

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 30, 2014

P. Fan
China Mobile
July 29, 2013

Information Elements for Application Layer Information Export
draft-fan-ipfix-content-info-ie-01

Abstract

This document specifies extended Information Elements used in the IP Flow Information Export (IPFIX) to export content related information.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 30, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	New Information Elements	3
2.1.	httpRequestMethod	3
2.2.	httpRequestURI	3
2.3.	httpVersion	3
2.4.	httpResponseStatuscode	4
2.5.	httpRequestHost	4
2.6.	httpRequestReferer	5
2.7.	httpContentType	5
2.8.	httpOctetDeltaCount	5
2.9.	httpOctetTotalCount	6
2.10.	dnsQueryName	6
2.11.	dnsQueryType	6
2.12.	dnsQueryDeltaCount	7
2.13.	dnsQueryTotalCount	7
3.	Security Considerations	7
4.	IANA Considerations	8
5.	Normative References	8
	Author's Address	8

[1.](#) Introduction

Our internet today employs a large and increasing number of devices with content aware ability. These devices detect packet content of traffic flows rather than just packet headers, and perform specific functions using content information together with traditional information on layer 3 or layer 4. Content information is used for various purposes: analyzing, optimizing, business, security, etc. Examples of functions utilizing content information include traffic visualizing, policy based control, content based charging, etc.

Although content related information is vital in the smart operation of internet traffic and has already been widely referred to in the network, there is still not an effective, well defined method to export content information, especially in a standardized, interoperable way.

The IP Flow Information Export (IPFIX) working group has produced a series of specifications that help export flow information, including protocol [[I-D.ietf-ipfix-protocol-rfc5101bis](#)] and information model [[I-D.ietf-ipfix-information-model-rfc5102bis](#)]. However, higher-layer

content related information export is not yet well standardized.
This document specifies Information Elements used to export content information.

[2.](#) New Information Elements

This section describes a list of new Information Elements that are used to export content information. The list is subject to change in later revisions of this documents.

[2.1.](#) `httpRequestMethod`

Description:

The request method of an HTTP request message to be performed on the resource identified by the request URI.

Abstract Data Type: string

Data Type Semantics:

ElementId: TBD01

Status: current

Reference: [[RFC2616](#)]

[2.2.](#) `httpRequestURI`

Description:

The Uniform Resource Identifier indicated by the Request-URI field in the first line of an HTTP request message. The URI is used to identify the resource upon which to apply the request.

Abstract Data Type: string

Data Type Semantics:

ElementId: TBD02

Status: current

Reference: [[RFC2616](#)]

[2.3.](#) httpVersion

Description:

The version of the HTTP protocol indicated by the HTTP-Version field in the first line of an HTTP message.

Fan

Expires January 30, 2014

[Page 3]

Internet-Draft Application Layer Information Elements

July 2013

Abstract Data Type: string

Data Type Semantics:

ElementId: TBD03

Status: current

Reference: [[RFC2616](#)]

[2.4.](#) httpResponseStatusCode

Description:

The value of the Status-Code field in the first line of an HTTP response message. The Information Element consists of 3 numeric characters indicating the result of the attempt to understand and satisfy the HTTP request.

Abstract Data Type: string

Data Type Semantics:

ElementId: TBD04

Status: current

Reference: [[RFC2616](#)]

[2.5.](#) httpRequestHost

Description:

The Host request-header field in an HTTP request message used to specify the Internet host and port number of the resource being requested.

Abstract Data Type: string

Data Type Semantics:

ElementId: TBD05

Status: current

Reference: [[RFC2616](#)]

[2.6.](#) httpRequestReferer

Description:

The Referer request-header field in an HTTP request message used to specify the address (URI) of the resource from which the Request-URI was obtained.

Abstract Data Type: string

Data Type Semantics:

ElementId: TBD06

Status: current

Reference: [[RFC2616](#)]

[2.7.](#) httpContentType

Description:

The Content-Type response-header field in an HTTP response message indicating the type of the content.

Abstract Data Type: string

Data Type Semantics:

ElementId: TBD07

Status: current

Reference: [[RFC2616](#)]

[2.8.](#) httpOctetDeltaCount

Description:

The number of HTTP layer octets since the previous report (if any) in incoming packets for this Flow at the Observation Point. The number of octets includes HTTP message header(s) and message body.

Abstract Data Type: unsigned64

Data Type Semantics: deltaCounter

ElementId: TBD08

Fan

Expires January 30, 2014

[Page 5]

Internet-Draft Application Layer Information Elements

July 2013

Status: current

Reference:

[2.9.](#) httpOctetTotalCount

Description:

The total number of HTTP layer octets in incoming packets for this Flow at the Observation Point since the Metering Process (re-)initialization for this Observation Point. The number of octets includes HTTP message header(s) and message body.

Abstract Data Type: unsigned64

Data Type Semantics: totalCounter

ElementId: TBD09

Status: current

Reference:

[2.10.](#) dnsQueryName

Description:

The domain name a DNS query is made for.

Abstract Data Type: string

Data Type Semantics:

ElementId: TBD10

Status: current

Reference: [[RFC1035](#)]

[2.11.](#) dnsQueryType

Description:

A two octet code which specifies the type of a DNS query.

Abstract Data Type: unsigned16

Data Type Semantics: identifier

Fan

Expires January 30, 2014

[Page 6]

Internet-Draft Application Layer Information Elements

July 2013

ElementId: TBD11

Status: current

Reference: [[RFC1035](#)]

[2.12.](#) dnsQueryDeltaCount

Description:

The number of incoming DNS query messages since the previous report (if any) for this Flow at the Observation Point. The number is counted at the DNS protocol layer, so possible fragmentation at lower layer must not affect the counting.

Abstract Data Type: unsigned64

Data Type Semantics: deltaCounter

ElementId: TBD12

Status: current

Reference:

[2.13.](#) dnsQueryTotalCount

Description:

The total number of incoming DNS query message for this Flow at the Observation Point since the Metering Process (re-)initialization for this Observation Point. The number is counted at the DNS protocol layer, so possible fragmentation at lower layer must not affect the counting.

Abstract Data Type: unsigned64

Data Type Semantics: totalCounter

ElementId: TBD13

Status: current

Reference:

[3.](#) Security Considerations

TBD.

[4.](#) IANA Considerations

The document makes a request to IANA to register the Information Elements defined in [section 2](#).

[5](#). Normative References

- [I-D.ietf-ipfix-information-model-rfc5102bis]
Claise, B. and B. Trammell, "Information Model for IP Flow Information eXport (IPFIX)", [draft-ietf-ipfix-information-model-rfc5102bis-10](#) (Work in Progress), February 2013.
- [I-D.ietf-ipfix-protocol-rfc5101bis]
Claise, B., Trammell, B., Aitken, P., Bryant, S., Leinen, S., and T. Dietz, "Specification of the IP Flow Information eXport (IPFIX) Protocol for the Exchange of Flow Information", [draft-ietf-ipfix-protocol-rfc5101bis-08](#) (Work in Progress), June 2013.
- [RFC1035] Mockapetris, P., "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION", [RFC 1035](#), November 1987.
- [RFC2616] Fielding, R., Gettys, J., and J. Mogul, "Hypertext Transfer Protocol -- HTTP/1.1", [RFC 2616](#), June 1999.
- [RFC5322] Resnick, P., "Internet Message Format", [RFC 5322](#), October 2008.

Author's Address

Peng Fan
China Mobile
32 Xuanwumen West Street, Xicheng District
Beijing 100053
P.R. China

Email: fanpeng@chinamobile.com