary	67
2.16.3 UNIX™ Account Extension	69
2.16.3.1 Properties.....	69
2.17 Windows™ Registry Key Object.....	70
2.17.1 Properties	70
2.17.2 Windows™ Registry Value Type.....	71
2.17.2.1 Properties.....	71
2.17.3 Windows™ Registry Datatype Enumeration	71

2.18 X.509 Certificate Object.....	73
2.18.1 Properties	73
2.18.2 X.509 v3 Extensions Type.....	74
2.18.2.1 Properties.....	75
3 Conformance	78
3.1 Defined Object Producers.....	78
3.2 Defined Object Consumers.....	78
Appendix A. Glossary.....	79
Appendix B. Acknowledgments	80
Appendix C. Revision History.....	81

1 Introduction

The STIX 2.0 specification defines structured representations for observable objects and their properties in the cyber domain. These can be used to describe data in many different functional domains, including but not limited to:

- Malware characterization
- Intrusion detection
- Incident response & management
- Digital forensics

STIX Cyber Observables document the facts concerning **what** happened on a network or host, but not necessarily the who or when, and never the why. For example, information about a file that existed, a process that was observed running, or that network traffic occurred between two IPs can all be captured as Cyber Observable data.

STIX Cyber Observables are used by various STIX Domain Objects (SDOs) to provide additional context to the data that they characterize. The Observed Data SDO, for example, indicates that the raw data was observed at a particular time and by a particular entity.

The Cyber Observable Objects chosen for inclusion in STIX 2.0 represent a minimally viable product (MVP) that fulfills basic consumer and producer requirements. Objects and properties not included in STIX 2.0, but deemed necessary by the community, will be included in future releases.

This document (*STIX™ Version 2.0. Part 4: Cyber Observable Objects*) contains the definitions for the various Cyber Observable Objects.

1.0.1 IPR Policy

This Committee Specification Public Review Draft is provided under the [Non-Assertion Mode of the OASIS IPR Policy](#), the mode chosen when the Technical Committee was established.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (<https://www.oasis-open.org/committees/cti/ipr.php>).

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 [\[RFC2119\]](#).

All text is normative except for examples and any text marked non-normative.

~~CAPEC – Common Attack Pattern Enumeration and Classification~~

~~Consumer – Any entity that receives STIX content.~~

~~CTI – Cyber Threat Intelligence~~

~~Entity – Anything that has a separately identifiable existence (e.g., organization, person, group, etc.).~~

~~IEP – FIRST (Forum of Incident Response and Security Teams) Information Exchange Policy~~

~~**Instance** – A single occurrence of a STIX object version.~~

~~**MTI** – Mandatory To Implement~~

~~**MVP** – Minimally Viable Product~~

~~**Object Creator** – The entity that created or updated a STIX object (see section 3.3 of).~~

~~**Object Representation** – An instance of an object version that is serialized as STIX.~~

~~**Producer** – Any entity that distributes STIX content, including object creators as well as those passing along existing content.~~

~~**SDO** – STIX Domain Object~~

~~**SRO** – STIX Relationship Object~~

~~**STIX** – Structured Threat Information Expression~~

~~**STIX Content** – STIX documents, including STIX Objects, STIX Objects grouped as bundles, etc.~~

~~**STIX Object** – A STIX Domain Object (SDO) or STIX Relationship Object (SRO)~~

~~**TAXII** – An application layer protocol for the communication of cyber threat information.~~

~~**TLP** – Traffic Light Protocol~~

~~**TTP** – Tactic, technique, or procedure; behaviors and resources that attackers use to carry out their attacks~~

1.2 Normative References

[Character Sets] N. Freed and M. Dürst, “Character Sets”, IANA, December 2013, [Online]. Available:-: <http://www.iana.org/assignments/character-sets/character-sets.xhtml>

[IPFIX] IANA, “IP Flow Information Export (IPFIX) Entities”, December 2016, [Online]. Available:-: <http://www.iana.org/assignments/ipfix/ipfix.xhtml>

[ISO639-2] “ISO 639-2:1998 Codes for the representation of names of languages -- Part 2: Alpha-3 code”, 1998. [Online]. Available:-: http://www.iso.org/iso/catalogue_detail?csnumber=4767

[Media Types] N. Freed, M. Kucherawy, M. Baker and B. Hoehrmann, “Media Types”, IANA, December 2016. [Online]. Available: <http://www.iana.org/assignments/media-types/media-types.xhtml>

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <http://www.rfc-editor.org/info/rfc1034>:-.

[RFC2047] Moore, K., "MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text", RFC 2047, DOI 10.17487/RFC2047, November 1996, <http://www.rfc-editor.org/info/rfc2047>:-.

[RFC2119] Bradner, S., ““Key words for use in RFCs to Indicate Requirement Levels””, BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997:-, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <http://www.rfc-editor.org/info/rfc3986>:-.

- [RFC5322]** Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <http://www.rfc-editor.org/info/rfc5322>.
- [RFC5890]** Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <http://www.rfc-editor.org/info/rfc5890>.
- [Port Numbers]** J. Touch, A. Mankin, E. Kohler, et. al., "Service Name and Transport Protocol Port Number Registry", IANA, January 2017. [Online]. Available: <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>
- [NVD]** Official Common Platform Enumeration (CPE) Dictionary, National Vulnerability Database [Online]. Available: <https://nvd.nist.gov/cpe.cfm>
- [X.509]** X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, ITU, October 2016. [Online]. Available: <https://www.itu.int/rec/T-REC-X.509/>

1.3 Naming Requirements

1.3.1 Property Names and String Literals

In the JSON serialization all property names and string literals **MUST** be exactly the same, including case, as the names listed in the property tables in this specification. For example, the SDO common property created by ref must result in the JSON key name "created by ref". Properties marked required in the property tables **MUST** be present in the JSON serialization.

1.3.2 Reserved Names

Reserved property names are marked with a type called RESERVED and a description text of "RESERVED FOR FUTURE USE". Any property name that is marked as RESERVED **MUST NOT** be present in STIX content conforming to this version of the specification.

1.3.1.4 Document Conventions

1.3.1.1.4.1 Naming Conventions

All type names, property names, and literals are in lowercase, except when referencing canonical names defined in another standard (e.g., literal values from an IANA registry). Words in property names are separated with an underscore(_), while words in type names and string enumerations are separated with a dash (-). All type names, property names, object names, and vocabulary terms are between three and 250 characters long.

~~In the JSON serialization all property names and string literals **MUST** be exactly the same, including case, as the names listed in the property tables in this specification. For example, the Cyber Observable Object property extensions must result in the JSON key name "extensions". Properties marked required in the property tables **MUST** be present in the JSON serialization.~~

1.3.2.1.4.2 Font Colors and Style

The following color, font and font style conventions are used in this document:

- The Consolas font is used for all type names, property names and literals.
 - type names are in red with a light red background - `hashes-type`
 - property names are in bold style - `protocols`
 - literals (values) are in `greenblue` with a `greenblue` background - `SHA-256`
- In an object's property table, if a common property is being redefined in some way, then the background is dark gray.
- All examples in this document are expressed in JSON. They are in Consolas 9-point font, with straight quotes, black text and a light `bluegrey` background, and 2-space indentation.
- Parts of the example may be omitted for conciseness and clarity. These omitted parts are denoted with the ellipses (...).

2 Defined Object Data Models

2.1 Artifact Object

Type Name: `artifact`

The Artifact Object permits capturing an array of bytes (8-bits), as a base64-encoded string, or linking to a file-like payload. The size of the base64-encoded data captured in the `payload_bin` property **MUST** be less than or equal to 10MB.

One of `payload_bin` or `url` **MUST** be provided. It is incumbent on object creators to ensure that the URL is accessible for downstream consumers. If a URL is provided, then the `hashes` property **MUST** contain the hash of the URL contents.

2.1.1 Properties

Common Properties		
<code>type</code> , <code>description</code> , <code>extensions</code>		
Artifact Object Specific Properties		
<code>mime_type</code> , <code>payload_bin</code> , <code>url</code> , <code>hashes</code>		
Property Name	Type	Description
<code>type</code> (required)	<code>string</code>	The value of this property MUST be <code>artifact</code> .
<code>mime_type</code> (optional)	<code>string</code>	The value of this property MUST be a valid MIME type as specified in the IANA Media Types registry [Media Types].
<code>payload_bin</code> (optional)	<code>binary</code>	Specifies the binary data contained in the artifact as a base64-encoded string. This property MUST NOT be present if <code>url</code> is provided.
<code>url</code> (optional)	<code>string</code>	The value of this property MUST be a valid URL that resolves to the unencoded content. This property MUST NOT be present if <code>payload_bin</code> is provided.
<code>hashes</code> (optional)	<code>hashes-type</code>	Specifies a dictionary of hashes for the contents of the <code>url</code> or the <code>payload_bin</code> . This MUST be provided when the <code>url</code> property is present.

Examples

Basic Image Artifact

```
{
  "0": {
    "type": "artifact",
    "mime_type": "image/jpeg",
    "payload_bin": "VBORw0KGgoAAAANSUhEUgAAADI== ..."
  }
}
```

2.2 AS Object

Type Name: `autonomous-system`

The AS object represents the properties of an Autonomous System (AS).

2.2.1 Properties

Common Properties		
type, description , extensions		
AS Object Specific Properties		
number, name, rir		
Property Name	Type	Description
type (required)	string	The value of this property MUST be <code>autonomous-system</code> .
number (required)	integer	Specifies the number assigned to the AS. Such assignments are typically performed by a Regional Internet Registry (RIR).
name (optional)	string	Specifies the name of the AS.
rir (optional)	string	Specifies the name of the Regional Internet Registry (RIR) that assigned the number to the AS.

Examples

Basic AS Object

```
{
  "0": {
    "type": "autonomous-system",
    "number": 15139,
    "name": "Slime Industries",
    "rir": "ARIN"
  }
}
```

}

2.3 Directory Object

Type Name: `directory`

The Directory Object represents the properties common to a file system directory.

2.3.1 Properties

Common Properties		
type, description , extensions		
File Object Specific Properties		
path, path_enc, created, modified, accessed, contains_refs		
Property Name	Type	Description
type (required)	string	The value of this property MUST be <code>directory</code> .
path (required)	string	Specifies the path, as originally observed, to the directory on the file system.
path_enc (optional)	string	Specifies the observed encoding for the path. The value MUST be specified if the path is stored in a non-Unicode encoding. This value MUST be specified using the corresponding name from the 2013-12-20 revision of the IANA character set registry [Character Sets] . If the preferred MIME name for a character set is defined, this value MUST be used; if it is not defined, then the Name value from the registry MUST be used instead.
created (optional)	timestamp	Specifies the date/time the directory was created.
modified (optional)	timestamp	Specifies the date/time the directory was last written to/modified.
accessed (optional)	timestamp	Specifies the date/time the directory was last accessed.
contains_refs (optional)	list of type object-ref	<p>Specifies a list of references to other File and/or Directory Objects contained within the directory.</p> <p>The objects referenced in this list MUST be of type <code>file</code> or <code>directory</code>.</p>

Examples

Basic directory

```
{
  "0": {
    "type": "directory",
    "path": "C:\\Windows\\System32"
  }
}
```

2.4 Domain Name Object

Type Name: `domain-name`

The Domain Name represents the properties of a network domain name.

2.4.1 Properties

Common Properties		
type, description , extensions		
Domain Name Object Specific Properties		
value, resolves_to_refs		
Property Name	Type	Description
type (required)	string	The value of this property MUST be <code>domain-name</code> .
value (required)	string	Specifies the value of the domain name. <u>The value of this property MUST conform to [RFC1034], and each domain and sub-domain contained within the domain name MUST conform to [RFC5890].</u>
resolves_to_refs (optional)	list of type <code>object-ref</code>	<p>Specifies a list of references to one or more IP addresses or domain names that the domain name resolves to.</p> <p>The objects referenced in this list MUST be of type <code>ipv4-addr</code> or <code>ipv6-addr</code> or <code>domain-name</code> (for cases such as CNAME records).</p>

Examples

Basic FQDN

```
{
  "0": {
    "type": "domain-name",

```

```

    "value": "example.com",
    "resolves_to_refs": [
      "1"
    ]
  },
  "1": {
    "type": "ipv4-addr",
    "value": "198.51.100.2"
  }
}

```

2.5 Email Address Object

Type Name: `email-addr`

The Email Address Object represents a single email address.

2.5.1 Properties

Common Properties		
type, description , extensions		
Email Address Object Specific Properties		
value, display_name, belongs_to_ref		
Property Name	Type	Description
type (required)	string	The value of this property MUST be <code>email-addr</code> .
value (required)	string	<p>Specifies a single email address. This MUST NOT include the display name.</p> <p>This property corresponds to the <i>addr-spec</i> construction in section 3.4 of [RFC5322], for example, <code>jane.smith@example.com</code>.</p>
display_name (optional)	string	<p>Specifies a single email display name, i.e., the name that is displayed to the human user of a mail application.</p> <p>This property corresponds to the <i>display-name</i> construction in section 3.4 of [RFC5322], for example, <code>Jane Smith</code>.</p>
belongs_to_ref (optional)	object-ref	Specifies the user account that the email address belongs to, as a reference to a User Account Object.

		The object referenced in this property MUST be of type user-account .
--	--	---

Examples

Basic Email Address

```
{
  "0": {
    "type": "email-addr",
    "value": "john@example.com",
    "display_name": "John Doe"
  }
}
```

2.6 Email Message Object

Type Name: **email-message**

The Email Message Object represents an instance of an email message, corresponding to the internet message format described in [RFC5322](#) and related RFCs.

Header field values that have been encoded as described in section 2 of [RFC2047](#) **MUST** be decoded before inclusion in Email Message Object properties. For example, this is some text **MUST** be used instead of `=?iso-8859-1?q?this=20is=20some=20text?=. Any characters in the encoded value which cannot be decoded into Unicode SHOULD be replaced with the 'REPLACEMENT CHARACTER' (U+FFFD). If it is necessary to capture the header value as observed, this can be achieved by referencing an Artifact Object through the raw_email_ref property.`

2.6.1 Properties

Common Properties		
type, description , extensions		
Email Message Object Specific Properties		
is_multipart, date, content_type, from_ref, sender_ref, to_refs, cc_refs, bcc_refs, subject, received_lines, additional_header_fields, body, body_multipart, raw_email_ref		
Property Name	Type	Description
type (required)	string	The value of this property MUST be email-message .

is_multipart (required)	boolean	Indicates whether the email body contains multiple MIME parts.
date (optional)	timestamp	Specifies the date/time that the email message was sent.
content_type (optional)	string	Specifies the value of the "Content-Type" header of the email message.
from_ref (optional)	object-ref	<p>Specifies the value of the "From:" header of the email message. The "From:" field specifies the author(s) of the message, that is, the mailbox(es) of the person(s) or system(s) responsible for the writing of the message.</p> <p>The object referenced in this property MUST be of type email-address.</p>
sender_ref (optional)	object-ref	<p>Specifies the value of the "Sender" field of the email message. The "Sender:" field specifies the mailbox of the agent responsible for the actual transmission of the message.</p> <p>The object referenced in this property MUST be of type email-address.</p>
to_refs (optional)	list of type object-ref	<p>Specifies the mailboxes that are "To:" recipients of the email message.</p> <p>The objects referenced in this list MUST be of type email-address.</p>
cc_refs (optional)	list of type object-ref	<p>Specifies the mailboxes that are "CC:" recipients of the email message.</p> <p>The objects referenced in this list MUST be of type email-address.</p>
bcc_refs (optional)	list of type object-ref	<p>Specifies the mailboxes that are "BCC:" recipients of the email message.</p> <p>As per RFC5322, this list may be empty, which should not be treated the same as the key being absent.</p> <p>The objects referenced in this list MUST be of type email-address.</p>

subject (optional)	string	Specifies the subject of the email message.
received_lines (optional)	list of type string	<p>Specifies one or more "Received" header fields that may be included in the email headers.</p> <p>List values MUST appear in the same order as present in the email message.</p>
additional_header_fields (optional)	dictionary	<p>Specifies any other header fields (except for date, received_lines, content_type, from_ref, sender_ref, to_refs, cc_refs, bcc_refs, and subject) found in the email message, as a dictionary.</p> <p>Each key/value pair in the dictionary represents the name/value of a single header field or names/values of a header field that occurs more than once. Each dictionary key SHOULD be a case-preserved version of the header field name. For cases where a header field occurs exactly once, the corresponding value for the dictionary key MUST be a string. For cases where a header field occurs more than once, the corresponding value for the dictionary key MUST be a list of type string, where each string in the list represents a single value of the header field.</p>
body (optional)	string	Specifies a string containing the email body. This property MAY only be used if is_multipart is false.
body_multipart (optional)	list of type mime-part-type	Specifies a list of the MIME parts that make up the email body. This property MAY only be used if is_multipart is true.
raw_email_ref (optional)	object-ref	<p>Specifies the raw binary contents of the email message, including both the headers and body, as a reference to an Artifact Object.</p> <p>The object referenced in this property MUST be of type artifact.</p>

2.6.2 Email MIME Component Type

Type Name: **mime-part-type**

Specifies one component of a multi-part email body.

There is no property to capture the value of the “Content-Transfer-Encoding” header field, since the body **MUST** be decoded before being represented in the **body** property.

One of **body** OR **body_raw_ref** **MUST** be included.

2.6.2.1 2.6.2.1 Properties

Property Name	Type	Description
body (optional)	string	<p>Specifies the contents of the MIME part if the content_type is not provided or starts with <code>text/</code> (e.g., in the case of plain text or HTML email).</p> <p>For inclusion in this property, the contents MUST be decoded to Unicode. Note that the charset provided in content_type is for informational usage and not for decoding of this property.</p>
body_raw_ref (optional)	object-ref	<p>Specifies the contents of non-textual MIME parts, that is those whose content_type does not start with <code>text/</code>, as a reference to an Artifact Object or File Object.</p> <p>The object referenced in this property MUST be of type <code>artifact</code> or <code>file</code>. For use cases where conveying the actual data contained in the MIME part is of primary importance, <code>artifact</code> SHOULD be used. Otherwise, for use cases where conveying metadata about the file-like properties of the MIME part is of primary importance, <code>file</code> SHOULD be used.</p>
content_type (optional)	string	<p>Specifies the value of the “Content-Type” header field of the MIME part.</p> <p>Any additional “Content-Type” header field parameters such as <code>charset</code> SHOULD be included in this property.</p> <p>Example: <code>text/html; charset=UTF-8</code></p>
content_disposition (optional)	string	<p>Specifies the value of the “Content-Disposition” header field of the MIME part.</p>

Examples

Simple Email Message

```
{  
  "0": {  
    "type": "email-addr",
```

```

    "value": "jdoe@example.com",
    "display_name": "John Doe"
  },
  "1": {
    "type": "email-addr",
    "value": "mary@example.com",
    "display_name": "Mary Smith"
  },
  "2": {
    "type": "email-message",
    "from_ref": "0",
    "to_refs": ["1"],
    "is_multipart": false,
    "date": "1997-11-21T15:55:06.000Z",
    "subject": "Saying Hello"
  }
}

```

Simple Email Message with Additional Header Properties

```

{
  "0": {
    "type": "email-addr",
    "value": "joe@example.com",
    "display_name": "Joe Smith"
  },
  "1": {
    "type": "email-addr",
    "value": "bob@example.com",
    "display_name": "Bob Smith"
  },
  "2": {
    "type": "email-message",
    "from_ref": "0",
    "to_refs": [
      "1"
    ],
    "is_multipart": false,
    "date": "2004-04-19T12:22:23.000Z",
    "subject": "Did you see this?",
    "additional_header_fields": {
      "Reply-To": [
        "steve@example.com",
        "jane@example.com"
      ]
    }
  }
}

```

```
}  
}
```

Complex MIME Email Message

```
{  
  "0": {  
    "type": "email-message",  
    "is_multipart": true,  
    "received_lines": [  
      "from mail.example.com ([198.51.100.3]) by smtp.gmail.com with ESMTPSA id  
q23sm23309939wme.17.2016.07.19.07.20.32 (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256  
bits=128/128); Tue, 19 Jul 2016 07:20:40 -0700 (PDT)"  
    ],  
    "content_type": "multipart/mixed",  
    "date": "2016-06-19T14:20:40.000Z",  
    "from_ref": "1",  
    "to_refs": [  
      "2"  
    ],  
    "cc_refs": [  
      "3"  
    ],  
    "subject": "Check out this picture of a cat!",  
    "additional_header_fields": {  
      "Content-Disposition": "inline",  
      "X-Mailer": "Mutt/1.5.23",  
      "X-Originating-IP": "198.51.100.3"  
    },  
    "body_multipart": [  
      {  
        "content_type": "text/plain; charset=utf-8",  
        "content_disposition": "inline",  
        "body": "Cats are funny!"  
      },  
      {  
        "content_type": "image/png",  
        "content_disposition": "attachment; filename=\"tabby.png\"",  
        "body_raw_ref": "4"  
      },  
      {  
        "content_type": "application/zip",  
        "content_disposition": "attachment; filename=\"tabby_pics.zip\"",  
        "body_raw_ref": "5"  
      }  
    ]  
  },  
}
```

```

"1": {
  "type": "email-addr",
  "value": "jdoe@example.com",
  "display_name": "John Doe"
},
"2": {
  "type": "email-addr",
  "value": "bob@example.com",
  "display_name": "Bob Smith"
},
"3": {
  "type": "email-addr",
  "value": "mary@example.com",
  "display_name": "Mary Jones"
},
"4": {
  "type": "artifact",
  "mime_type": "image/jpeg",
  "payload_bin": "VBORw0KGgoAAAANSUgAAADI== ...",
  "hashes": {
    "MD5": "69D0D97D02A03C43782DD571394E6869"
    "SHA-256": "effb46bba03f6c8aea5c653f9cf984f170dcdd3bbbe2ff6843c3e5da0e698766"
  }
},
"5": {
  "type": "file",
  "name": "tabby_pics.zip",
  "magic_number_hex": "504B0304",
  "hashes": {
    "MD5": "22A0FB8F3879FB569F8A3FF65850A82E"
    "SHA-256": "fe90a7e910cb3a4739bed9180e807e93fa70c90f25a8915476f5e4bfbac681db"
  }
}
}

```

2.7 File Object

Type Name: `file`

The File Object represents the properties of a file. A File Object **MUST** contain at least one of `hashes` or `name`.

2.7.1 Properties

Common Properties

type, description , extensions		
File Object Specific Properties		
hashes, size, name, name_enc, magic_number_hex, mime_type, created, modified, accessed, parent_directory_ref, is_encrypted, encryption_algorithm, decryption_key, contains_refs, content_ref		
Property Name	Type	Description
type (required)	string	The value of this property MUST be file.
extensions (optional)	dictionary	<p>The File Object defines the following extensions. In addition to these, producers MAY create their own.</p> <p>ntfs-ext, raster-image-ext, pdf-ext, archive-ext, windows-pebinary-ext</p> <p>Dictionary keys MUST identify the extension type by name.</p> <p>The corresponding dictionary values MUST contain the contents of the extension instance.</p>
hashes (optional)	hashes-type	Specifies a dictionary of hashes for the file.
size (optional)	integer	Specifies the size of the file, in bytes. The value of this property MUST NOT be negative.
name (optional)	string	Specifies the name of the file.
name_enc (optional)	string	<p>Specifies the observed encoding for the name of the file. This value MUST be specified using the corresponding name from the 2013-12-20 revision of the IANA character set registry [Character Sets]. If the value from the Preferred MIME Name column for a character set is defined, this value MUST be used; if it is not defined, then the value from the Name column in the registry MUST be used instead.</p> <p>This property allows for the capture of the original text encoding for the file name, which may be forensically relevant; for example, a file on an NTFS volume whose name was created using the windows-1251 encoding, commonly used for languages based on Cyrillic script.</p>

magic_number_hex (optional)	hex	Specifies the hexadecimal constant ("magic number") associated with a specific file format that corresponds to the file, if applicable.
mime_type (optional)	string	<p>Specifies the MIME type name specified for the file, e.g., application/msword.</p> <p>Whenever feasible, this value SHOULD be one of the values defined in the Template column in the IANA media type registry [Media Types].</p> <p>Maintaining a comprehensive universal catalog of all extant file types is obviously not possible. When specifying a MIME type not included in the IANA registry, implementers should use their best judgement so as to facilitate interoperability.</p>
created (optional)	timestamp	Specifies the date/time the file was created.
modified (optional)	timestamp	Specifies the date/time the file was last written to/modified.
accessed (optional)	timestamp	Specifies the date/time the file was last accessed.
parent_directory_ref (optional)	object-ref	<p>Specifies the parent directory of the file, as a reference to a Directory Object.</p> <p>The object referenced in this property MUST be of type directory.</p>
is_encrypted (optional)	boolean	Specifies whether the file is encrypted.
encryption_algorithm (optional)	open-vocab	<p>Specifies the name of the encryption algorithm used to encrypt the file. This is an open vocabulary and values SHOULD come from the encryption-algo-ov vocabulary.</p> <p>This property MUST NOT be used if is_encrypted is false or not included.</p>
decryption_key (optional)	string	<p>Specifies the decryption key used to decrypt the file.</p> <p>This property MUST NOT be used if is_encrypted is false or not included.</p>
contains_refs (optional)	list of type	Specifies a list of references to other Observable Objects contained within the file, such as another file that is

	object-ref	<p>appended to the end of the file, or an IP address that is contained somewhere in the the file.</p> <p>This is intended for use cases other than those targeted by the Archive extension.</p>
content_ref (optional)	object-ref	<p>Specifies the content of the file, represented as an Artifact Object.</p> <p>The object referenced in this property MUST be of type artifact.</p>

Examples

Basic file with file system properties without observed encoding

```
{
  "0": {
    "type": "file",
    "hashes": {
      "MD5": "4472ea40dc71e5bb701574ea215a81a1"
      "SHA-256": "fe90a7e910cb3a4739bed9180e807e93fa70c90f25a8915476f5e4bfbac681db"
    },
    "size": 25536,
    "name": "foo.dll"
  }
}
```

Basic file with file system properties with observed encoding

```
{
  "0": {
    "type": "file",
    "hashes": {
      "MD5": "66e2ea40dc71d5ba701574ea215a81f1"
      "SHA-256": "841a8921140aba50671ebb0770fecc4ee308c4952cfeff8de154ab14eeef4649"
    },
    "name": "quêry.dll",
    "name_enc": "windows-1252"
  }
}
```

In this example, the file name would have originally appeared using the bytes 71 75 **ea** 72 79 2e 64 6c 6c. Representing it in UTF-8, as required for JSON, would use the bytes 71 75 **c3 aa** 72 79 2e 64 6c 6c.

Basic file with parent directory

```
{
```

```

"0": {
  "type": "directory",
  "path": "C:\\Windows\\System32"
},
"1": {
  "type": "file",
  "hashes": {
    "MD5": "A2FD2B3F4D5A1BD5E7D283299E01DCE9"
    "SHA-256": "ceafbfd424be2ca4a5f0402cae090dda2fb0526cf521b60b60077c0f622b285a"
  },
  "parent_directory_ref": "0",
  "name": "qwerty.dll"
}
}

```

2.7.2 Archive File Extension

Type Name: `archive-ext`

The Archive File extension specifies a default extension for capturing properties specific to archive files. The key for this extension when used in the **extensions** dictionary **MUST** be `archive-ext`.

2.7.2.1 Properties

Property Name	Type	Description
contains_refs (required)	<code>list</code> of type <code>object-ref</code>	Specifies the files contained in the archive, as a reference to one or more other File Objects. The objects referenced in this list MUST be of type <code>file</code> .
version (optional)	<code>string</code>	Specifies the version of the archive type used in the archive file.
comment (optional)	<code>string</code>	Specifies a comment included as part of the archive file.

Examples

Basic unencrypted ZIP Archive

```

{
  "0": {
    "type": "file",
    "hashes": {
      "MD5": "66e2ea40dc71d5ba701574ea215a81f1"
      "SHA-256": "ceafbfd424be2ca4a5f0402cae090dda2fb0526cf521b60b60077c0f622b285a"
    }
  },
}

```

```

    "1": {
      "type": "file",
      "hashes": {
        "MD5": "22A0FB8F3879FB569F8A3FF65850A82E"
        "SHA-256": "19c549ec2628b989382f6b280cbd7bb836a0b461332c0fe53511ce7d584b89d3"
      }
    },
    "2": {
      "type": "file",
      "hashes": {
        "MD5": "8D98A25E9D0662B1F4CA3BF22D6F53E9"
        "SHA-256": "0969de02ecf8a5f003e3f6d063d848c8a193aada092623f8ce408c15bcb5f038"
      }
    },
    "3": {
      "type": "file",
      "name": "foo.zip",
      "hashes": {
        "MD5": "B365B9A80A06906FC9B400C06C33FF43"
        "SHA-256": "35a01331e9ad96f751278b891b6ea09699806faedfa237d40513d92ad1b7100f"
      },
      "mime_type": "application/zip",
      "extensions": {
        "archive-ext": {
          "contains_refs": [
            "0",
            "1",
            "2"
          ],
          "version": "5.0"
        }
      }
    }
  }
}

```

2.7.3 NTFS File Extension

Type Name: `ntfs-ext`

The NTFS file extension specifies a default extension for capturing properties specific to the storage of the file on the NTFS file system. The key for this extension when used in the **extensions** dictionary **MUST** be `ntfs-ext`. An object using the NTFS File Extension **MUST** contain at least one property from this extension.

2.7.3.1 Properties

Property Name	Type	Description
sid (optional)	string	Specifies the security ID (SID) value assigned to the file.
alternate_data_streams (optional)	list of type alternate-data-stream	Specifies a list of NTFS alternate data streams that exist for the file.

2.7.3.2 Alternate Data Stream Type

Type Name: alternate-data-stream

The Alternate Data Stream type represents an NTFS alternate data stream.

2.7.3.2.1 Properties

Property Name	Type	Description
name (required)	string	Specifies the name of the alternate data stream.
hashes (optional)	hashes-type	Specifies a dictionary of hashes for the data contained in the alternate data stream.
size (optional)	integer	Specifies the size of the alternate data stream, in bytes. The value of this property MUST NOT be negative.

Examples

NTFS File with a single alternate data stream

```
{
  "0": {
    "type": "file",
    "hashes": {
      "MD5": "B4D33B0C7306351B9ED96578465C5579"
      "SHA-256": "35a01331e9ad96f751278b891b6ea09699806faedfa237d40513d92ad1b7100f"
    },
    "extensions": {
      "ntfs-ext": {
        "alternate_data_streams": [
          {
            "name": "second.stream",
            "size": 25536
          }
        ]
      }
    }
  }
}
```

```

    ]
  }
}
}
}
}

```

2.7.4 PDF File Extension

Type Name: pdf-ext

The PDF file extension specifies a default extension for capturing properties specific to PDF files. The key for this extension when used in the **extensions** dictionary **MUST** be pdf-ext. An object using the PDF File Extension **MUST** contain at least one property from this extension.

2.7.4.1 Properties

Property Name	Type	Description
version (optional)	string	Specifies the decimal version number of the string from the PDF header that specifies the version of the PDF specification to which the PDF file conforms. E.g., 1.4.
is_optimized (optional)	boolean	Specifies whether the PDF file has been optimized.
document_info_dict (optional)	dictionary	Specifies details of the PDF document information dictionary (DID), which includes properties like the document creation data and producer, as a dictionary. Each key in the dictionary SHOULD be a case-preserved version of the corresponding entry in the document information dictionary without the prepended forward slash, e.g., Title. The corresponding value for the key MUST be the value specified for the document information dictionary entry, as a string.
pdfid0 (optional)	string	Specifies the first file identifier found for the PDF file.
pdfid1 (optional)	string	Specifies the second file identifier found for the PDF file.

Examples

Basic PDF file

```

{
  "0": {
    "type": "file",
    "hashes": {
      "MD5": "66e2ea40dc71d5ba701574ea215a81f1"
      "SHA-256": "35a01331e9ad96f751278b891b6ea09699806faedfa237d40513d92ad1b7100f"
    },
  },
}

```

```

    "extensions": {
      "pdf-ext": {
        "version": "1.7",
        "document_info_dict": {
          "Title": "Sample document",
          "Author": "Adobe Systems Incorporated",
          "Creator": "Adobe FrameMaker 5.5.3 for Power Macintosh",
          "Producer": "Acrobat Distiller 3.01 for Power Macintosh",
          "CreationDate": "20070412090123-02"
        },
        "pdfid0": "DFCE52BD827ECF765649852119D",
        "pdfid1": "57A1E0F9ED2AE523E313C"
      }
    }
  }
}

```

2.7.5 Raster Image File Extension

Type Name: `raster-image-ext`

The Raster Image file extension specifies a default extension for capturing properties specific to raster image files. The key for this extension when used in the **extensions** dictionary **MUST** be `raster-image-ext`. An object using the Raster Image File Extension **MUST** contain at least one property from this extension.

2.7.5.1 Properties

Property Name	Type	Description
image_height (optional)	<code>integer</code>	Specifies the height of the image in the image file, in pixels.
image_width (optional)	<code>integer</code>	Specifies the width of the image in the image file, in pixels.
bits_per_pixel (optional)	<code>integer</code>	Specifies the sum of bits used for each color channel in the image file, and thus the total number of pixels used for expressing the color depth of the image.
image_compression_algorithm (optional)	<code>string</code>	Specifies the name of the compression algorithm used to compress the image in the image file, if applicable.
exif_tags (optional)	<code>dictionary</code>	Specifies the set of EXIF tags found in the image file, as a dictionary. Each key/value pair in the dictionary represents the name/value of a single

		EXIF tag. Accordingly, each dictionary key MUST be a case-preserved version of the EXIF tag name, e.g., <code>XResolution</code> . Each dictionary value MUST be either an <code>integer</code> (for int* EXIF datatypes) or a <code>string</code> (for all other EXIF datatypes).
--	--	--

Examples

Simple Image File with EXIF Data

```
{
  "0": {
    "type": "file",
    "name": "picture.jpg",
    "hashes": {
      "MD5": "B4D33B0C7306351B9ED96578465C5579"
      "SHA-256": "35a01331e9ad96f751278b891b6ea09699806faedfa237d40513d92ad1b7100f"
    },
    "extensions": {
      "raster-image-ext": {
        "exif_tags": {
          "Make": "Nikon",
          "Model": "D7000",
          "XResolution": 4928,
          "YResolution": 3264
        }
      }
    }
  }
}
```

2.7.6 Windows™ PE Binary File Extension

Type Name: `windows-pebinary-ext`

The Windows™ PE Binary File extension specifies a default extension for capturing properties specific to Windows portable executable (PE) files. The key for this extension when used in the **extensions** dictionary **MUST** be `windows-pebinary-ext`.

2.7.6.1 Properties

Property Name	Type	Description
<code>pe_type</code> (required)	<code>open-vocab</code>	Specifies the type of the PE binary. This is an open vocabulary and values SHOULD come from the <code>windows-pebinary-type-ov</code> vocabulary.

<code>imphash</code> (optional)	<code>string</code>	Specifies the special import hash, or 'imphash', calculated for the PE Binary based on its imported libraries and functions. For more information on the imphash algorithm, see the original article by Mandiant/FireEye: https://www.fireeye.com/blog/threat-research/2014/01/tracking-malware-import-hashing.html .
<code>machine_hex</code> (optional)	<code>hex</code>	Specifies the type of target machine.
<code>number_of_sections</code> (optional)	<code>integer</code>	Specifies the number of sections in the PE binary, as a non-negative integer.
<code>time_date_stamp</code> (optional)	<code>timestamp</code>	Specifies the time when the PE binary was created. The timestamp value MUST be precise to the second.
<code>pointer_to_symbol_table_hex</code> (optional)	<code>hex</code>	Specifies the file offset of the COFF symbol table.
<code>number_of_symbols</code> (optional)	<code>integer</code>	Specifies the number of entries in the symbol table of the PE binary, as a non-negative integer.
<code>size_of_optional_header</code> (optional)	<code>integer</code>	Specifies the size of the optional header of the PE binary. The value of this property MUST NOT be negative.
<code>characteristics_hex</code> (optional)	<code>hex</code>	Specifies the flags that indicate the file's characteristics.
<code>file_header_hashes</code> (optional)	<code>hashes-type</code>	Specifies any hashes that were computed for the file header.
<code>optional_header</code> (optional)	<code>windows-pe-optional-header-type</code>	Specifies the PE optional header of the PE binary.
<code>sections</code> (optional)	<code>list of type windows-pe-section</code>	Specifies metadata about the sections in the PE file.

2.7.6.2 Windows™ PE Binary Vocabulary

Vocabulary Name: `windows-pebinary-type-ov`

An open vocabulary of Windows PE binary types.

Value	Description
exe	Specifies that the PE binary is an executable image (i.e., not an OBJ or DLL).
dll	Specifies that the PE binary is a dynamically linked library (DLL).
sys	Specifies that the PE binary is a device driver (SYS).

2.7.6.3 PE Optional Header Type

Type Name: windows-pe-optional-header-type

The Windows PE Optional Header type represents the properties of the PE optional header.

2.7.6.3.1 Properties

Property Name	Type	Description
magic_hex (optional)	hex	Specifies the hex value that indicates the type of the PE binary.
major_linker_version (optional)	integer	Specifies the linker major version number.
minor_linker_version (optional)	integer	Specifies the linker minor version number.
size_of_code (optional)	integer	Specifies the size of the code (text) section. If there are multiple such sections, this refers to the sum of the sizes of each section. The value of this property MUST NOT be negative.
size_of_initialized_data (optional)	integer	Specifies the size of the initialized data section. If there are multiple such sections, this refers to the sum of the sizes of each section. The value of this property MUST NOT be negative.
size_of_uninitialized_data (optional)	integer	Specifies the size of the uninitialized data section. If there are multiple such sections, this refers to the sum of the sizes of each section. The value of this property MUST NOT be negative.
address_of_entry_point (optional)	integer	Specifies the address of the entry point relative to the image base when the executable is loaded into

		memory.
base_of_code (optional)	integer	Specifies the address that is relative to the image base of the beginning-of-code section when it is loaded into memory.
base_of_data (optional)	integer	Specifies the address that is relative to the image base of the beginning-of-data section when it is loaded into memory.
image_base (optional)	integer	Specifies the preferred address of the first byte of the image when loaded into memory.
section_alignment (optional)	integer	Specifies the alignment (in bytes) of PE sections when they are loaded into memory.
file_alignment (optional)	integer	Specifies the factor (in bytes) that is used to align the raw data of sections in the image file.
major_os_version (optional)	integer	Specifies the major version number of the required operating system.
minor_os_version (optional)	integer	Specifies the minor version number of the required operating system.
major_image_version (optional)	integer	Specifies the major version number of the image.
minor_image_version (optional)	integer	Specifies the minor version number of the image.
major_subsystem_version (optional)	integer	Specifies the major version number of the subsystem.
minor_subsystem_version (optional)	integer	Specifies the minor version number of the subsystem.
win32_version_value_hex (optional)	hex	Specifies the reserved win32 version value.
size_of_image (optional)	integer	Specifies the size of the image in bytes, including all headers, as the image is loaded in memory. The value of this property MUST NOT be negative.
size_of_headers (optional)	integer	Specifies the combined size of the MS-DOS, PE header, and section headers, rounded up to a multiple of the value specified in the file_alignment

		header. The value of this property MUST NOT be negative.
checksum_hex (optional)	hex	Specifies the checksum of the PE binary.
subsystem_hex (optional)	hex	Specifies the subsystem (e.g., GUI, device driver, etc.) that is required to run this image.
dll_characteristics_hex (optional)	hex	Specifies the flags that characterize the PE binary.
size_of_stack_reserve (optional)	integer	Specifies the size of the stack to reserve, in bytes. The value of this property MUST NOT be negative.
size_of_stack_commit (optional)	integer	Specifies the size of the stack to commit, in bytes. The value of this property MUST NOT be negative.
size_of_heap_reserve (optional)	integer	Specifies the size of the local heap space to reserve, in bytes. The value of this property MUST NOT be negative.
size_of_heap_commit (optional)	integer	Specifies the size of the local heap space to commit, in bytes. The value of this property MUST NOT be negative.
loader_flags_hex (optional)	hex	Specifies the reserved loader flags.
number_of_rva_and_sizes (optional)	integer	Specifies the number of data-directory entries in the remainder of the optional header.
hashes (optional)	hashes-type	Specifies any hashes that were computed for the optional header.

2.7.6.4 Windows™ PE Section Type

Type Name: windows-pe-section

The Windows PE Section type specifies metadata about a PE file section.

2.7.6.4.1 Properties

Property Name	Type	Description
name (required)	string	Specifies the name of the section.

size (optional)	integer	Specifies the size of the section, in bytes. The value of this property MUST NOT be negative.
entropy (optional)	float	Specifies the calculated entropy for the section, as calculated using the Shannon algorithm (https://en.wiktionary.org/wiki/Shannon_entropy). The size of each input character is defined as a byte, resulting in a possible range of 0 through 8.
hashes (optional)	hashes-type	Specifies any hashes computed over the section.

Examples

Typical EXE File

```
{
  "0": {
    "type": "file",
    "hashes": {
      "MD5": "1C19FC56AEF2048C1CD3A5E67B099350",
      "SHA-256": "35a01331e9ad96f751278b891b6ea09699806faedfa237d40513d92ad1b7100f"
    },
    "extensions": {
      "windows-pebinary-ext": {
        "pe_type": "exe",
        "machine_hex": "014c",
        "number_of_sections": 4,
        "time_date_stamp": "2016-01-22T12:31:12Z",
        "pointer_to_symbol_table_hex": "74726144",
        "number_of_symbols": 4542568,
        "size_of_optional_header": 224,
        "characteristics_hex": "818f",
        "optional_header": {
          "magic_hex": "010b",
          "major_linker_version": 2,
          "minor_linker_version": 25,
          "size_of_code": 512,
          "size_of_initialized_data": 283648,
          "size_of_uninitialized_data": 0,
          "address_of_entry_point": 4096,
          "base_of_code": 4096,
          "base_of_data": 8192,
          "image_base": 14548992,
          "section_alignment": 4096,
          "file_alignment": 4096,
          "major_os_system_version": 1,
```

```

        "minor_os_system_version": 0,
        "major_image_version": 0,
        "minor_image_version": 0,
        "major_subsystem_version": 4,
        "minor_subsystem_version": 0,
        "win32_version_value_hex": "00",
        "size_of_image": 299008,
        "size_of_headers": 4096,
        "checksum_hex": "00",
        "subsystem_hex": "03",
        "dll_characteristics_hex": "00",
        "size_of_stack_reserve": 100000,
        "size_of_stack_commit": 8192,
        "size_of_heap_reserve": 100000,
        "size_of_heap_commit": 4096,
        "loader_flags_hex": "abdbffde",
        "number_of_rva_and_sizes": 3758087646
    },
    "sections": [
        {
            "name": "CODE",
            "entropy": 0.061089
        },
        {
            "name": "DATA",
            "entropy": 7.980693
        },
        {
            "name": "NicolasB",
            "entropy": 0.607433
        },
        {
            "name": ".idata",
            "entropy": 0.607433
        }
    ]
}
}
}
}

```

2.8 IPv4 Address Object

Type Name: `ipv4-addr`

The IPv4 Address Object represents one or more IPv4 addresses expressed using CIDR notation.

2.8.1 Properties

Common Properties		
type, description , extensions		
IPv4 Address Object Specific Properties		
value, resolves_to_refs, belongs_to_refs		
Property Name	Type	Description
type (required)	string	The value of this property MUST be <code>ipv4-addr</code> .
value (required)	string	<p>Specifies one or more IPv4 addresses expressed using CIDR notation.</p> <p>If a given IPv4 Address Object represents a single IPv4 address, the CIDR /32 suffix MAY be omitted.</p> <p>Example: 10.2.4.5/24</p>
resolves_to_refs (optional)	list of type object-ref	<p>Specifies a list of references to one or more Layer 2 Media Access Control (MAC) addresses that the IPv4 address resolves to.</p> <p>The objects referenced in this list MUST be of type <code>mac-addr</code>.</p>
belongs_to_refs (optional)	list of type object-ref	<p>Specifies a list of references to one or more autonomous systems (AS) that the IPv4 address belongs to.</p> <p>The objects referenced in this list MUST be of type <code>autonomous-system</code>.</p>

Examples

IPv4 Single Address

```
{
  "0": {
    "type": "ipv4-addr",
    "value": "198.51.100.3"
  }
}
```

IPv4 CIDR Block

```
{
  "0": {
    "type": "ipv4-addr",
    "value": "198.51.100.0/24"
  }
}
```

2.9 IPv6 Address Object

Type Name: `ipv6-addr`

The IPv6 Address Object represents one or more IPv6 addresses expressed using CIDR notation.

2.9.1 Properties

Common Properties		
type, description , extensions		
IPv6 Address Object Specific Properties		
value, resolves_to_refs, belongs_to_refs		
Property Name	Type	Description
type (required)	string	The value of this property MUST be <code>ipv6-addr</code> .
value (required)	string	Specifies one or more IPv6 addresses expressed using CIDR notation. If a given IPv6 Address Object represents a single IPv6 address, the CIDR /128 suffix MAY be omitted.
resolves_to_refs (optional)	list of type <code>object-ref</code>	Specifies a list of references to one or more Layer 2 Media Access Control (MAC) addresses that the IPv6 address resolves to. The objects referenced in this list MUST be of type <code>mac-addr</code> .
belongs_to_refs (optional)	list of type <code>object-ref</code>	Specifies a list of references to one or more autonomous systems (AS) that the IPv6 address belongs to. The objects referenced in this list MUST be of type <code>autonomous-system</code> .

Examples

IPv6 Single Address

```
{
  "0": {
    "type": "ipv6-addr",
    "value": "2001:0db8:85a3:0000:0000:8a2e:0370:7334"
  }
}
```

IPv6 CIDR block

```
{
  "0": {
    "type": "ipv6-addr",
    "value": "2001:0db8::/96"
  }
}
```

2.10 MAC Address Object

Type Name: `mac-addr`

The MAC Address Object represents a single Media Access Control (MAC) address.

2.10.1 Properties

Common Properties		
type, description , extensions		
MAC Address Object Specific Properties		
value		
Property Name	Type	Description
type (required)	string	The value of this property MUST be <code>mac-addr</code> .
value (required)	string	Specifies a single MAC address. The MAC address value MUST be represented as a single colon-delimited, lowercase MAC-48 address, which MUST include leading zeros for each octet. Example: <code>00:00:ab:cd:ef:01</code>

Examples

Typical MAC address

```
{
  "0": {
    "type": "mac-addr",
    "value": "d2:fb:49:24:37:18"
  }
}
```

2.11 Mutex Object

Type Name: `mutex`

The Mutex Object represents the properties of a mutual exclusion (mutex) object.

2.11.1 Properties

Common Properties		
type, description , extensions		
File Object Specific Properties		
name		
Property Name	Type	Description
type (required)	<code>string</code>	The value of this property MUST be <code>mutex</code> .
name (required)	<code>string</code>	Specifies the name of the mutex object.

Examples

Malware mutex

```
{
  "0": {
    "type": "mutex",
    "name": "__CLEANSWEEP__"
  }
}
```

2.12 Network Traffic

Type Name: `network-traffic`

The Network Traffic Object represents arbitrary network traffic that originates from a source and is addressed to a destination. The network traffic **MAY** or **MAY NOT** constitute a valid unicast, multicast, or broadcast network connection. This **MAY** also include traffic that is not established, such as a SYN flood.

To allow for use cases where a source or destination address may be sensitive and not suitable for sharing, such as addresses that are internal to an organization's network, the source and destination properties (**src_ref** and **dst_ref**, respectively) are defined as optional in the properties table below. However, a Network Traffic Object **MUST** contain the **protocols** property and at least one of the **src_ref** or **dst_ref** properties and **SHOULD** contain the **src_port** and **dst_port** properties.

2.12.1 Properties

Common Properties		
type, description , extensions		
Network Traffic Specific Properties		
start, end, is_active, src_ref, dst_ref, src_port, dst_port, protocols, src_byte_count, dst_byte_count, src_packets, dst_packets, ipfix, src_payload_ref, dst_payload_ref, encapsulates_refs, encapsulated_by_ref		
Property Name	Type	Description
type (required)	string	The value of this property MUST be <code>network-traffic</code> .
extensions (optional)	dictionary	<p>The Network Traffic Object defines the following extensions. In addition to these, producers MAY create their own.</p> <p><code>http-ext</code>, <code>tcp-ext</code>, <code>icmp-ext</code>, <code>socket-ext</code></p> <p>Dictionary keys MUST identify the extension type by name.</p> <p>The corresponding dictionary values MUST contain the contents of the extension instance.</p>
start (optional)	timestamp	Specifies the date/time the network traffic was initiated, if known.
end (optional)	timestamp	<p>Specifies the date/time the network traffic ended, if known.</p> <p>If the is_active property is true, then the end property MUST NOT be included.</p>
is_active (optional)	boolean	Indicates whether the network traffic is still ongoing.

src_ref (optional)	object-ref	<p>Specifies the source of the network traffic, as a reference to one or more Observable Objects.</p> <p>The objects referenced in this list MUST be of type <code>ipv4-addr</code> or <code>ipv6-addr</code> or <code>mac-addr</code> or <code>domain-name</code> (for cases where the IP address for a domain name is unknown).</p>
dst_ref (optional)	object-ref	<p>Specifies the destination of the network traffic, as a reference to one or more Observable Objects.</p> <p>The objects referenced in this list MUST be of type <code>ipv4-addr</code> or <code>ipv6-addr</code> or <code>mac-addr</code> or <code>domain-name</code> (for cases where the IP address for a domain name is unknown).</p>
src_port (optional)	integer	<p>Specifies the source port used in the network traffic, as an integer. The port value MUST be in the range of 0 - 65535.</p>
dst_port (optional)	integer	<p>Specifies the destination port used in the network traffic, as an integer. The port value MUST be in the range of 0 - 65535.</p>
protocols (required)	list of type string	<p>Specifies the protocols observed in the network traffic, along with their corresponding state.</p> <p>Protocols MUST be listed in low to high order, from outer to inner in terms of packet encapsulation. That is, the protocols in the outer level of the packet, such as IP, MUST be listed first.</p> <p>The protocol names SHOULD come from the service names defined in the Service Name column of the IANA Service Name and Port Number Registry [Port Numbers]. In cases where there is variance in the name of a network protocol not included in the IANA Registry, content producers should exercise their best judgement, and it is recommended that lowercase names be used for consistency with the IANA registry.</p> <p>Examples:</p> <pre> ipv4, tcp, http ipv4, udp ipv6, tcp, http ipv6, tcp, ssl, https </pre>
src_byte_count (optional)	integer	<p>Specifies the number of bytes sent from the source to the destination.</p>

dst_byte_count (optional)	integer	Specifies the number of bytes sent from the destination to the source.
src_packets (optional)	integer	Specifies the number of packets sent from the source to the destination.
dst_packets (optional)	integer	Specifies the number of packets sent destination to the source.
ipfix (optional)	dictionary	Specifies any IP Flow Information Export [IPFIX] data for the traffic, as a dictionary. Each key/value pair in the dictionary represents the name/value of a single IPFIX element. Accordingly, each dictionary key SHOULD be a case-preserved version of the IPFIX element name, e.g., <code>octetDeltaCount</code> . Each dictionary value MUST be either an integer or a string, as well as a valid IPFIX property.
src_payload_ref (optional)	object-ref	Specifies the bytes sent from the source to the destination. The object referenced in this property MUST be of type artifact.
dst_payload_ref (optional)	object-ref	Specifies the bytes sent from the destination to the source. The object referenced in this property MUST be of type artifact.
encapsulates_refs (optional)	list of type object-ref	Links to other network-traffic objects encapsulated by this network-traffic object. The objects referenced in this property MUST be of type network-traffic.
encapsulated_by_ref (optional)	object-ref	Links to another network-traffic object which encapsulates this object. The object referenced in this property MUST be of type network-traffic.

Examples

Basic TCP Network Traffic

```
{
  "0": {
    "type": "ipv4-addr",
    "value": "198.51.100.2"
```

```

    },
    "1": {
      "type": "ipv4-addr",
      "value": "198.51.100.3"
    },
    "2": {
      "type": "network-traffic",
      "src_ref": "0",
      "dst_ref": "1",
      "protocols": [
        "tcp"
      ]
    }
  }
}

```

Basic HTTP Network Traffic

```

{
  "0": {
    "type": "domain-name",
    "value": "example.com"
  },
  "1": {
    "type": "network-traffic",
    "dst_ref": "0",
    "protocols": [
      "ipv4",
      "tcp",
      "http"
    ]
  }
}

```

Network Traffic with Netflow Data

```

{
  "0": {
    "type": "ipv4-addr",
    "value": "203.0.113.1"
  },
  "1": {
    "type": "ipv4-addr",
    "value": "203.0.113.5"
  },
  "2": {
    "type": "network-traffic",
    "src_ref": "0",

```

```

    "dst_ref": "1",
    "protocols": [
      "ipv4",
      "tcp"
    ],
    "src_byte_count": 147600,
    "src_packets": 100,
    "ipfix": {
      "minimumIpTotalLength": 32,
      "maximumIpTotalLength": 2556
    }
  }
}

```

Basic Tunneled Network Traffic

```

{
  "0": {
    "type": "ipv4-addr",
    "value": "198.51.100.2"
  },
  "1": {
    "type": "ipv4-addr",
    "value": "203.0.113.1"
  },
  "2": {
    "type": "ipv4-addr",
    "value": "203.0.113.2"
  },
  "3": {
    "type": "network-traffic",
    "src_ref": "0",
    "dst_ref": "1",
    "src_port": 2487,
    "dst_port": 1723,
    "protocols": [
      "ipv4",
      "pptp"
    ],
    "src_byte_count": 35779,
    "dst_byte_count": 935750,
    "encapsulates_refs": [
      "4"
    ]
  },
  "4": {

```

```

    "type": "network-traffic",
    "src_ref": "0",
    "dst_ref": "2",
    "src_port": 24678,
    "dst_port": 80,
    "protocols": [
        "ipv4",
        "tcp",
        "http"
    ],
    "src_packets": 14356,
    "dst_packets": 14356,
    "encapsulated_by_ref": "3"
  }
}

```

Web traffic tunneled over DNS

```

{
  "0": {
    "type": "ipv4-addr",
    "value": "203.0.113.1"
  },
  "1": {
    "type": "ipv4-addr",
    "value": "198.51.100.34"
  },
  "2": {
    "type": "ipv4-addr",
    "value": "198.51.100.54"
  },
  "3": {
    "type": "network-traffic",
    "src_ref": "0",
    "dst_ref": "1",
    "src_port": 2487,
    "dst_port": 53,
    "protocols": [
        "ipv4",
        "udp",
        "dns"
    ],
    "src_byte_count": 35779,
    "dst_byte_count": 935750,
    "encapsulates_refs": [
        "4"
    ]
  }
}

```



```

    ]
  },
  "4": {
    "type": "network-traffic",
    "src_ref": "0",
    "dst_ref": "2",
    "src_port": 24678,
    "dst_port": 443,
    "protocols": [
      "ipv4",
      "tcp",
      "ssl",
      "http"
    ],
    "src_packets": 14356,
    "dst_packets": 14356,
    "encapsulated_by_ref": "3"
  }
}

```

2.12.2 HTTP Request Extension

Type Name: `http-request-ext`

The HTTP request extension specifies a default extension for capturing network traffic properties specific to HTTP requests. The key for this extension when used in the **extensions** dictionary **MUST** be `http-request-ext`.

2.12.2.1 2.12.2.1 Properties

Property Name	Type	Description
request_method (required)	<code>string</code>	Specifies the HTTP method portion of the HTTP request line, as a lowercase string.
request_value (required)	<code>string</code>	Specifies the value (typically a resource path) portion of the HTTP request line.
request_version (optional)	<code>string</code>	Specifies the HTTP version portion of the HTTP request line, as a lowercase string.
request_header (optional)	<code>dictionary</code>	<p>Specifies all of the HTTP header fields that may be found in the HTTP client request, as a dictionary.</p> <p>Each key in the dictionary MUST be the name of the header field and SHOULD preserve case, e.g., User-Agent. The corresponding value for each dictionary</p>

		key MUST be a string .
message_body_length (optional)	integer	Specifies the length of the HTTP message body, if included, in bytes.
message_body_data_ref (optional)	object-ref	Specifies the data contained in the HTTP message body, if included. The object referenced in this property MUST be of type artifact .

Examples

Basic HTTP Request

```
{
  "0": {
    "type": "ipv4-addr",
    "value": "198.51.100.53"
  },
  "1": {
    "type": "network-traffic",
    "dst_ref": "0",
    "protocols": [
      "tcp",
      "http"
    ],
    "extensions": {
      "http-request-ext": {
        "request_method": "get",
        "request_value": "/download.html",
        "request_version": "http/1.1",
        "request_header": {
          "Accept-Encoding": "gzip,deflate",
          "User-Agent": "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6)
Gecko/20040113",
          "Host": "www.example.com"
        }
      }
    }
  }
}
```

2.12.3 ICMP Extension

Type Name: **icmp-ext**

The ICMP extension specifies a default extension for capturing network traffic properties specific to ICMP. The key for this extension when used in the **extensions** dictionary **MUST** be [icmp-ext](#).

2.12.3.1 Properties

Property Name	Type	Description
icmp_type_hex (required)	hex	Specifies the ICMP type byte.
icmp_code_hex (required)	hex	Specifies the ICMP code byte.

Examples

Basic ICMP Traffic

```
{
  "0": {
    "type": "ipv4-addr",
    "value": "198.51.100.9"
  },
  "1": {
    "type": "ipv4-addr",
    "value": "203.0.113.5"
  },
  "2": {
    "type": "network-traffic",
    "src_ref": "0",
    "dst_ref": "1",
    "protocols": [
      "icmp"
    ],
    "extensions": {
      "icmp-ext": {
        "icmp_type_hex": "08",
        "icmp_code_hex": "00"
      }
    }
  }
}
```

2.12.4 Network Socket Extension

Type Name: [socket-ext](#)

The Network Socket extension specifies a default extension for capturing network traffic properties associated with network sockets. The key for this extension when used in the extensions dictionary **MUST** be [socket-ext](#).

2.12.4.1 Properties

Property Name	Type	Description
address_family (required)	network-socket-address-family-enum	Specifies the address family (AF_*) that the socket is configured for.
is_blocking (optional)	boolean	Specifies whether the socket is in blocking mode.
is_listening (optional)	boolean	Specifies whether the socket is in listening mode.
protocol_family (optional)	network-socket-protocol-family-enum	Specifies the protocol family (PF_*) that the socket is configured for.
options (optional)	dictionary	Specifies any options (SO_*) that may be used by the socket, as a dictionary. Each key in the dictionary SHOULD be a case-preserved version of the option name, e.g., SO_ACCEPTCONN. Each key value in the dictionary MUST be the value for the corresponding options key.
socket_type (optional)	network-socket-type-enum	Specifies the type of the socket.
socket_descriptor (optional)	integer	Specifies the socket file descriptor value associated with the socket, as a non-negative integer.
socket_handle (optional)	integer	Specifies the handle or inode value associated with the socket.

2.12.4.2 Network Socket Address Family Enumeration

Enumeration Name: network-socket-address-family-enum

An enumeration of network socket address family types.

Vocabulary Value	Description
AF_UNSPEC	Specifies an unspecified address family.

AF_INET	Specifies the IPv4 address family.
AF_IPX	Specifies the IPX (Novell Internet Protocol) address family.
AF_APPLETALK	Specifies the APPLETALK DDP address family.
AF_NETBIOS	Specifies the NETBIOS address family.
AF_INET6	Specifies the IPv6 address family.
AF_IRDA	Specifies IRDA sockets.
AF_BTH	Specifies BTH sockets.

-

2.12.4.3 Network Socket Protocol Family Enumeration

Enumeration Name: network-socket-protocol-family-enum

An enumeration of network socket protocol family types.

Vocabulary Value	Description
PF_INET	Specifies the IP protocol family.
PF_AX25	Specifies the amateur radio AX.25 family.
PF_IPX	Specifies the Novell Internet Protocol family.
PF_INET6	Specifies the IP version 6 family.
PF_APPLETALK	Specifies the Appletalk DDP protocol family.
PF_NETROM	Specifies the Amateur radio NetROM protocol family.
PF_BRIDGE	Specifies the Multiprotocol bridge protocol family.
PF_ATMPVC	Specifies the ATM PVCs protocol family.
PF_X25	Specifies the protocol family reserved for the X.25 project.

PF_ROSE	Specifies the PF_KEY key management API family.
PF_DECNET	Specifies the protocol family reserved for the DECnet project.
PF_NETBEUI	Specifies the protocol family reserved for the 802.2LLC project.
PF_SECURITY	Specifies the Security callback pseudo AF protocol family.
PF_KEY	Specifies the PF_KEY key management API protocol family.
PF_NETLINK	Specifies the netlink routing API family.
PF_ROUTE	Specifies the PF_ROUTE routing API family.
PF_PACKET	Specifies the packet family.
PF_ASH	Specifies the Ash family.
PF_ECONET	Specifies the Acorn Econet family.
PF_ATMSVC	Specifies the ATM SVCs protocol family.
PF_SNA	Specifies the Linux SNA Project protocol family.
PF_IRDA	Specifies IRDA sockets.
PF_PPPOX	Specifies PPPoX sockets.
PF_WANPIPE	Specifies Wanpipe API sockets.
PF_BLUETOOTH	Specifies Bluetooth sockets.

2.12.4.4 Network Socket Type Enumeration

Enumeration **Name:** `network-socket-type-enum`

An enumeration of network socket types.

Vocabulary Value	Description
------------------	-------------

<code>SOCK_STREAM</code>	Specifies a pipe-like socket which operates over a connection with a particular remote socket, and transmits data reliably as a stream of bytes.
<code>SOCK_DGRAM</code>	Specifies a socket in which individually-addressed packets are sent (datagram).
<code>SOCK_RAW</code>	Specifies raw sockets which allow new IP protocols to be implemented in user space. A raw socket receives or sends the raw datagram not including link level headers.
<code>SOCK_RDM</code>	Specifies a socket indicating a reliably-delivered message.
<code>SOCK_SEQPACKET</code>	Specifies a datagram congestion control protocol socket.

Examples

Basic Stream Socket

```
{
  "0": {
    "type": "ipv4-addr",
    "value": "198.51.100.2"
  },
  "1": {
    "type": "network-traffic",
    "src_ref": "0",
    "src_port": 223,
    "protocols": [
      "ip",
      "tcp"
    ],
    "extensions": {
      "socket-ext": {
        "is_listening": "true",
        "address_family": "AF_INET",
        "protocol_family": "PF_INET",
        "socket_type": "SOCK_STREAM"
      }
    }
  }
}
```

2.12.5 TCP Extension

Type Name: `tcp-ext`

The TCP extension specifies a default extension for capturing network traffic properties specific to TCP. The key for this extension when used in the **extensions** dictionary **MUST** be `tcp-ext`. An object using the TCP Extension **MUST** contain at least one property from this extension.

2.12.5.1 Properties

Property Name	Type	Description
src_flags_hex (optional)	hex	<p>Specifies the source TCP flags, as the union of all TCP flags observed between the start of the traffic (as defined by the start property) and the end of the traffic (as defined by the end property).</p> <p>If the start and end times of the traffic are not specified, this property SHOULD be interpreted as the union of all TCP flags observed over the entirety of the network traffic being reported upon.</p>
dst_flags_hex (optional)	hex	<p>Specifies the destination TCP flags, as the union of all TCP flags observed between the start of the traffic (as defined by the start property) and the end of the traffic (as defined by the end property).</p> <p>If the start and end times of the traffic are not specified, this property SHOULD be interpreted as the union of all TCP flags observed over the entirety of the network traffic being reported upon.</p>

Examples

Basic TCP Traffic

```
{
  "0": {
    "type": "ipv4-addr",
    "value": "198.51.100.5"
  },
  "1": {
    "type": "ipv4-addr",
    "value": "198.51.100.6"
  },
  "2": {
    "type": "network-traffic",
    "src_ref": "0",
    "dst_ref": "1",
    "src_port": 3372,
    "dst_port": 80,
    "protocols": [
      "tcp"
    ],
    "extensions": {
      "tcp-ext": {
```



```

    "src_flags_hex": "00000002"
  }
}
}
}

```

2.13 Process Object

Type Name: `process`

The Process Object represents common properties of an instance of a computer program as executed on an operating system. A Process Object **MUST** contain at least one property (other than **type**) from this object (or one of its extensions).

2.13.1 Properties

Common Properties		
<code>type</code> , <code>description</code> , <code>extensions</code>		
Process Object Specific Properties		
<code>is_hidden</code> , <code>pid</code> , <code>name</code> , <code>created</code> , <code>cwd</code> , <code>arguments</code> , <code>command_line</code> , <code>environment_variables</code> , <code>opened_connection_refs</code> , <code>creator_user_ref</code> , <code>binary_ref</code> , <code>parent_ref</code> , <code>child_refs</code>		
Property Name	Type	Description
<code>type</code> (required)	<code>string</code>	The value of this property MUST be <code>process</code> .
<code>extensions</code> (optional)	<code>dictionary</code>	<p>The Process Object defines the following extensions. In addition to these, producers MAY create their own.</p> <p><code>windows-process-ext</code>, <code>windows-service-ext</code></p> <p>Dictionary keys MUST identify the extension type by name.</p> <p>The corresponding dictionary values MUST contain the contents of the extension instance.</p>
<code>is_hidden</code> (optional)	<code>boolean</code>	Specifies whether the process is hidden.
<code>pid</code> (optional)	<code>integer</code>	Specifies the Process ID, or PID, of the process.
<code>name</code> (optional)	<code>string</code>	Specifies the name of the process.

created (optional)	timestamp	Specifies the date/time at which the process was created.
cwd (optional)	string	Specifies the current working directory of the process.
arguments (optional)	list of type string	Specifies the list of arguments used in executing the process. Each argument MUST be captured separately as a string.
command_line (optional)	string	Specifies the full command line used in executing the process, including the process name (depending on the operating system).
environment_variables (optional)	dictionary	Specifies the list of environment variables associated with the process as a dictionary. Each key in the dictionary MUST be a case preserved version of the name of the environment variable, and each corresponding value MUST be the environment variable value as a string.
opened_connection_refs (optional)	list of type object-ref	<p>Specifies the list of network connections opened by the process, as a reference to one or more Network Traffic Objects.</p> <p>The objects referenced in this list MUST be of type network-traffic.</p>
creator_user_ref (optional)	object-ref	<p>Specifies the user that created the process, as a reference to a User Account Object.</p> <p>The object referenced in this property MUST be of type user-account.</p>
binary_ref (optional)	object-ref	<p>Specifies the executable binary that was executed as the process, as a reference to a File Object.</p> <p>The object referenced in this property MUST be of type file.</p>
parent_ref (optional)	object-ref	<p>Specifies the other process that spawned (i.e. is the parent of) this one, as a reference to a Process Object.</p> <p>The object referenced in this property MUST be of type process.</p>

child_refs (optional)	list of type object-ref	Specifies the other processes that were spawned by (i.e. children of) this process, as a reference to one or more other Process Objects. The objects referenced in this list MUST be of type process .
------------------------------	---------------------------------------	---

Examples

Basic Process

```
{
  "0": {
    "type": "file",
    "hashes": {
      "MD5": "B4D33B0C7306351B9ED96578465C5579"
    },
    "SHA-256": "35a01331e9ad96f751278b891b6ea09699806faedfa237d40513d92ad1b7100fSHA"
  },
  "1": {
    "type": "process",
    "pid": 1221,
    "name": "gedit-bin",
    "created": "2016-01-20T14:11:25.55Z",
    "arguments" :[
      "--new-window"
    ],
    "binary_ref": "0"
  }
}
```

2.13.2 Windows™ Process Extension

Type Name: **windows-process-ext**

The Windows Process extension specifies a default extension for capturing properties specific to Windows processes. The key for this extension when used in the **extensions** dictionary **MUST** be **windows-process-ext**. An object using the Windows Process Extension **MUST** contain at least one property from this extension.

2.13.2.1 Properties

Property Name	Type	Description
aslr_enabled (optional)	boolean	Specifies whether Address Space Layout Randomization (ASLR) is enabled for the process.

dep_enabled (optional)	boolean	Specifies whether Data Execution Prevention (DEP) is enabled for the process.
priority (optional)	string	Specifies the current priority class of the process in Windows. This value SHOULD be a string that ends in CLASS .
owner_sid (optional)	string	Specifies the Security ID (SID) value of the owner of the process.
window_title (optional)	string	Specifies the title of the main window of the process.
startup_info (optional)	dictionary	Specifies the STARTUP_INFO struct used by the process, as a dictionary. Each name/value pair in the struct MUST be represented as a key/value pair in the dictionary, where each key MUST be a case-preserved version of the original name. For example, given a name of "_lpDesktop" the corresponding key would be lpDesktop .

Examples

Basic Windows Process

```
{
  "0": {
    "type": "process",
    "pid": 314,
    "name": "foobar.exe",
    "extensions": {
      "windows-process-ext": {
        "aslr_enabled": true,
        "dep_enabled": true,
        "priority": "HIGH_PRIORITY_CLASS",
        "owner_sid": "S-1-5-21-186985262-1144665072-74031268-1309"
      }
    }
  }
}
```

2.13.3 Windows™ Service Extension

Type Name: **windows-service-ext**

The Windows Service extension specifies a default extension for capturing properties specific to Windows services. The key for this extension when used in the **extensions** dictionary **MUST** be **windows-service-ext**.

2.13.3.1 Properties

Property Name	Type	Description
service_name (required)	string	Specifies the name of the service.
descriptions (optional)	list of type string	Specifies the descriptions defined for the service.
display_name (optional)	string	Specifies the displayed name of the service in Windows GUI controls.
group_name (optional)	string	Specifies the name of the load ordering group of which the service is a member.
start_type (optional)	windows-service-start-type-enum	Specifies the start options defined for the service.
service_dll_refs (optional)	list of type object-ref	Specifies the DLLs loaded by the service, as a reference to one or more File Objects. The objects referenced in this property MUST be of type file.
service_type (optional)	windows-service-type-enum	Specifies the type of the service.
service_status (optional)	windows-service-status-enum	Specifies the current status of the service.

2.13.3.2 Windows™ Service Start Type Enumeration

Enumeration Name: windows-service-start-type-enum

An enumeration of Windows service start types.

Vocabulary Value	Description
SERVICE_AUTO_START	A service started automatically by the service control manager during system startup.
SERVICE_BOOT_START	A device driver started by the system loader. This value is valid only for driver services.

<code>SERVICE_DEMAND_START</code>	A service started by the service control manager when a process calls the StartService function.
<code>SERVICE_DISABLED</code>	A service that cannot be started. Attempts to start the service result in the error code ERROR_SERVICE_DISABLED.
<code>SERVICE_SYSTEM_ALERT</code>	A device driver started by the IoInitSystem function. This value is valid only for driver services.

2.13.3.3 Windows™ Service Type Enumeration

Enumeration Name: `windows-service-type-enum`

An enumeration of Windows service types.

Vocabulary Value	Description
<code>SERVICE_KERNEL_DRIVER</code>	The service is a device driver.
<code>SERVICE_FILE_SYSTEM_DRIVER</code>	The service is a file system driver.
<code>SERVICE_WIN32_OWN_PROCESS</code>	The service runs in its own process.
<code>SERVICE_WIN32_SHARE_PROCESS</code>	The service shares a process with other services.

2.13.3.4 Windows™ Service Status Enumeration

Enumeration Name: `windows-service-status-enum`

An enumeration of Windows service statuses.

Value	Description
<code>SERVICE_CONTINUE_PENDING</code>	The service continue is pending.
<code>SERVICE_PAUSE_PENDING</code>	The service pause is pending.
<code>SERVICE_PAUSED</code>	The service is paused.

<code>SERVICE_RUNNING</code>	The service is running.
<code>SERVICE_START_PENDING</code>	The service is starting.
<code>SERVICE_STOP_PENDING</code>	The service is stopping.
<code>SERVICE_STOPPED</code>	The service is not running.

Examples

Basic Windows Service

```
{
  "0": {
    "type": "file",
    "hashes": {
      "MD5": "B4D33B0C7306351B9ED96578465C5579"
      "SHA-256": "35a01331e9ad96f751278b891b6ea09699806faedfa237d40513d92ad1b7100f"
    },
    "name": "sirvizio.exe"
  },
  "1": {
    "type": "process",
    "pid": 2217,
    "name": "sirvizio",
    "command_line": "C:\\Windows\\System32\\sirvizio.exe /s",
    "binary_ref": "0",
    "extensions": {
      "windows-service-ext": {
        "service_name": "sirvizio",
        "display_name": "Sirvizio",
        "start_type": "SERVICE_AUTO_START",
        "service_type": "SERVICE_WIN32_OWN_PROCESS",
        "service_status": "SERVICE_RUNNING"
      }
    }
  }
}
```

2.14 Software Object

Type Name: `software`

The Software Object represents high-level properties associated with software, including software products.

2.14.1 Properties

Common Properties		
type, description , extensions		
Software Object Specific Properties		
name, cpe, languages, vendor, version		
Property Name	Type	Description
type (required)	string	The value of this property MUST be software .
name (required)	string	Specifies the name of the software.
cpe (optional)	string	<p>Specifies the Common Platform Enumeration (CPE) entry for the software, if available. The value for this property MUST be a CPE v2.3 entry from the official NVD CPE Dictionary [NVD].</p> <p>While the CPE dictionary does not contain entries for <i>all</i> software, whenever it <i>does</i> contain an identifier for a given instance of software, this property SHOULD be present.</p>
languages (optional)	list of type string	Specifies the languages supported by the software. The value of each list member MUST be an ISO 639-2 language code [ISO639-2] .
vendor (optional)	string	Specifies the name of the vendor of the software.
version (optional)	string	Specifies the version of the software.

Examples

Typical Software Instance

```
{
  "0": {
    "type": "software",
    "name": "Word",
    "cpe": "cpe:2.3:a:microsoft:word:2000.*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:*:**",
    "version": "2002",
    "vendor": "Microsoft"
  }
}
```


2.15 URL Object

Type Name: `url`

The URL Object represents the properties of a uniform resource locator (URL).

2.15.1 Properties

Common Properties		
type, description , extensions		
URL Object Specific Properties		
value		
Property Name	Type	Description
type (required)	<code>string</code>	The value of this property MUST be <code>url</code> .
value (required)	<code>string</code>	Specifies the value of the URL. <u>The value of this property MUST conform to [RFC3986], more specifically section 1.1.3 with reference to the definition for "Uniform Resource Locator".</u>

Examples

Typical URL

```
{
  "0": {
    "type": "url",
    "value": "https://example.com/research/index.html"
  }
}
```

2.16 User Account Object

Type Name: `user-account`

The User Account Object represents an instance of any type of user account, including but not limited to operating system, device, messaging service, and social media platform accounts.

2.16.1 Properties

Common Properties

type, ~~description~~, extensions

User Account Object Specific Properties

user_id, account_login, account_type, display_name, is_service_account, is_privileged, can_escalate_privs, is_disabled, account_created, account_expires, password_last_changed, account_first_login, account_last_login

Property Name	Type	Description
type (required)	string	The value of this property MUST be <code>user-account</code> .
extensions (optional)	dictionary	<p>The User Account Object defines the following extensions. In addition to these, producers MAY create their own.</p> <p><code>unix-account-ext</code></p> <p>Dictionary keys MUST identify the extension type by name.</p> <p>The corresponding dictionary values MUST contain the contents of the extension instance.</p>
user_id (required)	string	Specifies the identifier of the account. The format of the identifier depends on the system the user account is maintained in, and may be a numeric ID, a GUID, an account name, an email address, etc. The <code>user_id</code> property should be populated with whatever field is the unique identifier for the system the account is a member of. For example, for UNIX systems it would be populated with the UID.
account_login (optional)	string	<p>Specifies the account login string, used in cases where the <code>user_id</code> property specifies something other than what a user would type when they login.</p> <p>For example, in the case of a Unix account with <code>user_id</code> 0, the <code>account_login</code> might be "root".</p>
account_type (optional)	open-vocab	<p>Specifies the type of the account.</p> <p>This is an open vocabulary and values SHOULD come from the <code>account-type-ov</code> vocabulary.</p>
display_name (optional)	string	Specifies the display name of the account, to be shown

		<p>in user interfaces, if applicable.</p> <p>On Unix, this is equivalent to the GECOS field.</p>
is_service_account (optional)	boolean	Indicates that the account is associated with a network service or system process (daemon), not a specific individual.
is_privileged (optional)	boolean	Specifies that the account has elevated privileges (i.e., in the case of root on Unix or the Windows Administrator account).
can_escalate_privs (optional)	boolean	Specifies that the account has the ability to escalate privileges (i.e., in the case of sudo on Unix or a Windows Domain Admin account)
is_disabled (optional)	boolean	Specifies if the account is disabled.
account_created (optional)	timestamp	Specifies when the account was created.
account_expires (optional)	timestamp	Specifies the expiration date of the account.
password_last_changed (optional)	timestamp	Specifies when the account password was last changed.
account_first_login (optional)	timestamp	Specifies when the account was first accessed.
account_last_login (optional)	timestamp	Specifies when the account was last accessed.

2.16.2 Account Type Vocabulary

Vocabulary Name: account-type-ov

An open vocabulary of User Account types.

Vocabulary Value	Description
unix	Specifies a POSIX account.
windows-local	Specifies a Windows local account.

<code>windows-domain</code>	Specifies a Windows domain account.
<code>ldap</code>	Specifies an LDAP account.
<code>tacacs</code>	Specifies a TACACS account.
<code>radius</code>	Specifies a RADIUS account.
<code>nis</code>	Specifies a NIS account
<code>openid</code>	Specifies an OpenID account.
<code>facebook</code>	Specifies a Facebook account.
<code>skype</code>	Specifies a Skype account.
<code>twitter</code>	Specifies a Twitter account.

Examples

Basic Unix Account

```
{
  "0": {
    "type": "user-account",
    "user_id": "1001",
    "account_login": "jdoe",
    "account_type": "unix",
    "display_name": "John Doe",
    "is_service_account": false,
    "is_privileged": false,
    "can_escalate_privs": true,
    "account_created": "2016-01-20T12:31:12Z",
    "password_last_changed": "2016-01-20T14:27:43Z",
    "account_first_login": "2016-01-20T14:26:07Z",
    "account_last_login": "2016-07-22T16:08:28Z"
  }
}
```

Basic Twitter Account

```
{
  "0": {
    "type": "user-account",
    "user_id": "thegrugq_ebooks",
```

```

    "account_login": "thegrugq_ebooks",
    "account_type": "twitter",
    "display_name": "the grugq"
  }
}

```

2.16.3 UNIX™ Account Extension

Type Name: `unix-account-ext`

The UNIX™ account extension specifies a default extension for capturing the additional information for an account on a UNIX system. The key for this extension when used in the **extensions** dictionary **MUST** be `unix-account-ext`. An object using the UNIX Account Extension **MUST** contain at least one property from this extension.

2.16.3.1 Properties

Property Name	Type	Description
gid (optional)	<code>number</code>	Specifies the primary group ID of the account.
groups (optional)	<code>list</code> of type <code>string</code>	Specifies a list of names of groups that the account is a member of.
home_dir (optional)	<code>string</code>	Specifies the home directory of the account.
shell (optional)	<code>string</code>	Specifies the account's command shell.

Examples

Basic UNIX Account

```

{
  "0": {
    "type": "user-account",
    "user_id": "1001",
    "account_login": "jdoe",
    "account_type": "unix",
    "display_name": "John Doe",
    "is_service_account": false,
    "is_privileged": false,
    "can_escalate_privs": true,
    "extensions": {
      "unix-account-ext": {
        "gid": 1001,
        "groups": ["wheel"],
        "home_dir": "/home/jdoe",

```

```

    "shell": "/bin/bash"
  }
}
}
}

```

2.17 Windows™ Registry Key Object

Type Name: windows-registry-key

The Registry Key Object represents the properties of a Windows registry key.

2.17.1 Properties

Common Properties		
type, description , extensions		
File Object Specific Properties		
key, values, modified, creator_user_ref, number_of_subkeys		
Property Name	Type	Description
type (required)	string	The value of this property MUST be windows-registry-key.
key (required)	string	Specifies the full registry key including the hive. The value of the key, including the hive portion, SHOULD be case-preserved. The hive portion of the key MUST be fully expanded and not truncated; e.g., HKEY_LOCAL_MACHINE must be used instead of HKLM.
values (optional)	list of type windows-registry-value-type	Specifies the values found under the registry key.
modified (optional)	timestamp	Specifies the last date/time that the registry key was modified.
creator_user_ref (optional)	object-ref	Specifies a reference to the user account (represented as a User Account Object) that created the registry key.

		The object referenced in this property MUST be of type <code>user-account</code> .
number_of_subkeys (optional)	<code>integer</code>	Specifies the number of subkeys contained under the registry key.

2.17.2 Windows™ Registry Value Type

Type Name: `windows-registry-value-type`

The Windows Registry Value type captures the properties of a Windows Registry Key Value.

2.17.2.1 Properties

Property Name	Type	Description
name (required)	<code>string</code>	Specifies the name of the registry value. For specifying the default value in a registry key, an empty string MUST be used.
data (optional)	<code>string</code>	Specifies the data contained in the registry value.
data_type (optional)	<code>windows-registry-datatype-enum</code>	Specifies the registry (REG_*) data type used in the registry value.

2.17.3 Windows™ Registry Datatype Enumeration

Enumeration Name: `windows-registry-datatype-enum`

An enumeration of Windows registry data types.

Vocabulary Value	Description
<code>REG_NONE</code>	No defined value type.
<code>REG_SZ</code>	A null-terminated string. This will be either a Unicode or an ANSI string, depending on whether you use the Unicode or ANSI functions.
<code>REG_EXPAND_SZ</code>	A null-terminated string that contains unexpanded references to environment variables (for example, "%PATH%"). It will be a Unicode or ANSI string depending on whether you use the Unicode or ANSI functions.

REG_BINARY	Binary data in any form.
REG_DWORD	A 32-bit number.
REG_DWORD_BIG_ENDIAN	A 32-bit number in big-endian format.
REG_LINK	A null-terminated Unicode string that contains the target path of a symbolic link.
REG_MULTI_SZ	A sequence of null-terminated strings, terminated by an empty string (\0).
REG_RESOURCE_LIST	A series of nested lists designed to store a resource list used by a hardware device driver or one of the physical devices it controls. This data is detected and written into the ResourceMap tree by the system and is displayed in Registry Editor in hexadecimal format as a Binary Value.
REG_FULL_RESOURCE_DESCRIPTION	A series of nested lists designed to store a resource list used by a physical hardware device. This data is detected and written into the HardwareDescription tree by the system and is displayed in Registry Editor in hexadecimal format as a Binary Value.
REG_RESOURCE_REQUIREMENTS_LIST	Device driver list of hardware resource requirements in Resource Map tree.
REG_QWORD	A 64-bit number.
REG_INVALID_TYPE	Specifies an invalid key.

Examples

Simple registry key

```
{
  "0": {
    "type": "windows-registry-key",
    "key": "HKEY_LOCAL_MACHINE\\System\\Foo\\Bar"
  }
}
```

Registry key with values

```
{
  "0": {
    "type": "windows-registry-key",
    "key": "hkey_local_machine\\system\\bar\\foo",

```



```

    "values": [
      {
        "name": "Foo",
        "data": "qwerty",
        "data_type": "REG_SZ"
      },
      {
        "name": "Bar",
        "data": "42",
        "data_type": "REG_DWORD"
      }
    ]
  }
}

```

2.18 X.509 Certificate Object

Type Name: `x509-certificate`

The X.509 Certificate Object represents the properties of an X.509 certificate, as defined by [ITU recommendation X.509 \[X.509\]](#). An X.509 Certificate Object **MUST** contain at least one property (other than **type**) from this object (or one of its extensions).

2.18.1 Properties

Common Properties		
type, description , extensions		
File Object Specific Properties		
is_self_signed, hashes, version, serial_number, signature_algorithm, issuer, validity_not_before, validity_not_after, subject, subject_public_key_algorithm, subject_public_key_modulus, subject_public_key_exponent, x509_v3_extensions		
Property Name	Type	Description
type (required)	string	The value of this property MUST be <code>x509-certificate</code> .
is_self_signed (optional)	boolean	Specifies whether the certificate is self-signed, i.e., whether it is signed by the same entity whose identity it certifies.
hashes (optional)	hashes -type	Specifies any hashes that were calculated for the entire contents of the certificate.

version (optional)	string	Specifies the version of the encoded certificate.
serial_number (optional)	string	Specifies the unique identifier for the certificate, as issued by a specific Certificate Authority.
signature_algorithm (optional)	string	Specifies the name of the algorithm used to sign the certificate.
issuer (optional)	string	Specifies the name of the Certificate Authority that issued the certificate.
validity_not_before (optional)	timestamp	Specifies the date on which the certificate validity period begins.
validity_not_after (optional)	timestamp	Specifies the date on which the certificate validity period ends.
subject (optional)	string	Specifies the name of the entity associated with the public key stored in the subject public key field of the certificate.
subject_public_key_algorithm (optional)	string	Specifies the name of the algorithm with which to encrypt data being sent to the subject.
subject_public_key_modulus (optional)	string	Specifies the modulus portion of the subject's public RSA key.
subject_public_key_exponent (optional)	integer	Specifies the exponent portion of the subject's public RSA key, as an integer.
x509_v3_extensions (optional)	x509-v3-extensions-type	Specifies any standard X.509 v3 extensions that may be used in the certificate.

2.18.2 X.509 v3 Extensions Type

Type Name: x509-v3-extensions-type

The X.509 v3 Extensions type captures properties associated with X.509 v3 extensions, which serve as a mechanism for specifying additional information such as alternative subject names. An object using the X.509 v3 Extensions type **MUST** contain at least one property from this type.

Note that the X.509 v3 Extensions type is not a STIX Cyber Observables extension, it is a type that describes X.509 extensions.

2.18.2.1 Properties

Property Name	Type	Description
basic_constraints (optional)	string	Specifies a multi-valued extension which indicates whether a certificate is a CA certificate. The first (mandatory) name is CA followed by <i>TRUE</i> or <i>FALSE</i> . If CA is <i>TRUE</i> then an optional pathlen name followed by a non-negative value can be included. Also equivalent to the object ID (OID) value of 2.5.29.19.
name_constraints (optional)	string	Specifies a namespace within which all subject names in subsequent certificates in a certification path MUST be located. Also equivalent to the object ID (OID) value of 2.5.29.30.
policy_constraints (optional)	string	Specifies any constraints on path validation for certificates issued to CAs. Also equivalent to the object ID (OID) value of 2.5.29.36.
key_usage (optional)	string	Specifies a multi-valued extension consisting of a list of names of the permitted key usages. Also equivalent to the object ID (OID) value of 2.5.29.15.
extended_key_usage (optional)	string	Specifies a list of usages indicating purposes for which the certificate public key can be used for. Also equivalent to the object ID (OID) value of 2.5.29.37.
subject_key_identifier (optional)	string	Specifies the identifier that provides a means of identifying certificates that contain a particular public key. Also equivalent to the object ID (OID) value of 2.5.29.14.
authority_key_identifier (optional)	string	Specifies the identifier that provides a means of identifying the public key corresponding to the private key used to sign a certificate. Also equivalent to the object ID (OID) value of 2.5.29.35.
subject_alternative_name (optional)	string	Specifies the additional identities to be bound to the subject of the certificate. Also equivalent to the object ID (OID) value of 2.5.29.17.
issuer_alternative_name	string	Specifies the additional identities to be bound to

(optional)		the issuer of the certificate. Also equivalent to the object ID (OID) value of 2.5.29.18.
subject_directory_attributes (optional)	string	Specifies the identification attributes (e.g., nationality) of the subject. Also equivalent to the object ID (OID) value of 2.5.29.9.
crl_distribution_points (optional)	string	Specifies how CRL information is obtained. Also equivalent to the object ID (OID) value of 2.5.29.31.
inhibit_any_policy (optional)	string	Specifies the number of additional certificates that may appear in the path before anyPolicy is no longer permitted. Also equivalent to the object ID (OID) value of 2.5.29.54.
private_key_usage_period_not_before (optional)	timestamp	Specifies the date on which the validity period begins for the private key, if it is different from the validity period of the certificate.
private_key_usage_period_not_after (optional)	timestamp	Specifies the date on which the validity period ends for the private key, if it is different from the validity period of the certificate.
certificate_policies (optional)	string	Specifies a sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers. Also equivalent to the object ID (OID) value of 2.5.29.32.
policy_mappings (optional)	string	Specifies one or more pairs of OIDs; each pair includes an issuerDomainPolicy and a subjectDomainPolicy. The pairing indicates whether the issuing CA considers its issuerDomainPolicy equivalent to the subject CA's subjectDomainPolicy. Also equivalent to the object ID (OID) value of 2.5.29.33.

Examples

Basic X.509 certificate

```
{
  "0": {
    "type": "x509-certificate",
    "issuer": "C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification
Services Division, CN=Thawte Server CA/emailAddress=server-certs@thawte.com",
    "validity_not_before": "2016-03-12T12:00:00Z",
    "validity_not_after": "2016-08-21T12:00:00Z".
```

```
"subject": "C=US, ST=Maryland, L=Pasadena, O=Brent Baccala, OU=FreeSoft,  
CN=www.freesoft.org/emailAddress=baccala@freesoft.org",  
}  
  
}  
  
"validity_not_before": "2016-03-12T12:00:00Z",  
"validity_not_after": "2016-08-21T12:00:00Z"  
}  
}
```

3 Conformance

3.1 Defined Object Producers

A "Defined Object Producer" that creates an Object from section [2](#) (Defined Object Data Models) is a "Producer" of that Object. Defined Object Producers **MUST** conform to all normative requirements in the section for that Object along with all of the general requirements pertaining to Objects as defined in section 3 of [STIX™ Version 2.0. Part 3: Cyber Observable Core Concepts](#).

For example, a "Defined Object Producer" that can produce File Object is a "File Object Producer". That producer has to conform to all normative requirements in Cyber Observable Objects ~~S~~ection 2.7, File Object.

3.2 Defined Object Consumers

A "Defined Object Consumer" that receives an Object from section [2](#) (Defined Object Data Models) is a "Consumer" of that Object. Defined Object Consumers **MUST** conform to all normative requirements in the section for that Object along with all of the general requirements pertaining to Objects as defined in section 3 of [STIX™ Version 2.0. Part 3: Cyber Observable Core Concepts](#).

For example, an "Object Consumer" that can receive Network Traffic Objects is a "Network Traffic Object Consumer". That consumer has to conform to all normative requirements in Cyber Observable Objects Section 2.12, Network Traffic Object.

Appendix A. Glossary

CAPEC - Common Attack Pattern Enumeration and Classification

Consumer - Any entity that receives STIX content

CTI - Cyber Threat Intelligence

Embedded Relationship - A link (an "edge" in a graph) between one STIX Object and another represented as a property on one object containing the ID of another object

Entity - Anything that has a separately identifiable existence (e.g., organization, person, group, etc.)

IEP - FIRST (Forum of Incident Response and Security Teams) Information Exchange Policy

Instance - A single occurrence of a STIX object version

MTI - Mandatory To Implement

MVP - Minimally Viable Product

Object Creator - The entity that created or updated a STIX object (see section 3.3 of [*STIX™ Version 2.0. Part 1: STIX Core Concepts*](#)).

Object Representation - An instance of an object version that is serialized as STIX

Producer - Any entity that distributes STIX content, including object creators as well as those passing along existing content

SDO - STIX Domain Object (a "node" in a graph)

SRO - STIX Relationship Object (one mechanism to represent an "edge" in a graph)

STIX - Structured Threat Information Expression

STIX Content - STIX documents, including STIX Objects, STIX Objects grouped as bundles, etc.

STIX Object - A STIX Domain Object (SDO) or STIX Relationship Object (SRO)

STIX Relationship - A link (an "edge" in a graph) between two STIX Objects represented by either an SRO or an embedded relationship

TAXII - An application layer protocol for the communication of cyber threat information

TLP - Traffic Light Protocol

TTP - Tactic, technique, or procedure; behaviors and resources that attackers use to carry out their attacks

~~Appendix A.~~Appendix B. Acknowledgments

The contributions of the OASIS Cyber Threat Intelligence (CTI) Technical Committee members, enumerated in [STIX™ Version 2.0. Part 1: STIX Core Concepts](#), are gratefully acknowledged.

Appendix B. Appendix C. Revision History

Revision	Date	Editor	Changes Made
01	2017-01-20	Bret Jordan, John Wunder, Rich Piazza, Ivan Kirillov, Trey Darley	Initial Version
<u>02</u>	<u>2017-04-24</u>	<u>Bret Jordan,</u> <u>John Wunder,</u> <u>Rich Piazza,</u> <u>Ivan Kirillov,</u> <u>Trey Darley</u>	<u>Changes made from first public review</u>