NetFlow and IxFlow Fields

Standard Mandatory Fields

NetFlow Field Name	IPFIX ID	Version	Data Type	Length	Reverse field for Bidirectional	Added in Version	Description
Octets	1	9	UINT64	8		1.0.0	Number of Octets for a flow
Packets	2	9	UINT64	8		1.0.0	Number of Packets for a flow
Protocol	4	9	UINT8	1		1.0.0	Protocol
tcpControlBits	6	9	UINT8	1		1.5.0	TCP Control Bits
SrcPort	7	9	UINT16	2		1.0.0	Source Port
sourceIPv4Address	8	9	UINT32	4		1.0.0	Source Address (for IPv4 flow)
sourceIPv6Address	27	9	UINT32	4		1.0.0	Source Address (for IPv6 flow)
InputInt	10	9	UINT32	4		1.0.0	Ingress Interface
DstPort	11	9	UINT16	2		1.0.0	Destination Port
destinationIPv4Address	12	9	UINT32	4		1.0.0	Destination Address (for IPv4 flow)
destinationIPv6Address	28	9	UINT32	4		1.0.0	Destination Address (for IPv6 flow)
OutputInt	14	9	UINT32	4		1.0.0	Egress Interface
SrcAS	16	9	UINT32	4		1.1.0	BGP Source AS Number
DstAS	17	9	UINT32	4		1.1.0	BGP Destination AS Number
icmpTypeCodeIPv4	32	9	UINT16	2	yes	1.5.4	ICMP type (in upper octet) and code (in lower octet)
Flow End Reason	136	10	UINT8	1		1.3.2	Reason for Flow termination.
icmpTypeCodeIPv6	139	10	UINT16	2	yes	1.5.4	ICMP type (in upper octet) and code (in lower octet)
flowStartMilliseconds	152	10	UINT64	8		1.0.0	The absolute timestamp of the first packet of this Flow
flowEndMilliseconds	153	10	UINT64	8		1.0.0	The absolute timestamp of the last packet of this Flow

Optional Fields

IxFlow Field	IXIA-IPFIX ID	Data Type	Length	Added in Version	Max Length	Description
L7 Application ID	110	UINT32	4	1.0.0		Application Identification number. Note: since applications are dynamically detected, this ID is unique to each exporter

L7 Application Name	111	STRING	Variable	1.0.0	128	Application name, truncated at 128 characters.
Source IP Country Code	120	STRING	4	1.0.0	2	2 Letter country code for the source IP address
Source IP Country Name	121	STRING	Variable	1.0.0	32	Country name for the source IP address. Truncated at 128 characters.
Source IP Region Code	122	STRING	4	1.0.0	4	2 Letter region code for the source IP address
Source IP Region Name	123	STRING	Variable	1.0.0	48	Region name for the source IP address. Truncated at 128 characters.
Source IP City Name	125	STRING	Variable	1.0.0	48	City name for the source IP address. Truncated at 128 characters.
Source IP Latitude	126	FLOAT32	4	1.0.0		Latitude for the source IP address
Source IP Longitude	127	FLOAT32	4	1.0.0		Longitude for the source IP address
Destination IP Country Code	140	STRING	4	1.0.0	2	2 Letter country code for the destination IP address.
Destination IP Country Name	141	STRING	Variable	1.0.0	32	Country name for the destination IP address. Truncated at 128 characters.
Destination IP Region Code	142	STRING	4	1.0.0	4	2 Letter region code for the destination IP address.
Destination IP Region Name	143	STRING	Variable	1.0.0	48	Region name for the destination IP address. Truncated at 128 characters.
Destination IP City Name	145	STRING	Variable	1.0.0	48	City name for the destination IP address. Truncated at 128 characters.
Destination IP Latitude	146	FLOAT32	4	1.0.0		Latitude for the destination IP address
Destination IP Longitude	147	FLOAT32	4	1.0.0		Longitude for the destination IP address
OS Device ID	160	UINT8	1	1.0.0		Unique ID for each OS
OS Device Name	161	STRING	Variable	1.0.0	128	String containing OS name, truncated at 128 characters.
Browser ID	162	UINT8	1	1.0.0		Unique ID for each browser type
Browser Name	163	STRING	Variable	1.0.0	128	Unique Name for each browser type

Reverse Octet Delta Count	176	UINT64	8	1.0.0		When exporting bidirectional flows, this field contains the byte count for the server back to the client side of the connection
Reverse Packet Delta Count	177	UINT64	8	1.0.0		When exporting bidirectional flows, this field contains the packet count for the server back to the client side of the connection
SSL Connection Encryption Type	178	STRING	Variable	1.2.0/1.5.5		When SSL decryption is enabled, the encryption type: 'Encrypted' - flow encrypted and was not decrypted 'Decrypted' - flow encrypted and was decrypted by ATIP 'Cleartext' - flow not encrypted Starting 1.5.5, this field will be available even if SSL decryption is turned off or even when not licensed
SSL Encryption Cipher Name	179	STRING	Variable	1.2.0/1.5.5	128	For decrypted flows only, the name of the cipher used for decryption. Truncated at 128 characters. Starting 1.5.5, this field will be available even if SSL decryption is turned off or even when not licensed
SSL Encryption Key Length	180	UINT16	2	1.2.0/1.5.5		For decrypted flows only, the bit length of the key used Starting 1.5.5, this field will be available even if SSL decryption is turned off or even when not licensed
User Agent	182	STRING	Variable	1.3.3	128	The user agent sent in the request HTTP header, truncated at 128 characters.
Host Name	183	STRING	Variable	1.3.3	128	The hostname field sent in the request HTTP header, truncated at 128 characters.
URI	184	STRING	Variable	1.3.3	128	The URI sent in the request HTTP header, truncated at 128 characters.

DNS Text	185	STRING	Variable	1.3.3	128	The DNS TXT field sent as part of a DNS request /response, truncated at 128 characters.
Source AS NAME	186	STRING	Variable	1.5.0	128	The Service Provider name corresponding to the AS number of the source IP
Destination AS NAME	187	STRING	Variable	1.5.0	128	The Service Provider name corresponding to the AS number of the destination IP
Transaction Latency	188	UINT32	4	1.5.0		Transaction latency of the first transaction in a bidirectional flow.
DNS Query HostName	189	STRING	Variable	1.5.4	256	Names from the Query section of DNS messages (multiple unique occurrences are appended with commas)
DNS Response HostName	190	STRING	Variable	1.5.4	256	Names from the Answer section of DNS messages (multiple unique occurrences are appended with commas)
DNS Classes	191	STRING	Variable	1.5.4	16	String representation of the record class types e.g. IN, CS, CH, HS (multiple unique occurrences are appended with commas)
Threat Type	192	STRING	Variable	2.1.0	16	String showing the threat type for a flow matching a rap sheet IP. e.g. "malware", "phishing", "botnet"
Threat IPv4	193	IPv4	4	2.1.0	4	The IP corresponding to the threat, one endpoint of the flow.
Threat IPv6	194	IPv6	16	2.1.0	16	The IP corresponding to the threat, one endpoint of the flow.
HTTP Session	195	SUBTEMPLATELIST	Variable		65535	List of fields for each HTTP Session.
Request Time	196	UINT32	4		4	Time that the request arrives.
DNS Record	197	SUBTEMPLATELIST	Variable		65535	This will provide the details of individual Answer records in a DNS response.
DNS Name	198	STRING	Variable		128	The "Name" field in a DNS response

DNS IPv4 Address	199	IPv4	4		4	The "Address" field in a A or AAAA record
DNS IPv6 Address	200	IPv6	16		16	The "Address" field in a A or AAAA record
SNI	201	STRING	Variable		128	Server Name Identification for TLS
httpStatusCode	457	UINT16	2		2	Status code response from server (200, 404, etc)
httpRequestMethod	459	STRING	Variable		8	Request method in request from client (GET, POST, PUT, etc)
httpMessageVersion	462	STRING	Variable		10	HTTP/1.x or HTTP /2.x

Netflow Enhancement for SSL Encryption Fields (ATIP 1.5.5)